HOMEWORK 1

The Real Numbers

MATH S4061 | Introduction to Modern Analysis I

Rudin Ch. 1–2, Induction, an Equivalence Relation, an Ordered-Field Obstruction

Problems in This Set

Problem A1 Rudin Ch. 1, Ex. 1 — A Rational Plus an Irrational

Problem A2 Rudin Ch. 1, Ex. 2 — No Rational Squares to 12

Problem A3 Rudin Ch. 1, Ex. 3 — Multiplicative Cancellation Laws

Problem A4 Rudin Ch. 1, Ex. 4 — A Lower Bound Is at Most an Upper Bound

Problem A5 Rudin Ch. 1, Ex. 5 — $\inf A = -\sup(-A)$

Problem A6 Rudin Ch. 1, Ex. 6 — Real Powers from Rational Powers

Problem A7 Rudin Ch. 1, Ex. 7 — Logarithms from Completeness

Problem A8 Rudin Ch. 1, Ex. 8 — $\mathbb{C}$ Admits No Order

Problem A9 Rudin Ch. 1, Ex. 9 — Lexicographic Order on $\mathbb{C}$

Problem A10 Rudin Ch. 1, Ex. 10 — Complex Square Roots

Problem A11 Rudin Ch. 1, Ex. 11 — Polar Decomposition

Problem A12 Rudin Ch. 1, Ex. 12 — The Finite Triangle Inequality

Problem A13 Rudin Ch. 1, Ex. 13 — The Reverse Triangle Inequality

Problem A14 Rudin Ch. 1, Ex. 14 — A Unit-Circle Identity

Problem A15 Rudin Ch. 1, Ex. 15 — Equality in Schwarz

Problem A16 Rudin Ch. 1, Ex. 16 — Intersecting Two Spheres

Problem A17 Rudin Ch. 1, Ex. 17 — The Parallelogram Identity

Problem A18 Rudin Ch. 1, Ex. 18 — Orthogonal Vectors

Problem A19 Rudin Ch. 1, Ex. 19 — An Apollonius Sphere

Problem A20 Rudin Ch. 1, Ex. 20 — Cuts Without the No-Largest Condition

Problem B Induction: $3 \mid n^3 + 2n$

Problem C Induction: $2^n > n^2$ for $n > 4$

Problem D The Defining Relation of $\mathbb{Q}$ Is an Equivalence Relation

Problem E $ab = c \Rightarrow a \leq \sqrt{c}$ or $b \leq \sqrt{c}$

Problem F Rudin Ch. 2, Ex. 2 — The Algebraic Numbers Are Countable

Problem A1 *Rudin, Chapter 1, Exercise 1*

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

SOLUTION.

Recall that $\mathbb{Q}$ is a field: it is closed under subtraction and multiplication, and every nonzero rational has a rational inverse.

Suppose, toward a contradiction, that $r + x$ is rational. Since r is rational and $\mathbb{Q}$ is closed under subtraction, $x = (r + x) - r \in \mathbb{Q}$, contradicting that x is irrational. Hence $r + x$ is irrational.

Suppose instead that rx is rational. Since $r \neq 0$, its inverse r^{-1} is rational, so $x = (rx)\, r^{-1} \in \mathbb{Q}$, again a contradiction. Hence rx is irrational. The hypothesis $r \neq 0$ is used exactly once, to form r^{-1}; without it the product claim is false, since $0 \cdot x = 0$.

■

REFLECTIONS.

The word that sets the strategy is *irrational*. It is a negative property—it says a number is *not* in $\mathbb{Q}$—and a negative conclusion gives a direct proof nothing to push on, so the reflex is contradiction (0.5.5): assume the conclusion fails and manufacture a rational number that has no right to exist. The only other ingredient on offer is that r is a nonzero rational, which is exactly the raw material such a contradiction runs on, because $\mathbb{Q}$ is a field (1.3.1; the quotable "$\mathbb{Q}$ is an ordered field"): closed under the operations, with an inverse for every nonzero element.

So the plan writes itself—assume rationality and undo the rational part with a field operation:

(1) if $r + x \in \mathbb{Q}$, then $x = (r + x) - r$ is rational by closure under subtraction, and the contradiction is immediate;

(2) if $rx \in \mathbb{Q}$, then $x = (rx)\, r^{-1}$ is rational—and here $r \neq 0$ earns its keep, since r^{-1} exists exactly when $r \neq 0$.

Seeing where each hypothesis is spent shows the statement is sharp in both directions: drop "r rational" and it collapses ($\sqrt{2} + (-\sqrt{2}) = 0$, $\sqrt{2} \cdot \sqrt{2} = 2$); drop $r \neq 0$ and the product fails, since $rx = 0$ for every x.

The lasting lesson is how to handle "irrational" at all. The irrationals have no closure of their own, so you rarely argue with them head-on: assume rationality, isolate the known irrational using only operations that keep you inside $\mathbb{Q}$, and let field closure spring the trap.

Problem A2 *Rudin, Chapter 1, Exercise 2*

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

Solution.

Suppose, toward a contradiction, that $p \in \mathbb{Q}$ and $p^2 = 12$. Write $p = m/n$ in lowest terms, with $m, n \in \mathbb{Z}$, $n \neq 0$, and no prime dividing both m and n. Then

$$m^2 = 12n^2 = 3 \cdot 4n^2.$$

Thus $3 \mid m^2$, hence $3 \mid m$ by Euclid's lemma. Write $m = 3k$. Substituting back gives

$$9k^2 = 12n^2, \qquad \text{so} \qquad 3k^2 = 4n^2.$$

The right-hand side is divisible by 3, so $3 \mid n^2$, hence $3 \mid n$. This contradicts that m/n was in lowest terms. Therefore no rational number has square 12.

■

Reflections.

