

Proofs from Definitions: Sets and Functions

Every definition of analysis is a sentence about sets and functions. “The supremum of A is the least element of the set of upper bounds of A .” “A function is continuous if the preimage of every open set is open.” *Logic and Proof*, Chapters 1 to 8 supplied the grammar of such sentences: the connectives, the quantifiers, and the prose that carries their rules. This chapter supplies the nouns: sets and subsets, unions and intersections of whole families of sets, ordered pairs and products, relations, functions, inverses, images and preimages. It is also where proofs start being about mathematics rather than about logic: each section teaches one method of proof on the material it introduces, starting in Section 1.1 with statements about integers proved straight from their definitions. And it is where the logic of the first eight chapters becomes visible inside mathematics. Inclusion is a “for every” around an “implies”, a union is an “or”, the union of a family is a “there exists”, and a function is a “for every there exists exactly one”. *The laws of sets are the laws of logic, read through membership*, and the chapter uses this from its second section to its last.

Two surprises drive the chapter. The first is that the naive rule “any property defines a set” is contradictory (Russell’s paradox), so we must say which sets exist, and every set in this book is cut out of a set already given. The second is the chapter’s motivating problem. *For $f(x) = x^2$, is $f(A \cap B) = f(A) \cap f(B)$? Is $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$? Why is the second always true and the first not?* The answer is a single quantifier: membership in an image hides a “there exists”, and membership in a preimage hides nothing. Preimages therefore respect every set operation, and images only unions. This asymmetry is why analysis defines continuity by preimages.

What you need. *Logic and Proof*, Chapters 1–8. From *Logic and Proof*, Chapters 1 and 2: the rules for the connectives and the derived laws used as rules, above all distributivity (Logic and Proof, Proposition 1.6.1), De Morgan’s laws (Logic and Proof, Proposition 2.5.5), an iff as two implications (Logic and Proof, Proposition 2.4.1), the contrapositive (Logic and Proof, Proposition 2.3.2), vacuous implication (Logic and Proof, Proposition 2.1.2), and derived rules (Logic and Proof, Definition 2.3.1). From *Logic and Proof*, Chapter 4: induction (Logic and Proof, Axiom 4.2.1), the standard equivalences (Logic and Proof, Proposition 4.5.1) and completeness (Logic and Proof, Theorem 4.8.4). From *Logic and Proof*, Chapters 5 and 6: the rules for “for every” and “there exists”, bounded quantifiers (Logic and Proof, Definition 5.1.1) and their rules (Logic and Proof, Proposition 6.1.1), the rules for equality (Logic and Proof, Definition 5.7.1), unique existence (Logic and Proof, Definition 5.8.1, Logic and Proof, Proposition 5.8.1), and the laws for negating quantifiers. From *Logic and Proof*, Chapter 8: plain-prose proofs, the convention on which steps may be silent, and the catalogue of what is not allowed (Logic and Proof, Example (What is not allowed)). The number sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ are used as familiar sets, with their school arithmetic and order.

Time. About 40 hours on the core track (all of A, one B and one C per section, the exit checks); about 55 hours for everything.

1.-1.1 Roadmap

- **Proofs from definitions.** Even, odd, divides and prime; a direct proof unwinds a definition and rewinds another; proofs by cases and without loss of generality; refuting a claim by one counterexample; a puzzle about lattice points that the book finishes in Chapter 2.
- **Sets, subsets and Russell’s paradox.** What a set is allowed to be, equality by ele-

ments, the subset relation and the element-chasing proofs that establish it, equality by two inclusions, describing sets by a property cut out of an ambient set, the empty set, and why no set contains every set.

