1 Chapter 1 Exercises

Exercises with solutions from Chapter 1 of [PMA].

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

Solution. In both cases we shall prove the contrapositive. Suppose $r+x = p \in \mathbb{Q}$. Then $x = p-r$, a rational number. Similarly, $rx = q \in \mathbb{Q}$ implies that $x = \frac{q}{r}$, a rational number.

2. Prove that there is no rational number whose square is 12.

Solution. Taking as given that each positive integer has a unique prime factorization, we shall prove the following stronger result:

> Let n be a positive integer. If n is not the square of an integer then there is no rational number whose square is n.

In fact, we shall prove the contrapositive. Suppose there is a rational $\frac{a}{b}$ such that $a^2 = nb^2$. The primes in the factorizations of a^2 and b^2 must appear to even powers; unique prime factorization implies that the primes in the factorization of nb^2 must be the same as those in the factorization of a^2. It follows that the factorization of n contains only primes raised to even powers, else the factorization of nb^2 would contain a prime raised to an odd power. Hence n is the square of an integer.

3. Prove Proposition 1.15.

1.15 Proposition *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 $y = x^{-1}$.*

(d) *If $x \neq 0$ then $(x^{-1})^{-1} = x$.*

Solution. For (a), we have

$$y = 1y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = 1z = z.$$

Take $z = 1$ in (a) to obtain (b), $z = x^{-1}$ in (a) to obtain (c), and for (d), replace x with x^{-1} and y with x in (c).

4. Let E be a non-empty subset of an ordered set; suppose α is a lower bound of E and β is an upper bound of E. Prove that $\alpha \leq \beta$.

Solution. Since E is non-empty, there exists $x \in E$. Then $\alpha \leq x \leq \beta$.

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

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

Solution. $-A$ is non-empty since A is non-empty and $-A$ is bounded above since A is bounded below ($x \geq y$ implies $-x \leq -y$ in an ordered field). Hence $\sup(-A)$ exists in $\mathbb{R}$. Let $x \in A$ be given. Then $-x \leq \sup(-A)$, which gives $x \geq -\sup(-A)$, so that $-\sup(-A)$ is a lower bound of A. Now suppose $y > -\sup(-A)$. Then $-y < \sup(-A)$, so that $-y$ is not an upper bound for $-A$, i.e. there exists $x \in A$ such that $-y < -x$. This gives $y > x$, demonstrating that y is not a lower bound of A. It follows that $-\sup(-A)$ is the infimum of A.

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

Solution. Let $x = (b^m)^{1/n}$ and $y = (b^p)^{1/q}$. Then observe that

$$b^{np} = b^{mq} \iff (b^p)^n = (b^m)^q \iff (y^q)^n = (x^n)^q \iff y^{nq} = x^{nq}.$$

Since x, y, n, q are all positive, this implies that $x = y$.

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

Solution. The result is certainly true if r and s are integers; we shall use this freely. Suppose $r = m/n$ and $s = p/q$. Then

$$b^{r+s} = b^{\frac{mq+np}{nq}} = (b^{mq+np})^{1/nq} = (b^{mq}b^{np})^{1/nq} = (b^{mq})^{1/nq}(b^{np})^{1/nq} = b^{mq/nq}b^{np/nq} = b^{m/n}b^{p/q} = b^r b^s,$$

where we have used the corollary to Theorem 1.21 of [PMA].

(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

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

when r is rational. Hence it makes sense to define

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

for every real x.

Solution. First, let us work from the field axioms and Theorem 1.21 of [PMA] to prove some useful lemmas.

Lemma 1. Suppose we have a real number $b > 1$ and integers m, n. Then $m \leq n$ if and only if $b^m \leq b^n$.

Proof. Since $b > 1$, induction on k shows that $b^k \geq 1$ for any non-negative integer k, with equality exactly when $k = 0$. Suppose $m \leq n$; then $1 \leq b^{n-m}$. Multiply both sides of this inequality by the positive quantity b^m to obtain $b^m \leq b^n$. Now suppose $m > n$. Then $b^{m-n} > 1$, and $b^m > b^n$ follows since b^n is positive. ☐

Lemma 2. Suppose we have positive real numbers x, y and a positive integer n. Then $x \leq y$ if and only if $x^{1/n} \leq y^{1/n}$.

