Summer Programme 2021

Solutions to exercises from Walter Rudin's *Principles of Mathematical Analysis*

Satvik Saha
19MS154

Indian Institute of Science Education and Research, Kolkata,
Mohanpur, West Bengal, 741246, India.

Chapter 1

The Real and Complex Number Systems

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

Solution. Use the fact that the field of rationals is closed under additiona and multiplication, as well as the existence of the additive inverse $-r$ and the multiplicative inverse $1/r$. If $r + x$ and rx were rational, then both

$$(-r) + r + x = x, \qquad (1/r)rx = x$$

must also be rational. These are contradictions.

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

Solution. Suppose that $x \in \mathbb{Q}$, $x^2 = 12$, and $x = p/q$ where $q \neq 0$ and p and q are coprime integers. This would imply that

$$p^2 = 12q^2 = 3(2q)^2,$$

so 3 divides p^2, hence 3 divides p. Write $p = 3m$ for some integer m, giving

$$3(2q)^2 = p^2 = (3m)^2 = 9m^2, \qquad (2q)^2 = 3m^2.$$

This means that 3 divides $(2q)^2$, hence 3 divides $2q$, hence 3 divides q. This contradicts the fact that p and q are coprime, which means that there is no rational number whose square is 12.

Exercise 3. Prove that the axioms of multiplication in a field 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 $1/(1/x) = x$.

Solution. The axioms of multiplication guarantee the existence of an element $1/x$ such that $x(1/x) = 1$. Left multiply on both sides of $xy = xz$, use associativity and $1w = w$ for all w in the field to get

$$(1/x)xy = (1/x)xz, \qquad y = z.$$

This proves (a). Setting $z = 1$ proves (b), and setting $z = 1/x$ proves (c). Using $x(1/x) = 1$, replace x with $1/x$ in (c) to give

$$(1/x)(1/(1/x)) = 1,$$

then left multiply with x yielding

$$x(1/x)(1/(1/x)) = x, \qquad 1/(1/x) = x.$$

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

Solution. By definition, $\alpha \leq x$ for all $x \in E$ and $x \leq \beta$ for all $\in E$. Since E is non-empty, simply select some $x \in E$, whence $\alpha \leq x \leq \beta$. Thus, we either have $\alpha = x = \beta$, $\alpha = x < \beta$, $\alpha < x = \beta$, or $\alpha < x < \beta$. In the last case, transitivity gives $\alpha < \beta$. Hence, $\alpha \leq \beta$.

Exercise 5. Let A be a non-empty subset of the 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. Fix $\alpha = -\sup(-A)$. We claim that $\alpha = \inf A$, i.e. $\beta \leq \alpha \leq x$ for all lower bounds β of A and for all $x \in A$.

First, note that $-\alpha = \sup(-A)$, which means that $-\alpha \geq x$ for all $x \in -A$, whence $\alpha \leq -x$ for all $-x \in A$. However, for each $x \in A$, we have $-x \in -A$ so $\alpha \leq x$ for all $x \in A$.

Now, let β be a lower bound of A. This means that $\beta \leq x$ for all $x \in A$, so $-\beta \geq -x$ for all $x \in A$. Again, $-x \in -A$ for all $x \in A$, so $-\beta \geq x$ for all $x \in -A$. This means that β is an upper bound of $-A$, which means $-\beta \geq \sup(-A) = -\alpha$. Thus, $\beta \leq \alpha$.

This proves that $\inf A = -\sup(-A)$.

Exercise 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

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

Hence is 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.

Solution.

