

baby-rudin reading notes

weiyuan

2022 年 10 月 25 日

第一章 the real and complex number system

1.1 Introduction

First we use $\sqrt{2}$ to construct real number system from integer and rational numbers.

Example 1.1.

$$p^2 = 2 \quad (1.1)$$

p is not a rational number.

证明. (反证法) 假设 p 是有理数, $\exists m, n \in \mathbf{N}$, s.t. $p = m/n$. $\gcd(m, n) = 1$. Then 1.1

$$m^2 = 2n^2. \quad (1.2)$$

m is even, $m = 2k$. 那么有 $(2k)^2 = 2n^2$, $2k^2 = n^2$, k is even, $\gcd(m, n) = 2 \neq 1$, contrary to our choice of m and n . Hence p can't be a rational number. \square

After proving $\sqrt{2}$ isn't a rational number, rudin use $\sqrt{2}$ to divide the rationals 在证明 $\sqrt{2}$ 不是有理数后, 使用 $\sqrt{2}$ 将有理数集分成两部分. 引出了分划的概念?

$$A = \{p | p^2 < 2\}$$

$$B = \{p | p^2 > 2\}$$

A contains no largest number,

B contains no smallest number.

$$\forall p \in A, \exists q \in A, \text{ s.t. } p < q,$$

$$\forall p \in B, \exists q \in B, \text{ s.t. } p > q,$$

$$\forall p > 0$$

$$q = p - \frac{p^2 - 2}{p + 2} = \frac{2p + 2}{p + 2} \quad (1.3)$$

Then

$$q^2 - 2 = \frac{2(p^2 - 2)}{(p + 2)^2} \quad (1.4)$$

If $p \in A$, $p^2 < 2$. 1.3 shows that $q > p$, 1.4 shows that $q^2 < 2$, $q \in A$. If $p \in B$, $p^2 > 2$. 1.3 shows that $q < p$, 1.4 shows that $q^2 > 2$, $q \in B$.

Remark 1.2. The purpose of the above discussion has been to show that the rational number system has certain gaps, in spite of the fact that between any two rationals there is another: If $r < s$ then $r < (r + s)/2 < s$. The real number system fills these gaps. This is the principal reason for the fundamental role which it plays in analysis.

mynotes:

有理数的稠密性与实数的连续性. 在分析中, 考察极限等需要的是数系的连续性, 因此需要先建立实数系. 事实上, 我们是先有微积分, 后有实数理论的. 三次数学危机: 无理数, 微积分基础, 集合论实数理论是极限的基础.

In order to elucidate its structure, as well as that of the complex numbers, we start with a brief discussion of the genral concepts of *ordered set* and *field*.

mynotes:

rudin 引入复数的方法非常怪, 对初学者非常不友好, 过于抽象了. 想起一个法国笑话, 问小学生 $2 + 3$ 等于几, 回答 $2 + 3 = 3 + 2$ 加法是一个交换群 (Abel 群) ...

Here is some of the standard set-theoretic terminology taht will be used throughout this book.

mynotes:

接下来引入一些集合论的定义

Definition 1.3. If A is any set (whose elements¹ may be numbers or any other objects²), we write $x \in A$ to indicate that x is a member (or an element) of A .

If x is not a member of A , we write: $x \notin A$.

empty set \emptyset contains no element, If a set has at least one element, it is called *nonempty*.

A, B are sets, $\forall x \in A, x \in B$, we say that A is a *subset* of B , $A \subset B$ or $B \supset A$. If $\exists x \in B, x \notin A$, A is a *proper subset* of B , $A \subsetneq B$. Note that $A \subset A$ for every set A .

(Bernstein) If $A \subset B$ and $B \subset A$, we write $A = B$. Otherwise $A \neq B$.

mynotes:

这条性质在证明集合相等时很常用

Definition 1.4. Throughout Chap. 1, the set of all rational numbers will be denoted by \mathbb{Q} .

有理数集 \mathbb{Q}

1.2 Ordered sets

有序集

¹这里 elements 还没定义, 笑啦

²object 指代什么? 我个人认为集合理解的难点在于集合的集合. 这一点可以引出罗素悖论

Definition 1.5. Let S be a set. An *order* on S is a relation, denoted by $<$, with the following two properties:

(i) If $x \in S$ and $y \in S$ then one and only one of the statements

$$x < y, \quad x = y, \quad y < x$$

The statement $x < y$ may be read as x is less than y , or x is smaller than y , or x precedes y . (It's often convenient to write $y > x$ in place of $x < y$) (less-great, smaller-bigger, precedes-succeeds)

(ii) If $x, y, z \in S$, if $x < y$ and $y < z$, then $x < z$.

$x \leq y$ indicates that $x < y$ or $x = y$, without specifying which of these two is to hold. In other words, $x \leq y$ is the negation of $x > y$.

mynotes:

偏序关系: 1. 三歧性, 2. 传递性.

建立偏序关系后, 可以使用不等式进行分析. 在后续根据极限定义计算时, 需要大量使用不等式分析数列和函数的极限计算结果.

Definition 1.6. An *ordered set* is a set S in which an order is defined.

For Example, \mathbb{Q} is an ordered set if $r < s$ is defined to mean that $s - r$ is a positive rational number.

mynotes:

存在偏序关系的集合称为有序集 \mathbb{Q}, \mathbb{R} 均是有序集, 但 \mathbb{C} 不是有序集.

Definition 1.7. Suppose S is an ordered set, and $E \subset S$. If there exists a $\beta \in S$ such that $x \leq \beta$ for every $x \in E$, we say that E is *bounded above*, and call β an *upper bound* of E .

