Contents

Preface 8

1 Chapter 1 10

Proofs from Definitions: Sets and Functions 10
1.0.1 Roadmap . . . 11
1.0.2 Named moves . . . 11
1.0.3 Threads . . . 12
1.0.4 Summary . . . 12
1.0.5 Terms . . . 12

1.1 Proofs from Definitions 13
1.1.1 A puzzle about lattice points . . . 13
1.1.2 Definitions first . . . 14
1.1.3 Direct proof . . . 15
1.1.4 Proof by cases . . . 16
1.1.5 Without loss of generality . . . 18
1.1.6 Counterexamples and examples . . . 19
1.1.7 Back to the lattice points . . . 20
1.1.8 Exercises . . . 21
1.1.8.1 A. Check your understanding . . . 21
1.1.8.2 B. Practice . . . 22
1.1.8.3 C. Going deeper . . . 23

1.2 Sets, Subsets and Russell's Paradox 26
1.2.1 A naive idea, and what goes wrong with it . . . 26
1.2.2 Sets and membership . . . 26
1.2.3 Subsets . . . 28
1.2.3.1 Two inclusions make an equality . . . 30
1.2.3.2 Inclusions chain . . . 32
1.2.4 Describing sets: listing and specification . . . 33
1.2.5 The empty set . . . 35
1.2.6 Computing with set-builders . . . 36
1.2.7 Russell's paradox as a theorem . . . 37
1.2.8 Exercises . . . 38
1.2.8.1 A. Check your understanding . . . 38
1.2.8.2 B. Practice . . . 39
1.2.8.3 C. Going deeper . . . 41

1.3 Unions, Intersections, Complements and Families 42
1.3.1 Union, intersection and difference . . . 42
1.3.2 Laws of sets are laws of logic . . . 44

1.3.3 Power sets . . . 48
1.3.4 Families of sets . . . 49
1.3.4.1 The smallest set closed under some steps . . . 51
1.3.4.2 Worked examples with a real parameter . . . 52
1.3.5 De Morgan's laws for families . . . 53
1.3.6 Exercises . . . 55
1.3.6.1 A. Check your understanding . . . 55
1.3.6.2 B. Practice . . . 55
1.3.6.3 C. Going deeper . . . 58

1.4 Ordered Pairs, Products and Relations 60
1.4.1 Order matters: ordered pairs . . . 60
1.4.2 Cartesian products . . . 62
1.4.3 Products and the set operations . . . 65
1.4.4 Relations . . . 67
1.4.5 Exercises . . . 70
1.4.5.1 A. Check your understanding . . . 70
1.4.5.2 B. Practice . . . 70
1.4.5.3 C. Going deeper . . . 72

1.5 Functions, Composition, Injections and Surjections 74
1.5.1 What is a function? . . . 74
1.5.2 When are two functions equal? . . . 78
1.5.3 Families, sequences, and the set of all functions . . . 79
1.5.4 Composition . . . 81
1.5.5 Injective, surjective, bijective . . . 83
1.5.5.1 Injective functions . . . 83
1.5.5.2 Surjective functions . . . 83
1.5.5.3 Bijective functions . . . 84
1.5.5.4 Worked examples . . . 84
1.5.6 Composites of injections and surjections . . . 88
1.5.7 Exercises . . . 90
1.5.7.1 A. Check your understanding . . . 90
1.5.7.2 B. Practice . . . 90
1.5.7.3 C. Going deeper . . . 93

1.6 Left, Right and Two-Sided Inverses 95
1.6.1 Undoing a function . . . 95
1.6.2 Left and right inverses . . . 95
1.6.3 A left inverse exists exactly for injective functions . . . 97
1.6.4 A right inverse forces surjectivity . . . 100
1.6.5 Does every surjection have a right inverse? . . . 101
1.6.6 Two-sided inverses . . . 102
1.6.7 What the section proved . . . 105
1.6.8 Exercises . . . 106
1.6.8.1 A. Check your understanding . . . 106
1.6.8.2 B. Practice . . . 106
1.6.8.3 C. Going deeper . . . 109

1.7 Images and Preimages 111
1.7.1 A question about squares . . . 111
1.7.2 Images and preimages . . . 111

1.7.3 Computing images and preimages . . . 113
1.7.4 Sets of numbers as images . . . 115
1.7.5 Preimages respect every operation . . . 116
1.7.6 Images respect unions . . . 118
1.7.7 Images and intersections . . . 119
1.7.8 There and back . . . 121
1.7.9 Two readings of the inverse symbol . . . 122
1.7.10 Exercises . . . 123
1.7.10.1 A. Check your understanding . . . 123
1.7.10.2 B. Practice . . . 123
1.7.10.3 C. Going deeper . . . 125
1.7.10.4 R. Review . . . 127

2 Chapter 2 **131**

Induction, Contradiction, and Finite Sets **131**
2.0.1 Roadmap . . . 132
2.0.2 Named moves . . . 133
2.0.3 Threads . . . 133
2.0.4 Summary . . . 134
2.0.5 Terms . . . 134

2.1 The Natural Numbers and Well-Ordering **134**
2.1.1 What we assume about the natural numbers . . . 134
2.1.2 The arithmetic of the natural numbers . . . 135
2.1.3 The integers . . . 138
2.1.4 Well-ordering . . . 139
2.1.5 The least element as a tool . . . 141
2.1.6 Induction and well-ordering are the same principle . . . 142
2.1.7 Sets of integers . . . 144
2.1.8 Exercises . . . 145
2.1.8.1 A. Check your understanding . . . 145
2.1.8.2 B. Practice . . . 146
2.1.8.3 C. Going deeper . . . 148

2.2 Induction, Strong Induction and Divisibility **150**
2.2.1 Induction from any integer . . . 151
2.2.2 Finding $P(n)$ inside $P(n+1)$ . . . 152
2.2.3 Divisibility and the division algorithm . . . 154
2.2.4 Lowest terms and prime factors . . . 156
2.2.5 A gallery of broken inductions . . . 158
2.2.6 Exercises . . . 160
2.2.6.1 A. Check your understanding . . . 160
2.2.6.2 B. Practice . . . 160
2.2.6.3 C. Going deeper . . . 163

2.3 Definition by Recursion **165**
2.3.1 Definitions that define something . . . 166
2.3.2 Starting elsewhere, looking two steps back . . . 168
2.3.3 Sums, products and powers . . . 170
2.3.4 Recursion, then induction . . . 172

2.3.5 When the claim is too weak to carry its step . . . 176
2.3.6 Exercises . . . 177
2.3.6.1 A. Check your understanding . . . 177
2.3.6.2 B. Practice . . . 178
2.3.6.3 C. Going deeper . . . 179

2.4 Contrapositive and Contradiction in Practice 182
2.4.1 Choosing the form . . . 182
2.4.2 Infinitely many primes . . . 184
2.4.3 An irrational number by lowest terms . . . 185
2.4.4 The smallest counterexample . . . 186
2.4.5 Existence without a witness . . . 187
2.4.6 Exercises . . . 188
2.4.6.1 A. Check your understanding . . . 188
2.4.6.2 B. Practice . . . 188
2.4.6.3 C. Going deeper . . . 190

2.5 Equinumerous Sets and Finite Sets 192
2.5.1 Same size without counting . . . 192
2.5.2 Finite sets . . . 195
2.5.3 Back to the pigeons . . . 196
2.5.4 Subsets and unions of finite sets . . . 200
2.5.5 No finite set is equinumerous with a proper subset . . . 204
2.5.6 Exercises . . . 205
2.5.6.1 A. Check your understanding . . . 205
2.5.6.2 B. Practice . . . 206
2.5.6.3 C. Going deeper . . . 208
2.5.6.4 R. Review . . . 211

3 Chapter 3 213

Countable and Uncountable Sets 213
3.0.1 Roadmap . . . 214
3.0.2 Named moves . . . 215
3.0.3 Threads . . . 215
3.0.4 Summary . . . 215
3.0.5 Terms . . . 216

3.1 Countable Sets 216
3.1.1 Lists . . . 216
3.1.2 Subsets of the natural numbers . . . 218
3.1.3 Three ways to say countable . . . 219
3.1.4 Closure properties . . . 220
3.1.5 Pairs of natural numbers . . . 222
3.1.6 The integers and the rationals . . . 225
3.1.7 Listing in practice . . . 226
3.1.8 Exercises . . . 226
3.1.8.1 A. Check your understanding . . . 226
3.1.8.2 B. Practice . . . 227
3.1.8.3 C. Going deeper . . . 229

3.2 Countable Unions and the Axiom of Choice 232

3.2.1 A union of countably many lists . . . 232
3.2.2 The obstacle, rule by rule . . . 232
3.2.3 The axiom of choice . . . 233
3.2.4 When choice is not needed . . . 234
3.2.5 Right inverses . . . 236
3.2.6 Countable unions . . . 236
3.2.7 Unions without choice . . . 238
3.2.8 Algebraic numbers . . . 239
3.2.9 Exercises . . . 240
3.2.9.1 A. Check your understanding . . . 240
3.2.9.2 B. Practice . . . 240
3.2.9.3 C. Going deeper . . . 243

3.3 Diagonal Arguments: Uncountable Sets and Cantor's Theorem 245
3.3.1 Back to the five strings . . . 245
3.3.2 A sequence that is not on the list . . . 246
3.3.3 Back to Russell: Cantor's theorem . . . 248
3.3.4 Decimal expansions . . . 250
3.3.5 The real numbers are uncountable . . . 251
3.3.6 Transcendental numbers . . . 253
3.3.7 Exercises . . . 253
3.3.7.1 A. Check your understanding . . . 253
3.3.7.2 B. Practice . . . 254
3.3.7.3 C. Going deeper . . . 256

3.4 Comparing Sizes: the Schröder–Bernstein Theorem 258
3.4.1 Comparing sizes with injections . . . 258
3.4.2 The Schröder–Bernstein Theorem . . . 260
3.4.3 Intervals of real numbers . . . 263
3.4.4 Exercises . . . 265
3.4.4.1 A. Check your understanding . . . 265
3.4.4.2 B. Practice . . . 266
3.4.4.3 C. Going deeper . . . 268

3.5 Infinite Sets 269
3.5.1 Every infinite set contains a copy of the natural numbers . . . 270
3.5.2 Consequences: the smallest infinite size . . . 271
3.5.3 Infinite sets are the same size as a proper part . . . 272
3.5.4 Exercises . . . 273
3.5.4.1 A. Check your understanding . . . 273
3.5.4.2 B. Practice . . . 273
3.5.4.3 C. Going deeper . . . 275

3.6 Cardinal Arithmetic 276
3.6.1 The plane and the line . . . 276
3.6.2 Adding sizes: disjoint unions . . . 276
3.6.3 Multiplying, raising to powers, and comparing . . . 278
3.6.4 Encoding: the diagonals of $\mathbb{N} \times \mathbb{N}$ . . . 280
3.6.5 The laws of exponents, for all sets . . . 281
3.6.6 Subsets are 0–1 functions . . . 284
3.6.7 No set of all sets, once more . . . 285
3.6.8 The size of the line . . . 285

3.6.9 Back to the plane . . . 286
3.6.10 Exercises . . . 289
3.6.10.1 A. Check your understanding . . . 289
3.6.10.2 B. Practice . . . 289
3.6.10.3 C. Going deeper . . . 292
3.6.10.4 R. Review . . . 294

4 Chapter 4 297

Relations: Equivalence and Order 297
4.0.1 Roadmap . . . 298
4.0.2 Named moves . . . 298
4.0.3 Threads . . . 298
4.0.4 Summary . . . 299
4.0.5 Terms . . . 299

4.1 Properties of Relations 300
4.1.1 Four properties . . . 300
4.1.2 Prove or disprove, property by property . . . 301
4.1.3 Divisibility . . . 303
4.1.4 A table of examples . . . 304
4.1.5 Exercises . . . 305
4.1.5.1 A. Check your understanding . . . 305
4.1.5.2 B. Practice . . . 306
4.1.5.3 C. Going deeper . . . 309

4.2 Equivalence Relations and Partitions 310
4.2.1 Arithmetic on a clock . . . 310
4.2.2 Equivalence relations . . . 310
4.2.3 Equivalence classes . . . 312
4.2.4 The classes form a partition . . . 314
4.2.5 Every partition comes from one equivalence relation . . . 316
4.2.6 Congruence modulo n . . . 317
4.2.7 Two more sources of equivalence relations . . . 319
4.2.8 Operations on classes . . . 320
4.2.9 Exercises . . . 324
4.2.9.1 A. Check your understanding . . . 324
4.2.9.2 B. Practice . . . 324
4.2.9.3 C. Going deeper . . . 326

4.3 Partial Orders, Maximal and Greatest Elements 328
4.3.1 Partial orders . . . 328
4.3.2 Bounds, greatest and maximal elements . . . 330
4.3.3 Least upper bounds, a first look . . . 333
4.3.4 Well-ordered sets . . . 335
4.3.5 Exercises . . . 336
4.3.5.1 A. Check your understanding . . . 336
4.3.5.2 B. Practice . . . 336
4.3.5.3 C. Going deeper . . . 338
4.3.5.4 R. Review . . . 340

5 Chapter 5 **343**

Building Functions **343**
5.0.1 Roadmap . . . 344
5.0.2 Named moves . . . 344
5.0.3 Threads . . . 345
5.0.4 Summary . . . 345
5.0.5 Terms . . . 346

5.1 Restriction, Extension and Gluing **346**
5.1.1 A function in two pieces . . . 346
5.1.2 Restriction and extension . . . 347
5.1.3 Gluing . . . 348
5.1.4 Indicator functions . . . 351
5.1.5 Exercises . . . 354
5.1.5.1 A. Check your understanding . . . 354
5.1.5.2 B. Practice . . . 354
5.1.5.3 C. Going deeper . . . 356

5.2 Fibers and the Canonical Factorization **358**
5.2.1 Functions on the clock . . . 358
5.2.2 The fibers of a function . . . 358
5.2.3 Every function factors . . . 360
5.2.4 Functions out of a quotient . . . 362
5.2.5 Exercises . . . 365
5.2.5.1 A. Check your understanding . . . 365
5.2.5.2 B. Practice . . . 366
5.2.5.3 C. Going deeper . . . 368

5.3 Binary Operations **370**
5.3.1 Brackets . . . 370
5.3.2 Operations . . . 371
5.3.3 Properties . . . 372
5.3.4 One identity, one inverse . . . 374
5.3.5 Operations on functions . . . 377
5.3.6 Operations on a quotient . . . 379
5.3.7 Exercises . . . 380
5.3.7.1 A. Check your understanding . . . 380
5.3.7.2 B. Practice . . . 381
5.3.7.3 C. Going deeper . . . 383

5.4 Permutations and Iteration **385**
5.4.1 Shuffling twelve cards . . . 385
5.4.2 Permutations and iterates . . . 386
5.4.3 Orbits . . . 388
5.4.4 Following an orbit . . . 390
5.4.5 Cycles . . . 392
5.4.6 Maps that are not permutations . . . 395
5.4.7 Exercises . . . 396
5.4.7.1 A. Check your understanding . . . 396
5.4.7.2 B. Practice . . . 397
5.4.7.3 C. Going deeper . . . 398

5.4.7.4 R. Review 400

6 Chapter 6 **402**

Zorn's Lemma **402**
6.0.1 Roadmap 402
6.0.2 Named moves 403
6.0.3 Threads 403
6.0.4 Summary 403
6.0.5 Terms 403

6.1 Chains and Zorn's Lemma **404**
6.1.1 Matching two sets, one pair at a time 404
6.1.2 Chains 404
6.1.3 Zorn's lemma 406
6.1.4 The maximality template 407
6.1.5 Exercises 410
6.1.5.1 A. Check your understanding 410
6.1.5.2 B. Practice 411
6.1.5.3 C. Going deeper 413

6.2 Using Zorn's Lemma **414**
6.2.1 Back to comparing sizes 414
6.2.2 Extending a partial order 416
6.2.3 Optional: every vector space has a basis 420
6.2.4 Exercises 420
6.2.4.1 A. Check your understanding 420
6.2.4.2 B. Practice 420
6.2.4.3 C. Going deeper 422
6.2.4.4 R. Review 423

Preface

Every definition of analysis is a sentence about sets and functions. *Logic and Proof* supplied the grammar of such sentences: the connectives, the quantifiers, and the prose that carries their rules. This volume supplies the nouns, and above all the two that every other one is made of: sets and functions. Around them it builds the natural numbers and induction, the sizes of infinite sets and their arithmetic, relations and orders, and the ways a function is built from others.

Who it is for. The reader we have in mind has worked through *Logic and Proof*, or has its habits from elsewhere: reading a statement with its quantifiers in place, proving a "for every" by taking an arbitrary element, naming a witness before using it. The chapters point back to *Logic and Proof* where they use one of its rules, so a reader who is unsure of a step can look it up.

What it covers.

Chapter	What it does
1	Proofs from definitions: sets and functions. Proofs straight from definitions (direct proof, cases, counterexamples) on even, odd, divides and prime; sets and the working rules that say which sets exist, Russell's paradox, families of sets, products and relations, functions and their inverses, images and preimages, each section with its method of proof
2	The arithmetic of $\mathbb{N}$ and $\mathbb{Z}$ from induction, well-ordering, induction as a craft, definition by recursion, contrapositive and contradiction, infinitely many primes, equinumerous and finite sets and the pigeonhole principle
3	Countable sets, the axiom of choice, diagonal arguments and Cantor's theorem, the Schröder–Bernstein theorem, infinite sets; cardinal arithmetic: sums, products and powers of sizes, $\lvert\mathbb{R}\rvert = \lvert\mathcal{P}(\mathbb{N})\rvert$, $\mathbb{R}^2$ and $\mathbb{N}^{\mathbb{N}}$ as large as $\mathbb{R}$ (Section 3.6)
4	Relations: properties of relations decided one at a time, equivalence relations and partitions, the integers modulo n, well-definedness, partial orders, maximal and greatest elements, least upper bounds

Chapter	What it does
5	Building functions: restriction, extension and gluing, indicator functions; fibers and the factorization of every function through a quotient; binary operations and their identities and inverses; permutations, iteration, orbits and cycles
6	Zorn's lemma, stated without proof, and the maximality template: the axiom of choice from Zorn's lemma, any two sets are comparable in size, every partial order extends to a total order

The real numbers are used throughout as familiar objects, with their school arithmetic and order, and every use of a school fact is named where it occurs. *Analysis on the Real Line* turns those facts into consequences of axioms, and *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$ builds the numbers out of sets.

How to read it. Read the chapters in order: each uses the ones before it. Every section has Quick checks with folded answers; answer each one before you unfold it. When a section uses a method of proof for the first time, it sets the method out in a box marked *Method*, with a template, when to use it and the usual failure; later sections cite the box instead of explaining the method again, and each chapter's opening page lists its boxes under Named moves. The exercises of a section come in three groups, A to check understanding, B for practice and C to go deeper, and the last section of each chapter adds R items that reach back to earlier chapters. A chapter's opening page lists what it needs, with links, and the time it takes: about 160 hours for the whole volume on the core track, and about 225 hours for everything.

Chapter 1

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.

1.0.1 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 elements, 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.

1.0.2 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 $L = R$:

$x \in L \iff \cdots \iff x \in R$, 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 $x \coloneqq \ldots$", 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.

1.0.3 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.

1.0.4 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.

1.0.5 Terms

- **bijective**: 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**: $g \circ f = \mathrm{id}_X$; $f \circ g = \mathrm{id}_Y$ (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).

1.1 Proofs from Definitions

Logic and Proof taught the rules of proof and how to write them as prose. From here on the statements are about mathematical objects, and every word in them that matters has a definition. A proof begins by writing the hypotheses out by their definitions, writes out what the conclusion demands, and closes the gap between them. This section practices that on the integers, where the definitions are one line long and every claim can be tested by hand. It teaches five moves: direct proof, proof by cases, without loss of generality, disproof by counterexample, and proof of existence by an example.

1.1.1 A puzzle about lattice points

A **lattice point** is a point (a, b) of the plane whose coordinates a and b are both integers, as in school geometry: the corners of the squares on squared paper. The midpoint of (a, b) and (c, d) is

$$\left(\frac{a+c}{2}, \frac{b+d}{2}\right),$$

and it may or may not be a lattice point. The points $(0, 0)$ and $(2, 4)$ have midpoint $(1, 2)$, a lattice point; the points $(0, 0)$ and $(1, 4)$ have midpoint $(\frac{1}{2}, 2)$, which is not. That raises two questions.

- **(Q1)** Among **any five** lattice points, must there be two whose midpoint is a lattice point?
- **(Q2)** Among **any four** lattice points, must there be two whose midpoint is a lattice point?

Before reading on, place a few sets of points on squared paper and compute their midpoints.

Both answers come from two words this section defines, even and odd. Question (Q2) is settled in this section. Question (Q1) needs, besides parity, a principle about finite collections that sounds too obvious to need proof; we will state it but not yet prove it.

1.1.2 Definitions first

The first two words are the ones the puzzle needs.

Definition 1.1.1. Even and Odd

An integer n is **even** if $n = 2k$ for **some** $k \in \mathbb{Z}$, and **odd** if $n = 2k + 1$ for **some** $k \in \mathbb{Z}$.

Logic and Proof used these words informally, and wrote "n is even" as $\exists k\,(n = 2k)$ in its derivations (for instance Logic and Proof, Example (The sum of two even integers is even)); from now on they mean exactly this, a "there exists".

Evenness is divisibility by 2, so the next word generalizes it. One might define "a divides b" as "b/a is an integer". That works for 3 and 12, but it says nothing when $a = 0$, since $0/0$ and $5/0$ are undefined; yet $0 = 0 \cdot 0$ suggests that 0 should divide 0. The definition avoids division altogether and asks for a multiplier.

Definition 1.1.2. Divisibility

Let $a, b \in \mathbb{Z}$. We say that a **divides** b, written $a \mid b$, if **there exists** $k \in \mathbb{Z}$ with $b = ka$. Then a is a **divisor** of b, and b is a **multiple** of a.

Quick check. Decide, from the definitions alone: (a) Is 0 even? (b) Does -4 divide 6? Does 0 divide 5? (c) Is -7 odd? (d) Does 12 divide 3?

Solution.

(a) Yes: $0 = 2 \cdot 0$, with $k = 0 \in \mathbb{Z}$.

(b) No. If $6 = k \cdot (-4)$ with $k \in \mathbb{Z}$, then $k \leq -2$ gives $-4k \geq 8$ and $k \geq -1$ gives $-4k \leq 4$, so $-4k \neq 6$ in either case. And no: $k \cdot 0 = 0 \neq 5$ for every k.

(c) Yes: $-7 = 2 \cdot (-4) + 1$, with $k = -4 \in \mathbb{Z}$.

(d) No. If $3 = 12k$ with $k \in \mathbb{Z}$, then $k \geq 1$ gives $12k \geq 12$ and $k \leq 0$ gives $12k \leq 0$.

So $3 \mid 12$, with $k = 4$, and $-3 \mid 12$, with $k = -4$. Every integer a divides 0, with $k = 0$; this is the degenerate case, and it shows that "$a \mid b$" is a statement, not the number b/a: $0 \mid 0$ is true, while $0/0$ is not defined. Also $1 \mid b$ and $b \mid b$ for every integer b, and "n is even" is "$2 \mid n$". We write $a \nmid b$ when a does not divide b.

The last definition singles out the integers with as few divisors as possible.

Definition 1.1.3. Prime Number

An integer p is **prime** if $p \geq 2$ and the only **positive** divisors of p are 1 and p. A **prime factor** of an integer n is a prime p with $p \mid n$.

So 2, 3, 5 and 7 are prime (for 7: a positive divisor of 7 is at most 7, and none of $2, 3, 4, 5, 6$ divides it); $9 = 3 \cdot 3$ and $15 = 3 \cdot 5$ are not, and neither is 1, which fails the clause $p \geq 2$.

1.1.3 Direct proof

The first claim to prove from these definitions is that divisibility passes along a chain.

Proposition 1.1.1. Divisibility Is Transitive

For all integers a, b, c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

Idea (Scratch work). Unwind every defined word. The hypotheses $a \mid b$ and $b \mid c$ are two "there exists" statements, so each hands us a multiplier. Give them **different** names, k and l: nothing says the two multipliers agree, and one name for both is the error (N4) of Logic and Proof, Example (What is not allowed), met in Logic and Proof, Example (The sum of two even integers is even). The goal $a \mid c$ is also a "there exists": we must **produce** an integer m with $c = ma$.

Givens	Goal
$a \mid b$, $b \mid c$	$a \mid c$
$b = ka$, $c = lb$, with $k, l \in \mathbb{Z}$	$c = ma$ for some $m \in \mathbb{Z}$: find m
$b = ka$, $c = lb$	$c = l(ka) = (lk)a$: try $m = lk$, and check that $lk \in \mathbb{Z}$

The last row closes the gap. The proof writes this forwards: the witness m is named, then checked.

Proof. Let $a, b, c \in \mathbb{Z}$ with $a \mid b$ and $b \mid c$. By Definition 1.1.2 there are $k, l \in \mathbb{Z}$ with $b = ka$ and $c = lb$. Then $c = l(ka) = (lk)a$, and $lk \in \mathbb{Z}$, as a product of integers. So $a \mid c$, with witness lk, by Definition 1.1.2.

■

The proof used only the definition of divisibility and integer arithmetic, and it read the definition in both directions: once to unwind the hypotheses, once to rewind the conclusion.

Example. Method: direct proof from a definition

Template. To prove "if P, then Q": (1) assume P and write it out by its definition, giving each witness a new name; (2) write out what Q demands, for example which object must be produced; (3) close the gap by computation, on scrap paper if need be; (4) write the proof

forwards: assume, unwind, compute, and rewind into the definition of Q, naming the witness and checking that it is of the required kind.

When to use it. The hypotheses and the conclusion are defined notions, and the gap between them is computation.

The usual failure. Stopping at the computation, as in "$c = (lk)a$, done", without checking that $lk \in \mathbb{Z}$, which is the clause the definition demands. Also one name for two witnesses (N4), and using what is to be proved (N9).

Example. Divisors of a combination

Let $a, b, c \in \mathbb{Z}$ with $a \mid b$ and $a \mid c$. Show that $a \mid bx + cy$ for all $x, y \in \mathbb{Z}$.

Solution. By the method of Example (Method: direct proof from a definition): unwind both hypotheses with two names, then look for a multiplier of a in $bx + cy$.

Let $x, y \in \mathbb{Z}$. By Definition 1.1.2 there are $k, l \in \mathbb{Z}$ with $b = ka$ and $c = la$. Then

$$bx + cy = kax + lay = (kx + ly)a,$$

and $kx + ly \in \mathbb{Z}$, since sums and products of integers are integers. So $a \mid bx + cy$, with witness $kx + ly$.

Three special cases are used constantly. With $x = y = 1$, $a \mid b + c$; with $x = 1$ and $y = -1$, $a \mid b - c$; with $y = 0$, $a \mid bx$. With $a = 2$ and $x = y = 1$, the first case is "even plus even is even", the claim derived in Logic and Proof, Example (The sum of two even integers is even).

Quick check. The proof of Proposition 1.1.1 named two witnesses, k and l. Find integers a, b, c with $a \mid b$ and $b \mid c$ for which one name could not serve for both.

Solution. Take $a = 1$, $b = 2$, $c = 6$. Then $b = 2a$ and $c = 3b$, and no single k has both $2 = k \cdot 1$ and $6 = k \cdot 2$: the first forces $k = 2$, the second $k = 3$. Writing one name would claim that the two multipliers are equal, which is (N4).

1.1.4 Proof by cases

Some claims depend on what kind of integer we have. The first such fact is the one behind every parity argument.

Theorem 1.1.2. Every Integer Is Even or Odd

Every integer is even or odd, and no integer is both.

Idea (Scratch work). Start on $\mathbb{N}$, where induction is available (Logic and Proof, Axiom 4.2.1), with $P(n)$: "n is even or n is odd". The base $P(0)$ is $0 = 2 \cdot 0$. The step needs $P(n+1)$ from $P(n)$. But $P(n)$ is an "or", and knowing that n is even **or** odd does not tell us which. So split into the two cases, as $\vee$E does (Logic and Proof, Definition 1.6.1). Each case is a new given, and each must reach the same goal.

Givens	Goal
$P(n)$: n even or n odd	$n+1$ even or $n+1$ odd
Case 1: $n = 2k$	$n+1 = 2k+1$: odd
Case 2: $n = 2k+1$	$n+1 = 2(k+1)$: even

The negative integers come next, by cases again: for $n < 0$, $-n \in \mathbb{N}$ is already known to be even or odd, and the sign can be moved inside. Finally "not both" is a negation: assume $n = 2a$ and $n = 2b+1$, and aim for a contradiction ($\neg$I). The two equations give $2(a-b) = 1$, and no integer doubles to 1.

Proof. Every natural number is even or odd. We argue by induction on n. For $n = 0$, $0 = 2 \cdot 0$ is even. Let $n \in \mathbb{N}$ be even or odd. *Case 1:* $n = 2k$ with $k \in \mathbb{Z}$. Then $n+1 = 2k+1$ is odd. *Case 2:* $n = 2k+1$ with $k \in \mathbb{Z}$. Then $n+1 = 2(k+1)$, with $k+1 \in \mathbb{Z}$, is even. In either case $n+1$ is even or odd. By Logic and Proof, Axiom 4.2.1, every $n \in \mathbb{N}$ is even or odd.

Every integer is even or odd. Let $n \in \mathbb{Z}$. If $n \geq 0$, then $n \in \mathbb{N}$, and we are done. If $n < 0$, then $-n \in \mathbb{N}$ is even or odd. If $-n = 2k$, then $n = 2(-k)$ is even. If $-n = 2k+1$, then $n = -2k-1 = 2(-k-1)+1$ is odd.

No integer is both. Suppose $n = 2a$ and $n = 2b+1$ with $a, b \in \mathbb{Z}$. Then $2(a-b) = 1$, with $c \coloneqq a - b \in \mathbb{Z}$. If $c \geq 1$, then $2c \geq 2$; if $c \leq 0$, then $2c \leq 0$. Either way $2c \neq 1$, a contradiction. So no integer is both even and odd ($\neg$I).

■

A fact *Logic and Proof* took from school is now proved from the definitions. The proof has four case splits, each into cases that together cover everything.

Example. Method: proof by cases

Template. Find a disjunction you already have, such as "n is even or n is odd" (Theorem 1.1.2), "$x \geq 0$ or $x < 0$", or excluded middle (Logic and Proof, Proposition 2.5.3). Write one paragraph per case, labeled *Case 1.*, *Case 2.*. In each, add the case to the givens, unwind it, and reach the **same** goal.

When to use it. The definitions or the algebra behave differently on different kinds of input, so the givens give no grip until you know which kind you have.

The usual failure. Cases that do not cover every possibility (N8), or a case forgotten (N7). Before splitting, say why the cases are exhaustive.

Example. A proof by cases

Show that $n^3 + 5n$ is even for every integer n.

Idea. A general n gives no grip, but $2k$ and $2k+1$ can be expanded, and by Theorem 1.1.2 these two cases cover $\mathbb{Z}$. So use Example (Method: proof by cases), and in each case pull out a factor 2.

Solution. Let $n \in \mathbb{Z}$. By Theorem 1.1.2, n is even or odd.

Case 1: $n = 2k$ with $k \in \mathbb{Z}$. Then $n^3 + 5n = 8k^3 + 10k = 2(4k^3 + 5k)$.

Case 2: $n = 2k+1$ with $k \in \mathbb{Z}$. Then $n^3 = 8k^3 + 12k^2 + 6k + 1$ and $5n = 10k + 5$, so

$$n^3 + 5n = 8k^3 + 12k^2 + 16k + 6 = 2(4k^3 + 6k^2 + 8k + 3).$$

In each case the bracket is an integer, so $n^3 + 5n$ is even by Definition 1.1.1.

Quick check. Why does the proof of Example (A proof by cases) need no third case?

Solution. By Theorem 1.1.2 every integer is even or odd, so the two cases already cover every $n \in \mathbb{Z}$.

1.1.5 Without loss of generality

When two cases are mirror images, a proof writes one and says that the other is "the same with the roles exchanged". *Logic and Proof*, Section 8.2 read the phrase "without loss of generality" as a $\vee$E whose second box is the first with the letters swapped, and it is licensed only when the statement and the hypotheses are unchanged by the swap (Logic and Proof, Example (An induction, and a legitimate symmetry) (b)).

Example. The parity of a sum

Let $m, n \in \mathbb{Z}$.

(a) If m and n have the same parity (both even or both odd), then $m + n$ is even.
(b) If they have opposite parity (one even and the other odd), then $m + n$ is odd.

Solution.

(a) *Case 1: both even.* Then $2 \mid m+n$ by Example (Divisors of a combination) with $a = 2$, $x = y = 1$. *Case 2: both odd*, say $m = 2k + 1$ and $n = 2l + 1$ with $k, l \in \mathbb{Z}$. Then $m + n = 2(k + l + 1)$, with $k + l + 1 \in \mathbb{Z}$. In both cases $m + n$ is even.
(b) The statement is symmetric in m and n: $m + n = n + m$, and "opposite parity" does

not change when the two are exchanged. So, without loss of generality, m is even and n is odd, say $m = 2k$ and $n = 2l + 1$ with $k, l \in \mathbb{Z}$. Then $m + n = 2(k + l) + 1$ is odd. The case m odd and n even is the same with m and n exchanged.

Warning. **Check the symmetry first.** "Without loss of generality $m \leq n$" is legitimate for a claim about $m + n$, and not for a claim about $m - 2n$: exchanging m and n changes that claim. Before writing the phrase, exchange the letters in the statement and in the hypotheses, and check that nothing changes.

1.1.6 Counterexamples and examples

A universal claim, "for every x, if $P(x)$ then $Q(x)$", is refuted by one x with $P(x)$ true and $Q(x)$ false. That is the negation laws at work (Logic and Proof, Proposition 6.2.1, Logic and Proof, Proposition 6.2.2): $\neg\forall x\,(P(x) \to Q(x))$ is equivalent to $\exists x\,(P(x) \wedge \neg Q(x))$, and an existential is proved by one example ($\exists$I).

Example. A pattern that breaks

Is $2p + 1$ prime for every prime p?

Solution. For $p = 2, 3, 5$ we get $5, 7, 11$, all prime. At $p = 7$ the pattern breaks: 7 is prime, and $2 \cdot 7 + 1 = 15 = 3 \cdot 5$ has the positive divisor $3 \notin \{1, 15\}$, so 15 is not prime (Definition 1.1.3). The claim is false, and $p = 7$ is a counterexample. The three successes proved nothing, since verifying instances never gives a "for all" (N1); one failure settles the question.

Warning. **A counterexample must satisfy the hypothesis.** The choice $p = 4$ makes $2p + 1 = 9$, which is not prime; but 4 is not prime either, so $p = 4$ says nothing about the claim. A counterexample to "if $P(x)$, then $Q(x)$" needs $P(x)$ true **and** $Q(x)$ false, and both are checked on the page.

Example. Two divisors, one product

Prove or disprove: for all integers a, b, c, if $a \mid c$ and $b \mid c$, then $ab \mid c$.

Idea (Scratch work). Try small a and b. For $a = 2$, $b = 3$, the c with $2 \mid c$ and $3 \mid c$ are $0, \pm 6, \pm 12, \ldots$, and 6 divides each of them: no counterexample there. The pair $a = 2$, $b = 5$ resists too. What made those work? The two divisors had nothing in common, so c had to contain both separately. Try a and b sharing a factor, as small as possible: $a = b = 2$, and then $c = 2$.

Givens	Goal
(none: we are looking for an example)	integers a, b, c with $a \mid c$, $b \mid c$, $ab \nmid c$

$a = b = 2$, $c = 2$	$2 \mid 2$ (twice), and $4 \nmid 2$
$2 = 1 \cdot 2$	$4 \nmid 2$: no $k \in \mathbb{Z}$ with $2 = 4k$

Solution. False. Take $a = b = c = 2$. Then $2 = 1 \cdot 2$, so $a \mid c$ and $b \mid c$. But $ab = 4$, and $4 \nmid 2$: if $2 = 4k$ with $k \in \mathbb{Z}$, then $k \geq 1$ gives $4k \geq 4$ and $k \leq 0$ gives $4k \leq 0$, so $4k \neq 2$.

The search failed while a and b had no common factor greater than 1, and that is no accident: for coprime a and b the statement is true, a fact *Number Systems*, Chapter 3 proves.

Example. Method: disproof by counterexample, proof by example

Template. To refute "for every x, if $P(x)$ then $Q(x)$": name one x, check $P(x)$, and check that $Q(x)$ fails. To prove "there is an x with $P(x)$": name one x and check $P(x)$.

When to use it. The claim survives a few tries, yet you doubt it; or the statement is existential. Search small and extreme cases first: 0, 1, negative numbers, the smallest sets.

The usual failure. A "counterexample" that does not satisfy the hypothesis; refuting a different claim from the one stated; and the mirror error, concluding "for every" from examples (N1). One example refutes a universal claim, and no number of examples proves one.

An existence claim, proved by one example: there is an integer $n > 1$ with $n \mid 2^n + 1$, namely $n = 3$, since $2^3 + 1 = 9 = 3 \cdot 3$.

Quick check. Is $p = 2$ a counterexample to the claim of Example (A pattern that breaks)? Is $p = 11$?

Solution. No and no. For $p = 2$, $2p + 1 = 5$ is prime; for $p = 11$, $2p + 1 = 23$ is prime. In each case the conclusion holds.

1.1.7 Back to the lattice points

(Q2) is false. Take the four corners of a unit square, $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$. Their six midpoints are

$$(0, \tfrac{1}{2}), \quad (\tfrac{1}{2}, 0), \quad (\tfrac{1}{2}, \tfrac{1}{2}), \quad (\tfrac{1}{2}, \tfrac{1}{2}), \quad (\tfrac{1}{2}, 1), \quad (1, \tfrac{1}{2}),$$

and none is a lattice point. A counterexample to a universal claim is also an existence proof by example: there are four lattice points no two of which have a lattice point as midpoint.

The **parity pattern** of a lattice point (a, b) is the pair of words (parity of a, parity of b): even–even, even–odd, odd–even or odd–odd. By Theorem 1.1.2 every integer is even or odd and not both, so every lattice point has exactly one of the four patterns. The four corners above have one pattern each, and that is why they fail.

Example. Same pattern, lattice midpoint

Show that if two lattice points have the same parity pattern, then their midpoint is a lattice point.

Solution. Let (a, b) and (c, d) have the same parity pattern. Then a and c have the same parity, so $a + c$ is even by Example (The parity of a sum) (a): $a + c = 2s$ with $s \in \mathbb{Z}$, and $(a + c)/2 = s \in \mathbb{Z}$. Likewise b and d have the same parity, so $(b + d)/2 \in \mathbb{Z}$. Hence the midpoint is a lattice point.

Quick check. Which pattern does $(-3, 8)$ have? Find a second point with the same pattern, and their midpoint.

Solution. Odd–even: $-3 = 2 \cdot (-2) + 1$ and $8 = 2 \cdot 4$. For example $(1, 0)$, with midpoint $(-1, 4)$.

(Q1), almost. Among five lattice points, each point has one of only four patterns, so two of the points must share a pattern, and then Example (Same pattern, lattice midpoint) finishes. The step "five objects in four boxes put two in one box" is the **pigeonhole principle**. It is stated here, not proved, and so the answer to (Q1) is "yes, once the principle is proved". The four corners show that five cannot be lowered to four.

Remark (Looking ahead). Section 2.5 proves the pigeonhole principle, from a precise definition of "finite", and comes back to these five points.

1.1.8 Exercises

1.1.8.1 A. Check your understanding

Exercise. A1

(a) Write out "$6 \mid n$" and "n is odd" by their definitions, each as a "there exists".

(b) True or false, with reasons: -1 is odd; $7 \mid 0$; $0 \mid 7$; 1 is prime.

(c) What must a counterexample to "every multiple of 4 is a multiple of 8" satisfy? Give one.

(d) In the proof of Theorem 1.1.2, name the four case splits and say why each is exhaustive.

Solution.

(a) $6 \mid n$: there exists $k \in \mathbb{Z}$ with $n = 6k$ (Definition 1.1.2). n is odd: there exists $k \in \mathbb{Z}$ with $n = 2k + 1$ (Definition 1.1.1).

(b) True: $-1 = 2 \cdot (-1) + 1$. True: $0 = 0 \cdot 7$. False: $k \cdot 0 = 0 \neq 7$ for every $k \in \mathbb{Z}$. False:

$1 < 2$, so 1 fails the clause $p \geq 2$ of Definition 1.1.3.

(c) It must be a multiple of 4 that is not a multiple of 8. For example $4 = 1 \cdot 4$; and $4 = 8k$ has no integer solution, since $k \geq 1$ gives $8k \geq 8$ and $k \leq 0$ gives $8k \leq 0$.

(d) First, even or odd in the induction step: this is the induction hypothesis itself, a disjunction already derived. Second, $n \geq 0$ or $n < 0$: every integer is one or the other, by the order of $\mathbb{Z}$. Third, $-n$ even or $-n$ odd, for $n < 0$: the first half of the proof, applied to $-n \in \mathbb{N}$. Fourth, $c \geq 1$ or $c \leq 0$: no integer lies strictly between 0 and 1.

1.1.8.2 B. Practice

Exercise. B1: Direct proofs

Prove, for all integers a, b, c, d:

(a) if $a \mid b$, then $a^2 \mid b^2$;

(b) if $a \mid b$ and $c \mid d$, then $ac \mid bd$.

Solution.

(a) Let $a \mid b$. By Definition 1.1.2, $b = ka$ with $k \in \mathbb{Z}$. Then $b^2 = k^2a^2$, and $k^2 \in \mathbb{Z}$, so $a^2 \mid b^2$.

(b) Let $a \mid b$ and $c \mid d$. By Definition 1.1.2, $b = ka$ and $d = lc$ with $k, l \in \mathbb{Z}$, two different names since nothing says the multipliers agree. Then $bd = (ka)(lc) = (kl)(ac)$, and $kl \in \mathbb{Z}$, so $ac \mid bd$.

Exercise. B2: Two cases

Prove that for every integer n, either $4 \mid n^2$ or $4 \mid n^2 - 1$.

Solution. Let $n \in \mathbb{Z}$. By Theorem 1.1.2, n is even or odd. *Case 1:* $n = 2k$ with $k \in \mathbb{Z}$. Then $n^2 = 4k^2$, so $4 \mid n^2$. *Case 2:* $n = 2k + 1$ with $k \in \mathbb{Z}$. Then $n^2 - 1 = 4k^2 + 4k = 4(k^2 + k)$, with $k^2 + k \in \mathbb{Z}$, so $4 \mid n^2 - 1$. In either case one of the two divisibilities holds.

Exercise. B3: Name the move, then complete it

Here is the frame of a proof that if $m, n \in \mathbb{Z}$ have opposite parity, then $m^2 + n^2$ is odd.

> The statement is unchanged when m and n are exchanged, so we may assume ...
>
> ⋮
>
> ... Hence $m^2 + n^2$ is odd.

Name the move, then complete it.

Solution. The move is *without loss of generality*: the statement and the hypothesis are symmetric in m and n, so we may assume that m is even and n is odd, say $m = 2k$ and $n = 2l + 1$ with $k, l \in \mathbb{Z}$. Then

$$m^2 + n^2 = 4k^2 + 4l^2 + 4l + 1 = 2(2k^2 + 2l^2 + 2l) + 1,$$

with $2k^2 + 2l^2 + 2l \in \mathbb{Z}$. Hence $m^2 + n^2$ is odd. The case m odd and n even is the same with m and n exchanged.

Exercise. B4: Prove or disprove

Prove each true statement and refute each false one with a counterexample.

(a) For all integers a, b, c: if $a \mid b + c$ and $a \mid b$, then $a \mid c$.

(b) For all integers a, b, c: if $a \mid b + c$, then $a \mid b$ or $a \mid c$.

(c) For every integer n, $n^4 + n^2 + 1$ is odd.

(d) The sum of any three odd integers is even.

(e) There is an integer $n > 5$ with $n \mid n + 6$.

(f) For all integers m, n: if mn is even, then m and n are both even.

Solution.

(a) True. Let $a \mid b+c$ and $a \mid b$: $b+c = ka$ and $b = la$ with $k, l \in \mathbb{Z}$. Then $c = (b+c) - b = (k - l)a$, with $k - l \in \mathbb{Z}$, so $a \mid c$.

(b) False. Take $a = 2$, $b = c = 1$. Then $b+c = 2 = 1 \cdot 2$, so $a \mid b+c$. But $2 \nmid 1$: $1 = 2 \cdot 0 + 1$ is odd, hence not even (Theorem 1.1.2), and the same holds for $c = 1$.

(c) True. By Theorem 1.1.2, n is even or odd. *Case 1:* $n = 2k$. Then $n^4 + n^2 + 1 = 16k^4 + 4k^2 + 1 = 2(8k^4 + 2k^2) + 1$. *Case 2:* $n = 2k+1$. Then $n^2 = 4k^2 + 4k + 1 = 2j + 1$ with $j := 2k^2 + 2k \in \mathbb{Z}$, so

$$n^4 + n^2 = n^2(n^2 + 1) = (2j + 1)(2j + 2) = 2(2j + 1)(j + 1),$$

and $n^4 + n^2 + 1 = 2(2j+1)(j+1) + 1$. In both cases the bracket ($8k^4 + 2k^2$, respectively $(2j + 1)(j + 1)$) is an integer, so $n^4 + n^2 + 1$ is odd by Definition 1.1.1.

(d) False. Take 1, 1, 1: their sum $3 = 2 \cdot 1 + 1$ is odd, hence not even (Theorem 1.1.2).

(e) True. Take $n = 6$: $n + 6 = 12 = 2 \cdot 6$, so $6 \mid 12$.

(f) False. Take $m = 2$, $n = 1$. Then $mn = 2 = 2 \cdot 1$ is even, but $n = 1 = 2 \cdot 0 + 1$ is odd, hence not even (Theorem 1.1.2).

1.1.8.3 C. Going deeper

Exercise. C1: Three cases

(a) By the method of Theorem 1.1.2, show that every integer has the form $3k$, $3k + 1$ or $3k + 2$ for some $k \in \mathbb{Z}$, and that no integer has two of these forms.

(b) Deduce that for every integer n, n^2 has the form $3k$ (exactly when $3 \mid n$) or the form

$3k+1$.

(c) Prove that for all integers a, b: if $3 \mid a^2+b^2$, then $3 \mid a$ and $3 \mid b$.

Solution (Hint 1). For (c), use (b) on a and on b, and look at the cases.

Solution (Hint 2). First line: "Suppose $3 \mid a^2+b^2$, and suppose $3 \nmid a$."

Solution.

(a) *Every natural number has one of the forms*, by induction on n. For $n=0$, $0=3\cdot 0$. In the step, $n=3k$ gives $n+1=3k+1$; $n=3k+1$ gives $n+1=3k+2$; $n=3k+2$ gives $n+1=3(k+1)$. So every $n \in \mathbb{N}$ has one of the forms (Logic and Proof, Axiom 4.2.1). *Every integer.* For $n<0$, write $-n \in \mathbb{N}$ in one of the forms; then $-3k=3(-k)$, $-(3k+1)=3(-k-1)+2$ and $-(3k+2)=3(-k-1)+1$. *No two forms.* Suppose $3a+r=3b+s$ with $a, b \in \mathbb{Z}$ and $0 \le r < s \le 2$. Then $3(a-b)=s-r \in \{1,2\}$. With $c := a-b \in \mathbb{Z}$, $c \ge 1$ gives $3c \ge 3$ and $c \le 0$ gives $3c \le 0$, so $3c \notin \{1,2\}$, a contradiction ($\neg$I).

(b) By (a), n has one of the three forms. If $n=3k$, then $n^2=3(3k^2)$. If $n=3k+1$, then $n^2=9k^2+6k+1=3(3k^2+2k)+1$. If $n=3k+2$, then $n^2=9k^2+12k+4=3(3k^2+4k+1)+1$. So n^2 has the form $3k$ in the first case and $3k+1$ in the other two. Since no integer has two forms, n^2 has the form $3k$ exactly in the first case, that is, exactly when $3 \mid n$.

(c) Suppose $3 \mid a^2+b^2$, and suppose $3 \nmid a$. By (b), $a^2=3j+1$ with $j \in \mathbb{Z}$. *Case 1:* $3 \mid b$. Then $b^2=3l$ by (b), and $a^2+b^2=3(j+l)+1$. *Case 2:* $3 \nmid b$. Then $b^2=3l+1$ by (b), and $a^2+b^2=3(j+l)+2$. In both cases a^2+b^2 has a form other than $3k$; but $3 \mid a^2+b^2$ says it has the form $3k$, against the "no two forms" half of (a). This contradiction refutes $3 \nmid a$, so $3 \mid a$ (by RAA, or by excluded middle on $3 \mid a$, with the case $3 \nmid a$ closed by $\bot$E). The statement and the hypothesis are unchanged when a and b are exchanged, so the same argument gives $3 \mid b$.

Marking scheme. (10 points) - 2: (a) existence on $\mathbb{N}$ by induction, with the three step cases. - 1: (a) the negative integers. - 1: (a) uniqueness of the form, by the bound on $3c$. - 1: (b) the three cases computed. - 1: (b) "exactly when" derived from uniqueness, not only from the computation. - 2: (c) the case split complete (cases on b under $3 \nmid a$, or all four cases on a and b), each giving the right form. - 1: (c) the contradiction named as one with the uniqueness in (a). - 1: (c) both conclusions $3 \mid a$ and $3 \mid b$ obtained (by licensed symmetry, or by the full case split). Fatal errors (0 for the step): treating $3 \nmid a$ as "$a=3k+1$" only, forgetting $3k+2$ (N7); concluding $3 \mid a$ from $3 \mid a^2$ without (b).

Exercise. C2: Find the error

Claim: if $n \in \mathbb{Z}$ and n^2 is odd, then n is odd.

"Proof": Let n be odd, $n=2k+1$. Then $n^2=4k^2+4k+1=2(2k^2+2k)+1$ is odd.

(a) Is the conclusion true?

(b) Does the argument prove it? Name the failing line.

(c) Give a counterexample to the illegal step itself.

(d) Write a correct proof.

Solution. The conclusion is true: it is one half of Logic and Proof, Theorem 2.4.4.

The argument does not prove it. Its first line assumes the conclusion, "n is odd", and its last line reaches the hypothesis, so it proves the converse, "if n is odd, then n^2 is odd": entry (N5) of Logic and Proof, Example (What is not allowed). The $\to$I box must open with "n^2 is odd". The step "from $Q \to P$, conclude $P \to Q$" is illegal, and one instance shows it: "if $n > 0$, then $n^2 > 0$" is true, but the converse "if $n^2 > 0$, then $n > 0$" is false at $n = -1$.

A correct proof, by cases on n (Theorem 1.1.2). Let $n \in \mathbb{Z}$ with n^2 odd. *Case 1:* $n = 2k$. Then $n^2 = 2(2k^2)$ is even, hence not odd (Theorem 1.1.2), against the hypothesis; so this case cannot occur ($\bot$E). *Case 2:* $n = 2k + 1$. Then n is odd, as claimed. So n is odd.

Marking scheme. (6 points) - 1: (a) the conclusion is true, with the citation. - 2: (b) the error named as proving the converse (N5), pointing at the first line. - 1: (c) a false instance of the pattern "$Q \to P$, hence $P \to Q$". - 2: (d) a correct proof, using Theorem 1.1.2 (cases on the parity of n with the even case shown impossible, or the contrapositive). Fatal errors (0 for the step): calling the conclusion false; "fixing" the proof by assuming n odd again.

Exercise. C3: Lattice points in space

A lattice point of space is a point (a, b, c) with $a, b, c \in \mathbb{Z}$.

(a) Give eight lattice points of space no two of which have a lattice point as midpoint.

(b) Show that two lattice points of space with the same three parities have a lattice point as midpoint.

(c) Which principle, stated in this section and not yet proved, would show that among any nine lattice points of space two have a lattice point as midpoint?

Solution.

(a) The eight points whose coordinates all lie in $\{0, 1\}$. Two different such points differ in some coordinate, where one has 0 and the other 1; the sum there is 1, and $1/2 \notin \mathbb{Z}$, so the midpoint is not a lattice point.

(b) As in Example (Same pattern, lattice midpoint), coordinate by coordinate: in each coordinate the two entries have the same parity, so their sum is even by Example (The parity of a sum) (a), and half of it is an integer.

(c) The pigeonhole principle. Each coordinate is even or odd, so there are $2 \cdot 2 \cdot 2 = 2^3 = 8$ parity patterns; nine points in eight patterns put two points in one pattern, and (b) finishes.

1.2 Sets, Subsets and Russell's Paradox

Section 1.1 proved statements about integers straight from their definitions. Analysis needs the same for collections, and it talks about collections all the time: the set of upper bounds of a set of numbers, the set of points where a function is positive, the set of all formulas. This section says what a set is allowed to be, what it means for one set to lie inside another, and how sets are described. One new notion carries the weight, the **subset**; the rest is the vocabulary it needs.

We begin with the simplest possible idea of a set, and we will see it fail.

1.2.1 A naive idea, and what goes wrong with it

In everyday speech a collection is given by a property. "The students in this room", "the even numbers", "the prime numbers below 100": in each case we say what an object must satisfy, and the collection is everything that satisfies it. The naive rule is:

> *For every property, there is a set whose elements are exactly the objects having that property.*

It sounds harmless, and for the properties of everyday mathematics it gives the right answer. But a property may talk about sets themselves, and then the rule can be turned against itself. A set may be an element of another set: the set $\{\mathbb{N}, \mathbb{Z}\}$ has two elements, and each of them is a set. So it makes sense to ask of a set x whether $x \in x$, and the property "$x \notin x$" is a property like any other. Most sets we know have it: the set of even numbers is not an even number, so it is not an element of itself.

Apply the naive rule to this property. It promises a set

$$R = \text{the set of all } x \text{ with } x \notin x.$$

Now ask whether $R \in R$. By the way R was made, an object belongs to R exactly when it is not an element of itself; applied to the object R, this says $R \in R$ exactly when $R \notin R$. A statement that is equivalent to its own negation leads to a contradiction by the rules of *Logic and Proof*, Chapter 2 alone; lines 4–11 of the derivation after Russell's theorem, at the end of this section, carry out exactly this argument, with an extra conjunct carried along. So the naive rule is contradictory: it cannot be part of mathematics.

This is **Russell's paradox**. We hold it until the end of the section, where it becomes a theorem, Russell's theorem, about the sets that do exist. First we set out what does work.

1.2.2 Sets and membership

We do not define "set" or "element". They are the **primitive** notions of this chapter, in the way that "statement" was primitive in *Logic and Proof*, Chapter 1: we say how they are used, not what they are made of. A **set** is a collection of objects, its **elements**, and we write

$$x \in A$$

for "x is an element of A", or "x belongs to A", or "x lies in A". Its negation is written $x \notin A$. The objects may be numbers, or sets, or (later in this chapter) pairs and functions.

In the language of *Logic and Proof*, Chapter 5, "$\in$" is a two-place predicate: $x \in A$ is a statement about the two objects x and A, true or false like $x < y$. So everything *Logic and Proof*, Chapter 5 says about predicates, quantifiers, and their rules applies to it unchanged. A statement such

as "every element of A is positive" is $\forall x\,(x \in A \to x > 0)$, which the bounded notation of Logic and Proof, Definition 5.1.1 shortens to $\forall x \in A\ (x > 0)$.

Two conventions fix what kind of objects we deal with. First, the number sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are **given**: we use them as familiar sets, with their school arithmetic and order, as *Logic and Proof* and Section 1.1 did. (*Analysis on the Real Line*, Chapter 1 turns the facts we use about $\mathbb{R}$ into consequences of axioms.) Second, **numbers are not sets**: a number has no elements, and no number is equal to a set. So $1 \neq \{1\}$, and $z \in 5$ is false for every z. *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Chapters 1, 2 and 5 explain how numbers can be built out of sets; nothing in this volume depends on how that is done.

The single most important fact about sets is that **a set is determined by its elements**. It has no other features: no order in which the elements come, no count of how often each is listed, no color. Two sets with the same elements are the same set.

Definition 1.2.1. Equality of Sets

Sets A and B are equal, $A = B$, if and only if they have the same elements:

$$\forall x\,(x \in A \leftrightarrow x \in B).$$

In words: every element of A is an element of B, and every element of B is an element of A. This principle is called **extensionality**: a set is fixed by its extension, the things it contains, and not by the words used to describe it. The sign $=$ here is not new: it is the equality of Logic and Proof, Definition 5.7.1, "names of the same object". The direction from $A = B$ to the same elements is =E, with φ the formula $x \in z$ and z the variable replaced (and symmetry, Logic and Proof, Proposition 5.7.1, for the way back from B to A). The converse direction is the principle just stated, that a set has no features beyond its elements; it is what lets an equation proved from "same elements" be used with =E like any other. The principle is an "if and only if", so it is used in both directions: to prove $A = B$, prove the $\forall$ statement; from $A = B$, conclude $x \in A \leftrightarrow x \in B$ for any x we like.

Sets with finitely many elements can be written by **listing** their elements between braces: $\{1, 2, 3\}$ is the set whose elements are 1, 2, and 3, and nothing else. Extensionality has two immediate consequences for such lists.