This is the same descent obstruction as the standard proof that $\sqrt{2}$ is irrational (1.4.1). A square equal to 12 would force the prime 3 into the numerator, and then the same equation forces it into the denominator. The contradiction is not about the size of the number; it is about unique prime divisibility being incompatible with a fraction already reduced to lowest terms.

Problem A3 *Rudin, Chapter 1, Exercise 3*

Prove Rudin's Proposition 1.15: in any field, if $x \neq 0$ then multiplication by x can be cancelled, the multiplicative identity is unique, inverses are unique, and $1/(1/x) = x$.

Solution.

Let F be a field and let $x \in F$ with $x \neq 0$.

For cancellation, suppose $xy = xz$. Multiplying both sides by $1/x$ and using associativity, commutativity, and the identity law gives

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

This proves: if $x \neq 0$ and $xy = xz$, then $y = z$.

If $xy = x$, then $xy = x \cdot 1$, so cancellation gives $y = 1$. If $xy = 1$, then also $x(1/x) = 1$, so cancellation gives $y = 1/x$. Finally, since $x(1/x) = 1$ and multiplication is commutative, $(1/x)x = 1$; by uniqueness of the inverse of $1/x$, we have

$$\frac{1}{1/x} = x.$$

■

REFLECTIONS.

The proof is the multiplicative twin of Rudin's additive Proposition 1.14. The condition $x \neq 0$ is the only new issue: it lets us multiply by $1/x$, and after that the field axioms reduce every clause to the same cancellation step. Once cancellation is proved, the remaining parts are just special cases: cancel x from $xy = x \cdot 1$, cancel it from $xy = x(1/x)$, and read the last statement as uniqueness of the inverse of $1/x$.

Problem A4 *Rudin, Chapter 1, Exercise 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 $\alpha \leq \beta$.

SOLUTION.

Because E is nonempty, fix some $t \in E$. Since α is a lower bound of E we have $\alpha \leq t$, and since β is an upper bound of E we have $t \leq \beta$. Chaining these by transitivity of the order, $\alpha \leq t \leq \beta$, gives $\alpha \leq \beta$.

■

REFLECTIONS.

The tell here is that the hypotheses never relate α and β to each other: α is tied only to the elements of E, as a lower bound, and β only to the elements of E, as an upper bound (1.5.1). When two quantities share no direct link but each speaks to a common set, compare them *through* a member of that set. That single idea also picks out the hypothesis that does the work—$E \neq \varnothing$, which is what lets you draw a witness $t \in E$; the rest is reading $\alpha \leq t$ and $t \leq \beta$ off the two conditions and chaining by transitivity (1.3.2).

Nonemptiness is the crux, not a technicality, and you see that by asking what breaks without it. Over the empty set both bound conditions hold vacuously (0.1.6), so *every* pair would qualify, including $\alpha > \beta$—in $\mathbb{R}$ both 1 and 0 vacuously bound $\varnothing$. Arguing by contradiction instead ($\beta < \alpha$ gives $\beta < \alpha \leq t \leq \beta$) spends the same witness and the same nonemptiness, good evidence that the format is cosmetic and the real ingredient is the element of E.

Carry the principle: to compare two things each pinned only to a common set, route the comparison through a witness drawn from the set—and confirm the set is nonempty before you reach in.

Problem A5 *Rudin, Chapter 1, Exercise 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 $\inf A = -\sup(-A)$.

Solution.

Because A is bounded below it has a lower bound m; write $-A = \{-x : x \in A\}$.

The set $-A$ is nonempty and bounded above: nonempty because A is, and bounded above because negating $m \leq x$ (which reverses the order) gives $-x \leq -m$ for every $x \in A$, so $-m$ is an upper bound. By the least-upper-bound property the number $\beta := \sup(-A)$ exists in $\mathbb{R}$, and we show $\inf A = -\beta$ by checking that $-\beta$ is the greatest lower bound of A.

First, $-\beta$ is a lower bound: for each $x \in A$ we have $-x \in -A$, so $-x \leq \beta$, and negating gives $-\beta \leq x$. Second, it is the greatest one: if γ is any lower bound of A, then $-x \leq -\gamma$ for every $x \in A$, so $-\gamma$ is an upper bound of $-A$; since β is the *least* upper bound, $\beta \leq -\gamma$, and negating gives $\gamma \leq -\beta$.

Thus $-\beta$ is a lower bound of A at least as large as every other, so $\inf A = -\beta = -\sup(-A)$.

■

Reflections.

Two words in the statement fix the whole approach. The first is *infimum*: the only tool in our notes that conjures a supremum or infimum out of a bare set is the least-upper-bound property (1.6.1), so the moment a problem asks you to *produce* an infimum, that property is your destination. The second is the set $-A$, handed to you unbidden—ask why the statement bothers to name the reflection of A through 0. Because negation reverses order (1.3.3), it ought to trade lower bounds for upper bounds and inf for sup, and our completeness tool speaks only of suprema: the statement is quietly telling you to cross to the supremum side, prove the thing there, and cross back. And "prove $\inf A = \cdots$" asks you to *certify* a number as the infimum, whose only certificate is the definition (1.5.3)—a greatest lower bound, two conditions, not one.

Believe it before proving it. With $A = [2, \infty)$ we get $\inf A = 2$, while $-A = (-\infty, -2]$ has supremum -2 and $-(-2) = 2$. Reflecting A across the origin turned its bottom edge into the top edge of $-A$; that one picture is the whole content.

Now watch what each step rests on:

(1) naming a lower bound m is legitimate only because A is bounded below, and passing from $m \leq x$ to $-x \leq -m$ is the order-reversal of 1.3.3, which makes $-m$ an upper bound of $-A$;

(2) with $-A$ nonempty (from $A \neq \varnothing$) and bounded above, the least-upper-bound property (1.6.1; List of Facts) produces $\beta = \sup(-A)$—the one and only use of completeness;

(3) reading the definition of supremum (1.5.2) one way, β bounds $-A$ above, so $-x \leq \beta$

and hence $-\beta \le x$: the easy half, that $-\beta$ is *a* lower bound;

(4) the crux is the other half—for any lower bound γ, the number $-\gamma$ is an upper bound of $-A$, and because β is the *least*, $\beta \le -\gamma$, i.e. $\gamma \le -\beta$. Everything hinges on "least"; drop it and $-\beta$ is merely *a* lower bound, not the infimum.

