

8.5 Writing a Proof

Section 8.4 trained a reader to say what licenses each line of a proof, as Example (Explaining a proof, well and badly) did line by line. This section turns to the writer. A proof is written for a reader who will check it in exactly that way, so the writer's job is to make each line's warrant visible. The section gives a procedure that leads from a statement to plain prose, the conventions of written mathematics, each a rule of Chapters 1–7 made audible, and four worked examples.

8.5.1 A procedure

A reader checks a proof forwards, one line at a time. A writer finds a proof mostly backwards, from the goal. The two directions are not in conflict: Section 3.1 showed that the search for a derivation is goal-directed, and Definition 1.4.2 says that the derivation found is a list in which each line cites only lines above it. The procedure below keeps both, the search in scratch work and the derivation on the page. Its steps 3 and 6 use the levels of Definition 8.3.1 and the convention of Definition 8.3.2 from Section 8.3.

Algorithm. Writing a proof of a statement.

1. **Write the goal in symbols.** Translate the statement, its hypotheses and its conclusion into a formula, as in Section 6.1, with every quantifier and its bound. Read a letter that is not introduced as universally quantified (Section 5.1). Set up the Givens/Goal table: the hypotheses on the left, the goal on the right.
2. **Unwind the definitions.** Replace each defined word (“bounded”, “converges”, “irrational”, “ $\subseteq$ ”) by its definition, in the hypotheses and in the goal. This is $\leftrightarrow E$ on a definition.
3. **Read the skeleton off the goal** (Section 3.1, extended in Section 6.3), and write it at level 1: the boxes, their first lines and their last lines. Open the $\exists E$ boxes of existential hypotheses early.
4. **Fill the boxes:** backwards in scratch, forwards on the page. The search runs from the goal; the written proof runs from the hypotheses, each line citing lines above it. What the search found goes into the Idea, not into the Proof.
5. **Choose constants last in the search, and write them first on the page**, each with what it depends on.
6. **Write level 3**, leaving silent exactly the steps that Definition 8.3.2 allows, and no others.
7. **Reread as a checker:** for each line, is it true, and by which rule does it follow from which available lines? (Section 8.6 makes this a two-column check.)

Steps 1–3 involve no mathematics, only logical form, and they fix the first and last sentence of every box before anything is invented (“skeleton first”). A picture after the next example shows steps 4 and 5.

Quick check. Which step of the procedure produces the sentence “Let $\varepsilon > 0$ ” at the start of a proof that $a_n \rightarrow L$, and which step keeps it at level 3?

Solution. Step 3. Unwound in step 2, the goal begins $\forall \varepsilon > 0$, so its skeleton is a bounded $\forall I$ box whose assumption is $\varepsilon_0 > 0$; “Let $\varepsilon > 0$ ” is the first line of that box. Step 6 keeps it, because the opening of a $\forall I$ box is never silent (Definition 8.3.2). The closing “since ε was arbitrary” may be silent.

8.5.2 The procedure, run once

This example runs all seven steps on a statement not seen before. Sets of reals are used here as Chapter 5 used them, with “ $a \in A$ ” a one-place predicate and $A \subseteq B$ read as “every element of A is an element of B ”.

Example. A subset of a bounded set

Let A and B be sets of real numbers with $A \subseteq B$. Prove that if B is bounded above, then A is bounded above.

Solution. Steps 1 and 2: the goal in symbols, unwound. Over the domain $\mathbb{R}$, “ B is bounded above” is $\exists M \forall b \in B (b \leq M)$ (Section 6.1), and $A \subseteq B$ is $\forall x \in A (x \in B)$. The statement is an implication, so the derivation below is the inside of a $\rightarrow I$ box: its assumption is the first formula (line 2), the hypothesis is the second, and its goal is $\exists M \forall a \in A (a \leq M)$.

Givens	Goal
$A \subseteq B$; B bounded above	A bounded above
$\forall x \in A (x \in B)$; $\exists M \forall b \in B (b \leq M)$	$\exists M \forall a \in A (a \leq M)$
$\forall x \in A (x \in B)$; $\forall b \in B (b \leq M_0)$ ($\exists E$, M_0 fresh)	$\exists M \forall a \in A (a \leq M)$
the same	$\forall a \in A (a \leq M_0)$ (try the witness M_0)
the same, and $a_0 \in A$ ($\forall I$, a_0 fresh)	$a_0 \leq M_0$
the same, and $a_0 \in B$ ($\forall E$ at a_0)	$a_0 \leq M_0$ ✓ ($\forall E$ at a_0)

The second row is step 2; each later row is one move of steps 3 and 4; the table's last row is where the search ends.

Step 3: the skeleton. The goal is an existential, so it is postponed: no witness is in sight yet. The assumption “ B is bounded above” (line 2) is an existential, so its $\exists E$ box opens at once, with a fresh name M_0 and the assumption $\forall b \in B (b \leq M_0)$; the box's last line is the goal.

Step 4: filling the box. Backwards: the goal needs a witness M and a proof of $\forall a \in A (a \leq M)$. The only bound in sight is M_0 , so try it. Then the new goal is a bounded universal: a box “let $a_0 \in A$ ” whose last line is $a_0 \leq M_0$. That line comes from the bound on B , instantiated at a_0 , which needs $a_0 \in B$; and $a_0 \in B$ comes from $A \subseteq B$ instantiated at a_0 . Forwards, the same lines in the order of the list are the derivation below (with the bounded rules of Proposition 6.1.1; each bounded $\forall E$ abbreviates a $\forall E$ and a $\rightarrow E$, and the bounded $\forall I$ box a $\forall I$ box with a $\rightarrow I$ box inside).

1	$\forall x \in A x \in B$	
2	$\exists M \forall b \in B b \leq M$	
3	$M_0 \mid \forall b \in B b \leq M_0$	asm, for $\exists E$
4	$a_0 \mid a_0 \in A$	asm, for $\forall I$
5	$a_0 \in B$	$\forall E$ 1, 4
6	$a_0 \leq M_0$	$\forall E$ 3, 5
7	$\forall a \in A a \leq M_0$	$\forall I$ 4–6
8	$\exists M \forall a \in A a \leq M$	$\exists I$ 7
9	$\exists M \forall a \in A a \leq M$	$\exists E$ 2, 3–8

The side conditions hold: a_0 appears in neither line 1 nor line 2, not in line 7 and not in the open assumption on line 3; M_0 appears in none of lines 1, 2 and 9.