Lower bounds are defined in the same way (with \geq in place of \leq).

Definition 1.8. Suppose S is an ordered set, $E \subset S$, and E is bounded above. Suppose there exists an $\alpha \in S$ with the following properties:

(i) α is an upper bound of E . (ii) If $\gamma < \alpha$ then γ is not an upper bound of E .

Then α is called the *least upper bound* of E [that there is at most one such α is clear from (ii)] or the *supremum* of E , and we write

$$\alpha = \sup E.$$

The *greatest lower bound*, or *infimum*, of a set E which is bounded below is defined in the same manner: The statement

$$\alpha = \inf E$$

means that α is a lower bound of E and that no β with $\beta > \alpha$ is a lower bound of E .

mynotes:

从上界引出最小上界, 没有直接定义最大下界, 而是使用对称定义引出. 从最小上界引出的最小上界性质更为常用. Dedekind 分划

Example 1.9. (a) Consider the set A, B

$$A = \{p | p^2 < 2\}, \quad B = \{p | p^2 > 2\}.$$

A has no least upper bound in \mathbb{Q} . B has no greatest lower bound in \mathbb{Q} .

(b) If $\alpha = \sup E$ exists, α may be or may not be a member of E .

$$E_1 = \{r | r \in \mathbb{Q}, r < 0\}$$

$$E_2 = \{r | r \in \mathbb{Q}, r \leq 0\}$$

$$\sup E_1 = \sup E_2 = 0,$$

and $0 \notin E_1, 0 \in E_2$.

(c) $E = \{1/n | n = 1, 2, 3, \dots\}$. Then $\sup E = 1$, which is in E , and $\inf E = 0$, which is not in E .

Definition 1.10. *least-upper-bound property*

An ordered set S is said to have the *least-upper-bound property* if the following is true:

If $E \subset S$, E is not empty, and E is bounded above, then $\sup E$ exists in S .

Example 1.9(a) shows that \mathbb{Q} does not have the least-upper-bound property.

We shall now show that there is a close relation between greatest lower bounds and least upper bounds, and that every ordered set with the least-upper-bound property also has the greatest-lower-bound property.

Theorem 1.11. *Suppose S is an ordered set with the least-upper-bound property, $B \subset S$, B is not empty, and B is bounded below. Let L be the set of all lower bounds of B . Then*

$$\alpha = \sup L$$

exists in S , and $\alpha = \inf B$.

In particular, $\inf B$ exists in S .

证明. Since B is bounded below, L is not empty. Since L consists of exactly those $y \in S$ which satisfy the inequality $y \leq x$ for every $x \in B$, we see that every $x \in B$ is an upper bound of L . Thus L is bounded above. Our hypothesis about S implies therefore that L has a supremum in S ; call it α .

If $\gamma < \alpha$ then (see Definition 1.8) γ is not an upper bound of L , hence $\gamma \notin B$. It follows that $\alpha \leq x$ for every $x \in B$. Thus $\alpha \in L$.

If $\alpha < \beta$ then $\beta \notin L$, since α is an upper bound of L .

We have shown that $\alpha \in L$ but $\beta \notin L$ if $\beta > \alpha$. In other words, α is a lower bound of B , but α is not if $\beta > \alpha$. This means that $\alpha = \inf B$. □

mynotes:

这个证明第一次看比较难理清我试着用自己的话重写梳理一下：已知条件 S , ordered set + least-upper-bound property. $B \in S$, $B \neq \emptyset$, B is bounded below. L is the set of all lower bounds of B . $\exists \alpha \in S$, $\alpha = \sup L$, and $\alpha = \inf B$.

证明. 思路由最小上界 \rightarrow 最大下界 $L = \{y | y \in S; \forall x \in B, y \leq x\}$ 关于 L 中有没有不在 S 中的元素这一点我还没想明白. 定理中只是说 L 是 B 的下界组成的. B 是 S 的子集, 但 B 的下界不一定全在 S 中.

L 由 B 在 S 中的全部下界组成

$\forall x \in B$, x 为 L 的上界. $L \subset S$. S 有最小上界性质, $\therefore \exists \alpha \in S$, $\alpha = \sup L$.

$\forall \gamma < \alpha$ 由 $\alpha = \sup L$ 的定义 (1.8) γ 不是 L 的上界.

$\forall x \in B$, x 为 L 的上界, $x \geq \alpha$. $\therefore \alpha \in L$.

$\alpha < \beta$, $\alpha = \sup L$. $\therefore \beta \notin L$. L 由 B 在 S 中的全部下界组成, $\beta \notin L$. β 不是 B 的下界.

$\therefore \alpha = \inf B$, $\inf B \in S$. □

1.3 fields

mynotes:

域, 交换除环 $\langle \mathbb{R}, +, \times \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$, $\langle \mathbb{R} \setminus \{0\}, \times \rangle$ 都是交换群, 且满足分配律. 则 $\langle \mathbb{R}, +, \times \rangle$ 是域.

Definition 1.12. (A) Axioms for addition

(A1) If $x \in F$ and $y \in F$, then their sum $x + y$ is in F .

(A2) Addition is commutative: $x + y = y + x$ for all $x, y \in F$.

(A3) Addition is associative: $(x + y) + z = x + (y + z)$ for all $x, y, z \in F$.

(A4) F contains an element 0 such that $0 + x = x$ for every $x \in F$.

(A5) To every $x \in F$ corresponds an element $-x \in F$ such that

$$x + (-x) = 0.$$

(M) Axioms for multiplication

(M1) If $x \in F$ and $x \in F$, then their product xy is in F .

(M2) Multiplication is commutative: $xy = yx$ for all $x, y \in F$.