Two checks finish honestly. Both clauses of "greatest lower bound" (1.5.3) are present, and stopping after the first is the usual way this is half-solved and lost; and each hypothesis is load-bearing—without $A \neq \varnothing$ the set $-A$ is empty with no supremum, and without "bounded below" there is no m and $\inf A$ need not exist. Nothing is circular: we never assumed the infimum existed, we built it from a supremum.

That last fact is the lesson. It is exactly how the notes secure the greatest-lower-bound property with no second axiom—a set bounded below has an infimum because its reflection has a supremum, which is why infimum sits beside supremum at 1.5.3. Keep the technique: when a claim about infima resists you, reflect the set through 0 into a statement about suprema, settle it there, and reflect back. Negation is an order-reversing mirror that swaps inf with sup.

Problem A6 *Rudin, Chapter 1, Exercise 6*

Fix $b > 1$.

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

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

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

(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 $t \le x$. 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.

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

SOLUTION.

For (a), write $r = m/n = p/q$. Then $mq = np$. Both numbers in question are positive, and their (nq)th powers agree:

$$\left((b^m)^{1/n}\right)^{nq} = b^{mq} = b^{np} = \left((b^p)^{1/q}\right)^{nq}.$$

Uniqueness of positive roots gives $(b^m)^{1/n} = (b^p)^{1/q}$, so b^r is well defined.

For (b), write $r = m/n$ and $s = p/q$. By (a), use the common denominator nq:

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

The root product rule gives

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

For (c), first note that rational powers are increasing: if $t < r$, then

$$b^r = b^t b^{r-t} > b^t,$$

because $r - t > 0$ and $b^{r-t} > 1$. Hence every element of $B(r)$ is at most b^r, and $b^r \in B(r)$. Thus b^r is actually the maximum of $B(r)$, so $b^r = \sup B(r)$. For arbitrary real x, the set $B(x)$ is nonempty and bounded above: choose rationals below and above x using density of $\mathbb{Q}$ in $\mathbb{R}$ (1.7.2). Therefore completeness gives $\sup B(x)$, and the definition $b^x = \sup B(x)$ makes sense.

For (d), use rational approximation from below. If $r < x$ and $s < y$ are rational, then

$$b^r b^s = b^{r+s} \leq b^{x+y},$$

so taking suprema first over r and then over s gives $b^x b^y \leq b^{x+y}$. Conversely, first suppose $t < x + y$ is rational. Choose a rational r with $t - y < r < x$; then $s = t - r$ is rational and $s < y$, so

$$b^t = b^r b^s \leq b^x b^y.$$

If $t = x + y$ is rational, the same argument applied to $t - 1/n$ gives $b^{t-1/n} \leq b^x b^y$ for every large n. If $b^t > b^x b^y$, put $c = b^t/(b^x b^y) > 1$; the elementary estimate $b^{1/n} \to 1$ gives some n with $b^{1/n} < c$, and then $b^{t-1/n} = b^t/b^{1/n} > b^x b^y$, a contradiction. Thus $b^t \leq b^x b^y$ for every rational $t \leq x + y$.

Taking the supremum over all such t gives $b^{x+y} \leq b^x b^y$. The two inequalities prove $b^{x+y} = b^x b^y$.

■

Reflections.

The exercise builds real exponents by the same completeness pattern used throughout Lecture 1: define the object first on $\mathbb{Q}$, show the rational definition is independent of the chosen fraction, then fill the real gaps with a supremum. Part (d) is the only subtle step. It says the algebraic law survives passage from rationals to real suprema, and the density

of $\mathbb{Q}$ is what lets the rational approximants approach x, y, and $x+y$ from below.

Problem A7 *Rudin, Chapter 1, Exercise 7*

Fix $b > 1$, $y > 0$, and prove that there is a unique real x such that $b^x = y$ by completing Rudin's outline.

SOLUTION.

For every positive integer n,

$$b^n - 1 = (b-1)(1 + b + \cdots + b^{n-1}) \geq n(b-1),$$

which proves (a). Applying this to $b^{1/n}$ gives

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

which is (b). If $t > 1$ and $n > (b-1)/(t-1)$, then

$$b^{1/n} - 1 \leq \frac{b-1}{n} < t - 1,$$

so $b^{1/n} < t$, proving (c).

For (d), suppose $b^w < y$. Put $t = yb^{-w} > 1$. By (c), $b^{1/n} < t$ for all sufficiently large n, and hence

$$b^{w+1/n} = b^w b^{1/n} < b^w t = y.$$

For (e), suppose $b^w > y$. Put $t = b^w/y > 1$. Again $b^{1/n} < t$ for all sufficiently large n, so

$$b^{w-1/n} = b^w b^{-1/n} > y.$$

Let

$$A = \{w \in \mathbb{R} : b^w < y\}.$$

The set A is nonempty and bounded above. Indeed, by (a) and the Archimedean property, positive integer powers of b eventually exceed both y and $1/y$, so some negative integer belongs to A and some positive integer bounds A above. Let $x = \sup A$.

If $b^x < y$, part (d) gives $b^{x+1/n} < y$ for some n, so $x + 1/n \in A$, contradicting that x is an upper bound. If $b^x > y$, part (e) gives $b^{x-1/n} > y$ for some n; monotonicity then makes $x - 1/n$ an upper bound of A, contradicting the definition of x as the least upper bound. Hence $b^x = y$.