Proof. It follows from the uniqueness part of Theorem 1.21 of [PMA] that $x = (x^n)^{1/n} = (x^{1/n})^n$. Given this, the result of the lemma is equivalent to $x \leq y \iff x^n \leq y^n$. Both of the implications $x \leq y \implies x^n \leq y^n$ and $x > y \implies x^n > y^n$ follow quickly from the field axioms and induction on n. ☐

Lemmas 1 and 2 give us the following result.

Lemma 3. Suppose we have a real number $b > 1$ and rationals $r = m/n, t = p/q$, where $n, q > 0$. Then $r \leq t$ if and only if $b^r \leq b^t$.

Proof.

$$\begin{aligned} r \leq t &\iff mq \leq np \\ &\iff b^{mq} \leq b^{np} && \text{(Lemma 1)} \\ &\iff b^m \leq (b^{p/q})^n && \text{(Lemma 2)} \\ &\iff b^{m/n} \leq b^{p/q} && \text{(Lemma 2).} \end{aligned}$$

☐

Now, returning to the exercise, let us show that

$$B(x) = \{b^t : t \in \mathbb{Q}, t \leq x\}$$

is non-empty and bounded above for any real x. There are certainly rational numbers less than x, so $B(x)$ is non-empty, and there are certainly rational numbers greater than x, so by Lemma

3 $B(x)$ is bounded above by b to the power of any such rational. Hence $\sup B(x)$ always exists in $\mathbb{R}$.

Remark. Since any element of $B(x)$ is positive, $\sup B(x)$ is also positive, i.e. b^x is positive for any $b > 1$ and $x \in \mathbb{R}$.

Finally, let us show that $b^r = \sup B(r)$ for a rational r. It follows from Lemma 3 that b^r is an upper bound for $B(r)$, and since b^r belongs to $B(r)$ it must be the supremum of $B(r)$.

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

Solution. To prove this, we will show that both of the assumptions $b^{x+y} < b^x b^y$ and $b^x b^y < b^{x+y}$ lead to contradictions. First, suppose that $b^{x+y} < b^x b^y$, i.e. $\sup B(x+y) < \sup B(x) \cdot \sup B(y)$. This assumption is equivalent to $\frac{\sup B(x+y)}{\sup B(y)} < \sup B(x)$, so that $\frac{\sup B(x+y)}{\sup B(y)}$ is not an upper bound for $B(x)$. Then there must exist some rational r such that $r \leq x$ and

$$\frac{\sup B(x+y)}{\sup B(y)} < b^r \iff \frac{\sup B(x+y)}{b^r} < \sup B(y).$$

This demonstrates that $\frac{\sup B(x+y)}{b^r}$ is not an upper bound for $B(y)$, so there must exist a rational s such that $s \leq y$ and

$$\frac{\sup B(x+y)}{b^r} < b^s \iff \sup B(x+y) < b^r b^s = b^{r+s}.$$

This is a contradiction since

$$r + s \leq x + y \implies b^{r+s} \in B(x+y) \implies b^{r+s} \leq \sup B(x+y).$$

Now suppose that $b^x b^y < b^{x+y}$. We shall make use of the following inequality:

$$\forall n \in \mathbb{N} \qquad b^{1/n} \leq 1 + \frac{b-1}{n}.$$

This is proved in Exercise 7 (a) and (b). By assumption $b^{x+y} - b^x b^y > 0$, so by invoking the Archimedean property of $\mathbb{R}$ we may obtain a positive integer n such that

$$n(b^{x+y} - b^x b^y) > (b-1)b^x b^y \implies \frac{b^{x+y}}{b^x b^y} > 1 + \frac{b-1}{n} \geq b^{1/n} \implies b^x b^y b^{1/n} < b^{x+y}.$$

The density of $\mathbb{Q}$ in $\mathbb{R}$ implies that there exist rational numbers r and s such that $x - \frac{1}{2n} < r \leq x$ and $y - \frac{1}{2n} < s \leq y$, which implies that $x + y < r + s + \frac{1}{n}$. It follows that

$$b^{x+y} \leq b^{r+s+1/n} = b^r b^s b^{1/n} \leq b^x b^y b^{1/n} < b^{x+y},$$

i.e. $b^{x+y} < b^{x+y}$, a contradiction.

7. Fix $b > 1, y > 0$, and prove that there exists 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, $b^n - 1 \geq n(b-1)$.

Solution. Observe that
$$b^n - 1 = (\textstyle\sum_{j=0}^{n-1} b^j)(b-1).$$
The desired result follows since there are n terms in the sum $\sum_{j=0}^{n-1} b^j$ and $b > 1 \implies b^j > 1$.

