

# 1 Lecture 1: January 20, 2026

**Lecture Overview:** We begin by proving  $\sqrt{2}$  is irrational, motivating the need for a number system without “gaps.” This leads us to define **ordered sets** and the crucial **Least Upper Bound Property (LUBP)**—the defining feature of  $\mathbb{R}$  that  $\mathbb{Q}$  lacks. We then introduce **fields** as algebraic structures with addition and multiplication, and combine these ideas into **ordered fields**. The real numbers are the unique complete ordered field.

## 1.1 Ordered sets and the least-upper-bound property

**Section Overview:** This section motivates the need for the real numbers by showing that  $\mathbb{Q}$  has “gaps”— $\sqrt{2}$  is irrational, yet we can get arbitrarily close to it with rationals. We develop the machinery of **ordered sets**: partial orders, total orders, upper/lower bounds, and the supremum/infimum. The central concept is the **Least Upper Bound Property (LUBP)**: every non-empty bounded-above subset has a supremum. This property distinguishes  $\mathbb{R}$  from  $\mathbb{Q}$  and is the foundation for all of real analysis. We prove that LUBP implies GLBP.

Consider the ancient problem from Greek times: can we write  $\sqrt{2}$  as a quotient of two natural numbers?

**Theorem 1.1.**  $\sqrt{2}$  is irrational; that is, there do not exist  $p, q \in \mathbb{N}$  such that  $\sqrt{2} = \frac{p}{q}$ .

*Proof.* Suppose, for contradiction, that  $\sqrt{2} = \frac{p}{q}$  for some  $p, q \in \mathbb{N}$  with  $\gcd(p, q) = 1$  (i.e., the fraction is in lowest terms).

Then  $2 = \frac{p^2}{q^2}$ , so  $p^2 = 2q^2$ .

This means  $p^2$  is even, so  $p$  is even. Write  $p = 2k$  for some  $k \in \mathbb{N}$ .

Then  $(2k)^2 = 2q^2$ , so  $4k^2 = 2q^2$ , hence  $q^2 = 2k^2$ .

This means  $q^2$  is even, so  $q$  is even.

But then both  $p$  and  $q$  are even, contradicting  $\gcd(p, q) = 1$ . □

Now consider two sets:

$$A = \{p \in \mathbb{Q} : p > 0 \text{ and } p^2 < 2\}, \quad B = \{p \in \mathbb{Q} : p > 0 \text{ and } p^2 > 2\}.$$

**Proposition 1.2.** A contains no largest element and B contains no smallest element.

*Proof.* Let  $p_0 \in A$ . Define

$$q = p_0 + \frac{2 - p_0^2}{p_0^2 + 2}.$$

Since  $p_0 \in A$ , we have  $p_0^2 < 2$ , so  $2 - p_0^2 > 0$ . Thus  $q > p_0$ .

We claim  $q \in A$ , i.e.,  $q^2 < 2$ . One can verify that

$$q^2 - 2 = \frac{(p_0^2 - 2)^2 \cdot (\text{positive})}{(p_0^2 + 2)^2}$$

which shows  $q^2 < 2$  when  $p_0^2 < 2$ .

Hence  $A$  has no largest element.

A similar argument shows  $B$  has no smallest element. □

**Definition 1.3** (1.3). If  $A$  is any set, we write  $x \in A$  to say that  $x$  is a **member** of  $A$ . Otherwise,  $x \notin A$ . The set that contains no elements is called the **empty set**, denoted  $\emptyset$ . If  $A \neq \emptyset$ , we say that  $A$  is **non-empty**.

If  $A, B$  are sets and  $\forall x \in A$  we have  $x \in B$ , we say that  $A \subset B$ , or  $A$  is a **subset** of  $B$ . If there exists an element  $x \in B$  with  $x \notin A$ , then  $A$  is a **proper subset** of  $B$ , denoted  $A \subsetneq B$ .

**Example.**  $3 \in \mathbb{N}$ , but  $-1 \notin \mathbb{N}$ . We have  $\mathbb{N} \subset \mathbb{Z}$  and  $\mathbb{N} \subsetneq \mathbb{Z}$  (since  $-1 \in \mathbb{Z}$  but  $-1 \notin \mathbb{N}$ ).

**Definition 1.4.** A **binary relation** on a set  $S$  is a set of ordered pairs  $\langle x, y \rangle$  with  $x, y \in S$ .

**Example.** On  $\mathbb{Z}$ , the relation  $\leq$  is the set  $\{\langle x, y \rangle : x, y \in \mathbb{Z}, x \leq y\}$ , e.g.,  $\langle 2, 5 \rangle$  is in the relation.

