

Chapter 1: The Real and Complex Number Systems

Author: Meng-Gen Tsai

Email: plover@gmail.com

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

Exercise 1.1. *If r is a rational ($r \neq 0$) and x is irrational, prove that $r + x$ and rx are irrational.*

Proof. Assume $r + x \in \mathbb{Q}$. \mathbb{Q} is a field, then $-r \in \mathbb{Q}$ for any $r \in \mathbb{Q}$. So $(-r) + (r + x) = (-r + r) + x = 0 + x = x \in \mathbb{Q}$, a contradiction.

Similarly, assume $rx \in \mathbb{Q}$. $r \in \mathbb{Q}$ with $r \neq 0$ implies that there exists an element $1/r \in \mathbb{Q}$ such that $r \cdot (1/r) = 1$. So $(1/r) \cdot (rx) = ((1/r) \cdot r) \cdot x = 1 \cdot x = x \in \mathbb{Q}$, a contradiction. \square

Exercise 1.2. *Prove that there is no rational number whose square is 12.*

Apply the argument in Example 1.1. Again we can examine this situation a little more closely. Let A be the set of all positive rational p such that $p^2 < 12$ and let B be the set of all positive rational p such that $p^2 > 12$. We might show that A contains no largest number and B contains no largest number again.

In fact, we can associate with each rational $p > 0$ the number

$$q = p - \frac{p^2 - 12}{p + 12} = \frac{12p + 12}{p + 12}.$$

Then

$$q^2 - 12 = \frac{132(p^2 - 12)}{(p + 12)^2}.$$

If $p \in A$ then $p^2 - 12 < 0$, $q > p$ and $q^2 < 12$. Thus $q \in A$. If $p \in B$ then $p^2 - 12 > 0$, $0 < q < p$ and $q^2 > 12$. Thus $q \in B$.

Proof (Example 1.1). We now show that the equation

$$p^2 = 12$$

is not satisfied by any rational p . If there were such a $p \in \mathbb{Q}$, we could write $p = \frac{m}{n}$ where $m, n \in \mathbb{Z}$ are relatively prime. Let us assume this is done. Then

$p^2 = 12$ implies

$$m^2 = 12n^2.$$

This shows that $3 \mid m^2$. Hence $3 \mid m$ (since 3 is a prime in \mathbb{Z}), and so m^2 is divisible by 9. It follows that $12n^2$ is divisible by 9, so that $4n^2$ is divisible by 3, so that n^2 is divisible by 3, which implies that $3 \mid n$. That is, both m and n have a common factor $3 > 1$, contrary to our choice of m and n . Hence $p^2 = 12$ is impossible for rational p . \square

Exercise 1.3. *Prove Proposition 1.15.*

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 $1(1/x) = x$.*

Proof of (a). By the axioms for multiplication,

$$xy = xz, x \neq 0 \implies \exists 1/x \in F, (1/x) \cdot (xy) = (1/x) \cdot (xz) \quad (\text{M5})$$

$$\implies ((1/x)x)y = ((1/x)x)z \quad (\text{M3})$$

$$\implies (x(1/x))y = (x(1/x))z \quad (\text{M2})$$

$$\implies 1y = 1z$$

$$\implies y = z. \quad (\text{M4})$$

\square

Proof of (b). Let $z = 1$ in (a) and note that $x1 = 1x = x$ ((M2)(M4)). \square

Proof of (c). Let $z = 1/x$ in (a) and note that $x(1/x) = 1$ ((M5)). \square

Proof of (d). Since $x(1/x) = (1/x)x = 1$ ((M2)), by (c), $x = 1/(1/x)$. \square

Exercise 1.4. *Let E be a nonempty subset of an ordered set; suppose α is a lower bound of E and β is an upper bound of E . Prove that $\alpha \leq \beta$.*

Proof.

- (1) Since $E \neq \emptyset$, there is $y \in E$.
- (2) By the definition of the upper bound, $x \leq \beta$ for every $x \in E$. In particular, $y \leq \beta$.

(3) Similarly, $y \geq \alpha$.

(4) By (2)(3), $\alpha \leq y \leq \beta$ for some $y \in E$. In particular, $\alpha \leq \beta$ (Definition 1.5(ii)).

□

Exercise 1.5. Let A be a nonempty set of real numbers which is bounded below. Let $-A$ be the set of all numbers $-x$, where $x \in A$. Prove that

$$\inf A = -\sup(-A).$$

Proof. Let $\alpha = \inf A$ and $\beta = \sup(-A)$.

(1)

$$\begin{aligned} x \geq \alpha \quad \forall x \in A &\implies -x \leq -\alpha \quad \forall -x \in -A \\ &\implies -\alpha \text{ is an upper bound of } -A \\ &\implies \beta \leq -\alpha \\ &\implies \alpha \leq -\beta \end{aligned}$$

(2)

$$\begin{aligned} -x \leq \beta \quad \forall -x \in -A &\implies x \geq -\beta \quad \forall x \in A \\ &\implies -\beta \text{ is a lower bound of } A \\ &\implies \alpha \geq -\beta \end{aligned}$$

By (1)(2), $\alpha = -\beta$, or $\inf A = -\sup(-A)$. □

Exercise 1.6. Fix $b > 1$.

(a) If m, n, p, q are integers, $n > 0$, $q > 0$, and $r = m/n = p/q$, prove that

$$(b^m)^{1/n} = (b^p)^{1/q}.$$

Hence it makes sense to define $b^r = (b^m)^{1/n}$.