- **Unions, intersections, complements and families.** The set operations as the connectives read through membership, laws of sets proved by a chain of equivalences, the algebra of sets as propositional logic, power sets, unions and intersections of arbitrary families, and De Morgan’s laws for families, including the empty one.
- **Ordered pairs, products and relations.** An object that remembers order, proofs of existence and uniqueness, the product $A \times B$ and how it interacts with the set operations, and relations as sets of pairs.
- **Functions, composition, injections and surjections.** A function as a graph with a declared target, when two functions are equal, composition, and the two questions of injectivity and surjectivity, each with its method of proof (the second solved backwards and proved forwards), with the squaring map as three different functions.
- **Left, right and two-sided inverses.** Proofs that construct an object and then verify it: a left inverse exists exactly for injective maps (on a nonempty domain), a right inverse forces surjectivity, bijections are the maps with a two-sided inverse, and the question whether every surjection has a right inverse, which needs a new principle.
- **Images and preimages.** What a function does to sets, why preimages respect every operation and images only unions, where injectivity and surjectivity repair the failures, how to hunt for a counterexample, and sets of numbers such as $-A$ and $A + B$ as images.

1.-1.2 Named moves

The first ten are method boxes; each section that introduces one cites it from then on.

- **Direct proof from a definition** (Example (Method: direct proof from a definition)). Unwind the hypothesis into its definition, naming each witness; say what the goal demands; close the gap by computation; write it forwards. (Section 1.1)
- **Proof by cases** (Example (Method: proof by cases)). Split on a disjunction you already have, such as even or odd, and reach the same goal in every case; “without loss of generality” when the cases are symmetric. (Section 1.1)
- **Disproof by counterexample, proof by example** (Example (Method: disproof by counterexample, proof by example)). One instance refutes a “for every”; one witness proves a “there exists”. (Section 1.1)
- **Element-chasing** (Example (Method: element-chasing)). To prove $A \subseteq B$: “let $x \in A$ ”, unwind the definition of A , and rewind into the definition of B . (Section 1.2)
- **Two inclusions** (Example (Method: two inclusions)). To prove $A = B$: prove $A \subseteq B$ and $B \subseteq A$. (Section 1.2)
- **A chain of equivalences** (Example (Method: a chain of equivalences)). For $L = R$: $x \in L \iff \dots \iff x \in R$, each step a definition or a named law of logic. (Section 1.3)
- **Existence and uniqueness** (Example (Method: existence and uniqueness)). Produce one object, then show that any two are equal. (Section 1.4)
- **Proving injectivity** (Example (Method: proving injectivity)). From $f(x_1) = f(x_2)$, derive $x_1 = x_2$. (Section 1.5)
- **Proving surjectivity** (Example (Method: proving surjectivity)). Solve $f(x) = y$ backwards on scrap paper; prove forwards: “let $y \in Y$; put $x := \dots$ ”, and check. (Section 1.5)
- **Construct and verify** (Example (Method: construct and verify)). Find where the object’s values are forced and where they are free, define it, check it is the kind of object claimed, then verify the property. (Section 1.6)
- **Unwind the image.** “ $y \in f(A)$ ” means “there is $a \in A$ with $f(a) = y$ ”: name the witness

before using it. A preimage has no witness to name. (Section 1.7)

- **Refute with a small witness.** The method of Example (Method: disproof by counterexample, proof by example) for statements about sets and functions: a two- or three-element set, the map $x \mapsto x^2$, the empty set.

1.-1.3 Threads

- **The lattice points.** Section 1.1 asks why, among any five points with integer coordinates, two have a midpoint with integer coordinates, and states the principle the answer needs without using it. Section 2.5 proves the pigeonhole principle and comes back to the five points.
- **The five strings.** Section 1.5 plants a game: given five strings of five symbols 0 or 1, write one not on the list. Section 3.3 comes back to it with the diagonal argument.
- **Russell to Cantor.** Russell's theorem in Section 1.2 is the first contradiction about sets: a set built to disagree with each candidate on the candidate itself. Cantor's theorem in Section 3.3 is the same shape of argument, as a theorem rather than a paradox.
- **Same size.** The bijections of Section 1.6 are how the book says that two sets have the same size; Section 2.5 makes this a definition, and Section 4.2 meets it again as an example of an equivalence-like relation.