Finally, if $x_1 < x_2$, then $x_2 - x_1 > 0$, so $b^{x_2 - x_1} > 1$ and

$$b^{x_2} = b^{x_1} b^{x_2 - x_1} > b^{x_1}.$$

Thus b^x is strictly increasing, and at most one x can satisfy $b^x = y$.

■

Reflections.

This is the logarithm as a supremum argument. The set $A = \{w : b^w < y\}$ records all exponents that are still too small. Parts (a)–(e) prove there is no jump at the boundary: if the supremum exponent were still below y, one could move a little to the right; if it were above y, one could move the upper bound a little to the left. Completeness supplies the boundary point, and monotonicity supplies uniqueness.

Problem A8 *Rudin, Chapter 1, Exercise 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, toward a contradiction, that some total order makes $\mathbb{C}$ an ordered field.

First, every nonzero square is positive. Let $w \neq 0$; by trichotomy $w > 0$ or $w < 0$. If $w > 0$ then $w^2 = w \cdot w > 0$, a product of positives. If $w < 0$ then $-w > 0$, so $(-w)(-w) > 0$; and $(-w)(-w) = w^2$, so again $w^2 > 0$.

Apply this with $w = 1$ to get $1 = 1^2 > 0$, and adding -1 to both sides gives $-1 < 0$. Apply it with $w = i \neq 0$ to get $i^2 > 0$; but $i^2 = -1$, so $-1 > 0$. Then -1 is both positive and negative, contradicting trichotomy. Hence no order turns $\mathbb{C}$ into an ordered field.

■

Reflections.

The hint—-1 is a square—is the proof in disguise, and hearing what such a hint says is the real exercise. In any ordered field the order is rigid: from the axioms (1.3.3) a product of positives is positive, so two facts get pinned down that ordinarily live apart—every nonzero square is positive, and -1 is negative. They collide only if some single number is at once -1 and a square, and the hint supplies exactly that: $-1 = i^2$. Hence the natural shape is contradiction (0.5.5).

The argument has two moving parts:

(1) the lemma "nonzero squares are positive," got by splitting on the sign of w (a clean two-case argument, 0.5.7) and using product-positivity; it gives $1 = 1^2 > 0$, hence $-1 < 0$;

(2) the collision: apply the lemma to $i \neq 0$ to force $i^2 = -1 > 0$, against $-1 < 0$, breaking trichotomy.

Notice the lemma uses only trichotomy and product-positivity, while the collision uses only

that i is a nonzero square root of -1.

The reason to remember the problem is that nothing in it is special to $\mathbb{C}$: in *any* ordered field $1 > 0$ forces $-1 < 0$ while squares stay ≥ 0, so a field becomes unorderable the instant -1 acquires a square root. "Squares are nonnegative" is the master constraint an order imposes; to show a field admits none, exhibit a quantity the order would call both positive and negative.

Problem A9 *Rudin, Chapter 1, Exercise 9*

Suppose $z = a + bi$ and $w = c + di$. Define $z < w$ if $a < c$, and also if $a = c$ but $b < d$. Prove that this turns the set of complex numbers into an ordered set. Does this ordered set have the least-upper-bound property?

SOLUTION.

The relation is lexicographic order. For any two complex numbers $a + bi$ and $c + di$, trichotomy for real numbers gives exactly one of $a < c$, $a = c$, or $c < a$. If $a \neq c$, this decides exactly one of $z < w$ or $w < z$; if $a = c$, trichotomy for b and d decides exactly one of $b < d$, $b = d$, or $d < b$. Thus exactly one of $z < w$, $z = w$, or $w < z$ holds.

Transitivity follows by cases. If $z < w$ and $w < u$, compare first the real parts. A strict increase in the real part persists through the chain; if the real parts are equal throughout, transitivity of the imaginary parts gives the result. Hence this is an order on $\mathbb{C}$.

It does not have the least-upper-bound property. Let

$$E = \{a + bi : a < 0\}.$$

This set is nonempty and is bounded above: every number $0 + ti$ is an upper bound. But there is no least upper bound, because if $0 + ti$ is an upper bound, then $0 + (t - 1)i$ is a smaller upper bound.

■

REFLECTIONS.

Lexicographic order makes $\mathbb{C}$ an ordered set by reading complex numbers like dictionary entries: first compare real parts, and use imaginary parts only to break ties. The failure of completeness comes from the vertical line over real part 0; all of it bounds the left half-plane, and there is no lowest point on that vertical line.

Problem A10 *Rudin, Chapter 1, Exercise 10*

Suppose $z = a + bi$, $w = u + iv$, 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.

The displayed quantities are well defined because $|w| \geq |u|$. By construction,

$$a^2 - b^2 = u.$$

Also,

$$4a^2b^2 = (|w| + u)(|w| - u) = |w|^2 - u^2 = v^2,$$

so $2ab = |v|$. Therefore

$$z^2 = (a + bi)^2 = (a^2 - b^2) + 2abi = u + i|v|.$$

If $v \geq 0$, this is $u + iv = w$. If $v \leq 0$, then

$$\overline{z}^2 = (a - bi)^2 = (a^2 - b^2) - 2abi = u - i|v| = u + iv = w.$$

The exception is $w = 0$, whose only square root is 0. If $w \neq 0$, the construction gives one square root, and its negative gives a second; a quadratic equation over a field has at most two roots, so these are exactly the two square roots.

■

Reflections.

The formula is just the real and imaginary parts of $(a + bi)^2 = u + iv$ solved backward: $a^2 - b^2 = u$ and $2ab = v$. The absolute value decides the sign of the imaginary part. Once one square root of a nonzero complex number is found, the other is its negative, and there cannot be a third.

Problem A11 *Rudin, Chapter 1, Exercise 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

$$r = |z|, \qquad w = \frac{z}{|z|}.$$

Then $r > 0$, $|w| = |z|/|z| = 1$, and $rw = z$.

