

Notes for MATH 3210: Foundation of Analysis I

Jing Guo

September 24, 2017

Contents

1	Ring and Field	1
1.1	Ring	2
1.1.1	Addition Axiom	2
1.1.2	Multiplication Axiom	2
1.2	Field	2
1.3	Construction of Integers	3
1.4	Construction of Fractions (Rational Numbers)	4
1.5	Ordered Set	5
1.5.1	Partial Order	5
1.5.2	Total Order	6
1.5.3	Least-upper-bound Property	6
1.6	Real Numbers	8
1.6.1	Construction of Real Numbers	8
1.6.2	Archimedean Property	8
1.6.3	Density of Real Numbers	9
1.6.4	Property of Real Numbers	9
1.7	Complex Number	11
1.7.1	Construction of Complex Numbers	11
1.7.2	Automorphism of Complex Numbers	12
2	Basic Topology	12
2.1	Metric Space M	12
2.2	Open Sets	13
2.2.1	Metric Spaces X	13
2.2.2	Topological Spaces (X, U)	13
2.3	Compact Sets	13

1 Ring and Field

Notations:

- \mathbb{N} : The set of natural numbers;

- \mathbb{Z} : The set of integers (ring, not field, has no inverse);
- \mathbb{Q} : The set of rational numbers;
- \mathbb{R} : The set of real numbers (ring and field).

1.1 Ring

The set A has two binary operations, addition and multiplication.

For any $a, b \in A$,

$$\begin{aligned} A * A &\rightarrow A \\ a, b &\rightarrow a + b \end{aligned}$$

1.1.1 Addition Axiom

1. $a + b = b + a$ (commutative)
2. $(a + b) + c = a + (b + c)$ (associative)
3. There is an element 0 such that $a + 0 = a$ (additive identity)
4. There exists $-a$ (additive inverse) such that $a + (-a) = 0$

1.1.2 Multiplication Axiom

1. $a \cdot b = b \cdot a$
2. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. There is an element 1 such that $a \cdot 1 = a$ and $0 \neq 1$
4. $a \cdot (b + c) = a \cdot b + a \cdot c$ (distributive)

1.2 Field

A is a field if A is a *ring* for any $a \in A$ and $a \neq 0$, there exists a^{-1} (inverse of a) such that $a \cdot a^{-1} = 1$.

A has no zero divisors if $x \neq 0, y \neq 0 \rightarrow x \cdot y \neq 0$

Example: $x, y \in A, x \neq 0, y \neq 0, xy = 0$

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

1.3 Construction of Integers

We need to construct \mathbb{Z} from \mathbb{N} with **localization**.

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}$$

Set of equivalence class: $\mathbb{N} \times \mathbb{N} / \sim$

Equivalence relation: $(a, b) \sim (a', b')$ if $a + b' = b + a'$, since $a - b = a' - b'$

$$\begin{aligned} (a, b) &\sim (a', b') \sim (a'', b'') \\ a' + b'' &= b' + a'' \\ (a + b'') + b' &= (a + b') + b'' = b + a' + b'' = b + b' + a'' = (a'' + b) + b' \\ \therefore a + b'' &= a'' + b \\ \therefore (a, b) &\sim (a'', b'') \end{aligned}$$

We then should define addition:

$$[(a, b)] + [(a', b')] = [(a + a', b + b')] \quad (1)$$

$$[(a_1, b_1)] + [(a', b')] = [(a_1 + a', b_1 + b')] \quad (2)$$

Equation 1 and equation 2 are equal since independent of choice of equivalence classes:

$$\begin{aligned} a + a' + b_1 + b' &= a_1 + a' + b + b' \\ a + b_1 &= a_1 + b \end{aligned}$$

Additive identity: $0 = [(0, 0)]$

For example: $[(a, b)] + [(b, a)] = [(a + b, a + b)] = [(0, 0)] = 0$

We then need to define multiplication:

$$[(a, b)] \cdot [(a', b')] = [(aa' + bb', ab' + a'b)]$$

$$\begin{aligned} &(a - b)(a' - b') \\ &= aa' - ab' - a'b + bb' \\ &= (aa' + bb') - (ab' + a'b) \end{aligned}$$

Multiplicative identity: $1 = [(1, 0)]$

For example: $[(a, b)] \cdot [(1, 0)] = [(a, b)]$

$\therefore \mathbb{N} \times \mathbb{N} / \sim$ is a ring, that is, \mathbb{Z} .

$$\begin{aligned}
\mathbb{N} &\longrightarrow \mathbb{Z} \\
m &\longrightarrow [(m, 0)] \\
-m &\longrightarrow [(0, m)] = -[(m, 0)]
\end{aligned}$$