(M3) Multiplication is associative: $(xy)z = x(yz)$ for all $x, y, z \in F$.

(M4) F contains an element $1 \neq 0$ such that $1x = x$ for every $x \in F$.

(M5) If $x \in F$ and $x \neq 0$ then there exists an element $1/x \in F$ such that

$$x \cdot (1/x) = 1.$$

(D) The distributive law

$$x(y + z) = xy + xz$$

holds for all $x, y, z \in F$.

Remark 1.13. (a) Our usual writes (in any field)

只定义了加法和乘法, 使用逆元分别表示减法和除法. $x - y = x + (-y)$, $x/y = x \cdot (1/y)$.

(b) The field axioms clearly hold in \mathbb{Q} , the set of all rational numbers, if addition and multiplication have their customary meaning. Thus \mathbb{Q} is a field.

全体有理数的集合是一个域.

(c) Although it is not our purpose to study fields (or any other algebraic structures) in detail, it is worthwhile to prove that some familiar properties of \mathbb{Q} are consequences of the field axioms; once we do this, we will not need to do it again for the real numbers and for the complex numbers.

Proposition 1.14. The axioms for addition imply the following statements.

(a) If $x + y = x + z$ then $y = z$.

(b) If $x + y = x$ then $y = 0$.

(c) If $x + y = 0$ then $y = -x$.

(d) $-(-x) = x$.

Statement (a) is a cancellation law. Note that (b) asserts the uniqueness of the element whose existence is assumed in (A4), and that (c) does the same for (A5).

mynotes:

what is the difference between axiom and proposition?

An axiom is a proposition regarded as self-evidently true without proof. The word "axiom" is a slightly archaic synonym for postulate. Compare conjecture or hypothesis, both of which connote apparently true but not self-evident statements. A proposition is a mathematical statement such as "3 is greater than 4," "an infinite set exists," or "7 is prime." An axiom is a proposition that is assumed to be true. With sufficient information, mathematical logic can often categorize a proposition as true or false, although there are various exceptions (e.g., "This statement is false"). <https://www.nutritionmodels.com/terminology.html>

证明. Proof(rudin)

If $x + y = x + z$, the axioms (A) give

$$\begin{aligned} y &= 0 + y = (-x + x) + y = -x + (x + y) \\ &= -x + (x + z) = (-x + x) + z = 0 + z = z \end{aligned}$$

This proves (a). Take $z = 0$ in (a) to obtain (b). Take $z = -x$ in (a) to obtain (c). Since $-x + x = 0$, (c) (with $-x$ in place of x) gives (d). \square

mynotes:

mynotes 我自己证明上述四条性质时都是从定义开始的, 而 rudin 这里在后面的证明中都利用了刚推导出的结论, 这一点需要借鉴.

Proposition 1.15. The axioms for multiplication imply the following statements.

- (a) If $x \neq 0$ and $xy = xz$ then $y = z$.
- (b) If $x \neq 0$ and $xy = x$ then $y = 1$.
- (c) If $x \neq 0$ and $xy = 1$ then $y = 1/x$.
- (d) If $x \neq 0$ then $1/(1/x) = x$.

The proof is so similar to that of Proposition 1.14 that we omit it.

证明. mynotes (a),

$$\begin{aligned} y &= 1 \cdot y = \left(\frac{1}{x} \cdot x\right) y = \frac{1}{x} (xy) \\ &= \frac{1}{x} (xz) = \left(\frac{1}{x} x\right) z = z \end{aligned}$$

- (b), (a) 取 $z = 1$. $y = z = 1$.
- (c), (a) 取 $z = \frac{1}{x}$. $y = z = \frac{1}{x}$.
- (d), (c) 取 $x = \frac{1}{x'}$. $y = 1/(1/x')$.

□

Proposition 1.16. The field axioms imply the following statements, for any $x, y, z \in F$.

- (a) $0x = 0$.
- (b) If $x \neq 0$ and $y \neq 0$ then $xy \neq 0$.
- (c) $(-x)y = -(xy) = x(-y)$.
- (d) $(-x)(-y) = xy$.

证明. $0x + 0x = (0 + 0)x = 0x$. Hence 1.14(b) implies that $0x = 0$, and (a) holds.

Next, assume $x \neq 0$, $y \neq 0$, but $xy = 0$. Then (a) gives

$$1 = \left(\frac{1}{y}\right) \left(\frac{1}{x}\right) xy = \left(\frac{1}{y}\right) \left(\frac{1}{x}\right) 0 = 0.$$

a contradiction. Thus (b) holds.

The first equality in (c) comes from

$$(-x)y + xy = (-x + x)y = 0y = 0,$$

combined with 1.14(c); the other half of (c) is proved in the same way.

Finally,

$$(-x)(-y) = -[x(-y)] = -[-(xy)] = xy$$

by (c) and 1.14(d).

□

Definition 1.17. An ordered field is a field F which is also an ordered set, such that

- (i) $x + y < x + z$ if $x, y, z \in F$ and $y < z$,
- (ii) $xy > 0$ if $x \in F$, $y \in F$, $x > 0$, and $y > 0$.

If $x > 0$, we call x positive; if $x < 0$, x is negative.

For example, \mathbb{Q} is an ordered field.

All the familiar rules for working with inequalities apply in every ordered field: Multiplication by positive [negative] quantities preserves [reverses] inequalities, no square is negative, etc. The following proposition lists some of these.

mynotes:

有序域 F 也是有序集, 由于有理数域 \mathbb{Q} , 实数域 \mathbb{R} 都是有序域, 这里使用有理数域 \mathbb{Q} 证明的有序集的性质也可以直接用于实数域 \mathbb{R} .