(a) Write r with the common denominator $s = nq$, so $r = mq/s = pn/s$. Now, note that

$$\left((b^m)^{1/n}\right)^s = (b^m)^q = b^{mq}, \qquad \left((b^p)^{1/q}\right)^s = (b^p)^n = b^{np},$$

but $mq = np = rs$. Setting $b^{rs} = x$, use Theorem 1.21 to conclude that there is a unique y such that $y^s = x = b^{rs}$. However, we have just verified two such y, hence

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

(b) Set $r = m/n$, $s = p/q$ with $n > 0$, $q > 0$. Then,

$$b^{r+s} = b^{(mq+np)/nq} = (b^{mq+np})^{1/nq} = (b^{mq} b^{np})^{1/nq}.$$

The corollary of Theorem 1.21 lets us distribute the integer root over the product, giving

$$b^{r+s} = b^{mq/nq} b^{np/nq} = b^{m/n} b^{p/q} = b^r b^s.$$

(c) First, we show that $b^n - 1 \geq n(b-1)$ for all positive integers n. This is trivially true for $n = 1$. For $n > 1$, write $b = 1 + a$ where $a > 0$. Hence the Binomial Theorem gives

$$b^n = (1+a)^n = 1 + na + \frac{1}{2}n(n-1)a^2 + \cdots + a^n > 1 + na,$$

hence

$$b^n - 1 > na = n(b-1).$$

Note that this inequality becomes strict for $n > 1$. Replacing b with $b^{1/n} > 1$, we have $b - 1 > n(b^{1/n} - 1)$ for all positive integers n.

Now, given some $t > 1$, we can choose a positive integer $n > (b-1)/(t-1)$, which implies $n(t-1) > b - 1 > n(b^{1/n} - 1)$, hence $t > b^{1/n}$.

Now, note that for all $x \in B(r)$, $x = b^t$ for some rational t. First, note that for all rational $t \leq r$, we have $b^t \leq b^r$. This is because if we write t and r with a common positive integer denominator, $t = m/q$, $r = n/q$, then $m \leq n$ so $(b^{1/q})^m \leq (b^{1/q})^n$. Thus, b^r is an upper bound for $B(r)$.

Next, we show that b^r is the least upper bound to $B(r)$. Suppose that $\alpha = \sup B(r)$, and $b^t \leq \alpha < b^r$ for all $t \leq r$. Using the previously proven inequality, find a large enough integer n such that $b^{1/n} < b^r/\alpha$. Thus, $\alpha < b^{r-1/n}$, and $r - 1/n < r$ so $b^{r-1/n} \in B(r)$, which contradicts the fact that α is the supremum of $B(r)$. Hence, b^r is the least upper bound of $B(r)$, so

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

(d) We have been given

$$b^x = \sup B(x), \qquad b^y = \sup B^y, \qquad b^{x+y} = \sup B(x+y)$$

by definition for real x and y. Choose some rational $t \leq x + y$, so $b^t \in B(x+y)$. By choosing a rational r such that $t - y < r < x$ and setting $s = t - r$, we have $t = r + s$ and $r < x$, $s < y$. Thus, $b^r \in B(x)$ and $b^s \in B(y)$, so every element $b^t \in B(x+y)$ can be written as $b^{r+s} = b^r b^s$, which is the product of an element each from $B(x)$ and $B(y)$. Conversely, given elements $b^r \in B(x)$ and $b^s \in B(y)$, we have $r \leq x$ and $s \leq y$ so $t = r + s \leq x + y$, hence $b^{r+s} = b^t \in B(x+y)$. Thus, we have

$$B(x+y) = \{wz : w \in B(x), z \in B(y)\}.$$

Thus, for any element $wz \in B(x+y)$, $w \in B(x)$, $z \in B(y)$, we have $w \leq \sup B(x) = b^x$ and $z \leq \sup B(y) = b^y$, so $wz \leq b^x b^y$. This means that $b^x b^y$ is an upper bound of $B(x+y)$.

