Introduction to Real Analysis

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 421

Subsection 1

The Field Axioms

Fields

Definition (Field)

A **field** is a set F such that, for all a, b in F, there are defined $a+b$ and ab in F, called the **sum** and **product** of a and b, subject to:

(A1) $(a+b)+c = a+(b+c)$ (**associative law for addition**);

(A2) $a+b = b+a$ (**commutative law for addition**);

(A3) there is a unique element $0 \in F$ such that $a+0 = a$, for all $a \in F$ (**existence of a zero element**);

(A4) For each $a \in F$, there exists a unique element of F, denoted $-a$, such that $a+(-a) = 0$ (**existence of negatives**);

(M1) $(ab)c = a(bc)$ (**associative law for multiplication**);

(M2) $ab = ba$ (**commutative law for multiplication**);

(M3) There is a unique element 1 of F, different from 0, such that $1a = a$, for all $a \in F$ (**existence of a unity element**);

(M4) For each nonzero $a \in F$, there exists a unique element of F, denoted a^{-1}, such that $aa^{-1} = 1$ (**existence of reciprocals**);

(D) $a(b+c) = ab+ac$ (**distributive law**).

Examples I

- The field of rational numbers is the set $\mathbb{Q}$ of fractions, $\mathbb{Q} = \{\frac{m}{n} : m \text{ and } n \text{ integers, } n \neq 0\}$, with the usual operations:

$$\begin{aligned} \frac{m}{n} + \frac{m'}{n'} &= \frac{mn' + nm'}{nn'} \\ \frac{m}{n} \cdot \frac{m'}{n'} &= \frac{mm'}{nn'} \end{aligned}$$

  The fraction $\frac{0}{1}$ serves as zero element, $\frac{1}{1}$ as unity element, $\frac{-m}{n}$ as the negative of $\frac{m}{n}$, and $\frac{n}{m}$ as the reciprocal of $\frac{m}{n}$ (assuming m and n both nonzero).
- The smallest field consists of two elements 0 and 1, where $1 + 1 = 0$ and all other sums and products are defined in the expected way (for example, $1 + 0 = 1,\ 0 \cdot 1 = 0$)

The Field of Rational Forms

- Let F be any field. Write $F[t]$ for the set of all polynomials $p(t) = a_0 + a_1 t + \cdots + a_n t^n$ in an indeterminate t, with coefficients a_k in F, and write $F(t)$ for the set of all "fractions" $\frac{p(t)}{q(t)}$, with $p(t), q(t) \in F[t]$ and $q(t)$ not the zero polynomial. With sums and products defined by

$$\begin{aligned} \frac{p(t)}{q(t)} + \frac{p'(t)}{q'(t)} &= \frac{p(t)q'(t) + p'(t)q(t)}{q(t)q'(t)} \\ \frac{p(t)}{q(t)} \cdot \frac{p'(t)}{q'(t)} &= \frac{p(t)p'(t)}{q(t)q'(t)} \end{aligned}$$

$F(t)$ is a field. It is called the field of **rational forms** over F.

The Field of Gaussian Rationals

- Write $\mathbb{Q} + i\mathbb{Q}$ for the set of all expressions $a = r + is$, $r, s \in \mathbb{Q}$. If $a = r + is$ and $a' = r' + is'$ are two such expressions, $a = a'$ means that $r = r'$ and $s = s'$. Sums and products are defined by the formulas

$$\begin{aligned} a + a' &= (r + r') + i(s + s'), \\ a \cdot a' &= (rr' - ss') + i(rs' + sr'). \end{aligned}$$

  It is straightforward to verify that $\mathbb{Q} + i\mathbb{Q}$ is a field (called the field of **Gaussian rationals**), with $0 + i0$ serving as zero element, $-r + i(-s)$ as the negative of $r + is$, $1 + i0$ as unity element, and $\frac{r}{r^2+s^2} + i\left(\frac{-s}{r^2+s^2}\right)$ as the reciprocal of $r + is$ (assuming at least one of r and s nonzero).
- Abbreviating $r + i0$ as r, we can regard $\mathbb{Q}$ as a subset of $\mathbb{Q} + i\mathbb{Q}$.
- Abbreviating $0 + i1$ as i, we have $i^2 = -1$.