- **Repetition does not matter.** $\{1, 1, 2\} = \{1, 2\}$. An object x belongs to the left side exactly when $x = 1$ or $x = 1$ or $x = 2$, and to the right side exactly when $x = 1$ or $x = 2$; the two conditions are equivalent, since "$x = 1$ or $x = 1$" says no more than "$x = 1$".
- **Order does not matter.** $\{1, 2\} = \{2, 1\}$. Here the two conditions are "$x = 1$ or $x = 2$" and "$x = 2$ or $x = 1$", which are equivalent because $\vee$ commutes (Logic and Proof, Example (First derivations with "or")).

Order and repetition are exactly what a list has and a set does not. When order matters we will need a different object, the ordered pair of Section 1.4.

A set with one element, $\{a\}$, is a **singleton**. A singleton and its element are different things: $\{1\}$ is a set, and 1 is a number, so $1 \neq \{1\}$ by our convention. For sets the difference is just as real. The set $\{\mathbb{N}\}$ has exactly one element, namely $\mathbb{N}$, while $\mathbb{N}$ has infinitely many; so they differ, by extensionality, as $2 \in \mathbb{N}$ and $2 \notin \{\mathbb{N}\}$.

Quick check. Are the sets $\{1, 2, 2, 3\}$, $\{3, 2, 1\}$, and $\{1, \{2\}, 3\}$ equal?

Solution. The first two are equal: each has exactly the elements 1, 2, 3, and repetition and order do not count. The third is different: its elements are 1, $\{2\}$, and 3. The number 2 lies in the first set, but not in the third, since $2 \neq 1$, $2 \neq 3$, and $2 \neq \{2\}$ (a number is not a set). So by Definition 1.2.1 the third set differs from the other two.

1.2.3 Subsets

Most statements about sets in analysis are not equalities but **inclusions**: every Cauchy sequence converges, every continuous function on $[a, b]$ is bounded, every upper bound of a set is at least its supremum. Each has the shape "everything of this kind is also of that kind". Before a definition, look at one such statement in the language of sets. The multiples of 6 and the multiples of 3 form sets

$$S = \{\dots, -12, -6, 0, 6, 12, \dots\}, \qquad T = \{\dots, -6, -3, 0, 3, 6, \dots\},$$

and every element of S is an element of T, because $6k = 3 \cdot (2k)$. The sets are not equal ($3 \in T$ but $3 \notin S$), yet one sits inside the other. This relation between sets deserves a name.

A set is a subset of another if everything in the first is also in the second.

Definition 1.2.2. Subset

Let A and B be sets. A is a **subset** of B, written $A \subseteq B$, if **every** element of A is an element of B:

$$\forall x\,(x \in A \to x \in B).$$

We also say that A is **contained in** B, or that B **contains** A. If $A \subseteq B$ **and** $A \neq B$, then A is a **proper subset** of B, written $A \subsetneq B$.

In words, clause by clause. The quantifier $\forall x$ ranges over every object whatsoever, not over the elements of A only; the implication $x \in A \to x \in B$ restricts attention to the elements of A, and says nothing about objects outside A. With the bounded notation of Logic and Proof, Definition 5.1.1, the same condition is $\forall x \in A\ (x \in B)$: "for every x in A, x is in B". The symbol $\subseteq$ allows equality, as $\leq$ does for numbers; the symbol $\subsetneq$ excludes it, as $<$ does. This book never writes $\subset$, which some books use for $\subseteq$ and others for $\subsetneq$.

The definition is a $\forall$ around an $\to$, and its rules are the rules of those two symbols. To **prove** $A \subseteq B$, we prove the $\forall$ statement: by the rule $\forall$I of *Logic and Proof*, Chapter 5 we open a box for an arbitrary x (in prose, "let x be arbitrary"), and inside it we prove $x \in A \to x \in B$ by $\to$I (Logic and Proof, Definition 1.4.1): assume $x \in A$ and reach $x \in B$. The two openings are always written together, as "let $x \in A$". To **use** $A \subseteq B$, we apply $\forall$E (*Logic and Proof*, Chapter 5) at the element we care about, and then $\to$E: from $A \subseteq B$ and $a \in A$, conclude $a \in B$. This gives the first named move about sets.

We call this move **element-chasing**:

Example. Method: element-chasing

Template. Begin "Let $x \in A$." Unwind the definition of A to see what is known about x. Rewind the definition of B to see what must be shown, and reach it. End "Hence $x \in B$; since x was arbitrary, $A \subseteq B$."

When to use it. The goal is an inclusion $A \subseteq B$, or any statement of the shape $\forall x\,(x \in A \to \dots)$.

The usual failure. Checking some elements of A and stopping, entry (N1) of Logic and Proof, Example (What is not allowed) (the second warning below shows it). Starting from $x \in B$ instead, which proves the converse inclusion, entry (N5). Choosing a particular x, such as $x = 0$, where an arbitrary one is needed.

Quick check. Write the first and the last sentence of an element-chasing proof that $\{n \in \mathbb{Z} : 4 \mid n\} \subseteq \{n \in \mathbb{Z} : 2 \mid n\}$. Then fill in the middle.

Solution. First: "Let $n \in \mathbb{Z}$ with $4 \mid n$." Last: "Since n was arbitrary, the inclusion holds." Middle: by Definition 1.1.2, $n = 4k$ for some $k \in \mathbb{Z}$. Then $n = 2(2k)$ with $2k \in \mathbb{Z}$, so $2 \mid n$. (Or cite Proposition 1.1.1 with $2 \mid 4$.)

Here is the move three times: two ordinary inclusions, then the degenerate one. In each, the first sentence is the pair of openings, $\forall$I and $\to$I, and the rest reaches $x \in B$.

Example. Three inclusions

(a) Show that $[1, 2] \subseteq [0, 3]$.

(b) Let S be the set of integer multiples of 6 and T the set of integer multiples of 3, as above. Show that $S \subseteq T$. By Definition 1.1.2, S consists of the integers x with $6 \mid x$, and T of those with $3 \mid x$.

(c) Let A be any set. Show that $A \subseteq A$.

Solution.

(a) Let $x \in [1, 2]$. Then $1 \le x \le 2$, by the meaning of the interval. Hence $0 \le 1 \le x$ and $x \le 2 \le 3$, so $0 \le x \le 3$, that is, $x \in [0, 3]$. Since x was arbitrary, $[1, 2] \subseteq [0, 3]$.

(b) Let $x \in S$, that is, let x be an integer with $6 \mid x$. By the definition of $\mid$, there is an integer k with $x = 6k$; choose such a k (this is $\exists$E of *Logic and Proof*, Chapter 5, and the name k is new). Then $x = 3 \cdot (2k)$, and $2k$ is an integer, so $3 \mid x$, with $2k$ as the witness ($\exists$I). Hence $x \in T$. Since x was arbitrary, $S \subseteq T$.

(c) Let $x \in A$. Then $x \in A$. Since x was arbitrary, $A \subseteq A$. The box of $\to$I opens on $x \in A$ and closes on the same line; in a derivation it is the one-line box that proves $x \in A \to x \in A$.

Part (c) is the degenerate case: every set is a subset of itself. It matters because it shows that $\subseteq$ allows equality, and so "$A \subseteq B$" alone never tells us that B has anything A lacks. To say that A is a **proper** subset, $A \subsetneq B$, we also need an element of B outside A. In part (b) that element is 3: it lies in T, not in S.

A nonexample by minimal change. Replace 6 by 4 and 3 by 6 in (b): is the set of multiples of 4 a subset of the set of multiples of 6? The first sentence of the proof still works (let $x = 4k$), but the last step fails: $4k$ need not be 6 times an integer. One element is enough to show the failure:

4 is a multiple of 4, and it is not a multiple of 6. What fails is the clause "**every** element of A" of Definition 1.2.2; here it fails at the element 4.

That last observation is worth recording in symbols, because it is how every inclusion is refuted. By the negation laws of *Logic and Proof*, Chapter 6 ($\neg\forall x\,\varphi$ is equivalent to $\exists x\,\neg\varphi$, and $\neg(\varphi \to \psi)$ to $\varphi \wedge \neg\psi$),

$$A \not\subseteq B \quad \text{means} \quad \exists x\,(x \in A \wedge x \notin B).$$

To refute an inclusion, exhibit one element of the first set that is not in the second.

Why this definition. The definition says nothing about objects outside A; that is the implication doing its job. If the $\to$ were replaced by $\wedge$, the condition $\forall x\,(x \in A \wedge x \in B)$ would say that **every object** lies in A and in B, which is false for every set we will meet (Russell's theorem at the end of this section shows that no set contains every set). This is the reason why a bounded "for every" always unfolds to an implication (Logic and Proof, Definition 5.1.1).

Warning. **Element or subset?** The symbols $\in$ and $\subseteq$ relate different things. $x \in A$ says that x is one of the objects collected in A; $B \subseteq A$ says that every object collected in B is also collected in A. For example $1 \in \{1\}$ and $\{1\} \subseteq \{1\}$, but $\{1\} \notin \{1\}$: the only element of $\{1\}$ is the number 1, which is not the set $\{1\}$. And "$1 \subseteq \{1\}$" is not a comparison worth making: 1 is a number, not a set, so the definition of $\subseteq$ does not apply to it. Before writing either symbol, ask whether the thing on the left is **one of the objects** in the set on the right, or a **collection** of such objects.

↻ **Second reading** · *An element and a subset at once*

Sometimes a set is both an element and a subset of the same set. In $C = \{1, \{1\}\}$, the set $\{1\}$ is an element (it is listed) and also a subset (its only element, 1, is listed too). Change one entry: in $\{1, 2\}$, the set $\{1\}$ is still a subset, but it is no longer an element, since the two elements are the numbers 1 and 2. Whether $\{1\} \in D$ and whether $\{1\} \subseteq D$ are two separate questions, and each is answered by looking at the elements of D.

Warning. **Checking some elements proves nothing about all of them.** To prove $A \subseteq B$, checking that a few elements of A lie in B is not enough, however many are checked. "The integers $0, 12, 24$ and -12 are multiples of 4 and of 3" does not prove that the set of multiples of 4 is a subset of the set of multiples of 3, and that inclusion is false (4 is a witness). The error is entry (N1) of the catalogue of *Logic and Proof*, Chapter 8: verifying instances and concluding a $\forall$. The rule $\forall$I needs an **arbitrary** element, one about which nothing is known except that it lies in A.

1.2.3.1 Two inclusions make an equality

The first payoff of the definition connects it with equality. An equality of sets is an $\leftrightarrow$ under a $\forall$, and by Logic and Proof, Proposition 2.4.1 an $\leftrightarrow$ is two implications. So an equality should be two inclusions.

Proposition 1.2.1. Equality Is Two Inclusions

For all sets A and B, $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

Idea. Unwind all three definitions. $A = B$ is $\forall x\,(x \in A \leftrightarrow x \in B)$; the right side is $\forall x\,(x \in A \to x \in B)$ and $\forall x\,(x \in B \to x \in A)$. Inside the $\forall$, the statements are $P \leftrightarrow Q$ on one side and $P \to Q$, $Q \to P$ on the other, with P the statement $x \in A$ and Q the statement $x \in B$; Logic and Proof, Proposition 2.4.1 says exactly that these are interchangeable. So the proof is that proposition applied at an arbitrary x, once in each direction.

Proof. ($\Rightarrow$) Suppose $A = B$. Let x be arbitrary. By Definition 1.2.1, $x \in A \leftrightarrow x \in B$, so by the first half of Logic and Proof, Proposition 2.4.1 (with P the statement $x \in A$ and Q the statement $x \in B$, used as a derived rule, Logic and Proof, Definition 2.3.1), $x \in A \to x \in B$ and $x \in B \to x \in A$. Since x was arbitrary, $\forall x\,(x \in A \to x \in B)$ and $\forall x\,(x \in B \to x \in A)$; by Definition 1.2.2, $A \subseteq B$ and $B \subseteq A$.

($\Leftarrow$) Suppose $A \subseteq B$ and $B \subseteq A$. Let x be arbitrary. By Definition 1.2.2, $x \in A \to x \in B$ and $x \in B \to x \in A$, so by the second half of Logic and Proof, Proposition 2.4.1, $x \in A \leftrightarrow x \in B$. Since x was arbitrary, $A = B$ by Definition 1.2.1.

■

The name of the proposition in words is **antisymmetry** of $\subseteq$: as for $\leq$ on numbers, $A \subseteq B$ and $B \subseteq A$ together force equality. It licenses the move that proves almost every set identity in this chapter.

Example. Method: two inclusions

Template. To prove $A = B$, write two paragraphs, labeled ($\subseteq$) and ($\supseteq$), each an element-chase (Example (Method: element-chasing)). The two paragraphs are separate boxes: neither uses the other's assumption. To compute a set, first guess it from small cases, then prove the guess this way.

When to use it. A set equality that no known law gives at once. For "$S = \emptyset$", only ($\subseteq$) needs work.

The usual failure. Proving one inclusion only, or using the assumption of the ($\subseteq$) paragraph inside the ($\supseteq$) paragraph. *Logic and Proof* wrote such a proof in prose (Logic and Proof, Example (Two inclusions)).

Quick check. To prove $\{x \in \mathbb{R} : x^2 = 1\} = \{-1, 1\}$, which inclusion needs algebra, and which only a check?

Solution. ($\subseteq$) needs algebra: $x^2 = 1$ gives $(x-1)(x+1) = 0$, so $x = 1$ or $x = -1$. ($\supseteq$) checks two cases: $1^2 = 1$ and $(-1)^2 = 1$.

1.2.3.2 Inclusions chain

The second payoff is that inclusions chain, as $\leq$ does.

Proposition 1.2.2. Inclusion Is Transitive

For all sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Idea (Scratch work). The goal $A \subseteq C$ is a $\forall$ around an $\rightarrow$, so the method of Example (Method: element-chasing) applies: let $x \in A$, and we must reach $x \in C$. Each hypothesis is a $\forall$ around an $\rightarrow$ too, and we use each at the same x. The table records the search, one move per row.

Givens	Goal
$A \subseteq B$, $B \subseteq C$	$A \subseteq C$
$A \subseteq B$, $B \subseteq C$, $x \in A$ (x arbitrary)	$x \in C$
$\ldots$, $x \in B$ (by $A \subseteq B$ at x)	$x \in C$: gap closed by $B \subseteq C$ at x

The first hypothesis carries x from A into B, the second from B into C, and nothing else is needed.

Proof. Let $x \in A$. Since $A \subseteq B$, $x \in B$; since $B \subseteq C$, $x \in C$. Since x was arbitrary, $A \subseteq C$. ■

↻ **Second reading** · *Transitivity, rule by rule*

The proof above is level-3 prose. Here is the same proof at two lower levels: first as a derivation, then as prose in which each sentence carries its rule in brackets. (These are levels 0 and 2 of *Logic and Proof*, Chapter 8; from here on the book writes level-3 prose; after one more fully tagged proof, in Section 1.3, brackets appear only on the step a proof is about.)

Unwound by Definition 1.2.2, the hypotheses are $\forall x\,(x \in A \rightarrow x \in B)$ and $\forall x\,(x \in B \rightarrow x \in C)$, and the goal is $\forall x\,(x \in A \rightarrow x \in C)$. The following is a derivation of the goal from the hypotheses. The outer box, flagged x_0, is the box of $\forall$I (*Logic and Proof*, Chapter 5); it has no assumption line.

1	$\forall x(x \in A \to x \in B)$		
2	$\forall x(x \in B \to x \in C)$		
3	x_0 | $x_0 \in A$		
4	$x_0 \in A \to x_0 \in B$		$\forall$E 1
5	$x_0 \in B$		$\to$E 4, 3
6	$x_0 \in B \to x_0 \in C$		$\forall$E 2
7	$x_0 \in C$		$\to$E 6, 5
8	$x_0 \in A \to x_0 \in C$		$\to$I 3–7
9	$\forall x(x \in A \to x \in C)$		$\forall$I 3–8

The same proof in prose, with each step's rule in brackets:

> Suppose $A \subseteq B$ and $B \subseteq C$. Let x be arbitrary [$\forall$I, opening], and suppose $x \in A$ [$\to$I, opening]. Since $A \subseteq B$, in particular $x \in A \to x \in B$ [$\forall$E], so $x \in B$ [$\to$E]. Since $B \subseteq C$, in particular $x \in B \to x \in C$ [$\forall$E], so $x \in C$ [$\to$E]. Hence $x \in A \to x \in C$ [$\to$I, closing], and since x was arbitrary, $A \subseteq C$ [$\forall$I, closing].

This proves the proposition.

At level 3, the prose a mathematician writes, the same proof is one line: *let $x \in A$; then $x \in B$ since $A \subseteq B$, and $x \in C$ since $B \subseteq C$.* The silent steps are those *Logic and Proof*, Chapter 8's convention allows: the two instances of $\forall$E at the obvious term x, and the two closing sentences. What may never be silent is the opening "let $x \in A$", and the two citations, "since $A \subseteq B$" and "since $B \subseteq C$".

Quick check. Let $A = \{1, 2\}$, $B = \{1, 2, 3\}$, and $C = \{1, 3\}$. Which of the six statements $A \subseteq B$, $B \subseteq A$, $A \subseteq C$, $C \subseteq A$, $B \subseteq C$, $C \subseteq B$ are true? For each false one, name a witness.

Solution. True: $A \subseteq B$ and $C \subseteq B$ (every listed element of A, and of C, is listed in B). False: $B \subseteq A$ (witness $3 \in B$, $3 \notin A$); $A \subseteq C$ (witness 2); $C \subseteq A$ (witness 3); $B \subseteq C$ (witness 2). Both A and C are proper subsets of B, and neither of A, C is a subset of the other.

1.2.4 Describing sets: listing and specification

Listing works for a handful of elements. For a set such as "the real numbers whose square is less than 2" we need to describe the elements by a property, as the naive rule wanted. The repair of the naive rule is small but essential: we may cut a set out **of a set we already have**.

Definition 1.2.3. Specification

Let A be a set and $P(x)$ a property of objects x. Then there is a set, written

$$\{x \in A : P(x)\},$$

whose elements are exactly the elements of A that have the property P: for every y,

$$y \in \{x \in A : P(x)\} \iff y \in A \text{ and } P(y).$$

The notation is read "the set of x in A such that $P(x)$"; the colon is read "such that" (the book never writes a bar here, so that a bar stays free for divisibility and absolute value). The letter x is a bound variable, like the x of $\forall x$: $\{x \in A : P(x)\}$ and $\{t \in A : P(t)\}$ are the same set. The set A is the **ambient set** of the description, and every set-builder in this book has one, named or fixed by the context; a set written $\{f(a) : a \in A\}$ is the image of A under f (Section 1.7), and any other set the book defines is shown to exist by (W1)–(W6) where it is introduced. By Definition 1.2.1, the equivalence in the definition determines the set completely, so "the" set is justified.

In the language of the rules: to show that y belongs to $\{x \in A : P(x)\}$, show $y \in A$ and $P(y)$; from $y \in \{x \in A : P(x)\}$, conclude both. Each is one $\leftrightarrow$E (Logic and Proof, Definition 2.4.1) with the definition, followed or preceded by $\wedge$I or $\wedge$E (Logic and Proof, Definition 1.2.5); at level 3 all of these are silent, and a proof simply writes "by definition" or nothing at all.

Specification is one of a short list of **working rules** that say which sets exist. We state them once, here, and use them from now on without comment.

(W1) **Specification.** For a set A and a property P, $\{x \in A : P(x)\}$ is a set (Definition 1.2.3).

(W2) **Listing.** Any finitely many objects $a_1, \dots, a_n$ form a set $\{a_1, \dots, a_n\}$, whose elements are exactly $a_1, \dots, a_n$.

(W3) **Unions.** For sets A and B, there is a set whose elements are exactly the objects lying in A or in B; more generally, for a family of sets indexed by a set, there is a set whose elements are exactly the objects lying in at least one member of the family (Section 1.3).

(W4) **Power sets.** For a set X, the subsets of X form a set (Section 1.3).

(W5) **Products.** For sets A and B, the ordered pairs (a, b) with $a \in A$ and $b \in B$ form a set; more generally, for a set X and $n \in \mathbb{N}$ with $n \geq 2$, the n-tuples $(x_1, \dots, x_n)$ with every $x_k \in X$ form a set (Section 1.4).

(W6) **Numbers.** $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are sets.

What matters here is what is **missing** from the list: there is no rule that collects all objects with a property, without an ambient set. The end of this section shows that such a rule would be contradictory.

↻ **Second reading** · *Where the working rules come from*

These rules are enough for everything the book does with sets until Chapter 3, which adds one more: a principle for making infinitely many choices at once (Section 1.6 shows where it is first needed). They are not axioms in the formal sense, and we do not try to derive them from fewer principles; *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 1 states the axioms of set theory behind them and shows how (W1)–(W5) and the set $\mathbb{N}$ follow from them, (W3) only for families of subsets of one given set (a family with no such ambient set needs a further axiom, which *Axiomatic Set Theory* adds), and *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapters 2 and 5 build $\mathbb{Z}$, $\mathbb{Q}$

and $\mathbb{R}$, which completes (W6).

1.2.5 The empty set

Among all sets, one is special: the set with nothing in it. It turns up constantly: as the set of real solutions of $x^2 = -1$, as the intersection of two sets with nothing in common (Section 1.3), as the domain of a function with no inputs (Section 1.5). Without it, "the set of solutions" would not always name a set.

Definition 1.2.4. Empty Set

An **empty set** is a set with no elements: a set E such that $\forall x\,(x \notin E)$.

Such a set exists. Take any set we are given, say $\mathbb{N}$, and collect its elements x with $x \neq x$; by specification (Definition 1.2.3), this is a set, and since $x = x$ for every x (=I, Logic and Proof, Definition 5.7.1), nothing has the property, so the set has no elements. There is also at most one empty set, which justifies the article "**the**".

Proposition 1.2.3. The Empty Set Is Unique

If E and E' are empty sets, then $E = E'$.

Proof. Let x be arbitrary. Since E and E' are empty, $x \notin E$ and $x \notin E'$. By Logic and Proof, Proposition 2.1.2, $x \notin E$ gives $x \in E \to x \in E'$, and $x \notin E'$ gives $x \in E' \to x \in E$. So $x \in E \leftrightarrow x \in E'$ by Logic and Proof, Proposition 2.4.1. Since x was arbitrary, $E = E'$ by Definition 1.2.1. ■

We write $\emptyset$ for **the** empty set. The same vacuous truth gives its most useful property at once: $\emptyset \subseteq A$ **for every set** A. Indeed, let x be arbitrary; $x \notin \emptyset$, so $x \in \emptyset \to x \in A$ by Logic and Proof, Proposition 2.1.2; since x was arbitrary, $\emptyset \subseteq A$. In words: to refute $\emptyset \subseteq A$ we would need an element of $\emptyset$ outside A, and $\emptyset$ has no elements at all.

The empty set is a set with no elements, and a set **containing** it is not empty. The set $\{\emptyset\}$ has exactly one element, namely $\emptyset$; so $\{\emptyset\} \neq \emptyset$, with $\emptyset$ itself as the witness: $\emptyset \in \{\emptyset\}$ and $\emptyset \notin \emptyset$. A box containing an empty box is not an empty box.

Quick check.

(a) Is $\emptyset \subseteq \emptyset$?

(b) Is $\emptyset \in \emptyset$?

(c) Which of the sets $\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\}\}$ are equal?

Solution.

(a) Yes: $\emptyset \subseteq A$ for every set A, and in particular for $A = \emptyset$. (It also follows from $A \subseteq A$.)

(b) No: $\emptyset$ has no elements, so nothing, not even $\emptyset$, belongs to it.

(c) None. $\emptyset$ has no elements, and each of the other two has exactly one, so $\emptyset$ differs from both. The only element of $\{\emptyset\}$ is $\emptyset$, and the only element of $\{\{\emptyset\}\}$ is $\{\emptyset\}$; these two elements are different by the first observation, so $\emptyset \in \{\emptyset\}$ but $\emptyset \notin \{\{\emptyset\}\}$, and the two sets differ by Definition 1.2.1.

1.2.6 Computing with set-builders

The next worked example shows how a set-builder is computed: we guess the answer, then prove the guess by two inclusions (Proposition 1.2.1).

Example. Computing sets given by a property

(a) Show that $\{x \in \mathbb{Z} : x^2 < 5\} = \{-2, -1, 0, 1, 2\}$.

(b) Show that $\{x \in \mathbb{R} : x^2 < 0\} = \emptyset$.

Solution.

(a) Write S for the left side. *Scratch:* the squares of 0, ± 1, ± 2 are below 5 and $(\pm 3)^2 = 9$ is not, so guess $S = \{-2, \ldots, 2\}$. Then prove the guess by the method of Example (Method: two inclusions); ($\subseteq$) is the inclusion that needs an argument.
($\subseteq$) Let $x \in S$. Then $x \in \mathbb{Z}$ and $x^2 < 5$, by Definition 1.2.3. We claim $|x| \leq 2$. Otherwise $|x| \geq 3$, since x is an integer, and then $x^2 = |x|^2 \geq 9 > 5$, which contradicts $x^2 < 5$. So $|x| \leq 2$, and the integers with $|x| \leq 2$ are $-2, -1, 0, 1, 2$. Hence $x \in \{-2, -1, 0, 1, 2\}$.
($\supseteq$) Let $x \in \{-2, -1, 0, 1, 2\}$. Then x is one of five integers, and we check each case: x^2 is $4, 1, 0, 1, 4$ respectively, and each is less than 5. So $x \in \mathbb{Z}$ and $x^2 < 5$, that is, $x \in S$. By Proposition 1.2.1, $S = \{-2, -1, 0, 1, 2\}$.

(b) ($\subseteq$) Let $x \in \{x \in \mathbb{R} : x^2 < 0\}$. Then x is a real number with $x^2 < 0$; but $x^2 \geq 0$ for every real x, a contradiction. So this case cannot occur, and $x \in \emptyset$ holds in it vacuously ($\bot$E, Logic and Proof, Definition 2.1.1).

($\supseteq$) $\emptyset \subseteq \{x \in \mathbb{R} : x^2 < 0\}$, because $\emptyset$ is a subset of every set.

By Proposition 1.2.1, the set is $\emptyset$. A set-builder with an impossible property is a legitimate description of $\emptyset$.

Second reading · *A finite list of cases is a proof*

Two remarks on the example. In (a), the ($\supseteq$) direction is a proof by cases over a finite list, which is legitimate (the method of Example (Method: proof by cases)): the five cases exhaust the set, because the list says exactly which elements it has. That is quite different from the error of the second warning above, where finitely many cases were checked for an infinite set. In (b), the

($\supseteq$) direction is free, and only ($\subseteq$) needs an argument. For "$S = \emptyset$" this is always so: the claim amounts to "S has no elements".

1.2.7 Russell's paradox as a theorem

We return to the contradiction of the opening. The naive rule failed on $R =$ "all x with $x \notin x$". Specification allows only the version with an ambient set: for any set A,

$$R_A \coloneqq \{x \in A : x \notin x\}$$

is a set, by (W1). What happens to the paradox now?

Theorem 1.2.4. Russell's Theorem

For every set A, the set $R_A = \{x \in A : x \notin x\}$ is **not** an element of A. Hence there is no set of which every set is an element.

Try it first (five minutes): suppose $R_A \in A$. Is $R_A \in R_A$? Try each answer in turn, and see where each one leads.

Idea. The attempt runs into the old paradox, but with one extra condition. If $R_A \in R_A$, then by specification $R_A \notin R_A$: the first answer refutes itself. If $R_A \notin R_A$, then specification puts R_A into R_A, **provided** $R_A \in A$: the second answer refutes itself only under that proviso. So the two answers together are impossible exactly when $R_A \in A$, and the conclusion is not a contradiction in mathematics but a fact: $R_A \notin A$.

We do not need to split into the two answers. The first answer is refuted outright, with no proviso, by ¬I (Logic and Proof, Definition 2.2.1); so $R_A \notin R_A$ holds whenever $R_A \in A$. That fact, fed back into specification, gives $R_A \in R_A$, and the two collide.

Proof. Let A be a set, and write R for R_A. By Definition 1.2.3, for every y,

$$y \in R \iff y \in A \text{ and } y \notin y. \qquad (*)$$

Suppose $R \in A$, for ¬I. We first show $R \notin R$. Suppose $R \in R$. Then by $(*)$ at $y = R$, $R \in A$ and $R \notin R$; in particular $R \notin R$, which contradicts $R \in R$. Hence $R \notin R$, by ¬I. Now $R \in A$ and $R \notin R$, so $R \in R$ by $(*)$ read from right to left. This contradicts $R \notin R$. Hence $R \notin A$, by ¬I.

For the second claim, suppose U were a set of which every set is an element. By the first claim with $A = U$, the set R_U is not an element of U; but R_U is a set, so it is an element of U. This contradiction shows that no such U exists.

■

↻ **Second reading** · *Russell's theorem as a derivation*

Here is the first part of the proof as a derivation, with $(*)$ as its premise, written as the universal

statement it is, and R for R_A:

1	$\forall y(y \in R \leftrightarrow (y \in A \wedge y \notin y))$	
2	$\quad R \in A$	
3	$\quad R \in R \leftrightarrow (R \in A \wedge R \notin R)$	$\forall$E 1
4	$\quad\quad R \in R$	
5	$\quad\quad R \in A \wedge R \notin R$	$\leftrightarrow$E 3, 4
6	$\quad\quad R \notin R$	$\wedge$E 5
7	$\quad\quad \bot$	$\neg$E 4, 6
8	$\quad R \notin R$	$\neg$I 4–7
9	$\quad R \in A \wedge R \notin R$	$\wedge$I 2, 8
10	$\quad R \in R$	$\leftrightarrow$E 3, 9
11	$\quad \bot$	$\neg$E 10, 8
12	$R \notin A$	$\neg$I 2–11

Every rule in it is one of $\forall$E, $\leftrightarrow$E, $\wedge$E, $\wedge$I, $\neg$E, and $\neg$I. There is **no** RAA, and no excluded middle: the inner box (lines 4–7) refutes one answer outright instead of splitting into two answers. This is worth noticing. The paradox is not an artifact of classical logic, and cannot be escaped by giving up a classical rule; it is a genuine contradiction in the naive rule, and the only repair is to change which sets exist.

What the theorem says about sets. Read with A arbitrary, the theorem says that **no set contains everything**: for every set A we have produced a set, R_A, outside it. The naive rule "any property defines a set" is exactly specification **without** the phrase "$x \in A$", and the theorem shows that the phrase cannot be dropped: with A ranging over "everything", R_A would be the paradoxical R. This is why every set-builder in this book has an ambient set, and why (W1)–(W6) contain no "set of all sets". When we want "all objects with a property", we first say where to look.

Russell's theorem: contradiction about sets. Theorem 1.2.4 proves a negative statement, $R_A \notin A$, by the shape of the "not both" half of Theorem 1.1.2: suppose the statement to be refuted, $R_A \in A$, and derive a contradiction; $\neg$I (Logic and Proof, Definition 2.2.1) then gives its negation, which is the goal. So the proof needs neither RAA nor excluded middle, as the derivation in the fold after the proof shows.

The argument has a shape that will return: a set built from A so that it disagrees with each candidate on the candidate itself. Chapter 3 proves by the same shape of argument that no function from a set X to the set of its subsets reaches every subset.

1.2.8 Exercises

1.2.8.1 A. Check your understanding

Exercise. A1

(a) Negate "$A \subseteq B$" in symbols, and then in words, with the negation pushed through the quantifier and the implication.

(b) True or false: $\{1\} \in \{\{1\}, 2\}$; $\{1\} \subseteq \{\{1\}, 2\}$; $\emptyset \subseteq \emptyset$; $\{\emptyset\} \subseteq \{1\}$. Give a reason for each.

(c) List the elements of $\{n \in \mathbb{Z} : 0 < n^2 \leq 9\}$.

(d) In an element-chasing proof of $A \subseteq B$, the first sentence is "let $x \in A$". Which rule of logic gives its first clause, and which its second?

Solution.

(a) By Definition 1.2.2, $A \subseteq B$ is $\forall x\,(x \in A \to x \in B)$. By the quantifier negation law of *Logic and Proof*, Chapter 6, its negation is equivalent to $\exists x\,\neg(x \in A \to x \in B)$, and by the law for negated implications (also *Logic and Proof*, Chapter 6) to

$$\exists x\,(x \in A \wedge x \notin B).$$

In words: some element of A is not an element of B.

(b) True: $\{1\}$ is listed as an element of $\{\{1\}, 2\}$. False: the only element of $\{1\}$ is 1, and $1 \notin \{\{1\}, 2\}$, since $1 \neq \{1\}$ (a number is not a set) and $1 \neq 2$; so 1 is a witness. True: $\emptyset$ is a subset of every set. False: $\emptyset \in \{\emptyset\}$ but $\emptyset \notin \{1\}$, since $\emptyset \neq 1$; so $\emptyset$ is a witness.

(c) $\{-3, -2, -1, 1, 2, 3\}$. The integer 0 is excluded because $0^2 = 0$ is not > 0, and integers with $|n| \geq 4$ have $n^2 \geq 16 > 9$.

(d) "Let $x \in A$" opens two boxes. Its first clause, "let x be arbitrary", is $\forall$I (*Logic and Proof*, Chapter 5); its second, "suppose $x \in A$", is $\to$I (Logic and Proof, Definition 1.4.1). The proof must then reach $x \in B$ inside both boxes.

1.2.8.2 B. Practice

Exercise. B1: A set given by an equation

Prove that $\{x \in \mathbb{R} : x^2 - 3x + 2 = 0\} = \{1, 2\}$, by two inclusions.

Solution. Write S for the left side.

($\subseteq$) Let $x \in S$. Then x is real and $x^2 - 3x + 2 = 0$. Since $x^2 - 3x + 2 = (x - 1)(x - 2)$, we have $(x - 1)(x - 2) = 0$. A product of two real numbers is zero only if one of the factors is zero, so $x - 1 = 0$ or $x - 2 = 0$, that is, $x = 1$ or $x = 2$. In either case $x \in \{1, 2\}$.

($\supseteq$) Let $x \in \{1, 2\}$, so $x = 1$ or $x = 2$. If $x = 1$, then $x^2 - 3x + 2 = 1 - 3 + 2 = 0$. If $x = 2$, then $x^2 - 3x + 2 = 4 - 6 + 2 = 0$. In either case x is a real number satisfying the equation, so $x \in S$.

By Proposition 1.2.1, $S = \{1, 2\}$.

Exercise. B2: A subset of the empty set

Let A be a set with $A \subseteq \emptyset$. Prove that $A = \emptyset$.

Solution. We have $A \subseteq \emptyset$ by hypothesis, and $\emptyset \subseteq A$ because the empty set is a subset of every set. By Proposition 1.2.1, $A = \emptyset$.

Directly: if $x \in A$, then $x \in \emptyset$ because $A \subseteq \emptyset$, which is impossible; so A has no elements, and it is **the** empty set by Proposition 1.2.3.

Exercise. B3: Equal or not?

For each pair, determine whether the two sets are equal. Justify your answer: prove each equality, and give a witness element for each inequality.

(a) $\{x \in \mathbb{Z} : 4 \mid x\}$ and $\{x \in \mathbb{Z} : 2 \mid x\}$.
(b) $\{x \in \mathbb{R} : x^2 = 4\}$ and $\{-2, 2\}$.
(c) $\{\emptyset, \{\emptyset\}\}$ and $\{\{\emptyset\}, \emptyset, \emptyset\}$.
(d) $\{x \in \mathbb{Z} : x^2 < 2\}$ and $\{x \in \mathbb{N} : x < 2\}$.

Solution.

(a) Not equal. The integer 2 lies in the second set ($2 = 2 \cdot 1$) but not in the first, since $2 = 4k$ would need $k = \frac{1}{2}$, which is not an integer. (The first set is a proper subset of the second: $x = 4k$ gives $x = 2 \cdot (2k)$.)
(b) Equal. ($\subseteq$) If x is real with $x^2 = 4$, then $(x-2)(x+2) = x^2 - 4 = 0$, so $x = 2$ or $x = -2$. ($\supseteq$) $2^2 = 4$ and $(-2)^2 = 4$.
(c) Equal. Both sets have exactly the elements $\emptyset$ and $\{\emptyset\}$: an object lies in the first exactly when it is $\emptyset$ or $\{\emptyset\}$, and in the second exactly when it is $\{\emptyset\}$ or $\emptyset$ or $\emptyset$. Order and repetition do not count.
(d) Not equal. The first set is $\{-1, 0, 1\}$: an integer with $|x| \geq 2$ has $x^2 \geq 4$, and $(-1)^2 = 1$, $0^2 = 0$, $1^2 = 1$ are below 2. The second set is $\{0, 1\}$, since $\mathbb{N}$ starts at 0. The witness -1 lies in the first set and not in the second ($-1 \notin \mathbb{N}$).

Exercise. B4: Prove or disprove

Prove each true statement, by two inclusions where it is an equality, and refute each false one with a concrete counterexample.

(a) $\{n \in \mathbb{Z} : n = 2k + 1 \text{ for some } k \in \mathbb{Z}\} = \{n \in \mathbb{Z} : n = 2k - 1 \text{ for some } k \in \mathbb{Z}\}$.
(b) $\{n \in \mathbb{Z} : 2 \mid n \text{ and } 4 \mid n\} = \{n \in \mathbb{Z} : 8 \mid n\}$.
(c) $\{x \in \mathbb{R} : x^3 = x\} = \{-1, 0, 1\}$.
(d) For all sets A, B, C: if $A \subseteq B$ and $B \not\subseteq C$, then $A \not\subseteq C$.
(e) For all sets A, B, C: if $A \subseteq B$, $B \subseteq C$ and $C \subseteq A$, then $A = C$.

Solution.

(a) **True.** ($\subseteq$) Let $n = 2k+1$ with $k \in \mathbb{Z}$. Then $n = 2(k+1)-1$, and $k+1 \in \mathbb{Z}$, so n lies in the right set. ($\supseteq$) Let $n = 2k-1$ with $k \in \mathbb{Z}$. Then $n = 2(k-1)+1$, and $k-1 \in \mathbb{Z}$, so n lies in the left set. Each direction re-indexes the witness; both sets are the odd integers.

(b) **False.** The integer 4 lies in the left set, since $4 = 2 \cdot 2$ and $4 = 4 \cdot 1$. It does not lie in the right set: $4 = 8k$ has no integer solution k, because $k \geq 1$ gives $8k \geq 8$ and $k \leq 0$ gives $8k \leq 0$. (The left set is the set of multiples of 4.)

(c) **True.** For real x, $x^3 - x = x(x-1)(x+1)$. ($\subseteq$) If $x^3 = x$, this product is 0, so one factor is 0, and $x \in \{0, 1, -1\}$. ($\supseteq$) $0^3 = 0$, $1^3 = 1$ and $(-1)^3 = -1$.

(d) **False.** Take $A = C = \emptyset$ and $B = \{1\}$. Then $A \subseteq B$, and $B \not\subseteq C$ with the witness 1; but $A \subseteq C$, since $\emptyset \subseteq \emptyset$.

(e) **True.** From $A \subseteq B$ and $B \subseteq C$, Proposition 1.2.2 gives $A \subseteq C$. Together with the hypothesis $C \subseteq A$, Proposition 1.2.1 gives $A = C$.

1.2.8.3 C. Going deeper

Exercise. C1: Every set has something outside it

Let A be a set, and let $R_A = \{x \in A : x \notin x\}$ as in Theorem 1.2.4.

(a) Let A^+ be the set whose elements are the elements of A together with the object R_A (it exists by (W2) and (W3)). Show that $A \subsetneq A^+$.

(b) Deduce from Theorem 1.2.4 that no set A has the property "every subset of A is an element of A".

Solution (Hint 1). In (a), a proper inclusion needs two things: the inclusion, and a witness in the larger set that is not in the smaller one. The theorem supplies the witness. In (b), look for a subset of A that the theorem says is not an element of A.

Solution (Hint 2). For (b): suppose, for ¬I, that every subset of A is an element of A. First show that $R_A \subseteq A$.

Solution.

(a) First, $A \subseteq A^+$: an element of A is an element of A^+ by the description of A^+. Second, $A^+ \neq A$: the object R_A lies in A^+, and $R_A \notin A$ by Theorem 1.2.4. So R_A is a witness, and $A \subsetneq A^+$.

(b) Suppose, for ¬I, that A is a set such that every subset of A is an element of A. The set R_A is a subset of A: if $y \in R_A$, then $y \in A$ (and $y \notin y$) by Definition 1.2.3. So by the assumption, $R_A \in A$, which contradicts Theorem 1.2.4. Hence no set has the property.

Part (a) says that no set is "as large as possible": there is always a set with one more element. Part (b) rules out a set containing all of its own subsets; for instance, no set A has as its elements exactly the subsets of A.

Marking scheme. (10 points) - 2: (a) proves the inclusion $A \subseteq A^+$ from the description

of A^+. - 3: (a) names R_A as the witness to $A^+ \neq A$, citing Theorem 1.2.4 for $R_A \notin A$. - 3: (b) proves $R_A \subseteq A$ by element-chasing through Definition 1.2.3. - 2: (b) combines the assumption with $R_A \subseteq A$ to get $R_A \in A$, and cites the theorem for the contradiction.

Fatal errors (0 for the step): using "the set of all sets" or any set-builder without an ambient set; taking $A^+ \neq A$ as obvious "because an element was added" (if R_A were already in A, nothing would have been added).

Exercise. C2: Antisymmetry for sets of sets

Can there be sets A and B, whose elements are themselves sets, such that $A \subseteq B$, $B \subseteq A$, and $A \neq B$? Explain why the answer does not depend on what the elements of A and B are.

Solution. No. By Proposition 1.2.1, $A \subseteq B$ and $B \subseteq A$ give $A = B$, for **all** sets A and B.

The answer does not depend on the elements, because nothing in the proof of Proposition 1.2.1 looks at them. The proof works with the statements $x \in A$ and $x \in B$ for an arbitrary object x, and uses only Definition 1.2.2, Definition 1.2.1, and the propositional law Logic and Proof, Proposition 2.4.1 applied to those two statements. Whether x is a number, a set, or a set of sets never enters. For example, with $A = \{\emptyset, \{\emptyset\}\}$ and $B = \{\{\emptyset\}, \emptyset\}$, the two inclusions hold and indeed $A = B$.

The point of the question is a habit: an element-chasing proof treats its element as a black box, and so it proves the statement for sets of anything at all.

1.3 Unions, Intersections, Complements and Families

Section 1.2 said what sets are, when two of them are equal, and when one lies inside another. It gave us ways to describe a single set, by listing or by a property cut out of an ambient set. This section makes new sets from old ones. Each connective of *Logic and Proof*, Chapter 1 gives a set operation: "or" gives the union, "and" gives the intersection, "and not" gives the difference. That observation is the thesis of the chapter: *the laws of sets are the laws of logic, read through membership*. We state it, prove the standard laws of set algebra from it, and then take the step analysis needs constantly, from two sets to a whole family of them, where "or" becomes "there exists" and "and" becomes "for all".

1.3.1 Union, intersection and difference

Here is the standard example of a new set. Let A be the set of integers divisible by 2 and B the set of integers divisible by 3. Three natural questions about an integer x are: is it divisible by 2 **or** by 3? by 2 **and** by 3? by 2 **and not** by 3? Each question collects integers into a set, and each set is built from A and B by one connective applied to the statements $x \in A$ and $x \in B$. The pattern does not depend on divisibility at all, so we name the three constructions once, for any sets.

The union collects what lies in either set, the intersection what lies in both, the difference what

lies in the first and not the second.

Definition 1.3.1. Union, Intersection, Difference

Let A and B be sets.

(a) The **union** $A \cup B$ is the set whose elements are exactly the objects lying in A **or** in B: $x \in A \cup B \iff (x \in A \vee x \in B)$.

(b) The **intersection** $A \cap B$ is the set $\{x \in A : x \in B\}$: so $x \in A \cap B \iff (x \in A \wedge x \in B)$.

(c) The **difference** $A \setminus B$ is the set $\{x \in A : x \notin B\}$: so $x \in A \setminus B \iff (x \in A \wedge x \notin B)$.

Sets A and B are **disjoint** if $A \cap B = \emptyset$. If $A \subseteq X$, the difference $X \setminus A$ is called the **complement of A in X**.

In words, clause by clause. The union exists by the working rule (W3) of Section 1.2; it is not cut out of an ambient set, since its elements come from two sets at once. The intersection and the difference **are** cut out of an ambient set, namely A, so they exist by specification (W1), and the description $\{x \in A : \dots\}$ names its ambient set as Section 1.2 requires. The "or" of the union is inclusive, as $\vee$ always is: an object in both sets is in the union. "Disjoint" means "no common element".

The complement is always written $X \setminus A$, with the ambient set X named. Many books write A^c and leave X to the reader, and a reader who guesses X wrongly gets a different set: the complement of $[0,1]$ in $[0,2]$ is $(1,2]$, and in $\mathbb{R}$ it is $(-\infty,0) \cup (1,\infty)$. There is no "complement of A" on its own: by Russell's theorem (Theorem 1.2.4) there is no set of everything outside A (such a set, joined with A, would contain every set). So this book never writes A^c.

Examples, simplest first, each checked against the membership conditions.

- **Finite sets.** For $A = \{1,2,3\}$ and $B = \{2,4\}$: $A \cup B = \{1,2,3,4\}$, $A \cap B = \{2\}$, $A \setminus B = \{1,3\}$, $B \setminus A = \{4\}$. For instance $3 \in A \setminus B$ because $3 \in A$ and $3 \notin B$; and $4 \notin A \setminus B$ because $4 \notin A$.
- **Intervals.** For $A = [0,2]$ and $B = [1,3]$: $A \cup B = [0,3]$, $A \cap B = [1,2]$, $A \setminus B = [0,1)$. The last one shows how an endpoint behaves: $1 \in B$, so $1 \notin A \setminus B$, while every x with $0 \le x < 1$ lies in A and not in B.
- **Divisibility.** With A and B the multiples of 2 and of 3 in $\mathbb{Z}$, as in the opening, $A \cap B$ is the set of multiples of 6 (this uses the school fact that an integer divisible by 2 and by 3 is divisible by 6), and $\mathbb{Z} \setminus A$ is the set of odd integers, the complement of A in $\mathbb{Z}$.
- **Degenerate cases.** For every set A: $A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$, $A \setminus \emptyset = A$, and $A \setminus A = \emptyset$. Each is one line: for example, $x \in A \setminus A$ would mean $x \in A$ and $x \notin A$, which is impossible, so $A \setminus A$ has no element. They matter because $\emptyset$ behaves for $\cup$ as 0 does for $+$, and for $\cap$ as 0 does for $\times$.

Three inclusions hold for all sets and are used without comment from now on:

$$A \cap B \subseteq A \subseteq A \cup B, \qquad A \setminus B \subseteq A.$$

Each is one element-chase that drops or adds a disjunct or a conjunct: if $x \in A \cap B$, then $x \in A$ ($\wedge$E); if $x \in A$, then $x \in A \cup B$ ($\vee$I); if $x \in A \setminus B$, then $x \in A$ ($\wedge$E).

A nonexample by minimal change: the "difference" of two sets is **not** "everything in one but not in both". The set $\{x \in A \cup B : \text{not both } x \in A \text{ and } x \in B\}$ is a different set: for $A = \{1,2,3\}$ and $B = \{2,4\}$ it is $\{1,3,4\}$, while $A \setminus B = \{1,3\}$. The element 4 is in the first and not in $A \setminus B$, because the difference keeps only elements **of** A.

Warning. **The difference is not symmetric.** In general $A \setminus B \neq B \setminus A$. With $A = \{1\}$ and $B = \{2\}$, $A \setminus B = \{1\}$ and $B \setminus A = \{2\}$, and the witness 1 lies in the first and not the second. In fact $A \setminus B$ and $B \setminus A$ are always disjoint, since an element of both would lie in A and not in A; they are equal only when both are empty, that is, when $A = B$.

Quick check. Let $X = \{1, 2, 3, 4, 5, 6\}$, $A = \{1, 2, 3\}$, and $B = \{2, 4, 6\}$. Compute $A \cup B$, $A \cap B$, $X \setminus (A \cup B)$, and $(X \setminus A) \cap (X \setminus B)$.

Solution. $A \cup B = \{1, 2, 3, 4, 6\}$ and $A \cap B = \{2\}$. Then $X \setminus (A \cup B) = \{5\}$. Also $X \setminus A = \{4, 5, 6\}$ and $X \setminus B = \{1, 3, 5\}$, whose intersection is $\{5\}$. The last two answers agree. This is the two-set case of De Morgan's law for sets, which is proved for arbitrary families later in this section.

1.3.2 Laws of sets are laws of logic

Unwinding the three definitions turns every question about $\cup$, $\cap$, and $\setminus$ into a question about $\vee$, $\wedge$, and $\neg$. Here is the dictionary, with the notions of Section 1.2 included.

On sets	Unwound through membership	Logic
$x \in A \cup B$	$x \in A \vee x \in B$	$\vee$
$x \in A \cap B$	$x \in A \wedge x \in B$	$\wedge$
$x \in A \setminus B$	$x \in A \wedge \neg(x \in B)$	$\wedge$ and $\neg$
$A = \emptyset$	$\forall x \, \neg(x \in A)$	$\neg$ under $\forall$
$A \subseteq B$	$\forall x \, (x \in A \to x \in B)$	$\to$ under $\forall$
$A = B$	$\forall x \, (x \in A \leftrightarrow x \in B)$	$\leftrightarrow$ under $\forall$

The dictionary makes an idea precise. Fix an object x and write p, q, r for the statements $x \in A$, $x \in B$, $x \in C$. Then membership of x in any set built from A, B, C by $\cup$, $\cap$, $\setminus$ is a propositional formula in p, q, r: for instance,

$$x \in A \cap (B \cup C) \iff p \wedge (q \vee r).$$

Two such sets are equal if their membership formulas can each be derived from the other, for then x lies in one exactly when it lies in the other, and x was arbitrary. So a law of propositional logic, with letters replaced by membership statements, is a law of sets. That is the thesis of this chapter.

The laws of sets are the laws of logic, read through membership.

Here are the laws used most.

Theorem 1.3.1. Algebra of Sets

For all sets A, B, and C:

(a) (commutativity) $A \cup B = B \cup A$ and $A \cap B = B \cap A$;

(b) (associativity) $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$;
(c) (distributivity) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
(d) (differences) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ and $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

Idea. Each law is a propositional equivalence under $\forall x$. *Logic and Proof*, Chapter 4 gives a uniform license for all of them at once: an equivalence that holds in every row of a truth table is derivable in both directions, by completeness, and a derived sequent may be used with its letters replaced by any statements. So one argument covers every law, and the table after the proof names, for each law, the equivalence it comes from. Two of the laws are written out as element-chases in the fold after the proof, and the chain-of-equivalences method below is how a reader proves a new law by hand.

Proof. The uniform argument. Fix one of the eight equations, $L = R$, and let φ and ψ be the propositional formulas in the atoms p, q, r that describe membership in L and in R, as in the dictionary: for the first distributive law, $\varphi = p \wedge (q \vee r)$ and $\psi = (p \wedge q) \vee (p \wedge r)$. For (a)–(c), the semantic equivalence $\varphi \equiv \psi$ is a clause of Logic and Proof, Proposition 4.5.1, with p, q, r in the places of φ, ψ, χ: (f) for (a), (h) for (b), (g) for (c). For (d), it is checked by the truth table displayed below. By Logic and Proof, Definition 4.5.4, $\varphi \models \psi$ and $\psi \models \varphi$, so by Logic and Proof, Theorem 4.8.4 (as in the step TAUT, Logic and Proof, Definition 4.8.1), $\varphi \vdash \psi$ and $\psi \vdash \varphi$. Now let x be arbitrary. Each of these two sequents may be pasted in, like a derived rule (Logic and Proof, Definition 2.3.1), with p, q, r replaced by the statements $x \in A$, $x \in B$, $x \in C$; with Definition 1.3.1, the first gives $x \in L \to x \in R$ and the second $x \in R \to x \in L$. Hence $x \in L \leftrightarrow x \in R$, and since x was arbitrary, $L = R$ by Definition 1.2.1.

The truth table for (d), with the atoms in the book's order (T before F, the last atom alternating fastest):

p	q	r	$p \wedge \neg(q \vee r)$	$(p \wedge \neg q) \wedge (p \wedge \neg r)$	$p \wedge \neg(q \wedge r)$	$(p \wedge \neg q) \vee (p \wedge \neg r)$
T	T	T	F	F	F	F
T	T	F	F	F	T	T
T	F	T	F	F	T	T
T	F	F	T	T	T	T
F	T	T	F	F	F	F
F	T	F	F	F	F	F
F	F	T	F	F	F	F
F	F	F	F	F	F	F

The fourth and fifth columns agree in every row, and so do the sixth and seventh. This proves all eight laws.

■

↻ **Second reading** · *Two laws by element-chasing, and where each law comes from*

Here are two of the laws as element-chases.

The first distributive law, in full. ($\subseteq$) Let $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$, that is, $x \in A$ and ($x \in B$ or $x \in C$). By Logic and Proof, Proposition 1.6.1, with P, Q, R replaced by $x \in A$, $x \in B$, $x \in C$, we get ($x \in A$ and $x \in B$) or ($x \in A$ and $x \in C$); that is, $x \in A \cap B$ or $x \in A \cap C$, so $x \in (A \cap B) \cup (A \cap C)$. ($\supseteq$) The same chain read backwards, using the second sequent of Logic and Proof, Proposition 1.6.1. By Proposition 1.2.1 the two sets are equal.

The second difference law, in full. ($\subseteq$) Let $x \in A \setminus (B \cap C)$. Then $x \in A$ and $\neg(x \in B \wedge x \in C)$. By Logic and Proof, Proposition 2.5.5 (d), $x \notin B$ or $x \notin C$ [RAA, inside (d)]. So $x \in A$ and ($x \notin B$ or $x \notin C$), and by Logic and Proof, Proposition 1.6.1, ($x \in A$ and $x \notin B$) or ($x \in A$ and $x \notin C$); that is, $x \in (A \setminus B) \cup (A \setminus C)$. ($\supseteq$) Let $x \in (A \setminus B) \cup (A \setminus C)$. By the second sequent of Logic and Proof, Proposition 1.6.1, $x \in A$ and ($x \notin B$ or $x \notin C$). By Logic and Proof, Proposition 2.5.5 (c), $\neg(x \in B \wedge x \in C)$, so $x \notin B \cap C$, and $x \in A \setminus (B \cap C)$. By Proposition 1.2.1 the two sets are equal.

Each law is a propositional equivalence, and the table records where each comes from: the clause of Logic and Proof, Proposition 4.5.1, and the derivations of *Logic and Proof*, Chapters 1 and 2, where they exist, that prove one or both directions directly.

Law	Clause of Logic and Proof, Proposition 4.5.1	Derived in *Logic and Proof*, Chapters 1–2
$A \cap B = B \cap A$	(f)	Logic and Proof, Proposition 1.2.1 (either direction, letters exchanged)
$A \cup B = B \cup A$	(f)	Logic and Proof, Example (First derivations with "or") (likewise)
$(A \cap B) \cap C = A \cap (B \cap C)$	(h)	Logic and Proof, Proposition 1.2.2 (left to right)
$(A \cup B) \cup C = A \cup (B \cup C)$	(h)	Logic and Proof, Example (Regrouping a disjunction) (right to left)
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	(g)	Logic and Proof, Proposition 1.6.1 (both directions)
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	(g)	none in the text (both directions are exercises in *Logic and Proof*, Chapters 1 and 2)
$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$	(b), then regrouping of $\wedge$	Logic and Proof, Proposition 2.5.5 (a), (b)
$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$	(b), then (g)	Logic and Proof, Proposition 2.5.5 (c), (d); Logic and Proof, Proposition 1.6.1

The two difference laws look alike, but their element-chases are not alike. The first needs De Morgan's laws (a) and (b), which *Logic and Proof*, Section 2.5 derives without RAA, followed by regrouping the conjunction $x \in A \wedge (x \notin B \wedge x \notin C)$ into $(x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C)$, which takes only $\wedge$E and $\wedge$I. The second needs De Morgan (d) in its ($\subseteq$) direction, and (d) is

the one of the four De Morgan laws that *Logic and Proof*, Section 2.5 derives with RAA; its ($\supseteq$) direction uses (c), derived without it. Knowing that x is not in both B and C does not by itself tell us which of the two it misses; De Morgan (d) supplies the answer "one of them", and it is the classical rule that supplies it.

Example. Method: a chain of equivalences

Template. For $L = R$: let x be arbitrary, and write $x \in L \iff \cdots \iff x \in R$, one step per line. Each step either unwinds a definition (Definition 1.3.1) or applies a propositional equivalence to membership statements, with its name on the line; a step may act on a part of the line (Logic and Proof, Proposition 6.2.4). Since $\dashv\vdash$ is used like $=$ (Logic and Proof, Proposition 2.4.3 (b)), the chain gives $x \in L \dashv\vdash x \in R$, so $x \in L \leftrightarrow x \in R$ by (a), and Definition 1.2.1 finishes.

When to use it. Identities built from $\cup$, $\cap$, $\setminus$ and families, where every step is reversible.

The usual failure. A step that holds in one direction only, written as $\iff$: for example $x \in A \implies x \in A \cup B$. When a chain will not close, look for a small witness instead (Example (Method: disproof by counterexample, proof by example)); a truth table in the statements $x \in A$, $x \in B$, $x \in C$ finds one, each row saying which of A, B, C a witness should lie in.

Example. A law by a chain

Show that $(A \setminus B) \setminus C = A \setminus (B \cup C)$ for all sets A, B, C.

