Real Analysis 1

MATH1010

Professor Huy Nguyen

Brown University

Edited by

Richard Tang

Contents

Chapter 1

Real Numbers

In this class, we operate on the set of real numbers. It is important to rigorously define it, as well as all underlying sets of numbers (natural numbers, integers, rationals, etc).

§1.1 Natural Numbers

Definition 1.1.1: Natural Numbers

The set $\mathbb{N} = 1, 2, \ldots$ is the set of natural numbers. Each integer n has a **successor**, $succ(n) = n + 1$. 1 is not the successor of any number.
The following properties constitute the Peano Axioms of $\mathbb{N}$:

1. $1 \in \mathbb{N}$.
2. $n \in \mathbb{N} \Rightarrow succ(n) = n + 1 \in \mathbb{N}$
3. $\nexists n$ s.t. $succ(n) = 1$
4. If $n, m \in \mathbb{N}, succ(n) = succ(m)$, then $n = m$.
5. A subset $A \subset \mathbb{N}$ which contains 1, and which contains $n + 1$ whenever it contains n, must equal $\mathbb{N}$.

We accept only these 5 axioms to prove all other properties of $\mathbb{N}$.

(5) is the basis for the principle of induction.

Theorem 1.1.1: Principle of Mathematical Induction

Let $P_1, P_2, \ldots$ be a list of statements. Assume the following:

1. P_1 is true. [Basis of induction]
2. $\forall n \in N, n \geq 1$, if P_n is true, then P_{n+1} is true. [Inductive step]

Then all the statements $P_1, \ldots$ are true.

Proof. Let A be the set of integers n for which P_n is true. We want to prove $A = \mathbb{N}$. We use (5) to prove this.
Indeed, $1 \in A$ by assumption 1. Assuming that $n \in A$ for some n, we prove that $n + 1 \in A$. This is true by assumption 2: if $n \in A$, then P_n is true, hence P_{n+1} is true, hence $n + 1 \in A$. Thus, $A = \mathbb{N}$. □

Example 1. *Prove that* $2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 2$.

Proof. Let P_n: "$2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 2$".
P_1 is true because $2^1 = 2^2 - 2$.
For the induction step, we assume P_n is true for some n and prove P_{n+1} is true. Since P_n is true,

$$2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 2.$$

P_{n+1} states that

$$2^1 + \ldots + 2^n + 2^{n+1} = 2^{(n+1)+1} - 2.$$

Using P_n we have

$$2^1 + \ldots + 2^{n+2^{n+1}} = \left(2^{n+1} - 2\right) + 2^{n+1} = 2 \cdot 2^{n+1} - 2 = 2^{(n+1)+1} - 2,$$

Thus P_{n+1} is true. By the principle of induction, P_n is true for all $n \geq 1$. □

Example 2. *Let $x_1 = 1$ and define*

$$x_{n+1} = \frac{1}{2}x_n + 1.$$

Prove that $\forall x, x_n \leq x_{n+1}$ (or, x_n is inreasing).

Proof. Let P_n: "$x_n \leq x_{n+1}$".
P_1 is true because $x_1 = 1 \leq \frac{3}{2} = x_2$.
For the induction step, we assume P_n is true for some n and prove P_{n+1} is true. Since P_n is true,

$$x_n \leq x_{n+1}.$$

P_{n+1} states that

$$x_{n+1} \leq x_{n+2}.$$

Using P_n we have

$$x_{n+1} = \frac{1}{2}x_n + 1 \leq \frac{1}{2}x_{n+1} + 1 = x_{n+2} \text{ [by } P_n\text{, we know } x_n \leq x_{n+1}]$$

Thus P_{n+1} is true.
By the principle of induction, P_n is true for all $n \geq 1$. □

The principle of induction can be extended by allowing the first statement to begin at P_m instead of P_1 for some fixed integer m.