For example:

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

1.4 Construction of Fractions (Rational Numbers)

We need to show that K is a field (with addition and multiplication). Assume A is a commutative ring with no zero divisors, and $A^* = A - \{0\}$.

$$A \times A^* = \{(a, b) \mid a, b \in A, b \neq 0\}$$

Set of equivalence classes: $K = (A \times A^*) / \sim$ (elements of K are fractions)

We first need to define addition:

$$\begin{aligned}
(a, b) &\sim (a', b') \\
\frac{a}{b} &= \frac{a'}{b'} \\
ab' &= a'b
\end{aligned}$$

$[(a, b)]$: The equivalence class of (a, b)

$$\begin{aligned}
[(a, b)] + [(a', b')] &= [(ab' + a'b, bb')] = \frac{ab' + a'b}{bb'} \\
[(0, 1)] &= 0 \in K \quad (\text{additive identity})
\end{aligned}$$

The following is to prove that it is independent of the choice of equivalence class:

$$\begin{aligned}
[(a_1, b_1)] + [(a', b')] &= [(a_1b' + a'b_1, b_1b')] \\
\therefore (ab' + a'b) \cdot b_1b' &= (a_1b' + a'b_1) \cdot bb' \\
\therefore \text{left} &= \text{right}
\end{aligned}$$

We then need to define multiplication:

$$\begin{aligned}
[(a, b)][(a', b')] &= [(aa', bb')] = \frac{aa'}{bb'} \\
[(1, 1)] &= 1 \in K \quad (\text{multiplicative identity})
\end{aligned}$$

Examples:

$$\begin{aligned} [(x, y)] + [(0, 1)] &= [(x, y)] \\ [(x, y)] \cdot [(1, 1)] &= [(x, y)] \\ [(x, y)] &\neq [(0, 1)] \end{aligned}$$

So we need to show that K is a field:

$$\begin{aligned} [(x, y)] \cdot [(y, x)] &= [(xy, xy)] = [(1, 1)] \quad (\text{Non-zeros have inverse}) \\ \therefore ab' &= a'b \\ (a, b) &\sim (a', b') \\ \therefore [(xy, xy)] &= [(1, 1)] \end{aligned}$$

Therefore K is a field of fractions of A .

We need to show the following map is injective:

If $A = \mathbb{Z}$ and $K = \mathbb{Q}$:

$$\begin{aligned} A &\longrightarrow K \quad (\text{injective}) \\ x &\longrightarrow [(x, 1)] \\ x + y &\longrightarrow [(x + y, 1)] = [(x, 1)] + [(y, 1)] \\ x \cdot y &\longrightarrow [(xy, 1)] = [(x, 1)] \cdot [(y, 1)] \\ \text{Comm. ring without } 0 &\longrightarrow \text{Field containing the ring} \end{aligned}$$

Assume $[(a, 1)] = [(b, 1)]$ where $a, b \in A$:

$$\begin{aligned} a \cdot 1 &= b \cdot 1 \Rightarrow a = b \\ \therefore \text{The map is injective.} \end{aligned}$$

$P(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_n, a \in R$
 Ring of polynomials: $P(x) \times Q(x) \Rightarrow R(x)$ (with no zero divisors)

1.5 Ordered Set

1.5.1 Partial Order

(S, \leq) is a (partially) ordered set (poset), $\forall x, y, z \in S$:

1. $x \leq x$
2. $x \leq y, y \leq x \Rightarrow x = y$
3. $x \leq y, y \leq z \Rightarrow x \leq z$

1.5.2 Total Order

Total/Linear order: Either $x \leq y$ or $y \leq x$.

Ordered field is a field K with \leq total order.

Definition:

1. If $x \leq y$ then $x + z \leq y + z$ and
2. if $x \geq 0, y \geq 0$ then $x \times y \geq 0$

There is no total order in complex numbers.

First example:

$$\mathbb{Q} = \{(a, b)\}, (a, b) = \frac{a}{b}$$

$$\text{Since } a \geq 0, b > 0$$

$\therefore \mathbb{Q}$ is an ordered set.

Second example:

$$x \geq 0 \Leftrightarrow -x \leq 0$$

$$x \geq 0 \Rightarrow x^2 \geq 0$$

$$x \leq 0 \Rightarrow (-x)^2 = x^2 \geq 0$$

$$1^2 = 1 > 0$$

$$2 > 1$$

$$3 > 2$$

$$\vdots$$

$$n > n - 1$$

1.5.3 Least-upper-bound Property

\mathbb{Q} : Ordered field of rational numbers (with gaps)

Least-upper-bound property: K has least-upper-bound property if any bounded subset $E \subset K$ has least upper bound.