Now suppose that $\alpha = \sup B(x+y)$ such that $wz \leq \alpha < b^x b^y$ for all $wz \in B(x+y)$, where $w \in B(x)$ and $z \in B(y)$. Then, $\alpha/b^x < b^y$, so choose β such that $\alpha/b^x < \beta < b^y$. In other words, $\alpha/\beta < b^x$ and $\beta < b^y$, so we can choose rational $r < x$, $s < y$ such that $\alpha/\beta \leq b^r \in B(x)$ and $\beta \leq b^s \in B(y)$. Note that $r \neq x$ and $s \neq y$. Thus, the product $(\alpha/\beta)\beta = \alpha \leq b^r b^s \in B(x+y)$. However, recall that we chose α such that $b^r b^s \leq \alpha$ for all $b^r \in B(x)$, $b^s \in B(y)$, so we must have $\alpha = b^r b^s$ for our choice of r and s. Now, we can choose rational r' and s' such that $r < r' < x$ and $s < s' < y$, hence $b^r < b^{r'} \in B(x)$ and $b^s < b^{s'} \in B(y)$. This gives $\alpha = b^r b^s < b^{r'} b^{s'} \in B(x+y)$, which contradicts the fact that α is an upper bound. Thus, $b^x b^y$ must be the least upper bound of $B(x+y)$, so

$$b^{x+y} = b^x b^y.$$

Exercise 7. Fix $b > 1$, $y > 0$, and show the following.

(a) For any positive integer n, $b^n - 1 \geq n(b-1)$.

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

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

(d) If w is such that $b^w < y$, then $b^{w+1/n} < y$ for sufficiently large n.

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

Solution.

(a) See Exercise 1 (c).

(b) See Exercise 1 (c).

(c) See Exercise 1 (c).

(d) Set $t = yb^{-w} > 1$, and using the previous inequality, choose sufficiently large n such that $b^{1/n} < t = yb^{-w}$. Thus,
$$b^{w+1/n} < y.$$

(e) Set $t = (1/y)b^w > 1$, and using the inequality in (c), choose sufficiently large n such that $b^{1/n} < t = (1/y)b^w$. Thus,
$$y < b^{w-1/n}.$$

(f) Exactly one of the following must be true; $b^x < y$, $b^x = y$, $b^x > y$. If $b^x < y$, then $x \in A$ by definition. Using (d), we can find sufficiently large n such that
$$b^{x+1/n} < y,$$
hence $x < x + 1/n \in A$, contradicting the fact that x is an upper bound of A. If $b^x > y$, then using (e), we can find sufficiently large n such that
$$y < b^{x-1/n},$$
which means that $x - 1/n$ is also an upper bound of A, contradicting the fact that x is the lowest upper bound of A. This leaves us with $b^x = y$.

(g) Suppose that $x \neq x'$, and without loss of generality $x < x'$. Set $x' - x = h > 0$, and note that $b^{x'} = b^{x+h} = b^x b^h$. Now, $b > 1$ and $h > 0$, so $b^h > 1$. Thus, $b^{x'} > b^x$, which means that $b^{x'} \neq b^x$ for $x' \neq x$. Thus, if $b^x = y$, then x is unique.

Exercise 8. Prove that no order can be defined in the complex field that turns it into an ordered field.

Solution. In an ordered field, if $x > 0$, then we must have $-x < 0$, and vice versa by Proposition 1.18. The same proposition gives that if $x \neq 0$, then $x^2 > 0$. This forces $i^2 = -1 > 0$. Applying the same proposition again, this forces $(-1)^2 = 1 > 0$, which is a contradiction because we cannot have both $-1 > 0$ and $1 > 0$.

Exercise 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. Does this ordered set have the least-upper-bound property?

Solution. First, we show that for arbitrary $z = a+bi$ and $w = c+di$, exactly one of the following is true: $z < w$, $z = w$, $z > w$. To do this, note that the real numbers are ordered, so either $a < c$, $a = c$, or $a > c$. In the case $a < c$, we have $z < w$ and since $a \neq c$, $z \neq w$. Also, this excludes $w < z$. In the case $a > c$, the roles of z and w are interchanged, so $z > w$. In the case $a = c$, we note that either $b < d$, $b = d$, or $b > d$; when $b < d$, $z < w$ and when $b > d$, $z > w$. Finally, when $a = c$ and $b = d$, we have $z = w$.

Next, we show that transitivity holds, i.e. if $z < w$ and $w < x$, then $z < x$. Write $z = a+bi$, $w = c+di$ and $x = e+fi$. Note that the conditions $z < w$ and $w < x$ imply $a \leq c$ and $c \leq e$. This has to be further split into four cases.