Step 5: the constant. The witness for the goal is the bound M_0 . The search could choose it only once the $\exists E$ box supplied M_0 , and confirm it only at line 6; the page writes it first, in the sentence that chooses it. It depends on B only: its box is opened before the box of a_0 , so it cannot depend on a_0 , and it must not, because a single bound has to serve every element of A .

Step 6: level 3.

Suppose B is bounded above, and choose an upper bound M of B (depending on B only). Let $a \in A$. Since $A \subseteq B$, we have $a \in B$, and so $a \leq M$. Hence M is an upper bound of A , and A is bounded above.

The two instances of $\forall E$ (lines 5 and 6) are at the obvious term a , and each appears only as the citation that licenses it (“since $A \subseteq B$ ”, “so”, which cites the choice of M). The closing of the $\forall I$ box, “since a was arbitrary”, is silent. Two steps that are never silent are on the page: the $\exists E$ with its fresh name (“choose an upper bound M ”), and the $\exists I$ with its witness and dependence (“ M is an upper bound of A ”; “depending on B only”). “Suppose B is bounded above” opens the $\rightarrow I$ box; its closing is silent.

Step 7: reread. The order of the first two sentences matters. With “let $a \in A$ ” first and M chosen inside, the $\exists I$ would fall inside the box of a_0 , giving only $\forall a \in A \exists M (a \leq M)$, which

says nothing.

○ **Second reading** · *What the example used*

The example used $A \subseteq B$ once, at line 5, and “ B is bounded above” once, at line 9, by $\exists E$, whose box assumption is used at line 6. The two warnings below concern steps 4 and 5.

8.5.2.1 Scratch paper and the page

Steps 4 and 5 say that the search runs backwards and the page runs forwards. Here is the example’s search beside its page.

Scratch paper (from the goal, backwards)	The page (from the hypotheses, forwards)
1. Goal: an M with $a \leq M$ for every $a \in A$.	1. Suppose B is bounded above, and choose an upper bound M of B .
2. B bounded above gives some bound M : try it.	2. Let $a \in A$.
3. Need $a \leq M$ for an arbitrary $a \in A$.	3. Since $A \subseteq B$, $a \in B$.
4. That needs $a \in B$.	4. So $a \leq M$.
5. $a \in B$ comes from $A \subseteq B$. ✓	5. Hence M is an upper bound of A .

Read the scratch column from the bottom up and it is the page, except for the constant: M is found at scratch line 2, after the goal has been read, but on the page it is chosen in the first sentence, before anything uses it.

○ **Second reading** · *Why the page runs forwards*

Step 4 as a logical fact. The search of Section 3.1 opens a box for the goal before it knows how the box will be filled, and it postpones an existential goal until a witness appears; that is why it works backwards. But a derivation is a list in which line k cites only lines available at k (Definition 1.4.2), and a written proof is that list in sentences. So the order of the page is forced by the rules, not by taste: “ $|f(x) - f(a)| < \varepsilon$ holds if $|x - a| < \varepsilon/2$ ” points from a later line to an earlier one. The backward reasoning lives in the Idea block.

Step 5 as a logical fact. A chosen constant, such as “let $\delta := \varepsilon/2$ ”, is the witness of an $\exists I$ line. The search finds it last, because only the end of the search shows what it must do. On the page it comes first, right after the names it is built from, because later lines use it. Those names are its dependencies; they must be among the names of the boxes open where it is chosen (Section 6.4).

Warning. The search is not the proof. A page that reads “we want $x^2 < 4$; this holds if $x < 2$; so let $x < 2$ ” has copied the search, and each “holds if” points backwards. A backward step can be false, and the page hides it: “ $x < 2$ implies $x^2 < 4$ ” fails at $x = -3$. In scratch work every backward step must be checked as an implication pointing forwards; on the page

only the forward chain appears, each line citing lines above it.

Warning. A constant without its dependencies is a claim nobody can check. In a proof that x^2 is uniformly continuous on $\mathbb{R}$, the sentence “let $\delta := \min\{1, \varepsilon/(2|x| + 1)\}$ ” looks innocent. Asked “what does δ depend on?”, the formula answers: on ε **and on** x , so the δ was chosen inside the box of x , and the proof shows only continuity at every point. Uniform continuity is false here (Example (The square function on the real line)). Writing “(depending on ε only)” after the constant is what lets a reader catch the error.

Quick check. On the page, which sentence carries the witness of the final $\exists I$, and why can the choice of M not come after “Let $a \in A$ ”?

Solution. “Hence M is an upper bound of A ” offers M as the witness; it was chosen in sentence 1. Chosen after “Let $a \in A$ ”, M would sit inside the box of a , and the proof would give only $\forall a \in A \exists M (a \leq M)$, which says nothing (step 7 of the example).

Quick check. A writer’s scratch paper reads: “want $|3x - 6| < \varepsilon$ when $|x - 2| < \delta$; $|3x - 6| = 3|x - 2|$; so $\delta = \varepsilon/3$.” Write the first two sentences of the page.

Solution. “Let $\varepsilon > 0$, and let $\delta := \varepsilon/3$, which is positive and depends on ε only. Let x be a real number with $|x - 2| < \delta$.”

8.5.3 Conventions of written mathematics

A handful of conventions make a proof checkable. Each is a rule of Chapters 1–7 heard in a sentence.

- **Announce the skeleton.** “We prove the contrapositive”, “by induction on n ”, “we consider two cases”, “suppose, for a contradiction, that ...”. An announcement tells the reader which box is opening, and so what its last line must be.
- **Name every object when it is introduced,** by “let” (an arbitrary object, $\forall I$), “choose” (a witness, $\exists E$, with a fresh name), or “let ... := ...” (a constant, the witness of $\exists I$), and say what a chosen object depends on.
- **One claim per sentence.** A sentence carries one line, or a short chain of lines joined by “so”, each step of which the reader can name. Two unrelated claims joined by “and” hide which one is used later.
- **End with what was shown.** The last sentence of a proof states the goal, or the last line before only closings that Definition 8.3.2 lets be silent. If it is not the statement to be proved, the reader should be told how the two are related.
- **Label displayed claims that will be cited,** $(*)$ or (1) , and cite them by the label. A citation is a line number in prose.