If $z = 0$, take $r = 0$ and any complex number w with $|w| = 1$, for instance $w = 1$; then $z = rw$.

The number r is always unique, since $z = rw$ and $|w| = 1$ imply $|z| = r$. When $z \neq 0$,

$w = z/r$ is also unique. When $z = 0$, $r = 0$ is forced but w can be any unit complex number, so w is not unique.

■

REFLECTIONS.

This is the polar decomposition stripped of angles. The modulus supplies the size r, and division by the size leaves only direction. The only place direction is undefined is the origin, which explains exactly why w fails to be unique only when $z = 0$.

Problem A12 *Rudin, Chapter 1, Exercise 12*

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

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

SOLUTION.

We prove the claim by induction on n. For $n = 1$ it is equality, and for $n = 2$ it is Rudin's triangle inequality for complex numbers. Suppose the result holds for n terms. Then

$$\begin{aligned} |z_1 + \cdots + z_n + z_{n+1}| &\leq |z_1 + \cdots + z_n| + |z_{n+1}| \\ &\leq |z_1| + \cdots + |z_n| + |z_{n+1}|. \end{aligned}$$

Thus the inequality holds for every positive integer n.

■

REFLECTIONS.

The two-term triangle inequality is the whole engine. Induction lets the same inequality absorb one new summand at a time, turning a local estimate into a finite one.

Problem A13 *Rudin, Chapter 1, Exercise 13*

If x and y are complex, prove that

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

SOLUTION.

By the triangle inequality,

$$|x| = |(x - y) + y| \leq |x - y| + |y|,$$

so $|x| - |y| \leq |x - y|$. Swapping x and y gives

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

Together these two inequalities say

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

■

Reflections.

This is the reverse triangle inequality. The direct triangle inequality bounds a whole by its pieces; rearranging it says that changing a complex number by $x - y$ can change its length by no more than $|x - y|$.

Problem A14 *Rudin, Chapter 1, Exercise 14*

If z is a complex number such that $|z| = 1$, compute

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

Solution.

Since $|z| = 1$, we have $z\overline{z} = 1$. Then

$$|1 + z|^2 = (1 + z)(1 + \overline{z}) = 2 + z + \overline{z}$$

and

$$|1 - z|^2 = (1 - z)(1 - \overline{z}) = 2 - z - \overline{z}.$$

Adding gives

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

■

Reflections.

The mixed terms cancel. Geometrically, this is the parallelogram identity in the special case of the two vectors 1 and z on the unit circle: the two squared diagonal lengths add to 4.

Problem A15 *Rudin, Chapter 1, Exercise 15*

Under what conditions does equality hold in the Schwarz inequality?

Solution.

Let

$$A = \sum_{j=1}^{n} |a_j|^2, \qquad B = \sum_{j=1}^{n} |b_j|^2, \qquad C = \sum_{j=1}^{n} a_j \overline{b_j}.$$

In Rudin's proof, if $B > 0$ then

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

Equality in Schwarz means $AB = |C|^2$, so the sum of squares on the left is 0. Hence

$$Ba_j = Cb_j \qquad (1 \le j \le n),$$

which says $a_j = (C/B)b_j$ for every j.

If $B = 0$, then every $b_j = 0$ and equality is automatic. Therefore equality holds exactly when one of the two vectors is zero or when there is a complex scalar λ such that

$$a_j = \lambda b_j \qquad (1 \le j \le n).$$

■

REFLECTIONS.

Schwarz becomes an equality precisely when the "error vector" in Rudin's proof vanishes. That is the algebraic version of linear dependence: one vector is a scalar multiple of the other. If one vector is zero, the same description is understood as the degenerate equality case.

Problem A16 *Rudin, Chapter 1, Exercise 16*

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

(a) If $2r > d$, there are infinitely many $z \in \mathbb{R}^k$ such that $|z - x| = |z - y| = r$.

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

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

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

SOLUTION.

Let $m = (x+y)/2$ and let $u = (y-x)/d$. Then $|u| = 1$. A point z satisfies $|z-x| = |z-y|$ exactly when $z - m$ is orthogonal to u; geometrically, it lies in the perpendicular bisector hyperplane of the segment from x to y. For such z,

$$|z - x|^2 = |z - m|^2 + \left(\frac{d}{2}\right)^2.$$

Thus the equations $|z-x| = |z-y| = r$ are equivalent to

$$z - m \perp u, \qquad |z-m|^2 = r^2 - \frac{d^2}{4}.$$

If $2r > d$, the right-hand side is positive. In dimension $k \geq 3$, the perpendicular subspace has dimension $k-1 \geq 2$, so its sphere of that positive radius contains infinitely many points. If $2r = d$, the radius is 0, so $z = m$ is the unique point. If $2r < d$, the required squared radius is negative, so no point exists.

For $k = 2$, the perpendicular subspace is one-dimensional: if $2r > d$ there are exactly two points, if $2r = d$ one point, and if $2r < d$ none. For $k = 1$, the perpendicular subspace is zero-dimensional: there is one point when $2r = d$ and no point otherwise.

■

Reflections.

The problem is the intersection of two equal-radius spheres centered at x and y. The midpoint separates the geometry from the algebra: first move to the perpendicular bisector, then ask for a sphere of radius $\sqrt{r^2 - d^2/4}$ inside that perpendicular space. The dimension of that perpendicular space is why the answer changes for $k = 2$ and $k = 1$.

Problem A17 *Rudin, Chapter 1, Exercise 17*

Prove that

$$|x+y|^2 + |x-y|^2 = 2|x|^2 + 2|y|^2$$

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

Solution.

Using the inner product,

$$|x+y|^2 = (x+y)\cdot(x+y) = |x|^2 + 2x\cdot y + |y|^2$$

and

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

Adding cancels the cross terms and gives

$$|x+y|^2 + |x-y|^2 = 2|x|^2 + 2|y|^2.$$

Geometrically, x and y span a parallelogram whose diagonals are $x+y$ and $x-y$; the sum of the squares of the diagonals equals the sum of the squares of the four sides.