K is a field with order relation \leq , $E \subset K$ and E is *bounded above* if $\exists \alpha \in K$ such that $p \leq \alpha, p \in E$.



β is the *least-upper-bound* of E if

1. β is an upper bound,
2. for any other upper bound α , we have $\beta \leq \alpha$.

We call $\beta = \sup E$.

We then need to prove that \mathbb{Q} does not have least-upper-bound property, that is, there are gaps in \mathbb{Q} .

Proof.

$$\begin{aligned} E = \{q \in \mathbb{Q} : q^2 \leq 2\} &\Rightarrow \text{no } \sup E \\ q \in E &\Leftrightarrow -q \in E \quad \text{and} \quad q \geq 0 \end{aligned}$$

Let $p \in \mathbb{Q}$ such that $p \geq 0, p^2 > 2$.

$$\begin{aligned} \therefore p^2 > 2 &\geq q^2 \Rightarrow p^2 \geq q^2 \\ p^2 - q^2 &= (p+q)(p-q) \geq 0 \quad (\text{property of ordered field}) \\ \therefore p &\geq 0, q > 0 \\ \therefore p+q &\geq 0+q = q \geq 0 \\ \therefore p &\geq q \\ p \in \mathbb{Q}, p &\geq 0, p^2 > 2 \text{ are upper bound of } E. \end{aligned}$$

Remark: Let p be upper bound of E , $\forall q \in E, q \leq p, p > 0$.

Define p' :

$$\begin{aligned} p' &= p - \frac{p^2 - 2}{p + 2} = \frac{2p + 2}{p + 2} = 2\frac{p + 1}{p + 2} \\ \therefore p'^2 - 2 &= 2\frac{p^2 - 2}{(p + 2)^2} \end{aligned}$$

In the above equation, $p^2 - 2 \leq 0$ and $(p + 2)^2 \geq 0$.

Assume $p \in E \Rightarrow p^2 \leq 2 \Rightarrow p^2 - 2 \leq 0$.

$\therefore p'^2 - 2 \leq 0 \Rightarrow p' \in E$ and $p' \geq p$.

\therefore Either $p' = p$ or $p' > p$.

But neither of them is possible since $\sqrt{2}$ is irrational:

$$\begin{aligned} p = p' &\Rightarrow p^2 = 0, p \in \mathbb{Q} \text{ but } p \text{ is irrational.} \\ \therefore p &\notin E. \text{ All upper bounds of } E \text{ are } \{p \in \mathbb{Q}, p^2 > 2\} \end{aligned}$$

r : an upper bound, and $r^2 \geq 2$

$$r' = r - \frac{r^2 - 2}{r^2 + 2} \quad \therefore r' < r$$

$$r'^2 - 2 = 2 \frac{r^2}{(r + 2)^2} > 0 \quad \therefore r'^2 > 2$$

$\therefore r'$ is an upper bound of E .

So we have no upper bound property in E . □

1.6 Real Numbers

1.6.1 Construction of Real Numbers

Theorem. *There exists a total ordered field \mathbb{R} which has least upper bound property. So every subset $E \subset \mathbb{R}$, are bounded above, has a supremum.*

*Such field is **unique**.*

$$K \xrightarrow{\varphi} K'$$

$$\varphi(x + y) = \varphi(x) + \varphi(y)$$

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$$

if bijective, then isomorphism; otherwise, morphism.

History of construction of real numbers: Dedekind used cuts and Cantor used Cauchy sequence, which works for more general occasions, in 1872.

What is *cuts*?

$E \subset \mathbb{Q}, E \neq \mathbb{Q} \rightarrow E$ is bounded above

$q \in \mathbb{Q}, E_q = \{p \in \mathbb{Q} : p < q\}$

If $\alpha \in E, \beta < \alpha \Rightarrow \beta \in \alpha$

$\gamma \in E, \delta \in E, \delta > \gamma$

1.6.2 Archimedean Property

Theorem (Archimedean Property).

$$x, y \in \mathbb{R}, x > 0, y > 0$$

$$\exists n \in \mathbb{Z}_+, n \cdot x > y$$

Proof. Assume $\{nx \mid n \in \mathbb{Z}\}$ is bounded above, i.e. has least upper bound property.

$$\begin{aligned} \exists \alpha &= \sup\{nx \mid n \in \mathbb{Z}\} \\ n \cdot x &\leq \alpha, \forall n \text{ and } \alpha - x < \alpha \\ \therefore \alpha &= \sup\{nx \mid n \in \mathbb{Z}\} \\ \therefore \alpha - x &\text{ is NOT an upper bound.} \\ \exists m &\text{ such that } \alpha - x < n \cdot x \\ \therefore \alpha &< (n+1)x \\ \therefore &\text{ Contridication.} \\ \therefore \{nx \mid n \in \mathbb{R}\} &\text{ is not bounded above.} \end{aligned}$$

□

1.6.3 Density of Real Numbers

Proof. Assume $x, y \in \mathbb{R}$ and $x < y$.

