**Set theory interlude:**

A map \( f : S \to T \) is:
- **injective** if \( \forall a, b \in S \), \( f(a) = f(b) \Rightarrow a = b \). (or: \( a \neq b \Rightarrow f(a) \neq f(b) \)). Write \( f : S \hookrightarrow T \).
- **surjective** if \( \forall c \in T \exists a \in S \) such that \( f(a) = c \). Write \( f : S \to T \).
- A **bijection** \( f : S \leftrightarrow T \) if both hold.

Say two sets \( S, T \) have the same **cardinality** if \( \exists \) bijection \( f : S \to T \), and write \( |S| = |T| \).

If there exists an injection \( f : S \inj T \) then we write \( |S| \leq |T| \). This notation is legit thanks to the Schröder-Bernstein theorem:

If there exist injective maps \( f : S \inj T \) and \( g : T \inj S \) then \( |S| = |T| \).

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

**Ex:** \( \mathbb{N}, \mathbb{Z}, \mathbb{Q} \) all have the same cardinality, they are called **countably infinite**.

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

For \( \mathbb{Q} \), first understand how to enumerate \( \mathbb{N} \times \mathbb{N} = \text{pairs of integers} \).

**On the other hand, IR is uncountable**, using Cantor's diagonal argument:

No map \( f : \mathbb{N} \to \mathbb{R} \) can be surjective, because:

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

Then let \( y = b_0 b_1 b_2 b_3 \ldots \) where we choose \( b_i \neq a_{ij} \) 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 \( S \)**).

\[
\{0,1\}^S = \{\text{maps } f : S \to \{0,1\}\}
\]

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

Thus, if \( S \) is infinite then \( |\mathcal{P}(S)| > |S| \).

**Proof (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 \( a \notin f(a) \), contradiction. So \( A \notin f(S) \) \( \forall \) surjection.
Defn: A group $G$ is a set with an operation $G \times G \rightarrow G$ such that

1. identity: $\exists e \in G$ s.t. $\forall a \in G$, $ae = ea = a$.
2. inverse: $\forall a \in G$, $\exists a^{-1} \in G$ s.t. $ab = ba = e$.
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 $G \times H = \{ (g, h) \mid g \in G, h \in H \}$

  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: $\mathbb{Z}^n = \{ (a_1, \ldots, a_n) \mid a_i \in \mathbb{Z} \}$,
  $\langle a_1, a_n \rangle + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$

  (similarly $\mathbb{Q}^n$, $\mathbb{R}^n$, etc. with componentwise addition).

* Given infinitely many groups $G_1, G_2, G_3, \ldots$, there are two different notions:

  \begin{enumerate}
  \item the direct product \( \prod_{i=1}^{\infty} G_i = \{ (a_i) \mid a_i \in G_i \} \)
  
  \item the direct sum \( \bigoplus_{i=1}^{\infty} G_i = \{ (a_i) \mid a_i \in G_i \text{, all but finitely many are } \text{identity} \} \)
  \end{enumerate}

Ex: consider $G_0 = G_1 = \ldots = (\mathbb{R}, +)$, depth ($a_0, a_1, a_2, \ldots$) by $\Sigma x^i$.

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:

**Defn:** A subgroup $H$ of a group $G$ is a subset $H \subseteq G$ 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:

- $(\mathbb{Z}, +) \subseteq (\mathbb{Q}, +) \subseteq (\mathbb{R}, +)$.
- $(\mathbb{Q}^*, x) \subseteq (\mathbb{R}^*, x) \subseteq (\mathbb{C}^*, x) \supset (\mathbb{S}^1, x)$
- $\{ e \} \leq G$ trivial subgroup

- $H_i \subseteq G_i \Rightarrow H_1 \times \ldots \times H_n \subseteq G_1 \times \ldots \times G_n$
- $\bigoplus G_i \leq \prod G_i$.
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.

Proof: 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.

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

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

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, $\langle S \rangle = \bigcap_{H \supseteq S \text{ subgroup}} H$.

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 $\langle S \rangle = \{ a_1 \cdots a_k \mid a_i \in S \cup S^{-1} \}$

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: $SL_2(\mathbb{Z}) = \{ (a b) \mid a, b, c, d \in \mathbb{Z} \text{ and } ad - bc = 1 \}$ can be generated by two elements! [exercise! fairly hard without hint]

Homomorphisms:

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

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

$G \times G \xrightarrow{\phi \times \phi} H \times H$  "commutative diagram" means $G \xleftarrow{\phi} G$, give the same map:

$M_G \downarrow \phi \downarrow M_H$

\[ G \xrightarrow{\phi} H \]

It doesn't matter if we multiply first or apply $\phi$ first.
* An **isomorphism** is a bijective homomorphism (two isomorphic groups are "structurally the same").
* An **automorphism** is an isomorphism $G \to G$.

**Examples:**
- All groups of order 2 are isomorphic! $S_2 = \{(\text{id}, (12)) \mapsto ((\pm 1), x) = (\mathbb{Z}_2^+, +)\}$
- Because the table is always:

$$
\begin{array}{c|ccc}
 & e & x \\
\hline
\text{e} & e & e \\
\text{x} & e & x \\
\end{array}
$$

- $S_3$ is the symmetries of a triangle (permutation of vertices).

**Example:**
- $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto a$ and $n$ (remainder of Euclidean division by $n$).
- If $n|n$, $\mathbb{Z}/m \to \mathbb{Z}/n$, similarly (e.g., $\mathbb{Z}/100 \to \mathbb{Z}/10$).
- Determinant: $GL_n(\mathbb{R}) \to (\mathbb{R}_k^*, \cdot) \quad (\det(AB) = \det(A) \det(B))$.

**Definition:**
- The **kernel** 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.)
- $\varphi$ is injective iff $\ker(\varphi) = \{e_G\}$ (wrt: $\varphi(a) = \varphi(b) \iff a^{-1}b \in \ker(\varphi)$).

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

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

**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 $a$.

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

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 $\langle a \rangle = \{a^n \mid n = 0, \ldots, k-1\}$ is isomorphic to $\mathbb{Z}/k$.

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

**Example:** $\mathbb{Z}/6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ (observe: $(1,1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ has order 6, so generates).

$a \mapsto (a \mod 2, a \mod 3)$

Similarly, $\gcd(m,n) = 1 \Rightarrow \mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$. But $\mathbb{Z}_2 \times \mathbb{Z}_2 \not\cong \mathbb{Z}_4$.

$x + x = 0 \forall x \text{ vs. } 1 + 1 \neq 0$. 

\[\text{do not confuse order of } a \in G \text{ with order of } G (|G|)\]

Through, order($a$) = $|\langle a \rangle|$.