Proposition 1.18. The following statements are true in every ordered field.

- (a) If $x > 0$ then $-x < 0$, and vice versa.
- (b) If $x > 0$ and $y < z$ then $xy < xz$.
- (c) If $x < 0$ and $y < z$ then $xy > xz$.
- (d) If $x \neq 0$ then $x^2 > 0$. In particular, $1 > 0$.
- (e) If $0 < x < y$ then $0 < l/y < l/x$.

证明. (a) $x > 0, -x < 0$.

$$\begin{aligned} x > 0 &= (x + -x) \\ x + 0 &> x + (-x) \\ (-x) &< 0 \end{aligned}$$

(b) $x > 0, y < z, xy < xz$.

$$\begin{aligned} y < z, z - y &> y - y = 0 \\ x(z - y) &> 0 \\ x(z - y) + xy &> 0 + xy \\ xz &> xy \end{aligned}$$

(c)

$$\begin{aligned} (z - y) &> y - y = 0 \\ x < 0, (-x) &> 0. \quad (-x)(z - y) > 0 \\ x(z - y) &< 0 \\ xz &< xy \end{aligned}$$

(d)

$$\begin{aligned} x &> 0 & x^2 &> 0 \\ x &< 0 & (-x)^2 &> 0, (-x)^2 = -[x(-x)] = -(-(x \cdot x)) = x^2, x^2 > 0 \end{aligned}$$

$\therefore 1^2 = 1, 1 > 0$.

(e) If $y > 0$ and $v \leq 0$, then $yv \leq 0$. But $y \cdot (1/y) = 1 > 0$. Hence $1/y > 0$. Likewise, $1/x > 0$. If we multiply both sides of the inequality $x < y$ by the positive quantity $(1/x)(1/y)$, we obtain $1/y < 1/x$. \square

1.4 THE REAL FIELD

We now state the *existence theorem* which is the core of this chapter.

Theorem 1.19. *There exists an ordered field \mathbb{R} which has the least-upper-bound property.*

Moreover, \mathbb{R} contains \mathbb{Q} as a subfield.

The second statement means that $\mathbb{Q} \subset \mathbb{R}$ and that the operations of addition and multiplication in \mathbb{R} , when applied to members of \mathbb{Q} , coincide with the usual operations on rational numbers; also, the positive rational numbers are positive elements of \mathbb{R} .

The members of \mathbb{R} are called real numbers.

The proof of Theorem 1.19 is rather long and a bit tedious and is therefore presented in an Appendix to Chap. 1. The proof actually constructs \mathbb{R} from \mathbb{Q} .

The next theorem could be extracted from this construction with very little extra effort. However, we prefer to derive it from Theorem 1.19 since this provides a good illustration of what one can do with the least-upper-bound property.

mynotes:

\mathbb{R} 具有最小上界性质的有序域 least-upper-bound \rightarrow upper bound in the sets.
ordered field (ordered set, field).

$\mathbb{Q} \in \mathbb{R}$ subfield

$x \in \mathbb{R}$, x is a real number

mynotes:

proof of theorem 1.19 is tedious. construct \mathbb{R} from \mathbb{Q}

tedious 乏味的, 冗长的

derive 取得, 得到

Theorem 1.20. (*archimedean property of \mathbb{R}*) (a) *If $x \in \mathbb{R}$, $y \in \mathbb{R}$, and $x > 0$, then there is a positive integer n such that*

$$nx > y$$

(b) *If $x \in \mathbb{R}$, $y \in \mathbb{R}$, and $x < y$, then there exists a $p \in \mathbb{Q}$ such that $x < p < y$.*

Theorem 1.21. *For every real $x > 0$ and every integer $n > 0$ there is one and only one positive real y such that $y^n = x$.*

This number y is written $\sqrt[n]{x}$ or $x^{1/n}$.

Corollary If a and b are positive real numbers and n is a positive integer, then

$$(ab)^{1/n} = a^{1/n}b^{1/n}.$$

Definition 1.22. (Decimals) We conclude this section by pointing out the relation between real numbers and decimals.

1.5 THE EXTENDED REAL NUMBER SYSTEM

Definition 1.23. The extended real number system consists of the real field \mathbb{R} and two symbols, $+\infty$ and $-\infty$. We preserve the original order in \mathbb{R} , and define

$$-\infty < x < +\infty$$

for every $x \in \mathbb{R}$

(a) If x is real then

$$x + \infty = +\infty, \quad x - \infty = -\infty, \quad \frac{x}{+\infty} = \frac{x}{-\infty} = 0.$$

(b) If $x > 0$ then $x \cdot (+\infty) = +\infty$, $x \cdot (-\infty) = -\infty$.

(c) If $x < 0$ then $x \cdot (+\infty) = -\infty$, $x \cdot (-\infty) = +\infty$.

1.6 THE COMPLEX FIELD

mynotes:

rudin 引入复数定义的方法很奇怪, 代数角度是一致的, 但理解起来比较困难, 我觉得使用几何方法引入复数更为合理且直观, rudin 这里对初学者不太友好

Definition 1.24. A complex number is an ordered pair (a, b) of real numbers. "Ordered" means that (a, b) and (b, a) are regarded as distinct if $a \neq b$.

Let $x = (a, b)$, $y = (c, d)$ be two complex numbers. We write $x = y$ if and only if $a = c$ and $b = d$. (Note that this definition is not entirely superfluous; think of equality of rational numbers, represented as quotients of integers.) We define

$$\begin{aligned} x + y &= (a + c, b + d), \\ xy &= (ac - bd, ad + bc). \end{aligned}$$

Theorem 1.25. These definitions of addition and multiplication turn the set of all complex numbers into a field, with $(0, 0)$ and $(1, 0)$ in the role 0 and 1.

proof (A1)–(A5), (M1)–(M5) and (D), then we can prove that \mathbb{C} is a field.