There exists $q \in \mathbb{Q}$ such that $x < q < y$. Because $y - x > 0$ and $1 > 0$, so there exists n such that $n(y - x) > 1$.

$$\begin{aligned} nx &< m_1, \quad m_1 \in \mathbb{Z} \\ -nx &< m_2, \quad m_2 \in \mathbb{Z} \\ \therefore -m_2 &< nx < m_1 \end{aligned}$$

Conclusion: $\exists m \in \mathbb{Z}, m - 1 \leq nx < m$, so $nx < m \leq nx + 1 < ny$.

$$\begin{aligned} nx &< m < ny \\ m &\leq mx + 1 \\ \therefore x &< \frac{m}{n} < y \end{aligned}$$

□

1.6.4 Property of Real Numbers

We have $x > 0, y > 0, n \geq 2$, and $y^n = x$, such y is unique.

We first need to prove **uniqueness**:

Proof. We have $y_1, y_2 > 0, y_1^n = x, y_2^n = x \Rightarrow y_1 = y_2$

We assume $y_1 \neq y_2$ and $0 < y_1 < y_2$. If $a > 0$, then $ay_1 > ay_2$.

We claim $y_1^n < y_2^n$, then we apply mathematical induction:

When $n = 1$, $y_1 < y_2$.

$$\begin{aligned}
y_1 y_1^n &< y_1^n y_2 < y_2 y_2^n \\
y_1^{n+1} &< y_2^{n+1} \\
\therefore y_1^n &< y_2^n
\end{aligned}$$

But they should both be equal to x , therefore we have a contradiction. \square

We then need to prove **existence**:

$$E = \{t \in \mathbb{R} \mid t^n < x, x > 0, x \in \mathbb{R}\}$$

Proof. We first need to show that set E is not empty.

We construct $t = \frac{x}{x+1} \Rightarrow 0 < t < 1$ and $t^n < t^{n-1} < \dots < t < 1$

$$\begin{aligned}
t &= \frac{x}{x+1} \\
x &= t + tx \\
t &= x - tx < x \\
\therefore t^n &< t < x
\end{aligned}$$

\square

We then need to show that E is bounded above:

Proof. Suppose $S \geq x + 1 \Rightarrow S > 1$, so $S^m > S^{m-1} > \dots > S$, therefore $S^m > x + 1 > S$.

It follows that if $t \in E$, then $t < x + 1 \Rightarrow x + 1$ is an upper bound of E .

$\exists y = \sup E, y > 0$ \square

We claim $y^n = x$, since $y^n < x$ and $y^n > x$ are both contradictions.

For the first case of contradictions:

$$\frac{x - y^n}{n(y+1)^{n-1}} > 0$$

We have $0 < n < 1$ and $h < \frac{x - y^n}{n(y+1)^{n-1}}$.

$$(y + h)^n - y^n$$

$$\begin{aligned}
(y+h)^{n-k-1} * k &< (y+h)^{n-k-1} * (y+h)^k \\
&= (y+h)^{n-1} \\
&< n * h * (y+h)^{n-1} < x - y^n \\
\therefore (y+h)^n - y^n &< x - y^n \\
(y+h)^n &< x \\
y+h &\in E \text{ and } \sup E = y < y+h
\end{aligned}$$

Contradiction.