1.-1.4 Summary

Statements about integers were proved from the definitions of even, odd and divides: divisibility is transitive (Proposition 1.1.1), and every integer is even or odd and not both (Theorem 1.1.2), the first proof by cases of the volume. Sets are equal when they have the same elements (Definition 1.2.1), inclusion is proved by element-chasing, and no set contains every set (Theorem 1.2.4). The laws of sets are the laws of propositional logic (Theorem 1.3.1), and De Morgan's laws hold for families of any size (Theorem 1.3.3). A function has a left inverse exactly when it is injective, on a nonempty domain (Theorem 1.6.1); a right inverse forces surjectivity (Proposition 1.6.2); the bijections are exactly the maps with a two-sided inverse (Theorem 1.6.4). Preimages respect every set operation (Theorem 1.7.1), images respect unions (Theorem 1.7.3), and injectivity repairs intersections (Theorem 1.7.4).

What is open: does every surjection have a right inverse? Nothing proved so far builds one without a rule, and Chapter 3 adds the principle that does. Before that, Chapter 2 turns to the natural numbers, induction and finite sets, and finishes the lattice-point puzzle.

1.-1.5 Terms

- **bijjective:** injective and surjective (Definition 1.5.5).
- **Cartesian product:** $A \times B$, the set of pairs (a, b) with $a \in A$, $b \in B$ (Definition 1.4.2).
- **complement of A in X :** $X \setminus A$, for $A \subseteq X$ (Definition 1.3.1).
- **composite:** $g \circ f$, “ g after f ” (Definition 1.5.2).
- **difference:** $A \setminus B$, the elements of A not in B (Definition 1.3.1).
- **disjoint:** $A \cap B = \emptyset$ (Definition 1.3.1).
- **divides:** $a \mid b$ if $b = ka$ for some $k \in \mathbb{Z}$ (Definition 1.1.2).
- **empty set:** a set with no elements (Definition 1.2.4).
- **equality of sets:** the same elements (Definition 1.2.1).
- **even, odd:** $n = 2k$, $n = 2k + 1$, for some $k \in \mathbb{Z}$ (Definition 1.1.1).
- **function:** a graph with exactly one value at each input, and a declared codomain (Definition 1.5.1).
- **image:** $f(A)$, the values of f at points of A (Definition 1.7.1).

-
- **indexed family:** a set A_i for each $i \in I$ (Definition 1.3.3).
 - **injective:** different inputs, different outputs (Definition 1.5.3).
 - **intersection:** $A \cap B$; of a family, $\bigcap_{i \in I} A_i$ (Definition 1.3.1, Definition 1.3.4).
 - **inverse, two-sided:** a left and a right inverse at once, written f^{-1} (Definition 1.6.2).
 - **left inverse, right inverse:** $g \circ f = \text{id}_X$; $f \circ g = \text{id}_Y$ (Definition 1.6.1).
 - **ordered pair:** $(a, b) = (c, d)$ exactly when $a = c$ and $b = d$ (Definition 1.4.1).
 - **power set:** the set of all subsets (Definition 1.3.2).
 - **preimage:** $f^{-1}(B)$, the inputs whose values lie in B (Definition 1.7.2).
 - **prime:** an integer $p \geq 2$ whose only positive divisors are 1 and p (Definition 1.1.3).
 - **relation:** a subset of $A \times B$ (Definition 1.4.3).
 - **specification:** $\{x \in A : P(x)\}$, a set cut out of a given set (Definition 1.2.3).
 - **subset:** $A \subseteq B$, every element of A is in B (Definition 1.2.2).
 - **surjective:** every element of the codomain is a value (Definition 1.5.4).
 - **union:** $A \cup B$; of a family, $\bigcup_{i \in I} A_i$ (Definition 1.3.1, Definition 1.3.4).