Idea (Scratch work). Work from both ends. Unwind the left side as far as the definitions go, then the right side, and see what is left between them.

Givens	Goal
x arbitrary	$x \in (A \setminus B) \setminus C \iff x \in A \setminus (B \cup C)$
left unwound: $x \in A \wedge x \notin B \wedge x \notin C$	right unwound: $x \in A \wedge \neg(x \in B \vee x \in C)$
gap: $x \notin B \wedge x \notin C \iff \neg(x \in B \vee x \in C)$	closed by De Morgan (a), (b) (Logic and Proof, Proposition 2.5.5)

The gap is a propositional law with $x \in B$ and $x \in C$ in the places of P and Q, so the chain will close.

Solution. Let x be arbitrary. Then

$$\begin{aligned} & x \in (A \setminus B) \setminus C \\ \iff & (x \in A \wedge x \notin B) \wedge x \notin C && \text{[definition of } \setminus\text{, twice]} \\ \iff & x \in A \wedge (x \notin B \wedge x \notin C) && \text{[regrouping } \wedge\text{]} \\ \iff & x \in A \wedge \neg(x \in B \vee x \in C) && \text{[De Morgan (a), (b)]} \\ \iff & x \in A \wedge x \notin B \cup C && \text{[definition of } \cup\text{]} \\ \iff & x \in A \setminus (B \cup C) && \text{[definition of } \setminus\text{]} \end{aligned}$$

The definitions are those of Definition 1.3.1, the regrouping is Logic and Proof, Proposition 1.2.2 from left to right and takes only $\wedge$E and $\wedge$I from right to left, and De Morgan (a), (b) are Logic and Proof, Proposition 2.5.5, with $x \in B$, $x \in C$ for P, Q, applied to the second conjunct (Logic and Proof, Proposition 6.2.4), as is the definition of $\cup$. By Definition 1.2.1 the two sets are equal. No step needs RAA.

Quick check. Which step of the chain fails if $B \cup C$ is replaced by $B \cap C$? Show with a small witness that $(A \setminus B) \setminus C = A \setminus (B \cap C)$ can fail.

Solution. The De Morgan step. De Morgan's laws give $\neg(q \wedge r) \iff \neg q \vee \neg r$, not $\neg q \wedge \neg r$. Take $A = \{1, 2\}$, $B = \{1\}$, $C = \{2\}$: then $B \cap C = \emptyset$, so the right side is $\{1, 2\}$, while the left side is $\{2\} \setminus \{2\} = \emptyset$.

The laws let us calculate with sets as with numbers, but more symmetrically: each of $\cup$ and $\cap$ distributes over the other, whereas $\times$ distributes over $+$ and not conversely. They also let us drop brackets: by associativity, $A \cup B \cup C$ and $A \cap B \cap C$ are unambiguous.

Quick check. Which propositional equivalence proves $A \cap (A \cup B) = A$? Is it one of the clauses of Logic and Proof, Proposition 4.5.1?

Solution. Membership in the left side is $p \wedge (p \vee q)$, and in the right side p. The equivalence $p \wedge (p \vee q) \equiv p$ holds in all four rows: if p is true, both sides are true; if p is false, both are false. It is not one of the clauses of Logic and Proof, Proposition 4.5.1, so the uniform argument applies with a two-atom truth table instead of a clause. (Directly: $(\subseteq)$ is $\wedge$E; $(\supseteq)$ is $\vee$I followed by $\wedge$I.) This is one of the absorption laws.

1.3.3 Power sets

The operations so far build sets whose elements are elements of the old sets. The next construction collects **sets** as elements. Many questions of analysis quantify over subsets: "every non-empty set of reals that is bounded above has a supremum" is a statement about all subsets of $\mathbb{R}$. So the subsets of a set deserve to be collected into one set.

Definition 1.3.2. Power Set

Let X be a set. The **power set** of X is the set $\mathcal{P}(X)$ whose elements are exactly the subsets of X:

$$S \in \mathcal{P}(X) \iff S \subseteq X.$$

The set exists by the working rule (W4) of Section 1.2. Its elements are sets, and "$S \in \mathcal{P}(X)$" is just another way of writing "$S \subseteq X$". Two elements are always present: $\emptyset \in \mathcal{P}(X)$, because the empty set is a subset of every set, and $X \in \mathcal{P}(X)$, because $X \subseteq X$.

Example. Small power sets

Compute $\mathcal{P}(\emptyset)$, $\mathcal{P}(\{\emptyset\})$, and $\mathcal{P}(\{1,2\})$.

Solution. $\mathcal{P}(\emptyset) = \{\emptyset\}$. The only subset of $\emptyset$ is $\emptyset$ itself: if $S \subseteq \emptyset$, then an element of S would be an element of $\emptyset$, so S has no elements, and $S = \emptyset$ by Proposition 1.2.3. And $\emptyset \subseteq \emptyset$. So $\mathcal{P}(\emptyset)$ has exactly one element, $\emptyset$. It is **not** empty: the empty set has one subset.

$\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$. Let $S \subseteq \{\emptyset\}$. Either $\emptyset \in S$ or $\emptyset \notin S$ (excluded middle, Logic and Proof, Proposition 2.5.3). If $\emptyset \in S$, then S and $\{\emptyset\}$ have the same elements (S has no element other than $\emptyset$, since $S \subseteq \{\emptyset\}$), so $S = \{\emptyset\}$. If $\emptyset \notin S$, then S has no elements, so $S = \emptyset$. Conversely, both $\emptyset$ and $\{\emptyset\}$ are subsets of $\{\emptyset\}$.

$\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$. Let $S \subseteq \{1,2\}$. A subset of $\{1,2\}$ is determined by which of 1 and 2 it contains, by Definition 1.2.1, and for each of the two there are two cases, $1 \in S$ or $1 \notin S$, and $2 \in S$ or $2 \notin S$. The four combinations give $S = \{1,2\}$, $\{1\}$, $\{2\}$, $\emptyset$. All four are subsets of $\{1,2\}$. So $\mathcal{P}(\{1,2\})$ has exactly four elements.

In each case the number of subsets is a power of two: 1, 2, 4, for sets with 0, 1, 2 elements, because each element is independently in or out. That a set with n elements has exactly 2^n subsets is proved in Section 2.5, where counting is made exact. The name "power set" comes from this count.

Warning. **The elements of $\mathcal{P}(X)$ are subsets, not elements, of X.** For $X = \{1,2\}$: $1 \in X$ but $1 \notin \mathcal{P}(X)$, since 1 is a number, not a subset; whereas $\{1\} \in \mathcal{P}(X)$ and $\{1\} \notin X$. The correct translations are $a \in X \iff \{a\} \in \mathcal{P}(X)$, and $S \subseteq X \iff S \in \mathcal{P}(X)$.

1.3.4 Families of sets

Analysis rarely stops at two or three sets. It intersects all the intervals $(-t, t)$ with $t > 0$, or all the closed sets containing a given set, or all the subsets of $\mathbb{R}$ with some property. We need unions and intersections of many sets at once, and first a way to name "many sets at once".

Definition 1.3.3. Indexed Family

Let I be a set. A **family of sets indexed by** I, written $(A_i)_{i \in I}$, assigns to **each** $i \in I$ a set A_i. The set I is the **index set**, and A_i is the **member** of the family with index i. If X

is a set with $A_i \subseteq X$ for every $i \in I$, we speak of a **family of subsets of** X.

Here "assigns" is used in its everyday sense. Section 1.5 makes it exact for a family of subsets of a set X: such a family is a function $I \to \mathcal{P}(X)$, $i \mapsto A_i$, whose value at i is written A_i. The parentheses follow the book's rule that ordered or indexed things go in parentheses; the family $(A_i)_{i\in I}$ knows which set has which index, and two indices may carry the same set. Examples: for $I = \{1, 2\}$ the family is just a pair of sets A_1, A_2; for $I = (0, \infty)$ and $A_t = (-t, t)$ it is a family of intervals, one for each positive real t; for $I = \mathbb{N}$ it is a sequence of sets $A_0, A_1, A_2, \ldots$ (indexed from 0; the sequences of real numbers in Section 1.5 are indexed from 1), which Chapter 2 treats as a sequence defined by recursion and Chapter 3 uses to form countable unions.

"Or" becomes "for some index", and "and" becomes "for every index".

The union of a family collects what lies in at least one member; the intersection collects what lies in every member.

Definition 1.3.4. Union and Intersection of a Family

Let $(A_i)_{i\in I}$ be a family of sets.

(a) The **union** $\bigcup_{i\in I} A_i$ is the set whose elements are exactly the objects lying in A_i for **some** $i \in I$:

$$x \in \bigcup_{i\in I} A_i \iff \exists i \in I\ (x \in A_i).$$

(b) If $(A_i)_{i\in I}$ is a family of subsets of a set X, the **intersection** is

$$\bigcap_{i\in I} A_i \coloneqq \{x \in X : \forall i \in I\ (x \in A_i)\}.$$

For a set $\mathcal{S}$ whose elements are sets, $\bigcup \mathcal{S} \coloneqq \bigcup_{A\in\mathcal{S}} A$; and for a **non-empty** set $\mathcal{S} \subseteq \mathcal{P}(X)$, $\bigcap \mathcal{S} \coloneqq \bigcap_{A\in\mathcal{S}} A$. In both, the family is indexed by $\mathcal{S}$ itself, the member with index A being A.

In words, clause by clause. The union exists by (W3), like the union of two sets; when all $A_i \subseteq X$, it may also be written $\{x \in X : \exists i \in I\ (x \in A_i)\}$, since then every element of the union lies in X, and this form names its ambient set as Section 1.2 requires. The intersection is cut out of X by specification. The last sentence covers sets of sets that come with no index: $\bigcap \mathcal{S}$ is the set of objects lying in every set that belongs to $\mathcal{S}$. For example, *Analysis on the Real Line*, Chapter 1 defines $\mathbb{N}$ inside $\mathbb{R}$ as $\bigcap \mathcal{S}$, where $\mathcal{S}$ is the set of all subsets of $\mathbb{R}$ that contain 0 and are closed under $x \mapsto x + 1$; $\mathcal{S}$ is non-empty because $\mathbb{R}$ itself belongs to it.

With two sets the new definitions give the old ones back. For $I = \{1, 2\}$, "$\exists i \in \{1, 2\}$ with $x \in A_i$" says "$x \in A_1$ or $x \in A_2$", since an $i \in \{1, 2\}$ is 1 or 2; so $\bigcup_{i\in\{1,2\}} A_i = A_1 \cup A_2$, and likewise $\bigcap_{i\in\{1,2\}} A_i = A_1 \cap A_2$. The dictionary gains two rows:

On sets	Unwound through membership	Logic
$x \in \bigcup_{i\in I} A_i$	$\exists i \in I\ (x \in A_i)$	$\exists$
$x \in \bigcap_{i\in I} A_i$, for $x \in X$	$\forall i \in I\ (x \in A_i)$	$\forall$

Why the intersection is taken inside X. The ambient set is not decoration; it is forced by the case $I = \emptyset$. If I is empty, the condition $\forall i \in I\ (x \in A_i)$ is **vacuously true** for every object

x: there is no index at which it could fail (*Logic and Proof*, Chapter 5, vacuous truth for $\forall$). A definition without an ambient set, "$\bigcap_{i\in I} A_i$ = all x with $\forall i \in I$ $(x \in A_i)$", would then describe the set of all objects, which Theorem 1.2.4 forbids. Inside X, the empty intersection is simply X:

$$\bigcap_{i\in\emptyset} A_i = X, \qquad \bigcup_{i\in\emptyset} A_i = \emptyset.$$

The union needs no ambient set, because its condition $\exists i \in \emptyset$ $(x \in A_i)$ is false for every x; the empty union is empty. For a **non-empty** index set the choice of X does not matter: if some $i_0 \in I$ exists and x lies in every A_i, then in particular $x \in A_{i_0} \subseteq X$, so the condition "$x \in X$" adds nothing. Only the empty family sees X, and there it must. This is also why $\bigcap\mathcal{S}$ above asks $\mathcal{S}$ to be non-empty: a set of sets with no index carries no ambient set with it.

1.3.4.1 The smallest set closed under some steps

One use of the intersection pays a debt to *Logic and Proof*, Chapter 4. There, the formulas were described as the smallest collection of strings closed under (F1)–(F3) of Logic and Proof, Definition 4.1.1: the collection that contains the atoms and $\bot$ and is closed under the building steps (F2) and (F3). What does "smallest" mean, and why does such a collection exist? Intersections answer both questions, in any setting of this kind.

Let X be a set, and consider some **starting elements** of X and some **steps**, each of which turns elements of X into an element of X. Call a subset $S \subseteq X$ **closed** if it contains the starting elements and, whenever a step is applied to elements of S, the result lies in S.

Proposition 1.3.2. Smallest Closed Set

Let X be a set with given starting elements and steps, and let $\mathcal{S} \subseteq \mathcal{P}(X)$ be the set of closed subsets of X. Then $\mathcal{S}$ is non-empty, and $M \coloneqq \bigcap\mathcal{S}$ is closed and lies inside every closed set: M is the **smallest** closed subset of X.

Idea. An element of M is an object lying in every closed set. So M lies inside each closed set by its very definition, and each requirement of being closed, met by every closed set at once, is met by what they have in common.

Proof. The set $\mathcal{S}$ is non-empty, since X itself is closed; so $\bigcap\mathcal{S}$ is defined (Definition 1.3.4).

- M **lies inside every closed set.** If $S \in \mathcal{S}$ and $x \in M$, then x lies in every member of $\mathcal{S}$, in particular in S.
- M **is closed.** Each starting element lies in every $S \in \mathcal{S}$, hence in M. If a step is applied to elements of M, those elements lie in every $S \in \mathcal{S}$; since each such S is closed, the result lies in every $S \in \mathcal{S}$, hence in M.

This proves the proposition. ∎

For *Logic and Proof*, Chapter 4, X is the set of all strings of symbols, the starting elements are the atoms and $\bot$, and the steps are (F2) and (F3) of Logic and Proof, Definition 4.1.1; M is then the set of formulas. (That this M consists exactly of the strings with a formation sequence, as clause (F4) says, follows by strong induction along a formation sequence, Logic and Proof, Theorem 4.2.2; we do not need it here.) For *Analysis on the Real Line*, Chapter 1, $X = \mathbb{R}$, the

starting element is 0, the step is $x \mapsto x + 1$, and M is $\mathbb{N}$, the set *Analysis on the Real Line*, Chapter 1 works with.

1.3.4.2 Worked examples with a real parameter

Families indexed by an interval of real numbers are the ones analysis meets most. In each example we guess the answer, then prove it by two inclusions; the union needs a **witness index** for each point, and the intersection needs, for each point outside the answer, an index whose member **excludes** it.

Example. Unions and intersections of intervals

Show that:

(a) $\bigcup_{t\in(0,1)}[t,1] = (0,1]$;
(b) $\bigcap_{t\in(0,\infty)}(-t,t) = \{0\}$, inside $X = \mathbb{R}$;
(c) $\bigcap_{t\in(0,\infty)}(0,t) = \emptyset$, inside $X = \mathbb{R}$.

Solution.

(a) ($\subseteq$) Let $x \in \bigcup_{t\in(0,1)}[t,1]$. Then there is $t \in (0,1)$ with $x \in [t,1]$; choose such a t. So $0 < t \leq x \leq 1$, and $x \in (0,1]$.
($\supseteq$) Let $x \in (0,1]$. We need an index $t \in (0,1)$ with $t \leq x$. Take $t := x/2$. Then $0 < x/2 \leq 1/2 < 1$, so $t \in (0,1)$; and $x/2 < x \leq 1$, so $x \in [t,1]$. Hence x lies in the union. (The witness depends on x, which is allowed: the union asks for **some** index for each point.)

(b) ($\supseteq$) For every $t > 0$, $-t < 0 < t$, so $0 \in (-t,t)$. Since t was arbitrary, 0 lies in the intersection.
($\subseteq$) Let x lie in the intersection. For a real number, $x < 0$ or $x = 0$ or $x > 0$, and we argue by cases. If $x < 0$ or $x > 0$, then $|x| > 0$, so $t := |x|$ is an index, and $x \in (-|x|, |x|)$ would give $|x| < |x|$ (since x is $|x|$ or $-|x|$), which is false; this contradicts the assumption that x lies in every member, so these cases cannot occur. In the remaining case $x = 0$, and $x \in \{0\}$. The index $t = |x|$ depends on the point x it excludes.

(c) Let x lie in the intersection. With the index $t = 1$, $x \in (0,1)$, so $x > 0$. Then x is itself an index, and $x \in (0,x)$ would give $x < x$, which is false. So nothing lies in the intersection, and it is empty.

Part (c) is a degenerate case worth remembering. Each interval $(0,t)$ is non-empty, and the intervals are **nested**: $(0,s) \subseteq (0,t)$ whenever $s \leq t$. Yet nothing lies in all of them. *Analysis on the Real Line*, Chapter 1 meets the same phenomenon with a sequence of intervals, and it is why its nested interval theorem needs **closed** intervals.

A nonexample by minimal change. Close the left endpoint of (c): $\bigcap_{t>0}[0,t) = \{0\}$. The number 0 now lies in every member, since $0 \leq 0 < t$; and any $x \neq 0$ is excluded as before (if $x < 0$, by $[0,1)$; if $x > 0$, by $[0,x)$). One endpoint changes the answer from $\emptyset$ to $\{0\}$, and the element that (c) loses is exactly the endpoint 0.

Quick check. Compute $\bigcup_{t\in[1,2]}[0,t]$ and $\bigcap_{t\in[1,2]}[0,t]$, inside $X = \mathbb{R}$.

Solution. The union is $[0,2]$: each $[0,t] \subseteq [0,2]$ since $t \leq 2$, and $[0,2]$ is itself a member ($t = 2$). The intersection is $[0,1]$: $[0,1] \subseteq [0,t]$ for every $t \geq 1$, and $[0,1]$ is itself a member ($t = 1$). In general, when the members are nested and there is a largest and a smallest member, the union is the largest and the intersection the smallest.

1.3.5 De Morgan's laws for families

The laws of set algebra have versions for families, and the most used are De Morgan's laws: the complement of a union is the intersection of the complements, and the complement of an intersection is the union of the complements. In analysis they convert statements about open sets into statements about closed sets, and back. By the dictionary, they should be the quantifier negation laws of *Logic and Proof*, Chapter 6, read through membership: "not in some A_i" is "outside every A_i", and "not in every A_i" is "outside some A_i".

Theorem 1.3.3. De Morgan's Laws for Families

Let X be a set and $(A_i)_{i \in I}$ a family of subsets of X, with any index set I, including $I = \emptyset$. Then

$$X \setminus \bigcup_{i \in I} A_i = \bigcap_{i \in I} (X \setminus A_i) \quad \text{and} \quad X \setminus \bigcap_{i \in I} A_i = \bigcup_{i \in I} (X \setminus A_i).$$

All intersections here are taken inside X; the family $(X \setminus A_i)_{i \in I}$ is again a family of subsets of X, so both sides make sense.

Idea. Element-chasing (Example (Method: element-chasing)), with "or" and "and" replaced by "for some index" and "for every index". Unwind both sides of each law through membership. The first law is then a chain (Example (Method: a chain of equivalences)):

$$\begin{aligned}
& x \in X \setminus \textstyle\bigcup_{i \in I} A_i \\
\iff\ & x \in X \wedge \neg \exists i \in I\ (x \in A_i) && \text{[definitions]} \\
\iff\ & x \in X \wedge \forall i \in I\ (x \notin A_i) && \text{[quantifier negation]} \\
\iff\ & x \in X \wedge \forall i \in I\ (x \in X \setminus A_i) && \text{[using } x \in X\text{]} \\
\iff\ & x \in \textstyle\bigcap_{i \in I} (X \setminus A_i) && \text{[definition of } \textstyle\bigcap\text{]}
\end{aligned}$$

The definitions are Definition 1.3.1 and Definition 1.3.4, and the second step is Logic and Proof, Proposition 6.2.3 (b), applied to the second conjunct (Logic and Proof, Proposition 6.2.4). The third step is no law applied to a part: it uses the first conjunct $x \in X$ under the quantifier. In the second law, the left side says $\neg \forall i \in I\ (x \in A_i)$, and the right side says $\exists i \in I\ \neg(x \in A_i)$. So each law is a quantifier negation law, and each inclusion is one of its directions. We write the first law out rule by rule, since it is the chapter's model element-chase for families, and the second at level 3, tagging only the step it is about.

Before reading on: which law of Logic and Proof, *Chapter 6 turns "not in every A_i" into "outside some A_i", and which of its directions is classical?*

Proof. First law. ($\subseteq$) Let $x \in X \setminus \bigcup_{i \in I} A_i$ [$\forall$I and $\to$I, opening]. By Definition 1.3.1, $x \in X$

and $x \notin \bigcup_{i\in I} A_i$ [$\leftrightarrow$E, $\wedge$E]. Let $i \in I$ [F1, Proposition 6.1.1]. Suppose $x \in A_i$ [$\neg$I, opening]. Then $\exists j \in I\ (x \in A_j)$, with i as the witness [$\exists$I], so $x \in \bigcup_{j\in I} A_j$ by Definition 1.3.4. This contradicts $x \notin \bigcup_{j\in I} A_j$ [$\neg$E]. Hence $x \notin A_i$ [$\neg$I, closing]. With $x \in X$, this gives $x \in X \setminus A_i$ [$\wedge$I, $\leftrightarrow$E]. Since $i \in I$ was arbitrary, $\forall i \in I\ (x \in X \setminus A_i)$ [$\forall$I, closing]. With $x \in X$, this is $x \in \bigcap_{i\in I}(X \setminus A_i)$ by Definition 1.3.4. Since x was arbitrary, the inclusion holds [$\rightarrow$I, $\forall$I, closing].

($\supseteq$) Let $x \in \bigcap_{i\in I}(X \setminus A_i)$ [$\forall$I and $\rightarrow$I, opening]. Then $x \in X$, and $x \in X \setminus A_i$ for every $i \in I$ [$\leftrightarrow$E, $\wedge$E]. Suppose $x \in \bigcup_{i\in I} A_i$ [$\neg$I, opening]. Then there is $i \in I$ with $x \in A_i$; choose such an index i_0 [$\exists$E, opening, with the new name i_0]. Applying the hypothesis at i_0, $x \in X \setminus A_{i_0}$ [$\forall$E], so $x \notin A_{i_0}$ [$\leftrightarrow$E, $\wedge$E], which contradicts $x \in A_{i_0}$ [$\neg$E]. The contradiction $\bot$ does not mention i_0, so it stands outside the choice [$\exists$E, closing]. Hence $x \notin \bigcup_{i\in I} A_i$ [$\neg$I, closing], and with $x \in X$, $x \in X \setminus \bigcup_{i\in I} A_i$ [$\wedge$I, $\leftrightarrow$E]. Since x was arbitrary, the inclusion holds [$\rightarrow$I, $\forall$I, closing].

By Proposition 1.2.1, the first law holds.

Second law. ($\subseteq$) Let $x \in X \setminus \bigcap_{i\in I} A_i$, so $x \in X$ and $x \notin \bigcap_{i\in I} A_i$. Then $\forall i \in I\ (x \in A_i)$ fails: if it held, then together with $x \in X$ it would put x in $\bigcap_{i\in I} A_i$. By the bounded quantifier negation law of *Logic and Proof*, Chapter 6 ($\neg\forall i \in I\ \varphi$ gives $\exists i \in I\ \neg\varphi$, the bound kept), there is $i \in I$ with $x \notin A_i$ [RAA, inside the quantifier negation law]. Choose such an index i_0. Then $x \in X \setminus A_{i_0}$, so $x \in \bigcup_{i\in I}(X \setminus A_i)$, with i_0 as the witness.

($\supseteq$) Let $x \in \bigcup_{i\in I}(X \setminus A_i)$, and choose $i_0 \in I$ with $x \in X \setminus A_{i_0}$. Then $x \in X$ and $x \notin A_{i_0}$. If x were in $\bigcap_{i\in I} A_i$, then $x \in A_{i_0}$ by the definition, applied at i_0; so $x \notin \bigcap_{i\in I} A_i$, and $x \in X \setminus \bigcap_{i\in I} A_i$.

By Proposition 1.2.1, the second law holds. This proves the theorem.

■

The answer to the prompt: the bounded quantifier negation law of *Logic and Proof*, Chapter 6 turns $\neg\forall i \in I$ into $\exists i \in I\ \neg$, and that direction is classical because it rests on the unbounded law $\neg\forall x\,\varphi \vdash \exists x\,\neg\varphi$, which needs RAA. It is used once, in the ($\subseteq$) half of the second law. The first law and the ($\supseteq$) half of the second use no classical rule: they are the directions of quantifier negation that *Logic and Proof*, Chapter 6 derives without RAA. The pattern is the one met in the difference laws of Theorem 1.3.1, which are the case $I = \{1, 2\}$, $X = A$, $A_1 = A \cap B$, $A_2 = A \cap C$ (replacing B and C by $A \cap B$ and $A \cap C$ changes neither side): "not in every member" does not by itself name the member it misses.

The empty family. The theorem was stated for every index set, and the conventions of Definition 1.3.4 are what make that true. For $I = \emptyset$, the first law reads $X \setminus \emptyset = X$, since the empty union is $\emptyset$ and the empty intersection is X; and the second reads $X \setminus X = \emptyset$, since the empty intersection is X and the empty union is $\emptyset$. Both are true. Had the empty intersection been defined as anything other than X, the laws would have needed the hypothesis $I \neq \emptyset$.

Quick check. For $X = \mathbb{R}$ and the family indexed by $I = \{1\}$ with $A_1 = [0, 1]$, what are $\bigcup_{i\in I} A_i$ and $\bigcap_{i\in I} A_i$? What are the two sides of each of De Morgan's laws?

Solution. Both are $[0, 1]$: an x lies in A_i for some $i \in \{1\}$, or for every $i \in \{1\}$, exactly when $x \in A_1$. First law: $X \setminus \bigcup_{i\in I} A_i = \mathbb{R} \setminus [0, 1]$, and $\bigcap_{i\in I}(X \setminus A_i) = X \setminus A_1 = \mathbb{R} \setminus [0, 1]$. Second

law: $X \setminus \bigcap_{i\in I} A_i = \mathbb{R} \setminus [0,1] = \bigcup_{i\in I}(X \setminus A_i)$. A one-member family is its member, and both laws say $\mathbb{R} \setminus [0,1] = \mathbb{R} \setminus [0,1]$.

Warning. **De Morgan swapped the wrong way.** "The complement of a union is the union of the complements" is false. Take $X = \{1,2\}$, $A_1 = \{1\}$, $A_2 = \{2\}$. Then $X \setminus (A_1 \cup A_2) = X \setminus X = \emptyset$, but $(X \setminus A_1) \cup (X \setminus A_2) = \{2\} \cup \{1\} = \{1,2\}$. Complementing turns $\cup$ into $\cap$ and $\cap$ into $\cup$, just as negation turns $\exists$ into $\forall$ and $\vee$ into $\wedge$; nothing stays the same.

1.3.6 Exercises

1.3.6.1 A. Check your understanding

Exercise. A1

These parts are about Theorem 1.3.3 and its proof.

(a) Which law of *Logic and Proof*, Chapter 6 is used in the ($\subseteq$) half of the second law, and which of its directions is classical?

(b) Run the first law on $X = \mathbb{Z}$, $I = \{2,3\}$, and A_i the set of integer multiples of i. Describe both sides in words, and name two integers in each side and two outside it.

(c) What are the two sides of each law when $I = \emptyset$?

(d) Let $x \in X$. Translate $x \notin \bigcap_{i\in I} A_i$ into a statement with $\exists$. What is the correct translation if $x \in X$ is **not** assumed?

Solution.

(a) The bounded quantifier negation law of *Logic and Proof*, Chapter 6: $\neg\forall i \in I\ \varphi$ gives $\exists i \in I\ \neg\varphi$, with the bound kept. That direction is classical: it rests on the unbounded law $\neg\forall x\, \varphi \vdash \exists x\, \neg\varphi$, which needs RAA.

(b) The left side $\mathbb{Z} \setminus (A_2 \cup A_3)$ is the set of integers divisible by neither 2 nor 3. The right side $(\mathbb{Z} \setminus A_2) \cap (\mathbb{Z} \setminus A_3)$ is the set of integers that are odd and not multiples of 3. By the theorem they are equal. For instance 1 and 5 (also -1, 7) lie in both, and 3 and 4 (also 6) lie in neither.

(c) For $I = \emptyset$, the empty union is $\emptyset$ and the empty intersection is X. First law: $X \setminus \emptyset = X$ and $\bigcap_{i\in\emptyset}(X \setminus A_i) = X$. Second law: $X \setminus X = \emptyset$ and $\bigcup_{i\in\emptyset}(X \setminus A_i) = \emptyset$.

(d) By Definition 1.3.4, $x \in \bigcap_{i\in I} A_i$ means $x \in X \wedge \forall i \in I\ (x \in A_i)$. For $x \in X$, its negation is $\neg\forall i \in I\ (x \in A_i)$, which by the law of (a) is $\exists i \in I\ (x \notin A_i)$. Without $x \in X$, the negation of the conjunction is, by Logic and Proof, Proposition 2.5.5 (d), "$x \notin X$ or $\exists i \in I\ (x \notin A_i)$": an object may fail to be in the intersection simply because it is not in X, since the intersection is taken inside X.

1.3.6.2 B. Practice

Exercise. B1: Intersection and difference

Prove that $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$ for all sets A, B, C, and name the propositional

equivalence behind it.

Solution. With p, q, r for $x \in A$, $x \in B$, $x \in C$, the membership conditions are $p \wedge (q \wedge \neg r)$ and $(p \wedge q) \wedge \neg(p \wedge r)$, and the equivalence behind the law is $p \wedge (q \wedge \neg r) \equiv (p \wedge q) \wedge \neg(p \wedge r)$. Both directions have short direct derivations, which the element-chase follows.

($\subseteq$) Let $x \in A \cap (B \setminus C)$. Then $x \in A$, $x \in B$, and $x \notin C$. So $x \in A \cap B$. If x were in $A \cap C$, then $x \in C$, a contradiction; so $x \notin A \cap C$. Hence $x \in (A \cap B) \setminus (A \cap C)$.

($\supseteq$) Let $x \in (A \cap B) \setminus (A \cap C)$. Then $x \in A$, $x \in B$, and $x \notin A \cap C$. If x were in C, then, since $x \in A$, $x \in A \cap C$, a contradiction; so $x \notin C$. Hence $x \in B \setminus C$, and $x \in A \cap (B \setminus C)$.

By Proposition 1.2.1 the sets are equal. Both halves use ¬I and no classical rule.

Exercise. B2: Three families of intervals

For each family, indexed by $t \in (0, \infty)$, compute the union and the intersection (inside $X = \mathbb{R}$), and prove each answer by two inclusions.

(a) $A_t = [t, 1 + t]$;
(b) $B_t = (-t, 1/t)$;
(c) $C_t = (t, 2t)$.

Solution.

(a) *Union* $(0, \infty)$. ($\subseteq$) If $x \in [t, 1 + t]$ for some $t > 0$, then $x \geq t > 0$. ($\supseteq$) If $x > 0$, take $t := x$: then $x \in [x, 1 + x]$. *Intersection* $\emptyset$. Let x be any real number and take $t := |x| + 1 > 0$. Then $x \leq |x| < t$, so $x \notin [t, 1 + t]$. So no real number lies in every A_t.

(b) *Union* $\mathbb{R}$. ($\subseteq$) Every B_t is a set of reals. ($\supseteq$) Let $x \in \mathbb{R}$. If $x \leq 0$, take $t := 1 - x \geq 1$: then $-t = x - 1 < x$, and $1/t > 0 \geq x$, so $x \in B_t$. If $x > 0$, take $t := 1/(2x)$: then $-t < 0 < x$ and $1/t = 2x > x$, so $x \in B_t$. *Intersection* $\{0\}$. ($\supseteq$) For every $t > 0$, $-t < 0 < 1/t$. ($\subseteq$) Let x lie in every B_t. If $x < 0$, take $t := -x > 0$: $x \in B_t$ would need $-t < x$, that is, $x < x$. If $x > 0$, take $t := 1/x$: $x \in B_t$ would need $x < 1/t = x$. Both cases are impossible, so the remaining case of $x < 0$, $x = 0$, $x > 0$ holds: $x = 0$.

(c) *Union* $(0, \infty)$. ($\subseteq$) If $t < x < 2t$ for some $t > 0$, then $x > 0$. ($\supseteq$) If $x > 0$, take $t := 2x/3$: then $t = 2x/3 < x$ and $2t = 4x/3 > x$, so $x \in C_t$. *Intersection* $\emptyset$. Already two members are disjoint: $C_1 = (1, 2)$ and $C_2 = (2, 4)$ have no common element, since $x < 2$ and $x > 2$ cannot both hold. An element of every C_t would lie in both.

In each union the witness t depends on the point x. In the intersections of (a) and (b) the index that excludes x depends on x too; in (c) two fixed disjoint members, C_1 and C_2, already exclude every x. All of these are allowed by the definitions.

Exercise. B3: Canceling a union

Give sets A, B, C with $A \cup B = A \cup C$ and $B \neq C$. Then list the properties that any correct answer must have, so that a different answer can be checked against them.

Solution. Take $A = \{1\}$, $B = \emptyset$, $C = \{1\}$. Then $A \cup B = \{1\} = A \cup C$, and $B \neq C$, with the witness $1 \in C$, $1 \notin B$.

Properties of any answer. Call an element **odd one out** if it lies in exactly one of B and C.

- $B \neq C$ holds exactly when there is at least one odd one out (by Definition 1.2.1; getting such an element from $B \neq C$ uses the classical direction of quantifier negation, *Logic and Proof*, Chapter 6).
- $A \cup B = A \cup C$ holds exactly when **every** odd one out lies in A. Indeed, if $x \in B \setminus C$ and $x \notin A$, then $x \in A \cup B$ but $x \notin A \cup C$; symmetrically for $x \in C \setminus B$. Conversely, if every odd one out lies in A, then an element of $A \cup B$ either lies in A, or lies in B and then, by excluded middle on $x \in C$ (Logic and Proof, Proposition 2.5.3), in C or in A; so it lies in $A \cup C$, and symmetrically.

So an answer is correct exactly when some element lies in exactly one of B, C, and every such element lies in A. The union with A "hides" the difference between B and C; the lesson is that $\cup$ cannot be canceled.

Exercise. B4: Prove or disprove

For all sets A, B, C, decide which of these hold. Prove each true one by a chain of equivalences (Example (Method: a chain of equivalences)), and refute each false one with a concrete counterexample.

(a) $A \setminus (A \setminus B) = A \cap B$.
(b) $(A \cup B) \setminus B = A$.
(c) $(A \cup B) \setminus B = A \setminus B$.
(d) $A \cup (B \setminus C) = (A \cup B) \setminus C$.
(e) $A \cap (B \setminus C) = (A \cap B) \setminus C$.

Solution. Throughout, x is arbitrary, and p, q, r stand for $x \in A$, $x \in B$, $x \in C$.

(a) **True.** $x \in A \setminus (A \setminus B) \iff p \wedge \neg(p \wedge \neg q)$. By De Morgan (d) and (c) (Logic and Proof, Proposition 2.5.5) and double negation, this is $\iff p \wedge (\neg p \vee q)$; the direction ($\Rightarrow$) is classical, since it uses (d) and removes a double negation. By distributivity (Logic and Proof, Proposition 1.6.1) it is $\iff (p \wedge \neg p) \vee (p \wedge q)$, and $\iff p \wedge q$, since the first disjunct is impossible: in $\vee$E its case gives $\bot$ by $\wedge$E and $\neg$E, hence $p \wedge q$ by $\bot$E, and the way back is $\vee$I. That is, $x \in A \cap B$. The De Morgan and double negation steps act on the second conjunct, the double negation inside a disjunct there (Logic and Proof, Proposition 6.2.4).

(b) **False.** Take $A = B = \{1\}$. Then $(A \cup B) \setminus B = \{1\} \setminus \{1\} = \emptyset$, while $A = \{1\}$.

(c) **True.** $x \in (A \cup B) \setminus B \iff (p \vee q) \wedge \neg q \iff \neg q \wedge (p \vee q)$, by commutativity of $\wedge$ (Logic and Proof, Proposition 1.2.1), $\iff (\neg q \wedge p) \vee (\neg q \wedge q)$, by distributivity (Logic and Proof, Proposition 1.6.1), $\iff (p \wedge \neg q) \vee (q \wedge \neg q)$, by commutativity of $\wedge$ in each disjunct (Logic and Proof, Proposition 6.2.4), $\iff p \wedge \neg q$, since the second disjunct is impossible, as in (a); that is, $x \in A \setminus B$.

(d) **False.** Take $A = C = \{1\}$ and $B = \emptyset$. Then $A \cup (B \setminus C) = \{1\} \cup \emptyset = \{1\}$, while $(A \cup B) \setminus C = \{1\} \setminus \{1\} = \emptyset$.

(e) **True.** $x \in A \cap (B \setminus C) \iff p \wedge (q \wedge \neg r) \iff (p \wedge q) \wedge \neg r$, by regrouping $\wedge$ (associativity), that is, $x \in (A \cap B) \setminus C$.

In each true case the chain ends with $x \in L \iff x \in R$ for arbitrary x, and Definition 1.2.1 gives $L = R$. The false ones (b) and (d) are the minimal changes of (c) and (e): (b) forgets that the elements of $A \cap B$ are removed, and (d) forgets that C is removed from A too.

1.3.6.3 C. Going deeper

Exercise. C1: Power sets and operations

Let A and B be sets.

(a) Decide whether $\mathcal{P}(A \setminus B) = \mathcal{P}(A) \setminus \mathcal{P}(B)$ can hold. Then prove that every **non-empty** element of $\mathcal{P}(A \setminus B)$ lies in $\mathcal{P}(A) \setminus \mathcal{P}(B)$.

(b) Show by an example that $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$ can fail. Then prove that it holds if and only if $A \subseteq B$ or $B \subseteq A$.

Solution (Hint 1). In (a), test the empty set against both sides. In (b), one inclusion always holds; for the other, ask which subset of $A \cup B$ could fail to be a subset of A and of B.

Solution (Hint 2). For (b) ($\Rightarrow$), argue by the contrapositive: if $A \not\subseteq B$ and $B \not\subseteq A$, choose $a \in A \setminus B$ and $b \in B \setminus A$.

Solution.

(a) **Never.** $\emptyset \in \mathcal{P}(A \setminus B)$, since $\emptyset$ is a subset of every set. But $\emptyset \in \mathcal{P}(B)$ as well, so $\emptyset \notin \mathcal{P}(A) \setminus \mathcal{P}(B)$. The empty set is a witness for every A and B.
Now let $S \in \mathcal{P}(A \setminus B)$ be non-empty, and choose $s \in S$. Since $S \subseteq A \setminus B \subseteq A$, we have $S \in \mathcal{P}(A)$. Since $s \in A \setminus B$, $s \notin B$; so s is an element of S outside B, and $S \not\subseteq B$, that is, $S \notin \mathcal{P}(B)$. Hence $S \in \mathcal{P}(A) \setminus \mathcal{P}(B)$.

(b) *Failure.* For $A = \{1\}$, $B = \{2\}$: $\{1, 2\} \in \mathcal{P}(A \cup B)$, but $\{1, 2\}$ is a subset of neither A nor B, so $\{1, 2\} \notin \mathcal{P}(A) \cup \mathcal{P}(B)$.

One inclusion always holds. If $S \in \mathcal{P}(A)$, then $S \subseteq A \subseteq A \cup B$ (Proposition 1.2.2), so $S \in \mathcal{P}(A \cup B)$; likewise for $S \in \mathcal{P}(B)$. So $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

($\Leftarrow$) Suppose $A \subseteq B$. Then $A \cup B = B$ (if $x \in A \cup B$, then $x \in A \subseteq B$ or $x \in B$; and $B \subseteq A \cup B$). Let $S \in \mathcal{P}(A \cup B)$. Then $S \subseteq B$, so $S \in \mathcal{P}(B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B)$. With the inclusion above, equality holds. The case $B \subseteq A$ is the same with A and B exchanged.

($\Rightarrow$) We prove the contrapositive. Suppose that neither $A \subseteq B$ nor $B \subseteq A$. By the negation of $\subseteq$ (Exercise (A1) (a) records it), there is $a \in A$ with $a \notin B$, and there is $b \in B$ with $b \notin A$; choose such a and b. Let $S := \{a, b\}$. Then $S \subseteq A \cup B$, so $S \in \mathcal{P}(A \cup B)$. But $S \not\subseteq A$, because $b \in S$ and $b \notin A$; and $S \not\subseteq B$, because $a \in S$ and $a \notin B$. So $S \notin \mathcal{P}(A) \cup \mathcal{P}(B)$, and the two sets differ. Two steps here are classical: turning "$A \not\subseteq B$" into a witness uses the classical directions of quantifier negation and of the law for negated implications (*Logic and Proof*, Chapter 6; see Exercise (A1) (a)), and concluding the implication from its contrapositive is

Logic and Proof, Proposition 2.5.2.

Marking scheme. (10 points) - 2: (a) the empty set as the witness that the equality never holds, with both memberships checked. - 2: (a) a non-empty $S \subseteq A \setminus B$ is shown to lie in $\mathcal{P}(A)$ and, via an element outside B, not in $\mathcal{P}(B)$. - 1: (b) a counterexample with the offending subset named. - 2: (b) the inclusion $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$ and the direction ($\Leftarrow$). - 3: (b) ($\Rightarrow$): witnesses $a \in A \setminus B$ and $b \in B \setminus A$ named, and $\{a, b\}$ shown to lie in $\mathcal{P}(A \cup B)$ and in neither $\mathcal{P}(A)$ nor $\mathcal{P}(B)$.

A direct proof also earns the 3: assume equality and $A \not\subseteq B$, fix $a \in A \setminus B$ (1 point); for arbitrary $b \in B$, $\{a, b\} \in \mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$, and $\{a, b\} \not\subseteq B$ because $a \notin B$, so $\{a, b\} \subseteq A$ and $b \in A$, giving $B \subseteq A$ (2 points). Both routes also end with a classical step: excluded middle on $A \subseteq B$ in the direct route, the contrapositive in the book's.

Fatal errors (0 for the step): in (a), testing only non-empty subsets and concluding equality; in (b) ($\Rightarrow$), in the contrapositive route, using one witness a for both failures, or a set such as $\{a\}$ that lies in $\mathcal{P}(A)$.

Exercise. C2: Find the error

Here is a "proof" that $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$ for all sets A, B, C.

> (1) Let $x \in (A \cup B) \cap (A \cup C)$. (2) Then $x \in A \cup B$ and $x \in A \cup C$. (3) We consider two cases, according to $x \in A \cup B$. (4) *Case* $x \in A$. Then $x \in A \cup (B \cap C)$. (5) *Case* $x \in B$. Since $x \in A \cup C$, $x \in C$. (6) So $x \in B \cap C$, and hence $x \in A \cup (B \cap C)$. (7) In both cases $x \in A \cup (B \cap C)$, which proves the inclusion.

(a) Is the conclusion true?

(b) Which line fails, which rule does it break, and which entry of the catalogue of *Logic and Proof*, Chapter 8 does it commit?

(c) Give a counterexample to the illegal step itself: sets and an element for which the line's premise holds and its conclusion fails.

(d) Repair the proof.

Solution.

(a) Yes. It is the ($\supseteq$) half of the second distributive law of Theorem 1.3.1 (c).

(b) Line (5). From $x \in A \cup C$, that is, $x \in A$ or $x \in C$, it concludes $x \in C$, dropping the case $x \in A$. A disjunction is used by $\vee$E, which needs **both** cases; the line uses only one. This is a missing case, entry (N7) of the catalogue of *Logic and Proof*, Chapter 8.

(c) Take $A = \{1\}$, $B = \{1\}$, $C = \emptyset$, and $x = 1$. Then $x \in B$ (the case of line (5)) and $x \in A \cup C$ (the premise of the line), but $x \notin C$. The step is illegal although the conclusion of the whole proof is true: here $x \in A$, so $x \in A \cup (B \cap C)$ by the other case.

(d) Replace lines (5)–(6) by: *Case* $x \in B$. Since $x \in A \cup C$, there are two sub-cases. If $x \in A$, then $x \in A \cup (B \cap C)$. If $x \in C$, then $x \in B \cap C$, so $x \in A \cup (B \cap C)$. In both sub-cases $x \in A \cup (B \cap C)$. The rest of the proof stands.

1.4 Ordered Pairs, Products and Relations

Sections 1.2 and 1.3 built sets and combined them: a set is fixed by its elements, and $\cup$, $\cap$, $\setminus$ are $\vee$, $\wedge$, $\wedge\neg$ read through membership. None of this can yet say "the point $(1, 2)$ of the plane", "3 is less than 5", or "y is the square of x". Each of these is about two objects **in a given order**, and a set forgets order. This section adds one new kind of object, the ordered pair (with its longer versions, the n-tuples), and then uses it twice: to build the product $A \times B$ of two sets, and to say what a relation between two sets is. The next section needs exactly this much: a function will be given by a relation of a special kind, its graph, together with a declared target set.

1.4.1 Order matters: ordered pairs

A set remembers which objects are its elements and nothing else. By extensionality (Definition 1.2.1), $\{1, 2\} = \{2, 1\}$, since both sets have the elements 1 and 2; and $\{1, 1\} = \{1\}$, since both have the element 1 and nothing else. For a set that is exactly right. For a point of the plane it is exactly wrong. The point $(1, 2)$ lies one unit to the right of the vertical axis and two units above the horizontal one; the point $(2, 1)$ lies elsewhere. And the point $(1, 1)$ on the diagonal is a perfectly good point, with the same number in both places.

So we need an object built from two objects a and b that remembers **which came first**, and that still has two places when $a = b$. What we need to know about such an object is one fact: when two of them are equal.

An ordered pair is equal to another exactly when they agree in the first place and in the second place.

Definition 1.4.1. Ordered pair

For any objects a and b there is an object (a, b), the **ordered pair** of a and b; we call a its **first coordinate** and b its **second coordinate**. Ordered pairs have the **characteristic property**: for all a, b, c, d,

$$(a, b) = (c, d) \iff a = c \text{ and } b = d.$$

In words: to decide whether two pairs are equal, compare first coordinates with first coordinates and second with second; nothing else matters, and both comparisons must succeed. The direction ($\Leftarrow$) is nothing new: equal inputs give equal pairs, as for any construction (= E, Logic and Proof, Definition 5.7.1). The direction ($\Rightarrow$) is the content. It says that from the pair we can read off its coordinates, each in its place.

We do not say here **what** the object (a, b) is. Besides the characteristic property, we use one working convention: pairs and n-tuples are a different kind of object from numbers, just as sets are (Section 1.2), so **a pair is not a number**; and tuples of different lengths are different kinds of object, so a triple is not a pair. Nothing else about pairs is used in this chapter. *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Chapter 1 shows that a pair with this property can be built from sets alone, so that nothing new has to be assumed. Until then, the existence of pairs with this property is taken as given, alongside the working rules (W1)–(W6) of Section 1.2.

A convention about parentheses. The symbol (a, b) now has two meanings. For real numbers $a < b$ it is also the open interval $\{x \in \mathbb{R} : a < x < b\}$. The book keeps both, and context decides, as it does in every analysis text. In "$(0, 1)$ contains $\frac{1}{2}$" it is an interval. In "the point $(0, 1)$ lies

on the unit circle" it is a pair. Where both readings are near each other, the text says which is meant. This convention is stated once, here.

Example. Solving an equation between pairs

Find all real numbers x and y with $(x+y, x-y) = (3, 1)$. Then decide whether $(1, 2) = (2, 1)$ and whether $(1, 1) = (1, 1)$.

Solution. Uniqueness. By the characteristic property, $(x+y, x-y) = (3, 1)$ holds if and only if

$$x + y = 3 \quad \text{and} \quad x - y = 1.$$

Adding the two equations gives $2x = 4$, so $x = 2$; subtracting them gives $2y = 2$, so $y = 1$. *Existence.* Conversely, $x = 2$ and $y = 1$ give $(x + y, x - y) = (3, 1)$. So there is exactly one solution, $x = 2$, $y = 1$.

The pairs $(1, 2)$ and $(2, 1)$ are **not** equal. If they were, the characteristic property would give $1 = 2$ for the first coordinates. So $(1, 2) \neq (2, 1)$, by ¬I. The same test on $(1, 1)$ and $(1, 1)$ passes in both places, so they are equal; and $(1, 1)$ has two places, although both hold the same number.

The first part is typical. One equation between pairs is **two** equations between coordinates, and this is how pairs are used: an equation of pairs is split by the characteristic property, and the coordinates are compared one at a time.

The solution also has a shape worth naming. "Exactly one solution" was two claims, proved separately: any solution must be $(2, 1)$, and $(2, 1)$ is a solution. Claims of this kind come with every "the" in a definition, so the shape gets a box.

Example. Method: existence and uniqueness

Template. "There is exactly one x with $P(x)$" is two claims (Logic and Proof, Definition 5.8.1, Logic and Proof, Proposition 5.8.1). For *existence*, name a candidate x_0 and check $P(x_0)$, or obtain one from a given "there exists". For *uniqueness*, take x and x' with $P(x)$ and $P(x')$, two names about which nothing else is assumed, and prove $x = x'$; or show that every x with $P(x)$ equals x_0.

When to use it. Whenever a definition says "the": the coordinates of a pair, the value $f(x)$, the empty set (Proposition 1.2.3), an inverse.

The usual failure. Proving only one half: a uniqueness proof with no candidate, or a candidate never shown to be the only one. Also checking $P(x_0)$ twice and calling it uniqueness, and naming "the" object before either half is proved (entry (N14) of Logic and Proof, Example (What is not allowed)).

Quick check. Is there exactly one real x with $(x^2, x^3) = (4, -8)$? Is there exactly one with $(x^2, x) = (4, 3)$?

Solution. Yes for the first: $x^3 = -8$ forces $x = -2$ (uniqueness), and $(-2)^2 = 4$ (existence). No for the second: $x = 3$ is forced, but $3^2 = 9 \neq 4$, so there is no such x at all. Uniqueness held and existence failed.

Nonexample by minimal change. Replace the parentheses by braces. The set $\{1, 2\}$ has the same two numbers as the pair $(1, 2)$, but the characteristic property fails for sets: $\{1, 2\} = \{2, 1\}$, and yet $1 \neq 2$. What survives is membership: 1 and 2 are both in $\{1, 2\}$. What is lost is order, the one thing the pair was made to keep.

Why this definition. Only ($\Rightarrow$) carries content. Without it, the pair could forget its coordinates, as $\{1, 2\}$ forgets which number came first. The direction ($\Leftarrow$) could be dropped from the definition without loss: $=$ E already gives it for (a, b), as for any construction. It is stated so that the property reads as a single test for equality of pairs.

Longer lists. The same idea gives ordered triples (a, b, c), and more generally ordered **n-tuples** $(x_1, \ldots, x_n)$ for $n \in \mathbb{N}$, $n \geq 2$. Like pairs, n-tuples are taken as given, and the n-tuples with all coordinates in a set form a set, by the working rule (W5) of Section 1.2. Two n-tuples are equal if and only if they agree in every place: $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ means $x_k = y_k$ for every $k \in \{1, \ldots, n\}$. A triple is a new kind of object, not a pair whose first coordinate is a pair (by the convention stated after Definition 1.4.1). The pairs $((1, 2), 3)$ and $(1, (2, 3))$ carry the same three numbers in the same order, and it is tempting to call both "the triple $(1, 2, 3)$"; that is an identification made by convention, and exercise A1 asks whether the two pairs are equal.

Quick check. For which real numbers t is $(t^2, t) = (1, -1)$? For which is $\{t^2, t\} = \{1, -1\}$?

Solution. The pair equation holds if and only if $t^2 = 1$ and $t = -1$, so exactly for $t = -1$. The set equation holds for $t = -1$ too, since $\{1, -1\} = \{1, -1\}$. It holds for no other t: the element -1 of the right side must be t^2 or t, and $t^2 \geq 0$, so $t = -1$. Here the sets agree exactly where the pairs do, but that is luck. The pair equation $(t, 1) = (1, t)$ holds only for $t = 1$, while the set equation $\{t, 1\} = \{1, t\}$ holds for every t.

1.4.2 Cartesian products

With pairs in hand, the plane is the set of all pairs of real numbers. More generally, from any two sets we can collect all pairs whose first coordinate comes from the first set and whose second comes from the second. Taking such a collection is the working rule (W5) of Section 1.2: it is a set.

Definition 1.4.2. Cartesian product

Let A and B be sets. Their **Cartesian product** is the set

$$A \times B := \{(a, b) : a \in A,\ b \in B\}$$

of all ordered pairs with first coordinate in A and second coordinate in B. Written out, an

object p is an element of $A \times B$ if and only if

$$\exists a \in A\ \exists b \in B\ \ p = (a, b).$$

For a set X we write $X^2 := X \times X$, and, for $n \in \mathbb{N}$ with $n \geq 2$, X^n is the set of all n-tuples $(x_1, \ldots, x_n)$ with every $x_k \in X$.

In words: an element of $A \times B$ is **a pair**, and **there exist** coordinates, one in A and one in B, from which it is made. The membership condition hides two existential quantifiers, so using it means naming the coordinates, by ∃E (Logic and Proof, Proposition 6.1.1), and then matching them against any other naming by the characteristic property of pairs. That two-step move is the basic move for products; $(*)$ below packages it.

For a pair the condition simplifies, and we use the simpler form constantly:

$$(x, y) \in A \times B \iff x \in A \text{ and } y \in B. \qquad (*)$$

Here is why. If $x \in A$ and $y \in B$, then x and y themselves are coordinates of the required kind, and $(x, y) \in A \times B$ by ∃I. Conversely, let $(x, y) \in A \times B$. Then there are $a \in A$ and $b \in B$ with $(x, y) = (a, b)$ [∃E], and the characteristic property (Definition 1.4.1) gives $x = a$ and $y = b$. So $x \in A$ and $y \in B$. The characteristic property is used exactly once, in the direction $(\Rightarrow)$; without it, (x, y) might equal (a, b) with the coordinates swapped or lost, and nothing could be concluded.

We write $(*)$ for this equivalence in the rest of the section. It is the reason a product is easy to work with: membership of a pair in a product is checked one coordinate at a time.

The membership condition says that an element of $A \times B$ is made from **some** pair of coordinates. Can it be made from two different ones? The method of Example (Method: existence and uniqueness) answers this, and the answer is what lets us speak of "the first coordinate" of an element of a product.

Example. The coordinates of an element of a product

Let $p \in A \times B$. Show that there is exactly one a and exactly one b such that $a \in A$, $b \in B$ and $p = (a, b)$.

Idea (Scratch work). Existence should come straight from the definition, since membership in $A \times B$ **is** an existence statement. For uniqueness, take two namings of p and ask what connects them. Only p itself does, so the two pairs are equal, and an equation between pairs is exactly what Definition 1.4.1 splits. As givens and goal:

Givens	Goal
$p \in A \times B$	some $a \in A$, $b \in B$ with $p = (a, b)$; any two such agree
$p = (a, b)$, $a \in A$, $b \in B$ (∃E twice, Definition 1.4.2)	existence: done
$p = (a, b)$ and $p = (a', b')$	$a = a'$, $b = b'$: the gap is $(a, b) = (a', b')$ (= E), then Definition 1.4.1

The last row is the gap. Once $(a, b) = (a', b')$ is written down, the characteristic property closes it in one step.

Solution. Existence. By Definition 1.4.2 there are $a \in A$ and $b \in B$ with $p = (a, b)$. *Uniqueness.* If also $p = (a', b')$ with $a' \in A$, $b' \in B$, then $(a, b) = p = (a', b')$, so $a = a'$ and $b = b'$ by the characteristic property (Definition 1.4.1).

This licenses "**the** first coordinate of p", and so the assignment $p \mapsto$ its first coordinate, which the next section will call a function.

Quick check. Which half of the solution used Definition 1.4.2, and which used Definition 1.4.1?

Solution. Existence used Definition 1.4.2: membership in the product hands over the coordinates. Uniqueness used Definition 1.4.1: the characteristic property matches two namings of the same pair.

Set-builders with a pair pattern. We write $\{(x, y) \in A \times B : P(x, y)\}$ for $\{p \in A \times B :$ there are x, y with $p = (x, y)$ and $P(x, y)\}$, a set-builder in the sense of Definition 1.2.3. By $(*)$ and the characteristic property, (x, y) belongs to it if and only if $x \in A$, $y \in B$ and $P(x, y)$. The notation $\{(a, b) : a \in A,\ b \in B\}$ in Definition 1.4.2 is different: it names no ambient set, so it is not a set-builder. It is notation for the set that (W5) provides, and the displayed membership condition is its definition.

Example. Products, small and large

(a) Let a, b, c be three different objects, none of them a number. List $\{1, 2\} \times \{a, b, c\}$ and $\{a, b, c\} \times \{1, 2\}$.

(b) Describe $\mathbb{R}^2$ and $[0, 1] \times [0, 1]$ as sets of points of the plane.

(c) What is $\{1, 2\} \times \emptyset$?

Solution.

(a) Each of the 2 first coordinates is paired with each of the 3 second coordinates:

$$\{1, 2\} \times \{a, b, c\} = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\},$$

six pairs, all different by the characteristic property, since $1 \neq 2$ and a, b, c are different. Swapping the factors gives the six pairs $(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)$. No pair of the first list is in the second: every pair in the first list has a number as its first coordinate, and every pair in the second list has one of a, b, c there, none of which is a number; so by the characteristic property no pair of one list equals a pair of the other.

