Chapter 1 Proofs

Item	Summary
Definition 1.1	Set definitions andddextension
Definition 1.2	Rational number set Q
Definition 1.3	Order ($<$) and two properties
Definition 1.4	Ordered set
Definition 1.5	Bounded above and upper Bound Bounded below and lower bound
Definition 1.6	Least upper bound (supremum) Greatest lower bound (infimum)
Definition 1.7	Least-upper-bound property
Theorem 1.1	Supremum existence principle
Definition 1.8	Field and field axioms
Proposition 1.1	Addition statements
Proposition 1.2	Multiplication statements
Proposition 1.3	Other statements
Definition 1.9	Ordered field
Proposition 1.4	Ordered field statements
Theorem 1.2	Real number set R
Theorem 1.3	Archimedean property Density of Q
Theorem 1.4	The existence theorem of real roots
Corollary 1.1	The roots of real products
Definition 1.10	$+\infty$ and $-\infty$
Definition 1.11	Complex number
Theorem 1.5	Addition and multiplication statements of complex numbers
Theorem 1.6	Real addition and multiplication in complex field
Definition 1.12	i
Theorem 1.7	$i^2 = -1$
Theorem 1.8	$(a, b) = a + bi$

Definition 1.13	Conjugate
Theorem 1.9	Complex statements
Definition 1.14	Absolute values of complex numbers
Theorem 1.10	Absolute values statements
Theorem 1.11	Cauchy–Schwarz inequality
Definition 1.15	Coordinates of Euclidean spaces
Theorem 1.12	Statements of Euclidean spaces

Theorem 1.1 Suppose S is an ordered set with the least-upper-bound property, $B \subseteq S$, 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.

Proof. First of all, we should prove that $\alpha = \sup L$ exists in S.

(a) Because L is the set of all lower bounds of B and $B \subseteq S$, then $L \subseteq S$.

(b) Because B is bounded below, there exists a $\beta \in S$ such that $x \geq \beta$ for every $x \in B$. Therefore, β is a lower bound of B, $\beta \in L$, so L is not empty.

(c) Because L is the set of all lower bounds of B and B is not empty, there exists a $\gamma \in B$ such that $y \leq \gamma$ for every $y \in L$, then L is bounded above.

Because S is an ordered set with the least-upper-bound property, then $\alpha = \sup L$ exists in S. Now, we should prove that $\alpha = \inf B$.

(a) Suppose that α is not the lower bound of B, then there exists $z \in B$ such that $z < \alpha$. However, α is the supremum of L. Because $z < (z+\alpha)/2 < \alpha$, $(z+\alpha)/2$ is not a upper bound of L, so there exists a $s \in L$ such that $s > (z+\alpha)/2$. Because L is the set of all lower bounds of B, s is a lower bounds of B. However, $z < s$ and $z \in B$, which is a cotradiction. Thus, α is the lower bound of B.

For all $\mu < \alpha$, μ is not an upper bound of L. Because L is the set of all lower bounds of B, $\mu \notin B$. It follows that $\alpha \leq x$ for every $x \in B$. Thus $\alpha \in L$.

(b) For all $\lambda > \alpha$, there is $\lambda > \alpha \geq t$ for every $t \in L$, so λ is not an element of L. Because L is the set of all lower bounds of B and $B \subseteq S$, λ is not a lower bound of B.

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

■

Proposition 1.1 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) $-(-x) = x$.

Proof.

(a)

$$\begin{aligned} y &\overset{\text{(A4)}}{=\!=} 0 + y \overset{\text{(A5)}}{=\!=} [x + (-x)] + y \overset{\text{(A2)}}{=\!=} (x + y) + (-x) \\ &= (x + z) + (-x) \overset{\text{(A2)}}{=\!=} [x + (-x)] + z \overset{\text{(A5)}}{=\!=} 0 + z \overset{\text{(A4)}}{=\!=} z. \end{aligned}$$

(b) With the (a) statement, let $z = 0$,

$$x + y = x + z = x + 0 \overset{\text{(A2)}}{=\!=} 0 + x \overset{\text{(A4)}}{=\!=} x \quad \overset{\text{(a)}}{\Longrightarrow} \quad y = z = 0.$$

(c) With the (a) statement, let $z = -x$,

$$x + y = x + z = x + (-x) \overset{\text{(A5)}}{=\!=} 0 \quad \overset{\text{(a)}}{\Longrightarrow} \quad y = z = -x.$$

(d)

$$x + (-x) \left\{ \begin{array}{l} \overset{\text{(A2)}}{=\!=} (-x) + x \\ \overset{\text{(A5)}}{=\!=} 0 \end{array} \right\} \quad \Rightarrow \quad (-x) + x = 0 \quad \overset{\text{(A5)}}{\Longrightarrow} \quad -(-x) = 0.$$

■

Proposition 1.2 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 $1/(1/x) = x$.

Proof.