**Definition 1.5.** A **partial order** is a binary relation  $\leq$  on  $S$  such that:

1. **Reflexive:**  $\forall x \in S, x \leq x$ .
2. **Anti-symmetric:**  $\forall x, y \in S$ , if  $x \leq y$  and  $y \leq x$ , then  $x = y$ .
3. **Transitive:**  $\forall x, y, z \in S$ , if  $x \leq y$  and  $y \leq z$ , then  $x \leq z$ .

**Example.** On the power set  $\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$ , the subset relation  $\subseteq$  is a partial order (but not a total order, since  $\{1\} \not\subseteq \{2\}$  and  $\{2\} \not\subseteq \{1\}$ ).

**Definition 1.6.** A **total order** is a partial order with the additional axiom that any two elements are comparable. That is, for any  $x, y \in S$ , either  $x \leq y$  or  $y \leq x$  (non-exclusive).

**Example.** The usual  $\leq$  on  $\mathbb{R}$  is a total order: for any  $x, y \in \mathbb{R}$ , either  $x \leq y$  or  $y \leq x$ .

**Definition 1.7.** An **ordered set** is a set equipped with a total order.

**Example.**  $(\mathbb{Q}, \leq)$  and  $(\mathbb{R}, \leq)$  are ordered sets.

**Definition 1.8.** Suppose  $S$  is an ordered set and  $E \subset S$ . If there exists  $\beta \in S$  such that  $x \leq \beta$  for all  $x \in E$ , we say  $\beta$  is an **upper bound** of  $E$ . Similarly, if there exists  $\alpha \in S$  such that  $\alpha \leq x$  for all  $x \in E$ , we say  $\alpha$  is a **lower bound** of  $E$ .

**Example.** Let  $E = (0, 1) \subset \mathbb{R}$ . Then  $1, 2, 100$  are all upper bounds of  $E$ , and  $0, -5$  are lower bounds of  $E$ .

**Definition 1.9.** Suppose  $S$  is an ordered set and  $E \subset S$  is bounded above. If there exists  $\alpha \in S$  such that:

1.  $\alpha$  is an upper bound of  $E$ , and
2. if  $\gamma < \alpha$ , then  $\gamma$  is not an upper bound of  $E$ ,

then  $\alpha$  is called the **least upper bound** of  $E$  (or **supremum**), denoted  $\sup E$ .

**Example.**  $\sup(0, 1) = 1$  and  $\sup[0, 1] = 1$  in  $\mathbb{R}$ .

**Definition 1.10.** Suppose  $S$  is an ordered set and  $E \subset S$  is bounded below. If there exists  $\alpha \in S$  such that:

1.  $\alpha$  is a lower bound of  $E$ , and
2. if  $\gamma > \alpha$ , then  $\gamma$  is not a lower bound of  $E$ ,

then  $\alpha$  is called the **greatest lower bound** of  $E$  (or **infimum**), denoted  $\inf E$ .

**Example.**  $\inf(0, 1) = 0$  and  $\inf[0, 1] = 0$  in  $\mathbb{R}$ .

*Remark 1.11.* If  $\sup E$  or  $\inf E$  exists, it need not be an element of  $E$ . For example, the set  $A = \{p \in \mathbb{Q} : p > 0, p^2 < 2\}$  has  $\sup A = \sqrt{2}$  (in  $\mathbb{R}$ ), but  $\sqrt{2} \notin A$  since  $\sqrt{2} \notin \mathbb{Q}$ .

**Definition 1.12.** Let  $S$  be an ordered set.

1.  $S$  has the **least upper bound property** if for any non-empty  $E \subset S$  that is bounded above,  $\sup E$  exists in  $S$ .
2.  $S$  has the **greatest lower bound property** if for any non-empty  $E \subset S$  that is bounded below,  $\inf E$  exists in  $S$ .

**Example.**  $\mathbb{R}$  has the LUBP (and hence GLBP). However,  $\mathbb{Q}$  does not: the set  $A = \{p \in \mathbb{Q} : p > 0, p^2 < 2\}$  is bounded above in  $\mathbb{Q}$ , but  $\sup A = \sqrt{2} \notin \mathbb{Q}$ .

**Theorem 1.13** (LUBP implies GLBP). *Suppose  $S$  is an ordered set with the least upper bound property. Let  $B \subset S$ ,  $B \neq \emptyset$ , and suppose  $B$  is bounded below. Let  $L$  be the set of all lower bounds of  $B$ . Then  $\alpha = \sup L$  exists in  $S$ , and  $\alpha = \inf B$ .*

*Proof.* First,  $L \neq \emptyset$  since  $B$  is bounded below.