(b) $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ is the set of all pairs (x, y) of real numbers: the plane, with x the horizontal and y the vertical coordinate. By $(*)$, $(x, y) \in [0, 1] \times [0, 1]$ if and only if $0 \leq x \leq 1$ and $0 \leq y \leq 1$: the closed unit square, with its four sides.

(c) It is empty. An element p would be (a, b) with $b \in \emptyset$, and $\emptyset$ has no elements. So $\{1, 2\} \times \emptyset$ has no elements, and a set with no elements is $\emptyset$ (Proposition 1.2.3).

Part (c) is the degenerate case, and it matters: a product is empty as soon as **one** factor is. The general statement is part of the next proposition.

Quick check. List $\{0, 1\} \times \{0, 1, 2\}$. Is $(1, 1) \in \{1\} \times \emptyset$?

Solution. $\{0, 1\} \times \{0, 1, 2\} = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}$, six pairs. And $(1, 1) \notin \{1\} \times \emptyset$: by $(*)$ it would need $1 \in \emptyset$. In fact $\{1\} \times \emptyset$ has no elements at all, as in part (c) of the example.

Warning. The product is not commutative: $A \times B$ and $B \times A$ are in general different sets. For $A = \{1\}$ and $B = \{2\}$, $A \times B = \{(1, 2)\}$ and $B \times A = \{(2, 1)\}$, and $(1, 2) \neq (2, 1)$ by Example (Solving an equation between pairs). The two products have "the same size", but they do not have the same elements. (They are equal when $A = B$, and when one of the sets is empty. Exercise C2 finds exactly when even the inclusion $A \times B \subseteq B \times A$ holds.)

1.4.3 Products and the set operations

Section 1.3 showed that $\cup$, $\cap$, and $\setminus$ obey the laws of $\vee$, $\wedge$, and $\wedge\neg$. The product interacts with them just as simply, one factor at a time. We use these laws for regions of the plane (exercise B1) and for functions out of the empty set (Section 1.5), so we state them all.

Proposition 1.4.1. Products and Set Operations

For all sets A, B, C:

$$\begin{aligned} A \times (B \cup C) &= (A \times B) \cup (A \times C), \\ A \times (B \cap C) &= (A \times B) \cap (A \times C), \\ A \times (B \setminus C) &= (A \times B) \setminus (A \times C), \\ A \times \emptyset &= \emptyset, \end{aligned}$$

and the mirror-image laws, with the varying factor on the left:

$$\begin{aligned} (B \cup C) \times A &= (B \times A) \cup (C \times A), \\ (B \cap C) \times A &= (B \times A) \cap (C \times A), \\ (B \setminus C) \times A &= (B \times A) \setminus (C \times A), \\ \emptyset \times A &= \emptyset. \end{aligned}$$

Idea. As in Example (Method: element-chasing), we take an element of one side and unwind; here every element is a pair, so its coordinates are named first, by $\exists$E, and membership is then tested one coordinate at a time, by $(*)$. The first coordinate lies in A on both sides; the second lies in $B \cup C$ on one side and in "B or C" on the other, which is the same condition by Definition 1.3.1. Each law is a law of Section 1.3 in the second coordinate, with the first

coordinate carried along unchanged.

Proof. The $\cup$ law. We prove two inclusions and conclude by Proposition 1.2.1.

($\subseteq$) Let $p \in A \times (B \cup C)$. By Definition 1.4.2 there are $a \in A$ and $d \in B \cup C$ with $p = (a, d)$ [F1, Proposition 6.1.1]. By Definition 1.3.1, $d \in B$ or $d \in C$, and we argue by cases. If $d \in B$, then $p = (a, d) \in A \times B$ by $(*)$, so $p \in (A \times B) \cup (A \times C)$. If $d \in C$, then likewise $p \in A \times C \subseteq (A \times B) \cup (A \times C)$. In either case $p \in (A \times B) \cup (A \times C)$.

($\supseteq$) Let $p \in (A \times B) \cup (A \times C)$. Then $p \in A \times B$ or $p \in A \times C$. If $p \in A \times B$, there are $a \in A$ and $b \in B$ with $p = (a, b)$ [$\exists$E]; since $b \in B \subseteq B \cup C$, $(*)$ gives $p \in A \times (B \cup C)$. If $p \in A \times C$, the same argument with C in place of B gives $p \in A \times (B \cup C)$.

The $\cap$ law. Let $p \in A \times (B \cap C)$, so $p = (a, d)$ with $a \in A$ and $d \in B \cap C$. Then $d \in B$ and $d \in C$, and $(*)$ gives $p \in A \times B$ and $p \in A \times C$. Conversely, let $p \in (A \times B) \cap (A \times C)$. Since $p \in A \times B$, $p = (a, b)$ with $a \in A$ and $b \in B$. Since also $(a, b) = p \in A \times C$, $(*)$ gives $b \in C$. So $b \in B \cap C$, and $p = (a, b) \in A \times (B \cap C)$.

The $\setminus$ law. Let $p \in A \times (B \setminus C)$, so $p = (a, d)$ with $a \in A$, $d \in B$, and $d \notin C$. Then $p \in A \times B$ by $(*)$. If p were in $A \times C$, then $(*)$ would give $d \in C$, which is false; so $p \notin A \times C$, and $p \in (A \times B) \setminus (A \times C)$. Conversely, let $p \in (A \times B) \setminus (A \times C)$. Then $p = (a, b)$ with $a \in A$ and $b \in B$, and $p \notin A \times C$. If b were in C, then $(*)$ would give $p = (a, b) \in A \times C$, which is false; so $b \notin C$. Hence $b \in B \setminus C$ and $p \in A \times (B \setminus C)$.

The $\emptyset$ law. An element of $A \times \emptyset$ would be a pair (a, b) with $b \in \emptyset$, and there is no such b. So $A \times \emptyset$ has no elements, and it equals $\emptyset$ by Proposition 1.2.3.

The mirror-image laws. The same four arguments, with the roles of the two coordinates exchanged throughout, prove them: the varying set now sits in the first coordinate, and $(*)$ is applied to it there. This proves the proposition.

■

The proofs of the $\setminus$ law do not use excluded middle: both "$\notin$" conclusions are reached by assuming membership and deriving a contradiction, which is $\neg$I. Only the first law was written with every $\exists$E marked; from here on, "$p = (a, b)$ with $a \in A$ and $b \in B$" is understood to name fresh coordinates.

A proof about products usually runs like the one above: take an element, write it as a pair with named coordinates, and work coordinatewise. Here is the pattern on concrete sets.

Example. Two rectangles

Show that $([0, 2] \times [0, 1]) \cap ([1, 3] \times [0, 2]) = [1, 2] \times [0, 1]$.

Solution. Draw the two rectangles first: the first is 2 wide and 1 high, with its lower left corner at the origin; the second is 2 wide and 2 high, with its lower left corner at $(1, 0)$. They overlap in the rectangle over $[1, 2]$ of height 1. Now the proof, by two inclusions.

($\subseteq$) Let p be in the intersection. Since $p \in [0, 2] \times [0, 1]$, $p = (x, y)$ with $0 \leq x \leq 2$ and $0 \leq y \leq 1$. Since also $(x, y) = p \in [1, 3] \times [0, 2]$, $(*)$ gives $1 \leq x \leq 3$ and $0 \leq y \leq 2$. Together,

$1 \le x \le 2$ and $0 \le y \le 1$, so $p = (x, y) \in [1, 2] \times [0, 1]$ by $(*)$.

$(\supseteq)$ Let $p \in [1, 2] \times [0, 1]$, so $p = (x, y)$ with $1 \le x \le 2$ and $0 \le y \le 1$. Then $0 \le x \le 2$, so $p \in [0, 2] \times [0, 1]$; and $1 \le x \le 3$, $0 \le y \le 2$, so $p \in [1, 3] \times [0, 2]$. Hence p is in the intersection.

By Proposition 1.2.1, the two sets are equal. The picture found the answer; the element-chase proved it.

The degenerate law of the proposition deserves a second look, because it is easy to misuse.

Remark. Combining the two $\emptyset$ laws with one more step gives the full description of an empty product: $A \times B = \emptyset$ **if and only if** $A = \emptyset$ or $B = \emptyset$. The direction $(\Leftarrow)$ is the pair of $\emptyset$ laws. For $(\Rightarrow)$, suppose $A \times B = \emptyset$. If A has an element a and B has an element b, then $(a, b) \in A \times B = \emptyset$, which is impossible. So it is not the case that both sets have an element; by excluded middle (Logic and Proof, Proposition 2.5.3) applied to "A has an element", either A has none, and then $A = \emptyset$ by Proposition 1.2.3, or A has one, and then B has none, so $B = \emptyset$.

Warning. "$A \times B = \emptyset$, so $A = \emptyset$" misses a case. The product $\{1, 2\} \times \emptyset$ is empty, and $\{1, 2\}$ is not. The correct conclusion is the disjunction "$A = \emptyset$ or $B = \emptyset$" of the remark, and an argument that continues from it must treat both cases. Dropping one is the missing case of the catalogue in *Logic and Proof*, Chapter 8, entry (N7): a $\vee$E with one of its boxes left out.

1.4.4 Relations

"Is less than", "divides", "is the square of", "lies on the unit circle with": each of these connects an object of one set with an object of another, or of the same set. Each can be described by a rule, a formula, or a sentence. But two different descriptions can pick out exactly the same connections: "$x < y$" and "$y - x > 0$" are different sentences about real numbers, and they hold for exactly the same pairs (x, y). In mathematics we want these to count as the **same** relation.

The way to make them the same is to forget the description and keep what it picks out: the set of pairs (x, y) for which it holds. Two descriptions that pick out the same pairs then give the same set, by extensionality.

A relation is the set of pairs it relates.

Definition 1.4.3. Relation

Let A and B be sets. A **relation from** A **to** B is a subset $R \subseteq A \times B$. For $a \in A$ and $b \in B$ we write $a\ R\ b$, read "a is R-related to b", to mean $(a, b) \in R$. A **relation on** A is a relation from A to A, that is, a subset of A^2.

The **domain** of R is the set of first coordinates that occur, $\{a \in A : \exists b \in B \ \ a\ R\ b\}$, and its **range** is the set of second coordinates that occur, $\{b \in B : \exists a \in A \ \ a\ R\ b\}$. Turning every pair of R around gives a relation from B to A, the **inverse relation**

$$R^{-1} \coloneqq \{(b, a) \in B \times A : (a, b) \in R\}.$$

In words: a relation **is** a set, namely a set of pairs whose coordinates come from the two given sets. The notation $a\ R\ b$ is only a way of writing "$(a, b) \in R$" that reads like "$a < b$". The domain collects the elements of A that are related to **at least one** element of B; the range collects those of B that something is related to. The inverse relation turns each pair around: $b\ R^{-1}\ a$ exactly when $a\ R\ b$.

Two relations are equal exactly when they relate the same pairs, since relations are sets (Definition 1.2.1). So the relation "$x < y$" on $\mathbb{R}$ and the relation "$y - x > 0$" on $\mathbb{R}$ are one relation, as we wanted. That is the whole reason for the definition: a relation is determined by **what** it relates, not by **how** it is described.

Example. Relations as sets of pairs

Write each relation as a set, and find its domain and range.

(a) The relation $<$ on $\{1, 2, 3\}$.
(b) Divisibility on $\{1, \dots, 6\}$: $a\ D\ b$ when $a \mid b$.
(c) The unit circle, as a relation on $\mathbb{R}$.
(d) The graph of squaring, as a relation on $\mathbb{R}$.
(e) The two extreme relations from A to B: $\emptyset$ and $A \times B$.

Solution.

(a) The pairs (a, b) of elements of $\{1, 2, 3\}$ with $a < b$ are

$$L \coloneqq \{(1, 2), (1, 3), (2, 3)\},$$

three of the nine elements of $\{1, 2, 3\}^2$. Its domain is $\{1, 2\}$, since nothing in the set is larger than 3; its range is $\{2, 3\}$, since nothing is smaller than 1.

(b) Write $a \mid b$ when $b = ak$ for some integer k. For each first coordinate a, the second coordinates $b \in \{1, \dots, 6\}$ with $a \mid b$ are the multiples of a up to 6:

a	the $b \in \{1, \dots, 6\}$ with $a \mid b$
1	$1, 2, 3, 4, 5, 6$
2	$2, 4, 6$
3	$3, 6$
4	4
5	5
6	6

So D has $6+3+2+1+1+1 = 14$ elements, the pairs (a, b) read off the rows. Its domain and range are both all of $\{1, \ldots, 6\}$, because every a divides itself: $(a, a) \in D$.

(c) The unit circle is

$$S \coloneqq \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\},$$

a relation on $\mathbb{R}$; for instance $0\ S\ 1$, $0\ S\ (-1)$, and $1\ S\ 0$. Its domain is $[-1, 1]$. If $x\ S\ y$, then $x^2 = 1 - y^2 \leq 1$, so $-1 \leq x \leq 1$. Conversely, for $-1 \leq x \leq 1$ the number $1 - x^2$ is nonnegative and so has a square root $y = \sqrt{1 - x^2}$, which satisfies $x^2 + y^2 = 1$. By the symmetry of the equation, the range is $[-1, 1]$ too.

(d) The graph of squaring is $Q \coloneqq \{(x, y) \in \mathbb{R}^2 : y = x^2\}$. Its domain is all of $\mathbb{R}$: every x is related to x^2. Its range is $[0, \infty)$: a square is nonnegative, and every $y \geq 0$ is the square of $\sqrt{y}$.

(e) Both are subsets of $A \times B$, so both are relations. The **empty relation** $\emptyset$ relates nothing, and its domain and range are empty. The **full relation** $A \times B$ relates everything to everything. If A and B both have elements, its domain is A and its range is B.

The circle and the graph of squaring look alike, both being curves in the plane, but they differ in a way that the next section makes precise. In Q every x is related to **exactly one** y. In S the number 0 is related to two numbers, 1 and -1, and the number 2 to none. A relation of the first kind will be the graph of a function.

Quick check. Write the inverse relation L^{-1} of part (a) as a set. Which familiar relation on $\{1, 2, 3\}$ is it?

Solution. Turning each pair of L around gives $L^{-1} = \{(2, 1), (3, 1), (3, 2)\}$: the pairs (b, a) with $b > a$. So L^{-1} is the relation $>$ on $\{1, 2, 3\}$. Its domain $\{2, 3\}$ is the range of L, and its range $\{1, 2\}$ is the domain of L.

Nonexample by minimal change. The set $\{(1, 2), (2, 3), 3\}$ looks like the relation "is one less than" on $\{1, 2, 3\}$, with one pair damaged. It is not a relation on $\{1, 2, 3\}$: the element 3 is a number, not a pair (the convention after Definition 1.4.1), so the set is not a subset of $\{1, 2, 3\}^2$. Remove the 3, or replace it by the pair $(3, 4)$ and enlarge the second set to $\{1, 2, 3, 4\}$, and it becomes a relation. The clause that failed is "$R \subseteq A \times B$": every element of a relation must be a pair with coordinates in the right sets.

Why this definition. A relation could be defined as a rule, a sentence, or a formula. Each of those raises the question of when two rules are "the same", and that question has no good answer: "$x < y$" and "$y - x > 0$" are different sentences. The definition as a set answers it by extensionality. The price is small: a relation may be any set of pairs whatever, such as $\{(1, 3), (2, 2)\}$ on $\{1, 2, 3\}$, and the definition never asks for a rule that produces it. That is a gain, not a loss: in analysis we meet relations and functions that no formula describes.

Warning. A relation "from A to B" has its direction built in: $R \subseteq A \times B$, and the first coordinate comes from A. The relation L of part (a) contains $(1, 2)$ and not $(2, 1)$. Reading a relation backwards, "since $1\ L\ 2$, also $2\ L\ 1$", treats it as a symmetric relation; relations with

that property, and other properties such as transitivity, are studied in Chapter 4. Relating b to a is the job of the inverse relation R^{-1}, a different set.

This definition is all the next section needs. The graph of a function from X to Y will be a relation from X to Y in which every element of X is related to exactly one element of Y; the function is that graph together with the declared codomain Y. The graph Q qualifies and the circle S does not. The properties that make a relation an order or an equivalence (reflexive, symmetric, antisymmetric, transitive) are the subject of Chapter 4.

1.4.5 Exercises

1.4.5.1 A. Check your understanding

Exercise. A1

(a) Define $A \times B$ in symbols, with its membership condition written out using quantifiers.

(b) Is $((1,2),3) = (1,(2,3))$? Justify your answer.

(c) Write the inverse of the relation $<$ on $\{1,2,3\}$ as a set of pairs.

(d) Is $\emptyset$ a relation on every set A? Justify your answer.

Solution.

(a) $A \times B = \{(a,b) : a \in A,\ b \in B\}$; that is, $p \in A \times B$ if and only if $\exists a \in A\ \exists b \in B\ \ p = (a,b)$ (Definition 1.4.2).

(b) No. Both are ordered pairs, so by the characteristic property (Definition 1.4.1) they are equal if and only if their first coordinates are equal and their second coordinates are equal. The first coordinates are the pair $(1,2)$ and the number 1. A pair is not a number, by the working convention stated after Definition 1.4.1 (*Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Chapter 1, which builds both from sets, bears it out). So the first coordinates differ, and the pairs are not equal. Calling both "the triple $(1,2,3)$" is an identification made by convention, not an equality.

(c) $\{(2,1),(3,1),(3,2)\}$, which is the relation $>$ on $\{1,2,3\}$.

(d) Yes. A relation on A is a subset of $A \times A$, and $\emptyset \subseteq A \times A$: the condition "$x \in \emptyset \to x \in A \times A$" holds for every x, because its hypothesis is false (Logic and Proof, Proposition 2.1.2, Definition 1.2.2).

1.4.5.2 B. Practice

Exercise. B1: An L-shaped region

Let $E := ([0,1] \times [0,2]) \cup ([1,2] \times [0,1])$. Describe E as a region of the plane. Then use Proposition 1.4.1 to write E as $([0,2] \times [0,1]) \cup (P \times Q)$ for intervals P and Q, and prove the equality.

Solution. The first rectangle is 1 wide and 2 high, standing on the origin; the second is 1 wide and 1 high, standing on $[1,2]$. Together they form an "L": a bottom strip $[0,2] \times [0,1]$ of width 2, with a square $[0,1] \times [1,2]$ on top of its left half. So we expect $P = [0,1]$ and

$Q = [1, 2]$.

Now the proof. Since $[0, 2] = [0, 1] \cup [1, 2]$, the first law of Proposition 1.4.1 gives

$$[0, 1] \times [0, 2] = ([0, 1] \times [0, 1]) \cup ([0, 1] \times [1, 2]),$$

and the mirror-image $\cup$ law gives

$$[0, 2] \times [0, 1] = ([0, 1] \times [0, 1]) \cup ([1, 2] \times [0, 1]).$$

Substituting the first equation into the definition of E and regrouping the unions ($\cup$ is commutative and associative by Theorem 1.3.1),

$$\begin{aligned} E &= ([0, 1] \times [0, 1]) \cup ([0, 1] \times [1, 2]) \cup ([1, 2] \times [0, 1]) \\ &= ([0, 2] \times [0, 1]) \cup ([0, 1] \times [1, 2]), \end{aligned}$$

where the second line uses the mirror-image equation. So $P = [0, 1]$ and $Q = [1, 2]$. (The equality $[0, 2] = [0, 1] \cup [1, 2]$ is an order fact: $0 \le x \le 2$ holds exactly when $0 \le x \le 1$ or $1 \le x \le 2$.)

Exercise. B2: The intersection law, written with two pairs

Here is a proof of the inclusion ($\supseteq$) of $A \times (B \cap C) = (A \times B) \cap (A \times C)$ that works from the definition of the product and the characteristic property directly, without the shortcut ($*$). Its last sentence is blank. *Name the move, then complete it.*

> Let $p \in (A \times B) \cap (A \times C)$. Since $p \in A \times B$, there are $a \in A$ and $b \in B$ with $p = (a, b)$. Since $p \in A \times C$, there are $a' \in A$ and $c \in C$ with $p = (a', c)$; the names a' and c are new, because nothing says that this second pair of coordinates is the first one again. Hence $(a, b) = (a', c)$. _____

Solution. The move is the second half of the section's move, the characteristic property of pairs (Definition 1.4.1) in the direction ($\Rightarrow$). An equation between pairs splits into equations between coordinates.

The completed last sentence: *By the characteristic property, $a = a'$ and $b = c$; so $b \in B$ and $b = c \in C$, hence $b \in B \cap C$, and $p = (a, b) \in A \times (B \cap C)$.*

The names a' and c had to be fresh (a second $\exists$E may not reuse the names of the first), and the characteristic property is what shows, afterwards, that the two namings name the same coordinates. The proof of Proposition 1.4.1 took the same step through ($*$), which packages exactly this use of the characteristic property.

Exercise. B3: Two products crossed

Prove that $(A \times B) \cap (B \times A) = (A \cap B) \times (A \cap B)$ for all sets A and B.

Solution. We prove two inclusions and conclude by Proposition 1.2.1.

($\subseteq$) Let $p \in (A \times B) \cap (B \times A)$. Since $p \in A \times B$, $p = (x, y)$ with $x \in A$ and $y \in B$. Since also $(x, y) = p \in B \times A$, $(*)$ gives $x \in B$ and $y \in A$. So $x \in A \cap B$ and $y \in A \cap B$, and $p = (x, y) \in (A \cap B) \times (A \cap B)$ by $(*)$.

($\supseteq$) Let $p \in (A \cap B) \times (A \cap B)$, so $p = (x, y)$ with $x, y \in A \cap B$. Then $x \in A$ and $y \in B$, so $p \in A \times B$; and $x \in B$ and $y \in A$, so $p \in B \times A$. Hence $p \in (A \times B) \cap (B \times A)$.

Exercise. B4: Prove or disprove

Prove each true statement by the method of Example (Method: existence and uniqueness), or the section's element arguments, and refute each false one with a concrete counterexample.

(a) For all real a and b there is exactly one pair (x, y) of real numbers with $(3x-y, x+2y) = (a, b)$.

(b) For every real a there is exactly one pair (x, y) of real numbers with $(x^2, y) = (a, 0)$.

(c) For all sets A, B, C: if $A \times B = A \times C$, then $B = C$.

(d) For all sets A, B, C such that A has an element: if $A \times B = A \times C$, then $B = C$.

(e) There is exactly one set E with $E \times E = \emptyset$.

Solution.

(a) **True.** *Uniqueness.* Let (x, y) be a solution. By the characteristic property (Definition 1.4.1), $3x - y = a$ and $x + 2y = b$. The first equation gives $y = 3x - a$, and then $x + 2(3x - a) = b$, so $7x = 2a + b$. Hence $x = (2a + b)/7$ and $y = 3x - a = (3b - a)/7$. *Existence.* For these values,

$$3 \cdot \frac{2a+b}{7} - \frac{3b-a}{7} = \frac{7a}{7} = a, \qquad \frac{2a+b}{7} + 2 \cdot \frac{3b-a}{7} = \frac{7b}{7} = b,$$

so $(3x - y, x + 2y) = (a, b)$.

(b) **False.** For $a = 1$, both $(1, 0)$ and $(-1, 0)$ qualify, since $1^2 = (-1)^2 = 1$, and they are different pairs because $1 \neq -1$. (For $a = -1$ there is no pair at all; one failing a is enough.)

(c) **False.** Take $A = \emptyset$, $B = \{1\}$, $C = \{2\}$. Both products are $\emptyset$ by Proposition 1.4.1, so $A \times B = A \times C$, but $B \neq C$.

(d) **True.** Let a be an element of A, and suppose $A \times B = A \times C$. For $b \in B$, $(a, b) \in A \times B = A \times C$ by $(*)$, so $b \in C$ by $(*)$ again. Hence $B \subseteq C$, and the other inclusion is the same argument with B and C exchanged. So $B = C$ by Proposition 1.2.1. Part (c) shows where the element a was needed.

(e) **True.** *Existence.* $\emptyset \times \emptyset = \emptyset$, by the $\emptyset$ law of Proposition 1.4.1. *Uniqueness.* Let $E \times E = \emptyset$. If $e \in E$, then $(e, e) \in E \times E = \emptyset$ by $(*)$, which is impossible; so E has no elements, and $E = \emptyset$ by Proposition 1.2.3.

1.4.5.3 C. Going deeper

Exercise. C1: The square of a union

(a) Determine whether $(A \cup B) \times (A \cup B) = (A \times A) \cup (B \times B)$ for all sets A and B. Justify

your answer.

(b) Prove the inclusion $(A \times A) \cup (B \times B) \subseteq (A \cup B) \times (A \cup B)$.

(c) Prove, from Proposition 1.4.1, that

$$(A \cup B) \times (A \cup B) = (A \times A) \cup (A \times B) \cup (B \times A) \cup (B \times B).$$

Solution.

(a) No. Take $A = \{1\}$ and $B = \{2\}$. Then $(1,2) \in \{1,2\} \times \{1,2\} = (A \cup B) \times (A \cup B)$. But $(A \times A) \cup (B \times B) = \{(1,1),(2,2)\}$, and $(1,2)$ is neither $(1,1)$ nor $(2,2)$, since in each case the second (or first) coordinates differ. So the two sets are different.

(b) Let $p \in (A \times A) \cup (B \times B)$. If $p \in A \times A$, then $p = (x,y)$ with $x, y \in A$; so $x, y \in A \cup B$, and $p \in (A \cup B) \times (A \cup B)$ by $(*)$. If $p \in B \times B$, the same argument with B in place of A applies. In either case $p \in (A \cup B) \times (A \cup B)$.

(c) The mirror-image $\cup$ law, with $A \cup B$ as the fixed factor on the right, gives

$$(A \cup B) \times (A \cup B) = (A \times (A \cup B)) \cup (B \times (A \cup B)).$$

The first $\cup$ law, applied to each of the two products, gives

$$A \times (A \cup B) = (A \times A) \cup (A \times B), \qquad B \times (A \cup B) = (B \times A) \cup (B \times B).$$

Substituting, and using that $\cup$ is associative (Theorem 1.3.1), so that no brackets are needed, gives the formula. Part (a)'s counterexample is the term $A \times B$ at work: $(1,2) \in A \times B$.

Exercise. C2: When one inclusion forces equality

Let A and B be sets. Prove that $A \times B \subseteq B \times A$ if and only if $A = B$ or $A = \emptyset$ or $B = \emptyset$.

Solution (Hint 1). For $(\Rightarrow)$, the empty cases are easy, so assume both sets have elements. To show $A \subseteq B$, you need to test an element $a \in A$; put it into a pair that is sure to lie in $A \times B$.

Solution (Hint 2). Fix $b_0 \in B$. For $a \in A$, the pair (a, b_0) lies in $A \times B$.

Solution. $(\Leftarrow)$ If $A = B$, then $A \times B = B \times A$, and in particular $A \times B \subseteq B \times A$. If $A = \emptyset$, then $A \times B = \emptyset$ by Proposition 1.4.1, and $\emptyset$ is a subset of every set. If $B = \emptyset$, likewise $A \times B = A \times \emptyset = \emptyset$.

$(\Rightarrow)$ Suppose $A \times B \subseteq B \times A$. By excluded middle (Logic and Proof, Proposition 2.5.3), each of A and B either has an element or has none, and a set with no elements is $\emptyset$ (Proposition 1.2.3). If $A = \emptyset$ or $B = \emptyset$, we are done. In the remaining case both have elements: fix $a_0 \in A$ and $b_0 \in B$ ($\exists$E twice, with fresh names).

$A \subseteq B$. Let $a \in A$. Then $(a, b_0) \in A \times B$ by $(*)$, so $(a, b_0) \in B \times A$ by the hypothesis. By

$(*)$ again, $a \in B$ (and $b_0 \in A$).

$B \subseteq A$. Let $b \in B$. Then $(a_0, b) \in A \times B \subseteq B \times A$, and $(*)$ gives $b \in A$ (and $a_0 \in B$).

By Proposition 1.2.1, $A = B$. This proves the equivalence.

Both witnesses are needed. With $B = \emptyset$ there is no b_0, and indeed then $A \times B \subseteq B \times A$ holds for every A, including $A \neq B$: the inclusion $\{1\} \times \emptyset \subseteq \emptyset \times \{1\}$ is $\emptyset \subseteq \emptyset$.

Marking scheme. (10 points) - 2: ($\Leftarrow$): all three cases, including that an empty factor makes $A \times B$ empty and hence a subset of anything. - 2: ($\Rightarrow$): splits off the empty cases and, in the remaining case, names witnesses $a_0 \in A$ and $b_0 \in B$. - 2: $A \subseteq B$, through a pair (a, b_0) with an arbitrary $a \in A$. - 2: $B \subseteq A$, through a pair (a_0, b) with an arbitrary $b \in B$. - 2: uses the characteristic property (directly or through $(*)$) to read the coordinates off a pair of $B \times A$, and concludes $A = B$ by two inclusions.

Fatal errors (0 for the step): testing inclusion on particular elements only (entry (N1) of *Logic and Proof*, Chapter 8's catalogue); using b_0 without having shown that B has an element; concluding $A = B$ from $A \times B = B \times A$ "by canceling" without an element argument. A proof of ($\Rightarrow$) by contraposition (assume $A \neq B$ and both nonempty, and exhibit a pair of $A \times B$ outside $B \times A$) earns full marks if it finds the pair: 2 points for the witnesses and 4 for the pair and the check that it is outside $B \times A$, in place of the two inclusions.

1.5 Functions, Composition, Injections and Surjections

Section 1.4 made "the pairs a description picks out" into a set: a relation from A to B is a subset of $A \times B$. Among its examples, the graph of squaring relates each real number to exactly one number, and the unit circle relates 0 to two numbers and 2 to none. This section gives the first kind its name, **function**, and builds the rest on it: we restrict functions, use them to make families, sequences and the set Y^X precise, compose them, and ask the two questions that the rest of the chapter turns on: does a function send different inputs to different outputs, and does it reach every point of its target?

1.5.1 What is a function?

Everyone has used functions since school, and the everyday definition is "a rule that assigns to each input one output". Look at the word "rule". The rules $x \mapsto x^2$ and $x \mapsto (x+1)^2 - 2x - 1$ are different: one squares, the other adds, squares, subtracts, and subtracts again. Yet on every real number they give the same answer, and nobody would call them different functions. Other functions have no rule at all that one could write down. A table of measured temperatures, one per day, assigns to each day one number, and no formula produces it.

So the rule is not what matters. What matters is **which output goes with which input**: the set of input–output pairs. That set is a relation, and Section 1.4 said exactly when two relations are the same, namely when they contain the same pairs. So we forget the rule and keep the pairs. One more piece of data is needed, the set in which the outputs are **declared** to lie; the reason is given after the definition.

A function is its graph, with a declared target.

Definition 1.5.1. Function

Let X and Y be sets. A **function from X to Y**, written $f\colon X \to Y$, is given by a relation $G \subseteq X \times Y$, the **graph** of f, such that

$$\text{for every } x \in X \text{ there is exactly one } y \in Y \text{ with } (x, y) \in G,$$

together with the set Y, the **codomain** of f. Formally, f is the pair (G, Y). The set X is the **domain** of f. For $x \in X$, the unique y with $(x, y) \in G$ is written $f(x)$, the **value** of f at x. We write $(x, y) \in f$ for $(x, y) \in G$, and $x \mapsto f(x)$ for the whole function when its domain and codomain are clear.

In symbols, the condition on the graph is

$$\forall x \in X \;\; \exists!\, y \in Y \;\; (x, y) \in G,$$

where, as with the bounded quantifiers of Logic and Proof, Definition 5.1.1, $\exists!\, y \in Y \;\; \psi$ abbreviates $\exists!\, y\, (y \in Y \wedge \psi)$.

The whole definition is the quantifier pattern $\forall\exists!$. By Logic and Proof, Definition 5.8.1, "$\exists!\, y$" is an existence claim and a uniqueness claim, and by Logic and Proof, Proposition 5.8.1 the uniqueness claim may be stated without reference to the witness; so the condition on the graph is two clauses:

- **(Fn1)** (existence) for every $x \in X$ there is **at least one** $y \in Y$ with $(x, y) \in G$: every input has an output;
- **(Fn2)** (uniqueness) for every $x \in X$ and all $y, y' \in Y$, if $(x, y) \in G$ and $(x, y') \in G$, then $y = y'$: no input has two outputs.

In words: the graph is a set of input–output pairs, with inputs from X and outputs from Y; (Fn1) says no input is left without an output, and (Fn2) says no input is given two. The codomain Y is where outputs are allowed to lie. It need not consist of outputs: $x \mapsto x^2$ can be declared as a function from $\mathbb{R}$ to $\mathbb{R}$, although no output is negative. The set of outputs that actually occur is the **range** of f,

$$\{y \in Y : \exists x \in X \;\; f(x) = y\},$$

which Section 1.7 will call the image of X and write $f(X)$. The domain needs no slot of its own in the pair (G, Y): by (Fn1) every $x \in X$ occurs as a first coordinate in G, and since $G \subseteq X \times Y$, nothing else does. So the graph determines the domain.

The notation $f(x)$ is well defined. Writing "**the** y with $(x, y) \in f$" is legitimate only if there is one, and only one. Clause (Fn1) supplies one, and clause (Fn2) says that any two are equal; together they license the article "the". This gives the equivalence that every argument with functions uses:

$$(x, y) \in f \iff y = f(x) \qquad (x \in X,\; y \in Y). \tag{$**$}$$

For ($\Leftarrow$): $(x, f(x)) \in f$ by the choice of $f(x)$, and if $y = f(x)$ then $(x, y) \in f$ by substituting equals (= E, Logic and Proof, Definition 5.7.1). For ($\Rightarrow$): both (x, y) and $(x, f(x))$ lie in f, so $y = f(x)$ by (Fn2). Two consequences follow at once. Equal inputs give equal outputs: if $x_1 = x_2$, then $f(x_1) = f(x_2)$. And every value lies in the codomain: $f(x) \in Y$ for every $x \in X$.

Functions given by formulas. Most functions in this book are introduced by a formula: "let $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$". This means the function whose graph is $\{(x, y) \in \mathbb{R}^2 : y = x^2\}$. Clause (Fn2) holds for any such graph: if $y = x^2$ and $y' = x^2$, then $y = y'$. So for a formula only (Fn1) needs checking, and it says: for each x in the domain, the formula **makes sense** and its value

lies in the codomain. For x^2 on $\mathbb{R}$ both are clear. For "$f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = 1/x$" the formula makes no sense at $x = 0$, and (Fn1) fails there; for "$f\colon \mathbb{R} \to [0, \infty)$, $f(x) = x^2$" the value must be checked to lie in $[0, \infty)$, which it does, since squares are nonnegative.

A function whose domain is a product $A \times B$ is a **function of two variables**. Its inputs are pairs, and we write $f(a, b)$ rather than $f((a, b))$. Addition $(m, n) \mapsto m + n$ from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$ is an example.

Example. First functions

Check (Fn1) and (Fn2), and find the range, for each of the following.

(a) $f\colon \{1, 2, 3\} \to \{a, b\}$ with graph $\{(1, a), (2, b), (3, a)\}$.

(b) The **identity function** $\mathrm{id}_X\colon X \to X$, $\mathrm{id}_X(x) = x$, for a set X.

(c) A **constant function** $X \to Y$, $x \mapsto c$, for a fixed $c \in Y$.

(d) The **indicator function** $\mathbf{1}_A\colon X \to \{0, 1\}$ of a subset $A \subseteq X$:

$$\mathbf{1}_A(x) = \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } x \in X \setminus A. \end{cases}$$

Solution.

(a) The graph is a subset of $\{1, 2, 3\} \times \{a, b\}$. Each of 1, 2, 3 occurs as a first coordinate (Fn1), and each occurs exactly once, so no input has two outputs (Fn2). So f is a function, with $f(1) = a$, $f(2) = b$, $f(3) = a$. Its range is $\{a, b\}$, the whole codomain. A function on a small finite set is often given this way, by listing its values; no formula is needed.

(b) The graph is the **diagonal** $\{(x, x) : x \in X\}$. For each x, the pair (x, x) is in it (Fn1); and if (x, y) is in it, then $(x, y) = (z, z)$ for some $z \in X$, and the characteristic property (Definition 1.4.1) gives $x = z = y$ (Fn2). The range is X.

(c) The graph is $X \times \{c\}$. For each $x \in X$, (x, c) is in it (Fn1); if (x, y) is in it, then $y \in \{c\}$ by the membership test $(*)$ for pairs in a product (Definition 1.4.2), so $y = c$ (Fn2). If X has an element, the range is $\{c\}$. If $X = \emptyset$, the range is $\emptyset$.

(d) The graph is $(A \times \{1\}) \cup ((X \setminus A) \times \{0\})$. For (Fn1), let $x \in X$. By excluded middle (Logic and Proof, Proposition 2.5.3), $x \in A$ or $x \notin A$; in the first case $(x, 1)$ is in the graph, in the second $x \in X \setminus A$ and $(x, 0)$ is. For (Fn2), the two cases cannot both hold, so x never receives both 0 and 1, and each case gives only one pair with first coordinate x. The range is $\{0, 1\}$ if A has an element and $X \setminus A$ has an element; it is $\{0\}$ if $A = \emptyset$ and X has an element, $\{1\}$ if $A = X$ and X has an element, and $\emptyset$ if $X = \emptyset$. This is the first function of the chapter whose existence clause needs excluded middle: the definition by cases is a function only because every x falls into one of the cases.

The next example collects relations that fail to be functions. Each failure is one clause, and it pays to say which.

Example. Relations that are not functions

(a) Is the unit circle $S = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ the graph of a function $\mathbb{R} \to \mathbb{R}$?

(b) "Send a fraction p/q to its numerator p." Is this a function from $\mathbb{Q}$ to $\mathbb{Z}$? As a relation it is

$$N := \{(r, p) \in \mathbb{Q} \times \mathbb{Z} : \exists q \in \mathbb{Z}_{>0} \quad r = p/q\}.$$

Solution.

(a) No, and both clauses fail, at different points. Clause (Fn2) fails at $x = 0$: both $(0, 1)$ and $(0, -1)$ lie in S, and $1 \neq -1$. Clause (Fn1) fails at $x = 2$: a pair $(2, y) \in S$ would need $y^2 = 1 - 4 = -3$, and no real square is negative. Restricting the inputs to $[-1, 1]$ repairs (Fn1) but not (Fn2); keeping only the upper half, $y \geq 0$, repairs (Fn2) as well, and gives the function $[-1, 1] \to \mathbb{R}$, $x \mapsto \sqrt{1 - x^2}$.

(b) No. Clause (Fn1) holds: every rational number is p/q for some $p \in \mathbb{Z}$ and $q \in \mathbb{Z}_{>0}$. But (Fn2) fails, because a rational number has many ways of being written as a fraction. Since $\frac{1}{2} = \frac{2}{4}$, both $(\frac{1}{2}, 1)$ and $(\frac{1}{2}, 2)$ lie in N, and $1 \neq 2$. The "rule" gives an output that depends on **how the input is written**, not on the input. A function may not do that, since its value is attached to the input itself. This is why definitions of the form "write x as ..., then send it to ..." must be checked for **well-definedness**, a check that returns in Chapter 4 for functions defined on classes. Here the repair is to fix the way of writing: let q_0 be the least $q \in \mathbb{Z}_{>0}$ with $rq \in \mathbb{Z}$ (such q exist, by the first sentence, so there is a least one by well-ordering, proved in Chapter 2; a least element is unique), and send r to rq_0. This is a function.

Second reading · *Why each clause, and why a codomain*

Why this definition. Each clause has a job, and dropping one lets in the failures of Example (Relations that are not functions). Without (Fn1), a "function" could be undefined at some inputs, like $1/x$ at 0; then $f(x)$ would not name anything, and statements "for every $x \in X$" about $f(x)$ would lose their meaning. Without (Fn2), $f(x)$ would not name **one** thing, and $f(\frac{1}{2})$ in part (b) would be both 1 and 2. The graph replaces the rule because two rules can describe one function, and sets are compared by their elements.

Why is the codomain part of the data? A relation is a set, so if a function were only its graph, two functions with the same graph would be equal (Definition 1.2.1), whatever target was declared. The graph of $x \mapsto x^2$ as a function $[0, \infty) \to \mathbb{R}$ is the same set as its graph as a function $[0, \infty) \to [0, \infty)$. But these should be different functions, because the second reaches every point of its target and the first does not: this is the property called surjectivity below, and an example later in this section shows it changing with the codomain. Recording the codomain in the pair (G, Y) keeps the two apart. Many books take the same convention, some without saying so.

Warning. A formula is not yet a function. "The function $1/x$" names no function until a domain and a codomain are given, and the domain must be chosen so that (Fn1) holds: $x \mapsto 1/x$ is a function $\mathbb{R} \setminus \{0\} \to \mathbb{R}$, and there is no function $\mathbb{R} \to \mathbb{R}$ given by this formula.

Likewise $\sqrt{x}$ makes sense on $[0, \infty)$ and not on $\mathbb{R}$. When you meet "let $f(x) = \ldots$", ask first where x lives and where $f(x)$ is meant to lie.

Quick check. Which of these relations on $\{1, 2, 3\}$ are graphs of functions $\{1, 2, 3\} \to \{1, 2, 3\}$: $\{(1, 2), (2, 2), (3, 2)\}$, $\{(1, 1), (2, 2)\}$, $\{(1, 3), (2, 1), (3, 2), (2, 3)\}$? For each that is not, name the clause that fails.

Solution. The first is a function: the constant function with value 2. The second fails (Fn1) at 3, which has no output. The third fails (Fn2) at 2, which has the two outputs 1 and 3.

1.5.2 When are two functions equal?

A function is a pair (G, Y), so two functions are equal when their graphs are equal and their codomains are equal. In practice we compare functions by their values, and the next result says that this is the same test.

Proposition 1.5.1. Equality of Functions

Let $f\colon X \to Y$ and $g\colon X' \to Y'$ be functions. Then $f = g$ if and only if $X = X'$, $Y = Y'$, and $f(x) = g(x)$ for every $x \in X$.

Idea. Write $f = (G, Y)$ and $g = (G', Y')$. The characteristic property of pairs splits $f = g$ into "same graph" and "same codomain". Two graphs are equal when they have the same elements, and by $(**)$ an element of a graph is a pair $(x, f(x))$; so "same graph" is "same inputs, same outputs".

Proof. Write $f = (G, Y)$ and $g = (G', Y')$, as in Definition 1.5.1.

($\Rightarrow$) Suppose $f = g$. By the characteristic property of pairs (Definition 1.4.1), $G = G'$ and $Y = Y'$. The domain is determined by the graph, as the set of first coordinates of its elements, so $X = X'$. Let $x \in X$. By $(**)$, $(x, f(x)) \in G = G'$, so $(x, f(x)) \in g$, and $(**)$ for g gives $f(x) = g(x)$.

($\Leftarrow$) Suppose $X = X'$, $Y = Y'$, and $f(x) = g(x)$ for every $x \in X$. We show $G \subseteq G'$. Let $p \in G$. Since $G \subseteq X \times Y$, $p = (x, y)$ with $x \in X$ and $y \in Y$. By $(**)$, $y = f(x)$, so $y = g(x)$ by the hypothesis, and then $p = (x, y) \in G'$ by $(**)$ for g. The same argument with f and g exchanged gives $G' \subseteq G$, so $G = G'$ by Proposition 1.2.1. Since also $Y = Y'$, the characteristic property gives $(G, Y) = (G', Y')$, that is, $f = g$.

■

So to show two functions equal, check three things: the same domain, the same codomain, and the same value at an arbitrary point. To show them different, one witness suffices: a point where the values differ, or a difference in domain or codomain.

Example. Equal and unequal functions

Decide which of these functions are equal.

(a) $f, g\colon \mathbb{R} \to \mathbb{R}$, $f(x) = (x+1)^2 - 2x - 1$ and $g(x) = x^2$.
(b) $h, k\colon \mathbb{R} \to \mathbb{R}$, $h(x) = |x|$ and $k(x) = \sqrt{x^2}$.
(c) $s_1\colon [0,\infty) \to \mathbb{R}$ and $s_2\colon [0,\infty) \to [0,\infty)$, both given by $x \mapsto x^2$.

Solution.

(a) Equal. The domains are both $\mathbb{R}$ and the codomains both $\mathbb{R}$. For every real x, $(x+1)^2 - 2x - 1 = x^2 + 2x + 1 - 2x - 1 = x^2$. By Proposition 1.5.1, $f = g$: two rules, one function.
(b) Equal. Same domain and codomain, and for every real x, $\sqrt{x^2} = |x|$: the number $|x|$ is nonnegative and its square is x^2, and $\sqrt{x^2}$ is by definition the nonnegative number with square x^2, which is unique by Logic and Proof, Theorem 2.4.5.
(c) Not equal. They have the same domain, the same values, and even the same graph; but their codomains $\mathbb{R}$ and $[0,\infty)$ are different sets (-1 is in one and not the other), so by Proposition 1.5.1 $s_1 \neq s_2$.

Restriction. A function can be cut down to a smaller domain. For $f\colon X \to Y$ and $A \subseteq X$, the **restriction** of f to A is the function

$$f|_A\colon A \to Y, \qquad f|_A(a) \coloneqq f(a),$$

whose graph is $G \cap (A \times Y)$: the pairs of f whose input lies in A. The squaring function $\mathbb{R} \to \mathbb{R}$ restricted to $[0,\infty)$ is s_1 of part (c). The bar in $f|_A$ is one of the uses of a vertical bar that the book's colon-for-set-builder convention keeps free.

1.5.3 Families, sequences, and the set of all functions

Section 1.3 used families of sets $(A_i)_{i\in I}$ and described them informally, as "a set A_i for each index $i \in I$". We can now say exactly what a family is, once its members are known to lie in some set. A **family of subsets of X indexed by I** is a function $I \to \mathcal{P}(X)$, $i \mapsto A_i$, with the power set $\mathcal{P}(X)$ as the codomain the definition asks for. More generally, if S is a set whose elements are sets, a family of members of S indexed by I is a function $I \to S$. A codomain must be named, because there is no set of all sets (Theorem 1.2.4). The value of a family at i is written A_i rather than $A(i)$, and the family is written $(A_i)_{i\in I}$, in parentheses because it is indexed. A family is not the same thing as its set of values $\{A_i : i \in I\}$: the family $(A_i)_{i\in\{1,2\}}$ with $A_1 = A_2 = \{0\}$ has two indices and one value.

In the same way, a **sequence** of real numbers $(a_n)_{n\geq 1}$ is a function $\mathbb{Z}_{>0} \to \mathbb{R}$, $n \mapsto a_n$, with the value at n written a_n. The sequence $(1/n)$ is the function $n \mapsto 1/n$, and its set of values is $\{1/n : n \geq 1\}$. Sequences are the main object of *Analysis on the Real Line*.

Finally, all functions from X to Y form a set, written

$$Y^X \coloneqq \{f \in \mathcal{P}(X \times Y) \times \{Y\} : f \text{ is a function from } X \text{ to } Y\}.$$

Second reading · *Where Y^X comes from*

It is a set by the working rules of Section 1.2: every function $X \to Y$ is a pair (G, Y) with $G \in \mathcal{P}(X \times Y)$, so Y^X is the subset of $\mathcal{P}(X \times Y) \times \{Y\}$ cut out by the condition of Definition 1.5.1, and this product is a set by (W2), (W4), and (W5), so Y^X is a set by specification (W1).

The letters are in this order because, for finite sets, Y^X has m^n elements when Y has m and X has n, as the next example suggests; counting is the business of Section 2.5. The set $\{0,1\}^{\mathbb{N}}$ of all sequences of zeros and ones, indexed from 0, plays a leading role in Chapter 3.

Example. All functions between two small sets

List the elements of $\{0,1\}^{\{1,2\}}$, and say which are indicator functions of subsets of $\{1,2\}$.

Solution. A function $f\colon \{1,2\} \to \{0,1\}$ is determined by its two values $f(1)$ and $f(2)$ (Proposition 1.5.1), and each may be 0 or 1. So there are four:

$f(1)$	$f(2)$	graph	indicator of
0	0	$\{(1,0),(2,0)\}$	$\emptyset$
0	1	$\{(1,0),(2,1)\}$	$\{2\}$
1	0	$\{(1,1),(2,0)\}$	$\{1\}$
1	1	$\{(1,1),(2,1)\}$	$\{1,2\}$

Every one of them is an indicator function: $f = \mathbf{1}_A$ for $A = \{x \in \{1,2\} : f(x) = 1\}$. The four subsets of $\{1,2\}$ and the four functions correspond one to one.

The correspondence at the end of the example, between subsets of X and functions $X \to \{0,1\}$, holds for every set X: send f to $\{x \in X : f(x) = 1\}$ and A to $\mathbf{1}_A$. So counting the subsets of a finite set and counting the functions from it to $\{0,1\}$ are one problem, which Section 2.5 solves.

A game with five strings. A string of five symbols 0 or 1, such as 01101, is a function $\{1,\dots,5\} \to \{0,1\}$: its value at k is its k-th symbol. One player lists five strings, say 00000, 11111, 01010, 10101, 00111; the other must write a string not on the list. Searching all 32 always works, but is there a rule that builds a missing string from **any** list of five in five steps? Try one. Chapter 3 comes back to this game.

Quick check. Which string is the indicator function of $\{1,4\} \subseteq \{1,\dots,5\}$? What is the value at 2 of the string 01100?

Solution. The indicator of $\{1,4\}$ has value 1 at 1 and 4 and value 0 elsewhere, so it is the string 10010. The value of 01100 at 2 is its second symbol, 1.

The empty set gives the degenerate cases, and they are worth settling now, since they are the test cases of many later statements.

Proposition 1.5.2. Functions and the Empty Set

(a) For every set Y there is exactly one function from $\emptyset$ to Y: the pair $(\emptyset, Y)$, called the **empty function**.

(b) If X is nonempty (it has an element), there is no function from X to $\emptyset$.

↻ **Second reading** · *The empty function, proved*

Proof.

(a) *Existence.* The empty relation satisfies $\emptyset \subseteq \emptyset \times Y$, since $\emptyset$ is a subset of every set (Section 1.2). The condition of Definition 1.5.1 reads "for every x, if $x \in \emptyset$, then there is exactly one $y \in Y$ with $(x, y) \in \emptyset$". For each x the hypothesis $x \in \emptyset$ is false, so the implication holds (Logic and Proof, Proposition 2.1.2). So $(\emptyset, Y)$ is a function from $\emptyset$ to Y.
Uniqueness. Let (G, Y) be any function from $\emptyset$ to Y. Its graph satisfies $G \subseteq \emptyset \times Y = \emptyset$, by the mirror-image $\emptyset$ law of Proposition 1.4.1. So an element of G would be an element of $\emptyset$; G has no elements, and $G = \emptyset$ by Proposition 1.2.3. Hence $(G, Y) = (\emptyset, Y)$.

(b) Let $x_0 \in X$, and suppose $f\colon X \to \emptyset$ were a function. By (Fn1) there would be $y \in \emptyset$ with $(x_0, y) \in f$; but $\emptyset$ has no elements. So there is no such function [¬I].

■

In the notation Y^X: the set $Y^\emptyset$ has exactly one element for every Y, including $Y = \emptyset$; and $\emptyset^X = \emptyset$ whenever X is nonempty. The empty function $\emptyset \to Y$ returns in Section 1.6 as the witness that a hypothesis there cannot be dropped.

1.5.4 Composition

Two functions can be applied one after the other when the outputs of the first are inputs of the second. Temperature in degrees Celsius, as a function of the day, followed by the conversion to degrees Fahrenheit, gives temperature in Fahrenheit as a function of the day.

Definition 1.5.2. Composition

Let $f\colon X \to Y$ and $g\colon Y \to Z$ be functions, the codomain of f being the domain of g. Their **composite** is the function

$$g \circ f\colon X \to Z, \qquad (g \circ f)(x) := g(f(x)),$$

read "g after f".

This is a function by the remark on formulas: for $x \in X$, the value $f(x)$ lies in Y, the domain

of g, so $g(f(x))$ makes sense, and it lies in Z. Its graph is $\{(x, z) \in X \times Z : z = g(f(x))\}$. The order of the letters is the order of the formula $g(f(x))$, which is the **reverse** of the order in which the functions act: f acts first.

Example. The order of composition matters

Let $f, g\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x + 1$ and $g(x) = 2x$. Compute $g \circ f$ and $f \circ g$, and decide whether they are equal.

Solution. By Definition 1.5.2, $(g \circ f)(x) = g(x+1) = 2x+2$ and $(f \circ g)(x) = f(2x) = 2x+1$. At $x = 0$ the values are 2 and 1, so by Proposition 1.5.1 $g \circ f \neq f \circ g$. In words: "add one, then double" is not "double, then add one". (In fact the two composites differ at every x, since $2x + 2 \neq 2x + 1$; one point already suffices.)

Second reading · *Composites defined in one order only*

Composition can also fail to be defined in one order only. For $f\colon \{1, 2\} \to \mathbb{R}$ and $g\colon \mathbb{R} \to \mathbb{R}$, the composite $g \circ f\colon \{1, 2\} \to \mathbb{R}$ is defined, and $f \circ g$ is not: g's outputs are real numbers, and f accepts only 1 and 2.

Composition is not commutative, but it is associative, and the identity functions do nothing.

Proposition 1.5.3. Composition Is Associative

Let $f\colon X \to Y$, $g\colon Y \to Z$, and $h\colon Z \to W$ be functions. Then

$$h \circ (g \circ f) = (h \circ g) \circ f,$$

and $f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f$.

Proof. Both sides of the first equation are functions from X to W, by Definition 1.5.2. For $x \in X$, applying Definition 1.5.2 twice on each side gives

$$(h \circ (g \circ f))(x) = h\big((g \circ f)(x)\big) = h(g(f(x))) = (h \circ g)(f(x)) = \big((h \circ g) \circ f\big)(x).$$

So the two functions agree at every point, and they are equal by Proposition 1.5.1. Likewise $f \circ \mathrm{id}_X$ and $\mathrm{id}_Y \circ f$ are functions from X to Y with values $f(\mathrm{id}_X(x)) = f(x)$ and $\mathrm{id}_Y(f(x)) = f(x)$, so both equal f.

■

Because of associativity, we write $h \circ g \circ f$ without brackets: every way of bracketing gives the same function, $x \mapsto h(g(f(x)))$.

Quick check. For $f, g\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ and $g(x) = x - 3$, compute $(g \circ f)(2)$ and $(f \circ g)(2)$.

Solution. $(g \circ f)(2) = g(4) = 1$ and $(f \circ g)(2) = f(-1) = 1$. The values agree at this point, but the functions are different: at $x = 0$, $(g \circ f)(0) = -3$ and $(f \circ g)(0) = 9$. Agreement at one point proves nothing about equality; disagreement at one point proves inequality.

1.5.5 Injective, surjective, bijective

Two questions can be asked of any function $f\colon X \to Y$, and much of mathematics turns on them. First: can we recover the input from the output, or can two different inputs give the same output? Second: is every point of the codomain an output? The first question is about how f treats X; the second is about how it covers Y.

1.5.5.1 Injective functions

An injective function never sends two different inputs to the same output.

Definition 1.5.3. Injective

A function $f\colon X \to Y$ is **injective** (an **injection**, or **one-to-one**) if, **for all** $x_1, x_2 \in X$, $f(x_1) = f(x_2)$ implies $x_1 = x_2$. In symbols:

$$\forall x_1 \in X \;\; \forall x_2 \in X \;\; \big(f(x_1) = f(x_2) \to x_1 = x_2\big).$$

In words: if two inputs give the same output, they were the same input. By Logic and Proof, Proposition 2.3.2, the definition gives the **contrapositive form**

$$\forall x_1 \in X \;\; \forall x_2 \in X \;\; \big(x_1 \neq x_2 \to f(x_1) \neq f(x_2)\big) :$$

different inputs give different outputs. The two forms are equivalent; the way back, from the contrapositive form to the definition, is Logic and Proof, Proposition 2.5.2, which uses RAA. A proof of injectivity usually uses the form of the definition, because an equation $f(x_1) = f(x_2)$ is something to compute with, while an inequation $x_1 \neq x_2$ is not.

The negation is found by the laws of *Logic and Proof*, Chapter 6 for negating bounded quantifiers and implications: "f is **not** injective" is

$$\exists x_1 \in X \;\; \exists x_2 \in X \;\; \big(f(x_1) = f(x_2) \wedge x_1 \neq x_2\big).$$

So a failure of injectivity is shown by **two witnesses**: two different inputs with the same output.

1.5.5.2 Surjective functions

A surjective function reaches every point of its codomain.

Definition 1.5.4. Surjective

A function $f\colon X \to Y$ is **surjective** (a **surjection**, or **onto**) if, **for every** $y \in Y$, **there**

exists $x \in X$ with $f(x) = y$. In symbols:

$$\forall y \in Y \quad \exists x \in X \quad f(x) = y.$$

In words: every point of the codomain is an output; equivalently, the range of f is all of Y. An x with $f(x) = y$ is called a **preimage** of y. The definition does not ask for the preimage to be unique. Negating as before, "f is **not** surjective" is

$$\exists y \in Y \quad \forall x \in X \quad f(x) \neq y,$$

so a failure of surjectivity is shown by **one witness**: a point of the codomain that no input reaches.

Surjectivity depends on the codomain, which is why Definition 1.5.1 records it: s_1 and s_2 of Example (Equal and unequal functions) have the same graph, and we shall see that s_2 is surjective and s_1 is not.