Properties of Fields

Theorem

Let F be a field, a and b elements of F.

(1) $a + a = a \Leftrightarrow a = 0$.

(2) $a0 = 0$, for all a.

(3) $-(-a) = a$, for all a.

(4) $a(-b) = -(ab) = (-a)b$, for all a and b.

(5) $(-a)^2 = a^2$, for all a.

(6) $ab = 0 \Rightarrow a = 0$ or $b = 0$; in other words,

(6') $a \neq 0$ & $b \neq 0 \Rightarrow ab \neq 0$;

(7) $a \neq 0$ & $b \neq 0 \Rightarrow (ab)^{-1} = a^{-1}b^{-1}$.

(8) $(-1)a = -a$, for all a.

(9) $-(a + b) = (-a) + (-b)$, for all a and b.

(10) Defining $a - b$ to be $a + (-b)$, we have $-(a - b) = b - a$.

Proof of the Theorem

(1) If $a+a=a$, add $-a$ to both sides: $(a+a)+(-a)=a+(-a)$, use (A1), $a+(a+(-a))=a+(-a)$, apply (A4), $a+0=0$ and, finally, apply (A3) $a=0$. This shows $a+a=a \Rightarrow a=0$. The converse is immediate from axiom (A3).

(2) By axiom (D), $a0=a(0+0)=a0+a0$, so $a0=0$ by (1).

(3) $(-a)+a=a+(-a)=0$, so $a=-(-a)$, by the uniqueness in (A4).

(4) $0=a0=a[b+(-b)]=ab+a(-b)$, so $a(-b)=-(ab)$ by (A4); it follows that $(-a)b=b(-a)=-(ba)=-(ab)$.

(5) Citing (4) twice, we have $(-a)(-a)=-[a(-a)]=-[-(aa)]=aa$, in other words $(-a)^2=a^2$.

(6,7) If a and b are nonzero, then $(ab)(a^{-1}b^{-1})=(aa^{-1})(bb^{-1})=1\cdot 1=1\neq 0$; it follows from (2) that ab must be nonzero, and $(ab)^{-1}=a^{-1}b^{-1}$ follows from uniqueness in axiom (M4).

(8) $(-1)a=-(1a)=-a$.

(9) $-(a+b)=(-1)(a+b)=(-1)a+(-1)b=(-a)+(-b)$.

(10) $-(a-b)=-[a+(-b)]=(-a)+(-(-b))=(-a)+b=b+(-a)=b-a$.

Notation: Division as an Analog of Subtraction

- In the rational field $\mathbb{Q}$, $\frac{m}{n} = \frac{m'}{n'}$ means that $mn' = nm'$. Abbreviating $\frac{m}{1}$ as m, the set $\mathbb{Z}$ of integers can be regarded as a subset of $\mathbb{Q}$.
- For a nonzero integer n, $n\frac{1}{n} = \frac{n}{1}\frac{1}{n} = \frac{n}{n} = \frac{1}{1} = 1$, whence $\frac{1}{n} = n^{-1}$.
- The fractional notation is useful in an arbitrary field F: one writes $\frac{a}{b}$ for ab^{-1}, where $a, b \in F$ and $b \neq 0$ (this is the multiplicative analog of subtraction $a - b = a + (-b)$).

Subsection 2

The Order Axioms

Ordered Fields

Definition (Ordered Field)

An **ordered field** is a field F having a subset P of nonzero elements, called **positive**, such that

(O1) $a, b \in P \Rightarrow a + b \in P$;

(O2) $a, b \in P \Rightarrow ab \in P$;

(O3) $a \in F, a \neq 0 \Rightarrow$ either $a \in P$ or $-a \in P$, but not both.

In words, the sum and product of positive elements are positive and for each nonzero element a, exactly one of a and $-a$ is positive.

- For elements a, b of F, we write $a < b$ (or $b > a$) if $b - a \in P$.