Theorem 1.26. *For any real numbers a and b we have*

$$(a, 0) + (b, 0) = (a + b, 0), \quad (a, 0)(b, 0) = (ab, 0).$$

The proof is trivial.

show that the notation (a, b) is equivalent to the more customary $a + bi$.

Definition 1.27. $i = (0, 1)$

Theorem 1.28. $i^2 = -1$

证明.

$$i^2 = (0, 1)(0, 1) = (-1, 0) = -1.$$

□

Theorem 1.29. *If a and b are real, then $(a, b) = a + bi$.*

证明.

$$\begin{aligned} a + bi &= (a, 0) + (b, 0)(0, 1) \\ &= (a, 0) + (0, b) = (a, b) \end{aligned}$$

□

Definition 1.30. $a, b \in \mathbb{R}$, $z = a + bi$, the complex number $\bar{z} = a - bi$ is called the conjugate of z . the numbers a and b are the real part and imaginary part of z . respectively.

$$a = \Re(z), \quad b = \Im(z)$$

Theorem 1.31. *If z and w are complex, then*

- (a) $z + w = \bar{z} + \bar{w}$,
- (b) $z\bar{w} = \bar{z} \cdot \bar{w}$,
- (c) $z + \bar{z} = 2\Re(z)$, $z - \bar{z} = 2\Im(z)$,
- (d) $z\bar{z}$ is real and positive (except when $z = 0$).

Proof (a), (b), and (c) are quite trivial. To prove (d), write $z = a + bi$, and note that $z\bar{z} = a^2 + b^2$.

Definition 1.32. If z is a complex number, its absolute value $|z|$ is the nonnegative square root of $z\bar{z}$; that is, $|z| = (z\bar{z})^{1/2}$.

The existence (and uniqueness) of $|z|$ follows from Theorem 1.21 and part (d) of Theorem 1.31.

Note that when x is real, then $\bar{x} = x$, hence $|x| = \sqrt{x^2}$. Thus $|x| = x$ if $x > 0$, $|x| = -x$ if $x < 0$.

Theorem 1.33. *Let z and w be complex numbers. Then*

$$(a) |z| > 0 \text{ unless } z = 0, |0| = 0,$$

$$(b) \bar{\bar{z}} = z,$$

$$(c) |zw| = |z||w|,$$

$$(d) |\Re(z)| \leq |z|,$$

$$(e) |z + w| \leq |z| + |w|.$$

Notation 1.34. (sum) $x_1, x_2, \dots, x_n \in \mathbb{C}$,

$$x_1 + x_2 + \dots + x_n = \sum_{j=1}^n x_j.$$

Theorem 1.35. (Schwarz Inequality)

If $a_1, \dots, a_n, b_1, \dots, b_n$, are complex numbers, then

$$\left| \sum_{j=1}^n a_j \bar{b}_j \right|^2 \leq \sum_{j=1}^n |a_j|^2 \sum_{j=1}^n |b_j|^2.$$

在正式证明之前, 先回忆 \mathbb{R} 中的施瓦茨不等式是怎么证明的. let $A = \sum a_j^2, B = \sum b_j^2, C = \sum a_j b_j$.

$$\sum (a_j + \lambda b_j)^2 = \sum a_j^2 + 2 \sum a_j b_j \lambda + \sum b_j^2 \lambda^2$$

由韦达定理, $\Delta \leq 0, \Delta = (2 \sum a_j b_j)^2 - 4 \sum a_j^2 \sum b_j^2$. 因此 $(\sum a_j b_j)^2 \leq \sum a_j^2 \sum b_j^2$

证明. Put $A = \sum |a_j|^2, B = \sum |b_j|^2, C = \sum a_j \bar{b}_j, j = 1, 2, \dots, n$.

If $B = 0, b_1 = \dots = b_n = 0$, this conclusion is trivial.

If $B > 0$,

$$\begin{aligned} \sum |Ba_j - Cb_j|^2 &= \sum (Ba_j - Cb_j)(B\bar{a}_j - C\bar{b}_j) \\ &= B^2 \sum |a_j|^2 - B\bar{C} \sum a_j \bar{b}_j - BC \sum \bar{a}_j b_j + |C|^2 \sum |b_j|^2 \\ &= B^2 A - B|C|^2 \\ &= B(AB - |C|^2). \end{aligned}$$

Since each term in the first sum is nonnegative, we see that

$$B(AB - |C|^2) \geq 0.$$

Since $B > 0$, it follows that $AB - |C|^2 \geq 0$. This is the desired inequality. \square

我的想法

$$\begin{aligned} \sum (a_j + \lambda \bar{b}_j)(\bar{a}_j + \lambda b_j) &= \sum (a_j \bar{a}_j + \lambda(\bar{a}_j b_j + a_j \bar{b}_j) + \lambda^2 b_j \bar{b}_j) \\ &= \sum (a_j \bar{a}_j + \lambda 2\Re(a_j \bar{b}_j) + \lambda^2 b_j \bar{b}_j) \end{aligned}$$

由韦达定理, $\Delta \leq 0, \Delta = (2 \sum \Re(a_j \bar{b}_j))^2 - 4 \sum a_j \bar{a}_j \sum b_j \bar{b}_j$, (这里推出的结论比原始结论弱? 为什么?)