Warning. Surjectivity cannot be checked by trying some y. The function $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 + x$, reaches $0 = f(0)$, $2 = f(1)$, $6 = f(2)$, and $12 = f(3)$, and a reader who tries these may believe it reaches everything. It does not reach -1: $x^2 + x = -1$ would mean $x^2 + x + 1 = 0$, but $x^2 + x + 1 = (x + \frac{1}{2})^2 + \frac{3}{4} > 0$ for every real x. Concluding "for every y" from a few instances is entry (N1) of the catalogue in *Logic and Proof*, Chapter 8.

1.5.5.3 Bijective functions

Definition 1.5.5. Bijective

A function is **bijective** (a **bijection**) if it is both injective and surjective.

A bijection is a function in which every point of the codomain is reached **exactly once**: for every $y \in Y$ there is exactly one $x \in X$ with $f(x) = y$. This is the $\exists!$ of Definition 1.5.1 again, now read from the codomain side, and its two halves are the two properties.

↻ **Second reading** · *Why a bijection reaches each point once*

In the terms of Example (Method: existence and uniqueness), the two halves are these. Existence of such an x, for every y, is surjectivity. Uniqueness is injectivity: if $f(x_1) = y = f(x_2)$, injectivity gives $x_1 = x_2$; and conversely, if every y has at most one preimage, then $f(x_1) = f(x_2)$ makes x_1 and x_2 two preimages of the same point $y := f(x_1)$, so $x_1 = x_2$.

1.5.5.4 Worked examples

Example. Method: proving injectivity

Template. "Let $x_1, x_2 \in X$ with $f(x_1) = f(x_2)$." Compute until $x_1 = x_2$. To refute injectivity, name two different inputs with one output.

When to use it. Any claim that f is injective. The equation form of Definition 1.5.3 is the one to compute with, as the paragraph after the definition explains.

The usual failure. Starting from $x_1 = x_2$ and reaching $f(x_1) = f(x_2)$, which proves the wrong implication (entry (N5) of Logic and Proof, Example (What is not allowed); a warning below shows it on squaring); or assuming $x_1 \neq x_2$ and never using it.

Example. Method: proving surjectivity

Template. On scrap paper, solve $f(x) = y$ for x, working **backwards**, and note what the solving needed. The proof runs **forwards**: "Let $y \in Y$. Put $x := \ldots$", check $x \in X$, check $f(x) = y$. To refute surjectivity, name one $y \in Y$ and show that $f(x) = y$ has no solution in X.

When to use it. Any claim that f is surjective.

The usual failure. Writing the scratch work as the proof, so that the proof assumes $y = f(x)$ and never checks that the x it found lies in X; and testing a few y (entry (N1), the warning after Definition 1.5.4).

The two methods meet in one function whose surjectivity has to be found, not guessed.

Example. Solving backwards, proving forwards

Let $f\colon \mathbb{R} \to (-1,1)$, $f(x) = x/(1+|x|)$. Show that f is a function, and that it is injective and surjective.

Idea (Scratch work). *A function into* $(-1,1)$. The denominator is safe, since $1+|x| \geq 1 > 0$, and $|f(x)| = |x|/(1+|x|) < 1$. Note also that $f(x)$ has the sign of x, and $f(0) = 0$.

Injectivity. If $f(x_1) = f(x_2)$, then x_1 and x_2 have the same sign. In each case $|x|$ is x or $-x$ for both, and clearing denominators should finish it.

Surjectivity, backwards. The absolute value suggests cases on the sign of y (Example (Method: proof by cases)). For $y \geq 0$, look for $x \geq 0$:

$$y = \frac{x}{1+x} \iff y + yx = x \iff x = \frac{y}{1-y}.$$

For $y < 0$, look for $x < 0$:

$$y = \frac{x}{1-x} \iff y - yx = x \iff x = \frac{y}{1+y}.$$

Both answers are $x = y/(1-|y|)$, one formula, and it needs $|y| \neq 1$. That is why the codomain is the open interval. As givens and goal:

Givens	Goal
$y \in (-1,1)$	some $x \in \mathbb{R}$ with $x/(1+\lvert x\rvert) = y$
$x := y/(1-\lvert y\rvert)$, defined since $\lvert y\rvert < 1$	$f(x) = y$: the one check left

Solution. Function. For every real x, $1 + |x| > 0$, and $|f(x)| = |x|/(1+|x|) < 1$, so $f(x) \in (-1,1)$.

Injective. Let $f(x_1) = f(x_2)$. Since $f(x)$ has the sign of x, x_1 and x_2 are both ≥ 0 or both < 0. In the first case $x_1/(1+x_1) = x_2/(1+x_2)$ gives $x_1 + x_1x_2 = x_2 + x_1x_2$, so $x_1 = x_2$. In the second, $x_1/(1-x_1) = x_2/(1-x_2)$ gives $x_1 - x_1x_2 = x_2 - x_1x_2$, so $x_1 = x_2$ in the same way.

Surjective. Let $y \in (-1, 1)$ and put $x := y/(1-|y|)$, a real number since $1 - |y| > 0$. Then $|x| = |y|/(1-|y|)$, so $1 + |x| = 1/(1-|y|)$, and

$$f(x) = \frac{x}{1+|x|} = x\,(1-|y|) = y.$$

The order is the one the box prescribes. The solving went backwards and needed two cases; the proof goes forwards, states one formula for x, and checks it once.

Quick check. Show that $n \mapsto 5n - 2$, as a function $\mathbb{Z} \to \mathbb{Z}$, is injective and not surjective.

Solution. Injective: $5n_1 - 2 = 5n_2 - 2$ gives $5n_1 = 5n_2$, so $n_1 = n_2$. *Not surjective:* the witness is 0. The equation $5n - 2 = 0$ means $5n = 2$, and no integer solves it: if $n \geq 1$, then $5n \geq 5$; if $n \leq 0$, then $5n \leq 0$.

Example. Deciding injective and surjective

For each function below, decide with proof whether it is injective and whether it is surjective.

(a) $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = 3x - 5$.

(b) $g\colon \mathbb{Z} \to \mathbb{Z}$, $g(n) = 3n$.

(c) $h\colon \{1,2,3\} \to \{a,b\}$, with $h(1) = a$, $h(2) = b$, $h(3) = a$.

(d) $k\colon \{1,2\} \to \{a,b,c\}$, with $k(1) = a$, $k(2) = c$.

Solution.

(a) *Injective.* Let $x_1, x_2 \in \mathbb{R}$ with $3x_1 - 5 = 3x_2 - 5$. Adding 5 and dividing by 3 gives $x_1 = x_2$.
Surjective. On scrap paper, $3x - 5 = y$ gives $x = (y+5)/3$. Now the proof: let $y \in \mathbb{R}$, and put $x := (y+5)/3$. Then $x \in \mathbb{R}$, and $f(x) = 3 \cdot \frac{y+5}{3} - 5 = y$. So f is bijective.

(b) *Injective.* Let $n_1, n_2 \in \mathbb{Z}$ with $3n_1 = 3n_2$. Dividing by 3 gives $n_1 = n_2$.
Not surjective. The witness is $1 \in \mathbb{Z}$. If $n \geq 1$, then $3n \geq 3$; if $n \leq 0$, then $3n \leq 0$. So $3n \neq 1$ for every integer n, and 1 has no preimage. (Solving $3n = 1$ gives $n = \frac{1}{3}$, which is not in the domain $\mathbb{Z}$: the same formula on $\mathbb{Q}$ would be surjective.)

(c) *Not injective:* $h(1) = a = h(3)$ and $1 \neq 3$. *Surjective:* the codomain has two points, and $a = h(1)$, $b = h(2)$. For a finite codomain, checking every point **is** a proof: the instances are all the cases.

(d) *Injective:* the two inputs have the different outputs $a \neq c$, and there are no other pairs of different inputs to check. *Not surjective:* b is not an output, since the only outputs are $k(1) = a$ and $k(2) = c$.

Parts (c) and (d) show two more things. A function from a three-element set to a two-element set cannot be injective, and one from a two-element set to a three-element set cannot be surjective: there are too many inputs in the first case and too few in the second. Section 2.5 proves facts of this kind in general, from the pigeonhole principle of the lattice-point puzzle of Section 1.1.

↻ **Second reading** · *Drawing finite pictures*

And the finite pictures are worth drawing: two columns of dots, with an arrow from each input to its output. Injective means no dot on the right receives two arrows; surjective means every dot on the right receives at least one.

The key example of the section is one formula read as three different functions.

Example. Squaring, three ways

For each of the three functions, settle both questions: injective or not, surjective or not.

(a) $q_1 \colon \mathbb{R} \to \mathbb{R}$, $q_1(x) = x^2$.
(b) $q_2 \colon [0, \infty) \to \mathbb{R}$, $q_2(x) = x^2$.
(c) $q_3 \colon [0, \infty) \to [0, \infty)$, $q_3(x) = x^2$.

Solution.

(a) *Not injective:* $q_1(1) = 1 = q_1(-1)$ and $1 \neq -1$. *Not surjective:* the witness is $-1 \in \mathbb{R}$, since $x^2 \geq 0 > -1$ for every real x. So q_1 is neither.
(b) *Injective.* Let $x_1, x_2 \geq 0$ with $x_1^2 = x_2^2$. Then $x_1^2 \leq x_2^2$, so $x_1 \leq x_2$ by Logic and Proof, Theorem 2.4.5, which applies since both numbers are nonnegative; and likewise $x_2 \leq x_1$. Hence $x_1 = x_2$. *Not surjective:* the witness -1 still works, for the same reason.
(c) *Injective*, by the same proof as in (b): injectivity concerns only the domain and the values, and these are the same as for q_2. *Surjective.* Let $y \in [0, \infty)$. A nonnegative real number has a nonnegative square root, so put $x \coloneqq \sqrt{y}$. Then $x \in [0, \infty)$ and $q_3(x) = (\sqrt{y})^2 = y$. So q_3 is bijective.

The same rule gives three different functions. Shrinking the domain from $\mathbb{R}$ to $[0, \infty)$ removed the two witnesses ± 1 against injectivity. Shrinking the codomain to $[0, \infty)$ removed the witness -1 against surjectivity. The graphs of q_2 and q_3 are the same set; only the declared codomain differs, and surjectivity changes with it.

Warning. Injectivity is not the defining property of a function read backwards. Every function satisfies "if $x_1 = x_2$, then $f(x_1) = f(x_2)$": equal inputs give equal outputs, which is part of $f(x)$ being well defined. Injectivity is the **converse**, "if $f(x_1) = f(x_2)$, then $x_1 = x_2$". A "proof" of injectivity that starts from $x_1 = x_2$ and reaches $f(x_1) = f(x_2)$ has proved the wrong implication, entry (N5) of *Logic and Proof*, Chapter 8's catalogue, and it "proves" q_1 injective, which is false.

Quick check. Is $n \mapsto n+1$ surjective as a function $\mathbb{N} \to \mathbb{N}$? As a function $\mathbb{Z} \to \mathbb{Z}$?

Solution. On $\mathbb{N}$: no. The witness is 0, since $n+1 \geq 1$ for every $n \in \mathbb{N}$, so $n+1=0$ has no solution in $\mathbb{N}$. On $\mathbb{Z}$: yes. For $m \in \mathbb{Z}$, the integer $m-1$ satisfies $(m-1)+1=m$. Both functions are injective, since $n_1+1=n_2+1$ gives $n_1=n_2$.

1.5.6 Composites of injections and surjections

Both properties survive composition. This is the first theorem about functions whose proof uses the definitions and nothing else, and it shows the two proof shapes of the last subsection working together.

Theorem 1.5.4. Composites of Injections and Surjections

Let $f\colon X \to Y$ and $g\colon Y \to Z$ be functions.

(a) If f and g are injective, then $g \circ f$ is injective.

(b) If f and g are surjective, then $g \circ f$ is surjective.

(c) If f and g are bijective, then $g \circ f$ is bijective.

Idea. For (a), start from equal outputs of $g \circ f$. They are equal outputs of g, at the points $f(x_1)$ and $f(x_2)$; peel off g by its injectivity, then f by its. For (b), work backwards along the chain $X \to Y \to Z$: to reach $z \in Z$, first find a point of Y that g sends to z, then a point of X that f sends there. Part (c) is (a) and (b) together.

Proof.

(a) Let $x_1, x_2 \in X$ with $(g \circ f)(x_1) = (g \circ f)(x_2)$, that is, $g(f(x_1)) = g(f(x_2))$ by Definition 1.5.2. The points $f(x_1)$ and $f(x_2)$ lie in Y, and g is injective, so $f(x_1) = f(x_2)$ [$\forall$E, $\to$E: injectivity of g at $f(x_1), f(x_2)$]. Since f is injective, $x_1 = x_2$ [$\forall$E, $\to$E: injectivity of f at x_1, x_2]. So $g \circ f$ is injective.

(b) Let $z \in Z$. Since g is surjective, there is $y \in Y$ with $g(y) = z$ [$\exists$E: the name y is fresh]. Since f is surjective, there is $x \in X$ with $f(x) = y$ [$\exists$E: x is fresh]. Then

$$(g \circ f)(x) = g(f(x)) = g(y) = z,$$

so z has the preimage x under $g \circ f$ [$\exists$I, witness x]. Since $z \in Z$ was arbitrary, $g \circ f$ is surjective.

(c) If f and g are bijective, they are injective and surjective, so $g \circ f$ is injective by (a) and surjective by (b), that is, bijective.

■

Second reading · *Part (a) as a derivation*

Part (a) is short enough to see whole at level 0 of *Logic and Proof*, Section 8.3, a full derivation. Here is its derivation, with the quantifiers bounded and handled by the bounded rules (Logic and Proof, Proposition 6.1.1), and $(g \circ f)(u)$ already unwound to $g(f(u))$ by Definition 1.5.2. Premises 1 and 2 are the injectivity of f and of g; premise 3 says that f maps X into Y, which the prose used in the clause "the points $f(x_1)$ and $f(x_2)$ lie in Y".

1		$\forall u \in X\, \forall v \in X\, (f(u) = f(v) \to u = v)$	
2		$\forall u \in Y\, \forall v \in Y\, (g(u) = g(v) \to u = v)$	
3		$\forall u \in X\, f(u) \in Y$	
4	x_1	$x_1 \in X$	
5	x_2	$x_2 \in X$	
6		$g(f(x_1)) = g(f(x_2))$	
7		$f(x_1) \in Y$	$\forall$E 3, 4
8		$f(x_2) \in Y$	$\forall$E 3, 5
9		$\forall v \in Y\, (g(f(x_1)) = g(v) \to f(x_1) = v)$	$\forall$E 2, 7
10		$g(f(x_1)) = g(f(x_2)) \to f(x_1) = f(x_2)$	$\forall$E 9, 8
11		$f(x_1) = f(x_2)$	$\to$E 10, 6
12		$\forall v \in X\, (f(x_1) = f(v) \to x_1 = v)$	$\forall$E 1, 4
13		$f(x_1) = f(x_2) \to x_1 = x_2$	$\forall$E 12, 5
14		$x_1 = x_2$	$\to$E 13, 11
15		$g(f(x_1)) = g(f(x_2)) \to x_1 = x_2$	$\to$I 6–14
16		$\forall v \in X\, (g(f(x_1)) = g(f(v)) \to x_1 = v)$	$\forall$I 5–15
17		$\forall u \in X\, \forall v \in X\, (g(f(u)) = g(f(v)) \to u = v)$	$\forall$I 4–16

Compare it with the prose of (a). "Let $x_1, x_2 \in X$" opens the two flagged boxes of lines 4 and 5, and "with $g(f(x_1)) = g(f(x_2))$" is the assumption of line 6. The first tagged sentence is lines 7–11, and the second is lines 12–14. The closing "so $g \circ f$ is injective" stands for lines 15–17, the closing lines of $\to$I and of the two $\forall$I's; by the convention of *Logic and Proof*, Chapter 8 on silent steps, the prose may state their result without naming them. The two tags in the prose mark the only steps where a hypothesis is used, and that is what the proof is about.

Second reading · *Each hypothesis is needed*

Each hypothesis is needed. In (a), dropping the injectivity of g breaks the conclusion: with $f = \mathrm{id}_{\mathbb{R}}$ and $g = q_1$, squaring on $\mathbb{R}$, the composite $g \circ f = q_1$ is not injective, although f is. Dropping the injectivity of f instead, with $f = q_1$ and $g = \mathrm{id}_{\mathbb{R}}$, gives the same composite. In

(b), with $f = \mathrm{id}_{\mathbb{R}}$ and $g = q_1$, the composite q_1 is not surjective, although f is; with $f = q_1$ and $g = \mathrm{id}_{\mathbb{R}}$, again $g \circ f = q_1$ is not surjective, although g is.

The converses are more interesting, and they are the exercises of this section. An injective composite $g \circ f$ forces f to be injective and says nothing of the kind about g (exit check C1). A surjective composite forces g to be surjective, and f may miss points (B2). Section 1.6 builds on these facts: a function f with a function g such that $g \circ f = \mathrm{id}_X$ is forced to be injective.

1.5.7 Exercises

1.5.7.1 A. Check your understanding

Exercise. A1

(a) Define "$f\colon X \to Y$ is injective" in symbols, and write its negation in symbols.

(b) Is the empty function $\emptyset \to \{1\}$ injective? Is it surjective? Justify your answers.

(c) Which of these relations on $\{1,2,3\}$ are graphs of functions $\{1,2,3\} \to \{1,2,3\}$? For each that is not, name the clause of the definition that fails. $R_1 = \{(1,2),(2,2),(3,1)\}$, $R_2 = \{(1,1),(2,3)\}$, $R_3 = \{(1,1),(1,2),(2,2),(3,3)\}$.

(d) How many functions $\{1,2\} \to \{a,b,c\}$ are there, and how many of them are injective? Answer by listing.

Solution.

(a) f is injective: $\forall x_1 \in X\ \forall x_2 \in X\ (f(x_1) = f(x_2) \to x_1 = x_2)$ (Definition 1.5.3). Its negation: $\exists x_1 \in X\ \exists x_2 \in X\ (f(x_1) = f(x_2) \wedge x_1 \neq x_2)$. The bounds stay as they are, and the negated implication becomes "hypothesis and not conclusion", by the negation laws of *Logic and Proof*, Chapter 6.

(b) Injective: yes. The condition "for all $x_1, x_2 \in \emptyset$, ..." holds vacuously, since there are no $x_1 \in \emptyset$ (Logic and Proof, Proposition 2.1.2). Surjective: no. The witness is 1: there is no $x \in \emptyset$ at all, so none with value 1.

(c) R_1 is a function ($1 \mapsto 2$, $2 \mapsto 2$, $3 \mapsto 1$). R_2 is not: clause (Fn1) fails at 3, which has no output. R_3 is not: clause (Fn2) fails at 1, which has the two outputs 1 and 2.

(d) A function $f\colon \{1,2\} \to \{a,b,c\}$ is determined by the pair of values $(f(1), f(2))$ (Proposition 1.5.1), and each value can be any of the three letters. Listing the pairs:

$$(a,a),\ (a,b),\ (a,c),$$
$$(b,a),\ (b,b),\ (b,c),$$
$$(c,a),\ (c,b),\ (c,c).$$

There are 9 functions. A function on $\{1,2\}$ is injective exactly when $f(1) \neq f(2)$, since 1 and 2 are the only two different inputs. Removing the three pairs with equal entries, on the diagonal of the list, leaves 6 injective functions.

1.5.7.2 B. Practice

Exercise. B1: Five functions

Determine which of the following are injective, which are surjective, and which are not functions at all. Justify your answers.

(a) $\mathbb{Z} \to \mathbb{Z}$, $n \mapsto 2n$.

(b) $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(m, n) \mapsto m + n$.

(c) $\mathbb{R} \to \mathbb{R}$, $x \mapsto x^3$.

(d) $\mathbb{R} \to (-1, 1)$, $x \mapsto x/\sqrt{1+x^2}$.

(e) $\mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$, $n \mapsto n + (-1)^n$.

Solution.

(a) *Injective:* $2n_1 = 2n_2$ gives $n_1 = n_2$. *Not surjective:* the witness is 1, which is odd, while every $2n$ is even, and no integer is both even and odd (Theorem 1.1.2).

(b) *Not injective:* $(1, 2) \neq (2, 1)$ (Definition 1.4.1), and both are sent to 3. *Surjective:* for $k \in \mathbb{N}$, the pair $(0, k)$ lies in $\mathbb{N} \times \mathbb{N}$ and is sent to k.

(c) *Injective.* Let $x_1^3 = x_2^3$. Then

$$0 = x_1^3 - x_2^3 = (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2), \qquad x_1^2 + x_1x_2 + x_2^2 = (x_1 + \tfrac{1}{2}x_2)^2 + \tfrac{3}{4}x_2^2.$$

If $x_1 \neq x_2$, the second factor is positive: if $x_2 \neq 0$, then $\frac{3}{4}x_2^2 > 0$; if $x_2 = 0$, it equals $x_1^2 > 0$, because $x_1 \neq 0$. Then the product is nonzero, a contradiction. So $x_1 = x_2$. *Surjective:* for $y \in \mathbb{R}$, every real number has a real cube root, and $x := \sqrt[3]{y}$ satisfies $x^3 = y$. So the function is bijective.

(d) *A function:* for every x, $1 + x^2 > x^2 \geq 0$, so $\sqrt{1+x^2}$ is defined and exceeds $\sqrt{x^2} = |x|$; hence $|x/\sqrt{1+x^2}| < 1$, and the value lies in $(-1, 1)$. *Injective.* Suppose $y = x/\sqrt{1+x^2}$. The denominator is positive, so y has the sign of x, and squaring gives $y^2(1+x^2) = x^2$, that is, $x^2(1-y^2) = y^2$. Since $|y| < 1$ (shown above), $1 - y^2 > 0$, so $x^2 = y^2/(1-y^2)$. Of the square roots of this number, x is the one with the sign of y:

$$x = \frac{y}{\sqrt{1-y^2}}.$$

So x is determined by y: two inputs with the same output y are both equal to $y/\sqrt{1-y^2}$, hence equal. *Surjective.* Let $y \in (-1, 1)$ and put $x := y/\sqrt{1-y^2}$, a real number since $1 - y^2 > 0$. Then $1 + x^2 = 1/(1-y^2)$, so $\sqrt{1+x^2} = 1/\sqrt{1-y^2}$, and

$$\frac{x}{\sqrt{1+x^2}} = \frac{y}{\sqrt{1-y^2}} \cdot \sqrt{1-y^2} = y.$$

So the function is bijective. (For example, $x = \frac{3}{4} \mapsto \frac{3/4}{5/4} = \frac{3}{5}$, and $y = \frac{3}{5}$ comes back to $x = \frac{3/5}{4/5} = \frac{3}{4}$.) The same plan as in Example (Solving backwards, proving forwards) works, with $\sqrt{1+x^2}$ in place of $1 + |x|$ and squaring in place of the split by sign.

(e) *Not a function* $\mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$: at $n = 1$ the formula gives $1 + (-1) = 0$, and $0 \notin \mathbb{Z}_{>0}$, so (Fn1) fails at 1. This is the planted failure: the question whether it is injective or surjective does not arise. (On $\mathbb{N} = \{0, 1, 2, \dots\}$ the same formula is a function, and a bijection: it swaps $0 \leftrightarrow 1$, $2 \leftrightarrow 3$, and so on.)

Exercise. B2: Put the proof in order

Let $f\colon X \to Y$ and $g\colon Y \to Z$ be functions. The following lines contain a proof that **if $g \circ f$ is surjective, then g is surjective**, shuffled, together with two lines that do not belong. Write the six correct lines in an order that makes a proof, and say why each of the other two lines fails.

(i) Then $g(y) = g(f(x)) = (g \circ f)(x) = z$, by Definition 1.5.2.
(ii) Let $y \in Y$.
(iii) Since $g \circ f$ is surjective, there is $x \in X$ with $(g \circ f)(x) = z$.
(iv) Since z was arbitrary, g is surjective.
(v) Let $y \coloneqq f(x)$, an element of Y.
(vi) Since f is surjective, $y = f(x)$ for some $x \in X$.
(vii) Let $z \in Z$.
(viii) So z has a preimage under g, namely y.

Solution. The order is (vii), (iii), (v), (i), (viii), (iv):

> Let $z \in Z$. Since $g \circ f$ is surjective, there is $x \in X$ with $(g \circ f)(x) = z$. Let $y \coloneqq f(x)$, an element of Y. Then $g(y) = g(f(x)) = (g \circ f)(x) = z$, by Definition 1.5.2. So z has a preimage under g, namely y. Since z was arbitrary, g is surjective.

No other order is admissible. Each line uses the one before it: (iii) needs the z of (vii); (v) needs the x of (iii); (i) needs the y of (v); (viii) is the $\exists$I that (i) makes possible; and (iv) closes the $\forall$I opened by (vii).

The distractor (ii) opens with an arbitrary element of the wrong set. The goal "g is surjective" is $\forall z \in Z\ \exists y \in Y\ g(y) = z$, so the proof must take an arbitrary $z \in Z$; the y is the witness to be found, not something given. The distractor (vi) uses a hypothesis the statement does not have: nothing says f is surjective, and the claim holds without it. For example, with $f\colon \{1\} \to \{1,2\}$, $f(1) = 1$, and $g\colon \{1,2\} \to \{1\}$ constant, $g \circ f$ and g are surjective and f is not.

Exercise. B3: Examples on the natural numbers

Give an example of a function $\mathbb{N} \to \mathbb{N}$ that is surjective and not injective, and one that is injective and not surjective. Check each property.

Solution. Surjective, not injective. Let $s(0) \coloneqq 0$ and $s(n) \coloneqq n - 1$ for $n \geq 1$; for $n \geq 1$, $n - 1 \in \mathbb{N}$, so $s\colon \mathbb{N} \to \mathbb{N}$ is a function. It is surjective: for $m \in \mathbb{N}$, $m + 1 \geq 1$, so $s(m+1) = m$. It is not injective: $s(0) = 0 = s(1)$ and $0 \neq 1$.

Injective, not surjective. Let $t(n) \coloneqq n + 1$. It is injective: $n_1 + 1 = n_2 + 1$ gives $n_1 = n_2$. It is not surjective: 0 is not an output, since $n + 1 \geq 1$.

Many other answers are correct. An answer to the first part must have: every value in $\mathbb{N}$ (so it is a function into $\mathbb{N}$); at least one value taken at two different inputs, with the two inputs

named; and every $m \in \mathbb{N}$ reached, with a preimage given as a formula in m, since checking some m is not enough. An answer to the second part must have: values in $\mathbb{N}$; a proof that equal outputs come from equal inputs; and one named natural number that is never reached, with the reason.

Exercise. B4: Prove or disprove

Prove each true statement by the methods of Example (Method: proving injectivity) and Example (Method: proving surjectivity), and refute each false one with a concrete counterexample.

(a) The function $\mathbb{Z} \to \mathbb{Z}$, $n \mapsto n^2 + n$, is injective.
(b) The function $\mathbb{R} \to \mathbb{R}$, $x \mapsto x^3 + 2x$, is injective.
(c) The function $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(m, n) \mapsto 2m + 3n$, is surjective.
(d) The function $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(m, n) \mapsto 2m + 4n$, is surjective.
(e) The formula $x \mapsto x^2 + 4x$ defines a bijection from $[-2, \infty)$ to $[-4, \infty)$.

Solution.

(a) **False.** The inputs 0 and -1 are different, and both are sent to 0: $0^2 + 0 = 0 = (-1)^2 + (-1)$.
(b) **True.** Let $x^3 + 2x = y^3 + 2y$. Then

$$0 = (x^3 - y^3) + 2(x - y) = (x - y)(x^2 + xy + y^2 + 2),$$

and $x^2 + xy + y^2 + 2 = (x + \frac{1}{2}y)^2 + \frac{3}{4}y^2 + 2 \geq 2 > 0$. A product of two reals is 0 only if a factor is 0, so $x - y = 0$, that is, $x = y$.
(c) **True.** Let $k \in \mathbb{Z}$. The pair $(-k, k)$ lies in $\mathbb{Z} \times \mathbb{Z}$, and $2(-k) + 3k = k$. (The scrap-paper search: $3 - 2 = 1$, so multiply that solution of $2m + 3n = 1$ by k.)
(d) **False.** The witness is 1. For all integers m and n, $2m + 4n = 2(m + 2n)$ is even, and 1 is odd; no integer is both (Theorem 1.1.2). So $2m + 4n \neq 1$.
(e) **True.** First, the formula is a function into $[-4, \infty)$: $x^2 + 4x = (x + 2)^2 - 4 \geq -4$. *Injective:* let $x_1, x_2 \geq -2$ with $x_1^2 + 4x_1 = x_2^2 + 4x_2$. Then $(x_1 + 2)^2 = (x_2 + 2)^2$, and both bases are ≥ 0, so $x_1 + 2 = x_2 + 2$ by Logic and Proof, Theorem 2.4.5 (used twice, as in Example (Squaring, three ways) (b)), and $x_1 = x_2$. *Surjective:* let $y \geq -4$ and put $x := -2 + \sqrt{y + 4}$, defined since $y + 4 \geq 0$. Then $x \geq -2$, and $x^2 + 4x = (x + 2)^2 - 4 = (y + 4) - 4 = y$.

1.5.7.3 C. Going deeper

Exercise. C1: Exit check: composites

Let $f\colon X \to Y$ and $g\colon Y \to Z$ be functions.

(a) Prove that if $g \circ f$ is injective, then f is injective.
(b) Give an example in which $g \circ f$ is injective and g is not injective, and check both claims.

Solution.

(a) Suppose $g \circ f$ is injective. Let $x_1, x_2 \in X$ with $f(x_1) = f(x_2)$; we must show $x_1 = x_2$. Applying g to both sides gives $g(f(x_1)) = g(f(x_2))$, because a function gives equal outputs at equal inputs. By Definition 1.5.2, this says $(g \circ f)(x_1) = (g \circ f)(x_2)$. Since $g \circ f$ is injective, $x_1 = x_2$. So f is injective.

(b) Let $X = \{1\}$, $Y = \{1, 2\}$, $Z = \{1\}$; let $f(1) = 1$, and let $g\colon \{1, 2\} \to \{1\}$ be the constant function $g(1) = g(2) = 1$. Then $g \circ f\colon \{1\} \to \{1\}$ is injective, because its domain has only one element: if $x_1, x_2 \in \{1\}$, then $x_1 = 1 = x_2$. And g is not injective: $g(1) = g(2)$ with $1 \neq 2$.

Marking scheme. (10 points) - 2: fixes arbitrary $x_1, x_2 \in X$ with $f(x_1) = f(x_2)$ and states the goal $x_1 = x_2$. - 2: applies g to both sides, with the reason that a function gives equal outputs at equal inputs. - 3: rewrites the result as an equation of values of $g \circ f$ and invokes the injectivity of $g \circ f$. - 3: an example with explicit sets and functions, and both claims checked: $g \circ f$ injective, and two different points with the same value under g.

Fatal errors (0 for the step): assuming g is injective; starting from $x_1 = x_2$ and deriving $f(x_1) = f(x_2)$ (the converse, entry (N5) of *Logic and Proof*, Chapter 8's catalogue); an example in which $g \circ f$ is not defined because the codomain of f is not the domain of g. A proof by contrapositive (from $x_1 \neq x_2$, $g \circ f$ injective gives $g(f(x_1)) \neq g(f(x_2))$, hence $f(x_1) \neq f(x_2)$, since equal values of f would give equal values of g) earns full marks: 2 points for fixing $x_1 \neq x_2$ and the goal, 3 for the use of the injectivity of $g \circ f$, and 2 for the step from $g(f(x_1)) \neq g(f(x_2))$ to $f(x_1) \neq f(x_2)$.

Exercise. C2: When the composite is a bijection

Let $f\colon X \to Y$ and $g\colon Y \to Z$ be functions.

(a) Deduce from Exercise (C1: Exit check: composites) and Exercise (B2: Put the proof in order) that if $g \circ f$ is bijective, then f is injective and g is surjective.

(b) Give an example in which $g \circ f$ is bijective and neither f nor g is bijective.

Solution.

(a) Suppose $g \circ f$ is bijective. Then $g \circ f$ is injective, so f is injective by part (a) of Exercise (C1: Exit check: composites). And $g \circ f$ is surjective, so g is surjective by the proof put in order in Exercise (B2: Put the proof in order).

(b) Take the functions of Exercise (C1: Exit check: composites) (b): $f\colon \{1\} \to \{1, 2\}$, $f(1) = 1$, and $g\colon \{1, 2\} \to \{1\}$, $g(1) = g(2) = 1$. Then $g \circ f\colon \{1\} \to \{1\}$ sends 1 to 1, so $g \circ f = \mathrm{id}_{\{1\}}$ by Proposition 1.5.1, which is bijective. But f is not surjective, since 2 is not an output; and g is not injective, since $g(1) = g(2)$. So neither is bijective. Part (a) is sharp: it gives exactly the half of each property that survives, and this example shows that the other halves can fail together.

1.6 Left, Right and Two-Sided Inverses

Section 1.5 sorted functions by two questions. Does f ever send two different inputs to the same output? Does f reach every point of its codomain? The answers were the words injective and surjective (Definition 1.5.3, Definition 1.5.4). This section asks a question that sounds different: can the work of f be **undone**? It turns out that it asks the same two questions again, one for each side of f. Undoing f after it has acted forces f to be injective, and when X is non-empty injectivity is also enough. Undoing it before, so that f finishes the job, forces f to be surjective. The one new idea in the section is an inverse on one side; an inverse on both sides, written f^{-1}, is simply a map that is both.

Throughout, $f\colon X \to Y$ is a function in the sense of Definition 1.5.1, and composites are formed as in Definition 1.5.2: $g \circ f$ is defined when the codomain of f is the domain of g, and $(g \circ f)(x) = g(f(x))$.

1.6.1 Undoing a function

Start with a function we can compute in our heads. Let $d\colon \mathbb{N} \to \mathbb{N}$ be the doubling map, $d(n) = 2n$. Suppose someone applies d to a secret number and tells us the result, say 14. We recover the secret by halving: it was 7. Halving undoes doubling.

But halving is not quite a function from $\mathbb{N}$ to $\mathbb{N}$: 7 has no half in $\mathbb{N}$. If we want a function $h\colon \mathbb{N} \to \mathbb{N}$ that undoes d, we must give h a value at every odd number as well. Those values do not matter for the undoing, because d never produces an odd number. Any choice will do. So one answer is

$$h(m) \coloneqq \begin{cases} m/2 & \text{if } m \text{ is even,} \\ 1 & \text{if } m \text{ is odd,} \end{cases}$$

and another is $h'(m) \coloneqq m/2$ for even m and $h'(m) \coloneqq m$ for odd m. Both are functions $\mathbb{N} \to \mathbb{N}$: every $m \in \mathbb{N}$ is even or odd and not both (Theorem 1.1.2), and an even m is $2k$ for exactly one $k \in \mathbb{N}$, which is $m/2$. Both undo d: for every $n \in \mathbb{N}$, the number $2n$ is even, so

$$h(d(n)) = h(2n) = \frac{2n}{2} = n,$$

and the same computation holds for h'. In the language of composition, $h \circ d = \mathrm{id}_{\mathbb{N}}$ and $h' \circ d = \mathrm{id}_{\mathbb{N}}$.

Now try to undo in the other order. Is there a function $k\colon \mathbb{N} \to \mathbb{N}$ with $d \circ k = \mathrm{id}_{\mathbb{N}}$, so that d undoes k? Such a k would give $d(k(1)) = 1$, that is $2k(1) = 1$, and 1 is odd, not twice a natural number. So there is no such k. The obstacle is visible: 1 is not in the range of d, so no input to d, however chosen, comes out as 1.

Two things happened here, and they are the whole section in miniature. Undoing d **afterwards** was possible, in more than one way, and the reason is that d loses no information: different inputs give different outputs. Undoing it **beforehand** was impossible, and the reason is that d misses a point of its codomain. The two sides behave differently, so they get two names.

1.6.2 Left and right inverses

A left inverse undoes f after it acts; a right inverse is undone by f.

Definition 1.6.1. Left and Right Inverses

Let $f\colon X \to Y$ be a function, and let $g\colon Y \to X$ be a function in the opposite direction.

(a) g is a **left inverse** of f if $g \circ f = \mathrm{id}_X$, that is, $g(f(x)) = x$ **for every** $x \in X$.

(b) g is a **right inverse** of f if $f \circ g = \mathrm{id}_Y$, that is, $f(g(y)) = y$ **for every** $y \in Y$.

In words: a left inverse is written on the **left** of f in the composite, and the composite $g \circ f$ does nothing to points of X. A right inverse is written on the right, and $f \circ g$ does nothing to points of Y. The two phrasings in each clause say the same thing. Two functions $X \to X$ are equal exactly when they agree at every point (Proposition 1.5.1), and $g \circ f$ and id_X have the same domain and codomain X; so $g \circ f = \mathrm{id}_X$ means $(g \circ f)(x) = \mathrm{id}_X(x)$ for every $x \in X$, which is $g(f(x)) = x$.

The phrase "g is a left inverse of f" and the phrase "f is a right inverse of g" say the same thing: both say $g \circ f = \mathrm{id}_X$. Which word applies depends on which function we are talking about.

Check the definition against the doubling map. With $d(n) = 2n$ on $\mathbb{N}$, the functions h and h' above are left inverses of d: the composite $h \circ d$ sends every n back to n. And d has **no** right inverse, because clause (b) fails at the single point $y = 1$. For a right inverse the "for every $y \in Y$" is the demanding part: one bad y is enough to rule it out.

Example. Left inverses on small sets

Let $X = \{1, 2\}$, $Y = \{1, 2, 3\}$, and $e\colon X \to Y$, $e(1) = 1$, $e(2) = 2$: the inclusion of X into Y.

(a) Show that $g\colon Y \to X$ with $g(1) = 1$, $g(2) = 2$, $g(3) = 2$ is a left inverse of e, and that e is a right inverse of g.

(b) Is g a right inverse of e?

(c) Let $c\colon X \to Y$ be constant, $c(1) = c(2) = 3$. Does c have a left inverse?

Solution.

(a) Clause (a) of Definition 1.6.1 asks for $g(e(x)) = x$ at each of the two points of X: $g(e(1)) = g(1) = 1$ and $g(e(2)) = g(2) = 2$. So $g \circ e = \mathrm{id}_X$, and g is a left inverse of e. Read with the roles exchanged, the same equation $g \circ e = \mathrm{id}_X$ is clause (b) for $g\colon Y \to X$ and $e\colon X \to Y$: e is a right inverse of g.

(b) No. Clause (b) would need $e(g(y)) = y$ for every $y \in Y$, and at $y = 3$ we get $e(g(3)) = e(2) = 2 \neq 3$. The equation $e \circ g = \mathrm{id}_Y$ fails at one point, which is enough.

(c) No. A left inverse g would need $g(c(1)) = 1$ and $g(c(2)) = 2$, that is $g(3) = 1$ and $g(3) = 2$. A function has one value at 3, and $1 \neq 2$. The information "which input was it" is gone once both inputs land on 3, and nothing applied afterwards can bring it back.

Part (c) is the degenerate case of the example, and it is the one to remember. A left inverse must recover x from $f(x)$, so it cannot exist when two inputs share an output. Part (b) shows the other side: g undoes e, but e does not undo g, because e never produces 3.

Warning. A left inverse need not be a right inverse. For the doubling map $d(n) = 2n$ on $\mathbb{N}$ and its left inverse h above, $h(d(n)) = n$ for every n, but $d(h(1)) = d(1) = 2 \neq 1$. The equation $h \circ d = \mathrm{id}_{\mathbb{N}}$ says nothing about $d \circ h$: composition is not commutative (Section 1.5), and here the two composites are different functions.

Quick check. Let $s\colon \mathbb{N} \to \mathbb{N}$ be the successor map, $s(n) = n + 1$. Does s have a left inverse? Does it have a right inverse?

Solution. It has a left inverse, for instance $p(m) := m - 1$ for $m \geq 1$ and $p(0) := 0$. This is a function $\mathbb{N} \to \mathbb{N}$, since $m - 1 \in \mathbb{N}$ when $m \geq 1$, and $p(s(n)) = p(n + 1) = n$ because $n + 1 \geq 1$. It has no right inverse: a right inverse $k\colon \mathbb{N} \to \mathbb{N}$ of s would need $s(k(0)) = 0$, that is $k(0) + 1 = 0$, which no $k(0) \in \mathbb{N}$ satisfies. The number 0 is not reached by s.

1.6.3 A left inverse exists exactly for injective functions

The examples point to a pattern. The doubling map, the inclusion e, and the successor map are injective, and each has a left inverse. The constant map c is not injective, and it has none. Here is the pattern as a theorem. Its hypothesis $X \neq \emptyset$ looks like a technicality; after the proof we will see that it is not.

We need the **range** of f from Section 1.5, and from now on we write it as $f(X)$:

$$f(X) = \{y \in Y : f(x) = y \text{ for some } x \in X\}.$$

Section 1.7 extends this notation to the image of any subset of X.

Theorem 1.6.1. Left Inverses and Injectivity

Let $f\colon X \to Y$ be a function.

(a) If f has a left inverse, then f is injective.

(b) If $X \neq \emptyset$ and f is injective, then f has a left inverse.

Consequently, if $X \neq \emptyset$, then f has a left inverse **if and only if** f is injective.

Part (a) carries no hypothesis on X, on purpose: the last theorem of this section uses it for every X, the empty set included. The hypothesis $X \neq \emptyset$ sits in (b) only, where it is used. As in Proposition 1.5.2 (b), "$X \neq \emptyset$" is read as "X is non-empty: it has an element", and the proof uses it in that form. (From an element, $X \neq \emptyset$ follows at once, since the empty set has none (Definition 1.2.4). The passage back, from "X is not the empty set" to "X has an element", is the classical law "not all fail, so one holds" of *Logic and Proof*, Chapter 6; reading the hypothesis as "has an element" avoids it.)

Idea (Scratch work). For (a), start from the goal. Injectivity asks: from $f(x_1) = f(x_2)$, get $x_1 = x_2$. A left inverse g turns each $f(x)$ back into x, so apply g to both sides.

For (b), build g point by point, the way halving was extended to the odd numbers. ① A point y of the range has a preimage, and injectivity says it has only one; let $g(y)$ be that one. ② A point outside the range has no preimage; send it to a fixed point $x_0 \in X$. This is where $X \neq \emptyset$ is needed. ③ Check that ① and ② together define a function, and that $g(f(x)) = x$.

① and ② are the two cases of a proof by cases on $y \in f(X)$ (Example (Method: proof by cases)). Laid out as givens and goal, the plan for (b) reads:

Givens	Goal
f injective, $x_0 \in X$	$g\colon Y \to X$ with $g(f(x)) = x$ for all $x \in X$
Case $y \in f(X)$: $y = f(x)$, with x unique by injectivity	$g(y) :=$ that x
Case $y \notin f(X)$: nothing is forced	$g(y) := x_0$
g defined on all of Y	check (Fn1), (Fn2); then $g(f(x)) = x$

The last row is the gap: a recipe for $g(y)$ is not yet a function, and the proof must show that the recipe gives every y exactly one value before it may use g at all.

Before reading on: where is $X \neq \emptyset$ used, and what would go wrong at that line if X were empty?

Proof.

(a) Let $g\colon Y \to X$ be a left inverse of f. Let $x_1, x_2 \in X$ with $f(x_1) = f(x_2)$. Since g is a function, equal inputs give equal outputs, so $g(f(x_1)) = g(f(x_2))$. By Definition 1.6.1 (a), $g(f(x)) = x$ for every $x \in X$, so

$$x_1 = g(f(x_1)) = g(f(x_2)) = x_2.$$

Since x_1 and x_2 were arbitrary, f is injective by Definition 1.5.3.

(b) Suppose $X \neq \emptyset$ and f is injective. Since X has an element, fix one and call it x_0 [∃E]. Let G be the subset of $Y \times X$ given by specification (Definition 1.2.3):

$$G := \{\, (y, x) \in Y \times X : (y \in f(X) \text{ and } f(x) = y) \text{ or } (y \notin f(X) \text{ and } x = x_0) \,\}.$$

We show that for every $y \in Y$ there is exactly one $x \in X$ with $(y, x) \in G$, by checking the two clauses (Fn1) (existence) and (Fn2) (uniqueness) into which Section 1.5 splits the condition of Definition 1.5.1 (Logic and Proof, Proposition 5.8.1). Then G, with codomain X, is a function $g\colon Y \to X$. Let $y \in Y$.

Existence (Fn1). By excluded middle (Logic and Proof, Proposition 2.5.3), $y \in f(X)$ or $y \notin f(X)$. *Case 1:* $y \in f(X)$. Then $f(x_1) = y$ for some $x_1 \in X$; name it x_1 [∃E]. The pair (y, x_1) satisfies the first alternative, so $(y, x_1) \in G$. *Case 2:* $y \notin f(X)$. Then (y, x_0) satisfies the second alternative, so $(y, x_0) \in G$. In either case some $x \in X$ has $(y, x) \in G$.

Uniqueness (Fn2). Let $x, x' \in X$ with $(y, x) \in G$ and $(y, x') \in G$. Each pair satisfies one of the two alternatives. If both satisfy the first, then $f(x) = y = f(x')$, so $x = x'$ because f is

injective. If both satisfy the second, then $x = x_0 = x'$. If one satisfies the first and the other the second, then $y \in f(X)$ and $y \notin f(X)$, a contradiction, so this case cannot occur. Hence $x = x'$.

So $g\colon Y \to X$ is a function, and $g(y) = x$ means $(y, x) \in G$. It remains to show $g \circ f = \mathrm{id}_X$. Let $x \in X$. Then $f(x) \in f(X)$, with x as the witness [$\exists$I], and $f(x) = f(x)$, so the pair $(f(x), x)$ satisfies the first alternative: $(f(x), x) \in G$, that is, $g(f(x)) = x$. The functions $g \circ f$ and id_X have domain and codomain X and agree at every point, so they are equal by Proposition 1.5.1. Hence g is a left inverse of f.

The last sentence of the theorem combines (a) and (b). This proves the theorem.

■

Look at where each hypothesis did its work. Injectivity was used once, in the uniqueness step: it is what makes "**the** preimage of y" a single point. The hypothesis $X \neq \emptyset$ was used once, in the first line of (b), to have a point x_0 for the second alternative. The case split on $y \in f(X)$ used excluded middle, a classical step: the proof does not tell us, for a given y, which case we are in.

Neither hypothesis of (b) can be dropped.

- **Without injectivity.** The constant map c of Example (Left inverses on small sets) (c) sends 1 and 2 to 3, and it has no left inverse. In the proof, the uniqueness step breaks: $(3, 1)$ and $(3, 2)$ both lie in G, so G is not a function.
- **Without $X \neq \emptyset$.** The empty function $\emptyset \to \{1\}$ is injective: the condition "for all $x_1, x_2 \in \emptyset$ ..." holds vacuously. A left inverse would be a function $\{1\} \to \emptyset$, and there is none, since the point 1 would need a value in the empty set (Proposition 1.5.2). In the proof, the first line fails: there is no x_0 to fix, and the point 1, which lies outside the range, has nowhere to go.

The proof of (b) builds an object and then checks it. The same pattern serves for many existence claims: build the object explicitly, then check it.

Example. Method: construct and verify

Template. To prove that an object with property P exists: on scrap paper, find where its values are forced and where they are free; define it explicitly, by cases if need be; check that it is the kind of object claimed (for a function, (Fn1) and (Fn2), with values in the codomain); then verify P. For an "if and only if", two directions: one uses the object, the other builds it.

When to use it. Existence of an inverse, a function or a set with stated properties.

The usual failure. Verifying P for an object never shown to exist or to be well defined, (N14) of Logic and Proof, Example (What is not allowed); and a definition that depends on how an input is written (Example (Relations that are not functions) (b)).

Quick check. Construct a left inverse of $u\colon \mathbb{N} \to \mathbb{N}$, $u(n) = 2n + 1$, verify it, and say where its values are free.

Solution. Let $g(m) := (m-1)/2$ for odd m and $g(m) := 0$ for even m. This is a function $\mathbb{N} \to \mathbb{N}$: every $m \in \mathbb{N}$ is even or odd and not both (Theorem 1.1.2), so exactly one clause applies, and for odd $m \geq 1$ the value $(m-1)/2$ lies in $\mathbb{N}$. For every $n \in \mathbb{N}$, the number $u(n) = 2n+1$ is odd, so $g(u(n)) = (2n+1-1)/2 = n$. The values at even m are free: no even number is of the form $u(n)$, so the equation $g(u(n)) = n$ never looks at them.

The proof of (b) describes g explicitly in terms of f and x_0, so on a small example the construction can be run by hand.

Example. Running the construction

Let $f\colon \{1,2\} \to \{a,b,c\}$ be given by $f(1) = a$ and $f(2) = c$, where a, b, c are three different objects. Run the proof of Theorem 1.6.1 (b) with $x_0 = 1$, then with $x_0 = 2$. How many left inverses does f have?

Solution. First the hypotheses: $\{1,2\} \neq \emptyset$, and f is injective because its two inputs have the different outputs a and c. The range is $f(\{1,2\}) = \{a,c\}$.

With $x_0 = 1$: the points a and c of the range go back to their unique preimages, $g(a) = 1$ and $g(c) = 2$. The point b lies outside the range, so $g(b) = x_0 = 1$. Check: $g(f(1)) = g(a) = 1$ and $g(f(2)) = g(c) = 2$, so $g \circ f = \mathrm{id}_{\{1,2\}}$.

With $x_0 = 2$: $g'(a) = 1$, $g'(c) = 2$ as before, and $g'(b) = 2$. The same check shows $g' \circ f = \mathrm{id}_{\{1,2\}}$.

These are all the left inverses. Any left inverse k must satisfy $k(a) = k(f(1)) = 1$ and $k(c) = k(f(2)) = 2$, so its values on the range are **forced**. Its value at b is free, and there are two points of $\{1,2\}$ to choose from. So f has exactly 2 left inverses, and the construction with $x_0 = 1$ and with $x_0 = 2$ produces both.

The example shows that a left inverse is **not unique** in general. The values on the range are forced by the equation $g(f(x)) = x$; the values off the range are free, and they may go to any point of X. (They are free but not always varied: if X has only one point, there is only one place to send them.)

1.6.4 A right inverse forces surjectivity

The doubling map has no right inverse because it misses 1. The same obstacle works for every function.

Proposition 1.6.2. Right Inverses Give Surjectivity

Let $f\colon X \to Y$ be a function. If f has a right inverse, then f is surjective.

Proof. Let $g\colon Y \to X$ be a right inverse of f, and let $y \in Y$. By Definition 1.6.1 (b), $f(g(y)) = y$. So $x := g(y)$ is an element of X with $f(x) = y$ [$\exists$I]. Since y was arbitrary, f is surjective by Definition 1.5.4.

■

The proof names its witness, as in Example (Method: proving surjectivity), with the right inverse supplying $x := g(y)$: the right inverse **is** a rule that hands us, for each y, a preimage $g(y)$. No hypothesis on X or Y is needed. If $Y = \emptyset$, then f is surjective vacuously; and $X = \emptyset$ as well, since there is no function from a non-empty set to $\emptyset$ (Proposition 1.5.2).

Right inverses are not unique either. Here is a small surjection with several.

Example. All right inverses of a small surjection

Let $q\colon \{1,2,3,4\} \to \{0,1\}$ send each number to 0 if it is even and to 1 if it is odd: $q(1) = 1$, $q(2) = 0$, $q(3) = 1$, $q(4) = 0$. Find all right inverses of q.

Solution. A right inverse is a function $k\colon \{0,1\} \to \{1,2,3,4\}$ with $q(k(0)) = 0$ and $q(k(1)) = 1$. The first condition says that $k(0)$ is a preimage of 0, so $k(0) \in \{2,4\}$. The second says $k(1) \in \{1,3\}$. The two choices are independent, and each combination gives a function $\{0,1\} \to \{1,2,3,4\}$ satisfying both conditions. So q has exactly 4 right inverses:

$$(k(0), k(1)) = (2,1), \quad (2,3), \quad (4,1), \quad (4,3).$$

Each one picks one preimage of each point of the codomain. By Proposition 1.6.2, the fact that one exists shows again that q is surjective.

1.6.5 Does every surjection have a right inverse?

Theorem 1.6.1 went both ways: for $X \neq \emptyset$, a left inverse exists exactly when f is injective. Does Proposition 1.6.2 go both ways too? Suppose $f\colon X \to Y$ is surjective. Must f have a right inverse?

Read what a right inverse must do. For **every** $y \in Y$, $g(y)$ must be a preimage of y: an x with $f(x) = y$. Surjectivity promises that each y has at least one preimage. It does not say which, and there may be many. So the right inverse must **choose** one preimage for every y, all at once, and assemble the choices into one set of pairs.

Now look at what our rules can do.

- **One y.** For a single y, the statement "there is $x \in X$ with $f(x) = y$" lets us name a preimage by ∃E (*Logic and Proof*, Section 5.6). That is one choice, made inside one proof.
- **Finitely many y.** For a particular finite $Y = \{y_1, \ldots, y_n\}$, with n a fixed number, we can apply ∃E n times, once for each point, and write down the n pairs. (To get this for every finite Y at once, with n arbitrary, one inducts on n, Logic and Proof, Axiom 4.2.1.) Example (All right inverses of a small surjection) picked one preimage per point in the same spirit, by listing the preimage sets and choosing from them.
- **Infinitely many y.** A proof is a finite object. It cannot contain one ∃E for each of infinitely many points, and no rule of *Logic and Proof*, Chapter 5 makes infinitely many choices in one step.

Sometimes the difficulty does not arise, because a **rule** picks the preimage. The squaring map from $\mathbb{R}$ onto $[0,\infty)$ is surjective, and each $y \geq 0$ has the preimages $\sqrt{y}$ and $-\sqrt{y}$. The rule "take

the non-negative one" defines $g(y) := \sqrt{y}$, and g is a right inverse: $(\sqrt{y})^2 = y$. Likewise the projection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(m, n) \mapsto m$, is surjective, and $m \mapsto (m, 1)$ is a right inverse. In each case the specification of Definition 1.2.3 writes g down, because the rule names one preimage for each y.

For a surjection with no such rule, nothing proved so far produces a right inverse. The missing ingredient is a new principle of set formation, which says that a choice of one element from each set of a family can be made. Chapter 3 states it and proves, with it, that every surjection has a right inverse. Until then, we use only the implication proved above: a right inverse gives surjectivity.

1.6.6 Two-sided inverses

The two halves meet in a single fact about composition: when a function has an inverse on each side, the two inverses coincide.

Proposition 1.6.3. Left and Right Inverses Agree

Let $f\colon X \to Y$ be a function. If $g\colon Y \to X$ is a left inverse of f and $h\colon Y \to X$ is a right inverse of f, then $g = h$.

Idea. As in the uniqueness half of Example (Method: existence and uniqueness), two names, shown equal by computing $g \circ f \circ h$ two ways; consequently a two-sided inverse is unique.

Proof. By Proposition 1.5.3 (associativity and the identity laws),

$$g = g \circ \mathrm{id}_Y = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_X \circ h = h,$$

where the first and last equalities are the identity laws, the second uses that h is a right inverse, the third is associativity, and the fourth uses that g is a left inverse. This proves the proposition.

■

The chain is worth reading twice. The composite $g \circ f \circ h$ can be simplified from either end: the left pair $g \circ f$ collapses to id_X, the right pair $f \circ h$ collapses to id_Y. Associativity says both simplifications are of the same function.

Definition 1.6.2. Inverse Function

Let $f\colon X \to Y$ be a function. A function $g\colon Y \to X$ is a **two-sided inverse**, or an **inverse**, of f if it is both a left inverse and a right inverse of f:

$$g \circ f = \mathrm{id}_X \quad \text{and} \quad f \circ g = \mathrm{id}_Y\,.$$

A function with an inverse is **invertible**. Its inverse is **unique**: if g and g' are both inverses of f, then g is a left inverse and g' a right inverse, so $g = g'$ by Proposition 1.6.3. We call it **the** inverse of f and write it $f^{-1}\colon Y \to X$.

In words: f^{-1} undoes f on both sides. It sends $f(x)$ back to x, and f sends $f^{-1}(y)$ back to y. The article "the" was earned by Proposition 1.6.3; without it, f^{-1} could name several functions, as "a left inverse" does.

The definition is symmetric in f and f^{-1}. The two equations that say f^{-1} is an inverse of f also say that f is an inverse of f^{-1}. So f^{-1} is invertible, and by uniqueness its inverse is f:

$$(f^{-1})^{-1} = f.$$

This is the pattern for every identity about inverses: to show that some function is **the** inverse of f, check the two equations of Definition 1.6.2, and uniqueness does the rest.

Example. Inverses found and checked

Show that each function is invertible by finding its inverse and checking both composites.

(a) $a\colon \mathbb{R} \to \mathbb{R}$, $a(x) = 3x - 2$.

(b) $r\colon (0,\infty) \to (0,\infty)$, $r(x) = 1/x$.

(c) $s\colon \mathbb{R} \to \mathbb{R}$, $s(x) = x|x|$, that is, $s(x) = x^2$ for $x \geq 0$ and $s(x) = -x^2$ for $x < 0$.

Solution. Idea. Solve $y = f(x)$ for x to find a candidate, then check both equations of Definition 1.6.2. The solving is scratch work; the two checks are the proof.

