1 Lecture 3: January 27, 2026

Lecture Overview: We develop the set-theoretic foundations needed for analysis. We define **functions** as special relations and introduce key properties: surjectivity, injectivity, and bijectivity. Using bijections, we define when two sets have the same **cardinality**, leading to the notions of **finite**, **infinite**, and **countable** sets.

1.1 Functions

Section Overview: We define functions as relations with a uniqueness property, introduce images and preimages, and classify functions as injective (one-to-one), surjective (onto), or bijective (both).

Definition 1.1. A **function** $f : A \to B$ is a relation $R \subseteq A \times B$ such that for all $x \in A$, there exists a unique $y \in B$ with $(x, y) \in R$. This y is denoted $f(x)$. The set A is called the **domain** of f, and B is the **codomain** (or **range**).

Remark 1.2. Not all relations are functions. A relation fails to be a function if some element of A maps to multiple elements of B, or to no element at all.

Definition 1.3. Let $f : A \to B$ be a function.

- If $E \subseteq A$, the **image** of E under f is $f(E) = \{f(x) : x \in E\}$.
- If $F \subseteq B$, the **preimage** of F under f is $f^{-1}(F) = \{x \in A : f(x) \in F\}$.

Definition 1.4. Let $f : A \to B$ be a function.

- f is **surjective** (or **onto**) if $f(A) = B$, i.e., for every $y \in B$, there exists $x \in A$ with $f(x) = y$.
- f is **injective** (or **one-to-one**) if $f(x_1) = f(x_2)$ implies $x_1 = x_2$, i.e., distinct inputs map to distinct outputs.
- f is **bijective** if it is both injective and surjective.

1.2 Equivalence Relations

Section Overview: We review equivalence relations and observe how function properties relate to composition and inverses.

Remark 1.5. Recall from Lecture 1 that an equivalence relation satisfies:

- **Reflexivity:** $x \sim x$ (like the identity function)
- **Symmetry:** $x \sim y \Rightarrow y \sim x$ (like invertible functions: if $f : A \to B$, then $f^{-1} : B \to A$)
- **Transitivity:** $x \sim y$ and $y \sim z \Rightarrow x \sim z$ (like composition: $f : A \to B$ and $g : B \to C$ give $g \circ f : A \to C$)

1.3 Cardinality

Section Overview: We define cardinality using bijections, then classify sets as finite, infinite, or countable.

Definition 1.6. Two sets A and B have the same **cardinality**, written $A \sim B$, if there exists a bijection $f : A \to B$.

Definition 1.7. Let $[n] = \{1, 2, 3, \dots, n\}$. We say that a set A is:

1. **finite** if there exists $n \in \mathbb{N}$ such that $A \sim [n]$,
2. **infinite** if A is not finite,
3. **countable** if $A \sim \mathbb{N}$.

Example. $\mathbb{Z}$ is countable. We can list the integers as:

$$0, 1, -1, 2, -2, 3, -3, \dots$$

This defines a bijection $f : \mathbb{N} \to \mathbb{Z}$ given by

$$f(n) = \begin{cases} -\frac{n}{2} & \text{if } n \text{ is even} \\ \frac{n+1}{2} & \text{if } n \text{ is odd} \end{cases}$$

(where we start $\mathbb{N}$ at 0). Thus $\mathbb{Z} \sim \mathbb{N}$, so $\mathbb{Z}$ is countable.

Definition 1.8. A **sequence** is a function $f : \mathbb{N} \to X$ where X is some set. If we denote $f(n)$ by x_n, then we write the sequence as $(x_n)_{n=1}^{\infty}$.

Remark 1.9. If A is a countable set, then there exists a surjection $f : \mathbb{N} \to A$. We say that A can be **arranged in a sequence**: the elements of A can be listed as $f(1), f(2), f(3), \dots$

Note: The **set difference** $A \setminus B$ (read "A minus B") is defined as

$$A \setminus B = \{x \in A : x \notin B\}.$$

Theorem 1.10. *Every infinite subset of a countable set is countable.*

Proof. Let A be a countable set and let $B \subseteq A$ be infinite. Since A is countable, we can arrange its elements as a sequence $(x_n)_{n=1}^{\infty}$.