(b) Prove that $b^{r+s} = b^r b^s$ if r and s are rational.

(c) If x is real, define $B(x)$ to be the set of all numbers b^t , where t is rational and $t \leq x$. Prove that

$$b^r = \sup B(r)$$

where r is rational. Hence it makes sense to define

$$b^x = \sup B(x)$$

for every real x .

(d) Prove that $b^{x+y} = b^x b^y$ for all real x and y .

Proof of (a).

(1) Define $k = mq = np \in \mathbb{Z}$ (since $r = m/n = p/q$). Notice that $nq > 0$ (since $n > 0$ and $q > 0$). So there is one and only one $y \in \mathbb{R}$ such that

$$y^{nq} = b^k$$

where b^k is defined in \mathbb{R} (Theorem 1.21).

(2) Show that $y = (b^m)^{1/n}$ and $y = (b^p)^{1/q}$ are solutions of $y^{nq} = b^k$. In fact,

$$\begin{aligned} ((b^m)^{1/n})^{nq} &= (b^m)^q = b^{mq} = b^k, \\ ((b^p)^{1/q})^{nq} &= (b^p)^n = b^{pn} = b^k. \end{aligned}$$

(3) By (1)(2), the uniqueness of y shows that $(b^m)^{1/n} = (b^p)^{1/q}$, or the map $r \mapsto b^r$ is well-defined for $r \in \mathbb{Q}$.

□

Proof of (b). Write $r = m/n$ and $s = p/q$ where m, n, p, q are integers with $n > 0, q > 0$.

$$\begin{aligned} b^{r+s} &= b^{\frac{mq+np}{nq}} \\ &= (b^{mq} \cdot b^{np})^{\frac{1}{nq}} && (mq + np \in \mathbb{Z}) \\ &= (b^{mq})^{\frac{1}{nq}} \cdot (b^{np})^{\frac{1}{nq}} && (\text{Corollary to Theorem 1.21}) \\ &= b^{\frac{mq}{nq}} \cdot b^{\frac{np}{nq}} \\ &= b^{\frac{m}{n}} \cdot b^{\frac{n}{n}} && ((a)) \\ &= b^r \cdot b^s. \end{aligned}$$

□

Proof of (c).

(1) Given any $r \in \mathbb{Q}^+$, $b^r > 1$ since $b > 1$ is given.

(2) Given any $r, s \in \mathbb{Q}$, $b^r > b^s$ whenever $r > s$. In fact,

$$\begin{aligned} b^r &= b^{r-s} b^s && ((b)) \\ &> 1 \cdot b^s && ((1)) \\ &= b^s. \end{aligned}$$

(3) Given any $r \in \mathbb{Q}$, $b^t \leq b^r$ for any $t \in \mathbb{Q}$ whenever $t \leq r$. So $\sup B(r) \leq b^r$. Conversely, since $r \in B(r)$, $b^r \leq \sup B(r)$. So $b^r = \sup B(r)$.

- (4) Given any $x \in \mathbb{R}$. We can always find $r, s \in \mathbb{Q}$ such that $r < x < s$. Therefore, $r \in B(x)$ and $B(s)$ is an upper bound of $B(x)$. So there is a least upper bound $\sup B(x)$ for $B(x)$, i.e., $b^r = \sup B(r)$ is well-defined.

□

Lemma. If x is real, define $B'(x)$ to be the set of all numbers b^t , where t is rational and $t < x$. Prove that $\sup B'(x) = \sup B(x)$ for all $x \in \mathbb{R}$.

Proof of Lemma (Reductio ad absurdum). It suffices to show that $\sup B'(r) = \sup B(r) = b^r$ for all $r \in \mathbb{Q}$. (The case $x \in \mathbb{R} - \mathbb{Q}$ is nothing to do.) Clearly, $\sup B'(r) \leq b^r$. If $\alpha = \sup B'(r) < b^r$, then for $\frac{b^r}{\alpha} > 1$ there is $n > (b - 1)/(\frac{b^r}{\alpha} - 1)$ such that

$$b^{\frac{1}{n}} < \frac{b^r}{\alpha}$$

(Exercise 1.7(c)). So $\alpha < b^{r - \frac{1}{n}}$. Therefore, $b^{r - \frac{1}{n}} \in B'(r)$ since $r - \frac{1}{n} \in \mathbb{Q}$, or we find an element in $B'(r)$ such that is greater than α , contrary to the maximality of α . □

Proof of (d). Apply Lemma to use $B(x)$ or $B'(x)$ interchangeably.

- (1) Show that

$$\sup B'(x + y) \leq \sup B'(x) \sup B'(y).$$

Given any $b^t \in B'(x + y)$ such that $t < x + y$. There are rational numbers r, s such that $r < x$, $s < y$ and $t = r + s$. (Rewrite $t < x + y$ as $t - y < x$. Let $s = t - r < y$.) (Here we use $B'(x + y)$ instead of $B(x + y)$ to ensure the existence of r and s . That is, if $0 = -\sqrt{2} + \sqrt{2}$, we cannot find rational numbers $r \leq -\sqrt{2}$ and $s \leq \sqrt{2}$ such that $r + s = 0$.) Therefore,

$$b^t = b^{r+s} = b^r b^s \leq \sup B'(x) \sup B'(y)$$

(by (b)). Take supremum, $\sup B'(x + y) \leq \sup B'(x) \sup B'(y)$.