Negative Elements and Trichotomy

- $b \in P \Leftrightarrow b > 0$;
- $-a \in P \Leftrightarrow a < 0$;
- Elements a with $a < 0$ are called **negative**.
- Properties (O1) and (O2) may be written

$$a > 0 \ \& \ b > 0 \Rightarrow a + b > 0 \ \& \ ab > 0.$$

- Property (O3) yields the following:
  If $a, b \in F$, and $a \neq b$ (in other words, $a - b \neq 0$) then either $a > b$ or $a < b$ but not both.
- Thus, for any pair of elements a, b of F, exactly one of the following three statements is true:

$$a < b, \quad a = b, \quad a > b.$$

  This form of (O3) is called the **law of trichotomy**.

Properties of Ordered Fields

Theorem

In an ordered field,

(1) $a < a$ is impossible;

(2) if $a < b$ and $b < c$ then $a < c$;

(3) $a < b \Leftrightarrow a + c < b + c$;

(4) $a < b \Leftrightarrow -a > -b$;

(5) $a < 0$ & $b < 0 \Rightarrow ab > 0$;

(6) $a < 0$ & $b > 0 \Rightarrow ab < 0$;

(7) $a < b$ & $c > 0 \Rightarrow ca < cb$;

(8) $a < b$ & $c < 0 \Rightarrow ca > cb$;

(9) $a \neq 0 \Rightarrow a^2 > 0$;

(10) $1 > 0$;

(11) $a + 1 > a$;

(12) $a > 0 \Rightarrow a^{-1} > 0$.

Proof of the Theorem

(1) $a - a = 0 \notin P$, whence $a < a$ cannot hold.

(2) $c - a = (c - b) + (b - a)$ is the sum of two positive elements, and, hence, positive. Thus, $a < c$.

(3) $(b + c) - (a + c) = b - a$.

(4) $-a - (-b) = b - a$.

(5) $ab = (-a)(-b)$ is the product of two positive elements.

(6) $0 - ab = (-a)b$ is the product of positives, whence $ab < 0$.

(7) $cb - ca = c(b - a)$.

(8) $ca - cb = (-c)(b - a)$.

(9) $a^2 = aa = (-a)(-a)$ is the product of two positives.

(10) $1 = 1^2 > 0$ by (9).

(11) $(a + 1) - a = 1 > 0$.

(12) If $a > 0$, then $aa^{-1} = 1 > 0$ precludes $a^{-1} < 0$ by (6).

Notation and Examples

Definition

In any ordered field, one defines

$$2 = 1 + 1, \quad 3 = 2 + 1, \quad 4 = 3 + 1, \quad \textit{etc.}$$

- By the preceding theorem $0 < 1 < 2 < 3 < 4 < \cdots$.

Definition

In an ordered field, we write $a \leq b$ (also $b \geq a$) if either $a < b$ or $a = b$. An element a such that $a \geq 0$ is said to be **nonnegative**.

- The relation $\leq$ has all the expected properties, e.g.:
  - $a \leq b$ and $b \leq c$ imply $a \leq c$;
  - $a \leq b$ and $c > 0$ imply $ca \leq cb$.
- Example: The rational field $\mathbb{Q}$ is ordered, with $P = \{\frac{m}{n} : m \text{ and } n \text{ positive integers}\}$ as the set of positive elements.
- Example: The field of Gaussian rationals is not orderable, because $i^2 = -1$. (In an ordered field, nonzero squares are positive and -1 is negative, so -1 cannot be a square.)

Comparing Powers

Theorem

Let F be an ordered field, a and b nonnegative elements of F, n any positive integer.

(i) $a < b \Leftrightarrow a^n < b^n$;

(ii) $a = b \Leftrightarrow a^n = b^n$;

(iii) $a > b \Leftrightarrow a^n > b^n$.

(i) $\Rightarrow$: By assumption, $0 \leq a < b$; We prove that $a^n < b^n$, for every positive integer n by induction on n:

- The case $n = 1$ is the given inequality.
- Assume $a^k < b^k$. Consider $b^{k+1} - a^{k+1} = b(b^k - a^k) + (b - a)a^k$. The right side is positive because $b > 0$, $b^k - a^k > 0$, $b - a > 0$ and $a^k > 0$. Thus, $a^{k+1} < b^{k+1}$.

(iii) $\Rightarrow$: Follows on interchanging the roles of a and b.

(ii) $\Rightarrow$: is obvious.

- The implications $\Leftarrow$ follow by trichotomy!