We construct a bijection $f : \mathbb{N} \to B$ inductively. Let $B_0 = \emptyset$. For each $k \geq 1$:

- Let $n_k = \min\{n \in \mathbb{N} : x_n \in B \setminus B_{k-1}\}$
- Define $f(k) = x_{n_k}$
- Set $B_k = B_{k-1} \cup \{x_{n_k}\}$

At each step, x_{n_k} is assigned position $k = |B_{k-1}| + 1$ in our enumeration of B. Since B is infinite, we never exhaust it, so each n_k exists.

This f is a bijection: it is injective since each element is added exactly once, and surjective since every element of B appears at some position n in the sequence (x_n) and will eventually be enumerated.

Thus $B \sim \mathbb{N}$, so B is countable. $\square$

1.4 Unions and Intersections of Sets

Section Overview: We define unions and intersections of collections of sets, including arbitrary (possibly infinite) unions and intersections.

$A \cup B$ (union) $A \cap B$ (intersection)

Definition 1.11. Let A and B be sets, and let $f : A \to \mathcal{P}(B)$ be a function assigning to each $\alpha \in A$ a subset $f(\alpha) \subseteq B$. We define:

- The **union** of the family is

$$\bigcup_{\alpha \in A} f(\alpha) = \{x \in B : x \in f(\alpha) \text{ for some } \alpha \in A\}.$$

- The **intersection** of the family is

$$\bigcap_{\alpha \in A} f(\alpha) = \{x \in B : x \in f(\alpha) \text{ for all } \alpha \in A\}.$$

Theorem 1.12 (De Morgan's Laws)**.** *Let A and B be subsets of a universal set U. Then:*

1. $(A \cup B)^c = A^c \cap B^c$
2. $(A \cap B)^c = A^c \cup B^c$

Proof. We prove (1); the proof of (2) is similar.

($\subseteq$) Let $x \in (A \cup B)^c$. Then $x \notin A \cup B$, so $x \notin A$ and $x \notin B$. Thus $x \in A^c$ and $x \in B^c$, so $x \in A^c \cap B^c$.

($\supseteq$) Let $x \in A^c \cap B^c$. Then $x \in A^c$ and $x \in B^c$, so $x \notin A$ and $x \notin B$. Thus $x \notin A \cup B$, so $x \in (A \cup B)^c$. $\square$

Note: To prove two sets are equal, $X = Y$, a standard technique is the **mutual subset argument**: show $X \subseteq Y$ and $Y \subseteq X$. For each direction, take an arbitrary element of one set and show it belongs to the other.

Theorem 1.13 (Distributive Law)**.** *Let A, B, and C be sets. Then*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Proof. ($\subseteq$) Let $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$. Since $x \in B \cup C$, either $x \in B$ or $x \in C$.

- If $x \in B$, then $x \in A \cap B$, so $x \in (A \cap B) \cup (A \cap C)$.

- If $x \in C$, then $x \in A \cap C$, so $x \in (A \cap B) \cup (A \cap C)$.

($\supseteq$) Let $x \in (A \cap B) \cup (A \cap C)$. Then $x \in A \cap B$ or $x \in A \cap C$.

- If $x \in A \cap B$, then $x \in A$ and $x \in B \subseteq B \cup C$, so $x \in A \cap (B \cup C)$.
- If $x \in A \cap C$, then $x \in A$ and $x \in C \subseteq B \cup C$, so $x \in A \cap (B \cup C)$.

$\square$

1.5 The (Un)countability of Number Systems

Section Overview: We apply our results to the classical number systems. We show $\mathbb{Q}$ is countable (as a countable union of countable sets), but $\mathbb{R}$ is **uncountable** using Cantor's diagonal argument on binary sequences. This reveals a hierarchy of infinities: $|\mathbb{N}| = |\mathbb{Q}| < |\mathbb{R}|$.