- (2) Show that

$$\sup B'(x + y) \geq \sup B'(x) \sup B'(y).$$

Given any $b^r \in B'(x)$, $b^s \in B'(y)$. $r < x$ and $s < y$. So $b^r b^s = b^{r+s} \in B'(x + y)$ (by (b)). So $b^r b^s \leq \sup B'(x + y)$. So

$$b^r \leq \frac{\sup B'(x + y)}{b^s}$$

since $b^s > 0$ for any $s \in \mathbb{Q}$. Here $\frac{\sup B'(x + y)}{b^s}$ is an upper bound for $B'(x)$. So

$$\sup B'(x) \leq \frac{\sup B'(x + y)}{b^s},$$

or $b^s \leq \frac{\sup B'(x+y)}{\sup B'(x)}$. Use the same argument again,

$$\sup B'(y) \leq \frac{\sup B'(x+y)}{\sup B'(x)}$$

or $\sup B'(x) \sup B'(y) \leq \sup B'(x+y)$.

By (1)(2), $\sup B'(x) \sup B'(y) = \sup B'(x+y)$ or $b^x b^y = b^{x+y}$. \square

Exercise 1.7. Fix $b > 1$, $y > 0$, and prove that there is a unique real x such that $b^x = y$, by completing the following outline. (This x is called the logarithm of y to the base b).

- (a) For any positive integer n , $b^n - 1 \geq n(b - 1)$.
- (b) Hence $b - 1 \geq n(b^{\frac{1}{n}} - 1)$.
- (c) If $t > 1$ and $n > \frac{b-1}{t-1}$, then $b^{\frac{1}{n}} < t$.
- (d) If w is such that $b^w < y$, then $b^{w+\frac{1}{n}} < y$ for sufficiently large n ; to see this, apply part (c) with $t = y \cdot b^{-w}$.
- (e) If $b^w > y$, then $b^{w-\frac{1}{n}} > y$ for sufficiently large n .
- (f) Let A be the set of all w such that $b^w < y$, and show that $x = \sup A$ satisfies $b^x = y$.
- (g) Prove that this x is unique.

Proof of (a).

$$\begin{aligned} b^n - 1 &= (b - 1)(b^{n-1} + b^{n-2} + \cdots + 1) \\ &\geq (b - 1)(1^{n-1} + 1^{n-2} + \cdots + 1) \\ &= (b - 1)n. \end{aligned}$$

The equality holds if and only if $n = 1$. (Or proved by the induction.) \square

Proof of (b). Put $b \mapsto b^{\frac{1}{n}}$ in (a). \square

Proof of (c). Since $n > \frac{b-1}{t-1}$ and (b), $n(t - 1) > b - 1 \geq n(b^{\frac{1}{n}} - 1)$. Cancel n on the both sides, $t - 1 > b^{\frac{1}{n}} - 1$ or $b^{\frac{1}{n}} < t$. \square

Proof of (d). Let $t = y \cdot b^{-w} > 1$. By (c), $b^{\frac{1}{n}} < y \cdot b^{-w}$ for $n > \frac{b-1}{y \cdot b^{-w} - 1}$, or $b^{w+\frac{1}{n}} < y$ for $n > \frac{b-1}{y \cdot b^{-w} - 1}$. \square

Proof of (e). Similar to (d). Let $t = y^{-1} \cdot b^w > 1$. By (c), $b^{\frac{1}{n}} < y^{-1} \cdot b^w$ for $n > \frac{b-1}{y^{-1} \cdot b^w - 1}$, or $b^{w+\frac{1}{n}} > y$ for $n > \frac{b-1}{y^{-1} \cdot b^w - 1}$. \square

Proof of (f). $x = \sup A < \infty$ by (a). (As $n > \frac{y-1}{b-1}$, $b^n > y$.) So there are only three possible cases.

- (1) $b^x < y$. By (d), $b^{x+\frac{1}{n}} < y$ for sufficiently large n , contrary to the maximality of x .
- (2) $b^x > y$. By (e), $b^{x-\frac{1}{n}} > y$ for sufficiently large n , contrary to the maximality of x .
- (3) By (1)(2), $b^x = y$ holds.

\square

Proof of (g) (Reductio ad absurdum). If there were another real $x' \neq x$ such that $b^{x'} = y$, then $x' > x$ or $x' < x$. For the case $x' > x$, $y = b^{x'} = b^x b^{x'-x} > b^x = y$, which is absurd. For the case $x' < x$, $y = b^x = b^{x'} b^{x-x'} > b^{x'} = y$, which is absurd too. \square

Exercise 1.8. *Prove that no order can be defined in the complex field that turns it into an ordered field. (Hint: -1 is a square.)*

Proof (Reductio ad absurdum). If \mathbb{C} were an ordered field, consider the complex number $i = \sqrt{-1}$.

- (1) $i \neq 0$. If i were 0, then $i \cdot i = 0 \cdot i$ or $-1 = 0$, or $1 = 0$, contrary to $1 > 0$ (Proposition 1.18).
- (2) Since $i \neq 0$, we have $i^2 > 0$ (Proposition 1.18). So $-1 > 0$, or $1 < 0$, contrary to the fact $1 > 0$ (Proposition 1.18).