■

Reflections.

The identity is algebraic cancellation of the cross terms $2x \cdot y$ and $-2x \cdot y$. Its geometry is that the two diagonals of a parallelogram encode the same total squared length as the four sides.

Problem A18 *Rudin, Chapter 1, Exercise 18*

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

SOLUTION.

If $x = 0$, take any nonzero y. If $x \neq 0$, choose an index j with $x_j \neq 0$ and choose $\ell \neq j$. Define y by

$$y_j = -x_\ell, \qquad y_\ell = x_j, \qquad y_i = 0 \quad (i \neq j, \ell).$$

Then $y \neq 0$, since $y_\ell = x_j \neq 0$, and

$$x \cdot y = x_j(-x_\ell) + x_\ell x_j = 0.$$

For $k = 1$ this is not true for every x: if $x \neq 0$, then $x \cdot y = xy = 0$ forces $y = 0$.

■

REFLECTIONS.

In dimension at least two there is room to turn one nonzero coordinate into a perpendicular direction. In one dimension there is no sideways direction, so only the zero vector is orthogonal to a nonzero vector.

Problem A19 *Rudin, Chapter 1, Exercise 19*

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

$$|x - a| = 2|x - b|$$

if and only if $|x - c| = r$. Rudin gives the solution $3c = 4b - a$, $3r = 2|b - a|$.

SOLUTION.

Assume first that $a \neq b$, so the displayed r is positive. Squaring the equation gives

$$|x - a|^2 = 4|x - b|^2.$$

Expanding with the inner product,

$$|x|^2 - 2a \cdot x + |a|^2 = 4|x|^2 - 8b \cdot x + 4|b|^2.$$

Move all terms to one side and complete the square with

$$c = \frac{4b - a}{3}.$$

A direct simplification gives

$$|x - a|^2 - 4|x - b|^2 = -3|x - c|^2 + \frac{4}{3}|b - a|^2.$$

Thus $|x - a| = 2|x - b|$ is equivalent to

$$|x - c|^2 = \frac{4}{9}|b - a|^2,$$

or $|x - c| = r$, where

$$r = \frac{2}{3}|b - a|.$$

If $a = b$, the original equation reduces to $|x - a| = 2|x - a|$, hence $x = a$; this is the degenerate case of the same formula with $r = 0$.

■

Reflections.

This is an Apollonius sphere: the points whose distance from a is twice their distance from b form a sphere with center shifted past b away from a. The computation is just completing the square after expanding the two squared distances.

Problem A20 *Rudin, Chapter 1, Exercise 20*

With reference to Rudin's Appendix, suppose 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.

Call the modified objects *weak cuts*: nonempty proper subsets of $\mathbb{Q}$ that are downward closed, but may have a largest element.

The least-upper-bound proof from Rudin's Appendix still works. If $\mathcal{A}$ is a nonempty family of weak cuts bounded above by a weak cut β, then

$$\gamma = \bigcup_{\alpha \in \mathcal{A}} \alpha$$

is nonempty, proper because $\gamma \subseteq \beta$, and downward closed. Hence γ is a weak cut. It is plainly an upper bound of $\mathcal{A}$, and any smaller weak cut fails to contain some element of some $\alpha \in \mathcal{A}$, so it is not an upper bound. Thus $\gamma = \sup \mathcal{A}$.

Addition is still defined by

$$\alpha + \beta = \{r + s : r \in \alpha,\ s \in \beta\}.$$

The sum of two weak cuts is again a weak cut, and commutativity and associativity come from the corresponding laws in $\mathbb{Q}$. The additive identity is now

$$0^\dagger = \{q \in \mathbb{Q} : q \leq 0\},$$

not Rudin's original open cut $\{q : q < 0\}$. Indeed, if α is downward closed, then $\alpha + 0^\dagger \subseteq \alpha$, while $p = p + 0 \in \alpha + 0^\dagger$ for every $p \in \alpha$. Thus axioms (A1)–(A4) hold.

Axiom (A5) fails. Let

$$\alpha = \{q \in \mathbb{Q} : q < 0\}.$$

If some weak cut β satisfied $\alpha + \beta = 0^\dagger$, then $0 \in \alpha + \beta$, so there would be $r < 0$ and $s \in \beta$ with $r + s = 0$. Thus $s = -r > 0$. But then $-s/2 \in \alpha$, so

$$(-s/2) + s = s/2 > 0$$

would belong to $\alpha + \beta$, contradicting $\alpha + \beta = 0^\dagger$. Hence this α has no additive inverse.

■

REFLECTIONS.

The no-largest-element condition is exactly what separates open cuts from rational endpoint cuts. If it is removed, completeness by unions survives and addition still has an identity, but the identity becomes the closed cut at 0. The old open zero-cut then has no additive inverse, so the field structure breaks at (A5).

Problem B *Induction: Divisibility by* 3

Prove by induction that $n^3 + 2n$ is divisible by 3 for every integer $n \geq 0$.

SOLUTION.

For $n \geq 0$ let $P(n)$ be the statement $3 \mid n^3 + 2n$. The base case $n = 0$ holds, since $0^3 + 2 \cdot 0 = 0 = 3 \cdot 0$.

Assume $P(n)$, say $n^3 + 2n = 3k$ with $k \in \mathbb{Z}$. Then

$$\begin{aligned}(n+1)^3 + 2(n+1) &= (n^3 + 3n^2 + 3n + 1) + (2n + 2) \\ &= (n^3 + 2n) + 3n^2 + 3n + 3 \\ &= 3k + 3\,(n^2 + n + 1) = 3\,(k + n^2 + n + 1),\end{aligned}$$

and $k + n^2 + n + 1 \in \mathbb{Z}$, so $3 \mid (n+1)^3 + 2(n+1)$, i.e. $P(n+1)$. By induction $P(n)$ holds

for all $n \geq 0$.