Theorem 1.14. *Let $\{E_n\}_{n=1}^{\infty}$ be a sequence of countable sets. Then*

$$\bigcup_{n=1}^{\infty} E_n$$

is countable.

Proof. Since each E_n is countable, we can enumerate its elements as

$$E_n = \{x_{n,1}, x_{n,2}, x_{n,3}, \ldots\}.$$

Arrange all elements in an infinite grid:

$$\begin{array}{cccccc}
 & \color{blue}{1} & \color{blue}{2} & \color{blue}{4} & \color{blue}{7} & \\
E_1: & x_{1,1} & x_{1,2} & x_{1,3} & x_{1,4} & \cdots \\
 & \color{blue}{3} & \color{blue}{5} & \color{blue}{8} & & \\
E_2: & x_{2,1} & x_{2,2} & x_{2,3} & x_{2,4} & \cdots \\
 & \color{blue}{6} & \color{blue}{9} & & & \\
E_3: & x_{3,1} & x_{3,2} & x_{3,3} & x_{3,4} & \cdots \\
 & \color{blue}{10} & & & & \\
E_4: & x_{4,1} & x_{4,2} & x_{4,3} & x_{4,4} & \cdots \\
 & \vdots & \vdots & \vdots & \vdots &
\end{array}$$

We enumerate the union by traversing diagonals: first $x_{1,1}$, then $x_{1,2}, x_{2,1}$, then $x_{1,3}, x_{2,2}, x_{3,1}$, and so on. The k-th diagonal contains all $x_{n,m}$ with $n + m = k + 1$.

This gives a surjection from $\mathbb{N}$ onto $\bigcup_{n=1}^{\infty} E_n$ (skipping repeats if sets overlap). Thus the union is countable. $\square$

Note: The **diagonal argument** is a powerful technique for enumerating countable unions. By arranging elements in a grid and traversing along diagonals, we reduce a "two-dimensional" infinite collection to a "one-dimensional" sequence.

Theorem 1.15. *If A is countable, then A^n is countable for all $n \in \mathbb{N}$.*

Proof. By induction on n.

Base case ($n = 1$): $A^1 = A$ is countable by assumption.

Inductive hypothesis: Assume A^n is countable for some $n \geq 1$.

Inductive step: We show A^{n+1} is countable. Observe that

$$A^{n+1} = A^n \times A.$$

By the inductive hypothesis, A^n is countable, so we can enumerate it as $A^n = \{b_1, b_2, b_3, \ldots\}$. Since A is countable by assumption, we can write $A = \{a_1, a_2, a_3, \ldots\}$. The Cartesian product $A^n \times A$ can then be arranged in a grid:

$$\begin{array}{cccc}
(b_1, a_1) & (b_1, a_2) & (b_1, a_3) & \cdots \\
(b_2, a_1) & (b_2, a_2) & (b_2, a_3) & \cdots \\
(b_3, a_1) & (b_3, a_2) & (b_3, a_3) & \cdots \\
\vdots & \vdots & \vdots & \ddots
\end{array}$$

By the diagonal argument, $A^n \times A$ is countable.

Conclusion: By the principle of mathematical induction, A^n is countable for all $n \in \mathbb{N}$. $\square$

Corollary 1.16. $\mathbb{Q}$ *is countable.*

Proof. For each $n \in \mathbb{N}$, let $E_n = \left\{\frac{m}{n} : m \in \mathbb{Z}\right\}$ be the set of rationals with denominator n. Each E_n is countable (since $E_n \sim \mathbb{Z}$ and $\mathbb{Z}$ is countable). Then

$$\mathbb{Q} = \bigcup_{n=1}^{\infty} E_n$$

is a countable union of countable sets, hence countable. $\square$

Theorem 1.17 ($\mathbb{R}$ is uncountable)**.** *The set of binary sequences $\{0,1\}^{\mathbb{N}}$ is uncountable.*