(a)

$$y \overset{\text{(M4)}}{=\!=} 1 \cdot y \overset{\text{(M5)}}{=\!=} (x \cdot \frac{1}{x}) \cdot y \overset{\text{(M2)}}{=\!=} xy \cdot \frac{1}{x} = xz \cdot \frac{1}{x} \overset{\text{(M2)}}{=\!=} (x \cdot \frac{1}{x}) \cdot z \overset{\text{(M5)}}{=\!=} 1 \cdot z \overset{\text{(M4)}}{=\!=} z.$$

(b) With the (a) statement, let $z = 1$,

$$xy = xz = x \cdot 1 \xlongequal{\text{(M2)}} 1 \cdot x \xlongequal{\text{(M4)}} x \quad \xRightarrow{\text{(a)}} \quad y = z = 1.$$

(c) With the (a) statement, let $z = 1/x$,

$$xy = xz = x \cdot \frac{1}{x} \xlongequal{\text{(M5)}} 1 \quad \xRightarrow{\text{(a)}} \quad = z = \frac{1}{x}.$$

(d)

$$x \cdot \frac{1}{x} \left\{ \begin{array}{l} \xlongequal{\text{(M2)}} \dfrac{1}{x} \cdot x \\ \xlongequal{\text{(M5)}} 1 \end{array} \right\} \quad \Rightarrow \quad \frac{1}{x} \cdot x = 1 \quad \xRightarrow{\text{(M5)}} \quad \frac{1}{\frac{1}{x}} = x.$$

■

Proposition 1.3 The field axioms imply the following statements, for any $x, y, z \in F$:

(a) $0 \cdot x = x$.

(b) If $x \neq 0$ and $y \neq 0$ then $xy \neq 0$.

(c) $(-x)y = -(xy) = x(-y)$.

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

Proof.

(a)

$$0 \cdot x \xlongequal{\text{(A5)}} [1 + (-1)]x \xlongequal{\text{(M2), (D)}} 1 \cdot x - 1 \cdot x \xlongequal{\text{(M4)}} x - x \xlongequal{\text{(A5)}} 0.$$

(b) Suppose that $xy = 0$, then

$$xy \cdot \frac{1}{y} \cdot \frac{1}{x} \xlongequal{\text{(M3)}} x \left(y \cdot \frac{1}{y} \right) \frac{1}{x} \xlongequal{\text{(M5)}} x \cdot 1 \cdot \frac{1}{x} \xlongequal{\text{(M2), (M4)}} x \cdot \frac{1}{x} \xlongequal{\text{(M5)}} 1.$$

However, according to (a) statement,

$$xy \cdot \frac{1}{y} \cdot \frac{1}{x} = 0 \cdot \frac{1}{y} \cdot \frac{1}{x} \xlongequal{\text{(a)}} 0 \cdot \frac{1}{x} \xlongequal{\text{(a)}} 0.$$

This is a cotradiction, so if $x \neq 0$ and $y \neq 0$ then $xy \neq 0$.

(c)

$$(-x)y + xy \xlongequal{\text{(M2), (D)}} [(-x)+x]y \xlongequal{\text{(M5)}} 0\cdot y \xlongequal{\text{(a)}} 0 \quad \xRightarrow{\text{(M5)}} \quad (-x)y = -(xy),$$
$$xy + x(-y) \xlongequal{\text{(D)}} x[y+(-y)] \xlongequal{\text{(A5)}} x\cdot 0 \xlongequal{\text{(M2)}} 0\cdot x \xlongequal{\text{(a)}} 0 \xRightarrow{\text{(M5)}} -(xy) = x(-y).$$

To sum up, $(-x)y = -(xy) = x(-y)$.

(d)

$$(-x)(-y) + (-x)y \left\{ \begin{array}{l} \xlongequal{\text{(D)}} (-x)(-y+y) \xlongequal{\text{(A2) (A5)}} (-x)\cdot 0 \xlongequal{\text{(M2) (a)}} 0 \\ \xlongequal{\text{(c)}} (-x)(-y) + (-xy) \end{array} \right\}$$
$$\xRightarrow{\text{(A5)}} (-x)(-y) = xy.$$
$$(-x)(-y) \xlongequal{\text{(c)}} -[x(-y)] \xlongequal{\text{(c)}} -[-(xy)] \xlongequal{\text{Proposition 1.4 (d)}} xy.$$

■

Proposition 1.4 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 $0 < 1/y < 1/x$.

Proof.

(a)

$$x > 0 \quad \xRightarrow{\text{Definition 1.9 (i)}} \quad x - x \xlongequal{\text{(A5)}} 0 > 0 - x \xlongequal{\text{(A4)}} -x \quad \Rightarrow \quad -x < 0.$$
$$x < 0 \quad \xRightarrow{\text{Definition 1.9 (i)}} \quad x - x \xlongequal{\text{(A5)}} 0 < 0 - x \xlongequal{\text{(A4)}} -x \quad \Rightarrow \quad -x > 0.$$

(b)

$$\left. \begin{array}{r} x > 0 \\ y < z \xRightarrow{\text{Definition 1.9 (i)}} z - y > 0 \end{array} \right\} \xRightarrow{\text{Definition 1.9 (ii)}} x(z-y) > 0 \xRightarrow{\text{(D)}} xy < xz.$$