■

Reflections.

"Divisible by 3 for every n" is indexed by the naturals with successive cases linked by a small algebraic change—the signature of induction (1.1.3, 0.6.2). But induction pays off only if the step *reuses* the previous case, so the genuine task is algebraic: write $f(n+1) = (n+1)^3 + 2(n+1)$ as $f(n)$ plus a remainder you can see is a multiple of 3.

Doing that exposes the increment $3n^2 + 3n + 3 = 3(n^2 + n + 1)$, and now the hypothesis in usable form ($f(n) = 3k$ for an actual integer k, not the vague "3 divides it") adds to a multiple of 3 and keeps $f(n+1)$ divisible. That increment is the entire engine.

Seeing the same statement without induction explains *why* it is true, not just *that* it is: $n^3 + 2n = (n-1)\,n\,(n+1) + 3n$, and among three consecutive integers one is a multiple of 3. (The notes prove the cousin $3 \mid n^3 - n$ the identical way at 0.6.8—worth reading side by side.)

The habit to carry: to prove $p \mid f(n)$ by induction, never stare at $f(n+1)$ whole—compute the increment $f(n+1) - f(n)$, check it is a multiple of p, and divisibility is inherited from one case to the next.

Problem C *Induction: An Exponential Inequality*

Prove by induction that $2^n > n^2$ for every integer $n > 4$.

Solution.

Induct on n, starting at $n = 5$, the least integer greater than 4. The base case holds: $2^5 = 32 > 25 = 5^2$.

Assume $2^n > n^2$ for some $n \geq 5$. Doubling (multiplication by $2 > 0$ preserves the inequality), $2^{n+1} = 2 \cdot 2^n > 2n^2$. Moreover $2n^2 \geq (n+1)^2$ for $n \geq 5$, since

$$2n^2 - (n+1)^2 = n^2 - 2n - 1 = (n-1)^2 - 2 \geq (5-1)^2 - 2 = 14 > 0.$$

Combining, $2^{n+1} > 2n^2 \geq (n+1)^2$, which is the statement at $n+1$. By induction $2^n > n^2$ for every $n > 4$.

■

Reflections.

Two features flag the method. "For every integer $n > 4$" is an inductive shape (1.1.3), and the oddly specific cutoff $n > 4$ is a clue in its own right: it says the inequality is *false* below 5 and the induction must begin exactly where the statement first holds for good. It does—$n = 2, 3, 4$ give $4 = 4$, $8 < 9$, $16 = 16$, and only from $n = 5$ onward is it true, the same result the notes establish at 0.6.7.

The step's idea is that an exponential, once doubled, overshoots a polynomial: $2^{n+1} = 2 \cdot 2^n > 2n^2$, and $2n^2$ already clears $(n+1)^2$. So the inductive step reduces to a purely polynomial inequality, $2n^2 \geq (n+1)^2$, i.e. $(n-1)^2 \geq 2$—which you must check across the *whole* range $n \geq 5$, not merely at the base, or the chain could snap somewhere up the line. The hypothesis carries the exponential growth; a side inequality, valid throughout, bridges $2n^2$ to $(n+1)^2$.

For any exponential-beats-polynomial claim the recipe is the same: double the hypothesis, reduce the step to a polynomial inequality, confirm it on the entire tail, and anchor the base case where the statement first becomes permanently true.

Problem D *An Equivalence Relation on the Rationals*

To define $\mathbb{Q}$, we declared $\frac{p}{q} \sim \frac{r}{s} \iff ps = rq$ in $\mathbb{Z}$. Show this relation is reflexive, symmetric, and transitive — an equivalence relation.

SOLUTION.

The relation acts on symbols $\frac{p}{q}$ with $p, q \in \mathbb{Z}$ and $q \neq 0$, by $\frac{p}{q} \sim \frac{r}{s} \iff ps = rq$.

Reflexivity is $pq = pq$, which is exactly $\frac{p}{q} \sim \frac{p}{q}$. Symmetry is immediate: $ps = rq$ reversed is $rq = ps$, i.e. $\frac{r}{s} \sim \frac{p}{q}$.

For transitivity, suppose $\frac{p}{q} \sim \frac{r}{s}$ and $\frac{r}{s} \sim \frac{m}{n}$, so $ps = rq$ and $rn = ms$. Multiplying the first by n and the second by q, $psn = rqn$ and $rnq = msq$, and since $rqn = rnq$ the right-hand sides agree, giving $psn = msq$, that is $s(pn) = s(mq)$. As $s \neq 0$ and $\mathbb{Z}$ has no zero divisors, we cancel s to get $pn = mq$, i.e. $\frac{p}{q} \sim \frac{m}{n}$. Being reflexive, symmetric, and transitive, $\sim$ is an equivalence relation.

■

REFLECTIONS.

On its face this asks you to check the three clauses of an equivalence relation (0.4.16), but the deeper clue is *which* relation: the very rule our construction of $\mathbb{Q}$ rests on (1.2.2), deciding when two fraction symbols name the same rational. So it is not a drill but the well-definedness check that makes $\mathbb{Q}$ a legitimate object—and the reason one rational has many names (1.2.3).

That reframing locates the content. Reflexivity and symmetry fall straight out of equality of integers ($pq = pq$; and $ps = rq$ reversed is $rq = ps$), so everything real lives in transitivity, where the shared symbol $\frac{r}{s}$ must be eliminated. From $ps = rq$ and $rn = ms$ you cannot chain directly, so you manufacture a common factor—multiply to reach $s(pn) = s(mq)$—and cancel s.

