Honors Calculus 1610

Lecture 2: Set Theory and Axioms for Numbers

August 31, 2026

Today

- Practice proving an identity about sets.
- See why naive set theory has limits.
- Ask what it means to specify the natural and real numbers.

Warm-up: a set identity

For sets A, B, and C, show that

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

As before, prove equality by proving two containments:

$$A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C)$$

and

$$(A \setminus B) \cap (A \setminus C) \subseteq A \setminus (B \cup C).$$

First containment

Suppose that $x \in A \setminus (B \cup C)$. Then

$$x \in A \qquad \text{and} \qquad x \notin B \cup C.$$

We will use the following lemma:

$$x \notin B \cup C \quad \Longrightarrow \quad x \notin B \quad \text{and} \quad x \notin C.$$

Therefore $x \in A \setminus B$ and $x \in A \setminus C$, so

$$x \in (A \setminus B) \cap (A \setminus C).$$

Lemma

To show that

$$x \notin B \cup C \implies x \notin B,$$

argue by contradiction. If $x \in B$, then $x \in B \cup C$, contrary to the hypothesis.

The same argument gives $x \notin C$. Equivalently, this is the contrapositive of

$$x \in B \implies x \in B \cup C.$$

Second containment

Suppose that

$$x \in (A \setminus B) \cap (A \setminus C).$$

Then $x \in A$, $x \notin B$, and $x \notin C$. Hence $x \notin B \cup C$, since an element of $B \cup C$ belongs to B or to C.

Thus

$$x \in A \setminus (B \cup C),$$

proving the second containment and therefore the identity.

A limit of naive set theory: Berry's paradox

Consider the set

$$S = \{n \in \mathbb{N} \mid n \text{ can be described by a sentence with at most 100 words}\}\,.$$

There are only finitely many sentences with at most 100 words, so S should be finite. Let N be the smallest natural number not in S.

But the phrase "the smallest natural number not in S" appears to describe N using fewer than 100 words.

Russell's paradox

Let

$$X = \{S \mid S \notin S\}.$$

Does X belong to X?

- If $X \in X$, then the defining condition gives $X \notin X$.
- If $X \notin X$, then the defining condition gives $X \in X$.

Set theory as a foundation

- Late-nineteenth-century work made sets central to modern mathematics.
- The paradoxes showed that naive set formation needs constraints.
- Zermelo–Fraenkel set theory, together with the Axiom of Choice, is usually abbreviated ZFC.

A foundational question remains: how do we know that a proposed system of axioms is consistent?

What is a number?

There are two related questions:

1. What properties do we want numbers to have?
2. Is there an actual consistent system with those properties?

We begin with the natural numbers and Peano's axioms.

Peano's axioms: the starting point

The natural numbers come with a distinguished element 0 and a successor function

$$S\colon \mathbb{N} \longrightarrow \mathbb{N}, \qquad S(n) = n + 1 \text{ intuitively.}$$

1. $0 \in \mathbb{N}$.
2. If $n \in \mathbb{N}$, then $S(n) \in \mathbb{N}$.
3. $0 \neq S(n)$ for every $n \in \mathbb{N}$.
4. If $n \neq m$, then $S(n) \neq S(m)$.

Peano's fifth axiom: induction

Let P be a proposition about natural numbers. If

a. $P(0)$ is true, and
b. whenever $P(n)$ is true, $P(S(n))$ is true,

then $P(n)$ is true for every natural number n.

This is the principle of mathematical induction.

Constructing natural numbers from sets

One standard set-theoretic construction defines

$$0 = \varnothing, \qquad 1 = \{0\} = \{\varnothing\},$$

and then

$$2 = \{0, 1\}, \qquad 3 = \{0, 1, 2\}, \qquad \dots$$

Thus each natural number is the set of all earlier natural numbers.

Care needs to be taken to show that this satisfies the prior system of axioms.

The real numbers

The real numbers should form a

complete ordered field.

Today we begin with the field axioms. The order and completeness axioms are additional structure that we will return to later.

Field axioms: operations and laws

A field is a set F equipped with addition and multiplication. If $a, b \in F$, then $a + b \in F$ and $ab \in F$.

Commutative laws:

$$a + b = b + a, \qquad ab = ba.$$

Associative laws:

$$(a + b) + c = a + (b + c), \qquad (ab)c = a(bc).$$

Distributive law:

$$a(b + c) = ab + ac.$$

Field axioms: identities and inverses

The following are also part of the field axioms.

Identities: there exist elements $0, 1 \in F$ such that, for every $a \in F$,

$$a + 0 = a, \qquad a \cdot 1 = a.$$

Additive inverses: every $a \in F$ has an element $-a \in F$ with

$$a + (-a) = 0.$$

Multiplicative inverses: every nonzero $a \in F$ has an element $a^{-1} \in F$ with

$$aa^{-1} = 1.$$

Cancellation for addition

Theorem

If $a, b, c \in F$ and $a + b = a + c$, then $b = c$.

Add $-a$ to both sides:

$$\begin{aligned}(-a) + (a + b) &= (-a) + (a + c),\\ ((-a) + a) + b &= ((-a) + a) + c,\\ 0 + b &= 0 + c.\end{aligned}$$

Therefore $b = c$.

Cancellation for multiplication

Lemma

If $ax = bx$ and $x \neq 0$, then $a = b$.

Since $x \neq 0$, it has a multiplicative inverse x^{-1}. Multiply both sides by x^{-1}:

$$(ax)x^{-1} = (bx)x^{-1}.$$

By associativity and $xx^{-1} = 1$, this gives $a = b$.

An example theorem about fractions

Division by a nonzero element is shorthand for multiplication by its inverse:

$$\frac{a}{b} = ab^{-1} \qquad (b \neq 0).$$

Theorem

If $b, c \neq 0$, then

$$\frac{a}{b} = \frac{ac}{bc}.$$

Proof: the common factor is nonzero

Suppose $bc = 0$. Multiplying by c^{-1} gives

$$b = (bc)c^{-1} = 0 \cdot c^{-1} = 0,$$

which contradicts $b \neq 0$. Hence $bc \neq 0$.

Proof: multiply the left-hand side by bc

$$\begin{aligned}\left(\frac{a}{b}\right)(bc) &= (ab^{-1})(bc) \\ &= a(b^{-1}b)c && \text{(commutativity and associativity)} \\ &= a \cdot 1 \cdot c \\ &= ac.\end{aligned}$$

An example theorem about fractions

Continuing the proof,

$$\begin{aligned} \left(\frac{ac}{bc}\right)(bc) &= (ac)(bc)^{-1}(bc) = ac\big((bc)^{-1}(bc)\big) && \text{(associativity)} \\ &= ac \cdot 1 \\ &= ac. \end{aligned}$$

Thus

$$\left(\frac{a}{b}\right)(bc) = \left(\frac{ac}{bc}\right)(bc).$$

Since $bc \neq 0$, multiplicative cancellation gives $\frac{a}{b} = \frac{ac}{bc}$.