\square

Supplement ($x^2 > 0$ if $x \neq 0$). *Show that the only automorphism of \mathbb{R} is the identity. (Hint: If σ is an automorphism, show that $\sigma|_{\mathbb{Q}} = \text{id}$, and if $a > 0$, then $\sigma(a) > 0$).*

It is an interesting fact that there are infinitely many automorphisms of \mathbb{C} , even though $[\mathbb{C} : \mathbb{R}] = 2$. Why is this fact not a contradiction to this problem?

Exercise 1.9. *Suppose $z = a + bi$, $w = c + di$. Define $z < w$ if $a < c$, and also if $a = c$ but $b < d$. Prove that this turns the set of all complex numbers into an ordered set. (This type of order relation is called a dictionary order, or lexicographic order, for obvious reasons.) Does this ordered set have the*

least-upper-bound property?

Proof.

(1) Show that \mathbb{C} is an ordered set.

(a) Show that if $x = a + bi, y = c + di \in \mathbb{C}$ then one and only one of the statements $x < y, x = y, y < x$ is true. Since \mathbb{R} is an ordered set, then one and only one of the statements $a < c, a = c, c < a$ is true.

(i) $a < c$. Hence $x < y$ (in the sense of the dictionary order).

(ii) $a = c$. Again since \mathbb{R} is an ordered set, then one and only one of the statements $b < d, b = d, d < b$ is true. That is, one and only one of the statements $x < y, x = y, y < x$ is true (in the sense of the dictionary order).

(iii) $c < a$. Hence $y < x$ (in the sense of the dictionary order).

By (i)(ii)(iii), the result is established.

(b) Show that if $x = a + bi, y = c + di, z = e + fi \in \mathbb{C}$, if $x < y$ and $y < z$, then $x < z$. Observe that if $x < y$ (resp. $y < z$) then $a \leq c$ (resp. $c \leq e$). Therefore, $a \leq c \leq e$. Thus, there are only two possible cases.

(i) Not every equality holds. $a < e$ or $x < z$ (in the sense of the dictionary order).

(ii) Every equality holds. $a = c = e$. Since $x < y$ (resp. $y < z$), $b < d$ (resp. $d < f$). So $b < d < f$, or $x < z$ (in the sense of the dictionary order).

In any case, $x < z$ if $x < y$ and $y < z$.

By (a)(b), \mathbb{C} is an ordered set (Definition 1.5).

(2) Show that \mathbb{C} has no least-upper-bound property. Assume \mathbb{C} has the least-upper-bound property. Consider

$$E = \{0\} \subseteq \mathbb{C}.$$

(a) E is bounded by $0 \in \mathbb{C}$. Thus E has the least upper bound $\alpha = a + bi \in \mathbb{C}$ where $a, b \in \mathbb{R}$. Here $a \geq 0$. (In fact $a = 0$.)

(b) Set $\gamma = a + (b - 1)i < a + bi = \alpha$. Note that $a \geq 0$ and thus γ is an upper bound of E , contrary to minimality of α .

Thus \mathbb{C} has no least-upper-bound property although E has the least upper bound ($= 0$) in \mathbb{R} .

□

Exercise 1.10. Suppose $z = a + bi$, $w = u + vi$, and

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

Prove that $z^2 = w$ if $v \geq 0$ and that $(\bar{z})^2 = w$ if $v \leq 0$. Conclude that every complex number (with one exception!) has two complex square roots.

Proof.

(1)

$$\begin{aligned} z^2 &= (a^2 - b^2) + 2abi \\ &= \left(\frac{|w| + u}{2} - \frac{|w| - u}{2} \right) + 2 \left(\frac{|w| + u}{2} \cdot \frac{|w| - u}{2} \right)^{\frac{1}{2}} i \\ &= u + (|w|^2 - u^2)^{\frac{1}{2}} i \\ &= u + (v^2)^{\frac{1}{2}} i \\ &= u + |v|i. \end{aligned}$$

Therefore, $z^2 = w$ if $v \geq 0$. $z^2 = \bar{w}$ if $v \leq 0$, or $(\bar{z})^2 = w$ if $v \leq 0$.

(2) Every complex number w has two complex square roots z and $-z$.

- (a) When $w \neq 0$, two square roots are distinct.
- (b) When $w = 0$, two square roots are identical, or there is only one square root for $w = 0$.

□

Exercise 1.11. If z is a complex number, prove that there exists an $r \geq 0$ and a complex number w with $|w| = 1$ such that $z = rw$. Are w and r always uniquely determined by z ?

To decide r and w in the relation $z = rw$, it is natural to take absolute values on the both sides. That is, $|z| = r|w| = r$.

Proof. Let $r = |z| \geq 0$.

- (1) $r \neq 0$. Define $w = \frac{z}{r} \in \mathbb{C}$. $|w| = \frac{|z|}{r} = 1$. In this case w and r are uniquely determined.
- (2) $r = 0$ (or $z = 0$). Define $w = e^{ix} = \cos x + i \sin x$ for any $x \in \mathbb{R}$. $|w| = 1$. Here r is uniquely determined but w is not uniquely determined.