(b) Hence $b - 1 \geq n(b^{1/n} - 1)$.

Solution. By Lemma 2, $b > 1 \implies b^{1/n} > 1$. So this result follows by replacing b with $b^{1/n}$ in the inequality of part (a).

(c) If $t > 1$ and $n > (b-1)/(t-1)$, then $b^{1/n} < t$.

Solution. By part (b), we have $b^{1/n} - 1 \leq (b-1)/n < t - 1$; the result follows.

(d) If w is such that $b^w < y$, then $b^{w+(1/n)} < y$ for sufficiently large n; to see this, apply part (c) with $t = yb^{-w}$.

Solution. Since $y > b^w$, we have $t = b^{-w}y > 1$. Take n large enough so that $n > (b-1)/(t-1)$ and apply part (c) to obtain $b^{1/n} < b^{-w}y$, from which the result follows.

(e) If $b^w > y$, then $b^{w-(1/n)} > y$ for sufficiently large n.

Solution. Similarly, we take $t = b^w y^{-1} > 1$, n large enough so that $n > (b-1)/(t-1)$, and apply part (c) to obtain $b^{1/n} < b^w y^{-1}$; the result follows.

(f) Let A be the set of all w such that $b^w < y$, and show that $x = \sup A$ satisfies $b^x = y$.

Solution. First, a lemma which generalises Lemma 3 above.

Lemma 4. Suppose we have real numbers b, x, y such that $b > 1$. Then $x \leq y$ if and only if $b^x \leq b^y$.

Proof. If $x \leq y$ then
$$B(x) = \{b^t : t \in \mathbb{Q}, t \leq x\} \subseteq B(y) = \{b^t : t \in \mathbb{Q}, t \leq y\},$$

whence $b^x = \sup B(x) \leq \sup B(y) = b^y$; the implication $x > y \implies b^x > b^y$ follows similarly. $\square$

Now let us show that $A = \{w \in \mathbb{R} : b^w < y\}$ is non-empty and bounded above. Since $b - 1 > 0$, there is a positive integer n such that $n(b-1) > y^{-1} - 1$. Part (a) then gives us $b^n - 1 > y^{-1} - 1$, so that $b^{-n} < y$. Hence $-n \in A$. Similarly, there is a positive integer N such that $b^N > y$. Then for any $w \in A$ we have $b^w < y < b^N$ and an application of Lemma 4 gives us $w < N$, so that N is an upper bound for A. Hence $x = \sup A$ exists in $\mathbb{R}$.

To show that $b^x = y$, we will show that both of the assumptions $b^x < y$ and $b^x > y$ lead to contradictions. If $b^x < y$, then by part (d) there is a positive integer n such that $b^{x+(1/n)} < y$; but then $x + (1/n) \in A$, contradicting that x is the supremum of A. If $b^x > y$, then by part (e) there is a positive integer n such that $b^{x-(1/n)} > y$; but then for any $w \in A$ we have

$$b^w < y < b^{x-(1/n)} \implies w < x - (1/n),$$

where we have used Lemma 4. This says that $x - (1/n)$ is an upper bound for A, contradicting that x is the supremum of A.

(g) Prove that this x is unique.

Solution. This follows from Lemma 4.

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

Solution. Suppose there was such an order $<$. Then by Proposition 1.18 of [PMA] we must have $i^2 = -1 > 0$, which contradicts the very same proposition.

9. Suppose $z = a + bi, w = c + di$. Define $z \prec w$ 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?

Solution. Consider the following cases.

Case 1. $a < c$. Then $z \prec w$.

Case 2. $a = c$.

Case 2.1. $b < d$. Then $z \prec w$.

Case 2.2. $b = d$. Then $z = w$.

Case 2.3. $b > d$. Then $z \succ w$.

Case 3. $a > c$. Then $z \succ w$.

These cases are exclusive and exhaustive since $<$ is an order on $\mathbb{R}$. So exactly one of $z \prec w, z = w$, or $z \succ w$ always holds. Suppose, for $u = x + yi$, we have $z \prec w$ and $w \prec u$. Then there are four cases:

Case 1. $a < c$.

Case 1.1. $c < x$. Then $a < x$, so that $z \prec u$.

Case 1.2. $c = x$ and $d < y$. Then $a < x$, so that $z \prec u$.

Case 2. $a = c$ and $b < d$.

Case 2.1. $c < x$. Then $a < x$, so that $z \prec u$.