None of these is a matter of style. An object used without being introduced is a line citing nothing, and an announcement that does not match its box (assuming the conclusion of an implication) proves the converse; these are entries (N9) and (N5) of the catalogue in Section 8.6.

8.5.4 Matching sentences and rules

The next two examples go in opposite directions.

Example. Label every sentence

Here is a short proof. Label each sentence with the rule it uses.

Claim. For a real number x , if $|x - 1| < 1$, then $x > 0$.

Proof. (1) Assume $|x - 1| < 1$. (2) Every real number is at least 1 or below it, so either $x \geq 1$ or $x < 1$. (3) Suppose first that $x \geq 1$. (4) Then $x \geq 1 > 0$. (5) Suppose instead that $x < 1$. (6) Then $x - 1 < 0$, so $|x - 1| = 1 - x$. (7) Hence $1 - x < 1$, that is, $x > 0$. (8) In either case $x > 0$, which proves the claim.

Solution.

Sentence	What it does	Rule
(1)	opens a box with the hypothesis	assumption for $\rightarrow$ I
(2)	states the disjunction the split needs	a fact about real numbers
(3)	opens the first case	assumption for $\vee$ E
(4)		algebra
(5)	opens the second case	assumption for $\vee$ E
(6)		algebra
(7)	uses the assumption of (1), whose box is still open	algebra
(8)	combines the cases, then closes the outer box	$\vee$ E on (2), (3)–(4), (5)–(7); then $\rightarrow$ I

Sentence (7) uses the assumption made in (1), and it may: that box is still open.

Measured against Definition 8.3.2, nothing that must be written is missing: the split is on the page with a disjunction that covers every real x , each case opens with its assumption, and what is left out may be silent. Labeling also shows where the work is: the case split exists only because $|\cdot|$ is defined by cases, and the school fact $-|u| \leq u$, used with $u = x - 1$, gives $-1 < x - 1$ in one step, with no $\vee$ E at all.

Sentence	What it does	Rule
(1)	opens a box with the hypothesis	assumption for $\rightarrow I$
(2)	states a fact about real numbers	a school fact, entered as a line
(3)	opens the first case box	assumption for $\forall E$
(4)	$x \geq 1$ and $1 > 0$ give $x > 0$	$\rightarrow E$, with the fact “ $a \geq b$ and $b > c$ imply $a > c$ ”
(5)	opens the second case box	assumption for $\forall E$
(6)	computes $ x - 1 $	$\rightarrow E$ twice, with the facts “ $x < 1$ implies $x - 1 < 0$ ” and “ $a < 0$ implies $ a = -a$ ”
(7)	uses the assumption of (1)	$=E$, putting (6) into (1), then $\rightarrow E$ with “ $1 - x < 1$ implies $x > 0$ ”
(8)	combines the cases, then closes the outer box	$\forall E$ on (2), (3)–(4), (5)–(7); then $\rightarrow I$ on (1)–(8)

The facts of school algebra enter as implications, each used by $\rightarrow E$. Sentence (8) closes two boxes, which is normal.

Measured against Definition 8.3.2, the proof leaves out nothing that must be written: the split in (2) is on the page, and the disjunction it splits is a school fact (every real number is at least 1 or below it), so it covers every case; each case box opens with its assumption; and every step it leaves unwritten is of a kind that may be silent, for instance the $\forall E$ instances of the school facts at the obvious terms, the conclusion $x > 0$ of case 1, which is left to the chain $x \geq 1 > 0$ of (4), the $\wedge I$ behind (4), whose conjuncts are displayed, the $=E$ of (7), and the closing of the $\rightarrow I$ box, for which “which proves the claim” stands. Labeling also shows where the work is. The case split exists only because $|\cdot|$ is defined by cases (Chapter 1); the school fact $-|u| \leq u$, used with $u = x - 1$, gives $-1 < x - 1$ in one step, and a proof written that way would have no $\forall E$ at all.

The second direction starts from a derivation whose premises are facts about integers.

Example. From a derivation to a paragraph

Let n be an integer. Write E for “ n is even”, O for “ n is odd”, F for “ $n + 1$ is even”, and G for “ $n(n + 1)$ is even”. The derivation below uses four facts about integers as premises. Write the paragraph a mathematician would write for it.

1	$E \vee O$	(every integer is even or odd)
2	$E \rightarrow G$	(an even factor makes a product even)
3	$O \rightarrow F$	(odd plus one is even)
4	$F \rightarrow G$	(an even factor again)
5	E	asm, for $\vee E$
6	G	$\rightarrow E$ 2, 5
7	O	asm, for $\vee E$
8	F	$\rightarrow E$ 3, 7
9	G	$\rightarrow E$ 4, 8
10	G	$\vee E$ 1, 5–6, 7–9

Solution.

Every integer is even or odd, so we consider two cases. If n is even, then $n(n+1)$ has an even factor, and so it is even. If n is odd, then $n+1$ is even, since an odd number plus one is even; so again $n(n+1)$ has an even factor and is even. In either case $n(n+1)$ is even.

Compare the two. The paragraph keeps one sentence for each box and each rule that matters: line 1 becomes “we consider two cases”, with its reason; the two boxes become the two “if” sentences; line 10 becomes “in either case”. It drops the line numbers and the rule names, and it merges the two $\rightarrow E$ steps of lines 8 and 9 into one sentence joined by “so”. It never skips a box: the reader still sees both cases and sees them combined.

By Definition 8.3.2, the closing “in either case ...” could be dropped at level 3; the split of line 1, with the reason it covers every integer, could not. The paragraph leaves the premises unproved. Premises 2–4 are one line of algebra each (for instance, $n = 2k$ gives $n(n+1) = 2(k(n+1))$), and a careful write-up includes them; premise 1, that every integer is even or odd, is the fact (E1) that this volume takes as known.