□

Exercise 1.12. If z_1, \dots, z_n are complex, prove that

$$|z_1 + z_2 + \dots + z_n| \leq |z_1| + |z_2| + \dots + |z_n|.$$

Proof. Use mathematical induction on n . $n = 2$ is established by Theorem 1.33 (e). Suppose the inequality holds on $n = k$, then $n = k + 1$ we again apply Theorem 1.33 (e) to get the result, say

$$\begin{aligned} |z_1 + z_2 + \dots + z_k + z_{k+1}| &\leq |z_1 + z_2 + \dots + z_k| + |z_{k+1}| \\ &\leq |z_1| + |z_2| + \dots + |z_k| + |z_{k+1}| \end{aligned}$$

□

Supplement. If $\mathbf{x}_1, \dots, \mathbf{x}_n \in \mathbb{R}^k$, then

$$|\mathbf{x}_1 + \mathbf{x}_2 + \dots + \mathbf{x}_n| \leq |\mathbf{x}_1| + |\mathbf{x}_2| + \dots + |\mathbf{x}_n|.$$

Here we might use Theorem 1.37 (e) to prove it. Since the norm $|\cdot|$ on \mathbb{C} is the same as the norm on \mathbb{R}^2 , we might prove this supplement first and then set $k = 2$ on $\mathbb{R}^k = \mathbb{R}^2$ to give another proof of Exercise 1.12.

Exercise 1.13. If x, y are complex, prove that

$$||x| - |y|| \leq |x - y|.$$

We can show $f(x) = |x|$ is uniformly continuous in \mathbb{R} by using this inequality.

Proof (Exercise 1.12). Since

$$\begin{aligned} |y| &\leq |x| + |y - x| = |x| + |x - y| \\ |x| &\leq |y| + |x - y|, \end{aligned}$$

we have

$$-|x - y| \leq |x| - |y| \leq |x - y|,$$

or

$$||x| - |y|| \leq |x - y|.$$

□

Exercise 1.14. If z is a complex number such that $|z| = 1$, that is, such that $z\bar{z} = 1$, compute

$$|1 + z|^2 + |1 - z|^2.$$

Proof ($|z|^2 = z\bar{z}$).

$$\begin{aligned} |1 + z|^2 &= (1 + z)\overline{(1 + z)} = (1 + z)(1 + \bar{z}) = 1 + z + \bar{z} + z\bar{z} \\ |1 - z|^2 &= (1 - z)\overline{(1 - z)} = (1 - z)(1 - \bar{z}) = 1 - z - \bar{z} + z\bar{z} \\ |1 + z|^2 + |1 - z|^2 &= 2 + 2z\bar{z} = 2 + 2 = 4. \end{aligned}$$

□

Proof (Exercise 1.17). Regard \mathbb{C} as \mathbb{R}^2 . Then put $\mathbf{x} = 1, \mathbf{y} = z$ in the parallelogram law (Exercise 1.17) to get

$$|1 + z|^2 + |1 - z|^2 = 2|1|^2 + 2|z|^2 = 4.$$

□

Exercise 1.15. Under what conditions does equality hold in the Schwarz inequality?

Theorem 1.35 (Schwarz inequality). If a_1, \dots, a_n and b_1, \dots, b_n are complex numbers, then

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

In fact, the Lagrange's identity for complex numbers shows

$$\left| \sum_{k=1}^n a_k \bar{b}_k \right|^2 = \sum_{k=1}^n |a_k|^2 \sum_{k=1}^n |b_k|^2 - \sum_{1 \leq k < j \leq n} |a_k b_j - a_j b_k|^2.$$

In general, the Binet-Cauchy identity shows

$$\begin{aligned} & \sum_{1 \leq k < j \leq n} (a_k b_j - a_j b_k)(A_k B_j - A_j B_k) \\ &= \left(\sum_{k=1}^n a_k A_k \right) \left(\sum_{k=1}^n b_k B_k \right) - \left(\sum_{k=1}^n a_k B_k \right) \left(\sum_{k=1}^n b_k A_k \right). \end{aligned}$$

Proof of Binet-Cauchy identity.

$$\begin{aligned}
& \sum_{1 \leq k < j \leq n} (a_k b_j - a_j b_k)(A_k B_j - A_j B_k) \\
&= \sum_{1 \leq k < j \leq n} (a_k b_j A_k B_j + a_j b_k A_j B_k) - \sum_{1 \leq k < j \leq n} (a_k b_j A_j B_k - a_j b_k A_k B_j) \\
&= \sum_{1 \leq k < j \leq n} (a_k A_k b_j B_j + a_j A_j b_k B_k) - \sum_{1 \leq k < j \leq n} (a_k B_k b_j A_j + a_j B_j b_k A_k) \\
&= \sum_{1 \leq k \neq j \leq n} a_k A_k b_j B_j - \sum_{1 \leq k \neq j \leq n} a_k B_k b_j A_j \\
&= \sum_{1 \leq k, j \leq n} a_k A_k b_j B_j - \sum_{1 \leq k, j \leq n} a_k B_k b_j A_j \\
&\quad (\text{since } a_k A_k b_j B_j - a_k B_k b_j A_j = 0 \text{ as } k = j) \\
&= \left(\sum_{k=1}^n a_k A_k \right) \left(\sum_{j=1}^n b_j B_j \right) - \left(\sum_{k=1}^n a_k B_k \right) \left(\sum_{j=1}^n b_j A_j \right) \\
&= \left(\sum_{k=1}^n a_k A_k \right) \left(\sum_{k=1}^n b_k B_k \right) - \left(\sum_{k=1}^n a_k B_k \right) \left(\sum_{k=1}^n b_k A_k \right).
\end{aligned}$$

□

Proof of Lagrange's identity. Put $(a_k, b_k, A_k, B_k) \mapsto (a_k, b_k, \overline{a_k}, \overline{b_k})$ in the Binet-Cauchy identity. □

Proof of Schwarz inequality (Lagrange's identity). Notice the term

$$\sum_{1 \leq k < j \leq n} |a_k b_j - a_j b_k|^2 \geq 0.$$

□

Write $\mathbf{a} = (a_1, \dots, a_n)$ and $\mathbf{b} = (b_1, \dots, b_n)$ as two vectors in the vector space \mathbb{C}^n over \mathbb{C} . Back to the exercise now.