Case 1 If $a < c$ and $c < e$, then $a < e$ so $z < x$.

Case 2 If $a = c$ and $c < e$, then $a < e$ again so $z < x$.

Case 3 If $a < c$ and $c = e$, then $a < e$ again so $z < x$.

Case 4 If $a = c$ and $c = e$, then we must have had $b < d$ and $d < f$, so $a = e$ and $b < f$ gives $z < x$.

No, this ordered set does not have the least upper bound property. Consider the set of complex numbers $S = \{a + bi : 0 < a < 1, b = 0\}$. If $w = c + di$ is to be an upper bound of S, i.e. $z \leq w$ for all $z \in S$, then either $z = w$ for some $z \in S$ or $z < w$ for all $z \in S$. The former implies that $w = a+0i$ for some $0 < a < 1$, in which case we have $w = a+0i < (a+1)/2+0i \in S$, a contradiction. The latter implies that $a \leq c$ for all $0 < a < 1$, which forces $1 \leq c$. If $w = c+di$ is the least upper bound of S with $1 < c$, then note that $(1 + c)/2 + di < c + di = w$ is smaller upper bound of S. Otherwise, if $w = 1 + di$ is the least upper bound of S, then $1 + (d - 1)i < 1 + di = w$ is a smaller upper bound. This means that the set S have no least upper bound.

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

Solution. Write

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

Now,

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

and

$$\begin{aligned} 2ab &= 2\left(\frac{|w| + u}{2}\right)^{1/2}\left(\frac{|w| - u}{2}\right)^{1/2} \\ &= 2\left(\frac{(|w| + u)(|w| - u)}{4}\right)^{1/2} \\ &= 2\left(\frac{|w|^2 - u^2}{4}\right)^{1/2} \\ &= 2\left(\left(\frac{v}{2}\right)^2\right)^{1/2}. \end{aligned}$$

Recall that $(x^2)^{1/2} = x$ if $x \geq 0$ and $(x^2)^{1/2} = -x$ if $x \leq 0$. Thus, when $v \geq 0$, we have $2ab = v$ and when $v \leq 0$, we have $2ab = -v$. This means that $w = u + 2abi = z^2$ when $v \geq 0$ and $w = u - 2abi = (\overline{z})^2$ when $v \leq 0$.

Note that when $w = 0$, it has only one square root, namely 0. Otherwise, every non-zero complex number $w = u + iv$ has two square roots, either $z, -z$ or $\overline{z}, -\overline{z}$ depending on the sign of v.

Exercise 11. If z is a complex number, prove that there exists an $r \geq 0$, a complex number w with $|w| = 1$ such that $z = rw$. Are w and r always uniquely determined by z?

Solution. Write $z = a + bi$, and if $z \neq 0$ define

$$r = \sqrt{a^2 + b^2}, \qquad w = z/r = \frac{a}{\sqrt{a^2 + b^2}} + \frac{bi}{\sqrt{a^2 + b^2}}.$$

If $z = 0$, simply take $r = 0$ and $w = 1$. Thus, $z = rw$.

When $z \neq 0$, this choice is unique, since $z = rw$ forces $|z| = |rw| = |r||w| = r$, hence $r = |z| = \sqrt{a^2 + b^2}$ and $w = z/r$. Otherwise for $z = 0$, we can choose any w (say $w = \pm 1$) as long as $r = 0$.

Exercise 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. We prove this by induction. The case $n = 1$ is trivially true. For $n = 2$, see Theorem 1.33. If this holds for some $n \geq 1$, then use the $n = 2$ case on $z_1 + \cdots + z_n$ and z_{n+1}, then the induction hypothesis to get

$$|z_1 + \cdots + z_n + z_{n+1}| \leq |z_1 + \cdots + z_n| + |z_{n+1}| \leq |z_1| + \cdots + |z_n| + |z_{n+1}|.$$

This proves the desired statement by induction.