8.5.5 Generalizing a proof

A proof written about one object sometimes proves much more. To **generalize** it, replace the object by a fresh name, the move of $\forall I$ (Section 5.4), and read every line again. A line that uses only what the new name’s box assumes stays. A line that uses a property of the particular object must be proved again, or the generalization fails.

Example. One of three, generalized

Here are two proofs that one of 17, 18, 19 is a multiple of 3. (P1) $18 = 3 \cdot 6$. (P2) $17 = 3 \cdot 5 + 2$, so $17 + 1 = 3 \cdot 6$. Which one generalizes to “for every integer n , one of n , $n+1$, $n+2$ is a multiple of 3”? Write the general proof.

Solution. (P1) does not generalize: it uses a fact about 18 alone. (P2) does, once its one particular fact, $17 = 3 \cdot 5 + 2$, is replaced by what every integer has: $n = 3k$, $n = 3k + 1$ or $n = 3k + 2$ for an integer k , a school fact.

Let n be an integer [assumption for $\forall I$]. Dividing by 3, there is an integer k with $n = 3k$, $n = 3k + 1$ or $n = 3k + 2$; choose such a k [$\exists E$]. If $n = 3k$, n is a multiple of 3. If $n = 3k + 1$, then $n + 2 = 3(k + 1)$. If $n = 3k + 2$, then $n + 1 = 3(k + 1)$. In every case one of the three is a multiple of 3 [$\vee E$]. Since n was arbitrary, this holds for every integer [$\forall I$].

(P2) was the third case, with $k = 5$.

The test: after renaming, can every line still be justified from what the box of n assumes? A line that computes with the particular number fails the test.

Quick check. A proof that $7^2 - 1$ is divisible by 8 reads “ $7^2 - 1 = 48 = 8 \cdot 6$ ”. Does it generalize to every odd n ? What would?

Solution. No: it computes with 7. A general proof writes $n = 2k + 1$, so $n^2 - 1 = 4k(k + 1)$, and shows that $k(k + 1)$ is even, since one of k , $k + 1$ is even. That is the proof of Exercise (B2: Back from prose to a skeleton, with blanks).

8.5.6 Exercises

8.5.6.1 A. Check your understanding

Exercise. A1

Here is a proof.

Claim. For real numbers x and y , if $x + y > 2$, then $x > 1$ or $y > 1$.

(1) Assume $x + y > 2$. (2) Suppose, for a contradiction, that it is not the case that $x > 1$ or $y > 1$. (3) Then $x > 1$ fails and $y > 1$ fails. (4) So $x \leq 1$ and $y \leq 1$. (5) Adding, $x + y \leq 2$. (6) This contradicts $x + y > 2$. (7) Hence $x > 1$ or $y > 1$, which proves the claim.

- Label each sentence with the rule it uses, as in [Example \(Label every sentence\)](#).
- Which sentence closes an RAA box, and which uses one of De Morgan’s laws (Proposition 2.5.5)? Which law?
- Everything inside the box of (2) follows from (2) alone, until the clash in (6). Which face of “by contradiction” (Section 8.1) does the proof wear, and which face is it really? Write the first sentence of the rewritten proof.
- Sentence (7) closes two boxes. Which of the two closings may be silent at level 3, by Definition 8.3.2?

Solution. (a)

Sentence	Rule
(1)	assumption, opening the $\rightarrow$ I box
(2)	assumption $\neg(x > 1 \vee y > 1)$, opening an RAA box
(3)	Proposition 2.5.5 (a), $\neg(P \vee Q) \vdash \neg P \wedge \neg Q$, applied to (2)
(4)	$\wedge$ E on (3), twice; $\rightarrow$ E with the order fact “ $\neg(a > 1)$ implies $a \leq 1$ ”, twice; then $\wedge$ I
(5)	$\wedge$ E on (4), then $\rightarrow$ E with “ $a \leq 1$ and $b \leq 1$ imply $a + b \leq 2$ ”
(6)	$\rightarrow$ E with the order fact “ $a \leq 2$ implies $\neg(a > 2)$ ” on (5), then $\neg$ E on (1) and the result
(7)	RAA on the box (2)–(6); then $\rightarrow$ I on (1)–(7)

(b) Sentence (7) closes the RAA box: the box opened with the negation of the goal $x > 1 \vee y > 1$ and closes with the goal itself. Sentence (3) uses De Morgan’s law (a), a direction derived without RAA.

(c) It wears face (iii), genuine RAA, but it is a contrapositive in costume, as in Example (A contrapositive in costume): the hypothesis (1) is used only at the clash, and everything else derives $x + y \leq 2$ from $x \leq 1$ and $y \leq 1$. The rewrite opens: “We prove the contrapositive: if $x \leq 1$ and $y \leq 1$, then $x + y \leq 2$.” The rewrite is clearer, but it does not remove the classical step: passing from the contrapositive back to the claim is Proposition 2.5.2, which uses RAA.

(d) The closing of the $\rightarrow$ I box (“so if $x + y > 2$, then ...”) may be silent. The conclusion of the RAA box, “hence $x > 1$ or $y > 1$ ”, may not.

Exercise. A2: Drill

Answer each part in a line. The parts follow the procedure: (a)–(b) symbols and unwinding, (c)–(d) the skeleton, (e) the order on the page, (f), (g), (i) the conventions, (h) the search and the page, (j)–(k) generalizing, (l) the Givens/Goal table.

- Write in symbols, with every quantifier and bound: “the square of every odd integer is odd” (domain $\mathbb{Z}$).
- Unwind “the sequence (a_n) is bounded” (Section 5.6).
- The goal is $\forall \varepsilon > 0 \exists \delta > 0 \forall x (|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon)$. What are the first and the last line of the outer box?
- A hypothesis says “some integer k has $n = 2k + 1$ ”. When does its box open?
- On the page, which comes first: “let $\delta := \varepsilon/4$ ” or “let x be a real number with $|x - 1| < \delta$ ”?
- “ x is positive and y is negative, and so $xy < 0$ and $x - y > 0$.” Which convention does this break?