Case 2.2. $c = x$ and $d < y$. Then $a = x$ and $b < y$, so that $z \prec u$.

In any case, we have transitivity and hence have shown that $\prec$ is an order on $\mathbb{C}$.

Now we claim that $(\mathbb{C}, \prec)$ does not have the least-upper-bound property. To see this, consider the set $E = \{0 + yi : y \in \mathbb{R}\}$; this is clearly non-empty and bounded above by, for example, any number of the form $x + 0i$ for a positive real number x. Suppose $a + bi$ is an upper bound for E. It follows that $a > 0$, for if $a \leq 0$ then $(b+1)i \succ a + bi$. But now $\frac{a}{2} + bi$ is also an upper bound for E and $\frac{a}{2} + bi \prec a + bi$. Hence E has no least upper bound.

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

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

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

Solution. First, suppose that $v \geq 0$. Then

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

So $z^2 = w$, which also gives us $(-z)^2 = w$. Hence w has two complex square roots, z and $-z$. These are distinct precisely when $z \neq 0 \iff z^2 = w \neq 0$. Now suppose that $v \leq 0$. Then

$$\begin{aligned} (\overline{z})^2 &= a^2 - b^2 - 2abi \\ &= u - (v^2)^{1/2} i \\ &= u - (-v)i \\ &= u + vi. \end{aligned}$$

So $(\overline{z})^2 = w$, which also gives us $(-\overline{z})^2 = w$. Hence w has two complex square roots, $\overline{z}$ and $-\overline{z}$. Similarly, these are distinct precisely when $\overline{z} \neq 0 \iff \overline{z}^2 = w \neq 0$. We conclude that every complex number other than 0 has (at least) two distinct complex square roots; 0 has itself as its unique square root.

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?

Solution. If $z \neq 0$, take $r = |z|$ and $w = \frac{z}{|z|}$. These choices are unique, since $z = rw$ implies that $|z| = |rw| = r$, which in turn gives $w = \frac{z}{|z|}$. If $z = 0$, then $r = 0$ and any w with $|w| = 1$ will do. In this case, $r = 0$ is uniquely determined, but there any infinitely many choices of w which satisfy the equation.

12. If $z_1, \ldots, z_n$ are complex, prove that

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

Solution. This follows from Theorem 1.33 (e) of [PMA] and induction on n.

13. If x, y are complex, prove that

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

Solution. Observe that

$$|x| = |x - y + y| \le |x - y| + |y| \implies |x| - |y| \le |x - y|,$$

$$|y| = |x - y - x| \le |x - y| + |x| \implies -(|x| - |y|) \le |x - y|.$$

Since $||x| - |y|| = |x| - |y|$ or $-(|x| - |y|)$, the result follows.

14. If z is a complex number such that $|z| = 1$, that is, such that $z\overline{z} = 1$, compute

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

Solution. This is a quick computation:

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

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

Solution. Let $\boldsymbol{a} = (a_1, \ldots, a_n)$ and $\boldsymbol{b} = (b_1, \ldots, b_n)$ be vectors in $\mathbb{C}^n$. We will show that equality holds in the Schwarz inequality

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

if and only if $\boldsymbol{a}$ and $\boldsymbol{b}$ are linearly dependent.

First, suppose that $\boldsymbol{a}$ and $\boldsymbol{b}$ are linearly dependent. Then one is a complex multiple of the other and equality in (†) is easily verified. Conversely, suppose that equality holds in (†). As in the proof of the Schwarz inequality in [PMA], put $A = \sum_{j=1}^{n} |a_j|^2$, $B = \sum_{j=1}^{n} |b_j|^2$, and $C = \sum_{j=1}^{n} a_j \overline{b_j}$, so that

$$\sum_{j=1}^{n} |Ba_j - Cb_j|^2 = B(AB - |C|^2). \tag{$*$}$$

Equality in (†) implies that the above quantity is zero, which gives us $Ba_j = Cb_j$ for each j. If $\boldsymbol{b}$ is the zero vector, then certainly $\boldsymbol{a}$ and $\boldsymbol{b}$ are linearly dependent. So assume that $\boldsymbol{b}$ is not the zero vector, which is the case precisely when $B > 0$. Then we have $a_j = \frac{C}{B} b_j$ for each j, i.e. $\boldsymbol{a} = \frac{C}{B} \boldsymbol{b}$, which demonstrates the linear dependence of $\boldsymbol{a}$ and $\boldsymbol{b}$.