(c)

$$\left.\begin{array}{ll} x<0 \xrightarrow{\text{Definition 1.9 (i)}} & -x>0 \\ y<z \xrightarrow{\text{Definition 1.9 (i)}} & z-y>0 \end{array}\right\} \xrightarrow{\text{Definition 1.9 (ii)}} -x(z-y)>0$$

$$\overset{\text{(D)}}{=\!=} -xz+(-x)(-y)>0 \xrightarrow{\text{Proposition 1.4 (d)}} xy>xz.$$

(d) • If $x<0$, then

$$x<0 \overset{(c)}{\Longrightarrow} x\cdot x=x^2>x\cdot 0 \overset{\text{(M2), Proposition 1.3 (a)}}{=\!=\!=\!=} 0.$$

• If $x>0$, then

$$x>0 \xrightarrow{\text{Definition 1.9 (ii)}} x\cdot x=x^2>0.$$

(e) Suppose that $1/x<0$, then

$$\left.\begin{array}{r} x>0 \\ \dfrac{1}{x}<0 \end{array}\right\} \overset{(b)}{\Longrightarrow} x\cdot\frac{1}{x} \overset{\text{(M5)}}{=\!=} 1<0\cdot 0 \overset{\text{Proposition 1.3 (a)}}{=\!=\!=\!=} 0.$$

This is a contradiction, so $1/x>0$. Likewise, $1/y>0$. Suppose that $0<1/x<1/y$, then

$$\left.\begin{array}{r} 0<x<y \\ 0<\dfrac{1}{x}<\dfrac{1}{y} \end{array}\right\} \overset{(b)}{\Longrightarrow} x\cdot\frac{1}{x} \overset{\text{(M5)}}{=\!=} 1<x\cdot\frac{1}{y}<y\cdot\frac{1}{y} \overset{\text{(M5)}}{=\!=} 1.$$

This is a contradiction, so $0<1/y<1/x$.

■

Theorem 1.2 There exists an ordered field R which has the least-upper-bound property. Moreover, R contains Q as a subfield.

Theorem 1.3 (Archimedean Property and Density of *Q*)

(a) If $x\in R, y\in R$, and $x>0$, then there is a positive integer n such that

$$nx>y.$$

(b) If $x\in R, y\in R$, and $x<y$, then there is a $p\in Q$ such that

$$x<p<y.$$

Proof.

(a) Let A be the set of all nx, where n runs through the positive integers. Suppose that this statement is false, then y would be an upper bound of A. But then A has a least upper bound in R. Put $\alpha = \sup A$. Since $x > 0$, $\alpha - x < \alpha$, and $\alpha - x$ is not an upper bound of A. Hence $\alpha - x < mx$ for some positive integer m. But then $\alpha < (m+1)x \in A$, which is impossible, since α is an upper bound of A.

(b) Because

$$x < y \quad \Rightarrow \quad y - x > 0.$$

According to Archimedean Property, there is a positive integer n such that

$$n(y - x) > 1.$$

With $1 > 0$, according to Archimedean Property, there is two positive integers m_1 and m_2 such that

$$m_1 \cdot 1 = m_1 > nx, \qquad m_2 \cdot 1 = m_2 > -nx.$$

Therefore,

$$-m_2 < nx < m_1.$$

Find the integer m with $-m_2 \leq m \leq m_1$ such that

$$m - 1 \leq nx < m.$$

Now, we obtain

$$nx < m \leq 1 + nx < ny.$$

With $n > 0$, it follows that

$$x < \frac{m}{n} < y.$$

■

Theorem 1.4 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 $x^{1/n}$.

Proof. Let x be any positive real and n be any positive integer, suppose that there is no positive real y such that $y^n = x$.

1. We will prove that for any positive real x and y such that $0 < x < y$, there is $0 < x^n < y^n$ for all positive integers n with mathematical induction.

   - **Basis**

     For $n = 1$, there is $0 < x < y$.

   - **Inductive Assumption**

     Assume that for $i = 1, 2, \cdots, n$ where n is a positive integer, there is $0 < x^i < y^i$.

   - **Inductive Step**

     For $i = n + 1$, then

$$0 < x^{n+1} = x^n \cdot x < x^n \cdot y < y^n \cdot y = y^{n+1}.$$

   To sum up, for any positive real x and y such that $0 < x < y$, there is $0 < x^n < y^n$ for all positive integers n.

2. For every real $y > 0$, if $y^n < x$, we put y into a set A; if $y^n > x$, we put y into a set B. For any element a in A and any element b in B, if $t = x/(1 + x)$ then $0 \leq t < 1$. Hence $t^n \leq t < x$. Thus $t \in A$, and A is not empty. With the conclusion in the part before, we have

$$0 < a^n < x < b^n \quad \Rightarrow \quad 0 < a < b.$$

   Thus, every element in A is a lower bound of B; every element in B is a upper bound of A. Let α be the least upper bound of A and let β be the greatest lower bound of A. We will prove that $\alpha = \beta$.