(a) Solving $y = 3x - 2$ gives $x = (y + 2)/3$. Let $b(y) := (y + 2)/3$, a function $\mathbb{R} \to \mathbb{R}$. For every $x \in \mathbb{R}$, $b(a(x)) = (3x - 2 + 2)/3 = x$, and for every $y \in \mathbb{R}$, $a(b(y)) = 3 \cdot (y + 2)/3 - 2 = y$. So $b = a^{-1}$.

(b) For $x > 0$, $1/x > 0$, so r does map $(0,\infty)$ to $(0,\infty)$. Here $r(r(x)) = 1/(1/x) = x$ for every $x > 0$. This one equation is both checks at once, with r in the roles of f and g. So $r^{-1} = r$: the function is its own inverse.

(c) Solve by cases on the sign of y, since $s(x)$ has the sign of x. For $y \geq 0$ the candidate is $\sqrt{y}$; for $y < 0$ it is $-\sqrt{-y}$. Let

$$t(y) := \begin{cases} \sqrt{y} & \text{if } y \geq 0, \\ -\sqrt{-y} & \text{if } y < 0. \end{cases}$$

First check, $t(s(x)) = x$, by cases on x. If $x \geq 0$, then $s(x) = x^2 \geq 0$, so $t(s(x)) = \sqrt{x^2} = x$, the non-negative square root of x^2 being x. If $x < 0$, then $s(x) = -x^2 < 0$, so $t(s(x)) = -\sqrt{x^2} = -(-x) = x$, since the non-negative square root of x^2 is $-x$.

Second check, $s(t(y)) = y$, by cases on y. If $y \geq 0$, then $t(y) = \sqrt{y} \geq 0$, so $s(t(y)) = (\sqrt{y})^2 = y$. If $y < 0$, then $t(y) = -\sqrt{-y} < 0$, so $s(t(y)) = -(\sqrt{-y})^2 = -(-y) = y$.

Both checks hold, so $t = s^{-1}$. Notice that each check needs its own case split: the first splits on the sign of the input x, the second on the sign of y.

Quick check. Give the inverse of $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = 2x^3 - 5$, and verify both composites.

Solution. Solving $y = 2x^3 - 5$ gives $x^3 = (y+5)/2$. Let $g(y) := \sqrt[3]{(y+5)/2}$, with the real cube root, which exists and is unique for every real number (a school fact). Then $f(g(y)) = 2 \cdot (y+5)/2 - 5 = y$ for every $y \in \mathbb{R}$, and $g(f(x)) = \sqrt[3]{(2x^3 - 5 + 5)/2} = \sqrt[3]{x^3} = x$ for every $x \in \mathbb{R}$. So $g = f^{-1}$.

Now the theorem that connects inverses with the words of Section 1.5.

Theorem 1.6.4. Bijections Are the Invertible Functions

A function $f\colon X \to Y$ is bijective if and only if it has a two-sided inverse.

Idea. ($\Leftarrow$) is already proved in two halves: an inverse is a left inverse, which gives injectivity by Theorem 1.6.1 (a), and a right inverse, which gives surjectivity by Proposition 1.6.2. Neither half asks anything of X.

($\Rightarrow$) looks like the open question of the last subsection, since we must pick a preimage of every y. But for a bijection there is nothing to pick. Surjectivity gives each y a preimage and injectivity says there is only one. So the set of pairs (y, x) with $f(x) = y$ already has the $\forall\exists!$ property of Definition 1.5.1. The proof is Example (Method: construct and verify) with every value forced: define g by this set of pairs, check that it is a function, then verify the two equations.

Proof. ($\Leftarrow$) Let g be a two-sided inverse of f. Then g is a left inverse of f, so f is injective by Theorem 1.6.1 (a); and g is a right inverse, so f is surjective by Proposition 1.6.2. Hence f is bijective by Definition 1.5.5.

($\Rightarrow$) Let f be bijective, and let

$$G := \{(y, x) \in Y \times X : f(x) = y\},$$

a subset of $Y \times X$ by specification (Definition 1.2.3). Let $y \in Y$. Since f is surjective, there is $x \in X$ with $f(x) = y$, so some x has $(y, x) \in G$. If $(y, x) \in G$ and $(y, x') \in G$, then $f(x) = y = f(x')$, so $x = x'$ since f is injective. So G satisfies (Fn1) and (Fn2) (Logic and Proof, Proposition 5.8.1): for every $y \in Y$ there is exactly one $x \in X$ with $(y, x) \in G$, and G with codomain X is a function $g\colon Y \to X$ (Definition 1.5.1). By construction, $g(y) = x$ holds exactly when $f(x) = y$.

Now let $y \in Y$. Then $g(y) = x$ for the x with $(y, x) \in G$, so $f(g(y)) = y$. And let $x \in X$. The pair $(f(x), x)$ lies in G, since $f(x) = f(x)$; so $g(f(x)) = x$. By Proposition 1.5.1, $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$. So g is a two-sided inverse of f. This proves the theorem. ∎

Quick check. Why does the inverse of a bijection need no fixed point x_0 and no case split?

Solution. Every $y \in Y$ has exactly one preimage: at least one because f is surjective, at most one because it is injective. So $g(y)$ is forced at every point of Y. There is no point outside the range to send to an x_0, and no second case to split off.

Compare the two constructions of this section. The left inverse of Theorem 1.6.1 (b) needed a fixed point x_0 and a case split by excluded middle, because some y have no preimage. The inverse of a bijection needs neither. Every y has **exactly one** preimage, so the definition "$g(y)$ is the preimage of y" names one element for each y without any choosing. This is why no new principle is needed here, while the open question about surjections needs one. The difference between the two is exactly the difference between "exactly one" and "at least one".

A bijection $f\colon X \to Y$ pairs each element of X with exactly one element of Y, and its inverse pairs them back. Section 2.5 takes the existence of such a pairing as the definition of "X and Y have the same size".

The theorem also covers the degenerate case. A function $f\colon \emptyset \to Y$ is surjective only if $Y = \emptyset$, since a point of Y would need a preimage in $\emptyset$. The empty function $\emptyset \to \emptyset$ is bijective, and it is its own inverse: both composites are the empty function $\emptyset \to \emptyset$, which is $\mathrm{id}_\emptyset$. The proof of ($\Leftarrow$) runs at $X = \emptyset$ without change, because it cites only part (a) of Theorem 1.6.1, which has no hypothesis on X.

Remark. The notation f^{-1} is reserved, as a function, for a bijection f. For a function that is not bijective, "$f^{-1}\colon Y \to X$" names nothing. Section 1.7 uses the symbol in a second way, $f^{-1}(B)$ for a **set** B, which makes sense for every function; it shows that for a bijection the two readings give the same set.

Warning. Do not write f^{-1} for a left inverse. The doubling map d has the two different left inverses h and h' of the first subsection, so "d^{-1}" would not say which one is meant. And neither is an inverse: $d(h(1)) = 2 \neq 1$. The notation is earned by Proposition 1.6.3, which needs an inverse on **both** sides.

Quick check. Does $x \mapsto x^3$ from $\mathbb{R}$ to $\mathbb{R}$ have a two-sided inverse? Does $x \mapsto x^2$ from $[0, \infty)$ to $\mathbb{R}$?

Solution. The first does: $y \mapsto \sqrt[3]{y}$, the real cube root, which exists and is unique for every real y (a school fact). Indeed $\sqrt[3]{x^3} = x$ and $(\sqrt[3]{y})^3 = y$. The second does not. It is injective (Example (Squaring, three ways) (b)), but it is not surjective, since -1 has no preimage; by Theorem 1.6.4 it has no two-sided inverse. (It has left inverses, by Theorem 1.6.1, for instance $y \mapsto \sqrt{y}$ for $y \geq 0$ and $y \mapsto 0$ for $y < 0$.)

1.6.7 What the section proved

For a function $f\colon X \to Y$, the section proved four facts and left one question open.

- A left inverse makes f injective (Theorem 1.6.1 (a)).
- If $X \neq \emptyset$, an injective f has a left inverse (Theorem 1.6.1 (b)). The empty function $\emptyset \to \{1\}$ shows that the hypothesis is needed.
- A right inverse makes f surjective (Proposition 1.6.2).
- A two-sided inverse exists exactly when f is bijective (Theorem 1.6.4), and it is unique (Proposition 1.6.3).
- **Open:** a surjective f has a right inverse. Chapter 3 proves it, with the new principle.

1.6.8 Exercises

1.6.8.1 A. Check your understanding

Exercise. A1

These parts are about Theorem 1.6.1 and its proof.

(a) At which line of the proof of (b) is $X \neq \emptyset$ used, and for what?

(b) The proof shows that the set G is a function by proving two things about the case split into $y \in f(X)$ and $y \notin f(X)$. What are they, and which step of the proof uses each?

(c) Run the construction on $f\colon \{1,2,3\} \to \{1,2,3,4\}$, $f(k) = k+1$, with $x_0 = 3$. Write out the left inverse g and check $g \circ f = \mathrm{id}_{\{1,2,3\}}$.

(d) Give the idea of the proof of (b) in two sentences.

(e) Let $f\colon \{1,2\} \to \{1\}$ be the only function between these sets. Which step of the proof of (b) fails for f, and why?

Solution.

(a) In the first line of (b): "fix one and call it x_0". The point x_0 is the value $g(y)$ for every y outside the range $f(X)$; without it, the second alternative in the definition of G would have nothing to send such y to.

(b) The two cases **exhaust** every y: by excluded middle, $y \in f(X)$ or $y \notin f(X)$; this is used in the existence step. And they **do not overlap**: a y cannot satisfy both, since $y \in f(X)$ and $y \notin f(X)$ contradict each other; this is used in the uniqueness step, to rule out a pair from each alternative. (Uniqueness inside the first case uses injectivity; inside the second, it is automatic.)

(c) The hypotheses hold: $\{1,2,3\} \neq \emptyset$, and f is injective, since $k+1 = k'+1$ gives $k = k'$. The range is $f(\{1,2,3\}) = \{2,3,4\}$. On the range, g returns the unique preimage: $g(2) = 1$, $g(3) = 2$, $g(4) = 3$. The point 1 is outside the range, so $g(1) = x_0 = 3$. Check: $g(f(1)) = g(2) = 1$, $g(f(2)) = g(3) = 2$, $g(f(3)) = g(4) = 3$. So $g \circ f = \mathrm{id}_{\{1,2,3\}}$.

(d) A point of the range has exactly one preimage, by injectivity, and g sends it there; a point outside the range is sent to a fixed point x_0 of the non-empty domain. Then $g(f(x))$ is the unique preimage of $f(x)$, which is x.

(e) The uniqueness step fails. The point $y = 1$ lies in the range and has the two preimages 1 and 2, so $(1,1)$ and $(1,2)$ both lie in G, and G is not a function. The step "$f(x) = y = f(x')$, so $x = x'$" needs injectivity, which this f lacks. (By part (a) of the theorem, f has no left inverse at all.)

1.6.8.2 B. Practice

Exercise. B1: Counting one-sided inverses

(a) Find all left inverses of $f\colon \{1,2\} \to \{1,2,3\}$, $f(k) = k$.

(b) Find all right inverses of $g\colon \{1,2,3\} \to \{1,2\}$, $g(1) = g(2) = 1$, $g(3) = 2$.

Solution.

(a) A left inverse $h\colon \{1,2,3\} \to \{1,2\}$ must satisfy $h(f(1)) = 1$ and $h(f(2)) = 2$, that is $h(1) = 1$ and $h(2) = 2$. The point 3 is outside the range $\{1,2\}$, so $h(3)$ is free: 1 or 2. Each choice satisfies both equations. So there are exactly 2 left inverses: $h(3) = 1$ and $h(3) = 2$, with $h(1) = 1$, $h(2) = 2$ in both.

(b) A right inverse $k\colon \{1,2\} \to \{1,2,3\}$ must satisfy $g(k(1)) = 1$ and $g(k(2)) = 2$. The preimages of 1 under g are 1 and 2, so $k(1) \in \{1,2\}$; the only preimage of 2 is 3, so $k(2) = 3$. So there are exactly 2 right inverses: $k(1) = 1$ or $k(1) = 2$, with $k(2) = 3$ in both.

Exercise. B2: The inverse of a composite

Let $f\colon X \to Y$ and $g\colon Y \to Z$ be bijections. Prove that $g \circ f$ is invertible and that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Hint: check the two equations of Definition 1.6.2 for the candidate $f^{-1} \circ g^{-1}$.

Solution. The candidate $f^{-1} \circ g^{-1}\colon Z \to X$ is defined, since $g^{-1}\colon Z \to Y$ and $f^{-1}\colon Y \to X$ exist by Theorem 1.6.4. We check the two equations of Definition 1.6.2, using Proposition 1.5.3 to regroup and for its identity laws $k \circ \mathrm{id} = k = \mathrm{id} \circ k$:

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \mathrm{id}_Y \circ f = f^{-1} \circ f = \mathrm{id}_X,$$
$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ \mathrm{id}_Y \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_Z\,.$$

So $f^{-1} \circ g^{-1}$ is a two-sided inverse of $g \circ f$. By the uniqueness of inverses (Proposition 1.6.3, as in Definition 1.6.2), it is **the** inverse: $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Notice the order: to undo "first f, then g", undo g first.

Exercise. B3: A bijection between an interval and the line

Let $h\colon (-1,1) \to \mathbb{R}$, $h(x) = x/(1 - |x|)$, and $k\colon \mathbb{R} \to (-1,1)$, $k(y) = y/(1 + |y|)$. Show that h and k are well defined (each denominator is non-zero, and k takes values in $(-1,1)$), and that k is the inverse of h, by checking both composites by cases on the sign. Hence h is a bijection.

Solution. Well defined. For $x \in (-1,1)$, $|x| < 1$, so $1 - |x| > 0$. For $y \in \mathbb{R}$, $1 + |y| \geq 1 > 0$, and $|k(y)| = |y|/(1 + |y|) < 1$ because $|y| < 1 + |y|$; so $k(y) \in (-1,1)$.

First check, $k(h(x)) = x$ for $x \in (-1, 1)$. If $0 \le x < 1$, then $h(x) = x/(1-x) \ge 0$, so

$$k(h(x)) = \frac{x/(1-x)}{1 + x/(1-x)} = \frac{x/(1-x)}{1/(1-x)} = x.$$

If $-1 < x < 0$, then $|x| = -x$ and $h(x) = x/(1+x) < 0$, so $|h(x)| = -x/(1+x)$ and

$$k(h(x)) = \frac{x/(1+x)}{1 - x/(1+x)} = \frac{x/(1+x)}{1/(1+x)} = x.$$

Second check, $h(k(y)) = y$ for $y \in \mathbb{R}$. If $y \ge 0$, then $k(y) = y/(1+y) \in [0, 1)$, so

$$h(k(y)) = \frac{y/(1+y)}{1 - y/(1+y)} = \frac{y/(1+y)}{1/(1+y)} = y.$$

If $y < 0$, then $k(y) = y/(1-y) \in (-1, 0)$, so $|k(y)| = -y/(1-y)$ and

$$h(k(y)) = \frac{y/(1-y)}{1 + y/(1-y)} = \frac{y/(1-y)}{1/(1-y)} = y.$$

Both composites are identities, so $k = h^{-1}$, and h is a bijection by Theorem 1.6.4.

Exercise. B4: Prove or disprove

Prove each true statement and refute each false one with a counterexample.

(a) The function $f\colon \mathbb{Z} \to \mathbb{Z}$, $f(n) = n + 3$, has a two-sided inverse.

(b) The function $f\colon \mathbb{N} \to \mathbb{N}$, $f(n) = n + 3$, has a right inverse.

(c) The function $f\colon \mathbb{N} \to \mathbb{N}$, $f(n) = n + 3$, has a left inverse.

(d) For functions $f\colon X \to Y$ and $g\colon Y \to X$, if $g \circ f = \mathrm{id}_X$ and $f \circ g \neq \mathrm{id}_Y$, then f is not surjective.

(e) Every function $\{1, 2\} \to \{1, 2, 3\}$ has a left inverse.

Solution.

(a) True. Let $g\colon \mathbb{Z} \to \mathbb{Z}$, $g(n) := n - 3$. For every $n \in \mathbb{Z}$, $g(f(n)) = (n+3) - 3 = n$ and $f(g(n)) = (n-3) + 3 = n$, so both composites are $\mathrm{id}_{\mathbb{Z}}$ and g is a two-sided inverse (Definition 1.6.2).

(b) False. Every value is $n + 3 \ge 3$, so 0 is not a value and f is not surjective. By Proposition 1.6.2, f has no right inverse.

(c) True. Let $g(m) := m - 3$ for $m \ge 3$ and $g(m) := 0$ for $m < 3$. This is a function $\mathbb{N} \to \mathbb{N}$: each $m \in \mathbb{N}$ falls under exactly one clause, and $m - 3 \in \mathbb{N}$ when $m \ge 3$. For every $n \in \mathbb{N}$, $f(n) = n + 3 \ge 3$, so $g(f(n)) = (n+3) - 3 = n$. The values at $0, 1, 2$ are free; any choice in $\mathbb{N}$ works.

(d) True. Suppose $g \circ f = \mathrm{id}_X$ and $f \circ g \neq \mathrm{id}_Y$, and suppose, for a contradiction, that f is surjective. By Theorem 1.6.1 (a), f is injective, since g is a left inverse; so f is bijective, and it has a two-sided inverse h by Theorem 1.6.4. Then h is a right inverse of f and g a left inverse, so $g = h$ by Proposition 1.6.3, and $f \circ g = f \circ h = \mathrm{id}_Y$, against the hypothesis. So f is not surjective.

(e) False. The constant map $c\colon \{1,2\} \to \{1,2,3\}$ with value 1 has $c(1) = c(2)$ and $1 \neq 2$, so it is not injective, and by Theorem 1.6.1 (a) it has no left inverse.

1.6.8.3 C. Going deeper

Exercise. C1: One composite equal to the identity

Let $f\colon X \to Y$ and $g\colon Y \to X$ be functions with $g \circ f = \mathrm{id}_X$.

(a) Prove that f is injective and g is surjective.

(b) Show by an example that neither f nor g need be bijective.

(c) Prove that if, in addition, f is surjective, then $g = f^{-1}$.

Solution (Hint 1). Read the equation $g \circ f = \mathrm{id}_X$ twice: once as a statement about f, once as a statement about g.

Solution (Hint 2). For g: let $x \in X$; you need a point of Y that g sends to x.

Solution.

(a) The equation says that g is a left inverse of f, so f is injective by Theorem 1.6.1 (a). The same equation says that f is a right inverse of g, so g is surjective by Proposition 1.6.2. (Directly: for $x \in X$, the point $f(x) \in Y$ satisfies $g(f(x)) = x$.)

(b) Let $f\colon \{1\} \to \{1,2\}$, $f(1) = 1$, and $g\colon \{1,2\} \to \{1\}$, $g(1) = g(2) = 1$. Then $g(f(1)) = 1$, so $g \circ f = \mathrm{id}_{\{1\}}$. But f is not surjective (2 has no preimage) and g is not injective ($g(1) = g(2)$ with $1 \neq 2$), so neither is bijective.

(c) If f is also surjective, it is bijective by (a), so f^{-1} exists by Theorem 1.6.4, and it is in particular a right inverse of f. Also g is a left inverse of f. By Proposition 1.6.3, $g = f^{-1}$.

Marking scheme. (10 points)

- 2: f injective, from the left-inverse equation (citing Theorem 1.6.1 (a) or arguing directly from $f(x_1) = f(x_2)$).
- 2: g surjective, either by citing Proposition 1.6.2 (f is a right inverse of g) or directly, naming the witness $f(x)$ for a given $x \in X$.
- 3: an example with explicit sets and both failures checked (a point missed by f, two points identified by g).
- 3: (c) obtains a right inverse of f (from bijectivity) and applies uniqueness of one-sided inverses, or checks $f \circ g = \mathrm{id}_Y$ directly (for $y = f(x)$, $f(g(y)) = f(g(f(x))) = f(x) = y$, using surjectivity to write $y = f(x)$).

Fatal errors (0 for the step): assuming $f \circ g = \mathrm{id}_Y$ in (a) or (c) without proof; in (c), writing f^{-1} before showing f bijective.

Exercise. C2: When is a left inverse unique?

Let $f\colon X \to Y$ be injective, with $X \neq \emptyset$.

(a) Prove that if f is surjective, or X has exactly one element, then f has exactly one left inverse.

(b) Prove that if some $y_1 \in Y$ is not in $f(X)$, and X has two different elements $x_0 \neq x_1$, then f has at least two different left inverses.

(c) Let $f\colon \{1,2\} \to \{1,2,3,4\}$, $f(k) = 2k$. List all left inverses of f, and explain in one sentence why there are $2^2 = 4$ of them.

Solution (Hint 1). For (a), a left inverse exists by Theorem 1.6.1 (b); only "at most one" needs proof. For (b), run the construction of that proof twice.

Solution (Hint 2). For (a), let g and g' be left inverses of f. If f is surjective, write a given $y \in Y$ as $y = f(x)$ and compare $g(y)$ with $g'(y)$.

Solution.

(a) A left inverse exists by Theorem 1.6.1 (b). For "at most one", let g and g' be left inverses of f. *Case 1:* f is surjective. Then f is bijective (Definition 1.5.5), so it has the inverse f^{-1} (Theorem 1.6.4), which is in particular a right inverse of f. By Proposition 1.6.3, $g = f^{-1}$ and $g' = f^{-1}$, so $g = g'$. *Case 2:* X has exactly one element x_0. For every $y \in Y$, both $g(y)$ and $g'(y)$ are elements of X, so $g(y) = x_0 = g'(y)$; hence $g = g'$ by Proposition 1.5.1. In either case any two left inverses are equal, so f has exactly one.

(b) Run the proof of Theorem 1.6.1 (b) once with the fixed point x_0 and once with x_1; call the resulting left inverses g_0 and g_1. The point y_1 is outside the range, so the second alternative in the definition of G applies to it: $g_0(y_1) = x_0$ and $g_1(y_1) = x_1$. Since $x_0 \neq x_1$, the functions g_0 and g_1 differ at y_1, so $g_0 \neq g_1$.

(c) The range is $\{2,4\}$. A left inverse $g\colon \{1,2,3,4\} \to \{1,2\}$ must satisfy $g(f(1)) = 1$ and $g(f(2)) = 2$, that is $g(2) = 1$ and $g(4) = 2$. The values $g(1)$ and $g(3)$ are free, each in $\{1,2\}$, and every choice gives a left inverse. The four are

$$(g(1), g(2), g(3), g(4)) = (1,1,1,2),\ (1,1,2,2),\ (2,1,1,2),\ (2,1,2,2).$$

The values on the range are forced, and each of the two points 1, 3 outside the range may go to either of the two points of the domain, independently: $2 \cdot 2 = 4$ choices. This is the situation of (b): f is not surjective and its domain has two elements.

Marking scheme. (10 points)

- 1: (a) existence of a left inverse, citing Theorem 1.6.1 (b).
- 2: (a) surjective case: an inverse exists, and uniqueness of one-sided inverses (Proposition 1.6.3) forces every left inverse to equal it (or a direct argument: for $y = f(x)$, $g(y) = x = g'(y)$).
- 2: (a) one-element case: any two functions into a one-element set agree at every point,

so they are equal.
- 3: (b) two left inverses that take the values x_0 and x_1 at y_1 (by the construction or defined directly), each checked to be a left inverse, and shown to differ at y_1.
- 2: (c) the forced values $g(2) = 1$, $g(4) = 2$, the four left inverses, and the count $2 \cdot 2$.

Fatal errors (0 for the step): in (a), writing f^{-1} before showing f bijective; in (b), concluding $g_0 \neq g_1$ without exhibiting a point where they differ.

1.7 Images and Preimages

A function $f\colon X \to Y$ sends points to points. Much of analysis asks what it does to **sets** of points. Where does f send an interval? Which inputs land in a given set of outputs? The first question is answered by the image $f(A)$, the second by the preimage $f^{-1}(B)$, and the two are the subject of this section. They look like mirror images of each other, and they are not: preimages respect every set operation of Section 1.3, while images respect only unions. The reason is one quantifier, and by the end of the section we will be able to point at it.

Throughout, $f\colon X \to Y$ is a function (Definition 1.5.1), and the unions and intersections of families are those of Definition 1.3.4. An intersection of a family of subsets of Y is taken inside Y; of subsets of X, inside X.

1.7.1 A question about squares

Let $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, and take the two intervals $A = [-1, 0]$ and $B = [0, 1]$. Squaring A gives every number from 0 to 1, and so does squaring B. So the set of squares of points of A and the set of squares of points of B are both $[0, 1]$, and the points they share make up $[0, 1]$.

Now intersect first. The intervals A and B share only the point 0, so $A \cap B = \{0\}$, and its only square is 0. Squaring the intersection gives $\{0\}$; intersecting the squares gives $[0, 1]$. The order of the two operations matters.

Try the same thing backwards. Instead of pushing sets forwards through f, pull them back: for a set C of outputs, collect the inputs whose squares lie in C. Take $C = [0, 1]$ and $D = [1, 4]$. The inputs with square in C form $[-1, 1]$, those with square in D form $[-2, -1] \cup [1, 2]$, and the inputs common to both are -1 and 1. Intersecting first gives $C \cap D = \{1\}$, whose inputs are again -1 and 1. This time the order does not matter.

Is that an accident of these intervals? No. Pulling back will turn out to respect intersections for every function and all sets, while pushing forwards respects them exactly for the injective functions. To see why, we first need names for the two operations.

1.7.2 Images and preimages

The two sets in the question above keep recurring: "all the values $f(a)$ for a in A" and "all the inputs x with $f(x)$ in B". The first was already used in Section 1.5 for $A = X$, where it is the range of f.

An image hides a "there exists"; a preimage hides nothing.

Definition 1.7.1. Image

Let $f\colon X \to Y$ be a function and $A \subseteq X$. The **image** of A under f is the set

$$f(A) \coloneqq \{y \in Y : \text{there exists } a \in A \text{ with } f(a) = y\}.$$

We also write it $\{f(a) : a \in A\}$. In symbols, for every y,

$$y \in f(A) \iff y \in Y \wedge \exists a \in A \;\; f(a) = y.$$

Definition 1.7.2. Preimage

Let $f\colon X \to Y$ be a function and $B \subseteq Y$. The **preimage** of B under f, also called its **inverse image**, is the set

$$f^{-1}(B) \coloneqq \{x \in X : f(x) \in B\}.$$

In symbols, for every x, $x \in f^{-1}(B) \iff x \in X \wedge f(x) \in B$. The preimage is defined for **every** function f, whether or not f has an inverse.

In Section 1.5 a point x with $f(x) = y$ was called a preimage of y; that is, $x \in f^{-1}(\{y\})$. So the preimages of a point y are the elements of the preimage of the set $\{y\}$.

Read the two definitions clause by clause.

- **The ambient sets.** Both are sets by specification (Definition 1.2.3): $f(A)$ is carved out of the codomain Y, and $f^{-1}(B)$ out of the domain X. So $f(A) \subseteq Y$ and $f^{-1}(B) \subseteq X$ always. The shorthand $\{f(a) : a \in A\}$ names the same subset of Y; it is a way of writing, not a new rule of set formation.
- **The image.** "$y \in f(A)$" says that y is **hit** by some point of A. The words "there exists" are part of the definition. To **use** a line $y \in f(A)$, we must name a witness: "let $a \in A$ with $f(a) = y$". That is the rule $\exists$E of *Logic and Proof*, Section 5.6, and the name must be fresh. To **prove** $y \in f(A)$, we exhibit a witness, by $\exists$I (*Logic and Proof*, Section 5.5).
- **The preimage.** "$x \in f^{-1}(B)$" says that x is sent **into** B. There is no quantifier. For $x \in X$, a line $x \in f^{-1}(B)$ is used and proved by one substitution: it is exchanged for $f(x) \in B$, and back.
- **The symbol f^{-1}.** In $f^{-1}(B)$, the symbol f^{-1} is not a function that is applied to B. The whole expression $f^{-1}(B)$ is the name of a set built from f and B. Section 1.6 used f^{-1} for the inverse function of a bijection; the remark at the end of this section reconciles the two readings.

The notation $f(A)$ puts a set where $f(x)$ puts a point. When the letter in the brackets has been declared a subset of X, the expression is an image; when it has been declared a point, it is a value. As with the pair and the interval of Section 1.4, the declaration decides.

Quick check. For $f(x) = x^2$ on $\mathbb{R}$, compute $f(\{-1, 2\})$ and $f^{-1}(\{9\})$.

Solution. $f(\{-1, 2\}) = \{1, 4\}$, the squares of the two points. $f^{-1}(\{9\}) = \{-3, 3\}$, the solutions of $x^2 = 9$.

Start with the smallest possible example, where everything can be listed.

Example. Images and preimages by listing

Let $X = \{1, 2, 3, 4\}$, $Y = \{0, 1, 2, 5\}$, and let $f\colon X \to Y$ be given by

$$f(1) = 1, \quad f(2) = 2, \quad f(3) = 0, \quad f(4) = 1.$$

Find $f(\{1, 4\})$, $f(\{2, 3\})$, $f(X)$, and $f(\emptyset)$; then $f^{-1}(\{1\})$, $f^{-1}(\{0, 2\})$, $f^{-1}(\{5\})$, $f^{-1}(\emptyset)$, and $f^{-1}(Y)$.

Solution. Images. A point y lies in $f(A)$ when some $a \in A$ has $f(a) = y$, so we apply f to each point of A and collect the results. $f(\{1, 4\}) = \{1\}$: both points go to 1, and a set lists 1 once. $f(\{2, 3\}) = \{0, 2\}$. $f(X) = \{0, 1, 2\}$, the range; 5 is not in it. $f(\emptyset) = \emptyset$: a point y in it would need some $a \in \emptyset$, and there is none.

Preimages. A point $x \in X$ lies in $f^{-1}(B)$ when $f(x) \in B$, so we test each of the four points of X. $f^{-1}(\{1\}) = \{1, 4\}$. $f^{-1}(\{0, 2\}) = \{2, 3\}$. $f^{-1}(\{5\}) = \emptyset$: no point of X is sent to 5. $f^{-1}(\emptyset) = \emptyset$, since $f(x) \in \emptyset$ never holds. $f^{-1}(Y) = X$, since $f(x) \in Y$ holds for every $x \in X$.

The two computations differ in shape. For the image we ran through the points of A and **produced** outputs. For the preimage we ran through the points of X and **tested** each one. That is the "there exists" of the image and the plain condition of the preimage, seen on a four-point set.

The example also contains a non-example by minimal change. The sets $\{1\}$ and $\{5\}$ are both one-point subsets of Y. The first has a two-point preimage; change 1 to 5 and the preimage becomes empty, because 5 lies outside the range. The preimage of a non-empty set can be empty. What fails is the existence of a point of X sent into the set.

Why is the preimage defined for **every** function, when f^{-1} as a function exists only for bijections? Because the question "which inputs land in B?" makes sense for any f: its answer may be empty, or contain many points, and neither is a problem for a set. The function f^{-1} of Section 1.6 asks for more: exactly one input for each output. This is why analysis states its definitions with preimages. "The preimage of every open set is open" makes sense for every function; *Metric and Topological Spaces*, Chapter 1 uses it to characterize continuity.

Warning. The preimage $f^{-1}(B)$ does not presuppose that f is invertible. For the squaring map on $\mathbb{R}$, which has no inverse function, $f^{-1}(\{4\}) = \{-2, 2\}$ is a perfectly good set. What the symbol does **not** give is a value "$f^{-1}(4)$": that would be a point, and there are two candidates.

1.7.3 Computing images and preimages

With an infinite set, listing is impossible, and the definitions are used as they stand. The image asks us to name witnesses; the preimage asks us to solve an inequality.

Example. Images and preimages of intervals under squaring

Let $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$. Prove that

(a) $f([-1,2]) = [0,4]$;
(b) $f^{-1}([1,4]) = [-2,-1] \cup [1,2]$;
(c) $f^{-1}(\{-1\}) = \emptyset$;
(d) $f^{-1}(f([0,1])) = [-1,1]$.

Solution. We use school facts about real numbers, $x^2 \geq 0$ and every $y \geq 0$ has a square root $\sqrt{y} \geq 0$, and, by Logic and Proof, Theorem 2.4.5, for $s, t \geq 0$, $s \leq t$ holds exactly when $s^2 \leq t^2$.

(a) *Idea.* An image is proved equal to a set by two inclusions. The inclusion $\subseteq$ uses $y \in f([-1,2])$, so it names a witness. The inclusion $\supseteq$ proves $y \in f([-1,2])$, so it exhibits one.
($\subseteq$) Let $y \in f([-1,2])$. Then $y = a^2$ for some $a \in [-1,2]$; name it a. Certainly $y = a^2 \geq 0$. If $a \geq 0$, then $0 \leq a \leq 2$, so $a^2 \leq 4$. If $a < 0$, then $0 < -a \leq 1$, so $a^2 = (-a)^2 \leq 1 \leq 4$. In either case $0 \leq y \leq 4$, that is, $y \in [0,4]$.
($\supseteq$) Let $y \in [0,4]$. Take $a := \sqrt{y}$. Then $0 \leq a \leq \sqrt{4} = 2$, so $a \in [-1,2]$, and $f(a) = y$. Hence $y \in f([-1,2])$.
The witness in ($\supseteq$) could have been $-\sqrt{y}$ for $y \leq 1$, but not for $y > 1$, where $-\sqrt{y} < -1$. One witness per y is all we need, so we choose the one that always works.

(b) *Idea.* A preimage is a set of solutions of a condition on x. No witness is needed: each line is an equivalence.
For every $x \in \mathbb{R}$,

$$\begin{aligned} x \in f^{-1}([1,4]) &\iff 1 \leq x^2 \leq 4 \iff 1 \leq |x| \leq 2 \\ &\iff x \in [-2,-1] \cup [1,2]. \end{aligned}$$

The first step is Definition 1.7.2. The second uses $x^2 = |x|^2$ and Logic and Proof, Theorem 2.4.5 with s, t among 1, $|x|$, 2. The third splits by the sign of x: for $x \geq 0$, $|x| = x$, and for $x < 0$, $|x| = -x$. So the two sets have the same elements.

(c) For every $x \in \mathbb{R}$, $f(x) = x^2 \geq 0 > -1$, so $f(x) \in \{-1\}$ never holds. The preimage is empty, although $\{-1\}$ is not.

(d) First $f([0,1]) = [0,1]$, by the argument of (a): a square of a number in $[0,1]$ lies in $[0,1]$, and each $y \in [0,1]$ is $(\sqrt{y})^2$ with $\sqrt{y} \in [0,1]$. Then, as in (b), for every $x \in \mathbb{R}$, $x \in f^{-1}([0,1]) \iff 0 \leq x^2 \leq 1 \iff |x| \leq 1 \iff x \in [-1,1]$.

Part (d) is worth a second look. We started with $[0,1]$, pushed it forwards and pulled it back, and got the bigger set $[-1,1]$. The negative numbers came in because they have the same squares as the positive ones. That is a failure of injectivity, and the subsection "There and back" later in this section proves that it is the only way the round trip can grow a set.

Quick check. For $f(x) = x^2$ on $\mathbb{R}$, find $f^{-1}(\{4\})$, $f^{-1}([-4,-1])$, and $f(f^{-1}([-1,1]))$.

Solution. $f^{-1}(\{4\}) = \{-2,2\}$, the solutions of $x^2 = 4$. $f^{-1}([-4,-1]) = \emptyset$, since $x^2 \geq 0 > -1$. For the last, $f^{-1}([-1,1]) = \{x \in \mathbb{R} : -1 \leq x^2 \leq 1\} = [-1,1]$, and then $f([-1,1]) = [0,1]$,

by the argument of Example (Images and preimages of intervals under squaring) (a). So $f(f^{-1}([-1,1])) = [0,1]$, which is smaller than $[-1,1]$: the negative numbers are not squares.

1.7.4 Sets of numbers as images

Analysis on the Real Line, Chapter 1 works with three ways of making new sets of real numbers from old ones: for $A, B \subseteq \mathbb{R}$ and $c \in \mathbb{R}$,

$$-A \coloneqq \{-a : a \in A\}, \quad cA \coloneqq \{ca : a \in A\}, \quad A + B \coloneqq \{a + b : a \in A,\ b \in B\}.$$

The first two are images in the sense of Definition 1.7.1. In the third, two letters vary, and the notation means, as for Definition 1.4.2,

$$A + B = \{y \in \mathbb{R} : \exists a \in A\ \exists b \in B\ \ y = a + b\}.$$

Each is an image, and seeing them as images tells us how to prove things about them: an element of $A + B$ is used by naming two witnesses.

Example. Reflections, scalings and sums as images

Let $A, B \subseteq \mathbb{R}$ and $c \in \mathbb{R}$.

(a) Let $n\colon \mathbb{R} \to \mathbb{R}$, $n(x) = -x$, and $m_c\colon \mathbb{R} \to \mathbb{R}$, $m_c(x) = cx$. Show that $-A = n(A)$ and $cA = m_c(A)$.

(b) Let $s\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $s(a,b) = a + b$. Show that $A + B = s(A \times B)$.

(c) Compute $-[0,1]$, $\{1,2\} + \{10,20\}$, and $\{1,2\} + \{1,2\}$.

Solution.

(a) By the shorthand of Definition 1.7.1, $n(A) = \{n(a) : a \in A\} = \{-a : a \in A\}$, which is $-A$ as written above. In the same way, $m_c(A) = \{ca : a \in A\} = cA$. Nothing more is needed: the set-builder $\{-a : a \in A\}$ **is** the image, written in the form of Definition 1.7.1.

(b) Here the domain is the product $\mathbb{R} \times \mathbb{R}$ of Section 1.4, and $A \times B \subseteq \mathbb{R} \times \mathbb{R}$. An element p of $A \times B$ is a pair (a,b) with $a \in A$ and $b \in B$ (Definition 1.4.2).
($\subseteq$) Let $y \in A + B$. Then $y = a + b$ for some $a \in A$ and $b \in B$; name them. The pair $p \coloneqq (a,b)$ lies in $A \times B$, and $s(p) = a + b = y$. So $y \in s(A \times B)$, with witness p.
($\supseteq$) Let $y \in s(A \times B)$. Then $y = s(p)$ for some $p \in A \times B$; name it p. Since $p \in A \times B$, $p = (a,b)$ for some $a \in A$ and $b \in B$; name them. Then $y = s(a,b) = a + b$, so $y \in A + B$.
Unwinding $y \in s(A \times B)$ took **two** layers of witnesses: first the pair p from the image, then its coordinates a, b from the product.

(c) $-[0,1] = [-1,0]$: if $y = -a$ with $0 \le a \le 1$, then $-1 \le y \le 0$; and if $-1 \le y \le 0$, then $a \coloneqq -y \in [0,1]$ and $y = -a$. Next, $\{1,2\} + \{10,20\}$ is the image of the four pairs $(1,10)$, $(1,20)$, $(2,10)$, $(2,20)$, so it is $\{11,21,12,22\}$, with 4 elements. Finally, $\{1,2\} + \{1,2\}$ is the image of $(1,1)$, $(1,2)$, $(2,1)$, $(2,2)$, which is $\{2,3,4\}$, with only 3 elements: the pairs $(1,2)$ and $(2,1)$ have the same image 3, because s is not injective.

This pays a debt. *Analysis on the Real Line*, Chapter 1 introduces these sets by set-builder, and

part (b) shows that even the two-variable form is an image, of $A \times B$ under s, so Definition 1.7.1 is what all three rest on: an element of $A + B$ is used by naming two witnesses, as in part (b).

1.7.5 Preimages respect every operation

Now the promised theorem. The preimage of a union is the union of the preimages, and the same holds for intersections, complements, and differences. No hypothesis on f is needed.

Theorem 1.7.1. Preimages of Set Operations

Let $f\colon X \to Y$ be a function.

(a) For every family $(B_i)_{i\in I}$ of subsets of Y, $f^{-1}\Big(\bigcup_{i\in I} B_i\Big) = \bigcup_{i\in I} f^{-1}(B_i)$.

(b) For every family $(B_i)_{i\in I}$ of subsets of Y, $f^{-1}\Big(\bigcap_{i\in I} B_i\Big) = \bigcap_{i\in I} f^{-1}(B_i)$, the intersection on the left taken in Y and on the right in X.

(c) For every $B \subseteq Y$, $f^{-1}(Y \setminus B) = X \setminus f^{-1}(B)$.

(d) For all $B, C \subseteq Y$, $f^{-1}(B \setminus C) = f^{-1}(B) \setminus f^{-1}(C)$.

Idea. Unwind each side at a point $x \in X$. A preimage turns "x is in the preimage of something" into "$f(x)$ is in that something". The set operation is then applied to **one** point, $f(x)$, and on the other side it is applied to one point, x, whose membership in each $f^{-1}(B_i)$ is again a statement about $f(x)$. The two sides say the same thing about the same point. No point is ever named as a witness for an image. The only "there exists" is over the index i in (a), and its witness is handed straight from ∃E to ∃I, so no witness can go wrong, and nothing is asked of f.

Proof. Every set in the four laws is a subset of X: a preimage is one by Definition 1.7.2, a union of subsets of X is one because each of its elements lies in some $f^{-1}(B_i) \subseteq X$, an intersection in X and a difference $X \setminus \cdot$ are subsets of X by Definition 1.3.4 and Definition 1.3.1, and $f^{-1}(B) \setminus f^{-1}(C) \subseteq f^{-1}(B)$. For two subsets S, T of X, a point outside X lies in neither, so by Definition 1.2.1, $S = T$ holds as soon as $x \in S \iff x \in T$ for every $x \in X$. Let $x \in X$. In each chain below, the steps labeled (P) are Definition 1.7.2, which applies because $x \in X$; the others are named.

(a)

$$\begin{aligned} x \in f^{-1}\Big(\bigcup_{i\in I} B_i\Big) &\iff f(x) \in \bigcup_{i\in I} B_i && \text{(P)} \\ &\iff \exists i \in I,\ f(x) \in B_i && \text{(union)} \\ &\iff \exists i \in I,\ x \in f^{-1}(B_i) && \text{(P)} \\ &\iff x \in \bigcup_{i\in I} f^{-1}(B_i) && \text{(union).} \end{aligned}$$

The steps marked "union" are Definition 1.3.4. In the third step, for each fixed $i \in I$ the statements $f(x) \in B_i$ and $x \in f^{-1}(B_i)$ are equivalent, so one holds for some i exactly when the other does: a witness i for one is a witness for the other.

(b)

$$\begin{aligned} x \in f^{-1}\Big(\bigcap_{i\in I} B_i\Big) &\iff f(x) \in \bigcap_{i\in I} B_i && \text{(P)} \\ &\iff \forall i \in I,\ f(x) \in B_i && \text{(intersection)} \\ &\iff \forall i \in I,\ x \in f^{-1}(B_i) && \text{(P)} \\ &\iff x \in \bigcap_{i\in I} f^{-1}(B_i) && \text{(intersection).} \end{aligned}$$

In the second step, the intersection in Y is $\{y \in Y : \forall i \in I,\ y \in B_i\}$, and the clause $f(x) \in Y$ holds because f maps into Y. In the last step, the intersection in X is $\{x' \in X : \forall i \in I,\ x' \in f^{-1}(B_i)\}$, and the clause $x \in X$ holds by assumption. The third step holds for each i, hence for all i at once.

(c)

$$\begin{aligned} x \in f^{-1}(Y \setminus B) &\iff f(x) \in Y \setminus B && \text{(P)} \\ &\iff f(x) \notin B && (f(x) \in Y) \\ &\iff x \notin f^{-1}(B) && \text{(P, negated)} \\ &\iff x \in X \setminus f^{-1}(B) && (x \in X). \end{aligned}$$

The second and fourth steps are Definition 1.3.1 for $\setminus$, with the clause that is known to hold dropped. The third negates both sides of the equivalence $x \in f^{-1}(B) \iff f(x) \in B$, as Logic and Proof, Example (Negating both sides of an iff) allows.

(d)

$$\begin{aligned} x \in f^{-1}(B \setminus C) &\iff f(x) \in B \wedge f(x) \notin C \\ &\iff x \in f^{-1}(B) \wedge x \notin f^{-1}(C) \\ &\iff x \in f^{-1}(B) \setminus f^{-1}(C), \end{aligned}$$

by (P) and Definition 1.3.1 in the first step, (P) and Logic and Proof, Example (Negating both sides of an iff) in the second, and Definition 1.3.1 in the third.

In each chain the equivalences link up, so the first statement is equivalent to the last, for every $x \in X$. This proves the theorem.

■

The proof never named a witness for an image (the index i in (a) is taken by $\exists$E and passed unchanged to $\exists$I) and never used a property of f beyond its being a function. That is the whole content of the slogan: a preimage hides nothing. Each law of sets was carried across by the corresponding law of logic, applied to the one point $f(x)$, exactly as in Section 1.3.

The empty family is covered. When $I = \emptyset$, the intersection of the empty family in Y is Y and in X is X (Definition 1.3.4), and (b) says $f^{-1}(Y) = X$, which is true. The union of the empty family is $\emptyset$, and (a) says $f^{-1}(\emptyset) = \emptyset$, also true. This is the payoff of taking intersections inside a named ambient set: the theorem holds with no exception for $I = \emptyset$.

Quick check. For $f(x) = x^2$ on $\mathbb{R}$, compute $f^{-1}([-1, 4])$ and $f^{-1}((-\infty, 0))$.

Solution. $f^{-1}([-1, 4]) = [-2, 2]$: since $x^2 \geq 0 \geq -1$ always, the condition is $x^2 \leq 4$, that is $|x| \leq 2$. $f^{-1}((-\infty, 0)) = \emptyset$: no square is negative.

Preimages also behave well under composition, with the order reversed. We will need this in *Metric and Topological Spaces*, Chapter 1, to show that composites of continuous maps are continuous.

Proposition 1.7.2. Preimage under a Composite

Let $f\colon X \to Y$ and $g\colon Y \to Z$ be functions, and $C \subseteq Z$. Then

$$(g \circ f)^{-1}(C) = f^{-1}(g^{-1}(C)).$$

Proof. Both sides are subsets of X by Definition 1.7.2, so, as in the proof of Theorem 1.7.1, it suffices to compare memberships of each $x \in X$. For $x \in X$,

$$\begin{aligned} x \in (g \circ f)^{-1}(C) &\iff g(f(x)) \in C \iff f(x) \in g^{-1}(C) \\ &\iff x \in f^{-1}(g^{-1}(C)). \end{aligned}$$

The first step is Definition 1.7.2 for $g \circ f$ with Definition 1.5.2; the second is Definition 1.7.2 for g, which applies because $f(x) \in Y$; the third is Definition 1.7.2 for f. This proves the proposition.

■

To pull a set back through "first f, then g", pull it back through g first. This is the same reversal as for the inverse of a composite (Exercise B2 of Section 1.6), and here no function needs an inverse.

1.7.6 Images respect unions

Now push forwards. For unions the result is the same as for preimages, but the proof is different in kind: it has to name witnesses.

Theorem 1.7.3. Image of a Union

Let $f\colon X \to Y$ be a function, and let $(A_i)_{i \in I}$ be a family of subsets of X. Then

$$f\Big(\bigcup_{i \in I} A_i\Big) = \bigcup_{i \in I} f(A_i).$$

Idea. Unwind the left side at a point y: there is a point a in the union with $f(a) = y$, and being in the union means there is an index i with $a \in A_i$. So "there is a, and there is i". The right side says "there is i, and there is a". The two differ only in the order of two "there exists", and two existential quantifiers can be exchanged: name both witnesses, then reintroduce them so that the quantifiers come out in the other order.

Proof. We prove two inclusions. The union $\bigcup_{i \in I} A_i$ is a subset of X, so its image is defined.

($\subseteq$) Let $y \in f(\bigcup_{i \in I} A_i)$. By Definition 1.7.1, $y \in Y$ and there is $a \in \bigcup_{i \in I} A_i$ with $f(a) = y$; name such a point a [$\exists$E]. By Definition 1.3.4, there is $j \in I$ with $a \in A_j$; name such an

index j [∃E]. Now $a \in A_j$ and $f(a) = y$, so $y \in f(A_j)$, with witness a [∃I]. Since $j \in I$, $y \in \bigcup_{i\in I} f(A_i)$, with witness j [∃I].

($\supseteq$) Let $y \in \bigcup_{i\in I} f(A_i)$. There is $j \in I$ with $y \in f(A_j)$; name it j [∃E]. So $y \in Y$, and there is $a \in A_j$ with $f(a) = y$; name it a [∃E]. Since $a \in A_j$ and $j \in I$, $a \in \bigcup_{i\in I} A_i$, with witness j [∃I]. Since $f(a) = y$, $y \in f(\bigcup_{i\in I} A_i)$, with witness a [∃I].

This proves the theorem.

■

Look at the order of the tags in ($\subseteq$): ∃E for a, ∃E for j, ∃I for a, ∃I for j. The witnesses are reintroduced in the same order they were named. Because ∃I builds the formula from the inside out, a, which was the outer witness, ends up as the inner one. To rebuild the quantifiers in their old order, the ∃I steps would have run in reverse, ∃I for j before ∃I for a. That the order is not reversed is the exchange of the two "there exists". The two ∃E boxes may close at the end because the conclusion $y \in \bigcup_i f(A_i)$ mentions neither a nor j: the side condition of ∃E (*Logic and Proof*, Section 5.6) holds. The case $I = \emptyset$ needs no separate treatment: both sides are $f(\emptyset) = \emptyset$ and $\emptyset$.

1.7.7 Images and intersections

For unions, images behave. For intersections, the question of the opening showed they do not: $f(A \cap B) = \{0\}$ and $f(A) \cap f(B) = [0, 1]$ for the squaring map. One inclusion survives, and the other fails in a way that is instructive, because the failing inclusion has a tempting false proof.

Example. Two witnesses under one name

Here is a "proof" that $f(A)\cap f(B) \subseteq f(A\cap B)$ for every function $f\colon X \to Y$ and all $A, B \subseteq X$.

> (1) Let $y \in f(A) \cap f(B)$. (2) Then $y \in f(A)$, so $y = f(x)$ for some $x \in A$. (3) Also $y \in f(B)$, so $y = f(x)$ for some $x \in B$. (4) Hence $x \in A$ and $x \in B$, so $x \in A \cap B$. (5) Therefore $y = f(x) \in f(A \cap B)$.

Show that the conclusion is false, and find the line that fails.

Solution. The conclusion is false. Take $f(x) = x^2$ on $\mathbb{R}$, $A = \{-1\}$, and $B = \{1\}$. Then $f(A) = f(B) = \{1\}$, so $f(A) \cap f(B) = \{1\}$; but $A \cap B = \emptyset$, so $f(A \cap B) = \emptyset$, and $1 \notin \emptyset$.

The failing line is (3). Line (2) is a correct ∃E: it names a witness $x \in A$ with $f(x) = y$. Line (3) performs a second ∃E, on $y \in f(B)$, and gives its witness the **same** name x. The rule requires a fresh name (*Logic and Proof*, Section 5.6). The statement "$y = f(b)$ for some $b \in B$" promises some point of B, not the point already named. Reusing the name silently asserts that the two witnesses are equal, and nothing says they are. This is the error "one name for two witnesses", entry (N4) of the catalogue of what is not allowed (*Logic and Proof*, Section 8.6).

A counterexample to the step. With the data above and $y = 1$: line (2) names $x = -1$, the only point of A. The only point of B with square 1 is $1 \neq -1$, so line (3), with the name x meaning the x of line (2), asserts $-1 \in B$, which is false. Lines (4) and (5) are correct inferences from what (3) wrongly asserts.

Hunting a counterexample. How would one find that counterexample without knowing it? The inclusion that might fail is $f(A) \cap f(B) \subseteq f(A \cap B)$. A failure needs a point y in both images with no preimage in $A \cap B$: a preimage $a \in A$ and a preimage $b \in B$, with $a \neq b$. So f must send two different points to one, and the smallest attempt is $A = \{a\}$, $B = \{b\}$ (Example (Method: disproof by counterexample, proof by example)). For squaring, $a = -1$ and $b = 1$ gives exactly the failure just found.

Quick check. For a constant map $c\colon X \to Y$ with value y_0 and two points $x_1 \neq x_2$ of X, compute $c(\{x_1\} \cap \{x_2\})$ and $c(\{x_1\}) \cap c(\{x_2\})$.

Solution. $\{x_1\} \cap \{x_2\} = \emptyset$, since $x_1 \neq x_2$, so $c(\{x_1\} \cap \{x_2\}) = c(\emptyset) = \emptyset$. And $c(\{x_1\}) = \{y_0\} = c(\{x_2\})$, so $c(\{x_1\}) \cap c(\{x_2\}) = \{y_0\}$.

Warning. When you unwind two images, give the two witnesses two names: "$y = f(a)$ with $a \in A$, and $y = f(b)$ with $b \in B$". A single name is a hidden claim that $a = b$, which is exactly what fails for $x \mapsto x^2$ with $a = -1$, $b = 1$. If the proof needs them equal, it must prove it.

With two names, the proof gets as far as $f(a) = y = f(b)$ and stops. To conclude $a = b$ we need exactly the property that injectivity supplies. So the inclusion should hold for injective functions, and only for them.

Theorem 1.7.4. Image of an Intersection

Let $f\colon X \to Y$ be a function.

(a) For all $A, B \subseteq X$, $f(A \cap B) \subseteq f(A) \cap f(B)$.

(b) The equality $f(A \cap B) = f(A) \cap f(B)$ holds for all $A, B \subseteq X$ **if and only if** f is injective.

Try it first (ten minutes): if f is injective, why should $f(A) \cap f(B) \subseteq f(A \cap B)$ hold? Start from "let $y \in f(A) \cap f(B)$" and unwind both images, with two names.

Idea. The attempt names $a \in A$ and $b \in B$ with $f(a) = y = f(b)$, and then has two points where it needs one in $A \cap B$. That is the obstacle Example (Two witnesses under one name) tried to wish away. Injectivity removes it: $f(a) = f(b)$ gives $a = b$, so a lies in both sets.

For the converse, run the failure backwards. If equality holds for **all** A, B, use it on the smallest sets that could show a failure of injectivity: two one-point sets $\{x_1\}$ and $\{x_2\}$ with $f(x_1) = f(x_2)$.

Before reading on: which line of the proof of ($\Leftarrow$) uses injectivity, and which line of ($\Rightarrow$) uses that equality holds for all sets rather than for one pair?

Proof.

(a) Let $y \in f(A \cap B)$. By Definition 1.7.1 there is $c \in A \cap B$ with $f(c) = y$; name it c. Since $c \in A$, $y \in f(A)$, with witness c; since $c \in B$, $y \in f(B)$, with witness c. So $y \in f(A) \cap f(B)$.

(b) ($\Leftarrow$) Suppose f is injective, and let $A, B \subseteq X$. By (a) it suffices to prove $f(A) \cap f(B) \subseteq f(A \cap B)$. Let $y \in f(A) \cap f(B)$. Since $y \in f(A)$, there is $a \in A$ with $f(a) = y$; name it a [$\exists$E]. Since $y \in f(B)$, there is $b \in B$ with $f(b) = y$; name it b, a new name [$\exists$E]. Then $f(a) = y = f(b)$, so $a = b$ because f is injective (Definition 1.5.3). Hence $a \in B$, so $a \in A \cap B$, and $y = f(a) \in f(A \cap B)$, with witness a [$\exists$I].

($\Rightarrow$) Suppose $f(A \cap B) = f(A) \cap f(B)$ for all $A, B \subseteq X$. Let $x_1, x_2 \in X$ with $f(x_1) = f(x_2)$, and apply the hypothesis to $A := \{x_1\}$ and $B := \{x_2\}$. Now $f(x_1) \in f(A)$, with witness x_1, and $f(x_1) = f(x_2) \in f(B)$, with witness x_2. So $f(x_1) \in f(A) \cap f(B) = f(A \cap B)$. Hence there is $c \in \{x_1\} \cap \{x_2\}$ with $f(c) = f(x_1)$; name it c. Then $c = x_1$ and $c = x_2$, so $x_1 = x_2$. Since x_1, x_2 were arbitrary, f is injective. This proves the theorem.

■

The proof of ($\Rightarrow$) is direct: it proves $x_1 = x_2$ by pushing the one-point sets through the hypothesis, without supposing $x_1 \neq x_2$. Read contrapositively, the same sets give the witness of failure: whenever $f(x_1) = f(x_2)$ with $x_1 \neq x_2$, the sets $\{x_1\}$ and $\{x_2\}$ have $f(\{x_1\} \cap \{x_2\}) = f(\emptyset) = \emptyset$ while $f(\{x_1\}) \cap f(\{x_2\}) = \{f(x_1)\}$. For the squaring map, $x_1 = -1$ and $x_2 = 1$ is such a pair, and the intervals $[-1, 0]$ and $[0, 1]$ of the opening are a larger failure of the same kind.

Compare with Example (Two witnesses under one name). The false proof and the true one begin identically. The false one reuses a name and thereby assumes $a = b$; the true one keeps two names and **proves** $a = b$, from injectivity, on the one line where the hypothesis is used. That line is the whole difference between a theorem and a false statement.

1.7.8 There and back

What happens when we push a set forwards and pull it back, or the other way round? Part (d) of Example (Images and preimages of intervals under squaring) and the quick check after it gave one answer each for the squaring map: $f^{-1}(f([0, 1])) = [-1, 1]$ is bigger than $[0, 1]$, and $f(f^{-1}([-1, 1])) = [0, 1]$ is smaller than $[-1, 1]$. In general, the round trip through Y can only grow a set, and the round trip through X can only shrink one.