Proof (Lagrange's identity). $\sum_{1 \leq k < j \leq n} |a_k b_j - a_j b_k|^2 = 0 \iff a_k b_j = a_j b_k$ for any $1 \leq k < j \leq n$. The equality holds in the Schwarz inequality $\iff \mathbf{a}$ and \mathbf{b} are linearly dependent. □

Proof (Theorem 1.35). The equality holds in the Schwarz inequality. $\iff B = 0$ or the term $\sum |Ba_j - Cb_j|^2$ in the proof of Theorem 1.35 is 0. $\iff \mathbf{b} = \mathbf{0}$ or $\mathbf{a} = c\mathbf{b}$ for some $c \in \mathbb{C}$. $\iff \mathbf{a}$ and \mathbf{b} are linearly dependent. □

Exercise 1.16. Suppose $k \geq 3$, $\mathbf{x}, \mathbf{y} \in \mathbb{R}^k$, $|\mathbf{x} - \mathbf{y}| = d > 0$, and $r > 0$. Prove:

(a) If $2r > d$, there are infinitely many $\mathbf{z} \in \mathbb{R}^k$ such that

$$|\mathbf{z} - \mathbf{x}| = |\mathbf{z} - \mathbf{y}| = r.$$

(b) If $2r = d$, there is exactly one such \mathbf{z} .

(c) If $2r < d$, there is no such \mathbf{z} .

How must these statements be modified if k is 2 or 1?

Proof (Brute-force). By Exercise 1.17, we have

$$\begin{aligned} |\mathbf{z} - \mathbf{x}|^2 + |\mathbf{z} - \mathbf{y}|^2 &= 2 \left| \mathbf{z} - \frac{\mathbf{x} + \mathbf{y}}{2} \right|^2 + 2 \left| \frac{\mathbf{x} - \mathbf{y}}{2} \right|^2, \\ r^2 + r^2 &= 2 \left| \mathbf{z} - \frac{\mathbf{x} + \mathbf{y}}{2} \right|^2 + \frac{1}{2}d^2, \\ \left| \mathbf{z} - \frac{\mathbf{x} + \mathbf{y}}{2} \right|^2 &= r^2 - \frac{d^2}{4} \end{aligned}$$

for every $k = 1, 2, 3, \dots$. Let $\mathbf{w} = \mathbf{z} - \frac{\mathbf{x} + \mathbf{y}}{2}$. So $|\mathbf{w}|^2 = r^2 - \frac{d^2}{4}$.

(a) Suppose $2r > d$.

(i) Show that $\mathbf{w} \cdot (\mathbf{x} - \mathbf{y}) = 0$.

$$\begin{aligned} |\mathbf{z} - \mathbf{x}| = |\mathbf{z} - \mathbf{y}| &\iff |\mathbf{z} - \mathbf{x}|^2 = |\mathbf{z} - \mathbf{y}|^2 \\ &\iff |\mathbf{z}|^2 - 2\mathbf{z} \cdot \mathbf{x} + |\mathbf{x}|^2 = |\mathbf{z}|^2 - 2\mathbf{z} \cdot \mathbf{y} + |\mathbf{y}|^2 \\ &\iff 2\mathbf{z} \cdot (\mathbf{x} - \mathbf{y}) = |\mathbf{x}|^2 - |\mathbf{y}|^2 = (\mathbf{x} + \mathbf{y}) \cdot (\mathbf{x} - \mathbf{y}) \\ &\iff \left(\mathbf{z} - \frac{\mathbf{x} + \mathbf{y}}{2} \right) \cdot (\mathbf{x} - \mathbf{y}) = 0 \\ &\iff \mathbf{w} \cdot (\mathbf{x} - \mathbf{y}) = 0. \end{aligned}$$

(ii) Since $\mathbf{x} \neq \mathbf{y}$, we may suppose that $x_1 \neq y_1$. So the solution of $\mathbf{w} \cdot (\mathbf{x} - \mathbf{y}) = 0$ is

$$\begin{cases} w_1 = -\frac{1}{x_1 - y_1}(t_2(x_2 - y_2) + \dots + t_k(x_k - y_k)) \\ w_2 = t_2 \\ \dots \\ w_k = t_k \end{cases}$$

where $\mathbf{w} = (w_1, \dots, w_k)$ and $t_2, \dots, t_k \in \mathbb{R}$.

(iii) Also

$$\begin{aligned}
|\mathbf{w}|^2 &= r^2 - \frac{d^2}{4} \\
\iff w_1^2 + \dots + w_k^2 &= r^2 - \frac{d^2}{4} \\
\iff \frac{(t_2(x_2 - y_2) + \dots + t_k(x_k - y_k))^2}{(x_1 - y_1)^2} + \dots + t_k^2 &= r^2 - \frac{d^2}{4}
\end{aligned}$$

That is, t_2 is uniquely determined by $t_3, \dots, t_k \in \mathbb{R}$. Clearly, such $\mathbf{z} = \mathbf{w} + \frac{\mathbf{x} + \mathbf{y}}{2}$ satisfies $|\mathbf{z} - \mathbf{x}| = |\mathbf{z} - \mathbf{y}| = r$.