Theorem 1.1.2: Generalized Principle of Induction

Let m be an integer, and consider a list of statements $P_m, P_{m+1}, \ldots$. Then all the statements are true if the following two properties are true:

1. P_m is true
2. $\forall n \geq m$, if P_n is true, then P_{n+1} is true.

Theorem § 1.1.2 follows from

Proposition 1.1.1: Specific Case of (5)

Let $m \in N$. Assume that a subset $A \subset \{m, m+1, \ldots\}$ contains m and $n+1$ whenever it contains n. Then $A = \{m, m+1, \ldots\}$.

Proof. In Peano Axiom 5, we start from 1; here, we start from m. Let $B = \{p = n-(m-1) \mid n \in A\}$. Since $A \subset \{m, m+1, \ldots\}$, $B \subset \{1, 2, \ldots\} = \mathbb{N}$.
We observe that $1 \in B$ (because $1 = m-(m-1)$, and $m \in A$ by definition). Assuming $p \in B$, we have $p = n-(m-1)$ for some $n \in A$. Then $p+1 = (n+1)-(m-1) \in B$, as we state that $n+1 \in A$ whenever $n \in A$. Thus, using Peano Axiom 5, we see that $A = B$.
Now, by definition of B, we have

$$\begin{aligned} A &= \{n = p + (m-1) \mid p \in B\} \\ &= \{n = p + (m-1) \mid p \in \mathbb{N}\} \\ &= \{m, m+1, \ldots\} \end{aligned}$$

$\square$

Example 3. *Prove that*

$$n! > n^2.$$

for all $n \geq 4$.

Proof. Recall $n! = 1 \cdot 2 \cdot \ldots \cdot n$. Let P_n: "$n! > n^2$". We prove P_n is true $\forall n \geq 4$.
P_4 is true because

$$4! = 24 > 16 = 4^2.$$

Assuming $n! > n^2$, we prove

$$(n+1)! > (n+1)^2.$$

Using P_n we have

$$(n+1)! = n!\,(n+1) = (1 \cdot 2 \cdot \ldots \cdot n) \cdot (n+1) > n^2(n+1) > (n+1)^2.$$

Thus P_{n+1} is true.
By the principle of induction, P_n is true for all $n \geq 4$. $\square$

§1.2 Rational Numbers

Definition 1.2.1: Integers

The set of integers is denoted by

$$\mathbb{Z} = \{\ldots -2, -1, 0, 1, 2, \ldots\}.$$

A rigorous construction is omitted, and left as an exercise for the reader.

Definition 1.2.2: Rational Numbers

The set $\mathbb{Q}$ of rational numbers is

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

We say $\frac{m}{n}$ and $\frac{p}{q}$ are equal if

$$mq = np.$$

We can define addition and multiplication of rational numbers in the usual way:

- (addition) $\frac{m}{n} + \frac{p}{q} = \frac{mq+np}{nq}$
- (multiplication) $\frac{m}{n} \cdot \frac{p}{q} = \frac{mp}{nq}$

$\mathbb{Q}$ is a nice algebraic system, until we solve systems like $x^2 = 2$. It turns out that this equation has no rational roots; but we know that by the Pythagorean theorem, this equation has positive roots.

Example 4. *Prove that $\sqrt{2}$ is not a rational number.*

Proof. Suppose that $\sqrt{2} \in \mathbb{Q}$; then $\sqrt{2} = \frac{p}{q}$ for some $p, q \in \mathbb{Z}$, and p, q have no common divisors other than 1. Then

$$2 = \frac{p^2}{q^2}$$
$$2q^2 = p^2$$

This implies p^2 is even; but p^2 is even if and only if p is even. Then $p = 2n$ for some $n \in N$; $p^2 = (2n)^2 = 4n^2$. From this, we get $2q^2 = 4n^2$, and so $q^2 = 2n^2$ and q is even as well. Since both p, q are even, they have a common divisor $2 \neq 1$, a contradiction. Thus $\sqrt{2}$ is not rational. □

Proposition 1.2.1: Algebraic Numbers

A number is an **algebraic number** if it satisfies the polynomial equation

$$c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0 = 0,$$

where $c_0, c_1, \ldots, c_n$ are integers, $c_n \neq 0, n \geq 1$. We say that the polynomial equation has **degree** n.