- (g) A proof uses c in its fourth sentence, and c appears nowhere before. Which convention, and which entry of Section 8.6?
- (h) Is “this holds if $x < 2$ ” a sentence of the page?
- (i) Claim: $x^2 - 4x + 3 < 0$ for $1 < x < 3$. A proof ends “... so $x^2 - 4x + 3 = (x - 1)(x - 3)$.” What is missing?
- (j) A proof about the number 12 uses only “12 is a multiple of 4”. For which integers does the same proof prove the same claim?
- (k) A proof about “an arbitrary odd n ” uses $n > 0$ in one line. What does it prove?
- (l) Givens $\forall x \in A (x \in B)$ and $\forall x \in B (x \in C)$; Goal $\forall x \in A (x \in C)$. Write the next row of the Givens/Goal table.

Solution.

- (a) $\forall n (\exists k (n = 2k + 1) \rightarrow \exists j (n^2 = 2j + 1))$.
- (b) $\exists M \in \mathbb{R} \forall n \in \mathbb{N} (|a_n| \leq M)$.
- (c) First: the assumption $\varepsilon_0 > 0$, “Let $\varepsilon > 0$ ” (assumption for $\forall I$). Last: $\exists \delta > 0 \forall x (|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon_0)$, by $\exists I$ with the chosen δ .
- (d) At once (step 3): an $\exists E$ box with a fresh name k .
- (e) The constant (step 5). The box of x needs δ ; chosen after x , δ could depend on x .
- (f) One claim per sentence: two claims joined by “and” hide which one is used later.
- (g) Name every object when it is introduced; (N9), a line that cites nothing.
- (h) No. It points backwards, from the goal, and belongs to scratch work or the Idea (step 4).
- (i) The end: $x - 1 > 0$ and $x - 3 < 0$, so the product is negative. The last sentence must be the claim (end with what was shown).
- (j) For every multiple of 4: rename 12 to a fresh n , with the assumption $4 \mid n$.
- (k) Only the claim for positive odd n . For all odd n , the box would have to assume no more than oddness, so that line must be proved again without $n > 0$.
- (l) Givens: the same, and $a_0 \in A$ ($\forall I$, a_0 fresh). Goal: $a_0 \in C$.

8.5.6.2 B. Practice

Exercise. B1: From skeleton to prose

Each part gives a statement and a level-1 skeleton of its proof. Write the proof at level 3, keeping every step that Definition 8.3.2 says is never silent.

- (a) For every integer n , if n is odd, then $3n + 5$ is even. (Domain $\mathbb{Z}$.)

1	n_0	$\exists k (n_0 = 2 \cdot k + 1)$	asm, for $\rightarrow$ I
2		$k_0 \mid n_0 = 2 \cdot k_0 + 1$	asm, for $\exists$ E
3		$3 \cdot n_0 + 5 = 2 \cdot (3 \cdot k_0 + 4)$	arith 2
4		$\exists k (3 \cdot n_0 + 5 = 2 \cdot k)$	$\exists$ I 3
5		$\exists k (3 \cdot n_0 + 5 = 2 \cdot k)$	$\exists$ E 1, 2–4
6		$\exists k (n_0 = 2 \cdot k + 1) \rightarrow \exists k (3 \cdot n_0 + 5 = 2 \cdot k)$	$\rightarrow$ I 1–5
7	$\forall n (\exists k (n = 2 \cdot k + 1) \rightarrow \exists k (3 \cdot n + 5 = 2 \cdot k))$		$\forall$ I 1–6

(b) No real number x satisfies $x^2 + 1 = 2x - 1$. (Domain $\mathbb{R}$.)

1		$\exists x (x^2 + 1 = 2 \cdot x - 1)$	asm, for $\neg$ I
2	x_0	$x_0^2 + 1 = 2 \cdot x_0 - 1$	asm, for $\exists$ E
3		$(x_0 - 1)^2 + 1 = 0$	arith 2
4		$(x_0 - 1)^2 \geq 0$	arith
5		$1 \leq 0$	arith 3, 4
6		$\neg(1 \leq 0)$	arith
7		$\perp$	$\neg$ E 5, 6
8		$\perp$	$\exists$ E 1, 2–7
9		$\neg \exists x (x^2 + 1 = 2 \cdot x - 1)$	$\neg$ I 1–8

(c) For a real number x : $x^3 = x$ if and only if $x = -1$, $x = 0$ or $x = 1$. (Here x is fixed; “or” chains group to the right.)

1		$x^3 = x$	asm, for $\leftrightarrow$ I
2		$(x + 1) \cdot (x \cdot (x - 1)) = 0$	arith 1
3		$x = -1 \vee (x = 0 \vee x = 1)$	product zero, arith 2
4		$x = -1 \vee (x = 0 \vee x = 1)$	asm, for $\leftrightarrow$ I
5		$x = -1$	asm, for $\vee$ E
6		$x^3 = x$	arith 5
7		$x = 0 \vee x = 1$	asm, for $\vee$ E
8		$x = 0$	asm, for $\vee$ E
9		$x^3 = x$	arith 8
10		$x = 1$	asm, for $\vee$ E
11		$x^3 = x$	arith 10
12		$x^3 = x$	$\vee$ E 7, 8–9, 10–11
13		$x^3 = x$	$\vee$ E 4, 5–6, 7–12
14		$x^3 = x \leftrightarrow (x = -1 \vee (x = 0 \vee x = 1))$	$\leftrightarrow$ I 1–3, 4–13

Hint: line 3 of (c) uses the school fact that a product of real numbers is zero only if one of its factors is zero.

Solution. (a) Let n be an integer, and suppose n is odd. Choose an integer k with $n = 2k + 1$. Then

$$3n + 5 = 6k + 3 + 5 = 2(3k + 4),$$

and $3k + 4$ is an integer, so $3n + 5$ is even.

“Choose an integer k ” is the $\exists E$ box, with a fresh name; the witness $3k + 4$ of line 4 is on the page, and it depends on k , hence on n . Lines 5, 6 and 7 close boxes and are silent.