Exercise 13. If x and y are complex, prove that

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

Solution. Use the triangle inequality to write

$$|x| = |x - y + y| \leq |x - y| + |y|, \qquad |y| = |y - x + x| \leq |x - y| + |x|.$$

Thus, if $|x| > |y|$, then $||x| - |y|| = |x| - |y| \leq |x - y|$ by the first inequality. If $|x| < |y|$, then $||x| - |y|| = |y| - |x| \leq |x - y|$ by the second inequality. If $|x| = |y|$, then $||x| - |y|| = 0$, so the inequality holds trivially.

Exercise 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. Write $z = a+bi$, so $a^2+b^2 = 1$. Now, $|1+z|^2 = (a+1)^2+b^2$, and $|1-z|^2 = (a-1)^2+b^2$. Adding,

$$|1 + z|^2 + |1 - z|^2 = 2(a^2 + b^2 + 1) + 2a - 2a = 4.$$

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

Solution. In Theorem 1.35, recall that

$$A = \sum |a_i|^2, \qquad B = \sum |b_i|^2, \quad C = \sum a_i \overline{b_i},$$

and the desired inequality was $AB \geq C^2$. If $B = 0$, then all $b_i = 0$ so equality holds. Otherwise, we concluded that with $B > 0$,

$$\sum |Ba_i - Cb_i|^2 = B(AB - |C|^2) \geq 0.$$

Here, equality means $AB = |C|^2$, so every $|Ba_i - Cb_i| = 0$, hence $a_i = (C/B)b_i$ for all i.

Exercise 16. Suppose $k \geq 3$, $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^k$, $|\boldsymbol{x} - \boldsymbol{y}| = d > 0$ and $r > 0$. Prove the following.

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

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

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

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

Solution. Note that by translating all the variables $\boldsymbol{x}' = \boldsymbol{x} - \boldsymbol{y}$, $\boldsymbol{y}' = \boldsymbol{0}$, our system of equations looks identical, with $|\boldsymbol{x}' - \boldsymbol{y}'| = d$ and the solutions are related by $\boldsymbol{z}' = \boldsymbol{z} - \boldsymbol{y}$. Thus, we may instead consider the system $|\boldsymbol{x}| = d$,

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

Consider an arbitrary solution $\boldsymbol{z}$ and write $\boldsymbol{v} = \boldsymbol{z} - \frac{1}{2}\boldsymbol{x}$. Now,

$$|\boldsymbol{z}|^2 = (\frac{1}{2}\boldsymbol{x} + \boldsymbol{v}) \cdot (\frac{1}{2}\boldsymbol{x} + \boldsymbol{v}) = \frac{1}{4}|\boldsymbol{x}|^2 + |\boldsymbol{v}|^2 + \boldsymbol{x} \cdot \boldsymbol{v}.$$

Also,

$$|\boldsymbol{z} - \boldsymbol{x}|^2 = (-\frac{1}{2}\boldsymbol{x} + \boldsymbol{v}) \cdot (-\frac{1}{2}\boldsymbol{x} + \boldsymbol{v}) = \frac{1}{4}|\boldsymbol{x}|^2 + |\boldsymbol{v}|^2 - \boldsymbol{x} \cdot \boldsymbol{v}.$$

Adding the above equations gives

$$|\boldsymbol{z}|^2 + |\boldsymbol{z} - \boldsymbol{x}|^2 = \frac{1}{2}|\boldsymbol{x}|^2 + 2|\boldsymbol{v}|^2, \qquad |\boldsymbol{v}|^2 = r^2 - \frac{d^2}{4}.$$

Subtracting the two equations gives $\boldsymbol{v} \cdot \boldsymbol{x} = 0$.

These conditions on $\boldsymbol{v}$ are necessary and sufficient to generate solutions $\boldsymbol{z} = \frac{1}{2}\boldsymbol{x} + \boldsymbol{v}$.