   - If $\alpha < \beta$, then $(\alpha+\beta)/2$ is also a positive real. Let $\gamma = (\alpha+\beta)/2$. Because $\gamma > \alpha$, γ is not an element of A, so γ^n can not be less than x; because $\gamma < \beta$, γ is not an element of B, γ^n can not be more than x; thus, $\gamma^n = x$. This contradicts with our assumption that there is no positive real y such that $y^n = x$.

   - If $\alpha > \beta$, then $(\alpha+\beta)/2$ is also a positive real. Let $\gamma = (\alpha+\beta)/2$. Because $\gamma < \alpha$, there is at least one element μ in A such that $\gamma < \mu$; because $\gamma > \beta$, there is at least one element ν in B such that $\gamma > \nu$. Thus, $0 < \nu < \gamma < \mu$. With the conclusion in the first part, we have $\nu^n < \mu^n$. However, we have $\mu^n < x < \nu^n$, so this is a contradiction.

To sum up, $\alpha = \beta$.

3. Because α is also a positive real, we will prove that α^n can not be less than x. Suppose that $\alpha^n < x$, then α is an element of A. Let ε be a positive real such that

$$\varepsilon = \min\left\{\frac{x-\alpha^n}{2\alpha^{n-1}n!n},\ \alpha\right\},$$

so

$$\frac{\varepsilon}{\alpha} \leq \frac{x-\alpha^n}{2\alpha^n n!n} < \frac{x-\alpha^n}{\alpha^n n!n} \qquad \text{and} \qquad 0 < \frac{\varepsilon}{\alpha} \leq 1.$$

Now, we have

$$\begin{aligned}(\alpha+\varepsilon)^n &= \alpha^n\left(1+\frac{\varepsilon}{\alpha}\right)^n = \alpha^n\left[1+\sum_{i=1}^{n}\binom{n}{i}\left(\frac{\varepsilon}{\alpha}\right)^i\right] \leq \alpha^n\left[1+n!\sum_{i=1}^{n}\left(\frac{\varepsilon}{\alpha}\right)^i\right]\\ &\leq \alpha^n\left[1+n!n\left(\frac{\varepsilon}{\alpha}\right)\right] < \alpha^n\left(1+n!n\frac{x-\alpha^n}{\alpha^n n!n}\right) = \alpha^n\left(1+\frac{x-\alpha^n}{\alpha^n}\right) = x.\end{aligned}$$

Therefore, $(\alpha+\varepsilon)$ is also an element of A. However, $\alpha+\varepsilon > \alpha$, α can not be the upper bound of A. This is a contradiction, so α^n can not be less than x.

4. Because α is also a positive real, we will prove that α^n can not be more than x. Suppose that $\alpha^n > x$, then α is an element of B. Let ε be a positive real such that

$$\varepsilon = \min\left\{\frac{\alpha^n - x}{2\alpha^{n-1}n!n},\ \alpha\right\},$$

so

$$\frac{\varepsilon}{\alpha} \leq \frac{\alpha^n-x}{2\alpha^n n!n} < \frac{\alpha^n-x}{\alpha^n n!n} \qquad \text{and} \qquad 0 < \frac{\varepsilon}{\alpha} \leq 1.$$

Then

$$-\frac{\varepsilon}{\alpha} > \frac{x-\alpha^n}{\alpha^n n!n} \qquad \text{and} \qquad -1 < -\frac{\varepsilon}{\alpha} \leq 0.$$

Now, we have

$$\begin{aligned}(\alpha-\varepsilon)^n &= \alpha^n\left(1-\frac{\varepsilon}{\alpha}\right)^n = \alpha^n\left[1+\sum_{i=1}^{n}\binom{n}{i}\left(-\frac{\varepsilon}{\alpha}\right)^i\right] \geq \alpha^n\left[1+\sum_{i=1}^{n}\binom{n}{i}\left(-\frac{\varepsilon}{\alpha}\right)\right]\\ &\geq \alpha^n\left[1+n!n\left(-\frac{\varepsilon}{\alpha}\right)\right] > \alpha^n\left(1+n!n\frac{x-\alpha^n}{\alpha^n n!n}\right) = \alpha^n\left(1+\frac{x-\alpha^n}{\alpha^n}\right) = x.\end{aligned}$$

Therefore, $(\alpha-\varepsilon)$ is also an element of B. However, $\alpha-\varepsilon < \alpha$, α can not be the lower bound of B. This is a contradiction, so α^n can not be more than x.

5. From the third part and the fourth part, we can conclude that $\alpha^n = x$, which contradicts with our assumption that there is no positive real y such that $y^n = x$.

To sum up, for every real $x > 0$ and every integer $n > 0$ there is at least one positive real y such that $y^n = x$. With the conclusion in the first part, for two positive real numbers y and z, if $y \neq z$, then $y^n \neq z^n$, so the real number that satisfies this is unique.