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

(Exercise 18 has been shifted up since the solution will be useful for Exercise 16 below.)

Solution. If $\boldsymbol{x} = \mathbf{0}$, any $\boldsymbol{y} \in \mathbb{R}^k$ will do. Assume therefore that $\boldsymbol{x} \neq \mathbf{0}$, so that there is some $1 \leq i \leq k$ such that $x_i \neq 0$. Choose any real numbers, other than all zeros, for the components of $\boldsymbol{y}$ other than y_i (there is at least one such component since $k \geq 2$). Now set

$$y_i = \frac{-(x_1 y_1 + \cdots + x_{i-1} y_{i-1} + x_{i+1} y_{i+1} + \cdots + x_k y_k)}{x_i}.$$

It then follows that: $\boldsymbol{y} \neq \mathbf{0}$ since we chose at least one non-zero component for $\boldsymbol{y}$, $\boldsymbol{x} \cdot \boldsymbol{y} = 0$, and, given the choices for the components of $\boldsymbol{y}$ other than y_i, only this choice of y_i will yield a $\boldsymbol{y}$ satisfying $\boldsymbol{x} \cdot \boldsymbol{y} = 0$; indeed

$$\boldsymbol{x} \cdot \boldsymbol{y} = 0 \iff \boldsymbol{x} \cdot \boldsymbol{y} - x_i y_i + x_i y_i = 0 \iff y_i = \frac{-1}{x_i}(\boldsymbol{x} \cdot \boldsymbol{y} - x_i y_i).$$

The result is no longer true if $k = 1$. It is still the case that if $x = 0$ then any $y \in \mathbb{R}$ will do, however for $x \neq 0$ there are no non-zero solutions for y; this would violate the field axioms (see Proposition 1.16 (b) of [PMA]).

16. Suppose $k \geq 3$, $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^k$, $|\boldsymbol{x} - \boldsymbol{y}| = d > 0$, and $r > 0$. Prove:
(a) If $2r > d$, there are infinitely many $\boldsymbol{z} \in \mathbb{R}^k$ such that

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

Solution. Suppose $\boldsymbol{w} \in \mathbb{R}^k$ satisfies the following two conditions:

(1) $\boldsymbol{w} \cdot (\boldsymbol{x} - \boldsymbol{y}) = 0$;

(2) $|\boldsymbol{w}| = \sqrt{r^2 - \frac{d^2}{4}}$.

(The quantity $\sqrt{r^2 - \frac{d^2}{4}}$ is a positive real number since $2r > d$.) Set $\boldsymbol{z} = \boldsymbol{w} + \frac{1}{2}\boldsymbol{x} + \frac{1}{2}\boldsymbol{y}$. Then

$$\begin{aligned}
|\boldsymbol{z} - \boldsymbol{x}|^2 &= \left|\boldsymbol{w} - \left(\tfrac{1}{2}\boldsymbol{x} - \tfrac{1}{2}\boldsymbol{y}\right)\right|^2 \\
&= \tfrac{1}{4}|2\boldsymbol{w} - (\boldsymbol{x} - \boldsymbol{y})|^2 \\
&= \tfrac{1}{4}(2\boldsymbol{w} - (\boldsymbol{x} - \boldsymbol{y})) \cdot (2\boldsymbol{w} - (\boldsymbol{x} - \boldsymbol{y})) \\
&= \boldsymbol{w} \cdot \boldsymbol{w} - \boldsymbol{w} \cdot (\boldsymbol{x} - \boldsymbol{y}) + \tfrac{1}{4}(\boldsymbol{x} - \boldsymbol{y}) \cdot (\boldsymbol{x} - \boldsymbol{y}) \\
&= |\boldsymbol{w}|^2 + \tfrac{1}{4}|\boldsymbol{x} - \boldsymbol{y}|^2 \\
&= r^2,
\end{aligned}$$

so that $|\boldsymbol{z}-\boldsymbol{x}| = r$. Similarly, one sees that $|\boldsymbol{z}-\boldsymbol{y}| = r$. In fact, all solutions are obtained in this way. That is, if $\boldsymbol{z} \in \mathbb{R}^k$ is such that $|\boldsymbol{z}-\boldsymbol{x}| = |\boldsymbol{z}-\boldsymbol{y}| = r$, then $\boldsymbol{w} = \boldsymbol{z} - \frac{1}{2}\boldsymbol{x} - \frac{1}{2}\boldsymbol{y}$ satisfies conditions (1) and (2). Indeed,

