MATHEMATICAL METHODS

LECTURE 4

1. Number sets

1.1. **Rational numbers.** The set of rational numbers is defined as

$$\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z} \wedge b \in \mathbb{Z} \setminus \{0\} \right\}.$$

This set consists of all *fractions*. For $a/b \in \mathbb{Q}$ and $c/d \in \mathbb{Q}$ we define $a/b = c/d \iff ad = bc$. Also,

$$\frac{a}{1} = a, \quad \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \left(\frac{a}{b}\right) \cdot \left(\frac{c}{d}\right) = \frac{ac}{bd}.$$

Then $\mathbb{Z} \subset \mathbb{Q}$. Historical motivation for $\mathbb{Q}$ is that we want to solve $bx = a$, where $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus \{0\}$. This equation is not always solvable in $\mathbb{Z}$.

1.2. **Fields and ordered fields, real numbers.** Let $\mathbb{F}$ be a (non-empty) set, equipped with two *binary operations*: *addition* $+$ and *multiplication* $\cdot$. This means that if $x \in \mathbb{F}$ and $y \in \mathbb{F}$, then $x+y \in \mathbb{F}$ and $xy \in \mathbb{F}$, where each of these two operations produces a unique result for each ordered pair $(x, y) \in \mathbb{F} \times \mathbb{F}$. A set $\mathbb{F}$ is called a *field*, if the following rules hold:

(A) Axioms for addition:
  (A1) If $x \in \mathbb{F}$ and $y \in \mathbb{F}$, then $x + y = y + x$;
  (A2) If $x \in \mathbb{F}$, $y \in \mathbb{F}$ and $z \in \mathbb{F}$, then $(x + y) + z = x + (y + z)$;
  (A3) There exists $0 \in \mathbb{F}$ such that $0 + x = x$ for every $x \in \mathbb{F}$;
  (A4) For every $x \in \mathbb{F}$ there exists $-x \in \mathbb{F}$ such that $x + (-x) = 0$;

(M) Axioms for multiplication:
  (M1) If $x \in \mathbb{F}$ and $y \in \mathbb{F}$, then $xy = yx$;
  (M2) If $x \in \mathbb{F}$, $y \in \mathbb{F}$ and $z \in \mathbb{F}$, then $(xy)z = x(yz)$;
  (M3) There exists $1 \in \mathbb{F}$ such that $1 \neq 0$ and $1 \cdot x = x$ for every $x \in \mathbb{F}$;
  (M4) For every $x \in \mathbb{F} \setminus \{0\}$ there exists an element $x^{-1} \in \mathbb{F}$ such that $x \cdot x^{-1} = 1$;

(D) The distributive law: If $x \in \mathbb{F}$, $y \in \mathbb{F}$ and $z \in \mathbb{F}$, then $x(y + z) = xy + xz$.

One can show that in A4 and M4, the existence of *additive inverse* $-x$ and the existence of *multiplicative inverse* x^{-1} is unique with respect to x. These two axioms then imply the following definitions: $x - y = x + (-y)$ and $x/y = x \cdot y^{-1}$. One can also show that $a + x = a + y$ implies $x = y$, and also that $a \cdot x = a \cdot y$ for $a \in \mathbb{F} \setminus \{0\}$ implies $x = y$.

Remark 1. It is obvious that $\mathbb{Q}$ satisfies all of the above axioms, implying that $\mathbb{Q}$ is a field.

Now, we define an *order* on a set A, by saying that there exists a relation $<$ such that:

(1) If $x \in A$ and $y \in A$, then one and only one of the statements $x < y$, $x = y$, $y < x$ is true;
(2) If $x \in A$, $y \in A$, $z \in A$, $x < y$ and $y < z$, then $x < z$.

By an *ordered set* A we mean a set A in which an order $<$ is defined. If $x < y$, then we read this as "x is less than y" or "x is smaller than y". Also, $y > x$ means $x < y$, and $x \leq y$ means $x < y$ or $x = y$. Note that $x \leq y$ is the negation of $x > y$.

(O) An *ordered field* $\mathbb{F}$ is a set with the following properties:
  (O1) $\mathbb{F}$ is a field;
  (O2) $\mathbb{F}$ is an ordered set with order relation $<$;
  (O3) If $x \in \mathbb{F}$, $y \in \mathbb{F}$, $z \in \mathbb{F}$ and $y < z$, then $x + y < x + z$;
  (O4) If $x \in \mathbb{F}$, $y \in \mathbb{F}$, $x > 0$ and $y > 0$, then $xy > 0$.

We call x *positive* if $x > 0$, and *negative* if $x < 0$. The element 0 is neither positive neither negative.

Date: 20. 10. 2026.

Remark 2. Set $\mathbb{Q}$ is an ordered field, where $<$ is the "usual" order. Then $\mathbb{Q}^+ = \{q \in \mathbb{Q}\colon q > 0\}$ is the set of all positive rational numbers, while $\mathbb{Q}^- = \{q \in \mathbb{Q}\colon q < 0\}$ is the set of all negative rational numbers.