The identity $b^n - a^n = (b-a)(b^{n-1} + b^{n-2}a + \cdots + a^{n-1})$ yields the inequality

$$b^n - a^n < (b-a)nb^{n-1}$$

when $0 < a < b$. Assume $\alpha^n < x$. Choose ε so that $0 < \varepsilon < 1$ and

$$\varepsilon < \frac{x - \alpha^n}{n(\alpha+1)^{n-1}}.$$

Put $a = \alpha, b = \alpha + \varepsilon$. Then

$$(\alpha+\varepsilon)^n - \alpha^n < \varepsilon n(\alpha+\varepsilon)^{n-1} < \varepsilon n(\alpha+1)^{n-1} < x - \alpha^n.$$

Thus $(\alpha+\varepsilon)^n < x$, and $\alpha + \varepsilon \in A$. Since $\alpha + \varepsilon > \alpha$, this contradicts the fact that α is an upper bound of A. Assume $\alpha^n > x$. Put

$$\varepsilon = \frac{\alpha^n - x}{n\alpha^{n-1}}.$$

Then $0 < \varepsilon < \alpha$. If $t \geq \alpha - \varepsilon$, we conclude that

$$\alpha^n - t^n \leq \alpha^n - (\alpha-\varepsilon)^n < \varepsilon n\alpha^{n-1} = \alpha^n - x.$$

Thus $t^n > x$, and $t \in A$. It follows that $\alpha - \varepsilon$ is an upper bound of A. But $\alpha - \varepsilon < \alpha$, which contradicts the fact that α is the least upper bound of A. Hence $\alpha^n = x$, and the proof is complete.

■

Corollary 1.1 If a and b are positive real numbers and n is a positive integer, then

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

Proof. Suppose that α and β are positive real numbers. Then

$$(\alpha\beta)^n = \alpha\beta\alpha\beta\cdots\alpha\beta \xlongequal{\text{(M2)}} \alpha\alpha\cdots\alpha\beta\beta\cdots\beta = \alpha^n\beta^n.$$

Let $\alpha = a^{1/n}, \beta = b^{1/n}$, then

$$\left(a^{\frac{1}{n}} b^{\frac{1}{n}}\right)^n = \left(a^{\frac{1}{n}}\right)^n \left(b^{\frac{1}{n}}\right)^n = ab \quad \Rightarrow \quad (ab)^{\frac{1}{n}} = a^{\frac{1}{n}} b^{\frac{1}{n}}.$$

$\blacksquare$

Theorem 1.5 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 of 0 and 1.

Proof. Suppose that x, y and z are any complex numbers. Let $x = (a,b), y = (c,d)$ and $z = (e,f)$.

(A1) If $x = (a,b) \in F$ and $y = (c,d) \in F$, then their sum $x + y = (a+c, b+d) \in F$.

(A2) For all $x = (a,b)$ and $y = (c,d)$

$$x + y = (a+c, b+d) = (c+a, d+b) = y + x.$$

(A3) For all $x = (a,b), y = (c,d)$ and $z = (e,f)$

$$\begin{aligned} x + y = (a+c, b+d) \quad &\Rightarrow \quad (x+y)+z = (a+c+e, b+d+f), \\ y + z = (c+e, d+f) \quad &\Rightarrow \quad x+(y+z) = (a+c+e, b+d+f). \end{aligned}$$

Therefore, $(x+y)+z = x+(y+z)$.

(A4) For every $x = (a,b) \in F$,

$$(0,0) + x = (0,0) + (a,b) = (0+a, 0+b) = (a,b) = x.$$

(A5) For every $x = (a,b) \in F$,

$$-x = (-1,0)x = (-1,0)\cdot(a,b) = (-1\cdot a - 0\cdot b, -1\cdot b + 0\cdot b) = (-a,-b).$$

Then

$$x + (-x) = (a,b) + (-a,-b) = (a-a, b-b) = (0,0).$$

(M1) If $x = (a,b) \in F$ and $y = (c,d) \in F$, then their product $xy = (ac - bd, ad + bc) \in F$.

(M2) For all $x = (a,b)$ and $y = (c,d)$

$$xy = (ac - bd, ad + bc) = (ac - bd, bc + ad) = (ca - db, cb + da) = yx.$$

(M3) For all $x = (a, b), y = (c, d)$ and $z = (e, f)$

$$\begin{aligned}(xy)z &= (ac - bd, ad + bc)(e, f)\\ &= (ace - bde - adf - bcf, acf - bdf + ade + bce)\\ &= (a, b)(ce - df, cf + de)\\ &= x(yz).\end{aligned}$$

Therefore, $(xy)z = x(yz)$.

(M4) For every $x = (a, b) \in F$,

$$(1, 0)x = (1 \cdot a - 0 \cdot b, 1 \cdot b + 0 \cdot a) = (a, b) = x.$$

(M5) For every $x = (a, b) \in F$ and $a^2 + b^2 \neq 0$, let

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

Then

$$x \cdot \frac{1}{x} = (a, b) \cdot \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) = \left(\frac{a^2 + b^2}{a^2 + b^2}, \frac{-ab + ab}{a^2 + b^2}\right) = (1, 0).$$

(D) For all $x = (a, b), y = (c, d)$ and $z = (e, f)$

$$\begin{aligned}x(y + z) &= (a, b) \cdot (c + e, d + f)\\ &= (ac + ae - bd - bf, ad + af + bc + be)\\ &= (ac - bd, ad + bc) + (ae - bf, af + be)\\ &= xy + xz.\end{aligned}$$

■

Theorem 1.6 For any real numbers a and b we have

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

Proof.

$$\begin{aligned}(a, 0) + (b, 0) &= (a + b, 0 + 0) = (a + b, 0),\\ (a, 0)(b, 0) &= (ab - 0 \cdot 0, a \cdot 0 + 0 \cdot b) = (ab - 0, 0 + 0) = (ab, 0).\end{aligned}$$

$\blacksquare$

Theorem 1.7 $i^2 = -1$.