(b) Suppose, to the contrary, that some real x satisfies $x^2 + 1 = 2x - 1$, and fix such an x . Rearranging, $x^2 - 2x + 2 = 0$, that is, $(x - 1)^2 + 1 = 0$. But $(x - 1)^2 \geq 0$, since a square is non-negative, so $1 \leq 0$, which is false. Hence no real x satisfies the equation.

“Suppose, to the contrary” opens the $\neg I$ box of line 1 (the goal is a negation, so no classical rule is used), and “fix such an x ” the $\exists E$ box. The clash of lines 5–7 is named, and the conclusion of the $\neg I$ box is written; line 8 is silent.

(c) Let x be real.

($\Rightarrow$) Suppose $x^3 = x$. Then $(x + 1)x(x - 1) = x^3 - x = 0$. A product of real numbers is zero only if a factor is zero, so $x + 1 = 0$, $x = 0$ or $x - 1 = 0$; that is, $x = -1$, $x = 0$ or $x = 1$.

($\Leftarrow$) Suppose $x = -1$, $x = 0$ or $x = 1$. In the three cases, $x^3 = -1 = x$, $x^3 = 0 = x$ and $x^3 = 1 = x$.

This proves the equivalence.

Both directions are written, and the citation in line 3 is visible. The two splits of ($\Leftarrow$) are merged into “in the three cases”; the disjunction split is the hypothesis itself, and the closing lines 12 and 13 are silent.

Exercise. B2: Put the proof in order

Let (a_n) and (b_n) be sequences of real numbers with $a_n \rightarrow L$ and $b_n \rightarrow M$, where “ $a_n \rightarrow L$ ” is the pattern of Section 6.1: for every $\varepsilon > 0$ there is $N \in \mathbb{N}$ such that $|a_n - L| < \varepsilon$ for every $n \geq N$. Eight of the ten sentences below, in a suitable order, form a level-3 proof that $a_n + b_n \rightarrow L + M$; two are distractors. Write down an order for the eight, say which other orders are also admissible, and say why each distractor is wrong.

- (i) Let $n \in \mathbb{N}$ with $n \geq N$.
- (ii) Since $b_n \rightarrow M$ and $\varepsilon/2 > 0$, choose $N_2 \in \mathbb{N}$ (depending on ε) such that $|b_n - M| < \varepsilon/2$ for every $n \geq N_2$.
- (iii) Let $N := \max\{N_1, N_2\}$, where N_1 and N_2 serve every ε at once.
- (iv) Then $n \geq N_1$ and $n \geq N_2$.
- (v) Let $\varepsilon > 0$.
- (vi) Since $n \geq N$ and $\varepsilon > 0$ were arbitrary, $a_n + b_n \rightarrow L + M$.
- (vii) Choose $N_1 \in \mathbb{N}$ such that $|a_n - L| < \varepsilon$ for every $n \geq N_1$.
- (viii) Let $N := \max\{N_1, N_2\}$.

- (ix) So $|(a_n + b_n) - (L + M)| \leq |a_n - L| + |b_n - M| < \varepsilon/2 + \varepsilon/2 = \varepsilon$.
 (x) Since $a_n \rightarrow L$ and $\varepsilon/2 > 0$, choose $N_1 \in \mathbb{N}$ (depending on ε) such that $|a_n - L| < \varepsilon/2$ for every $n \geq N_1$.

Solution. An admissible order: (v), (x), (ii), (viii), (i), (iv), (ix), (vi).

The only other admissible order swaps (x) and (ii), which use only ε and one hypothesis each. Nothing else moves: (viii) uses N_1 and N_2 ; (i) uses N ; (iv) uses $n \geq N$ and the definition of N ; (ix) uses (iv), (x) and (ii) at this n , and the triangle inequality (Example (The triangle inequality by cases)); (vi) closes the boxes of n and ε , with the $\exists I$ of the witness N inside “ $a_n + b_n \rightarrow L + M$ ”. The maximum exists because there are finitely many numbers.

Distractor (iii) claims that N_1 and N_2 serve every ε at once. They were chosen from $\forall \varepsilon \exists N$, inside the box of ε , so they depend on ε and serve only the ε they were chosen for; a uniform N would need $\exists N \forall \varepsilon$, which the hypothesis does not give. This is the error that Section 8.6 catalogues as (N2). For $a_n = 1/(n + 1)$, $L = 0$, no single N_1 serves every $\varepsilon > 0$: at $\varepsilon = 1/(N_1 + 2)$ the term $a_{N_1} = 1/(N_1 + 1)$ is too far from 0.

Distractor (vii) applies the hypothesis at ε instead of $\varepsilon/2$. It is a legal step, but with it in place of (x), the bound in (ix) becomes $|(a_n + b_n) - (L + M)| < \varepsilon + \varepsilon/2$, not $< \varepsilon$, so (ix) would no longer follow. It is an ε of the wrong kind for the goal.

Exercise. B3: The last step

Here is a level-1 skeleton for the statement “for real numbers x and y , if x is rational and y is irrational, then $x + y$ is irrational”, with x and y fixed:

1	$x \in \mathbb{Q} \wedge \neg(y \in \mathbb{Q})$	asm, for $\rightarrow I$
2	$x \in \mathbb{Q}$	$\wedge E$ 1
3	$\neg(y \in \mathbb{Q})$	$\wedge E$ 1
4	$x + y \in \mathbb{Q}$	asm, for $\neg I$
5	$(x + y) - x \in \mathbb{Q}$	difference of rationals 4, 2
6	$y \in \mathbb{Q}$	arith 5
7	$\perp$	$\neg E$ 6, 3
8	$\neg(x + y \in \mathbb{Q})$	$\neg I$ 4–7
9	$x \in \mathbb{Q} \wedge \neg(y \in \mathbb{Q}) \rightarrow \neg(x + y \in \mathbb{Q})$	$\rightarrow I$ 1–8

and its level-3 prose, with the closing sentence of the $\neg I$ box left blank:

Let x be rational and y irrational. Suppose $x + y$ is rational. Then $y = (x + y) - x$ is a difference of two rational numbers, so y is rational. This contradicts the irrationality of y . _____

Name the move, then complete it.