$$\begin{aligned}(\boldsymbol{z} - \tfrac{1}{2}\boldsymbol{x} - \tfrac{1}{2}\boldsymbol{y}) \cdot (\boldsymbol{x}-\boldsymbol{y}) &= \tfrac{1}{2}(\boldsymbol{z}-\boldsymbol{y}+\boldsymbol{z}-\boldsymbol{x}) \cdot (\boldsymbol{z}-\boldsymbol{y}-(\boldsymbol{z}-\boldsymbol{x})) \\ &= \tfrac{1}{2}\left(|\boldsymbol{z}-\boldsymbol{y}|^2 - |\boldsymbol{z}-\boldsymbol{x}|^2\right) \\ &= 0,\end{aligned}$$

whence $\boldsymbol{w}$ satisfies condition (1), i.e. $\boldsymbol{w}$ is orthogonal to $\boldsymbol{x}-\boldsymbol{y}$. Then $\boldsymbol{w}$ is also orthogonal to $\frac{1}{2}\boldsymbol{x} - \frac{1}{2}\boldsymbol{y}$, which has length $\frac{d}{2}$. An application of the Pythagorean theorem now shows that $\boldsymbol{w}$ satisfies condition (2). Given that $\boldsymbol{w} \mapsto \boldsymbol{w} + \frac{1}{2}\boldsymbol{x} + \frac{1}{2}\boldsymbol{y}$ is a bijection of $\mathbb{R}^k$, we have now classified all solutions to the given problem; note that this classification did not depend on k.

Focus now on the case $k \geq 3$. To show that there are infinitely many such $\boldsymbol{z}$, it will suffice to show that there are infinitely many $\boldsymbol{w} \in \mathbb{R}^k$ satisfying conditions (1) and (2). Since $|\boldsymbol{x}-\boldsymbol{y}| \neq 0$, $\boldsymbol{x}-\boldsymbol{y}$ is not the zero vector and so has at least one non-zero component, say $x_1 - y_1 \neq 0$ (a similar discussion holds for other non-zero components). As shown in the solution to Exercise 18, if we choose any real numbers, not all zero, for the components $u_2, \ldots, u_k$ of a vector $\boldsymbol{u}$, then setting

$$u_1 = \frac{-(u_2(x_2-y_2) + \cdots + u_k(x_k-y_k))}{x_1-y_1}$$

will yield a non-zero $\boldsymbol{u}$ satisfying condition (1). Any scalar multiple of $\boldsymbol{u}$ will also satisfy condition (1), so taking

$$\boldsymbol{w} = \frac{\sqrt{r^2 - \frac{d^2}{4}}}{|\boldsymbol{u}|}\boldsymbol{u}$$

gives us a non-zero $\boldsymbol{w}$ satisfying conditions (1) and (2). There are infinitely many choices for the components $u_2, \ldots, u_k$, yielding infinitely many distinct vectors $\boldsymbol{u}$. However, not all of these choices give us distinct vectors $\boldsymbol{w}$ (some of the choices for $\boldsymbol{u}$ give us vectors lying on the same line). To surmount this, suppose we have chosen $u_3, \ldots, u_k$ such that $u_3 \neq 0$ (note that this requires $k \geq 3$). Then observe that the ratio $\frac{u_2}{u_3} = \frac{w_2}{w_3}$, since $\boldsymbol{w}$ is a scalar multiple of $\boldsymbol{u}$. There are infinitely many choices of u_2 yielding a distinct ratio; it follows that each choice yields a distinct $\boldsymbol{w}$.

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

Solution. It is quickly verified that $\boldsymbol{z} = \frac{1}{2}\boldsymbol{x} + \frac{1}{2}\boldsymbol{y}$ has the desired properties. To see that this is the only solution, note that $2r = d$ implies equality in the triangle inequality:

$$|\boldsymbol{x}-\boldsymbol{y}| = |\boldsymbol{x}-\boldsymbol{z}| + |\boldsymbol{z}-\boldsymbol{y}|.$$

By studying the proof of the triangle inequality on page 17 of [PMA], one sees that equality occurs precisely when one has equality in the Schwarz inequality. By Exercise 15, this is the case exactly when $\boldsymbol{x} - \boldsymbol{z}$ and $\boldsymbol{z} - \boldsymbol{y}$ are linearly dependent, say $\boldsymbol{x} - \boldsymbol{z} = \lambda(\boldsymbol{z} - \boldsymbol{y})$. Taking absolute values and using that $r > 0$, it follows that $\lambda = \pm 1$. $\lambda = -1$ gives $\boldsymbol{x} = \boldsymbol{y}$, which is not the case since $|\boldsymbol{x} - \boldsymbol{y}| = d > 0$, so it must be that $\lambda = 1$, which in turn gives $\boldsymbol{z} = \frac{1}{2}\boldsymbol{x} + \frac{1}{2}\boldsymbol{y}$.