That cancellation is the whole game, and it is legal only because $s \neq 0$ and $\mathbb{Z}$ is an integral domain; it is exactly the step that consumes the nonzero-denominator convention. Allow

$s = 0$ and transitivity can fail, which is precisely why $\mathbb{Q}$ is built from fractions with nonzero denominators (1.2.2).

The lesson generalises: an equation-defined relation is typically shown transitive by combining its two defining equations into one that shares a factor and then cancelling, and such cancellation is licensed in an integral domain exactly when the shared factor is nonzero.

Problem E *An Inequality with Square Roots*

Prove that if real numbers a, b, c satisfy $ab = c$ then either $a \le \sqrt{c}$ or $b \le \sqrt{c}$.

Solution.

The symbol $\sqrt{c}$ is defined only for $c \ge 0$, so that is the domain of the statement (for $c < 0$ it is not well-posed, and $ab = c$ alone permits $c < 0$, e.g. $a = 1$, $b = -1$). Write $\sqrt{c} \ge 0$ for the nonnegative root, so $(\sqrt{c})^2 = c$.

Suppose, toward a contradiction, that $ab = c$ yet $a > \sqrt{c}$ and $b > \sqrt{c}$—the negation of the conclusion. Since $\sqrt{c} \ge 0$, both a and b are positive. Multiplying $a > \sqrt{c}$ by $b > 0$ gives $ab > \sqrt{c}\,b$, and multiplying $b > \sqrt{c}$ by $\sqrt{c} \ge 0$ gives $\sqrt{c}\,b \ge (\sqrt{c})^2 = c$. Hence $ab > c$, contradicting $ab = c$. Therefore $a \le \sqrt{c}$ or $b \le \sqrt{c}$.

■

Reflections.

The conclusion is a disjunction, and disjunctions resist a head-on attack because you cannot say in advance which alternative holds; the "or" is itself the clue to negate. Assuming *both* $a > \sqrt{c}$ and $b > \sqrt{c}$ collapses the two unknowns into one usable conjunction—the proving-disjunctions and negation strategy of 0.5.8 and 0.5.11, on the connective laws of 0.1.3.

A quieter clue comes first: a radical $\sqrt{c}$ appears, defined only for $c \ge 0$, so that is the genuine domain of the problem rather than an extra hypothesis ($ab = c$ by itself allows $c < 0$). Pinning the domain hands you $\sqrt{c} \ge 0$ and $(\sqrt{c})^2 = c$, the facts the argument leans on.

Now the negation does the work: $a, b > \sqrt{c} \ge 0$ makes both positive, which is what licenses multiplying the two inequalities in an ordered field (1.3.3), yielding $ab > (\sqrt{c})^2 = c$ against $ab = c$. The picture to keep is a threshold—$\sqrt{c}$ is a gate, and if a product equals c its two factors cannot both stand strictly above the gate. The $\le$ cannot be tightened to $<$, as $a = b = \sqrt{c}$ shows, so equality must be allowed.

Two reusable moves fall out: to prove "P or Q," assume $\neg P$ and $\neg Q$ together and hunt for a contradiction; and to weigh a product against a threshold T, compare each factor against $\sqrt{T}$.

Problem F *Rudin, Chapter 2, Exercise 2*

A complex number z is *algebraic* if there are integers $a_0, \dots, a_n$, not all zero, with $a_0 z^n + a_1 z^{n-1} + \cdots + a_n = 0$. Prove that the set of all algebraic numbers is countable. *Hint:* for each N there are finitely many equations with $n + |a_0| + \cdots + |a_n| = N$.

SOLUTION.

To each integer polynomial $a_0 z^n + \cdots + a_n$ (coefficients not all zero) assign the *height*

$$N = n + |a_0| + |a_1| + \cdots + |a_n| \geq 1.$$

Fix $N \geq 1$. A height-N polynomial has $n \leq N$ and $|a_i| \leq N$, so there are at most $N+1$ choices for n and at most $(2N+1)^{n+1}$ for the coefficients; hence only finitely many integer polynomials have height N. Each is nonzero of degree $\leq N$, so it has at most N roots in $\mathbb{C}$. Therefore the set A_N of roots of all height-N polynomials is a finite union of finite sets, hence finite.

Every algebraic number is a root of some integer polynomial, of some height $N \geq 1$, so it lies in A_N; conversely each element of every A_N is algebraic. Thus $\mathbb{A} = \bigcup_{N=1}^{\infty} A_N$ is a countable union of finite sets, so it is at most countable. Finally $\mathbb{A}$ is infinite, since every integer k is a root of $z - k$; an infinite, at-most-countable set is countable, so $\mathbb{A}$ is countable.

■

REFLECTIONS.

"Prove this set is countable" has, in our notes, essentially one playbook: present the set as a countable union of finite or countable pieces—the quotable "a countable union of countable sets is countable", with "a subset of a countable set is finite or countable" (2.1.9) in support. The art is choosing the slicing, and the hint points straight at it: organise the polynomials by an integer *height* $N = n + \sum |a_i|$. Why a height is the right device is the part to understand—it must be *finite-to-one*, only finitely many objects sharing each value, and this one is, since N simultaneously caps the degree ($n \leq N$) and every coefficient ($|a_i| \leq N$).

From there the steps are short, each closed by a specific fact:

(1) finitely many polynomials per height, and a nonzero degree-n polynomial has at most n roots, so each height contributes only finitely many algebraic numbers;

(2) assembling over all heights gives $\bigcup_N A_N$, a countable union of finite sets, hence at most countable;

(3) "at most countable" upgrades to "countable" only once you note the set is infinite—every integer k is a root of $z - k$, and $\mathbb{Z}$ is countable (2.1.4).

> That last step is the easy one to forget. And the transferable idea is the height itself: anything assembled from finite integer data—polynomials, finite words over a finite alphabet, finite sequences—can be sliced into finite layers by a well-chosen integer "size" with finite fibres, and then "countable union of countable sets" finishes the job.