(iv) As $k \geq 3$, there are infinitely many $\mathbf{z} = \mathbf{w} + \frac{\mathbf{x} + \mathbf{y}}{2} \in \mathbb{R}^k$.

(v) As $k = 2$,

$$\frac{t_2^2(x_2 - y_2)^2}{(x_1 - y_1)^2} + t_2^2 = r^2 - \frac{d^2}{4} \iff t_2^2 = \frac{r^2 - \frac{d^2}{4}}{1 + \frac{(x_2 - y_2)^2}{(x_1 - y_1)^2}} > 0,$$

that is, t_2 has exactly two solutions, or \mathbf{z} has two solutions in \mathbb{R}^2 .

(vi) As $k = 1$, there is no such t_2 . So $\mathbf{w} = \mathbf{0}$, contrary to the assumption $|\mathbf{w}| > 0$. In this case there are no solution \mathbf{z} in \mathbb{R}^2 .

(b) If $2r = d$, $|\mathbf{w}|^2 = 0$. $\mathbf{w} = \mathbf{0}$ or $\mathbf{z} = \frac{\mathbf{x} + \mathbf{y}}{2}$. Such \mathbf{z} satisfies $|\mathbf{z} - \mathbf{x}| = |\mathbf{z} - \mathbf{y}| = \frac{d}{2} = r$ for every $k = 1, 2, 3, \dots$

(c) If $2r < d$, $|\mathbf{w}|^2 < 0$, which is impossible. Therefore, there is no such \mathbf{z} for every $k = 1, 2, 3, \dots$

□

Exercise 1.17. Prove that

$$|\mathbf{x} + \mathbf{y}|^2 + |\mathbf{x} - \mathbf{y}|^2 = 2|\mathbf{x}|^2 + 2|\mathbf{y}|^2$$

if $\mathbf{x} \in \mathbb{R}^k$ and $\mathbf{y} \in \mathbb{R}^k$. Interpret this geometrically, as a statement about parallelograms.

Proof.

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

Interpret this geometrically, the sum of the squares of the lengths of the four sides of a parallelogram equals the sum of the squares of the lengths of the two diagonals.

If the parallelogram is a rectangle, the two diagonals are of equal lengths, so that the statement reduces to the Pythagorean theorem. \square

Exercise 1.18. If $k \geq 2$ and $\mathbf{x} \in \mathbb{R}^k$, prove that there exists $\mathbf{y} \in \mathbb{R}^k$ such that $\mathbf{y} \neq 0$ but $\mathbf{x} \cdot \mathbf{y} = 0$. Is this also true if $k = 1$?

Proof.

(1) There are only two possible cases.

- (a) $\exists i$ such that $x_i = 0$. Let $\mathbf{y} = (0, \dots, 0, 1, 0, \dots, 0) \neq 0$ whose entries are all 0 except for a 1 in the i -th position. So $\mathbf{x} \cdot \mathbf{y} = 0 + \dots + 0 = 0$.
- (b) $\forall i, x_i \neq 0$. Since $k \geq 2$, we can define $\mathbf{y} = (x_2, -x_1, 0, \dots, 0) \neq 0$. So $\mathbf{x} \cdot \mathbf{y} = x_1 x_2 + x_2(-x_1) + 0 + \dots + 0 = 0$.

(2) It is not true for $k = 1$ since $\mathbb{R}^1 = \mathbb{R}$ is a field.

\square

Exercise 1.19. Suppose $\mathbf{a} \in \mathbb{R}^k$, $\mathbf{b} \in \mathbb{R}^k$. Find $\mathbf{c} \in \mathbb{R}^k$ and $r > 0$ such that

$$|\mathbf{x} - \mathbf{a}| = 2|\mathbf{x} - \mathbf{b}|$$

if and only if $|\mathbf{x} - \mathbf{c}| = r$. (Solution: $3\mathbf{c} = 4\mathbf{b} - \mathbf{a}$, $3r = 2|\mathbf{b} - \mathbf{a}|$.)

Suppose $\mathbf{a} \neq \mathbf{b}$ to guarantee the existence of $r > 0$.

It is known as **circles of Apollonius**. In general, for any $\mu > 1$,

$$|\mathbf{x} - \mathbf{a}| = \mu|\mathbf{x} - \mathbf{b}|$$

if and only if $|\mathbf{x} - \mathbf{c}| = r$ where $\mathbf{c} = \frac{\mu^2 \mathbf{b} - \mathbf{a}}{\mu^2 - 1}$ and $r = \frac{\mu}{\mu^2 - 1} |\mathbf{b} - \mathbf{a}|$.