Example 5. *$\sqrt{2}$ is an algebraic number because it satisfies*

$$x^2 - 2 = 0.$$

Example 6. *Every rational number $x = \frac{p}{q}$ is an algebraic number because x satisfies*

$$qx - p = 0.$$

Example 7. $x = \sqrt{2 + \sqrt[3]{5}}$ *is an algebraic number because*

$$\begin{aligned} x^2 &= 2 + \sqrt[3]{5} \\ x^2 - 2 &= \sqrt[3]{5} \\ \left(x^2 - 2\right)^3 &= 5, \end{aligned}$$

hence x satisfies the polynomial

$$\left(x^2 - 2\right)^3 - 5 = 0.$$

From this, we see that algebraic numbers do not necessarily need to be rational numbers. The question now is: *when does a polynomial of order n have rational roots?*

Theorem 1.2.1: Rational Zeros Theorem

Let $c_0, c_1, \ldots, c_n \in \mathbb{Z}, c_n \neq 0, c_0 \neq 0$. Suppose r is a rational root of

$$P(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0 = 0 \tag{1.1}$$

Let $r = \frac{p}{q}, p, q \in \mathbb{Z}, q \neq 0, \gcd(p, q) = 1$. Then p divides c_0 and q divides c_n.

Proof. Suppose $r \in \mathbb{Q}$ is a rational root of

$$P(x) = c_n x^n + \ldots + c_1 x + c_0.$$

Note that $r = \frac{p}{q}, p, q \in \mathbb{Z}, q \neq 0, \gcd(p, q) = 1$. Then

$$P(r) = P(\frac{p}{q}) = c_n \left(\frac{p}{q}\right)^n + \ldots + c_1 \left(\frac{p}{q}\right) + c_0 = 0.$$

Multiplying both sides by q^n, we have

$$c_n p^n + c_{n-1} p^{n-1} q + \ldots + c_1 p q^{n-1} + c_0 q^n = 0.$$

Then

$$\begin{aligned} c_n p^n + \ldots + c_1 p q^{n-1} &= -c_0 q^n \\ p\left(c_n p^{n-1} + c_{n-1} p^{n-2} q + \ldots + c_1 q^{n-1}\right) &= -c_0 q^n. \end{aligned}$$

Thus, $-c_0 q^n$ is divisible by p. Since $\gcd(p, q) = 1$, it follows that c_0 is divisible by p. Similarly, if we move $c_n p^n$ to the other side, and factor out q, then we get

$$q\left(c_{n-1} p^{n-1} + c_{n-2} p^{n-2} q + \ldots + c_1 p q^{n-2} c_0 q^{n-1}\right) = -c_n p^n,$$

and since $c_n p^n$ is divisible by q and $\gcd(p, q) = 1$, c_n is divisible by q.
Thus, if $r = \frac{p}{q}$ is a rational root of $P(x)$, then $p \mid c_0$ and $q \mid c_n$. $\square$

Remark 1. *Theorem 1.2.1 allows us to find all possible rational roots of 1.1. Specifically, given a*

$$P(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0,$$

if

$$a \in \{p \in \mathbb{Z} \mid p \text{ divides } c_0\}, b \in \{q \in \mathbb{Z} \mid q \text{ divides } c_n\},$$

then any rational root must have the form $\frac{a}{b}$*.*

For example, given

$$P(x) = 3x^3 + x^2 - 8x + 4,$$

the only possible rational roots are

$$r = \pm 1, \pm\frac{1}{3}, \pm 2, \pm\frac{2}{3}, \pm 4, \text{ and } \pm\frac{4}{3}.$$

Corollary 1.2.1

Consider the polynomial equation

$$x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0 = 0,$$

with integer coefficients and $c_0 \neq 0$. Any rational solution of this equation must be an integer that divides c_0.

This corollary allows us to determine whether a number is a rational number; if its polynomial has no rational roots, then the number cannot be rational.