For the first case of contradictions:

$$y^n > x$$

We have $k = \frac{y^n - x}{ny^{n-1}} > 0$.

$$\begin{aligned}
\therefore 0 < k &< \frac{y^n}{ny^{n-1}} = \frac{y}{n} < y \\
\therefore 0 < k &< y \text{ and } 0 < y - k \leq t
\end{aligned}$$

$$\begin{aligned}
y^n - t^n &\leq y^n - (y-k)^n \\
&< y^{n-1} < kny^{n-1} = y^n - x \\
\therefore t^n &> x \Rightarrow t \notin E \\
\therefore y - k &\notin E \text{ is an upper bound of } E
\end{aligned}$$

1.7 Complex Number

1.7.1 Construction of Complex Numbers

$$\begin{aligned}
\mathbb{R}^2 &= \{(a, b) | a, b \in \mathbb{R}\} \text{ forms abelian group} \\
(a, b) + (a', b') &= (a + a', b + b') \quad \therefore (0, 0) = 0 \\
-(a, b) &= (-a, -b) \\
\text{Multiplication: } (a, b) \cdot (a', b') &= (aa' - bb', a'b + ab') \\
\text{Identity for mult.: } (1, 0) &= \mathbf{1} \text{ and } (a, b) \cdot (1, 0) = (a, b)
\end{aligned}$$

$\therefore \mathbb{R}^2$ is a ring and $(a, b) \neq (0, 0)$.

For any such elements, we can form

$$(a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right)$$

$$(a, b) \cdot (a, b)^{-1} = (1, 0) = \mathbf{1}$$

$\therefore \mathbb{R}^2$ is a field of complex numbers, that is, \mathbb{C} .

$$\therefore (0, 1)^2 = (-1, 0) = -\mathbf{1}$$

$$(0, -1)^2 = -\mathbf{1}$$

$$\therefore i = (0, 1)$$

$$(a, b) = a \cdot (1, 0) + b \cdot (0, 1) = a + ib$$

1.7.2 Automorphism of Complex Numbers

$$z = (a, b) \text{ and } \bar{z} = (a, -b) \text{ (complex conjugate)}$$

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$$

$$\overline{z_1 * z_2} = \bar{z}_1 * \bar{z}_2$$

$$z * \bar{z} = (a, b) * (a, -b) = (a^2 + b^2, 0) = (a^2, b^2)$$

We can extend from \mathbb{R} to \mathbb{C} , so we have $a \in \mathbb{R}$ and $(a, 0) \in \mathbb{C}$, therefore \mathbb{R} is a subfield of \mathbb{C} .

Absolute value of complex number z :

$$\sqrt{z\bar{z}} = \sqrt{a^2 + b^2} = |z| > 0$$

2 Basic Topology

Metric (distance function) of x_0 and x : $d(x_0, x) = |x - x_0|$

2.1 Metric Space M

$$d: M \times M \rightarrow \mathbb{R}$$

1. $d(x_0, x_1) \geq 0$ where $x_0, x_1 \in M$
2. $d(x_0, x_1) = 0 \iff x_0 = x_1$
3. $d(x_0, x_1) = d(x_1, x_0)$ (irrespective of order)

4. $d(x, z) \leq d(x, y) + d(y, z)$ (triangular inequity)

Euclidean metric on \mathbb{R}^2 : $d(x, y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2}$

Discrete metric: $d(x, y) = \begin{cases} 1 & \text{if } x \neq y \\ 0 & \text{if } x = y \end{cases}$

Open ball of radius ϵ : $B_\epsilon(x_0) = B(x_0, \epsilon) = \{y \in M \mid d(x_0, y) < \epsilon\}$

2.2 Open Sets

2.2.1 Metric Spaces X

$U \subset X$ is open if for any $x \in U$ there exists $\epsilon > 0$ such that $B(x, \epsilon) \subset U$.

Open interval is open set; closed interval is not open set.

2.2.2 Topological Spaces (X, U)

Let U be a family of all sets, X be a set. U is a **topology** on X if

1. \emptyset (Empty set) is always open; X is open. $\Leftrightarrow \emptyset$ and X itself belong to U .
2. F is a collection of open sets, then $\bigcup_{U \in F} U$ is open. \Leftrightarrow Any union of members of U still belongs to U . (Union)
3. F is a *finite* collection of open sets, then $\bigcap_{U \in F} U$ is open. \Leftrightarrow The intersection of any finite number of members of U belongs to U . (Intersection)

Finite case: $x \in \bigcap_{U \in F} U$, $x \in U$, hence $B(x, \epsilon_U) \subset U$

$$\delta = \min \epsilon_U > 0 \quad \text{where } U \in F$$

$$B(x, \delta) \subset B(x, \epsilon_U) \subset U$$

$$\therefore B(x, \delta) \subset \bigcap_{U \in F} U$$

Infinite case: For example, the intersection of all intervals of $(-\frac{1}{n}, \frac{1}{n})$, where n is a positive number, is the set $\{0\}$ which is not open in the real line.

2.3 Compact Sets

In metric space X , compact sets are closed.

Compact \Leftrightarrow closed and bounded (only for Euclidean metric, \mathbb{R}^n)