Proposition 1.7.5. Image and Preimage Round Trips

Let $f\colon X \to Y$ be a function.

(a) $A \subseteq f^{-1}(f(A))$ for every $A \subseteq X$. Equality holds for all $A \subseteq X$ if and only if f is injective.

(b) $f(f^{-1}(B)) = B \cap f(X)$ for every $B \subseteq Y$; in particular $f(f^{-1}(B)) \subseteq B$. Equality $f(f^{-1}(B)) = B$ holds for all $B \subseteq Y$ if and only if f is surjective.

Idea. For (a), a point $a \in A$ is sent into $f(A)$, with itself as witness, so it lies in the preimage. A point x of the preimage has $f(x) = f(a)$ for some $a \in A$, and it lies in A when $x = a$: that is injectivity again. For (b), a point of $f(f^{-1}(B))$ is $f(x)$ with $f(x) \in B$: so it lies in B, and

it is a value of f. Those two conditions are all there is to it.

Proof.

(a) Let $A \subseteq X$ and $a \in A$. Then $a \in X$, and $f(a) \in f(A)$, with witness a. So $a \in f^{-1}(f(A))$ by Definition 1.7.2. This proves $A \subseteq f^{-1}(f(A))$.
($\Leftarrow$) Suppose f is injective, and let $x \in f^{-1}(f(A))$. Then $x \in X$ and $f(x) \in f(A)$, so there is $a \in A$ with $f(a) = f(x)$; name it a [$\exists$E]. Since f is injective (Definition 1.5.3), $a = x$, so $x \in A$. With the inclusion already proved, $A = f^{-1}(f(A))$ by Proposition 1.2.1.
($\Rightarrow$) Suppose $A = f^{-1}(f(A))$ for every $A \subseteq X$. Let $x_1, x_2 \in X$ with $f(x_1) = f(x_2)$. Then $f(x_2) = f(x_1) \in f(\{x_1\})$, with witness x_1, so $x_2 \in f^{-1}(f(\{x_1\}))$ by Definition 1.7.2. The hypothesis with $A = \{x_1\}$, a subset of X because $x_1 \in X$, gives $f^{-1}(f(\{x_1\})) = \{x_1\}$, so $x_2 \in \{x_1\}$. Hence $x_2 = x_1$, and f is injective.

(b) Let $B \subseteq Y$. ($\subseteq$) Let $y \in f(f^{-1}(B))$. There is $x \in f^{-1}(B)$ with $f(x) = y$; name it x. Then $x \in X$ and $f(x) \in B$, so $y \in B$; and $y \in f(X)$, with witness x. ($\supseteq$) Let $y \in B \cap f(X)$. Since $y \in f(X)$, there is $x \in X$ with $f(x) = y$; name it x. Then $f(x) = y \in B$, so $x \in f^{-1}(B)$, and $y \in f(f^{-1}(B))$, with witness x. This proves $f(f^{-1}(B)) = B \cap f(X)$, and $B \cap f(X) \subseteq B$.

For the last statement: if f is surjective (Definition 1.5.4), every $y \in Y$ lies in $f(X)$; since $f(X) \subseteq Y$ by Definition 1.7.1, $f(X) = Y$ by Proposition 1.2.1, and $B \cap f(X) = B \cap Y = B$ for every $B \subseteq Y$, because $B \subseteq Y$. Conversely, if $f(f^{-1}(B)) = B$ for every $B \subseteq Y$, take $B = Y$: since $f^{-1}(Y) = X$, this says $f(X) = Y$, so every $y \in Y$ is $f(x)$ for some $x \in X$ (Definition 1.7.1), and f is surjective (Definition 1.5.4). This proves the proposition.

■

So the two round trips measure the two failures of Section 1.5. Pushing forwards and pulling back adds to A the points that share a value with a point of A: nothing is added, for every A, exactly when f is injective. Pulling back and pushing forwards removes from B the points that are never hit: nothing is removed, for every B, exactly when f is surjective.

Quick check. For $f(x) = x^2$ on $\mathbb{R}$, compute $f^{-1}(f([1,3]))$ and $f(f^{-1}([-4,9]))$, and compare each with the set you started from.

Solution. $f([1,3]) = [1,9]$, and $f^{-1}([1,9]) = [-3,-1] \cup [1,3]$, which contains $[1,3]$ and more: the points $-3 \leq x \leq -1$ share their squares with points of $[1,3]$. Next, $f^{-1}([-4,9]) = [-3,3]$, since the condition $-4 \leq x^2$ always holds, and $f([-3,3]) = [0,9]$, which is $[-4,9] \cap f(\mathbb{R}) = [-4,9] \cap [0,\infty)$, as Proposition 1.7.5 (b) predicts: the points of $[-4,0)$ are never hit.

1.7.9 Two readings of the inverse symbol

Remark. The symbol f^{-1} now has two uses. For **every** function $f\colon X \to Y$ and every $B \subseteq Y$, $f^{-1}(B)$ is the preimage of Definition 1.7.2. For a **bijection** f, $f^{-1}\colon Y \to X$ is also

the inverse function of Definition 1.6.2, and then $f^{-1}(B)$ could also be read as the image of B under that function. The two readings give the same set. Write g for the inverse function; both sets are subsets of X. If $x = g(b)$ with $b \in B$, then $f(x) = f(g(b)) = b \in B$, since $f \circ g = \mathrm{id}_Y$, so x lies in the preimage. If $x \in X$ and $f(x) \in B$, then $x = g(f(x)) \in g(B)$, since $g \circ f = \mathrm{id}_X$. So the two readings name the same set, and the notation is never ambiguous. When f is not a bijection only the first reading exists.

For example, $a(x) = 3x - 2$ on $\mathbb{R}$ is a bijection with inverse $a^{-1}(y) = (y + 2)/3$ (Section 1.6). The preimage $a^{-1}([1, 4])$ is $\{x \in \mathbb{R} : 1 \le 3x - 2 \le 4\} = [1, 2]$, and the image of $[1, 4]$ under the inverse function is $\{(y + 2)/3 : y \in [1, 4]\} = [1, 2]$ as well.

1.7.10 Exercises

1.7.10.1 A. Check your understanding

Exercise. A1

Parts (a)–(d) are about Theorem 1.7.1 and its proof.

(a) Suppose we tried to prove the image version of law (b), $f(\bigcap_{i\in I} A_i) = \bigcap_{i\in I} f(A_i)$, by the same kind of chain. At which step would a witness have to be named, and why does the preimage version need none?

(b) Run law (b) on $f(x) = x^2$ on $\mathbb{R}$, with $I = \{1, 2\}$, $B_1 = [0, 4]$, and $B_2 = [1, 9]$: compute both sides.

(c) What are both sides of law (b) when $I = \emptyset$?

(d) State law (c) in symbols, for $f\colon X \to Y$ and $B \subseteq Y$.

(e) True or false, with a reason: for every $A \subseteq X$, $f(X \cap A) = f(A)$.

Solution.

(a) At the step that unwinds $y \in \bigcap_i f(A_i)$ into "for every $i \in I$, $y \in f(A_i)$", and then each $y \in f(A_i)$ into "there is $a_i \in A_i$ with $f(a_i) = y$". The witnesses a_i may differ from one i to another, and the left side needs **one** point in every A_i. In the preimage version, the corresponding step is "for every i, $f(x) \in B_i$", a statement about the single point $f(x)$ with no "there exists" in it, so nothing needs naming.

(b) $B_1 \cap B_2 = [1, 4]$, so the left side is $f^{-1}([1, 4]) = [-2, -1] \cup [1, 2]$ (Example (Images and preimages of intervals under squaring) (b)). On the right, $f^{-1}([0, 4]) = [-2, 2]$ and $f^{-1}([1, 9]) = [-3, -1] \cup [1, 3]$, whose intersection is $[-2, -1] \cup [1, 2]$. The two sides agree.

(c) Both are X. The left side is $f^{-1}(Y) = X$, since the empty intersection in Y is Y; the right side is the empty intersection in X, which is X.

(d) $f^{-1}(Y \setminus B) = X \setminus f^{-1}(B)$: a point of X is sent outside B exactly when it is not in the preimage of B.

(e) True. Since $A \subseteq X$, $X \cap A = A$ (each element of A lies in X), so the two sides are the image of the same set.

1.7.10.2 B. Practice

Exercise. B1: Computing images and preimages

Compute each set, and prove each equality by two inclusions or by a chain of equivalences.

(a) For $d\colon \mathbb{N}\times\mathbb{N}\to\mathbb{Z}$, $d(m,n)=m-n$: the image $d(\{(m,n)\in\mathbb{N}\times\mathbb{N} : m>n\})$ and the preimage $d^{-1}(\{0\})$.

(b) For $\mathbf{1}_{[0,1]}\colon\mathbb{R}\to\{0,1\}$: the preimages of $\{1\}$ and $\{0\}$, and the image of $[2,3]$.

(c) For $g\colon\mathbb{R}\to\mathbb{R}$, $g(x)=x^2-2x$: the image $g([0,3])$ and the preimages $g^{-1}(\{0\})$ and $g^{-1}([-1,0])$.

Solution.

(a) The image is $\mathbb{Z}_{>0}$. ($\subseteq$) If $y=m-n$ with $m>n$, then y is an integer and $y>0$, so $y\in\mathbb{Z}_{>0}$. ($\supseteq$) Let $k\in\mathbb{Z}_{>0}$. The pair $(k,0)$ lies in $\mathbb{N}\times\mathbb{N}$, has $k>0$, and $d(k,0)=k$; so k is in the image. The preimage is $d^{-1}(\{0\})=\{(m,n)\in\mathbb{N}\times\mathbb{N} : m=n\}=\{(n,n) : n\in\mathbb{N}\}$, since $m-n=0$ exactly when $m=n$.

(b) By the definition of the indicator (Section 1.5), $\mathbf{1}_{[0,1]}(x)=1$ for $x\in[0,1]$ and 0 otherwise. So $\mathbf{1}_{[0,1]}^{-1}(\{1\})=[0,1]$ and $\mathbf{1}_{[0,1]}^{-1}(\{0\})=\mathbb{R}\setminus[0,1]$, each a chain of one equivalence. The image $\mathbf{1}_{[0,1]}([2,3])=\{0\}$: every point of $[2,3]$ lies outside $[0,1]$ and is sent to 0, and 0 is hit, for instance by 2.

(c) Write $g(x)=(x-1)^2-1$. The image is $g([0,3])=[-1,3]$. ($\subseteq$) If $0\le a\le 3$, then $-1\le a-1\le 2$, so $|a-1|\le 2$, and hence $0\le(a-1)^2=|a-1|^2\le 4$ by Logic and Proof, Theorem 2.4.5 applied to $|a-1|$ and 2, and $-1\le g(a)\le 3$. ($\supseteq$) Let $-1\le y\le 3$, and take $a:=1+\sqrt{y+1}$. Then $0\le\sqrt{y+1}\le 2$, so $a\in[1,3]\subseteq[0,3]$, and $g(a)=(y+1)-1=y$. For the preimages: $g(x)=0\iff x(x-2)=0\iff x\in\{0,2\}$, so $g^{-1}(\{0\})=\{0,2\}$; and $-1\le g(x)\le 0\iff 0\le(x-1)^2\le 1\iff|x-1|\le 1\iff x\in[0,2]$, so $g^{-1}([-1,0])=[0,2]$.

Exercise. B2: Two laws, element by element

Let $f\colon X\to Y$ be a function. Prove each law directly, by two inclusions or by a chain of equivalences at a point, tagging each step that names or exhibits a witness with [$\exists$E] or [$\exists$I].

(a) $f(A\cup B)=f(A)\cup f(B)$ for $A,B\subseteq X$. (This is a case of Theorem 1.7.3; prove it without citing it.)

(b) $f^{-1}(C\setminus D)=f^{-1}(C)\setminus f^{-1}(D)$ for $C,D\subseteq Y$. (This is Theorem 1.7.1 (d); prove it without citing it.) Which steps, if any, need a tag?

Solution.

(a) ($\subseteq$) Let $y\in f(A\cup B)$. There is $c\in A\cup B$ with $f(c)=y$; name it c [$\exists$E]. By Definition 1.3.1, $c\in A$ or $c\in B$. *Case 1:* $c\in A$. Then $y\in f(A)$, with witness c [$\exists$I], so $y\in f(A)\cup f(B)$. *Case 2:* $c\in B$. Then $y\in f(B)$, with witness c [$\exists$I], so $y\in f(A)\cup f(B)$. ($\supseteq$) Let $y\in f(A)\cup f(B)$. *Case 1:* $y\in f(A)$. There is $a\in A$ with $f(a)=y$; name it a [$\exists$E]. Then $a\in A\cup B$, so $y\in f(A\cup B)$, with witness a [$\exists$I]. *Case 2:* $y\in f(B)$ is the same with B in place of A. In either case $y\in f(A\cup B)$.

(b) Both sides are subsets of X. For $x\in X$: $x\in f^{-1}(C\setminus D)$ if and only if $f(x)\in C\setminus D$ (Definition 1.7.2) if and only if $f(x)\in C$ and $f(x)\notin D$ (Definition 1.3.1) if and only if

$x \in f^{-1}(C)$ and $x \notin f^{-1}(D)$ (Definition 1.7.2, and Logic and Proof, Example (Negating both sides of an iff) for the second clause) if and only if $x \in f^{-1}(C) \setminus f^{-1}(D)$. No step names or exhibits a witness, so no step carries a tag: this is the difference between (a) and (b).

Exercise. B3: The two readings of the inverse

Let $f\colon X \to Y$ be a bijection, with inverse function $f^{-1}\colon Y \to X$, and let $B \subseteq Y$. Prove that the image of B under the function f^{-1} equals the preimage of B under f. To keep the readings apart, write $g \coloneqq f^{-1}$ for the inverse function, and prove $g(B) = \{x \in X : f(x) \in B\}$. The remark in "Two readings of the inverse symbol" gives the argument in brief; write it out as two inclusions, tagging each step that names or exhibits a witness with [∃E] or [∃I].

Solution. ($\subseteq$) Let $x \in g(B)$. There is $b \in B$ with $g(b) = x$; name it b [∃E]. Then $x \in X$, and $f(x) = f(g(b)) = b \in B$, since $f \circ g = \mathrm{id}_Y$. So x lies in the preimage.

($\supseteq$) Let $x \in X$ with $f(x) \in B$. Then $g(f(x)) = x$, since $g \circ f = \mathrm{id}_X$. So $x \in g(B)$, with witness $f(x) \in B$ [∃I].

Hence $g(B)$ equals the preimage of B under f: for a bijection, the two readings of $f^{-1}(B)$ name the same set. Both equations of Definition 1.6.2 were used, one in each inclusion.

1.7.10.3 C. Going deeper

Exercise. C1: Images and differences

Let $f\colon X \to Y$ be a function and $A, B \subseteq X$.

(a) Here are the first lines of a proof that $f(A) \setminus f(B) \subseteq f(A \setminus B)$. *Name the move, then complete it.*

Let $y \in f(A) \setminus f(B)$. Then $y \in f(A)$, so there is $a \in A$ with $f(a) = y$; name it a [∃E]. Also $y \notin f(B)$.

(b) Show that the reverse inclusion can fail, with $f(x) = x^2$ on $\mathbb{R}$, $A = \{-1, 1\}$, and $B = \{1\}$.

(c) Prove that $f(A \setminus B) = f(A) \setminus f(B)$ holds for all $A, B \subseteq X$ if and only if f is injective.

Solution.

(a) The move is **element-chasing**: unwind the membership of the hypothesis into its definition, and rewind into the definition of the goal. The goal is $y \in f(A \setminus B)$, which needs a witness in $A \setminus B$, and the natural candidate is the a already named. We know $a \in A$; we need $a \notin B$.
Suppose $a \in B$. Then $y = f(a) \in f(B)$, with witness a [∃I], which contradicts $y \notin f(B)$. Hence $a \notin B$ [¬I]. So $a \in A \setminus B$ and $f(a) = y$, which gives $y \in f(A \setminus B)$, with witness a [∃I].

(b) $A \setminus B = \{-1\}$, so $f(A \setminus B) = \{1\}$. But $f(A) = \{1\} = f(B)$, so $f(A) \setminus f(B) = \emptyset$. The point 1 lies in $f(A \setminus B)$ and not in $f(A) \setminus f(B)$.

(c) ($\Leftarrow$) Suppose f is injective. By (a) it suffices to show $f(A \setminus B) \subseteq f(A) \setminus f(B)$. Let $y \in f(A \setminus B)$, and name $a \in A \setminus B$ with $f(a) = y$. Then $y \in f(A)$, with witness a. Suppose $y \in f(B)$, and name $b \in B$ with $f(b) = y$. Then $f(a) = f(b)$, so $a = b$ by injectivity, and $a \in B$, contradicting $a \in A \setminus B$. Hence $y \notin f(B)$, and $y \in f(A) \setminus f(B)$.

($\Rightarrow$) Suppose equality holds for all $A, B \subseteq X$. Let $x_1, x_2 \in X$ with $f(x_1) = f(x_2)$, and take $A \coloneqq \{x_1\}$, $B \coloneqq \{x_2\}$. Then $f(A) = \{f(x_1)\} = f(B)$, so $f(A \setminus B) = f(A) \setminus f(B) = \emptyset$. Suppose $x_1 \neq x_2$. Then $x_1 \in A \setminus B$, so $f(x_1) \in f(A \setminus B) = \emptyset$, which is impossible. Hence $x_1 = x_2$, by RAA (Logic and Proof, Definition 2.5.1), and f is injective.

Marking scheme. (10 points)

- 3: (a) shows $a \notin B$ by deriving $y \in f(B)$ from $a \in B$, and concludes $y \in f(A \setminus B)$ with the witness a.
- 2: (b) computes both sides for the given data.
- 3: (c) ($\Leftarrow$) names two witnesses, $a \in A \setminus B$ and $b \in B$, and uses injectivity to identify them.
- 2: (c) ($\Rightarrow$) applies the hypothesis to one-point sets (or any sets that separate x_1 from x_2) and concludes $x_1 = x_2$.

Fatal errors (0 for the step): using one name for the witnesses of $y \in f(A \setminus B)$ and $y \in f(B)$ (entry (N4) of *Logic and Proof*, Chapter 8's catalogue); in ($\Rightarrow$), assuming injectivity to compute $f(A \setminus B)$.

Exercise. C2: Find the error

A student proves the following claim: *if $f\colon X \to Y$ is injective and $A \subseteq X$, then $f^{-1}(f(A)) \subseteq A$.*

> (1) Let $x \in f^{-1}(f(A))$. (2) By the definition of preimage, $x \in X$ and $f(x) \in f(A)$. (3) Since $f(x) \in f(A)$, we have $x \in A$. (4) Since x was arbitrary, $f^{-1}(f(A)) \subseteq A$.

(a) Is the claim true?

(b) Which line fails, and which rule does it skip?

(c) Give a counterexample to the failing step, and repair the proof.

Solution.

(a) The claim is true: it is the ($\Leftarrow$) half of Proposition 1.7.5 (a).

(b) Line (3) fails. The statement $f(x) \in f(A)$ says only that $f(a) = f(x)$ for **some** $a \in A$ (Definition 1.7.1). To use it, the proof must name that witness by $\exists$E, with a fresh name. Line (3) skips the $\exists$E and silently takes the witness to be x itself. The name x is already in use (line (1) introduced it), so the step breaks the fresh-name condition of $\exists$E (*Logic and Proof*, Section 5.6), the condition behind entry (N4) of the catalogue of *Logic and Proof*, Chapter 8. The tell is that injectivity, a hypothesis, is never used: an argument that ignores a necessary hypothesis cannot be right.

(c) A counterexample to the step "$f(x) \in f(A)$, so $x \in A$" needs a non-injective function, since for injective ones the conclusion of the step is true. Take $f(x) = x^2$ on $\mathbb{R}$, $A = \{1\}$,

and $x = -1$. Then $f(x) = 1 \in f(A)$, but $x \notin A$.

Repair: replace (3) by "Since $f(x) \in f(A)$, there is $a \in A$ with $f(a) = f(x)$; name it a. Since f is injective, $a = x$. Hence $x \in A$."

Exercise. C3: Exit check: preimages

(a) Let $f\colon X \to Y$ be a function and $(B_i)_{i\in I}$ a family of subsets of Y. Prove that $f^{-1}(\bigcap_{i\in I} B_i) = \bigcap_{i\in I} f^{-1}(B_i)$, the intersections taken in Y and in X.

(b) Give a function f and sets A, B with $f(A \cap B) \neq f(A) \cap f(B)$, computing both sides.

Solution.

(a) We prove two inclusions.
($\subseteq$) Let $x \in f^{-1}(\bigcap_{i\in I} B_i)$. By Definition 1.7.2, $x \in X$ and $f(x) \in \bigcap_{i\in I} B_i$. By Definition 1.3.4, $f(x) \in B_i$ for every $i \in I$. Let $i \in I$. Then $f(x) \in B_i$ and $x \in X$, so $x \in f^{-1}(B_i)$. Since i was arbitrary, x lies in every $f^{-1}(B_i)$, and since $x \in X$, $x \in \bigcap_{i\in I} f^{-1}(B_i)$.
($\supseteq$) Let $x \in \bigcap_{i\in I} f^{-1}(B_i)$. Then $x \in X$ and $x \in f^{-1}(B_i)$ for every $i \in I$. Let $i \in I$. Then $f(x) \in B_i$ by Definition 1.7.2. Since i was arbitrary, and $f(x) \in Y$, $f(x) \in \bigcap_{i\in I} B_i$. So $x \in f^{-1}(\bigcap_{i\in I} B_i)$.
If $I = \emptyset$, both sides are X, and the argument above covers this case: the "for every i" statements hold vacuously.

(b) Let $f\colon \{1, 2\} \to \{0\}$ be the constant function, $A = \{1\}$, $B = \{2\}$. Then $A \cap B = \emptyset$, so $f(A \cap B) = \emptyset$. But $f(A) = \{0\} = f(B)$, so $f(A) \cap f(B) = \{0\} \neq \emptyset$. (The squaring map with $A = [-1, 0]$, $B = [0, 1]$ is another answer: $\{0\}$ against $[0, 1]$.)

Marking scheme. (10 points)

- 1: announces two inclusions (or a chain of equivalences at a point $x \in X$).
- 3: ($\subseteq$) unwinds $x \in f^{-1}(\bigcap B_i)$ to "$f(x) \in B_i$ for every i", then rewinds to $x \in f^{-1}(B_i)$ for an **arbitrary** i.
- 3: ($\supseteq$) the reverse chain, with i arbitrary.
- 1: the ambient sets are named ($x \in X$, $f(x) \in Y$) or the case $I = \emptyset$ is handled.
- 2: a correct example, with both sides computed.

A single chain of equivalences, each step justified, earns the first seven points. Fatal errors (0 for the step): fixing one i and concluding for all i (entry (N1) of *Logic and Proof*, Chapter 8's catalogue); stating the example's two sides without checking an element that lies in one and not the other.

1.7.10.4 R. Review

Exercise. R1

Here is a derivation of "if $A \subseteq B$, then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$". The steps "by def." unwind or rewind Definition 1.2.2 and Definition 1.3.2.

1		$A \subseteq B$	
2		$\forall x(x \in A \to x \in B)$	def. 1
3		S_0 | $S_0 \in \mathcal{P}(A)$	
4		$S_0 \subseteq A$	def. 3
5		$\forall x(x \in S_0 \to x \in A)$	def. 4
6		x_0 | $x_0 \in S_0$	
7		$x_0 \in S_0 \to x_0 \in A$	∀E 5
8		$x_0 \in A$	→E 7, 6
9		$x_0 \in A \to x_0 \in B$	∀E 2
10		$x_0 \in B$	→E 9, 8
11		$x_0 \in S_0 \to x_0 \in B$	→I 6–10
12		$\forall x(x \in S_0 \to x \in B)$	∀I 6–11
13		$S_0 \subseteq B$	def. 12
14		$S_0 \in \mathcal{P}(B)$	def. 13
15		$S_0 \in \mathcal{P}(A) \to S_0 \in \mathcal{P}(B)$	→I 3–14
16		$\forall S(S \in \mathcal{P}(A) \to S \in \mathcal{P}(B))$	∀I 3–15
17		$\mathcal{P}(A) \subseteq \mathcal{P}(B)$	def. 16
18	$A \subseteq B \to \mathcal{P}(A) \subseteq \mathcal{P}(B)$		→I 1–17

Write the proof as plain prose, the way a mathematician would. Then say which sentence of your proof carries each of the five boxes.

Solution. Proof. Suppose $A \subseteq B$. Let $S \in \mathcal{P}(A)$, so $S \subseteq A$. Let $x \in S$. Then $x \in A$, since $S \subseteq A$, and so $x \in B$, since $A \subseteq B$. Hence $S \subseteq B$, that is, $S \in \mathcal{P}(B)$. This proves $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

The boxes. "Suppose $A \subseteq B$" opens the →I box 1–17; its closing line 18 is the silent frame of the whole proof. "Let $S \in \mathcal{P}(A)$" opens two boxes at once: the ∀I box for S_0 and the →I box 3–14 inside it. "Let $x \in S$" likewise opens the ∀I box for x_0 and the →I box 6–10. "Hence $S \subseteq B$" closes the two inner boxes (lines 11 and 12) and rewinds the definition (line 13). "This proves $\mathcal{P}(A) \subseteq \mathcal{P}(B)$" closes the S boxes (lines 15, 16) and rewinds (line 17).

This is the passage from level 0 to level 3 of *Logic and Proof*, Section 8.3: each "let" carries a ∀I box together with the →I box of a subset statement, the ∀E and →E lines 7–10 become the two "since" clauses, the unwinding lines 2 and 5 go silent, line 4 becomes a "so" and line 14 a "that is", and the rewinding lines 13 and 17 are the two conclusions the prose states.

Exercise. R2

Decide whether $A \setminus (B \setminus C) = (A \setminus B) \setminus C$ for all sets A, B, C, by a table of the eight possible

memberships of a point x in A, B, C. If the two sides can differ, turn a row where they differ into a counterexample.

Solution. Write P, Q, R for the statements $x \in A$, $x \in B$, $x \in C$. By Definition 1.3.1, $x \in A \setminus (B \setminus C)$ is $P \wedge \neg(Q \wedge \neg R)$, and $x \in (A \setminus B) \setminus C$ is $(P \wedge \neg Q) \wedge \neg R$. The table:

P	Q	R	$P \wedge \neg(Q \wedge \neg R)$	$(P \wedge \neg Q) \wedge \neg R$
T	T	T	T	F
T	T	F	F	F
T	F	T	T	F
T	F	F	T	T
F	T	T	F	F
F	T	F	F	F
F	F	T	F	F
F	F	F	F	F

The columns differ in the first and third rows. Take the first row: put the point 1 in exactly the sets whose statement is true, all three, so $A = B = C = \{1\}$. Then $B \setminus C = \emptyset$, so $A \setminus (B \setminus C) = \{1\}$; and $A \setminus B = \emptyset$, so $(A \setminus B) \setminus C = \emptyset$. The two sides differ, so the identity is false. (The third row gives $A = C = \{1\}$, $B = \emptyset$, with the same two answers.)

Why a table suffices: each side's membership condition is a formula in P, Q, R, and a row with the two columns different gives sets directly, which are then checked by computing both sides, as above. The truth tables of *Logic and Proof*, Chapter 4 add one more thing: by Logic and Proof, Corollary 4.7.3, the first row shows that the sequent $P \wedge \neg(Q \wedge \neg R) \vdash (P \wedge \neg Q) \wedge \neg R$ is not derivable, so the propositional rules cannot carry a point of the left side into the right side.

Exercise. R3

Derive $(P \wedge \neg Q) \to R \vdash P \to (Q \vee R)$. Then read the derivation as a proof that for sets A, B, C, if $A \setminus B \subseteq C$, then $A \subseteq B \cup C$. Which step is classical?

Solution. The goal is an implication, so open a box on P with goal $Q \vee R$. The premise can fire only on $P \wedge \neg Q$, which needs $\neg Q$, and nothing gives $\neg Q$ outright. So split on $Q \vee \neg Q$, by excluded middle (Logic and Proof, Proposition 2.5.3): in the case Q the goal is immediate, and in the case $\neg Q$ the premise gives R.

1	$(P \wedge \neg Q) \to R$	
2	$\quad P$	
3	$\quad Q \vee \neg Q$	LEM
4	$\quad\quad Q$	
5	$\quad\quad Q \vee R$	$\vee$I 4
6	$\quad\quad \neg Q$	
7	$\quad\quad P \wedge \neg Q$	$\wedge$I 2, 6
8	$\quad\quad R$	$\to$E 1, 7
9	$\quad\quad Q \vee R$	$\vee$I 8
10	$\quad Q \vee R$	$\vee$E 3, 4–5, 6–9
11	$P \to (Q \vee R)$	$\to$I 2–10

As sets. Suppose $A \setminus B \subseteq C$, and let $x \in A$. Take P, Q, R to be $x \in A$, $x \in B$, $x \in C$. By Definition 1.2.2 and Definition 1.3.1, the hypothesis at this x is $(P \wedge \neg Q) \to R$, and the goal $x \in B \cup C$ is $Q \vee R$. The derivation, used as a derived rule (Logic and Proof, Definition 2.3.1), gives $P \to (Q \vee R)$, and with P it gives $x \in B \cup C$. In prose: either $x \in B$, and then $x \in B \cup C$; or $x \notin B$, and then $x \in A \setminus B \subseteq C$, so $x \in C \subseteq B \cup C$. Since x was arbitrary, $A \subseteq B \cup C$.

The classical step is line 3, the case split "$x \in B$ or $x \notin B$" by excluded middle, which is derived with RAA (Logic and Proof, Definition 2.5.1).

Exercise. R4

Show that there is no set that contains every singleton $\{x\}$ as an element.

Solution. Suppose S were such a set. Let $T \coloneqq \{s \in S : s \text{ is a singleton}\}$, a set by specification (Definition 1.2.3); its elements are sets, since S may also contain numbers, and those are excluded. Consider the union $\bigcup T$ of the sets in T (Definition 1.3.4, the form $\bigcup \mathcal{S}$ for a set $\mathcal{S}$ whose elements are sets). For every set x, the singleton $\{x\}$ lies in S, hence in T, and $x \in \{x\}$; so $x \in \bigcup T$. Thus $\bigcup T$ is a set of which every set is an element, and Theorem 1.2.4 says there is no such set. This contradiction shows that no such S exists.

The tool, and the look-alike. The tool is Russell's theorem, Theorem 1.2.4, applied not to S but to $\bigcup T$. Applied to S directly, it says only that $\{z \in S : z \notin z\} \notin S$, and that does not contradict anything: S was supposed to contain singletons, not that set. The move that makes it work is the union, which turns "contains the singleton of every set" into "contains every set". A direct diagonal construction inside S also works, but it repeats the proof of Theorem 1.2.4 instead of using it.

Chapter 2

Induction, Contradiction, and Finite Sets

Logic and Proof, Chapter 4 took one fact about the natural numbers on trust: induction. Everything else we have used about them came from school: that $7 - 3$ is a natural number, that none lies strictly between 3 and 4, and that every non-empty set of them has a least member. This chapter derives all of these from induction, extends them to the integers, and proves that the least-member property, **well-ordering**, is induction in another form. It then turns induction from a principle into a craft: which form fits a claim, where to start, when to argue by contrapositive, by contradiction or from a smallest counterexample, when to prove more than was asked, and how a flawed induction fails at exactly one step. It also proves that a starting value and a rule for the next value really do define a sequence, which is what makes $\sum$, $\prod$, $n!$ and powers definitions rather than abbreviations. The first motivating problem comes from *Logic and Proof*, Chapter 2, which reduced a fraction by halving numerator and denominator for as long as both were even: *what stops the halving from going on for ever?* It proves that there are infinitely many primes, and that $\sqrt[3]{2}$ is irrational.

The second half of the chapter is about size. Section 1.1 left a puzzle waiting for a principle: five objects in four boxes put two in one box. *What does "finite" mean, so that this can be proved?* The answer is a pairing: two sets have the same size when a bijection joins them, a set is finite when it pairs with $\{1, \ldots, n\}$, and the pigeonhole principle becomes a theorem, with the facts about counting that the earlier chapters took on trust. The proofs of these facts are where proof by contradiction works at full scale.

What you need. *Logic and Proof*, Chapters 1–8, and *Sets and Functions*, Chapter 1. From *Logic and Proof*, Chapters 1 and 2: the $\to$I box (Logic and Proof, Definition 1.4.1), proof by contradiction (Logic and Proof, Definition 2.5.1), De Morgan's laws (Logic and Proof, Proposition 2.5.5), the contrapositive and the converse (Logic and Proof, Proposition 2.5.2), odd squares (Logic and Proof, Theorem 2.4.4), the irrationality of $\sqrt{2}$ (Logic and Proof, Theorem 2.2.1), whose fact (L) this chapter proves, and Logic and Proof, Theorem 2.1.3, whose parity fact Section 1.1 proved and Section 2.2 derives again. From *Logic and Proof*, Chapter 4: the principle of induction (Logic and Proof, Axiom 4.2.1) and strong induction (Logic and Proof, Theorem 4.2.2), with the worked examples that introduced them (Logic and Proof, Example (A sum of products of neighbors), Logic and Proof, Example (An inequality by induction), Logic and Proof, Example (Threes and fives)), the cure of proving more (Logic and Proof, Example (Prove more to prove less)), and structural recursion and induction (Logic and Proof, Theorem 4.3.4, Logic and Proof, Theorem 4.3.1), which appear here as pointers back and in one review exercise, with truth values (Logic and Proof, Definition 4.4.2) and the set

$\{\wedge, \vee, \to\}$ that cannot express negation (Logic and Proof, Theorem 4.9.6). From *Logic and Proof*, Chapters 5 and 6: the rules for "for every" and "there exists" (Logic and Proof, Definition 5.4.1, Logic and Proof, Definition 5.6.1, Logic and Proof, Proposition 5.6.2), the rules for equality (Logic and Proof, Definition 5.7.1, Logic and Proof, Proposition 5.7.1), bounded quantifiers (Logic and Proof, Proposition 6.1.1), and negating quantifiers and implications (Logic and Proof, Proposition 6.2.3, Logic and Proof, Proposition 6.2.2). From *Logic and Proof*, Chapter 7: the counter-model exercises (Logic and Proof, Exercise (C1: True in every finite model, used later), Logic and Proof, Exercise (C2: A sentence with no finite model, used later)). From *Logic and Proof*, Chapter 8: how an induction is written in prose (Logic and Proof, Example (An induction, and a legitimate symmetry)), the three faces of "by contradiction" (Section 8.1; Logic and Proof, Example (One proof by contradiction, read two ways), the costume examples Logic and Proof, Example (A direct proof in costume) and Logic and Proof, Example (A contrapositive in costume), Euclid's list argument Logic and Proof, Exercise (C1: Euclid without the contradiction)), existence without a witness (Section 8.7, Logic and Proof, Theorem 8.7.1), and the catalogue of what a proof may not do (Logic and Proof, Example (What is not allowed)). From Chapter 1: the method boxes for direct proof, cases, counterexamples, double inclusion, injectivity and surjectivity (Example (Method: direct proof from a definition), Example (Method: proof by cases), Example (Method: disproof by counterexample, proof by example), Example (Method: two inclusions), Example (Method: proving injectivity), Example (Method: proving surjectivity)); even, odd, divides and prime (Definition 1.1.1, Definition 1.1.2, Definition 1.1.3, Theorem 1.1.2, Example (The parity of a sum), Proposition 1.1.1, Example (Divisors of a combination), Example (Same pattern, lattice midpoint)); Russell's paradox (Theorem 1.2.4) and equality of sets by two inclusions (Proposition 1.2.1); sets cut out by a property (Definition 1.2.3), power sets (Definition 1.3.2), unions of families (Definition 1.3.4); ordered pairs and products (Definition 1.4.1, Definition 1.4.2); relations and functions, equality of functions, the empty function (Definition 1.4.3, Definition 1.5.1, Proposition 1.5.1, Proposition 1.5.2); injections, surjections, composites and inverses (Definition 1.5.3, Definition 1.5.4, Example (Deciding injective and surjective), Definition 1.5.2, Definition 1.6.2, Theorem 1.5.4, Theorem 1.6.4, Theorem 1.6.1); images and preimages (Definition 1.7.1, Definition 1.7.2). The arithmetic and order of $\mathbb{R}$ are school facts, as in the earlier chapters; *Analysis on the Real Line*, Chapter 1 states them as axioms.

Time. About 30 hours on the core track (all of A, one B and one C per section, the exit checks); about 40 hours for everything.

2.0.1 Roadmap

- **The natural numbers and well-ordering.** From induction alone, the arithmetic of $\mathbb{N}$ and $\mathbb{Z}$, the proof that every non-empty set of natural numbers has a least element, and the theorem that induction and well-ordering are equivalent, with a witness for each hypothesis it needs, and the least element as a tool of proof.
- **Induction, strong induction and divisibility.** Induction from any integer, finding the inductive hypothesis inside the step and choosing the base, the division algorithm, lowest terms and prime factors, and a gallery of broken inductions, each located at one step.
- **Definition by recursion.** The theorem that a starting value and a rule define exactly one sequence, its variants from another base and with two previous values, sums, products and powers defined by it, and inductions that follow a definition's clauses or prove more than was asked.
- **Contrapositive and contradiction in practice.** Choosing among a direct proof, the contrapositive and a contradiction; infinitely many primes; an irrational cube root by lowest terms; the smallest counterexample as a method; existence without a witness.
- **Equinumerous sets and finite sets.** "The same size" defined by a bijection, finite sets

and their number of elements, the pigeonhole principle, which settles the five lattice points of Section 1.1, and the uniqueness of that number, subsets, disjoint unions and the 2^n subsets of an n-element set, and the theorem that no finite set is equinumerous with a proper subset, which Hilbert's hotel turns into a proof that $\mathbb{N}$ is infinite.

2.0.2 Named moves

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

- **The least element** (Example (Method: the least element)). Name a set whose least element would help, show it is a non-empty set of natural numbers, take its least element, and use leastness: an element below it is a contradiction, or leastness says what it must be. (Section 2.1)
- **Finding $P(n)$ inside $P(n+1)$** (Example (Method: finding $P(n)$ inside $P(n+1)$)). Write $P(n+1)$ out, split off the part that is $P(n)$, apply the induction hypothesis to it, close the rest by computation, and choose the base as the first n from which this works. (Section 2.2)
- **Choosing direct, contrapositive or contradiction** (Example (Method: choosing direct, contrapositive or contradiction)). Unwind P, Q and their negations: go direct when P gives something to compute with, prove the contrapositive when $\neg Q$ is the richer hypothesis, and assume the positive statement when the claim is a negation. (Section 2.4)
- **Smallest counterexample** (Example (Method: the smallest counterexample)). Suppose the claim fails; well-ordering gives a least failure m; below m the claim holds, and from that produce a failure smaller than m, or the claim at m itself. (Section 2.4)
- **Pigeonhole** (Example (Method: the pigeonhole principle)). Choose pigeons and fewer holes, define "the hole of a pigeon", conclude that two pigeons share a hole, and translate "same hole" back into the property you want. (Section 2.5)
- **Prove more (strengthen the hypothesis).** When the inductive step will not go through, ask what the induction hypothesis would need to say, and prove that stronger statement instead.
- **Recursion, then induction.** Define an object by a recursion, and prove facts about it by an induction that follows the same clauses: the base case uses the starting value, and the step uses the rule.

2.0.3 Threads

- **The halving.** Section 2.1 opens its subsection on well-ordering with the halving question of *Logic and Proof*, Chapter 2, and answers it with the first use of the least element (Example (No endless descent in the natural numbers)). Section 2.2 writes the argument out as the existence of lowest terms (Lemma 2.2.4), and Section 2.4 uses lowest terms to prove that $\sqrt[3]{2}$ is irrational (Proposition 2.4.2).
- **The lattice points.** Section 1.1 asks why, among any five points with integer coordinates, two have a midpoint with integer coordinates, and leaves the principle it needs unproved. Section 2.5 opens on the puzzle, proves the pigeonhole principle (Theorem 2.5.2) under the heading "Back to the pigeons", and finishes the five points (Example (Back to the five lattice points)).
- **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 (Definition 2.5.1), and Section 4.2 meets it again as an example of an equivalence-like relation.
- **Infinitely many primes.** Section 2.4 proves that above every natural number there is a prime (Theorem 2.4.1), before "infinite" has a definition; Section 2.5 defines infinite sets, and a Quick check there concludes that the set of primes is one.

2.0.4 Summary

Induction and well-ordering are one principle (Theorem 2.1.4). Every integer can be divided by a positive integer with a unique quotient and remainder (Theorem 2.2.3). Every integer at least 2 has a prime factor (Theorem 2.2.5), and there are infinitely many primes (Theorem 2.4.1). A starting value and a rule define exactly one sequence (Theorem 2.3.1), which makes sums, products and powers definitions. The number $\sqrt[3]{2}$ is irrational (Proposition 2.4.2), by lowest terms and a smallest counterexample. For $m > n$ there is no injection from $\{1, \ldots, m\}$ to $\{1, \ldots, n\}$ (Theorem 2.5.2), so a finite set has exactly one number of elements (Corollary 2.5.4), and no finite set is equinumerous with a proper subset of itself (Theorem 2.5.9).

What is open: are $\mathbb{Q}$ and $\mathbb{R}$ the same size as $\mathbb{N}$? Chapter 3.

2.0.5 Terms

- **equinumerous**: there is a bijection between the two sets (Definition 2.5.1).
- **factorial**: $n! = \prod_{k=1}^{n} k$, with $0! = 1$ (Definition 2.3.1).
- **finite, has n elements**: equinumerous with $\{1, \ldots, n\}$ for some $n \in \mathbb{N}$ (Definition 2.5.2).
- **greatest element**: an element $m \in S$ with $s \leq m$ for every $s \in S$ (Section 2.1, before Theorem 2.1.3).
- **infinite**: not finite (Definition 2.5.3).
- **least element**: an element $m \in S$ with $m \leq s$ for every $s \in S$ (Section 2.1, before Theorem 2.1.3).
- **maximum, minimum**: the greatest and the least element of a set (Section 2.3, before Proposition 2.3.8).
- **power**: $u^0 = 1$, $u^{n+1} = u^n u$ (Definition 2.3.2).
- **prime factor**: a prime that divides the integer (Definition 1.1.3, Section 1.1); every integer ≥ 2 has one (Theorem 2.2.5).
- **quotient, remainder**: the q and r of $a = qn + r$, $0 \leq r < n$ (Theorem 2.2.3).
- **smallest counterexample**: the least integer at which a claim fails, given by well-ordering (Example (Method: the smallest counterexample)).
- **sum, product**: $\sum_{k=m}^{n} a_k$ and $\prod_{k=m}^{n} a_k$, defined by recursion, empty sum 0, empty product 1 (Definition 2.3.1).

2.1 The Natural Numbers and Well-Ordering

Logic and Proof, Chapter 4 took one fact about the natural numbers on trust: the principle of induction (Logic and Proof, Axiom 4.2.1), which says that a property holding at 0 and passing from each n to $n + 1$ holds for every $n \in \mathbb{N}$. From it, *Logic and Proof*, Chapter 4 proved strong induction (Logic and Proof, Theorem 4.2.2), whose step may use the property at **every** smaller number. Everything else we have said about $\mathbb{N}$ was school knowledge: that $7 - 3$ is a natural number, that none lies strictly between 3 and 4, that every non-empty set of natural numbers has a least member. This section derives those facts from induction, extends them to the integers, and then proves that the least-member property, **well-ordering**, is induction in another form.

2.1.1 What we assume about the natural numbers

The principle of induction is usually used with a property written as a sentence. It has an equivalent form about sets, which is the one *Analysis on the Real Line*, Chapter 1 uses.

Remark. Let $S \subseteq \mathbb{N}$ contain 0, and suppose $n+1 \in S$ whenever $n \in S$. Apply Logic and Proof, Axiom 4.2.1 to the property "$n \in S$": its base case is $0 \in S$, and its step is the closure of S. So every $n \in \mathbb{N}$ lies in S, that is, $\mathbb{N} \subseteq S$, and with $S \subseteq \mathbb{N}$ this gives $S = \mathbb{N}$ (Proposition 1.2.1). In words: the only subset of $\mathbb{N}$ that contains 0 and is closed under $n \mapsto n+1$ is $\mathbb{N}$ itself. *Analysis on the Real Line*, Chapter 1 states this as "$\mathbb{N}$ is contained in every inductive set", where an inductive set contains 0, as here.

Here is everything the section assumes about $\mathbb{N}$. The natural numbers form a subset $\mathbb{N} \subseteq \mathbb{R}$ of the familiar real numbers such that

- (($\mathbb{N}$)0) $0 \in \mathbb{N}$;
- ($\mathbb{N}$S) for every $n \in \mathbb{N}$, also $n+1 \in \mathbb{N}$;

and Logic and Proof, Axiom 4.2.1 holds. The arithmetic and the order of the real numbers (the laws of $+$, $-$, $\cdot$ and $\leq$, trichotomy, multiplying an inequality by a positive number) are school facts in this volume and in *Logic and Proof*; *Analysis on the Real Line*, Chapter 1 states them as axioms of an ordered field. These three items are a description of $\mathbb{N}$, not new axioms: *Logic and Proof*, Chapter 4 already used all of them.

The rule for this section. From here to the end of the section, a fact about $\mathbb{N}$ is used only if it is (($\mathbb{N}$)0), ($\mathbb{N}$S), Logic and Proof, Axiom 4.2.1, a statement proved earlier in the section, or Logic and Proof, Theorem 4.2.2 once the paragraph after Lemma 2.1.1 has shown that its *Logic and Proof*, Chapter 4 proof rests only on these. The real-number arithmetic is used freely. In particular "$n \geq 0$" for a natural number n, which looks too obvious to mention, is not available until it is proved below, in Lemma 2.1.1 (a).

The integers and the rationals are then **defined** from $\mathbb{N}$, as subsets of $\mathbb{R}$:

$$\begin{aligned} \mathbb{Z} &\coloneqq \mathbb{N} \cup \{-n : n \in \mathbb{N}\}, \\ \mathbb{Z}_{>0} &\coloneqq \{n \in \mathbb{N} : n \neq 0\}, \\ \mathbb{Q} &\coloneqq \{m/n : m \in \mathbb{Z},\ n \in \mathbb{Z}_{>0}\}. \end{aligned}$$

In words: an integer is a natural number or the negative of one; a positive integer is a natural number other than 0; a rational number is a quotient of an integer by a positive integer. These are word for word the definitions of *Analysis on the Real Line*, Section 1.5, so the two chapters speak of the same sets. Examples: $-3 \in \mathbb{Z}$ because $3 \in \mathbb{N}$; 0 lies in $\mathbb{Z}$ twice over, as $0 \in \mathbb{N}$ and as -0, which a union does not mind; $-\frac{1}{2} = (-1)/2 \in \mathbb{Q}$. The definitions do not yet tell us that $\frac{1}{2} \notin \mathbb{Z}$, or that $\mathbb{Z}_{>0}$ is the set of natural numbers ≥ 1. Both need the lemma below.

Two pieces of notation will save words later. For $n \in \mathbb{N}$,

$$\{1, \ldots, n\} \coloneqq \{k \in \mathbb{N} : 1 \leq k \leq n\}, \qquad \{0, \ldots, n\} \coloneqq \{k \in \mathbb{N} : k \leq n\}.$$

So $\{1, \ldots, 0\} = \emptyset$, since no k has $1 \leq k \leq 0$. We do not write $[n]$ for these sets: square brackets will mean an equivalence class in Section 4.2.

2.1.2 The arithmetic of the natural numbers

The facts below are the ones *Logic and Proof*, Chapter 4 and *Analysis on the Real Line*, Chapter 1 used without proof. Each of (a)–(d) is one ordinary induction, and the only work is to choose the property to induct on; (e) follows from (a) and (d).

Lemma 2.1.1. Arithmetic of the Natural Numbers

For all $m, n \in \mathbb{N}$:

(a) $n \geq 0$; and if $n \neq 0$, then $n \geq 1$;
(b) $m + n \in \mathbb{N}$ and $mn \in \mathbb{N}$;
(c) if $n \neq 0$ (equivalently, by (a), $n \geq 1$), then $n - 1 \in \mathbb{N}$;
(d) if $m \leq n$, then $n - m \in \mathbb{N}$;
(e) there is **no** $k \in \mathbb{N}$ with $n < k < n + 1$; equivalently, if $m < n$, then $m + 1 \leq n$.

In words: (a) says that 0 is the smallest natural number and that nothing in $\mathbb{N}$ lies between 0 and 1. (b) says $\mathbb{N}$ is closed under sums and products, (c) that every natural number except 0 has a predecessor in $\mathbb{N}$, and (d) that a difference "larger minus smaller" stays in $\mathbb{N}$. (e) says the natural numbers come one unit apart, with no gaps to hide in.

Idea. Each induction needs a property that is true at 0 and survives the step, and the statement as written does not always qualify. "If $n \neq 0$, then $n \geq 1$" says nothing useful at 0, so for (a) we induct on the disjunction "$n = 0$ or $n \geq 1$". For (b) we fix one of the two numbers and induct on the other. For (d) we induct on m. The step from m to $m + 1$ uses the hypothesis only at the same n, with the weaker bound $m \leq n$, and then subtracts 1 using (c). So n could be fixed first, as m is in (b); the proof below puts "for every n" inside the property instead, which is harmless.

Proof. (a) Let $P(n)$ be "$n = 0$ or $n \geq 1$". *Base case:* $P(0)$ holds by its first disjunct. *Step:* let $n \in \mathbb{N}$ with $P(n)$. If $n = 0$, then $n + 1 = 1 \geq 1$; if $n \geq 1$, then $n + 1 \geq 2 \geq 1$. In both cases $n + 1 \geq 1$, so $P(n + 1)$ holds by its second disjunct. By Logic and Proof, Axiom 4.2.1, every $n \in \mathbb{N}$ satisfies $n = 0$ or $n \geq 1$. In both cases $n \geq 0$; and if $n \neq 0$, the first disjunct is excluded, so $n \geq 1$.

(b) Fix $m \in \mathbb{N}$. *Sums:* let $P(n)$ be "$m + n \in \mathbb{N}$". Then $P(0)$ holds, since $m + 0 = m \in \mathbb{N}$. If $m + n \in \mathbb{N}$, then $m + (n + 1) = (m + n) + 1 \in \mathbb{N}$ by ($\mathbb{N}$S). By Logic and Proof, Axiom 4.2.1, $m + n \in \mathbb{N}$ for every $n \in \mathbb{N}$; as m was arbitrary, this holds for all $m, n \in \mathbb{N}$. *Products:* let $Q(n)$ be "$mn \in \mathbb{N}$". Then $m \cdot 0 = 0 \in \mathbb{N}$ by (($\mathbb{N}$)0). If $mn \in \mathbb{N}$, then $m(n + 1) = mn + m$, a sum of the two natural numbers mn and m, so it lies in $\mathbb{N}$ by the half just proved. By Logic and Proof, Axiom 4.2.1, $mn \in \mathbb{N}$ for every n.

(c) Let $P(n)$ be "$n = 0$ or $n - 1 \in \mathbb{N}$". $P(0)$ holds by its first disjunct. Let $n \in \mathbb{N}$; then $(n+1)-1 = n \in \mathbb{N}$, so $P(n+1)$ holds by its second disjunct. By Logic and Proof, Axiom 4.2.1, $P(n)$ holds for every $n \in \mathbb{N}$, and for $n \neq 0$ its second disjunct is the claim.

(d) Let $P(m)$ be "for every $n \in \mathbb{N}$, if $m \leq n$, then $n - m \in \mathbb{N}$". *Base case:* $n - 0 = n \in \mathbb{N}$. *Step:* let $m \in \mathbb{N}$ with $P(m)$, and let $n \in \mathbb{N}$ with $m + 1 \leq n$. Then $m < m + 1 \leq n$, so $n - m \in \mathbb{N}$ by $P(m)$. Moreover $n - m \geq 1 > 0$, so $n - m \neq 0$, and (c) gives $(n - m) - 1 \in \mathbb{N}$. Since $(n - m) - 1 = n - (m + 1)$, this is $P(m + 1)$. By Logic and Proof, Axiom 4.2.1, $P(m)$ holds for every $m \in \mathbb{N}$.

(e) Let $m < n$. By (d), $n - m \in \mathbb{N}$, and $n - m > 0$, so $n - m \neq 0$ and (a) gives $n - m \geq 1$, that is, $m + 1 \leq n$. Now suppose $k \in \mathbb{N}$ with $n < k < n + 1$. Applying what we just proved to $n < k$ gives $n + 1 \leq k$, which contradicts $k < n + 1$. So no such k exists. This proves the lemma.

■

Read the proof of (c) again. Its inductive step never mentions $P(n)$.

Example. An induction that ignores its hypothesis

Logic and Proof, Chapter 4, after its first worked induction (Logic and Proof, Example (A sum of products of neighbors)), said: "A proof by induction that never uses its induction hypothesis is either not an induction or is hiding a gap." The proof of Lemma 2.1.1 (c) never uses its induction hypothesis. Is it an induction, and is it hiding a gap?

Solution. It is an induction, and it hides no gap. Its base case $P(0)$ is proved, and its step "$P(n) \Rightarrow P(n+1)$" is a valid implication for every $n \in \mathbb{N}$: the conclusion $P(n+1)$ is proved outright, so the implication holds whatever $P(n)$ says. Then Logic and Proof, Axiom 4.2.1 delivers $P(n)$ for every n. The hypothesis $n \in \mathbb{N}$ of the step is used, through $(n+1)-1 = n \in \mathbb{N}$; only $P(n)$ is not.

Nor can a case analysis replace the axiom here. A direct proof would have to say which numbers lie in $\mathbb{N}$, and the only thing that says so is induction: the step shows that every number of the form $n+1$ with $n \in \mathbb{N}$ has the property, and it is Logic and Proof, Axiom 4.2.1 that tells us every natural number other than 0 is of this form. *Logic and Proof*, Chapter 4's sentence is a rule of thumb, and a good one: an unused hypothesis is a reason to check the proof line by line. Here the check passes. The exception is a step whose conclusion is reached without the hypothesis, and the axiom is still what carries the property from 0 to every n.

The lemma also closes a gap in *Logic and Proof*, Chapter 4. The proof of Logic and Proof, Theorem 4.2.2 used two facts about $\mathbb{N}$ as school knowledge. In its base case it said "No natural number is less than 0, so $P(k)$ holds for every $k \in \mathbb{N}$ with $k < 0$, vacuously" and "The only $k \in \mathbb{N}$ with $k \leq 0$ is 0": both are (a), the second with trichotomy. In its inductive step it said "The natural numbers $k < n+1$ are exactly those with $k \leq n$, since no natural number lies strictly between n and $n+1$", and then "A natural number $k \leq n+1$ satisfies $k \leq n$ or $k = n+1$": both are (e), with trichotomy. The proofs of (a), (d) and (e) above use only Logic and Proof, Axiom 4.2.1, (($\mathbb{N}$)0), ($\mathbb{N}$S), part (c) and the arithmetic of $\mathbb{R}$, and none of them uses strong induction. So strong induction rests on those items alone, and from now on we may cite Logic and Proof, Theorem 4.2.2 with no school fact behind it.

Quick check. Where in the proof of Lemma 2.1.1 (d) is part (c) used, and could n have been fixed before the induction on m, as m was in (b)?

Solution. Part (c) is used to pass from $n - m \in \mathbb{N}$ to $n - (m+1) = (n-m) - 1 \in \mathbb{N}$, after checking $n - m \neq 0$. The step from m to $m+1$ is about one n with $m+1 \leq n$, and it uses $P(m)$ at that same n, with the weaker bound $m \leq n$. So yes: fixing $n \in \mathbb{N}$ and inducting on "if $m \leq n$, then $n - m \in \mathbb{N}$" proves the same thing, and then n was arbitrary. Putting "for every n" inside $P(m)$ is harmless but not needed. It would be needed only if the step used the hypothesis at a different n, such as $n - 1$.

2.1.3 The integers

Analysis on the Real Line, Chapter 1 uses that sums, differences and products of integers are integers, and that an integer greater than 3 is at least 4. Both now follow from the lemma, by sorting integers into natural numbers and their negatives.

Proposition 2.1.2. Arithmetic of the Integers

Let $m, n \in \mathbb{Z}$.

(a) $m+n$, $m-n$ and mn are integers.

(b) If $n \geq 0$, then $n \in \mathbb{N}$; if $n > 0$, then $n \in \mathbb{Z}_{>0}$. Hence

$$\mathbb{N} = \{n \in \mathbb{Z} : n \geq 0\}, \qquad \mathbb{Z}_{>0} = \{n \in \mathbb{Z} : n > 0\} = \{n \in \mathbb{N} : n \geq 1\}.$$

(c) (**Discreteness.**) If $m < n$, then $m + 1 \leq n$.

Idea. Every integer is a or $-a$ with $a \in \mathbb{N}$, so each claim splits into cases by signs. Only one case has content: $a + (-b) = a - b$ with $a, b \in \mathbb{N}$, which is in $\mathbb{N}$ when $b \leq a$, by Lemma 2.1.1 (d), and is the negative of a natural number when $a < b$. Discreteness then follows from (b) applied to the difference $n - m$: it is a positive integer, hence a natural number with $n - m \geq 1$, by (a) of the lemma.