Proof. From Definition 1.12, $i = (0, 1)$, we have

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

$\blacksquare$

Theorem 1.8 If a and b are real, then $(a, b) = a + bi$.

Proof. We have

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

$\blacksquare$

Theorem 1.9 If z and w are complex, then

(a) $\overline{z + w} = \overline{z} + \overline{w}$,

(b) $\overline{zw} = \overline{z} \cdot \overline{w}$,

(c) $z + \overline{z} = 2\,\mathrm{Re}(z),\ z - \overline{z} = 2i\,\mathrm{Im}(z)$,

(d) $z\overline{z}$ is real and positive (except when $z = 0$).

Proof. Let $z = a + bi$ and $w = c + di$, we have $\overline{z} = a - bi$ and $\overline{w} = c - di$. With Definition 1.13, we have

(a)

$$\left.\begin{aligned} z + w = (a + c) + (b + d)i \ \Rightarrow \overline{z + w} &= (a + c) - (b + d)i \\ \overline{z} + \overline{w} &= (a + c) - (b + d)i \end{aligned}\right\} \Rightarrow \ \overline{z + w} = \overline{z} + \overline{w}.$$

(b)

$$\left.\begin{aligned} zw = (ac - bd) + (ad + bc)i \;\Rightarrow\; \overline{zw} &= (ac - bd) - (ad + bc)i \\ \overline{z} \cdot \overline{w} &= (ac - bd) - (ad + bc)i \end{aligned}\right\} \Rightarrow\; \overline{zw} = \overline{z} \cdot \overline{w}.$$

(c)

$$\begin{aligned} z + \overline{z} &= (a + bi) + (a - bi) = 2a \;= 2\,\mathrm{Re}(z), \\ z - \overline{z} &= (a + bi) - (a - bi) = 2bi = 2i\,\mathrm{Im}(z). \end{aligned}$$

(d)

$$z\overline{z} = (a + bi)(a - bi) = a^2 + b^2.$$

If $z = 0 = 0 + 0i$, then $z\overline{z} = a^2 + b^2 = 0$; if $z \neq 0$, then $z\overline{z} = a^2 + b^2 > 0$, so $z\overline{z}$ is real and positive.

■

Theorem 1.10 Let z and w be complex numbers. Then

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

(b) $|\overline{z}| = |z|,$

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

(d) $|\mathrm{Re}(z)| \leq |z|,$

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

Proof. Let $z = a + bi$ and $w = c + di$, we have $\overline{z} = a - bi$. With Definition 1.13 and Definition 1.14, we have

(a) Because $|z| = \sqrt{z\overline{z}} = \sqrt{(a + bi)(a - bi)} = \sqrt{a^2 + b^2}$, if $z = 0 = 0 + 0i$, then $a = b = 0$, $|z| = \sqrt{|0|} = \sqrt{a^2 + b^2} = 0$; if $z \neq 0$, then a and b can not be both 0, so $|z| = \sqrt{a^2 + b^2} > 0$.

(b) Because $|z| = \sqrt{z\overline{z}} = \sqrt{a^2 + b^2}$, then

$$|\overline{z}| = \sqrt{\overline{z}\,\overline{\overline{z}}} = \sqrt{\overline{z}z} = \sqrt{z\overline{z}} = \sqrt{a^2 + b^2} = |z|.$$

(c) Because $zw = (ac - bd) + (ad + bc)i$, then

$$\begin{aligned} |zw| &= \sqrt{(ac-bd)^2 + (ad+bc)^2} \\ &= \sqrt{a^2c^2 + b^2d^2 + b^2c^2 + a^2d^2} \\ &= \sqrt{(a^2+b^2)(c^2+d^2)} \\ &= \sqrt{a^2+b^2}\sqrt{c^2+d^2} \\ &= |z||w|. \end{aligned}$$

(d) Because $|\mathrm{Re}(z)| = |a|$ and $|z| = \sqrt{a^2+b^2}$, we have

$$a^2 \le a^2 + b^2 \quad \Rightarrow \quad \sqrt{a^2} = |a| = |\mathrm{Re}(z)| \le \sqrt{a^2+b^2} = |z|.$$

(e) Because $z\overline{w} + \overline{z}w = 2\,\mathrm{Re}(z\overline{w})$, we have

$$\begin{aligned} |z+w|^2 &= (z+w)(\overline{z+w}) \\ &= (z+w)(\overline{z}+\overline{w}) \\ &= z\overline{z} + z\overline{w} + w\overline{z} + w\overline{w} \\ &= |z|^2 + 2\,\mathrm{Re}(z\overline{w}) + |w|^2 \\ &\le |z|^2 + 2|z\overline{w}| + |w|^2 \\ &= |z|^2 + 2|z||w| + |w|^2 \\ &= (|z|+|w|)^2. \end{aligned}$$

Therefore, $|z+w| \le |z| + |w|$.