Subsection 3

Bounded Sets, LUB and GLB

Bounded Sets in Ordered Fields

Definition

Let F be an ordered field. A nonempty subset A of F is said to be:

(i) **bounded above** if there exists an element $K \in F$, such that $x \leq K$ for all $x \in A$. Such an element K is called an **upper bound** for A.

(ii) **bounded below** if there exists an element $k \in F$, such that $k \leq x$, for all $x \in A$. Such an element k is called a **lower bound** for A.

(iii) **bounded** if it is both bounded above and bounded below;

(iv) **unbounded** if it is not bounded.

Intervals in Ordered Fields

- Let F be an ordered field, a and b elements of F with $a < b$. Each of the following subsets of F is bounded, with a serving as a lower bound and b as an upper bound:

$$[a,b] = \{x \in F : a \leq x \leq b\} \quad [a,b) = \{x \in F : a \leq x < b\}$$
$$(a,b) = \{x \in F : a < x < b\} \quad (a,b] = \{x \in F : a < x \leq b\}.$$

  Such subsets of F are called **intervals**, with **endpoints** a and b. More precisely,
  - $[a,b]$ is called a **closed interval** (because it contains the endpoints);
  - (a,b) is called an **open interval** (because it does not);
  - the intervals $[a,b)$ and $(a,b]$ are called **semiclosed** or **semi-open**.
- If $F = \mathbb{Q}$, then the term "interval" loses some of its intuitive meaning (an interval in $\mathbb{Q}$ is considerably more ventilated than the familiar intervals on the real line).
- Note that $(a,a) = [a,a) = (a,a] = \emptyset$ because $a < a$ is impossible. On the other hand, $[a,a] = \{a\}$.

Examples

- An ordered field is neither bounded above nor bounded below: e.g., any proposed upper bound K is topped by $K + 1$.
- In an ordered field F, the interval $[0, 1]$ has a largest element but $[0, 1)$ does not: If a is any element of $[0, 1)$ then $x = \frac{a+1}{2}$ is a larger element of $[0, 1)$.
  1 is an upper bound for $[0, 1)$, but nothing smaller will do:
  If $a < 1$ then $[0, 1)$ contains an element x larger than a:
  - If $a < 0$, let $x = \frac{1}{2}$.
  - If $0 \leq a < 1$, let $x = \frac{a+1}{2}$.

Least Upper Bound

Definition (Least Upper Bound)

Let F be an ordered field, A a nonempty subset of F. We say that A has a **least upper bound** in F if there exists an element $M \in F$, such that:

(a) M is an upper bound for A, i.e., $x \leq M$, for all $x \in A$;

(b) nothing smaller than M is an upper bound for A, i.e., $M' < M \Rightarrow \exists x \in A$ such that $x > M'$.

- By the contrapositive, (b) is equivalent to M' an upper bound for A implies $M \leq M'$.
- Conditions (a) and (b) can be combined into a single condition:

$$M' \text{ is an upper bound for } A \Leftrightarrow M' \geq M.$$

- If such a number M exists, it is unique and is called the **least upper bound**, or **supremum**, of A, written $M = \text{LUB } A$, or $M = \sup A$.

Greatest Lower Bound

- The supremum of a set need not belong to the set.
- A set that is bounded above need not have a least upper bound.
- For sets that are bounded below:

Definition (Greatest Lower Bound)

Let A be a nonempty subset of an ordered field F. We say that A has a **greatest lower bound** in F if there exists an element $m \in F$, such that:

(a) m is a lower bound for A,

(b) if m' is a lower bound for A then $m \geq m'$.

- If such an element m exists, it is unique and is called the **greatest lower bound**, or **infimum**, of A, written $m = \text{GLB } A$, or $m = \inf A$.

Duality Theorem

Theorem

Let F be an ordered field, A a nonempty subset of F. Write $-A = \{-x : x \in A\}$. Let $c \in F$. Then:

(i) c is an upper bound for A iff $-c$ is a lower bound for $-A$;

(ii) c is a lower bound for A iff $-c$ is an upper bound for $-A$;

(iii) If A has a least upper bound, then $-A$ has a greatest lower bound and $\inf(-A) = -(\sup A)$.

(iv) If A has a greatest lower bound, then $-A$ has a least upper bound and $\sup(-A) = -(\inf A)$.