(a) Pick a unit vector $\hat{\boldsymbol{v}}$ perpendicular to $\boldsymbol{x}$, i.e. $\hat{\boldsymbol{v}} \cdot \boldsymbol{x} = 0$. Note that the components satisfy

$$v_1 x_1 + \cdots + v_k x_k = 0.$$

Since $d > 0$, we have $\boldsymbol{x} \neq \boldsymbol{0}$, so without loss of generality let $x_1 \neq 0$. Then we have

$$v_1 = -\frac{1}{x_1}(v_2 x_2 + \cdots + v_k x_k).$$

Therefore, we may choose the components $v_2, \ldots, v_k$ arbitrarily. For example, fix $v_2 = 1$, vary $v_3 = 0, 1, 2, \ldots$ and vary the remaining components arbitrarily, then normalize. All of the generated unit vectors are distinct, because the ratio of components v_2 and v_3 is different in each case. Thus, we have generated infinitely many unit vectors $\hat{\boldsymbol{v}}$ this way.

Now define the real number $v \geq 0$, $v^2 = r^2 - d^2/4$. Then, all the vectors $\boldsymbol{z} = \frac{1}{2}\boldsymbol{x} + \boldsymbol{v}$ are solutions, where $\boldsymbol{v} = v\hat{\boldsymbol{v}}$.

(b) We have $|\boldsymbol{x}| = d = 2r$, which means

$$|\boldsymbol{v}|^2 = r^2 - \frac{1}{4}(2r)^2 = 0,$$

forcing $|\boldsymbol{v}| = 0$, $\boldsymbol{v} = \mathbf{0}$. Thus, there is only one solution, namely $\boldsymbol{z} = \frac{1}{2}\boldsymbol{x}$.

(c) When $2r < d$

$$|\boldsymbol{v}|^2 = r^2 - \frac{d^2}{4} < 0,$$

which is impossible. Thus, there are no solutions $\boldsymbol{z}$ of this system.

Note that when $k = 2$, we can only generate 2 unit vectors $\hat{\boldsymbol{v}}$ such that $\hat{\boldsymbol{v}} \cdot \boldsymbol{x} = 0$. This is because we want

$$v_1x_1 + v_2x_2 = 0, \qquad v_1 = -\frac{v_2x_2}{x_1}, \qquad v_1^2 = 1 - v_2^2.$$

Thus, there are only two solutions, when $2r > d$. When $k = 1$, the condition $vx = 0$ with $x \neq 0$ forces $v = 0$, yet we require $v^2 = r^2 - d^2/4 > 0$ when $2r > d$, so there are no solutions.

The remaining parts (b) and (c) remain identical for $k = 1, 2$.

Exercise 17. Prove that

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

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

Solution. Calculate

$$|\boldsymbol{x} + \boldsymbol{y}|^2 = (\boldsymbol{x} + \boldsymbol{y}) \cdot (\boldsymbol{x} + \boldsymbol{y}) = |\boldsymbol{x}|^2 + |\boldsymbol{y}|^2 + 2\boldsymbol{x} \cdot \boldsymbol{y},$$

$$|\boldsymbol{x} - \boldsymbol{y}|^2 = (\boldsymbol{x} - \boldsymbol{y}) \cdot (\boldsymbol{x} - \boldsymbol{y}) = |\boldsymbol{x}|^2 + |\boldsymbol{y}|^2 - 2\boldsymbol{x} \cdot \boldsymbol{y}.$$

Adding the two gives the desired equation.

If we interpret $\boldsymbol{x}$ and $\boldsymbol{y}$ to be two adjacent legs of a parallelogram, then $\boldsymbol{x} + \boldsymbol{y}$ and $\boldsymbol{x} - \boldsymbol{y}$ represent its diagonals. Thus, the sum of squares of the diagonals of a parallelogram is equal to twice the sum of squares of two adjacent sides.

Exercise 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 $k = 1$?

Solution. If $\boldsymbol{x} = \mathbf{0}$, then any non-zero vector in $\boldsymbol{y} \in \mathbb{R}^k$ satisfies $\boldsymbol{x} \cdot \boldsymbol{y} = 0$. Otherwise, $\boldsymbol{x} = (x_1, x_2, \ldots, x_k) \neq \mathbf{0}$ so without loss of generality let the component $x_1 \neq 0$. Set

$$\boldsymbol{y} = (-x_2, x_1, 0, \ldots, 0) \in \mathbb{R}^k,$$

so

$$\boldsymbol{x} \cdot \boldsymbol{y} = x_1(-x_2) + x_2(x_1) + 0 + \cdots + 0 = 0.$$

This is clearly not possible in $\mathbb{R}$ unless $x = 0$, because the product of any two non-zero real numbers is also non-zero.