∎

Theorem 1.11 (Cauchy–Schwarz Inequality) If $a_1, \cdots, a_n$ and $b_1, \cdots, b_n$ are complex numbers, then

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

Proof. With Theorem 1.12, we have

$$\left|\sum_{j=1}^{n} a_j\overline{b_j}\right|^2 \le \left(\sum_{j=1}^{n} |a_j\overline{b_j}|\right)^2 \le \left(\sum_{j=1}^{n} |a_j|\,|\overline{b_j}|\right)^2 = \left(\sum_{j=1}^{n} |a_j|\,|b_j|\right)^2.$$

We will use mathematical induction to prove that

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

- **Basis**

  For $n = 1$,

$$\left(\sum_{j=1}^{1} |a_j|\ |b_j|\right)^2 = (|a_1|\ |b_1|)^2 = |a_1|^2|b_1|^2 = \sum_{j=1}^{1} |a_j|^2 \sum_{j=1}^{1} |b_j|^2.$$

  Because $(|a_1||b_2| - |a_2||b_1|)^2 \geq 0$ and

$$(|a_1|\ |b_2| - |a_2|\ |b_1|)^2 = |a_1|^2|b_2|^2 + |a_2|^2|b_1|^2 - 2\ |a_1|\ |a_2|\ |b_1|\ |b_2|,$$

  we have

$$2\ |a_1|\ |a_2|\ |b_1|\ |b_2| \leq |a_1|^2|b_2|^2 + |a_2|^2|b_1|^2.$$

  Then we add $|a_1|^2|b_1|^2 + |a_2|^2|b_2|^2$ on both two sides of the inequation to get

$$(|a_1|\ |b_1| + |a_2|\ |b_2|)^2 \leq (|a_1|^2 + |a_2|^2)(|b_1|^2 + |b_2|^2).$$

  Therefore, for $n = 2$, we have

$$\left(\sum_{j=1}^{2} |a_j|\ |b_j|\right)^2 \leq \sum_{j=1}^{2} |a_j|^2 \sum_{j=1}^{2} |b_j|^2.$$

- **Inductive Assumption**

  Assume that for $i = 1, 2, \cdots, n$ where n is a positive integer, there is

$$\left(\sum_{j=1}^{i} |a_j|\ |b_j|\right)^2 \leq \sum_{j=1}^{i} |a_j|^2 \sum_{j=1}^{i} |b_j|^2.$$

- **Inductive Step**

  Let

$$\sum_{j=1}^{n} |a_j|\ |b_j| = \Sigma_{|a||b|}, \qquad \sum_{j=1}^{n} |a_j|^2 = \Sigma_{|a|}, \qquad \sum_{j=1}^{n} |b_j|^2 = \Sigma_{|b|},$$

  so we have $\left(\Sigma_{|a||b|}\right)^2 \leq \Sigma_{|a|}\Sigma_{|b|}$. Moreover, $(|a_{n+1}|\sqrt{\Sigma_{|b|}} - |b_{n+1}|\sqrt{\Sigma_{|a|}})^2 \geq 0$ and

$$(|a_{n+1}|\sqrt{\Sigma_{|b|}} - |b_{n+1}|\sqrt{\Sigma_{|a|}})^2 = |a_{n+1}|^2\Sigma_{|b|} + |b_{n+1}|^2\Sigma_{|a|} - 2\ |a_{n+1}|\ |b_{n+1}|\sqrt{\Sigma_{|a|}}\sqrt{\Sigma_{|b|}},$$

  we have

$$2\ |a_{n+1}|\ |b_{n+1}|\ \Sigma_{|a||b|} \leq 2\ |a_{n+1}|\ |b_{n+1}|\sqrt{\Sigma_{|a|}}\sqrt{\Sigma_{|b|}} \leq |a_{n+1}|^2\Sigma_{|b|} + |b_{n+1}|^2\Sigma_{|a|}.$$

For $i = n+1$, then

$$\begin{aligned}
\left(\sum_{j=1}^{n+1} |a_j|\,|b_j|\right)^2 &= \left(\Sigma_{|a||b|} + |a_{n+1}|\,|b_{n+1}|\right)^2 \\
&= \left(\Sigma_{|a||b|}\right)^2 + |a_{n+1}|^2|b_{n+1}|^2 + 2\,|a_{n+1}|\,|b_{n+1}|\,\Sigma_{|a||b|} \\
&\le \Sigma_{|a|}\Sigma_{|b|} + |a_{n+1}|^2|b_{n+1}|^2 + |a_{n+1}|^2\Sigma_{|b|} + |b_{n+1}|^2\Sigma_{|a|} \\
&= (\Sigma_{|a|} + |a_{n+1}|)(\Sigma_b + |b_{n+1}|) \\
&= \sum_{j=1}^{n+1} |a_j|^2 \sum_{j=1}^{n+1} |b_j|^2.
\end{aligned}$$