Solution. The move is skeleton first: the blank is line 8, the line written after the $\neg I$ box of lines 4–7 closes, a line the skeleton fixes before any arithmetic. That box assumed “ $x + y$ is rational” and reached $\perp$ at line 7, so line 8 concludes its negation. It is the first face of “by contradiction” (Section 8.1), proof of a negative statement, and uses no classical rule: “irrational” means “not rational”, so the goal of the outer box, line 8, is a negation, and the inner box is opened on $x + y \in \mathbb{Q}$ with goal $\perp$.

Completion. “Hence $x + y$ is not rational, that is, $x + y$ is irrational.”

The conclusion of a $\neg I$ box is never silent (Definition 8.3.2), so this sentence must be written even though the reader can guess it. Line 9, the closing of the $\rightarrow I$ box, may stay silent. The sentence before the blank, “this contradicts the irrationality of y ”, is line 7, the clash of $\neg E$, which names both lines it cites.

Exercise. B4: Which proof generalizes?

Two proofs that 6 divides $7^3 - 7 = 336$:

(P1) “ $336 = 6 \cdot 56$.”

(P2) “ $7^3 - 7 = 6 \cdot 7 \cdot 8$, a product of three consecutive integers; one of them is even and one is a multiple of 3, so 6 divides the product.”

- Which proof generalizes to “for every integer n , $6 \mid n^3 - n$ ”, and why does the other not?
- Write the general proof at level 3, with its fresh name and every fact it uses.
- Which fact about 6 does (P2) leave unstated?

Solution. (a) (P2) generalizes; (P1) computes with 7 and says nothing about another n .

(b) Let n be an integer. Then $n^3 - n = (n - 1)n(n + 1)$, a product of three consecutive integers. By [Example \(One of three, generalized\)](#), applied to $n - 1$, one of $n - 1$, n , $n + 1$ is a multiple of 3, so $3 \mid n^3 - n$ (a product with a factor divisible by d is divisible by d : if $a = dc$, then $ab = d(cb)$). By (E1), n is even or odd: if n is even, the factor n is even; if odd, $n - 1$ is even. So one factor is even, and $2 \mid n^3 - n$. Since 2 and 3 divide it, so does 6 (by Exercise (B3: Six, two and three, used later), the inclusion $\supseteq$: if $m = 2a = 3b$, then $b = 2(a - b)$ and $m = 6(a - b)$).

(c) “If $2 \mid m$ and $3 \mid m$, then $6 \mid m$ ”, the fact of Exercise (B3: Six, two and three, used later).

Marking scheme. (10 points) - 2: (a) (P2), with the reason (P1) fails. - 2: (b) the factorization and the fresh name. - 2: (b) a multiple of 3 among the factors, cited or proved. - 2: (b) an even factor, from (E1). - 1: (b) the step from 2 and 3 to 6, proved or cited. - 1: (c) the fact named. Fatal errors (0 for the step): a proof that checks finitely many n (N1); “ $2 \mid m$ and $3 \mid m$, so $6 \mid m$ ” with neither proof nor citation (N9).

8.5.6.3 C. Going deeper

Exercise. C1: A constant found backwards

Let $f(x) = 2x + 3$ and let a be a fixed real number. Prove that for every $\varepsilon > 0$ there is $\delta > 0$ such that $|f(x) - f(a)| < \varepsilon$ for every real x with $|x - a| < \delta$. Write your answer as an Idea, which finds δ backwards, followed by a Proof, which runs forwards. Say what δ depends on.

Solution (Hint 1). Compute $|f(x) - f(a)|$ in terms of $|x - a|$ before choosing anything.

Solution (Hint 2). The Proof begins: “Let $\varepsilon > 0$, and let $\delta := \dots$ ”.

Solution. Idea. We want $|f(x) - f(a)| < \varepsilon$. Compute: $f(x) - f(a) = (2x + 3) - (2a + 3) = 2(x - a)$, so $|f(x) - f(a)| = 2|x - a|$. This is below ε exactly when $|x - a| < \varepsilon/2$. So $\delta = \varepsilon/2$ should work, and it does not involve x or a .

Proof. Let $\varepsilon > 0$, and let $\delta := \varepsilon/2$, which is positive and depends on ε only. Let x be a real number with $|x - a| < \delta$. Then

$$|f(x) - f(a)| = |2(x - a)| = 2|x - a| < 2\delta = \varepsilon.$$

Since x was arbitrary, δ works for ε ; since $\varepsilon > 0$ was arbitrary, this proves the claim.

The Idea reads the computation from the goal back to $|x - a|$; the Proof places δ right after ε , before any x appears, and justifies it by the final display. Because δ does not depend on a either, the same proof shows that one δ serves every point: f is uniformly continuous on $\mathbb{R}$, in the sense of Section 6.4.

Marking scheme. (10 points) - 2: an Idea that computes $|f(x) - f(a)| = 2|x - a|$ and reads off δ from the goal. - 2: the Proof opens with $\varepsilon > 0$ arbitrary and introduces δ before any x , with $\delta > 0$ checked. - 2: says what δ depends on (ε only, or ε and a if the choice involves a). - 3: for arbitrary x with $|x - a| < \delta$, the forward chain to $|f(x) - f(a)| < \varepsilon$, each step justified. - 1: a closing sentence with the quantifiers in the order ε, δ, x . Any δ with $0 < \delta \leq \varepsilon/2$ earns full marks. Fatal errors (0 for the step): δ depending on x ; a Proof that runs backwards (“this holds if ...”).

Exercise. C2: Rewrite it properly

A sequence (a_n) is **bounded** if there is $M \in \mathbb{R}$ with $|a_n| \leq M$ for every $n \in \mathbb{N}$ (Section 5.6). The following proof that a sequence (a_n) with $a_n \rightarrow L$ is bounded is correct in substance but badly written.

We want some M with $|a_n| \leq M$. For big n , a_n is near L , so $|a_n|$ is less than $|L| + 1$ if we use 1 for ε . The small n are only finitely many, so take the biggest. So M is the max of all of them and it works.