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

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

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

Solution. Write $\boldsymbol{x'} = \boldsymbol{x} - \boldsymbol{a}$, $\boldsymbol{b'} = \boldsymbol{b} - \boldsymbol{a}$, $\boldsymbol{c'} = \boldsymbol{c} - \boldsymbol{a}$, so we want to find $\boldsymbol{c'}$ such that

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

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

Write $\boldsymbol{x'} = \frac{4}{3}\boldsymbol{b'} + \boldsymbol{r}$. Then

$$|\boldsymbol{x'}|^2 = \frac{16}{9}|\boldsymbol{b'}|^2 + |\boldsymbol{r}|^2 + \frac{8}{3}\boldsymbol{b'} \cdot \boldsymbol{r},$$

and

$$|\boldsymbol{x'} - \boldsymbol{b'}|^2 = |\frac{1}{3}\boldsymbol{b'} + \boldsymbol{r}|^2 = \frac{1}{9}|\boldsymbol{b'}|^2 + |\boldsymbol{r}|^2 + \frac{2}{3}\boldsymbol{b'} \cdot \boldsymbol{r}.$$

Using $|\boldsymbol{x'}|^2 = 4|\boldsymbol{x'} - \boldsymbol{b'}|^2$, we have

$$\frac{12}{9}|\boldsymbol{b'}|^2 = 3|\boldsymbol{r}|^2, \qquad |\boldsymbol{r}| = \frac{2}{3}|\boldsymbol{b'}|.$$

Thus, $|\boldsymbol{x'} - \frac{4}{3}\boldsymbol{b'}| = \frac{2}{3}|\boldsymbol{b'}|$, which is both necessary and sufficient. This means that $\boldsymbol{c'} = \frac{4}{3}\boldsymbol{b'}$ and $r = \frac{2}{3}|\boldsymbol{b'}|$. Translating everything back by $\boldsymbol{a}$, we have

$$\boldsymbol{c} = \frac{4}{3}\boldsymbol{b} - \frac{1}{3}\boldsymbol{a}, \qquad r = \frac{2}{3}|\boldsymbol{b} - \boldsymbol{a}|.$$

Exercise 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. We define a cut as any set $\alpha \subset \mathbb{Q}$ with the following properties.

(I) α is not empty, $\alpha \neq \mathbb{Q}$.

(II) If $p \in \alpha$, $q \in \mathbb{Q}$, and $q < p$, then $q \in \alpha$.

Property (III) used to state that if $p \in \alpha$, then $p < r$ for some $r \in \alpha$, which meant that α had no maximal element. Property (II) implies that if $p \in \alpha$ and $q \notin \alpha$, then $p < q$ (take the contrapositive, and note that $p \neq q$). It also implies that if $r \notin \alpha$ and $r < s$, then $s \notin \alpha$ ($s \in \alpha$ would have forced $r \in \alpha$).

Call the set of all these cuts $\mathbb{R}'$. Like before, the order $\alpha < \beta$ is defined to mean $\alpha \subset \beta$, for $\alpha, \beta \in \mathbb{R}'$. Again, $\mathbb{R}'$ has the least upper bound property.

To see this, let A be any non-empty subset of $\mathbb{R}'$ bounded above by $\beta \in \mathbb{R}'$, and let γ be the union of all $\alpha \in A$. Thus, $p \in \gamma$ if and only if $p \in \alpha$ for some $\alpha \in A$. To verify that γ is indeed a cut, note that A is non-empty so there is at least one element $\alpha_0 \in A$ which is non-empty, so $\alpha_0 \subset \gamma$ with γ non-empty. Also, $\gamma \subset \beta$ since β being an upper bound means that $\alpha < \beta$ for all $\alpha \in A$, which in turn means $\alpha \subset \beta$ for all $\alpha \in A$, hence $\gamma = \cup_{\alpha \in A} \alpha \subset \beta$. This verifies property (I). To verify property (II), pick $p \in \gamma$, and suppose that $p \in \alpha_1$ for some $\alpha \in A$. If $q \in \mathbb{Q}$ with $q < p$, this gives $q \in \alpha_1$, hence $q \in \gamma$. Thus, γ is indeed a cut, i.e. $\gamma \in \mathbb{R}'$.