Proof.

$$\begin{aligned} |\mathbf{x} - \mathbf{a}| &= \mu|\mathbf{x} - \mathbf{b}| \\ \iff |\mathbf{x} - \mathbf{a}|^2 &= \mu^2 |\mathbf{x} - \mathbf{b}|^2 \\ \iff |\mathbf{x}|^2 - 2\mathbf{a} \cdot \mathbf{x} + |\mathbf{a}|^2 &= \mu^2 |\mathbf{x}|^2 - 2\mu^2 \mathbf{b} \cdot \mathbf{x} + \mu^2 |\mathbf{b}|^2 \\ \iff (\mu^2 - 1)|\mathbf{x}|^2 - 2(\mu^2 \mathbf{b} - \mathbf{a}) \cdot \mathbf{x} + (\mu^2 |\mathbf{b}|^2 - |\mathbf{a}|^2) &= 0 \\ \iff |\mathbf{x}|^2 - 2\frac{\mu^2 \mathbf{b} - \mathbf{a}}{\mu^2 - 1} \cdot \mathbf{x} + \frac{\mu^2 |\mathbf{b}|^2 - |\mathbf{a}|^2}{\mu^2 - 1} &= 0. \end{aligned}$$

Write $\mathbf{c} = \frac{\mu^2 \mathbf{b} - \mathbf{a}}{\mu^2 - 1}$ and $r = \frac{\mu}{\mu^2 - 1} |\mathbf{b} - \mathbf{a}| > 0$. Note that $|\mathbf{c}|^2 - r^2 = \frac{\mu^2 |\mathbf{b}|^2 - |\mathbf{a}|^2}{\mu^2 - 1}$. Thus

$$\begin{aligned} |\mathbf{x} - \mathbf{a}| &= \mu |\mathbf{x} - \mathbf{b}| \\ \iff |\mathbf{x}|^2 - 2\mathbf{c} \cdot \mathbf{x} + |\mathbf{c}|^2 - r^2 &= 0. \\ \iff |\mathbf{x} - \mathbf{c}|^2 &= r^2 \\ \iff |\mathbf{x} - \mathbf{c}| &= r. \end{aligned}$$

□

Exercise 1.20. *With reference to the Appendix, suppose that property (III) were omitted from the definition of a Dedekind cut. Keep the same definitions of order and addition. Show that the resulting ordered set has the least-upper-bound property, that addition satisfies axioms (A1) to (A4) (with a slightly different zero-element!) but that (A5) fails.*

Proof of the least-upper-bound property.

- (1) Let A be a nonempty subset of \mathbb{R} , and assume that $\beta \in \mathbb{R}$ is an upper bound of A .
- (2) Define γ to be the union of all $\alpha \in A$. We shall prove that $\gamma \in \mathbb{R}$ and that $\gamma = \sup A$.
- (3) *Show that $\gamma \in \mathbb{R}$.* Property (I) is established by property (I) of $\alpha \in A$ and property (I) of β . Property (II) is established by property (I) of γ and property (II) of $\alpha \in A$.
- (4) *Show that $\gamma = \sup A$.* The result is established by property (II) of $\alpha \in A$.

□

Supplement (Noetherian modules). *Let M be a module over a commutative ring R . Then M is Noetherian (that is, every submodule of M is finitely generated) implies that every ascending chain of submodules of M terminates (“ascending chain condition”).*

Proof of Supplement. Given any ascending chain of submodules $N_1 \subseteq N_2 \subseteq \cdots$, let

$$N = \bigcup_{i=1}^{\infty} N_i.$$

- (a) N is a submodule. By the ascending chain condition, each pair of elements in N are in a common N_m .
- (b) N is finitely generated by assumption. By the ascending chain condition again, all generators of N are in a common N_m . So $N = N_m$ for some m .

(c) Since $N_m = N \supseteq N_n$ whenever $n \geq m$, $N_m = N_{m+1} = \dots$.

□

Proof of (A1). All the same as the textbook except: *show that $\alpha + \beta \in \mathbb{R}$* . Both property (I)(II) are established by property (I)(II) of α and of β . □

Proof of (A2)(A3). Established by the definition of Dedekind cuts. □

Proof of (A4).

(1) In the textbook (page 18), we cannot get the opposite inclusion $\alpha + 0^* \supseteq \alpha$ since no property (III) to guarantee the existence of $r \in \alpha$.

(2) Therefore, we define $0^\# = \{p \in \mathbb{Q} : p \leq 0\}$.

(3) *Show that $\alpha + 0^\# = \alpha$.*

(a) *Show that $\alpha + 0^\# \subseteq \alpha$.* Given any $r \in \alpha$, $s \in 0^\#$.

(i) If $s = 0$, $r + s = r \in \alpha$.

(ii) If $s < 0$, $r + s < r$. So $r + s \in \alpha$ by property (II).

Hence, $r + s$ is always in α .

(b) *Show that $\alpha + 0^\# \supseteq \alpha$.* Given any $r \in \alpha$, $r = r + 0 \in \alpha + 0^\#$.

□

Proof of failure of (A5)(Reductio ad absurdum).

(1) Consider $0^* = \{p \in \mathbb{Q} : p < 0\} \in \mathbb{R}$.

(2) If (A5) were true, then there were an element $\alpha \in \mathbb{R}$ such that $0^* + \alpha = 0^\#$.

(3) Note that $0^\#$ has the maximal element (namely 0), and thus $0^* + \alpha$ has the maximal element $s + r$ where $s \in 0^*$ and $r \in \alpha$.

(4) $s \in 0^*$ implies $s < 0$. Then there exists $s' \in \mathbb{Q}$ such that $s < s' < 0$. So $s' \in 0^*$ and $s' + r \in 0^* + \alpha$. $s' + r > s + r$, contrary to the maximality of $s + r$.

□