1.7 Euclidean space

欧式空间

Definition 1.36. For each positive integer k , let \mathbb{R}^k be the set of all ordered k -tuples

$$\mathbf{x} = (x_1, x_2, \dots, x_k),$$

where x_1, x_2, \dots, x_k are real numbers, called the **coordinates** of \mathbf{x} . The elements of \mathbb{R}^k are called points, or vectors, especially when $k > 1$. We shall denote vectors by boldfaced letters. If $\mathbf{y} = (y_1, y_2, \dots, y_k)$ and if α is a real number, put

$$\begin{aligned}\mathbf{x} + \mathbf{y} &= (x_1 + y_1, x_2 + y_2, \dots, x_k + y_k), \\ \alpha\mathbf{x} &= (\alpha x_1, \alpha x_2, \dots, \alpha x_k)\end{aligned}$$

so that $\mathbf{x} + \mathbf{y} \in \mathbb{R}^k$ and $\alpha\mathbf{x} \in \mathbb{R}^k$. This defines addition of vectors, as well as multiplication of a vector by a real number (a scalar). These two operations satisfy the commutative, associative, and distributive laws (the proof is trivial, in view of the analogous laws for the real numbers) and make \mathbb{R}^k into a vector space over the *real field*. The zero element of \mathbb{R}^k (sometimes called the origin or the null vector) is the point $\mathbf{0}$, all of whose coordinates are 0.

We also define the so-called “inner product” (or scalar product) of \mathbf{x} and \mathbf{y} by

$$\mathbf{x} \cdot \mathbf{y} = \sum_{j=1}^k x_j y_j$$

and the norm of \mathbf{x} by

$$|\mathbf{x}| = (\mathbf{x} \cdot \mathbf{x})^{1/2} = \left(\sum_{j=1}^k x_j^2 \right)^{1/2}.$$

The structure now defined (the vector space \mathbb{R}^k with the above inner product and norm) is called euclidean k -space.

Theorem 1.37. Suppose $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{R}^k$, and α is real. Then

- (a) $|\mathbf{x}| \geq 0$;
- (b) $|\mathbf{x}| = 0$ if and only if $\mathbf{x} = \mathbf{0}$;
- (c) $|\alpha\mathbf{x}| = |\alpha||\mathbf{x}|$;
- (d) $|\mathbf{x} \cdot \mathbf{y}| \leq |\mathbf{x}||\mathbf{y}|$;
- (e) $|\mathbf{x} + \mathbf{y}| \leq |\mathbf{x}| + |\mathbf{y}|$;
- (f) $|\mathbf{x} - \mathbf{z}| \leq |\mathbf{x} - \mathbf{y}| + |\mathbf{y} - \mathbf{z}|$.

(f) 为欧式空间中的三角不等式。

证明. Proof (a), (b), and (c) are obvious, and (d) is an immediate consequence of the Schwarz inequality 1.35. By (d) we have

$$\begin{aligned}
 |\mathbf{x} + \mathbf{y}|^2 &= (\mathbf{x} + \mathbf{y}) \cdot (\mathbf{x} + \mathbf{y}) \\
 &= \mathbf{x} \cdot \mathbf{x} + 2\mathbf{x} \cdot \mathbf{y} + \mathbf{y} \cdot \mathbf{y} \\
 &\leq |\mathbf{x}|^2 + 2|\mathbf{x}||\mathbf{y}| + |\mathbf{y}|^2 \\
 &= (|\mathbf{x}| + |\mathbf{y}|)^2.
 \end{aligned}$$

so that (e) is proved. Finally, (f) follows from (e) if we replace \mathbf{x} by $\mathbf{x} - \mathbf{y}$ and \mathbf{y} by $\mathbf{y} - \mathbf{z}$. \square

Remark 1.38. Theorem 1.37 (a), (b), and (f) will allow us (see Chap. 2) to regard \mathbb{R}^k as a metric space.

\mathbb{R}^1 (the set of all real numbers) is usually called the line, or the real line. Likewise, \mathbb{R}^2 is called the plane, or the complex plane (compare Definitions 1.24 and 1.36). In these two cases the norm is just the absolute value of the corresponding real or complex number.

appendix

Theorem 1.19 will be proved in this appendix by constructing \mathbb{R} from \mathbb{Q} . We shall divide the construction into several steps.

Step 1 The members of \mathbb{R} will be certain subsets of \mathbb{Q} , called *cuts*. A cut is, by definition, any set³ $\alpha \subset \mathbb{Q}$ with the following three properties.

- (I) α is not empty, and $\alpha \neq \mathbb{Q}$.
- (II) If $p \in \alpha, q \in \mathbb{Q}$, and $q < p$, then $q \in \alpha$.
- (III) If $p \in \alpha$, then $p < r$ for some $r \in \alpha$.

The letters p, q, r, \dots will always denote rational numbers, and $\alpha, \beta, \gamma, \dots$ will denote cuts.

mynotes:

建立分划定义的这三条性质说明了有理数集是稠密而不是连续的

Note that (III) simply says that α has no largest member: (II) implies two facts which will be used freely:

If $p \in \alpha$ and $q \notin \alpha$ then $p < q$.

If $r \notin \alpha$ and $r < s$ then $s \notin \alpha$.

Step 2 Define “ $\alpha < \beta$ ” to mean: α is a proper subset of β .⁴

Let us check that this meets the requirements of Definition 1.5.

If $\alpha < \beta$ and $\beta < \gamma$ it is clear that $\alpha < \gamma$. (A proper subset of a proper subset is a proper subset.) It is also clear that at most one of the three relations

$$\alpha < \beta, \quad \alpha = \beta, \quad \beta < \alpha.$$

³分划 α 是一个集合

⁴这里使用真子集关系定义了分划 (集合) 间的序

can hold for any pair α, β . To show that at least one holds, assume that the first two fail. Then α is not a subset of β . Hence there is a $p \in \alpha$ with $p \notin \beta$. If $q \in \beta$, it follows that $q < p$ (since $p \notin \beta$), hence $q \in \alpha$, by (II). Thus $\beta \subset \alpha$. Since $\beta \neq \alpha$, we conclude: $\beta < \alpha$.