- Name three faults of the text, each by the convention it breaks (this section) or the step that is not written.
- Rewrite the proof at level 3.

Solution (Hint 1). Which objects does the text use without introducing them, and what does each depend on?

Solution (Hint 2). The rewrite begins: “Apply the definition of $a_n \rightarrow L$ with $\varepsilon = 1$, and choose $N \in \mathbb{N}$ such that ...”.

Solution. (a) (i) It writes the search: “we want some M ” and “if we use 1 for ε ” describe what is being looked for, not lines that follow. (ii) It uses objects without introducing them: “big n ” hides an N , obtained from the hypothesis at $\varepsilon = 1$ by $\forall E$ and $\exists E$, which is never named; “the biggest” does not say of which numbers. (iii) It never says what M is or what it depends on: M is built from the finitely many terms before N , so it depends on N . (Also acceptable: the split into small and big n has no stated reason; the last sentence does not say what was shown.)

(b) Apply the definition of $a_n \rightarrow L$ with $\varepsilon = 1$, and choose $N \in \mathbb{N}$ such that $|a_n - L| < 1$ for every $n \geq N$. Let

$$M := \max\{|a_0|, |a_1|, \dots, |a_{N-1}|, |L| + 1\},$$

the largest of finitely many numbers, so it exists; it depends on N (when $N = 0$ the list is just $|L| + 1$). Let $n \in \mathbb{N}$. Either $n < N$ or $n \geq N$, since every natural number is one or the other. If $n < N$, then $|a_n|$ is in the list, so $|a_n| \leq M$. If $n \geq N$, then by the triangle inequality (Example (The triangle inequality by cases))

$$|a_n| = |(a_n - L) + L| \leq |a_n - L| + |L| < 1 + |L| \leq M.$$

In either case $|a_n| \leq M$. Hence (a_n) is bounded.

The $\forall E$ instance $\varepsilon = 1$ is named, because it is not the obvious one; the witness M of the final $\exists I$ is defined before it is used, with its dependence; the split on $n < N$ or $n \geq N$ carries its reason (every natural number is one or the other).

Marking scheme. (10 points) - 3: (a) three genuine faults, each tied to a convention or an unwritten step (1 each). - 2: (b) applies the hypothesis at a named positive ε and chooses N from it. - 2: defines M before using it, with its dependence on N , bounding the early terms and $|L| + \varepsilon$ (a maximum or a sum). - 2: the two cases $n < N$ and $n \geq N$, the second by the triangle inequality (cited) or an equivalent estimate from $|a_n - L| < \varepsilon$, such as $L - \varepsilon < a_n < L + \varepsilon$ and a split on the sign of a_n . - 1: ends with what was shown. Fatal errors (0 for the step): M chosen before N or as a maximum or sum of infinitely many numbers; the early terms omitted.

Exercise. C3: From $\sqrt{2}$ to $\sqrt{3}$, and not to $\sqrt{4}$

The level-3 proof of Theorem 2.2.1 in Example (The irrationality of the square root of two at four levels) uses (L) and Theorem 2.1.3.

- (a) Rewrite it as a proof that no rational number has square 3. You may use (L₃): every rational number is p/q with integers p, q , $q \neq 0$, not both multiples of 3. Prove the lemma your proof needs in place of Theorem 2.1.3.

- (b) Rewrite it once more for 4, with (L₄): every rational number is p/q with integers p, q , $q \neq 0$, not both multiples of 4, which is true. Which line fails? Why must some line fail?
- (c) Say in one sentence what a generalization keeps and what it must prove again.

Solution (Hint 1). The lemma is “if $3 \mid n^2$, then $3 \mid n$ ”. Split on the remainder of n on division by 3.

Solution (Hint 2). Let r be rational, and suppose $r^2 = 3$. By (L₃), write $r = p/q$ with integers p, q , not both multiples of 3.

Solution. (a) *Lemma:* if $3 \mid n^2$, then $3 \mid n$. Write $n = 3k, 3k + 1$ or $3k + 2$. In the first case $3 \mid n$. Otherwise $n^2 = 3(3k^2 + 2k) + 1$ or $n^2 = 3(3k^2 + 4k + 1) + 1$, and a number $3j + 1$ is not a multiple of 3: from $3j + 1 = 3t$ we get $3(t - j) = 1$, and no integer is $\frac{1}{3}$. So those cases clash with $3 \mid n^2$, and $3 \mid n$ holds in each by $\perp E$.

The proof. “Let r be rational, and suppose $r^2 = 3$. By (L₃), write $r = p/q$ with integers p, q , not both multiples of 3. Then $p^2 = 3q^2$, so $3 \mid p^2$, and by the lemma $3 \mid p$. Writing $p = 3m$ gives $9m^2 = 3q^2$, so $q^2 = 3m^2$, and by the lemma $3 \mid q$. So p and q are both multiples of 3, a contradiction; hence $r^2 \neq 3$.”

(b) The line “ $p^2 = 4q^2$, so $4 \mid p^2$, and by the lemma $4 \mid p$ ” fails: “if $4 \mid n^2$, then $4 \mid n$ ” is false at $n = 2$. Some line must fail, because the claim is false: $4 = (2/1)^2$, and $p = 2, q = 1$ satisfy (L₄). Lines that are all licensed, from true premises, cannot reach a false conclusion (soundness: Theorem 4.7.2, and the statement of Section 7.2 under “From counter-models to non-derivability” for the quantifier steps).

(c) A generalization keeps the skeleton (the boxes, the choices, the clash) and every line that used only properties shared by the new object; it must prove again each line that used a property of the old one, here the lemma.

Marking scheme. (10 points) - 3: (a) the lemma proved by the residues mod 3, with the clash $3j + 1 \neq 3t$ justified. - 2: (a) the rest of the proof, with (L₃) and the lemma used twice. - 2: (b) the failing line named, with the counterexample $n = 2$. - 1: (b) why a line must fail ($\sqrt{4} = 2$ is rational). - 2: (c) skeleton kept, particular lines re-proved. Fatal errors (0 for the step): the lemma asserted without proof (N9); in (b), blaming (L₄).