To sum up,

$$\left|\sum_{j=1}^{n} a_j\overline{b_j}\right|^2 \le \left(\sum_{j=1}^{n} |a_j|\,|b_j|\right)^2 \le \sum_{j=1}^{n} |a_j|^2 \sum_{j=1}^{n} |b_j|^2.$$

■

Theorem 1.12 Suppose $\mathbf{x}, \mathbf{y}, \mathbf{z} \in R^k$, and α is real. Then

(a) $|\mathbf{x}| \ge 0$;

(b) $|\mathbf{x}| = 0$ if and only if $\mathbf{x} = \mathbf{0}$;

(c) $|\alpha\mathbf{x}| = |\alpha|\,|\mathbf{x}|$;

(d) $|\mathbf{x}\cdot\mathbf{y}| \le |\mathbf{x}|\,|\mathbf{y}|$;

(e) $|\mathbf{x}+\mathbf{y}| \le |\mathbf{x}| + |\mathbf{y}|$;

(f) $|\mathbf{x}-\mathbf{z}| \le |\mathbf{x}-\mathbf{y}| + |\mathbf{y}-\mathbf{z}|$.

Proof. Suppose that $\mathbf{x} = (x_1, x_2, \cdots, x_k)$, $\mathbf{y} = (y_1, y_2, \cdots, y_k)$ and $\mathbf{z} = (z_1, z_2, \cdots, z_k)$. Then

(a)

$$|\mathbf{x}| = \sqrt{\mathbf{x}\cdot\mathbf{x}} = \sqrt{\sum_{i=1}^{k} x_i^2} \ge 0.$$

(b) • $|\mathbf{x}| = 0 \Rightarrow \mathbf{x} = \mathbf{0}$. We have

$$|\mathbf{x}| = \sqrt{\sum_{i=1}^{k} x_i^2} \ge 0 \quad\Rightarrow\quad x_1 = x_2 = \cdots = x_k = 0 \quad\Rightarrow\quad \mathbf{x} = \mathbf{0}.$$

- $|\mathbf{x}| = 0 \;\Leftarrow\; \mathbf{x} = \mathbf{0}$. We have

$$\mathbf{x} = \mathbf{0} \quad \Rightarrow \quad x_1 = x_2 = \cdots = x_k = 0 \quad \Rightarrow \quad |\mathbf{x}| = \sqrt{\sum_{i=1}^{k} x_i^2} = 0.$$

(c) Because $\alpha\mathbf{x} = (\alpha x_1, \alpha x_2, \cdots, \alpha x_k)$, we have

$$|\alpha\mathbf{x}| = \sqrt{\sum_{i=1}^{k} (\alpha x_i)^2} = \sqrt{\alpha^2 \sum_{i=1}^{k} x_i^2} = |\alpha| \sqrt{\sum_{i=1}^{k} x_i^2} = |\alpha|\ |\mathbf{x}|.$$

(d) With Cauchy–Schwarz inequality, we have

$$\left(\sum_{i=1}^{k} |x_i|\ |y_i| \right)^2 \leq \sum_{i=1}^{n} |x_i|^2 \sum_{i=1}^{n} |y_i|^2.$$

so we can get

$$|\mathbf{x} \cdot \mathbf{y}| = \left| \sum_{i=1}^{k} x_i y_i \right| \leq \left| \sum_{i=1}^{k} |x_i|\ |y_i| \right| \leq \sqrt{\sum_{i=1}^{n} |x_i|^2} \sqrt{\sum_{i=1}^{n} |y_i|^2} = |\mathbf{x}|\ |\mathbf{y}|.$$

(e) Becuase $\mathbf{x} \cdot \mathbf{y} \leq |\mathbf{x} \cdot \mathbf{y}| \leq |\mathbf{x}|\ |\mathbf{y}|$, we have

$$|\mathbf{x} + \mathbf{y}|^2 = (\mathbf{x} + \mathbf{y})^2 = |\mathbf{x}|^2 + |\mathbf{y}|^2 + 2\,\mathbf{x} \cdot \mathbf{y} \leq |\mathbf{x}|^2 + |\mathbf{y}|^2 + 2\,|\mathbf{x}|\ |\mathbf{y}| = (|\mathbf{x}| + |\mathbf{y}|)^2.$$

Therefore, we get $|\mathbf{x} + \mathbf{y}| \leq |\mathbf{x}| + |\mathbf{y}|$.

(f) Because $\mathbf{x} - \mathbf{y}, \mathbf{y} - \mathbf{z} \in R^k$, we have

$$|\mathbf{x} - \mathbf{z}| = |(\mathbf{x} - \mathbf{y}) + (\mathbf{y} - \mathbf{z})| \leq |\mathbf{x} - \mathbf{y}| + |\mathbf{y} - \mathbf{z}|.$$

■