Now, we claim that $\gamma = \sup A$. Clearly, for any $\alpha \in A$, we have $\alpha \subset \gamma$ by definition to $\alpha \leq \gamma$ for all $\alpha \in A$, meaning γ is an upper bound of A. Now suppose that $\delta \in \mathbb{R}'$, and $\delta < \gamma$. This means that δ is a proper subset of γ, so there is some $p \in \gamma$ such that $\notin \delta$. However, we must have $p \in \alpha_1$ for some $\alpha_1 \in A$, so α cannot be a proper subset of δ, meaning that δ is not an upper bound of A. Thus, γ is the least upper bound of A.

Like before, for $\alpha, \beta \in \mathbb{R}'$, define addition $\alpha + \beta$ as the set of sums $r + s$ with $r \in \alpha$, $s \in \beta$. We must now verify the axioms of addition.

(A1) We demand closure, which is easily seen because $\alpha + \beta$ is a non-empty proper subset of $\mathbb{Q}$, and if $p \in \alpha + \beta$, then we must be able to write $p = r + s$ for some $r \in \alpha$, $s \in \beta$. Now if $q \in \mathbb{Q}$ and $q < p$, then $q - s < p - s = r$, so $q - s \in \alpha$, hence $q = (q - s) + s \in \alpha + \beta$.

(A2) We demand commutativity, which follows trivially. $\alpha + \beta = \beta + \alpha$, both being the set of $r + s = s + r$ with $r \in \alpha$, $s \in \beta$.

(A3) We demand associativity, which follows again from the associativity of the rational numbers. Note that if $\alpha, \beta, \gamma \in \mathbb{R}'$, with $r \in \alpha$, $s \in \beta$, $t \in \gamma$, then $r + (s + t) = (r + s) + t$.

(A4) Here, select $0' = \{r \in \mathbb{Q} : r \leq 0\}$. To show that for any $\alpha \in \mathbb{R}'$, $0' + \alpha = \alpha$, note that $0' + \alpha$ is the set of all rational numbers $r + s$ with $r \leq 0$ and $s \in \alpha$, so $r + s \leq s \in \alpha$ hence $0' + \alpha \subseteq \alpha$. Now, if $s \in \alpha$, then $0 + s \in 0' + \alpha$ since $0 \in 0'$ and $s \in \alpha$, so $\alpha \subseteq 0' + \alpha$. This proves $0' + \alpha = \alpha$.

(A5) We demand the existence of an additive inverse $-\alpha$ for every α, such that $\alpha + (-\alpha) = 0'$. This fails with the choice $\alpha = 0^* = \{r \in \mathbb{Q} : r < 0\}$. Note that if $0^* + (-0^*) = 0'$, we require $r + s \leq 0$ for all $r \in 0^*$, $s \in -0^*$. There must also be some $r_0 \in 0^*$, $s_0 \in -0^*$ such that $r_0 + s_0 = 0$. Since $r_0 \in 0^*$, $r_0 < 0$, so $s_0 = -r_0 > 0$. Now, note that $-s_0/2 < 0$ so $-s_0/2 \in 0^*$, but the sum $(-s_0/2) + s_0 = s_0/2 > 0$, which is a contradiction.

In addition, note that 0^* does not serve as a zero element, since $0^* + 0' = 0'$, not 0^*. Furthermore, there is no choice of a zero element, say α_0, which makes (A1-4) hold as well as (A5), since our choice of the zero element $0'$ is forced (we have already shown that $0' + \alpha_0 = \alpha_0$, not $0'$ if $\alpha_0 \neq 0'$; the field axioms imply that the zero element once found is unique).