Example 8. $\sqrt{17}$ *is not a rational number.*

Proof. The only possible rational solutions of $x^2 - 17 = 0$ are ± 1 and ± 17, and none of these numbers are solutions. Hence $\sqrt{17}$ is not a rational number. ☐

§1.3 Real Numbers

As nice as the rationals are, $\mathbb{Q}$ is inadequate to describe all systems. For instance, $x^2 = 2$ clearly has a solution of $\sqrt{2}$, but this is impossible to describe using rationals. We get the intuition that $\mathbb{Q}$ has "gaps". We skip a rigorous development of $\mathbb{Q}$ based on $\mathbb{Z}$, but observe that $\mathbb{Q}$ satisfies the properties of a **field** .

Definition 1.3.1: Fields

A **field** $\mathbb{F}$ is an algebraic system (a set along with operations on elements of the set) that satisfies nine properties, for all $a, b, c \in \mathbb{F}$:

1. Additive associativity: $a + (b + c) = (a + b) + c$.

2. Additive commutativity: $a + b = b + a$.
3. Additive identity: $a + 0 = 0 + a = a$.
4. Additive inverse: For each a, there is an element $-a$ such that $a + (-a) = (-a) + a = 0$.
5. Multiplicative associativity: $a(bc) = (ab)c$.
6. Multiplicative commutativity: $ab = ba$.
7. Multiplicative identity: $a \cdot 1 = 1 \cdot a = a$.
8. Multiplicative inverse: For each $a \neq 0$, there is an element a^{-1} such that $aa^{-1} = 1$.
9. Distributive law: $a(b + c) = ab + ac$.

We can also define an order structure $\leq$ for a field $\mathbb{F}$:

Definition 1.3.2: Order

A **ordered field** $\mathbb{F}$ satisfies five properties for all $a, b \in \mathbb{F}$:

1. Given a, b, either $a \leq b$ or $b \leq a$.
2. If $a \leq b$ and $b \leq a$, then $a = b$.
3. (Transitive Law) If $a \leq b$ and $b \leq c$, then $a \leq c$.
4. If $a \leq b$, then $a + c \leq b + c$.
5. If $a \leq b$ and $0 \leq c$, then $ac \leq bc$.

Theorem 1.3.1: Properties of Fields

The following properties are consequences of the field axioms for $a, b, c \in \mathbb{F}$:

1. If $a + c = b + c$, then $a = b$.
2. $a \cdot 0 = 0$ for all a.
3. $(-a)b = -ab$ for all a, b.
4. $(-a)(-b) = ab$ for all a, b.
5. If $ac = bc$ and $c \neq 0$, then $a = b$.
6. If $ab = 0$, then either $a = 0$ or $b = 0$.

Proof. We provide a proof for some properties (the rest are left as an exercise for the reader).

1. $a + c = b + c$ implies $a + c + (-c) = b + c + (-c)$, which becomes $a + 0 = b + 0 \implies a = b$.
2. $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, which implies $0 + a \cdot 0 = a \cdot 0 + a \cdot 0$. By property 1, we get $0 = 0 \cdot a$.

3. $(-a)b + ab = (a + (-a))b = 0 \cdot b = 0$, which implies $(-a)b$ is the inverse of ab, and so $(-a)b = -ab$.

4. Exercise

5. Exercise

6. If $ab = 0$, and WLOG $b \neq 0$, we have $0 = 0 \cdot b^{-1} = (ab) \cdot b^{-1} = a(bb^{-1}) = a \cdot 1 = a$, which implies $a = 0$.

$\square$

The algebraic system of interest in analysis will be the **real numbers**, or $\mathbb{R}$, which will include all rational numbers and irrational numbers; it has no “gaps”. It turns out that $\mathbb{R}$ can be defined entirely in terms of $\mathbb{Q}$. [TODO]

$\mathbb{R}$ satisfies the same ordered field axioms as $\mathbb{Q}$ (since $\mathbb{R}$ is also a field).