Thus \mathbb{R} is now an ordered set.

mynotes:

利用集合关系定义的偏序关系具有传递性和三歧性

Step 3 The ordered set \mathbb{R} has the least-upper-bound property.

To prove this, let A be a nonempty subset of \mathbb{R} , and assume that $\beta \in \mathbb{R}$ is an upper bound of A . Define γ to be the union of all $\alpha \in A$. In other words, $p \in \gamma$ if and only if $p \in \alpha$ for some $\alpha \in A$. We shall prove that $\gamma \in \mathbb{R}$ and that $\gamma = \sup A$.

Since A is not empty, there exists an $\alpha_0 \in A$. This α is not empty. Since $\alpha_0 \in \gamma$, γ is not empty. Next, $\gamma \subset \beta$ (since $\alpha \subset \beta$ for every $\alpha \in A$), and therefore $\gamma \neq \mathbb{Q}$. Thus γ satisfies property (I). To prove (II) and (III), pick $p \in \gamma$. Then $p \in \alpha_1$ for some $\alpha_1 \in A$. If $q < p$, then $q \in \alpha_1$, hence $q \in \gamma$; this proves (II). If $r \in \alpha_1$ is so chosen that $r > p$, we see that $r \in \gamma$ (since $\alpha_1 \subset \gamma$), and therefore γ satisfies (III).

Thus $\gamma \in \mathbb{R}$.

It is clear that $\alpha \leq \gamma$ for every $\alpha \in A$.

Suppose $\delta < \gamma$. Then there is an $s \in \gamma$ and that $s \notin \delta$. Since $s \in \gamma$, $s \in \alpha$ for some $\alpha \in A$. Hence $\delta < \alpha$, and δ is not an upper bound of A .

This gives the desired result: $\gamma = \sup A$.

mynotes:

这里分划之间所用的 \in 让我很费解, 上文对分划的定义是集合, 那么应该用子集形式而不是元素形式来描述偏序关系. 分划是不是集合的一个元素? 查询原始 pdf 文件发现确实是子集形式描述的!

Step 4 If $\alpha \in \mathbb{R}$ and $\beta \in \mathbb{R}$ we define $\alpha + \beta$ to be the set of all sums $r + s$, where $r \in \alpha$ and $s \in \beta$.

We define 0^* to be the set of all negative rational numbers. It is clear that 0^* is a cut. We verify that the axioms for addition (see Definition 1.12) hold in \mathbb{R} , with 0^* playing the role of 0.

Step 5 Having proved that the addition defined in Step 4 satisfies Axioms (A) of Definition 1.12, it follows that Proposition 1.14 is valid in \mathbb{R} , and we can prove one of the requirements of Definition ??:

If $\alpha, \beta, \gamma \in \mathbb{R}$ and $\beta < \gamma$, then $\alpha + \beta < \alpha + \gamma$.

Indeed, it is obvious from the definition of $+$ in \mathbb{R} that $\alpha + \beta \subset \alpha + \gamma$; if we had $\alpha + \beta = \alpha + \gamma$, the cancellation law (Proposition 1.14) would imply $\beta = \gamma$.

It also follows that $\alpha > 0^*$ if and only if $-\alpha < 0^*$.

Step 6 Multiplication is a little more bothersome than addition in the present context, since products of negative rationals are positive. For this reason we confine ourselves first to \mathbb{R}^+ , the set

of all $\alpha \in \mathbb{R}$ with $\alpha > 0^*$.

If $\alpha \in \mathbb{R}^+$ and $\beta \in \mathbb{R}^+$, we define $\alpha\beta$ to be the set of all p such that $p \leq rs$ for some choice of $r \in \alpha, s \in \beta, r > 0, s > 0$.

We define 1^* to be the set of all $q < 1$.

Then the axioms (M) and (D) of Definition 1.12 hold, with \mathbb{R}^+ in place of F , and with 1^* in the role of 1.

The proofs are so similar to the ones given in detail in Step 4 that we omit them.

Note, in particular, that the second requirement of Definition 1.17 holds: If $\alpha > 0^*$ and $\beta > 0^*$ then $\alpha\beta > 0^*$.

Step 7 We complete the definition of multiplication by setting $\alpha 0^* = 0^* \alpha = 0^*$, and by setting

$$\alpha\beta = \begin{cases} (-\alpha)(-\beta) & \text{if } \alpha < 0^*, \beta < 0^*, \\ -[(-\alpha)\beta] & \text{if } \alpha < 0^*, \beta > 0^*, \\ -[\alpha \cdot (-\beta)] & \text{if } \alpha > 0^*, \beta < 0^*, \end{cases}$$

The products on the right were defined in Step 6.

Having proved (in Step 6) that the axioms (M) hold in \mathbb{R}^+ , it is now perfectly simple to prove them in \mathbb{R}^+ , by repeated application of the identity $\gamma = -(-\gamma)$ which is part of Proposition 1.14. (See Step 5.)

The proof of the distributive law

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$$

breaks into cases. For instance, suppose $\alpha > 0^*, \beta < 0^*, \beta + \gamma > 0^*$. Then $\gamma = (\beta + \gamma) + (-\beta)$, and (since we already know that the distributive law holds in \mathbb{R}^+)

$$\alpha\gamma = \alpha(\beta + \gamma) + \alpha \cdot (-\beta).$$

But $\alpha \cdot (-\beta) = -(\alpha\beta)$. Thus

$$\alpha\beta + \alpha\gamma = \alpha(\beta + \gamma).$$

The other cases are handled in the same way.