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

Solution. The existence of such a $\boldsymbol{z}$ would violate the triangle inequality

$$|\boldsymbol{x} - \boldsymbol{y}| \leq |\boldsymbol{x} - \boldsymbol{z}| + |\boldsymbol{z} - \boldsymbol{y}|,$$

which in this case says $d \leq 2r$.

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

Solution. The statements in **(b)** and **(c)** need no modification; the solutions there do not depend on k. We shall modify part **(a)** as follows.

$k = 2$. If $2r > d$, there are exactly two $\boldsymbol{z} \in \mathbb{R}^2$ such that

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

By the discussion in part **(a)**, it will suffice to show that there are exactly two $\boldsymbol{w} = (w_1, w_2) \in \mathbb{R}^2$ such that

(1) $\boldsymbol{w} \cdot (\boldsymbol{x} - \boldsymbol{y}) = 0$;

(2) $|\boldsymbol{w}| = \sqrt{r^2 - \frac{d^2}{4}}$.

Let us assume once again that $x_1 - y_1 \neq 0$, and for convenience let $D = \sqrt{r^2 - \frac{d^2}{4}}$. For any given w_2, it is necessary to set

$$w_1 = \frac{-w_2(x_2 - y_2)}{x_1 - y_1}$$

in order to satisfy condition (1). Substituting this expression for w_1 into condition (2) then constrains w_2:

$$\begin{aligned} &\frac{w_2^2(x_2-y_2)^2}{(x_1-y_1)^2}+w_2^2=D^2 \\ \iff & w_2^2\left(\frac{(x_2-y_2)^2}{(x_1-y_1)^2}+1\right)=D^2 \\ \iff & w_2^2\left(\frac{d^2}{(x_1-y_1)^2}\right)=D^2 \\ \iff & w_2=\frac{\pm D(x_1-y_1)}{d}. \end{aligned}$$

This gives us exactly two values for w_2, and hence for $\boldsymbol{w}$, since $D(x_1-y_1)\neq 0$.

$k=1$. If $2r>d$, there are no $z\in\mathbb{R}$ such that

$$|z-x|=|z-y|=r.$$

In this case, one is forced to take $w=0$ to satisfy condition (1); but then condition (2) cannot possibly be satisfied.

17. Prove that

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

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

Solution. This is a quick computation:

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

Geometrically, this result says that the sum of the squares of the lengths of the two diagonals of a parallelogram is equal to twice the sum of the squares of the lengths of the two sides; see here.

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

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

if and only if $|\boldsymbol{x}-\boldsymbol{c}|=r$.

(*Solution:* $3\boldsymbol{c} = 4\boldsymbol{b} - \boldsymbol{a}, 3r = 2|\boldsymbol{b} - \boldsymbol{a}|$.)

Solution. Rudin gives us the solution; to derive it ourselves we perform the following computation:

$$
\begin{aligned}
|\boldsymbol{x} - \boldsymbol{a}| = 2|\boldsymbol{x} - \boldsymbol{b}| &\iff \left[\sum_{j=1}^{k}(x_j - a_j)^2\right]^{1/2} = 2\left[\sum_{j=1}^{k}(x_j - b_j)^2\right]^{1/2} \\
&\iff \sum_{j=1}^{k}(x_j - a_j)^2 = 4\sum_{j=1}^{k}(x_j - b_j)^2 \\
&\iff \sum_{j=1}^{k} x_j^2 - 2x_ja_j + a_j^2 = \sum_{j=1}^{k} 4x_j^2 - 8x_jb_j + 4b_j^2 \\
&\iff \sum_{j=1}^{k} 3x_j^2 - (8b_j - 2a_j)x_j = \sum_{j=1}^{k} a_j^2 - 4b_j^2 \\
&\iff \sum_{j=1}^{k} x_j^2 - \tfrac{1}{3}(8b_j - 2a_j)x_j = \frac{1}{3}\sum_{j=1}^{k} a_j^2 - 4b_j^2 \\
\text{(complete the square)} &\iff \sum_{j=1}^{k}(x_j - \tfrac{1}{3}(4b_j - a_j))^2 - \tfrac{1}{9}(a_j - 4b_j)^2 = \frac{1}{9}\sum_{j=1}^{k} 3a_j^2 - 12b_j^2 \\
&\iff \sum_{j=1}^{k}(x_j - \tfrac{1}{3}(4b_j - a_j))^2 = \frac{1}{9}\sum_{j=1}^{k} 3a_j^2 - 12b_j^2 + (a_j - 4b_j)^2 \\
&\iff \sum_{j=1}^{k}(x_j - \tfrac{1}{3}(4b_j - a_j))^2 = \frac{1}{9}\sum_{j=1}^{k} 4a_j^2 - 8a_jb_j + 4b_j^2 \\
&\iff \sum_{j=1}^{k}(x_j - \tfrac{1}{3}(4b_j - a_j))^2 = \frac{4}{9}\sum_{j=1}^{k}(a_j - b_j)^2 \\
&\iff \left[\sum_{j=1}^{k}(x_j - \tfrac{1}{3}(4b_j - a_j))^2\right]^{1/2} = \frac{2}{3}\left[\sum_{j=1}^{k}(a_j - b_j)^2\right]^{1/2} \\
&\iff \left|\boldsymbol{x} - \tfrac{1}{3}(4\boldsymbol{b} - \boldsymbol{a})\right| = \tfrac{2}{3}|\boldsymbol{b} - \boldsymbol{a}|.
\end{aligned}
$$

This exercise concerns the circles of Apollonius; see here. It demonstrates that one may specify a sphere either by giving a centre and a radius (here, $\boldsymbol{c}$ and r), or by giving two distinct points (here, $\boldsymbol{a}$ and $\boldsymbol{b}$; Rudin should really specify $\boldsymbol{a} \neq \boldsymbol{b}$), known as the foci, and a ratio for the distances of a point on the sphere to the two foci (here, 2).

20. With reference to the Appendix, suppose that property (III) were omitted from the definition of a 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.

Solution. (I will instead make reference to my own write-up of the Appendix, where I have relabeled property (III) as property (IV).) Let us call this resulting ordered set $\tilde{\mathbb{R}}$. By examining the linked document, we see that property (IV) is not used at all when defining the order on $\mathbb{R}$, and is only used in the section on the least-upper-bound property to show that the proposed supremum has property (IV); so we lose nothing here by omitting property (IV). The same is true for axioms (A1) - (A3) in the section on addition, however we must modify axiom (A4) for $\tilde{\mathbb{R}}$ as follows.

(A4) There exists an element $0 \in \tilde{\mathbb{R}}$ such that $A + 0 = A$ (**additive identity**). We shall use a slightly different zero element; $0^* = \{p \in \mathbb{Q} : p \leq 0\}$. It is clear that 0^* satisfies properties (I) - (III). We claim that 0^* is the additive identity in $\tilde{\mathbb{R}}$. For the inclusion $A + 0^* \subseteq A$, suppose $r \in A$ and $s \in 0^*$, i.e. $s \in \mathbb{Q}$ with $s \leq 0$. Then either $r + s < r$ and so property (III) implies that $r + s \in A$, or $r + s = r \in A$. For the reverse inclusion $A \subseteq A + 0^*$, simply observe that any $r \in A$ can be written as $r + 0 \in A + 0^*$. Hence $A \subseteq A + 0^*$ and we conclude that $A + 0^* = A$.

Now we will show that axiom (A5) fails, by considering the set $1^* = \{p \in \mathbb{Q} : p < 1\} \in \tilde{\mathbb{R}}$. Suppose there exists some $A \in \mathbb{R}$ such that $1^* + A = 0^*$. Since $0 \in 0^*$, we must be able to write $0 = r + s$ for some $r \in 1^*$ and $s = -r \in A$. Since $r < 1$, we have $\frac{1+r}{2} \in 1^*$. It follows that

$$\tfrac{1+r}{2} - r = \tfrac{1-r}{2} \in 1^* + A \implies \tfrac{1-r}{2} \in 0^* \implies \tfrac{1-r}{2} \leq 0.$$

However, this is a contradiction:

$$r < 1 \implies 0 < \tfrac{1-r}{2}.$$

[PMA] Rudin, W. (1976) *Principles of Mathematical Analysis.* 3rd edn.