(i) The mapping $x \mapsto -x$ is a bijection $F \to F$ that reverses order: $a < b$ iff $-a > -b$. The condition $x \leq c$, for all $x \in A$, is therefore equivalent to the condition $-c \leq y$, for all $y \in -A$. This proves (i).

(ii) The proof of (ii) is similar.

Proof of (iii) and (iv)

(iii) If A has a least upper bound, then $-A$ has a greatest lower bound and $\inf(-A) = -(\sup A)$:
Suppose A has a least upper bound a. We know from (i) that $-a$ is a lower bound for $-A$. We have to show that it is larger than all others. Let k be any lower bound for $-A$. For all $a \in A$, we have $k \leq -a$, so $a \leq -k$. So $-k$ is an upper bound for A, whence $a \leq -k$, and, therefore, $-a \geq k$.

(iv) If A has a greatest lower bound, then $-A$ has a least upper bound and $\sup(-A) = -(\inf A)$:
The proof of (iv) is similar to that of (iii).

Subsection 4

The Completeness Axiom (Existence of LUBs)

The Field of Real Numbers $\mathbb{R}$

Definition (Complete Ordered Field)

An ordered field is said to be **complete** if it satisfies the condition: Every nonempty subset that is bounded above has a least upper bound.

- Do such fields exist? If so, how many? The point of departure of "real analysis" is the assumption that the answers are "yes" and "one".
- We assume that there exists a complete ordered field $\mathbb{R}$ and that it is unique in the sense that every complete ordered field is isomorphic to $\mathbb{R}$:

Definition (Real Number Field)

$\mathbb{R}$ is a complete ordered field whose elements are called **real numbers**.

- This definition means that $\mathbb{R}$ is a set with two operations (addition and multiplication) satisfying the field axioms, the order axioms and the completeness axiom.

Positive Integers and Natural Numbers

- Example: The ordered field $\mathbb{Q}(t)$ is not complete. The rational field $\mathbb{Q}$ is not complete either.
- The statements that follow are not self-evident, but we will take them for granted:
  - The set of **positive integers** is the set $\mathbb{P} = \{1, 2, 3, \ldots\}$, where $2 = 1 + 1$, $3 = 2 + 1$, etc. (The "etc." and the three dots "..." hide all the difficulties!)
  - Every positive integer is > 0, and 1 is the smallest.
  - The set $\mathbb{P}$ is closed under addition and multiplication.
  - The set of **natural numbers** is the set $\mathbb{N} = \{0\} \cup \mathbb{P} = \{0, 1, 2, 3, \ldots\}$.
  - $\mathbb{N}$ is also closed under addition and multiplication.

Integers and Rational Numbers

- The set of **integers** is the set $\mathbb{Z}$ of all differences of positive integers,

$$\mathbb{Z} = \{m - n : m, n \in \mathbb{P}\}.$$

- $\mathbb{Z}$ is closed under the operations $x + y$, xy and $-x$.
- The set of positive elements of $\mathbb{Z}$ is precisely the set $\mathbb{P}$, whence $\mathbb{Z} = \{0\} \cup \mathbb{P} \cup (-\mathbb{P})$, where $-\mathbb{P} = \{-n : n \in \mathbb{P}\}$.
- The set of **rational numbers** is the set

$$\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\},$$

  where $\frac{m}{n} = mn^{-1}$.
- $\mathbb{Q}$ contains sums, products, negatives and reciprocals (of its nonzero elements), thus $\mathbb{Q}$ is itself a field (a "subfield" of $\mathbb{R}$).
- We have the inclusions $\mathbb{P} \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Outline of a Rigorous Treatment

- Besides the overt axioms for $\mathbb{R}$ (field, order, completeness) we propose to accept a somewhat vague hidden one:
  $\mathbb{P}$ is "equal" to the set of "ordinary positive integers".
- For this to become rigorous, we should
  (1) set down axioms for the set of positive integers (for example, Peano's axioms);
  (2) show that there is essentially only one set satisfying the axioms;
  (3) give an unambiguous definition of the set $\mathbb{P}$ defined informally above;
  (4) verify that $\mathbb{P}$ satisfies the axioms in question.
- To avoid the complete axiomatic development with its associated formalism, we accept the informal description of $\mathbb{P}$.