One can show that axioms (O) imply the following statements that are true in every ordered field:

(1) If $x > 0$, then $-x < 0$ and vice versa;
(2) If $x < y$ and $y < z$, then $x < z$;
(3) If $x < y$ and $z > 0$, then $xz < yz$;
(4) If $x < y$ and $z < 0$, then $xz > yz$;
(5) If $x \neq 0$, then $x^2 > 0$. In particular, $1 > 0$;
(6) If $0 < x < y$, then $0 < 1/y < 1/x$.
(7) If $x_1 > y_1 > 0$ and $x_2 > y_2 > 0$, then $x_1 x_2 > y_1 y_2$.

Let A be an ordered set, and let $B \subseteq A$. We say that B is *bounded above*, if there exists $M \in A$ such that $x \leq M$ for every $x \in B$. We call M an *upper bound* of B. Similarly, we say that B is *bounded below*, if there exists $m \in A$ such that $x \geq m$ for every $x \in B$, and call such m a *lower bound* of B. Finally, B is *bounded*, if B is bounded above and below. Further, an element $M \in A$ is the *least upper bound* of B if:

(1) M is an upper bound of B;
(2) If $M' < M$ for some $M' \in A$, then M' is not an upper bound of B. Or equivalently, $M \leq M'$ for every upper bound M' of B.

An element $m \in A$ is the *greatest lower bound* of B if:

(1) m is a lower bound of B;
(2) If $m' > m$ for some $m' \in A$, then m' is not a lower bound of B. Or equivalently, $m' \leq m$ for every lower bound m' of B.

In symbols, $\sup B$ and $\inf B$ are the least upper bound and the greatest lower bound of B, respectively. It is not necessary that they exist, even if B is bounded. If they exist, then one can show that they are unique to the set B.

Example 1. If $\sup B$ or $\inf B$ exist, then they does not need to be elements of A. Let $A = \mathbb{Q}$ and

$$B = \left\{ \frac{n-1}{n} \colon n \in \mathbb{N} \right\} = \left\{ 0, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \dots \right\}.$$

Clearly $B \subset A$. Then we have $\sup B = 1$ and $\inf B = 0$. Therefore, $\inf B \in B$ but $\sup B \notin B$.

Example 2. Let $B = \{x \in \mathbb{Q}\colon 0 < x^2 < 2\}$. Obviously, $B \neq \varnothing$. It is also clear that B is bounded: for $x \in B$ we have $0 < x^2 < 2 < 9$, so $0 < x < 3$ or $-3 < x < 0$. Therefore, $M = 3$ and $m = -3$ are an upper and a lower bounds for B, respectively. We are going to show that $\sup B$ does *not* exists in $\mathbb{Q}$. Every $a > 0$ for which $a^2 > 2$ is an upper bound for B: if $x \in B$, then $x^2 < 2 < a^2$ and thus $x < a$. Every $a > 0$ for which $a^2 < 2$ is not an upper bound for B: if $a^2 < 2$, then $q = (2a + 2)/(a + 2) > a$ and $q^2 - 2 = 2(a^2 - 2)/(a + 2)^2 < 0$, so $q^2 < 2$ and $q > a$. From the former, $q \in B$. It follows that such an a is not an upper bound of B. We have the following: *If* $\sup B$ *exists, then* $(\sup B)^2 = 2$. *Moreover, if* $\sup B$ *exists, then* $\sup B \notin \mathbb{Q}$. Suppose that $M = \sup B \in \mathbb{Q}$. Then there exist $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus \{0\}$ such that $\gcd(a, b) = 1$ and $M = a/b$. Then $2b^2 = a^2$. Because $2 \mid a^2$, we have $2 \mid a$. Therefore, there exists $k \in \mathbb{Z}$ such that $a = 2k$. We have $2b^2 = a^2 + 4k^2$, which implies $b^2 = 2k^2$ and thus $2 \mid b^2$. But then $2 \mid b$ and $\gcd(a, b) \neq 1$. This is a contradiction, so $M \notin \mathbb{Q}$.

For mathematical analysis to be "useful" we need a number system that "fills the holes" between the rationals on the number line. This is the main reason behind the next axiom.

(D) (Dedekind's axiom) Every non-empty subset B of an ordered set A that is bounded above has the least upper bound, i.e., $\sup B$ *exists* and *is* an element of A.

Theorem 1 (The existence of real numbers)**.** *There exists an ordered field* $(\mathbb{R}, +, \cdot, <)$*, i.e., the elements of* $\mathbb{R}$ *(called* real numbers*) satisfy the axioms (A), (M), (D), and (O), on which also Dedekind's axiom (D) holds. Moreover,* $\mathbb{Q} \subset \mathbb{R}$ *and* $\mathbb{R}^+ \cap \mathbb{Q} = \mathbb{Q}^+$ *if* $\mathbb{R}^+$ *is the set of all positive real numbers, while the binary operations* $+$ *and* $\cdot$ *on* $\mathbb{R}$ *are the same as the standard addition and multiplication on* $\mathbb{Q}$*, and* $<$ *is the standard order on* $\mathbb{Q}$*.*