babyrudin reading notes

weiyuan

2022 年 10 月 24 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.

$$p^2 = 2 \tag{1.1}$$

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

$$m^2 = 2n^2. \tag{1.2}$$

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. □

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.
$\forall p \in A$, $\exists q \in A$, s.t. $p < q$,
$\forall p \in B$, $\exists q \in B$, s.t. $p > q$,
$\forall p > 0$

$$q = p - \frac{p^2 - 2}{p + 2} = \frac{2p + 2}{p + 2} \tag{1.3}$$

Then

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

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 elements[1] may be numbers or any other objects[2]), 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 $\varnothing$ 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

[2]object 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 taht $x < y$ or $x = y$, without specofying 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 $a\alpha \in S$ 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 great lower bound in $\mathbb{Q}$.

(b) If $\alpha = \sup E$ exists, $\alpha \in E$ or $\alpha \notin E$.

$$E_1 = \{r | r \in Q, r < 0\}$$
$$E_2 = \{r | r \in Q, r \leq 0\}$$

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

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

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

Definition 1.10. (least-upper-bound property)(important!!) 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. $B \in S$, $B \neq \varnothing$, 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 (myDefinition 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 <$\mathbb{R}, +, \times$> <$\mathbb{R}, +$>, <$\mathbb{R} \backslash \{0\}, \times$> 都是交换群, 且满足分配律. 则 <$\mathbb{R}, +, \times$> 是域.

Axiom 1.12. *(A) Axioms for addition*

(Al) 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 filed)

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). □

mynotes:
mynotes 我自己证明上述四条性质时都是从定义开始的, 而 rudin 这里在后一步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),

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

(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)

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

(d)

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

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

(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 $1/y < 1/x$. □

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 $\mathbb{Q} \in \mathbb{R}$ 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 → 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* $p \in Q$ *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 $x < \infty$ 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

$$x + y = (a + c, b + d),$$
$$xy = (ac - bd, ad + bc).$$

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) $z\pm w=\bar{z}+\bar{w}$,

(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) $|z| > 0$ *unless* $z = 0$, $|0| = 0$,

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

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

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

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

1.34 notation (sum) $x_1, x_2, \ldots, x_n \in \mathbb{C}$,

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

Theorem 1.34. *(Schwarz Inequality)*

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

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

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, $\Delta \le 0$, $\Delta = (2\sum a_j b_j)^2 - 4\sum a_j^2 \sum b_j^2$. 因此 $(\sum a_j b_j)^2 \le \sum a_j^2 \sum b_j^2$

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

If $B = 0$, $b_1 = \cdots = b_n = 0$, 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

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

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

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, $\Delta \le 0$, $\Delta = (2\sum \Re(a_j \bar{b_j}))^2 - 4\sum a_j \bar{a_j} \sum b_j \bar{b_j}$, (这里推出的结论比原始结论弱? 为什么?)