Proof. By contradiction. Suppose $\{0,1\}^{\mathbb{N}}$ is countable. Then we can list all binary sequences as $s_1, s_2, s_3, \ldots$ where each $s_n = (s_{n,1}, s_{n,2}, s_{n,3}, \ldots)$:

	pos 1	pos 2	pos 3	pos 4	pos 5		
s_1:	0	1	0	1	1	$\cdots$	
s_2:	1	1	0	0	1	$\cdots$	
s_3:	0	0	1	1	0	$\cdots$	
s_4:	1	0	1	0	0	$\cdots$	
s_5:	0	1	1	1	1	$\cdots$	flip diagonal
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		
d:	1	0	0	1	0	$\cdots$	

Construct a new sequence $d = (d_1, d_2, d_3, \ldots)$ by flipping the diagonal entries:

$$d_n = \begin{cases} 1 & \text{if } s_{n,n} = 0 \\ 0 & \text{if } s_{n,n} = 1 \end{cases}$$

Then d differs from s_n in the n-th position for every $n \in \mathbb{N}$. Thus $d \neq s_n$ for all n, so d is not in our list. But $d \in \{0,1\}^{\mathbb{N}}$, contradicting that our list contains all binary sequences.

Therefore $\{0,1\}^{\mathbb{N}}$ is uncountable. □

Note: This is **Cantor's diagonal argument**. Since there is a bijection between $\{0,1\}^{\mathbb{N}}$ and $\mathbb{R}$ (via binary expansions), this proves $\mathbb{R}$ is uncountable. The key insight is that any proposed enumeration can be "diagonalized" to produce a missing element.

Exercise: An **algebraic number** is a solution to a polynomial equation with coefficients in $\mathbb{Q}$:

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0, \quad a_i \in \mathbb{Q}.$$

Is the set of algebraic numbers countable?

Proof: Yes. We proceed by induction on the degree of the polynomial.

Base case ($n = 1$): A degree-1 polynomial $mx + b = 0$ has solution $x = -b/m \in \mathbb{Q}$. Since $\mathbb{Q}$ is countable, the set of algebraic numbers of degree 1 is countable.

Inductive step: Let A_n denote the set of algebraic numbers that are roots of some polynomial of degree at most n. Assume A_n is countable. Consider numbers of the form

$$\{a + b \cdot \sqrt[n+1]{z} : a, b, z \in A_n\}.$$

This set is countable since A_n^3 is countable (as a finite Cartesian product of a countable set). More generally, the set of polynomials of degree $n+1$ with coefficients in $\mathbb{Q}$ is $\mathbb{Q}^{n+2}$, which is countable. Each such polynomial has at most $n+1$ roots, so the roots form a countable union of finite sets, hence A_{n+1} is countable.

Conclusion: The set of all algebraic numbers is $\bigcup_{n=1}^{\infty} A_n$, a countable union of countable sets, hence countable.

Note: A real number that is *not* algebraic is called **transcendental**. Since the algebraic numbers are countable but $\mathbb{R}$ is uncountable, transcendental numbers must exist—in fact, "most" real numbers are transcendental! Examples include π, e, and $\tau = 2\pi$. Proving that a specific number is transcendental is typically very difficult: Lindemann proved π is transcendental in 1882, and Hermite proved e is transcendental in 1873.

Remark 1.18. Recall the **Cantor set** from Lecture 2: the set of all points in $[0,1]$ whose ternary expansion uses only the digits 0 and 2. The Cantor set is in bijection with $\{0,2\}^{\mathbb{N}} \sim \{0,1\}^{\mathbb{N}}$ (just map $0 \mapsto 0$ and $2 \mapsto 1$). By the same diagonal argument, the Cantor set is uncountable—despite being "sparse" (it contains no intervals and has measure zero).