We have now completed the proof that \mathbb{R} is an orderedfield with the least-upper-bound property.

Step 8 We associate with each $r \in \mathbb{Q}$ the set r^* which consists of all $p \in \mathbb{Q}$ such that $p < r$. It is clear that each r^* is a cut; that is, $r^* \in \mathbb{R}$. These cuts satisfy the following relations:

- (a) $r^* + s^* = (r + s)^*$,
- (b) $r^* s^* = (rs)^*$,
- (c) $r^* < s^*$ if and only if $r < s$.

To prove (a), choose $p \in r^* + s^*$. Then $p = u + v$, where $u < r, v < s$. Hence $p < r + s$, which says that $p \in (r + s)^*$.

Conversely, suppose $p \in (r + s)^*$. Then $p < r + s$. Choose t so that $2t = r + s - p$, put

$$r' = r - t, s' = s - t.$$

Then $r' \in r^*$, $s' \in s^*$, and $p = r' + s'$, so that $p \in r^* + s^*$

This proves (a). The proof of (b) is similar.

If $r < s$ then $r \in s^*$, but $r \notin r^*$; hence $r^* < s^*$.

If $r^* < s^*$ then there is a $p \in s^*$ such that $p \notin r^*$. Hence $r < p < s$, so that $r < s$.

This proves (c).

Step 9 We saw in Step 8 that the replacement of the rational numbers r by the corresponding “rational cuts” $r^* \in \mathbb{R}$ preserves sums, products, and order. This fact may be expressed by saying that the ordered field \mathbb{Q} is isomorphic to the ordered field \mathbb{Q}^* whose elements are the rational cuts. Of course, r^* is by no means the same as r , but the properties we are concerned with (arithmetic and order) are the same in the two fields.

It is this identification of \mathbb{Q} with \mathbb{Q}^* which allows us to regard \mathbb{Q} as a subfield of \mathbb{R} .

The second part of Theorem 1.19 is to be understood in terms of this identification. Note that the same phenomenon occurs when the real numbers are regarded as a subfield of the complex field, and it also occurs at a much more elementary level, when the integers are identified with a certain subset of \mathbb{Q} .

It is a fact, which we will not prove here, that any two ordered fields with the least-upper-bound property are isomorphic. The first part of Theorem 1.19 therefore characterizes the real field \mathbb{R} completely.

The books by Landau and Thurston cited in the Bibliography are entirely devoted to number systems. Chapter 1 of Knopp’s book contains a more leisurely description of how \mathbb{R} can be obtained from \mathbb{Q} . Another construction, in which each real number is defined to be an equivalence class of Cauchy sequences of rational numbers (see Chap. 3), is carried out in Sec. 5 of the book by Hewitt and Stromberg.

The cuts in \mathbb{Q} which we used here were invented by Dedekind. The construction of \mathbb{R} from \mathbb{Q} by means of Cauchy sequences is due to Cantor. Both Cantor and Dedekind published their constructions in 1872.

EXERCISES

Unless the contrary is explicitly stated, all numbers that are mentioned in these exercises are understood to be real.

1.

第二章 Basic topology

2.1 FINITE, COUNTABLE, AND UNCOUNTABLE SETS

We begin this section with a definition of the **function** concept.

Definition 2.1. Consider two sets A and B , whose elements may be any objects whatsoever, and suppose that with each element x of A there is associated, in some manner, an element of B , which we denote by $f(x)$. Then f is said to be a *function* from A to B (or a *mapping* of A into B). The set A is called the *domain* of f (we also say f is defined on A), and the elements $f(x)$ are called the *values* of f . The set of all values of f is called the *range* of f .

Definition 2.2. Let A and B be two sets and let f be a mapping of A into B . If $E \subset A$, $f(E)$ is defined to be the set of all elements $f(x)$, for $x \in E$. We call $f(E)$ the image of E under f . In this notation, $f(A)$ is the range of f . It is clear that $f(A) \subset B$. If $f(A) = B$, we say that f maps A *onto* B . (Note that, according to this usage, *onto* is more specific than *into*.)¹

If $E \subset B$, $f^{-1}(E)$ denotes the set of all $x \in A$ such that $f(x) \in E$. We call $f^{-1}(E)$ the *inverse image* of E under f . If $y \in B$, $f^{-1}(y)$ is the set of all $x \in A$ such that $f(x) = y$. If, for each $y \in B$, $f^{-1}(y)$ consists of at most one element of A , then f is said to be a 1-1 (*one-to-one*) mapping of A into B . This may also be expressed as follows: f is a 1-1 mapping of A into B provided that $f(x_1) \neq f(x_2)$ whenever $x_1 \neq x_2$, $x_1 \in A$, $x_2 \in A$.

(The notation $x_1 \neq x_2$, means that x_1 and x_2 are distinct elements; otherwise we write $x_1 = x_2$.)

Definition 2.3. If there exists a 1-1 mapping of A *onto* B , we say that A and B can be put in 1-1 correspondence, or that A and B have the same cardinal number, or, briefly, that A and B are equivalent, and we write $A \sim B$. This relation clearly has the following properties :

It is reflexive: $A \sim A$.

It is symmetric: If $A \sim B$, then $B \sim A$.

It is transitive: If $A \sim B$ and $B \sim C$, then $A \sim C$.

Any relation with these three properties is called an equivalence relation.²

¹onto 满射? into 映射?

²等价关系: 自反性, 对称性, 传递性