Second,  $L$  is bounded above: every  $b \in B$  is an upper bound for  $L$  (since if  $\ell \in L$ , then  $\ell \leq b$  by definition of lower bound).

By the LUBP,  $\alpha = \sup L$  exists in  $S$ .

We claim  $\alpha = \inf B$ :

1.  $\alpha$  is a lower bound of  $B$ : For any  $b \in B$ ,  $b$  is an upper bound of  $L$ , so  $\alpha \leq b$  (since  $\alpha$  is the least upper bound of  $L$ ).
2.  $\alpha$  is the greatest lower bound: If  $\gamma > \alpha$  and  $\gamma$  were a lower bound of  $B$ , then  $\gamma \in L$ , so  $\gamma \leq \sup L = \alpha$ , contradicting  $\gamma > \alpha$ . Thus  $\gamma$  is not a lower bound of  $B$ .

Thus  $\alpha = \inf B$ . □

## 1.2 Fields

**Section Overview:** This section introduces the algebraic structure underlying  $\mathbb{R}$ . We define **groups** (sets with an operation having identity, inverses, and associativity) and **fields** (sets with addition and multiplication that behave like we expect from  $\mathbb{Q}$  or  $\mathbb{R}$ ). We sketch how to construct  $\mathbb{N} \rightarrow \mathbb{Z} \rightarrow \mathbb{Q}$  using equivalence relations. The key definition is an **ordered field**: a field that is also an ordered set, allowing us to combine algebraic operations with comparison.  $\mathbb{R}$  is the unique complete ordered field.

**Definition 1.14.** A **binary operation** on  $S$  is a map  $S \times S \rightarrow S$ .

**Definition 1.15.** A **group** is a set  $G$  with a binary operation  $+$  satisfying the following axioms:

1. **Identity:** There exists  $0 \in G$  such that  $a + 0 = 0 + a = a$  for all  $a \in G$ .
2. **Existence of inverse:** For every  $a \in G$ , there exists  $-a \in G$  such that  $a + (-a) = 0$ .

3. **Associativity:** For all  $a, b, c \in G$ ,  $(a + b) + c = a + (b + c)$ .

If we add a fourth axiom:

4. **Commutativity:** For all  $a, b \in G$ ,  $a + b = b + a$ ,

then  $G$  is called an **abelian group**.

**Definition 1.16.** A **field** is a set  $F$  with two binary operations, addition (+) and multiplication ( $\cdot$ ), such that:

1.  $(F, +)$  is an abelian group with identity 0.
2.  $(F \setminus \{0\}, \cdot)$  is an abelian group with identity 1.

3. **Distributivity:** For all  $a, b, c \in F$ ,  $a \cdot (b + c) = a \cdot b + a \cdot c$ .

**Example.**  $\mathbb{Q}$ ,  $\mathbb{R}$ , and  $\mathbb{C}$  are fields.  $\mathbb{Z}$  is not a field (e.g., 2 has no multiplicative inverse in  $\mathbb{Z}$ ).

Zooming out, we can construct the number systems as follows:

The **natural numbers**  $\mathbb{N}$  can be defined by the cardinality of iterated power sets of  $\emptyset$ :

$$0 = |\emptyset|, \quad 1 = |\mathcal{P}(\emptyset)|, \quad 2 = |\mathcal{P}(\mathcal{P}(\emptyset))|, \quad \dots$$

The **integers** are defined as:

$$\mathbb{Z} = \{a - b : a, b \in \mathbb{N}\}.$$

**Definition 1.17.** An **equivalence relation**  $\sim$  on a set  $S$  has the following properties:

1. **Reflexive:**  $x \sim x$  for all  $x \in S$ .
2. **Symmetric:** If  $x \sim y$ , then  $y \sim x$ .
3. **Transitive:** If  $x \sim y$  and  $y \sim z$ , then  $x \sim z$ .

The **rational numbers** are defined as:

$$\mathbb{Q} = \left\{ \frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{N}, q \neq 0 \right\} / \sim$$

We can verify this is an equivalence relation:  $\frac{p}{q} \sim \frac{r}{s}$  if and only if  $ps = rq$ .

**Definition 1.18.** An **ordered field** is a field which is also an ordered set.

**Proposition 1.19.** If  $x > 0$  and  $y < z$ , then  $xy < xz$ .

*Proof.* Since  $y < z$ , we have  $z - y > 0$ . Since  $x > 0$  and  $z - y > 0$ , we have  $x(z - y) > 0$ . Thus  $xz - xy > 0$ , so  $xy < xz$ .  $\square$