Proof. *(a)* First, $\mathbb{Z}$ is closed under $x \mapsto -x$: if $x \in \mathbb{N}$, then $-x \in \mathbb{Z}$ by the definition of $\mathbb{Z}$; if $x = -k$ with $k \in \mathbb{N}$, then $-x = k \in \mathbb{N} \subseteq \mathbb{Z}$.

Next let $a, b \in \mathbb{N}$; we show $a - b \in \mathbb{Z}$. By trichotomy there are three cases. If $a > b$ or $a = b$, then $b \leq a$, and $a - b \in \mathbb{N}$ by Lemma 2.1.1 (d). If $a < b$, then $b - a \in \mathbb{N}$ by (d), and $a - b = -(b - a) \in \mathbb{Z}$.

Now write $m = \pm a$ and $n = \pm b$ with $a, b \in \mathbb{N}$. The table lists the four sign patterns; in each, $a+b$ and ab lie in $\mathbb{N}$ by Lemma 2.1.1 (b), and $a-b$, $b-a$ lie in $\mathbb{Z}$ by the previous paragraph.

m	n	$m+n$	mn
a	b	$a+b \in \mathbb{N}$	$ab \in \mathbb{N}$
a	$-b$	$a-b \in \mathbb{Z}$	$-(ab) \in \mathbb{Z}$
$-a$	b	$b-a \in \mathbb{Z}$	$-(ab) \in \mathbb{Z}$
$-a$	$-b$	$-(a+b) \in \mathbb{Z}$	$ab \in \mathbb{N}$

So $m+n$ and mn are integers. Finally $m-n = m+(-n)$, a sum of two integers, since $-n \in \mathbb{Z}$ by the first paragraph.

(b) Let $n \geq 0$. By the definition of $\mathbb{Z}$, either $n \in \mathbb{N}$, and we are done, or $n = -k$ with $k \in \mathbb{N}$. In the second case $k = -n \leq 0$, and $k \geq 0$ by Lemma 2.1.1 (a), so $k = 0$ and $n = 0 \in \mathbb{N}$ by (($\mathbb{N}$)0). If moreover $n > 0$, then n is a natural number with $n \neq 0$, so $n \in \mathbb{Z}_{>0}$.

For the set equalities: $\mathbb{N} \subseteq \mathbb{Z}$, and every $n \in \mathbb{N}$ has $n \geq 0$ by (a) of the lemma; with the first sentence of (b) this gives $\mathbb{N} = \{n \in \mathbb{Z} : n \geq 0\}$. Every element of $\mathbb{Z}_{>0}$ is a natural number $n \neq 0$, so $n \geq 1 > 0$ by (a) of the lemma; with the second sentence of (b) this gives $\mathbb{Z}_{>0} = \{n \in \mathbb{Z} : n > 0\}$. Finally, for $n \in \mathbb{N}$, $n \neq 0$ implies $n \geq 1$ by (a), and $n \geq 1$ implies $n \neq 0$; so $\mathbb{Z}_{>0} = \{n \in \mathbb{N} : n \geq 1\}$.

(c) Let $m < n$. By (a), $n-m \in \mathbb{Z}$, and $n-m > 0$, so $n-m \in \mathbb{Z}_{>0}$ by (b), that is, $n-m \geq 1$. Hence $m+1 \leq n$. This proves the proposition.

■

Discreteness is the fact behind "an integer greater than 3 is at least 4" (take $m = 3$), and behind "the integers x with $-2 \leq x \leq 2$ are $-2, -1, 0, 1, 2$": an integer x with $-2 \leq x$ is -2 or at least -1, and so on up to 2. It also settles the question left open above: $\frac{1}{2} \notin \mathbb{Z}$, since $0 < \frac{1}{2}$ would force $1 \leq \frac{1}{2}$.

2.1.4 Well-ordering

A fraction with even numerator and denominator can be halved, and halved again, and *Logic and Proof*, Chapter 2 claimed that this cannot go on for ever (the fact (L) in the proof of Logic and Proof, Theorem 2.2.1). The reason is that the absolute values of the denominators form a strictly decreasing list of positive integers, and such a list must stop. The precise form of "must stop" is a statement about least elements.

A **least element** of a set $S \subseteq \mathbb{R}$ is an element $m \in S$ such that $m \leq s$ for **every** $s \in S$. Not every set has one: $(0, 1]$ has none, since for every $x \in (0, 1]$ the number $x/2$ lies in the set and is smaller. The empty set has none either, as a least element must be an element. Reversing the inequality, a **greatest element** of S is an element $m \in S$ with $s \leq m$ for every $s \in S$; this is the maximum of *Logic and Proof*, Section 5.8.

Every non-empty set of natural numbers has a least element.

Theorem 2.1.3. Well-Ordering of the Natural Numbers

Every **non-empty** subset of $\mathbb{N}$ has a least element.

Try it first (ten minutes): suppose that $S \subseteq \mathbb{N}$ has no least element. Which property of n would you prove for every $n \in \mathbb{N}$ by strong induction, and why does it finish the proof?

Idea. A least element cannot be found by inspecting S, since we know nothing about S. So we suppose there is none and show S is empty, which contradicts "non-empty". The property to carry is "$n \notin S$". If no number below n is in S and n were in S, then n would be a least element; so n is not in S. The hypothesis must speak about **every** number below n, which is

why the induction is strong. *Before reading on: at which line is trichotomy used, and what would go wrong without it?*

Proof. Let $S \subseteq \mathbb{N}$ be non-empty, and suppose, for a contradiction, that S has no least element. For $n \in \mathbb{N}$, let $P(n)$ be "$n \notin S$".

Let $n \in \mathbb{N}$, and suppose $P(k)$ holds for every $k \in \mathbb{N}$ with $k < n$, that is, no natural number less than n lies in S. Suppose $n \in S$. Let $s \in S$. By trichotomy, $s < n$, $s = n$ or $s > n$. The first is impossible: s is a natural number less than n, so $s \notin S$ by the hypothesis. So $s \geq n$. As $s \in S$ was arbitrary, n is a least element of S, which contradicts our supposition. Hence $n \notin S$, that is, $P(n)$ holds.

By Logic and Proof, Theorem 4.2.2, $n \notin S$ for every $n \in \mathbb{N}$. Since $S \subseteq \mathbb{N}$, the set S has no elements, which contradicts S being non-empty. So S has a least element. This proves the theorem.

■

The outer frame is an RAA on the statement "S has a least element". The proof shows that a least element **exists**; it does not say how to find it. *Logic and Proof*, Section 8.7 explained why mathematicians have argued over proofs of this kind. Here the debate has a quiet ending: if S is given by a property that can be checked number by number, testing $0, 1, 2, \ldots$ in turn finds the least element, and the theorem says the search stops. Nothing in the proof above depends on such a test.

Quick check. In the proof of Theorem 2.1.3, to which property is strong induction applied, and what is the induction hypothesis at n?

Solution. To $P(n)$: "$n \notin S$". At n, the induction hypothesis is that $k \notin S$ for every natural number $k < n$: no element of S lies below n. Together with "$n \in S$" it would make n a least element, which is why $n \in S$ leads to a contradiction.

Warning. Well-ordering is a property of subsets of $\mathbb{N}$, not of every set of numbers. The set of positive rationals is non-empty and has no least element: for every positive rational q, the number $q/2$ is a smaller positive rational. Neither has $\mathbb{Z}$: $n - 1 < n$ is again an integer. A proof that takes "the least element" of a set must first show that the set is a non-empty subset of $\mathbb{N}$, or a non-empty set of integers with an integer lower bound, as in Corollary 2.1.5 below.

Quick check. Does $\{n \in \mathbb{N} : n^2 > 50\}$ have a least element? If so, which?

Solution. Yes. The set is non-empty, since $10^2 = 100 > 50$, and it is a subset of $\mathbb{N}$, so Theorem 2.1.3 applies. The least element is 8: $8^2 = 64 > 50$, while $7^2 = 49 \leq 50$, and for

$n \leq 7$ we have $n^2 \leq 49$. The theorem promised a least element; finding it took a search from below.

2.1.5 The least element as a tool

Well-ordering is used in two ways. The proof of Theorem 2.1.4 below uses it to compare principles; most proofs use it as a tool. They name a set of natural numbers, take its least element, and use the one thing a least element offers: nothing in the set lies below it. Here is the halving question that opened the subsection on well-ordering, answered that way.

Example. No endless descent in the natural numbers

Show that there is no function $f\colon \mathbb{N} \to \mathbb{N}$ with $f(n+1) < f(n)$ for every $n \in \mathbb{N}$.

Idea (Scratch work). The goal is a negation, so we suppose that such an f exists and aim for a contradiction (¬I). A direct attempt stalls at once: f is arbitrary, and there is nothing to compute. Well-ordering needs a set of natural numbers, and the question is which set has a least element worth having. The domain does not help: its least element is 0, which says nothing about f. The values do: in $V \coloneqq f(\mathbb{N}) = \{f(n) : n \in \mathbb{N}\}$, a least value would be undercut by the value after it.

Givens	Goal
$f\colon \mathbb{N} \to \mathbb{N}$, $f(n+1) < f(n)$ for every n	a contradiction
$V \coloneqq f(\mathbb{N}) \subseteq \mathbb{N}$, and $f(0) \in V$	a least element of V, and an element of V below it
$f(m)$ least in V (Theorem 2.1.3)	$f(m+1) \in V$ and $f(m+1) < f(m)$: the gap is closed

The hypothesis on f is used once, at the one place where it bites: just after the least value.

Solution. Suppose f is such a function, and let $V \coloneqq f(\mathbb{N})$ (Definition 1.7.1). Then $V \subseteq \mathbb{N}$, and $V \neq \emptyset$ since $f(0) \in V$. By Theorem 2.1.3, V has a least element, say $f(m)$ with $m \in \mathbb{N}$. Now $m+1 \in \mathbb{N}$ by (ℕS), so $f(m+1) \in V$, and $f(m+1) < f(m)$ by hypothesis, contradicting the choice of $f(m)$. So no such f exists.

Repeated halving of a fraction p/q with $q > 0$ and both entries even would give such a function, $n \mapsto$ the (positive) denominator after n halvings, if the halving never stopped: an even denominator $q > 0$ is $2k$ with $k \in \mathbb{Z}$ (Definition 1.1.1), so $k > 0$, $k \in \mathbb{Z}_{>0}$ by Proposition 2.1.2 (b), and $k < 2k = q$. So it stops. Section 2.2 writes this argument out as a proof, in its lemma on lowest terms.

The example follows a pattern that recurs throughout the book, and it is worth fixing as a method.

Example. Method: the least element

Template. (1) Name a set S whose least element would help: the failures, the values, the candidates. (2) Show that S is a non-empty subset of $\mathbb{N}$, by giving an element; or a non-empty set of integers with an integer lower bound. (3) Take its least element m (Theorem 2.1.3; for integers, Corollary 2.1.5 below). (4) Use leastness: produce an element of S below m, a contradiction; or conclude what m must be.

When to use it. A process that must stop; a quantity that can always be made smaller; the first time something happens; an object chosen to be extreme.

The usual failure. Taking "the least element" of a set not shown to be non-empty, or of a set of rationals, or of a set of integers with no integer lower bound (the warning above); and forgetting to check that the smaller element lies in S again.

Example. Going down by two

Let $S \subseteq \mathbb{N}$ be non-empty, and suppose $s - 2 \in S$ for every $s \in S$ with $s \geq 2$. Show that $0 \in S$ or $1 \in S$.

Idea. By the method of Example (Method: the least element), ending in the second form of its step (4): the least element of S itself must be 0 or 1.

Solution. Since S is a non-empty subset of $\mathbb{N}$, it has a least element m (Theorem 2.1.3). If $m \geq 2$, then $m - 2 \in S$ by hypothesis, and $m - 2 < m$, contradicting the choice of m. So $m < 2$, that is, $m \leq 1$ by Lemma 2.1.1 (e); and $m = 0$ or $m \geq 1$ by (a), so $m \in \{0, 1\}$. Hence $0 \in S$ or $1 \in S$.

The proof never asks whether $m-2$ is a natural number: the hypothesis puts it in S, and $S \subseteq \mathbb{N}$.

Quick check. Let $S := \{17 - 5k : k \in \mathbb{N},\ 5k \leq 17\}$. List S, find its least element, and say what that element has to do with dividing 17 by 5.

Solution. The admissible k are $0, 1, 2, 3$, since $5 \cdot 3 = 15 \leq 17 < 20 = 5 \cdot 4$ rules out $k \geq 4$, and the $k < 4$ are $0, 1, 2, 3$ (Lemma 2.1.1 (a), (e)). So $S = \{17, 12, 7, 2\}$, and its least element is 2, the remainder of 17 on division by 5: $17 = 5 \cdot 3 + 2$ with $0 \leq 2 < 5$. Section 2.2 proves that the least non-negative number of the form $a - qn$ is always the remainder.

2.1.6 Induction and well-ordering are the same principle

The proof of Theorem 2.1.3 derived well-ordering from induction. The derivation also runs the other way, and the cleanest way to say so is to ask which sets of numbers satisfy which principle. For a set $X \subseteq \mathbb{R}$, consider three structural properties:

- $0 \in X$;
- **closure:** for every $n \in X$, $n+1 \in X$;
- the **predecessor property:** for every $n \in X$ with $n \neq 0$, $n-1 \in X$.

The set $\mathbb{N}$ has all three, by (($\mathbb{N}$)0), ($\mathbb{N}$S) and Lemma 2.1.1 (c). Say that X has the **induction property** if every $S \subseteq X$ with $0 \in S$ and $n+1 \in S$ for every $n \in S$ equals X; and the **least-element property** if every non-empty subset of X has a least element. The closure of S in the induction property is plain closure under $n \mapsto n+1$, not "closure as long as one stays in X"; the witnesses below show why that matters.

Theorem 2.1.4. Induction Is Equivalent to Well-Ordering

Let $X \subseteq \mathbb{R}$ contain 0, be closed under $n \mapsto n+1$, and have the predecessor property. Then X has the induction property **if and only if** X has the least-element property.

Idea. ($\Rightarrow$) A set X with the induction property and the first two properties must be $\mathbb{N}$ itself: $\mathbb{N}$ sits inside X by Logic and Proof, Axiom 4.2.1, and the induction property of X, applied to the subset $\mathbb{N}$, forces equality. Then Theorem 2.1.3 applies. ($\Leftarrow$) Take S as in the induction property and suppose $S \neq X$; the least element m of $X \setminus S$ is then a smallest failure (the method of Example (Method: the least element), applied to the set $X \setminus S$ of failures, with the least-element property of X in place of Theorem 2.1.3); the number $m-1$ just below it is not a failure, so it lies in S, and closure passes that success up to $m = (m-1)+1$, a contradiction. *Before reading on: in ($\Leftarrow$), which of the three hypotheses on X gives $m-1 \in X$, and which two are not used at all?*

Proof. ($\Rightarrow$) Suppose X has the induction property. Apply Logic and Proof, Axiom 4.2.1 to the property "$n \in X$": its base case is $0 \in X$, and its step is the closure of X. So $\mathbb{N} \subseteq X$. Now $\mathbb{N}$ is a subset of X that contains 0 and is closed under $n \mapsto n+1$, by (($\mathbb{N}$)0) and ($\mathbb{N}$S); the induction property of X gives $\mathbb{N} = X$. By Theorem 2.1.3, every non-empty subset of $X = \mathbb{N}$ has a least element.

($\Leftarrow$) Suppose X has the least-element property. Let $S \subseteq X$ contain 0 and be closed under $n \mapsto n+1$. Suppose $S \neq X$. Then $X \setminus S$ is non-empty: if it were empty, every element of X would lie in S, so $X \subseteq S$, and with $S \subseteq X$ this would give $S = X$ by Proposition 1.2.1. So $X \setminus S$ has a least element m. We have $m \neq 0$, since $0 \in S$. So $m-1 \in X$, by the predecessor property. Since $m-1 < m$ and m is least in $X \setminus S$, $m-1 \notin X \setminus S$, that is, $m-1 \in S$. Hence $m = (m-1)+1 \in S$ by the closure of S, which contradicts $m \in X \setminus S$. So $S = X$, and X has the induction property. This proves the theorem.

■

Second reading · *Each hypothesis has a job*

Each hypothesis on X has a job, and dropping any one of them breaks the theorem. Each witness below names the direction that fails and the step of the proof it blocks.

- **Drop the predecessor property; ($\Leftarrow$) fails.** Let $X := \mathbb{N} \cup \{n + \frac{1}{2} : n \in \mathbb{N}\}$. It contains 0 and is closed, since $(n+\frac{1}{2})+1 = (n+1)+\frac{1}{2}$. It has the least-element property: for

non-empty $T \subseteq X$, compare a least element of $T \cap \mathbb{N}$ with $\frac{1}{2}$ plus a least element of $\{t - \frac{1}{2} : t \in T \setminus \mathbb{N}\}$, each of the two sets, when non-empty, being a subset of $\mathbb{N}$; the smaller of the candidates is least in T (Exercise C2 asks for the details). But $S \coloneqq \mathbb{N}$ contains 0, is closed, and is not X, since $\frac{1}{2} \notin \mathbb{N}$ by Lemma 2.1.1 (e). The proof of ($\Leftarrow$) breaks at "$m - 1 \in X$": here $m = \frac{1}{2}$ is least in $X \setminus S$, and $m \neq 0$, but $m - 1 = -\frac{1}{2} \notin X$.

- **Drop closure; ($\Rightarrow$) fails.** Let $X \coloneqq \{-n : n \in \mathbb{N}\} = \{0, -1, -2, \dots\}$. It contains 0, and it has the predecessor property, since $(-n) - 1 = -(n + 1)$. Its induction property holds **vacuously**: a subset $S \subseteq X$ containing 0 and closed under $n \mapsto n+1$ would contain 1, and $1 \notin X$, since $1 = -n$ would give $n = -1 < 0$, against Lemma 2.1.1 (a); so no such S exists, and every one of them (there are none) equals X. But X itself has no least element, since $-(n + 1) < -n$. The proof of ($\Rightarrow$) breaks at "$\mathbb{N} \subseteq X$ by Logic and Proof, Axiom 4.2.1": the property "$n \in X$" has no inductive step.
- **Drop $0 \in X$; ($\Rightarrow$) fails.** Let $X \coloneqq \{k + \frac{1}{2} : k \in \mathbb{Z}\}$. It is closed, and it has the predecessor property, since $(k+\frac{1}{2})\pm 1 = (k\pm 1)+\frac{1}{2}$ with $k\pm 1 \in \mathbb{Z}$ by Proposition 2.1.2 (a). Its induction property holds vacuously, because $0 \notin X$, so no subset of X contains 0. (Indeed $0 = k + \frac{1}{2}$ would need $k = -\frac{1}{2} \in \mathbb{Z}$, and then $\frac{1}{2} = -k \in \mathbb{Z}$ by Proposition 2.1.2 (a), which discreteness rules out, as shown above.) And X has no least element, since $(k - 1) + \frac{1}{2} < k + \frac{1}{2}$. The proof of ($\Rightarrow$) breaks at "$\mathbb{N} \subseteq X$ by Logic and Proof, Axiom 4.2.1": the property "$n \in X$" has no base case, since $0 \notin X$.

In the last two witnesses the induction property is not false but vacuous. That is why the theorem uses plain closure of S. Under a "closure relative to X" reading ($n + 1 \in S$ only when $n + 1 \in X$), the set $S = \{0\}$ would qualify in the closure witness, the induction property would fail there, and the witness would no longer separate the two properties.

So the slogan "induction and well-ordering are the same principle" means exactly Theorem 2.1.4: for a set of numbers with 0, closure and predecessors, either principle implies the other. So *Logic and Proof*, Chapter 4 could have taken, alongside (($\mathbb{N}$)0) and ($\mathbb{N}$S), the predecessor property and well-ordering as its axioms, and proved induction from them by the ($\Leftarrow$) half of Theorem 2.1.4. The first witness in the fold above shows that the predecessor property cannot be left out, and with induction gone it could no longer be proved as Lemma 2.1.1 (c) was. *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$*, Chapter 1 builds $\mathbb{N}$ from sets and proves the Peano axioms, induction among them, there.

2.1.7 Sets of integers

Well-ordering moves to sets of integers by a shift, provided the bound that makes the shift work is itself an integer.

Corollary 2.1.5. Well-Ordering of Sets of Integers

Let $S \subseteq \mathbb{Z}$ be non-empty. If S has a lower bound $b \in \mathbb{Z}$, then S has a least element. If S has an upper bound $b \in \mathbb{Z}$, then S has a greatest element.

Idea. Slide S to the right by $-b$, so that its lower bound lands on 0; the shifted set lies in $\mathbb{N}$, where Theorem 2.1.3 applies, and sliding back preserves order. For an upper bound, reflect: $-S$ is bounded below by $-b$.

Proof. Lower bound. Let $T := \{s - b : s \in S\}$. Each $s - b$ is an integer by Proposition 2.1.2 (a), and $s - b \geq 0$ since $b \leq s$; so $s - b \in \mathbb{N}$ by Proposition 2.1.2 (b). Thus T is a non-empty subset of $\mathbb{N}$, and by Theorem 2.1.3 it has a least element $m_0 - b$ with $m_0 \in S$. For every $s \in S$, $m_0 - b \leq s - b$, so $m_0 \leq s$. Hence m_0 is a least element of S.

Upper bound. Let $-S := \{-s : s \in S\}$. It is a non-empty set of integers (negatives of integers are integers, by the definition of $\mathbb{Z}$ and Proposition 2.1.2 (a)), and $-b$ is an integer lower bound for it, since $s \leq b$ gives $-b \leq -s$. By the first half, $-S$ has a least element $-m$ with $m \in S$. For every $s \in S$, $-m \leq -s$, so $s \leq m$: m is a greatest element of S. This proves the corollary.

■

Quick check. Does $\{n \in \mathbb{Z} : n^2 < 30\}$ have a least element? Which hypothesis of Corollary 2.1.5 do you check, and how?

Solution. Yes. The hypotheses to check are that the set is non-empty and that it has a lower bound in $\mathbb{Z}$. It is non-empty, since 0 is in it. And -6 is an integer lower bound: an integer $n \leq -6$ has $-n \geq 6 > 0$, so $n^2 = (-n)^2 \geq 36 > 30$, so every element n of the set has $n > -6$. The least element is -5: $(-5)^2 = 25 < 30$, and every element is > -6, hence ≥ -5 by discreteness (Proposition 2.1.2 (c)).

↻ **Second reading** · *Why the bound must be an integer*

The bound must be an integer, or at least have an integer below it. Given a set of integers bounded below by the real number $-\frac{7}{2}$, we would first replace $-\frac{7}{2}$ by the integer -4, and that step, for an arbitrary real bound, is the Archimedean property of *Analysis on the Real Line*, Chapter 1, whose integer-part lemma in Section 1.6 does exactly this. In an ordered field without the Archimedean property, a set of integers can be bounded below and have no least element (in the field $\mathbb{R}(x)$ of *Analysis on the Real Line*, Chapter 1's example of a non-Archimedean field, every $n \in \mathbb{N}$ has $n < x$, so the set $\{-n : n \in \mathbb{N}\}$ is bounded below by $-x$, and it has no least element, since $-(n+1) < -n$), so this chapter, which has no Archimedean property, proves the corollary with an integer bound, and *Analysis on the Real Line*, Chapter 1 supplies the rest.

2.1.8 Exercises

2.1.8.1 A. Check your understanding

Exercise. A1

Parts (a)–(d) are about the proof of Theorem 2.1.3.

(a) Where is trichotomy used?

(b) Why would ordinary induction (Logic and Proof, Axiom 4.2.1) on the same property

"$n \notin S$" not do?

(c) Run the proof on $S = \{4, 7, 9\}$: at which n does the argument meet an element of S, and what does it conclude there?

(d) State the idea of the proof in two sentences.

(e) Let $X = \mathbb{N} \cup \{n + \frac{1}{2} : n \in \mathbb{N}\}$. Which statements of Lemma 2.1.1 remain true when every "$\mathbb{N}$" in them is replaced by "X"? Decide each clause of (a), each half of (b), and (c), (d), (e) separately, with a witness for each failure.

Solution. *(a)* In the inductive step, to split an arbitrary $s \in S$ into $s < n$, $s = n$ or $s > n$. The first case is excluded by the hypothesis, so $s \geq n$. Without trichotomy, "s is not less than n" would not give "$s \geq n$", and n would not be shown to be least.

(b) Ordinary induction gives only $P(n-1)$, that is, $n-1 \notin S$, as hypothesis for $P(n)$. That does not exclude a smaller element of S, such as $n-5$, so "$n \in S$" would not make n least, and no contradiction would follow. The proof needs **all** numbers below n to be outside S.

(c) $S = \{4, 7, 9\}$ has a least element, so the supposition of the proof is false, and the argument meets its contradiction. For $n = 0, 1, 2, 3$, no smaller number is in S, and indeed $n \notin S$. At $n = 4$, no natural number below 4 is in S, and $4 \in S$; the argument shows that every $s \in S$ has $s \geq 4$, so 4 is a least element of S. That contradicts the supposition "S has no least element", and the proof concludes that S has a least element, namely 4.

(d) If S had no least element, then no n could be in S, because the first one would be least; strong induction makes "the first one" precise. So S would be empty, against the hypothesis.

(e) Holding: the first clause of (a) (every element is ≥ 0); the sum half of (b), since a sum of two halves $(m+\frac{1}{2})+(n+\frac{1}{2}) = m+n+1$ is a natural number and a half plus a natural number is a half; and (d): if $x \leq y$ in X, then $y - x \in X$. For (d) there are four cases. Two natural numbers, or two halves, have a difference in $\mathbb{N}$ by Lemma 2.1.1 (d). For $x = m \leq y = n + \frac{1}{2}$, we have $m \leq n$ (else $m \geq n + 1 > y$ by (e) of the lemma), so $y - x = (n - m) + \frac{1}{2} \in X$. For $x = m + \frac{1}{2} \leq y = n$, we have $m < n$, so $m + 1 \leq n$ and $y - x = (n - m - 1) + \frac{1}{2} \in X$.

Failing: the second clause of (a), since $\frac{1}{2} \neq 0$ and $\frac{1}{2} < 1$; the product half of (b), since $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \notin X$ (it is not a natural number, as $0 < \frac{1}{4} < 1$, and not a half, as $\frac{1}{4} - \frac{1}{2} < 0$); (c), since $\frac{1}{2} \neq 0$ and $\frac{1}{2} - 1 = -\frac{1}{2} \notin X$; (e), since $0 < \frac{1}{2} < 1$ with $\frac{1}{2} \in X$.

Each clause had to be decided by its own witness. The proofs of (a)–(d) were inductions over $\mathbb{N}$, and X does not have the induction property ($\mathbb{N} \subseteq X$ contains 0 and is closed), so none of those proofs carries over; some conclusions survive anyway. (c) fails because the predecessor property fails at $\frac{1}{2}$. (e) fails through the second clause of (a), not through (d), which still holds. The set $\mathbb{Z} \cup \{k + \frac{1}{2} : k \in \mathbb{Z}\}$ has the predecessor property and still has $\frac{1}{2}$ between 0 and 1, so the predecessor property alone (with 0 and closure) does not give (e); together with the least-element property it does: the set then has the induction property by Theorem 2.1.4, and, as in the proof of its ($\Rightarrow$) half, it equals $\mathbb{N}$.

2.1.8.2 B. Practice

Exercise. B1

Use only Lemma 2.1.1 and the arithmetic of $\mathbb{R}$.

(a) Prove that if $m, n \in \mathbb{N}$ and $mn = 1$, then $m = n = 1$.

(b) Prove that $n^2 \geq n$ for every $n \in \mathbb{N}$.

Solution. *(a)* Since $0 \cdot n = 0 \neq 1$, we have $m \neq 0$, and likewise $n \neq 0$. By the second clause of Lemma 2.1.1 (a), $m \geq 1$ and $n \geq 1$. Suppose $m > 1$. Multiplying by $n > 0$ gives $mn > n \geq 1$, which contradicts $mn = 1$. So $m = 1$, and then $n = mn = 1$.

(b) Let $n \in \mathbb{N}$. By Lemma 2.1.1 (a), $n = 0$ or $n \geq 1$. If $n = 0$, then $n^2 = 0 = n$. If $n \geq 1$, multiplying $n \geq 1$ by $n > 0$ gives $n^2 \geq n$. In both cases $n^2 \geq n$.

Exercise. B2: Putting a proof in order

The lines below, (i)–(ix), include the seven lines of a proof of ($\Leftarrow$) in Theorem 2.1.4, shuffled, and two lines that do not belong. Here X has $0 \in X$, closure and the predecessor property, and the least-element property. Write the seven lines in an order that makes a correct proof, and say why each of the other two lines fails.

(i) So $m - 1 \in X$, by the predecessor property.

(ii) Let m be the least element of S.

(iii) Then $X \setminus S$ is non-empty, so it has a least element m.

(iv) Hence $m = (m - 1) + 1 \in S$, a contradiction; so $S = X$.

(v) Let $S \subseteq X$ contain 0 and be closed under $n \mapsto n + 1$.

(vi) $m - 1 < m$, so $m - 1 \notin X \setminus S$, that is, $m - 1 \in S$.

(vii) Since m is least and $m - 1 < m$, $m - 1 \in X \setminus S$.

(viii) Suppose $S \neq X$.

(ix) $m \neq 0$, since $0 \in S$.

Solution. The order is (v), (viii), (iii), (ix), (i), (vi), (iv). It is the only admissible one. (v) introduces S, (viii) is the supposition the rest contradicts, and (iii) introduces m from it. (ix) must sit between (iii) and (i): it needs the m of (iii), and (i) applies the predecessor property, which needs $m \neq 0$. (vi) uses the $m - 1 \in X$ of (i): only an element of X can be sorted into S or $X \setminus S$. (iv) uses (vi) and closure.

Line (ii) takes the least element of the wrong set. The set whose least element locates a failure is $X \setminus S$: its least element is the first number of X missing from S. A least element of S says nothing about where S and X differ; in the case $X = \mathbb{N}$ it is 0, which lies in S by (v) and is no failure at all. Line (vii) reads leastness backwards: "m is least in $X \setminus S$" says that nothing **below** m lies in $X \setminus S$, so a smaller number of X is in S, not outside it.

Exercise. B3

Prove the second half of Corollary 2.1.5 directly from Theorem 2.1.3, without using the first half: if $S \subseteq \mathbb{Z}$ is non-empty and $b \in \mathbb{Z}$ is an upper bound of S, then S has a greatest element.

Hint: shift by $s \mapsto b - s$.

Solution. Let $T := \{b - s : s \in S\}$. For $s \in S$, $b - s$ is an integer by Proposition 2.1.2 (a), and $b - s \geq 0$ because $s \leq b$; so $b - s \in \mathbb{N}$ by Proposition 2.1.2 (b). Thus T is a non-empty subset of $\mathbb{N}$, and by Theorem 2.1.3 it has a least element, of the form $b - s_0$ with $s_0 \in S$. For every $s \in S$, $b - s_0 \leq b - s$, so $s \leq s_0$. Hence s_0 is a greatest element of S.

Exercise. B4: Prove or disprove

Prove each true statement, by the method of Example (Method: the least element) where it applies, and refute each false one with a concrete counterexample.

(a) Every non-empty set of integers has a least element.

(b) Every non-empty set of negative rational numbers has a greatest element.

(c) Every non-empty set of even natural numbers has a least element.

(d) Every non-empty subset of $\{1/n : n \in \mathbb{Z}_{>0}\}$ has a greatest element.

(e) Every non-empty subset of $\{1/n : n \in \mathbb{Z}_{>0}\}$ has a least element.

(f) If $S \subseteq \mathbb{Z}$ is non-empty and $s \geq -\frac{13}{3}$ for every $s \in S$, then S has a least element.

Solution.

(a) **False.** Take $\mathbb{Z}$ itself. For every $n \in \mathbb{Z}$, also $n - 1 \in \mathbb{Z}$ by Proposition 2.1.2 (a), and $n - 1 < n$, so no element is least.

(b) **False.** Take $\{-1/n : n \in \mathbb{Z}_{>0}\}$, a non-empty set of negative rationals. For each $-1/n$ in it, $-1/(n+1)$ is in it too, and $-1/n < -1/(n+1)$, so no element is greatest.

(c) **True.** Such a set is a non-empty subset of $\mathbb{N}$, so Theorem 2.1.3 gives it a least element.

(d) **True.** Let T be a non-empty subset, and let $N := \{n \in \mathbb{Z}_{>0} : 1/n \in T\}$. Then $N \subseteq \mathbb{Z}_{>0} \subseteq \mathbb{N}$, and N is non-empty: T has an element, which is $1/n$ for some $n \in \mathbb{Z}_{>0}$, and that n lies in N. So N has a least element n_0 (Theorem 2.1.3). Then $1/n_0 \in T$, and for every $1/n \in T$ we have $n \in N$, so $n \geq n_0 > 0$ and $1/n \leq 1/n_0$. So $1/n_0$ is a greatest element of T.

(e) **False.** Take the whole set. For each $1/n$ in it, $1/(n+1)$ is in it too, and $1/(n+1) < 1/n$, so no element is least.

(f) **True.** The integer -5 is a lower bound of S, since $-5 < -\frac{13}{3} \leq s$ for every $s \in S$. So Corollary 2.1.5 applies.

Items (c), (d) and (f) are well-ordering, sometimes after a change of view: (c) is a subset of $\mathbb{N}$ as it stands, (f) needs its bound $-\frac{13}{3}$ replaced by the integer -5, and (d) passes from $1/n$ to n, where "greatest" becomes "least". The false items are the warning after Theorem 2.1.3 in three costumes.

2.1.8.3 C. Going deeper

Exercise. C1: A greatest element from a least upper bound

Let $S \subseteq \mathbb{N}$ be non-empty, and suppose some $M \in \mathbb{N}$ satisfies $s \leq M$ for every $s \in S$.

(a) Prove that S has a greatest element by applying Theorem 2.1.3 to the set U of upper bounds of S that lie in $\mathbb{N}$, not by citing Corollary 2.1.5: show that the least element of

U lies in S.

(b) Show that the hypothesis "some $M \in \mathbb{N}$ bounds S above" cannot be dropped.

Solution (Hint 1). Consider $U := \{u \in \mathbb{N} : s \leq u \text{ for every } s \in S\}$.

Solution (Hint 2). U is non-empty because $M \in U$; let u be its least element, which exists by Theorem 2.1.3.

Solution. *(a)* Let $U := \{u \in \mathbb{N} : s \leq u \text{ for every } s \in S\}$. Then $M \in U$, so U is a non-empty subset of $\mathbb{N}$, and Theorem 2.1.3 gives a least element u of U. We show $u \in S$.

Suppose $u \notin S$. Then every $s \in S$ satisfies $s \leq u$ and $s \neq u$, so $s < u$, and $s + 1 \leq u$ by Lemma 2.1.1 (e); that is, $s \leq u - 1$. Since S is non-empty, it has an element s_0, and $0 \leq s_0 < u$ by Lemma 2.1.1 (a), so $u \neq 0$. By Lemma 2.1.1 (c), $u - 1 \in \mathbb{N}$. So $u - 1$ is an upper bound of S in $\mathbb{N}$, that is, $u - 1 \in U$, and $u - 1 < u$, which contradicts the choice of u. Hence $u \in S$.

Since $u \in S$ and $s \leq u$ for every $s \in S$, u is a greatest element of S.

(b) $S = \mathbb{N}$ is non-empty and has no greatest element: for every $n \in \mathbb{N}$, also $n + 1 \in \mathbb{N}$ by ($\mathbb{N}$S), and $n + 1 > n$. In the proof, U is then empty, and Theorem 2.1.3 has nothing to apply to.

The number u of (a) is the **least upper bound** of S among natural numbers, and the proof shows that it lies in S. Section 4.3 defines least upper bounds in any partially ordered set, and *Analysis on the Real Line*, Chapter 1 is about sets of real numbers whose least upper bound, when it exists, need **not** lie in the set.

Marking scheme. (10 points) - 2: defines the set of upper bounds in $\mathbb{N}$, shows it is non-empty, and takes its least element by Theorem 2.1.3. - 2: handles $u = 0$ separately, or shows $u \neq 0$ using that S is non-empty, before using $u - 1 \in \mathbb{N}$ (Lemma 2.1.1 (c)). - 3: uses the minimality of u: either shows directly that $u - 1 \notin U$, so some $s \in S$ has $s > u - 1$, or, supposing $u \notin S$, derives $u - 1 \in U$ and contradicts minimality. - 1: uses discreteness (Lemma 2.1.1 (e)) to show that an element of S greater than $u - 1$ equals u, or to get $s \leq u - 1$ in the contradiction route, and concludes that $u \in S$ is a greatest element. - 2: (b) the witness $S = \mathbb{N}$, with the reason it has no greatest element. Fatal errors (0 for the step): using $u - 1 \in \mathbb{N}$ without checking $u \neq 0$; taking a least element of U without showing U non-empty.

A second route, through the least element $M - s_0$ of $\{M - s : s \in S\} \subseteq \mathbb{N}$ (as in Exercise (B3)), proves the conclusion of (a) but not by the method the task names, so it earns at most 4 points for (a): 2 for showing that this set is a non-empty subset of $\mathbb{N}$ and taking its least element, and 2 for deducing $s \leq s_0$ for every $s \in S$ from $M - s_0 \leq M - s$, with $s_0 \in S$; and (b) as above.

Exercise. C2: A well-ordered set with gaps

Let $X := \mathbb{N} \cup \{n + \frac{1}{2} : n \in \mathbb{N}\}$. Prove that every non-empty subset of X has a least element.

Solution. Let $T \subseteq X$ be non-empty, and put

$$A := T \cap \mathbb{N}, \qquad B := \{t - \tfrac{1}{2} : t \in T \setminus \mathbb{N}\}.$$

Every $t \in T \setminus \mathbb{N}$ is $n + \frac{1}{2}$ for some $n \in \mathbb{N}$, since $t \in X$; so $t - \frac{1}{2} = n \in \mathbb{N}$, and $B \subseteq \mathbb{N}$. Since $T = A \cup (T \setminus \mathbb{N})$ is non-empty, A or B is non-empty. By Theorem 2.1.3, A, if non-empty, has a least element a, and B, if non-empty, has a least element b. Define

$$c := \begin{cases} a & \text{if } B = \emptyset, \\ b + \frac{1}{2} & \text{if } A = \emptyset, \\ \min\{a,\, b + \frac{1}{2}\} & \text{otherwise.} \end{cases}$$

In each case $c \in T$: $a \in A \subseteq T$, and $b = t - \frac{1}{2}$ for some $t \in T \setminus \mathbb{N}$, so $b + \frac{1}{2} = t \in T$.

Let $t \in T$. If $t \in \mathbb{N}$, then $t \in A$, so $A \neq \emptyset$ and $t \geq a \geq c$. If $t \notin \mathbb{N}$, then $t - \frac{1}{2} \in B$, so $B \neq \emptyset$ and $t - \frac{1}{2} \geq b$, that is, $t \geq b + \frac{1}{2} \geq c$. (In both chains, the last inequality holds in every case of the definition of c that can occur.) So c is a least element of T.

The set X has the least-element property, contains 0 and is closed under $n \mapsto n + 1$, but it does not have the induction property ($\mathbb{N} \subseteq X$ contains 0 and is closed, and $\mathbb{N} \neq X$). That is the first witness after Theorem 2.1.4: without the predecessor property, well-ordering does not give induction.

Marking scheme. (10 points) - 2: splits T into its natural-number part and its half part, and shows the shifted half part lies in $\mathbb{N}$. - 2: applies Theorem 2.1.3 to each non-empty part, saying that at least one part is non-empty. - 2: defines the candidate in all cases, including those where one part is empty, and checks it lies in T. - 3: checks the candidate is $\leq t$ for every $t \in T$, by cases on $t \in \mathbb{N}$ or not. - 1: concludes, with the quantifiers right: one least element for the given T. Fatal errors (0 for the step): applying Theorem 2.1.3 to T itself (it need not be a subset of $\mathbb{N}$); taking a least element of an empty part.

A second route, through the least element of $\{2t : t \in T\} \subseteq \mathbb{N}$, earns the same points. It earns 4 for showing that this set lies in $\mathbb{N}$, checking both $2n$ and $2n + 1$ by Lemma 2.1.1 (b), and that it is non-empty, and for taking its least element $2t_0$ with $t_0 \in T$ by Theorem 2.1.3. It earns 4 for deducing $t_0 \leq t$ from $2t_0 \leq 2t$ for every $t \in T$, and 2 for the conclusion. The same fatal errors apply.

2.2 Induction, Strong Induction and Divisibility

Logic and Proof, Chapter 4 gave the principle of induction (Logic and Proof, Axiom 4.2.1), its strong form (Logic and Proof, Theorem 4.2.2), and the first worked proofs: a sum (Logic and Proof, Example (A sum of products of neighbors)), an inequality (Logic and Proof, Example (An inequality by induction)), and a strong induction with three base cases (Logic and Proof, Example (Threes and fives)). *Logic and Proof*, Chapter 8 showed how an induction is written in prose (Logic and Proof, Example (An induction, and a legitimate symmetry)). This section is about the craft: which form of induction fits a claim, where it starts, how to find the induction

hypothesis inside the step, and how an induction goes wrong, each failure located at one step. On the way it proves two facts that *Logic and Proof* took from school: a fraction can be reduced until numerator and denominator are not both even, and every integer $n \geq 2$ has a prime factor.

2.2.1 Induction from any integer

Logic and Proof, Chapter 4 already started inductions at numbers other than 0 (*Logic and Proof*, Section 4.2, "Starting from another number"), for a starting point $b \in \mathbb{N}$. With $\mathbb{Z}$ and Proposition 2.1.2 in hand, the starting point may be any integer, negative ones included.

To prove a statement for every integer from n_0 on, prove it at n_0 and show that it passes from each integer to the next.

Theorem 2.2.1. Induction from a Base

Let n_0 be an integer, and for each integer $n \geq n_0$ let $P(n)$ be a statement. Suppose

(i) (**base case**) $P(n_0)$ is true, and

(ii) (**inductive step**) for **every** integer $n \geq n_0$, if $P(n)$ is true then $P(n+1)$ is true.

Then $P(n)$ is true for every integer $n \geq n_0$.

Idea. Count from the base. The integers $n \geq n_0$ are exactly $n_0 + k$ with $k \in \mathbb{N}$, and moving from n to $n+1$ moves k to $k+1$. So the statement "$P(n_0 + k)$" about $k \in \mathbb{N}$ is ready for Logic and Proof, Axiom 4.2.1, and its base case is $P(n_0)$.

Proof. For $k \in \mathbb{N}$, let $Q(k)$ be the statement $P(n_0 + k)$. This makes sense: $n_0 + k$ is an integer by Proposition 2.1.2 (a), and $n_0 + k \geq n_0$ since $k \geq 0$ by Lemma 2.1.1 (a).

Base case. $Q(0)$ is $P(n_0)$, which holds by (i).

Inductive step. Let $k \in \mathbb{N}$, and suppose $Q(k)$, that is, $P(n_0 + k)$. The integer $n \coloneqq n_0 + k$ satisfies $n \geq n_0$, so (ii) gives $P(n+1)$. Since $n + 1 = n_0 + (k+1)$, this is $Q(k+1)$.

By Logic and Proof, Axiom 4.2.1, $Q(k)$ holds for every $k \in \mathbb{N}$. Now let n be an integer with $n \geq n_0$. Then $k \coloneqq n - n_0$ is an integer by Proposition 2.1.2 (a), and $k \geq 0$, so $k \in \mathbb{N}$ by Proposition 2.1.2 (b). Hence $Q(k)$ holds, and $Q(k)$ is $P(n_0 + k) = P(n)$. This proves the theorem.

■

For $n_0 = 0$ the theorem is Logic and Proof, Axiom 4.2.1 itself, and for $n_0 \in \mathbb{N}$ it is *Logic and Proof*, Chapter 4's induction started at n_0. In the inductive step, "$P(n)$ is true" is the induction hypothesis: one implication, proved once, inside a $\to$I box whose assumption is $P(n)$ for one fixed but arbitrary integer $n \geq n_0$.

The strong form moves to a base in the same way.

Theorem 2.2.2. Strong Induction from a Base

Let n_0 be an integer, and for each integer $n \geq n_0$ let $P(n)$ be a statement. Suppose that, **for every** integer $n \geq n_0$: if $P(k)$ is true for **every** integer k with $n_0 \leq k < n$, then $P(n)$ is true. Then $P(n)$ is true for every integer $n \geq n_0$.

Proof. For $j \in \mathbb{N}$, let $Q(j)$ be $P(n_0 + j)$, as in the proof of Theorem 2.2.1. We check the hypothesis of Logic and Proof, Theorem 4.2.2 for Q. Let $j \in \mathbb{N}$, and suppose $Q(i)$ holds for every $i \in \mathbb{N}$ with $i < j$. Put $n := n_0 + j$, an integer with $n \geq n_0$. Let k be an integer with $n_0 \leq k < n$. Then $i := k - n_0$ is an integer with $i \geq 0$, so $i \in \mathbb{N}$ by Proposition 2.1.2 (b), and $i < n - n_0 = j$; so $Q(i)$, which is $P(k)$, holds. The hypothesis of the theorem at n now gives $P(n)$, that is, $Q(j)$. By Logic and Proof, Theorem 4.2.2, $Q(j)$ holds for every $j \in \mathbb{N}$, and every integer $n \geq n_0$ is $n_0 + j$ with $j = n - n_0 \in \mathbb{N}$, as in the proof of Theorem 2.2.1. This proves the theorem.

■

So Theorem 2.2.2 is a corollary of Logic and Proof, Theorem 4.2.2, by the same shift. When $n_0 \in \mathbb{N}$, it says what Logic and Proof, Example (Threes and fives) achieved with a guard: there the property was "if $n \geq 8$, then ...", stated for every $n \in \mathbb{N}$ and vacuous below 8. Here the property is stated only for $n \geq n_0$, and the hypothesis speaks only about $k \geq n_0$. The two are the same argument in two notations, and the base cases sit in the same place: they are the n for which the step reaches below n_0.

Quick check. Every integer $n \geq 24$ is $5a + 7b$ for some integers $a, b \geq 0$. A proof by Theorem 2.2.2 writes $n = (n - 5) + 5$ in its step. How many base cases does it need, and which? Can the base 24 be lowered?

Solution. The step uses $P(n-5)$, which the hypothesis supplies only when $n - 5 \geq 24$, that is, $n \geq 29$. So $n = 24, 25, 26, 27, 28$ are base cases, five of them, checked directly:

$$24 = 5 \cdot 2 + 7 \cdot 2, \quad 25 = 5 \cdot 5, \quad 26 = 5 \cdot 1 + 7 \cdot 3,$$
$$27 = 5 \cdot 4 + 7 \cdot 1, \quad 28 = 7 \cdot 4.$$

The base cannot be lowered: 23 is not of the form. With $b = 0, 1, 2, 3$ the difference $23 - 7b$ is $23, 16, 9, 2$, none a multiple of 5, and $b \geq 4$ gives $23 - 7b < 0$.

2.2.2 Finding $P(n)$ inside $P(n+1)$

In every induction the step is an implication $P(n) \Rightarrow P(n+1)$, proved for an arbitrary n. The work is to find, inside the statement $P(n+1)$, the statement $P(n)$, so that the hypothesis can be used: one more term to split off, one more factor to take out, one more case to bound. The first example is about divisibility (Definition 1.1.2).

Idea (Scratch work). The claim is $7 \mid 9^n - 2^n$ for every $n \in \mathbb{N}$, with the powers in their school meaning. The base is $9^0 - 2^0 = 0 = 7 \cdot 0$. For the step, the hypothesis is about $9^n - 2^n$, so write $P(n+1)$ out and look for that expression in it. The first try, $9^{n+1} - 2^{n+1} = 9 \cdot 9^n - 2 \cdot 2^n$, does not contain it: the two powers have different factors in front, 9 and 2. Force the old expression in.

Take 9 out of both terms, and pay back what that costs: $9\cdot 9^n - 2\cdot 2^n = 9(9^n - 2^n) + 9\cdot 2^n - 2\cdot 2^n$, and the payment $9\cdot 2^n - 2\cdot 2^n$ is $7\cdot 2^n$, a multiple of 7 again.

Givens	Goal
$P(n)$: $9^n - 2^n = 7k$ with $k \in \mathbb{Z}$	$P(n+1)$: $9^{n+1} - 2^{n+1} = 7m$ for some $m \in \mathbb{Z}$
$9^{n+1} = 9\cdot 9^n$, $2^{n+1} = 2\cdot 2^n$ (school meaning)	$9^{n+1} - 2^{n+1}$ rewritten so that $9^n - 2^n$ appears
$9^{n+1} - 2^{n+1} = 9(9^n - 2^n) + 7\cdot 2^n = 7(9k + 2^n)$	$m := 9k + 2^n \in \mathbb{Z}$: the gap is closed

The old expression appears once, the hypothesis turns it into $7k$, and what is left over is a multiple of 7 by computation.

Divisibility claims about powers are a staple of induction, because the step can usually be arranged to contain the old expression once. Here is the proof the scratch work found. *Claim:* $7 \mid 9^n - 2^n$ for every $n \in \mathbb{N}$, with 9^n and 2^n in their school meaning ($a^0 = 1$, $a^{n+1} = a^n \cdot a$, and a^n is an integer for an integer a; Section 2.3 makes this a definition). *Base case:* $9^0 - 2^0 = 0 = 7\cdot 0$. *Step:* if $9^n - 2^n = 7k$ with $k \in \mathbb{Z}$, then

$$9^{n+1} - 2^{n+1} = 9(9^n - 2^n) + 7\cdot 2^n = 7(9k + 2^n),$$

and $9k + 2^n \in \mathbb{Z}$. By Logic and Proof, Axiom 4.2.1, the claim holds for every $n \in \mathbb{N}$.

Example. Method: finding $P(n)$ inside $P(n+1)$

Template. (1) Write $P(n+1)$ out in full. (2) Find $P(n)$ inside it: split off the last term, take out one factor, or separate the new piece from the old. (3) Apply the induction hypothesis to the old part. (4) Close the rest by computation. (5) Choose the base: the first n the claim covers from which steps (2)–(4) work, with any smaller n the claim covers checked directly.

When to use it. $P(n+1)$ is built from $P(n)$ by one operation: a term added, a factor multiplied, an element added to a set.

The usual failure. Starting from $P(n+1)$ and deriving something true, which proves the converse, entry (N5) of Logic and Proof, Example (What is not allowed). A step that works only from some n on, with the base set lower (as in the gallery below). Using $P(n+1)$ inside its own step (N9).

Quick check. For a proof that $5 \mid 9^n - 4^n$ for every $n \in \mathbb{N}$, write $9^{n+1} - 4^{n+1}$ so that $9^n - 4^n$ appears.

Solution. $9^{n+1} - 4^{n+1} = 9\cdot 9^n - 4\cdot 4^n = 9(9^n - 4^n) + 5\cdot 4^n$. If $9^n - 4^n = 5k$ with $k \in \mathbb{Z}$, this is $5(9k + 4^n)$, and $9k + 4^n \in \mathbb{Z}$.

The fifth step of the template deserves an example of its own, because the place where the step starts working need not be the place where the claim starts being true.

Example. Where the step starts working

Prove that $3^n \geq n^3$ for every $n \in \mathbb{N}$, with the powers in their school meaning.

Idea. By Example (Method: finding $P(n)$ inside $P(n+1)$), write $P(n+1)$ out: it contains 3^n as $3^{n+1} = 3 \cdot 3^n \geq 3n^3$, so the step needs $3n^3 \geq (n+1)^3$. That holds from $n = 3$ on, and not before. So the base is 3, and 0, 1, 2 are checked directly.

Solution. Small cases. $3^0 = 1 \geq 0 = 0^3$, $3^1 = 3 \geq 1 = 1^3$, and $3^2 = 9 \geq 8 = 2^3$.

From 3 on, by Theorem 2.2.1 with base 3. *Base case:* $3^3 = 27 \geq 27 = 3^3$. *Step:* let $n \geq 3$ be an integer with $3^n \geq n^3$. Then $3^{n+1} = 3 \cdot 3^n \geq 3n^3$. Since $n \geq 3$,

$$2n^3 \geq 6n^2 = 3n^2 + 3n^2 \geq 3n^2 + 9n \geq 3n^2 + 3n + 1,$$

so $3n^3 = n^3 + 2n^3 \geq n^3 + 3n^2 + 3n + 1 = (n+1)^3$. Hence $3^{n+1} \geq (n+1)^3$.

The small cases and the induction together give $3^n \geq n^3$ for every $n \in \mathbb{N}$.

The claim is true at 0, 1 and 2, but the argument of the step fails from 2 to 3: $3 \cdot 2^3 = 24 < 27 = 3^3$. The base is where the step starts working, or the first n the claim covers if that is later. It need not be the first n at which the claim is true, and the cases below it are checked one by one.

Quick check. For which $n \in \mathbb{N}$ is $3n^3 \geq (n+1)^3$ false, and why does that make 3 the base although $3^n \geq n^3$ holds at 0, 1 and 2?

Solution. For $n = 0, 1, 2$: $0 < 1$, $3 < 8$ and $24 < 27$. The step is proved only from 3 on, so the three smaller cases need their own checks; an induction from base 0 would have three unproved transitions.

2.2.3 Divisibility and the division algorithm

The next results are about divisibility.

Divisibility and primes were defined in Section 1.1: for integers a and b, $a \mid b$ means $b = ka$ for some $k \in \mathbb{Z}$ (Definition 1.1.2), and a prime is an integer $p \geq 2$ whose only positive divisors are 1 and p (Definition 1.1.3); divisibility is transitive (Proposition 1.1.1). For instance, $3 \mid 12$, with $k = 4$.

Change 12 to 14: $3 \nmid 14$. The witness k would have to be $14/3$, and $4 < 14/3 < 5$, so $14/3$ is not an integer, by the discreteness clause of Proposition 2.1.2. The clause that fails is "$k \in \mathbb{Z}$": the equation $14 = k \cdot 3$ has a real solution, just not an integer one.

Section 1.1 worked the first examples of primes and non-primes after Definition 1.1.3. The clause $p \geq 2$ keeps 1 out so that factorizations into primes can be unique, a fact this chapter does not prove or use: Exercise B2 below is about existence only.

Every integer, divided by a positive integer n, leaves a remainder between 0 and $n-1$. This is school arithmetic, and it is the tool behind "even or odd".

Theorem 2.2.3. Division Algorithm

Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$. Then there are **unique** integers q and r with

$$a = qn + r \quad \text{and} \quad 0 \leq r < n.$$

The hypothesis $n > 0$ matters: for $n = 0$ no r satisfies $0 \leq r < 0$.

Try it first (ten minutes): which set of non-negative integers should have a least element, and why is that least element the remainder?

Idea. The obvious attempt subtracts n from a again and again until what is left lies in $[0, n)$, adding n instead when a is negative. "Again and again until" is a process, not yet a proof: why does it stop, and why at a number below n? Well-ordering replaces the process by its outcome. Among all the non-negative integers $a - qn$, take the **least** (the method of Example (Method: the least element): S the non-negative integers $a - qn$). If it were n or more, subtracting one more n would leave a smaller non-negative one. For uniqueness: two remainders differ by a multiple of n, yet lie less than n apart, so the multiple is 0.

Proof. Existence. Let

$$R := \{a - qn : q \in \mathbb{Z}\} \cap \{x \in \mathbb{Z} : x \geq 0\},$$

the set of non-negative integers of the form $a - qn$ (each $a - qn$ is an integer by Proposition 2.1.2 (a)). The set R is non-empty. If $a \geq 0$, take $q = 0$: then $a - 0 \cdot n = a \in R$. If $a < 0$, take $q = a$: then $a - an = a(1 - n) \geq 0$, since $a < 0$ and $1 - n \leq 0$ (as $n \geq 1$ by Proposition 2.1.2 (b)). The set R is a non-empty set of integers with the integer lower bound 0, so by Corollary 2.1.5 it has a least element r; write $r = a - qn$ with $q \in \mathbb{Z}$. Then $a = qn + r$ and $r \geq 0$.

Suppose $r \geq n$. Then $r - n = a - (q + 1)n$ is an integer of the required form with $r - n \geq 0$, so $r - n \in R$; and $r - n < r$, since $n > 0$. This contradicts the choice of r. Hence $r < n$.

Uniqueness. Let $a = qn + r = q'n + r'$ with $q, q', r, r' \in \mathbb{Z}$, $0 \leq r < n$ and $0 \leq r' < n$. Suppose $r \neq r'$. By symmetry (exchanging (q, r) and (q', r') changes neither the hypotheses nor the goal) we may suppose $r' < r$. Then $r - r' = (q' - q)n$, and $k := q' - q$ is an integer with $kn = r - r' > 0$. Since $n > 0$, also $k > 0$, so $k \geq 1$ by Proposition 2.1.2 (b), and

$$r - r' = kn \geq n.$$

But $r - r' \leq r < n$, since $r' \geq 0$. This contradiction shows $r = r'$. Then $qn = q'n$, and since $n \neq 0$, $q = q'$. This proves the theorem.

■

The integers q and r are the **quotient** and the **remainder** of a on division by n. For negative a the remainder is still non-negative: $-7 = 3 \cdot (-3) + 2$, with remainder 2, not -1. Existence and uniqueness do separate jobs, and the case $n = 2$ shows both:

- **Existence** says that every integer a is $2q$ or $2q+1$: every integer is **even or odd**.
- **Uniqueness** says that no integer is both. If $a = 2q = 2q'+1$, then a would have remainders 0 and 1.

Section 1.1 proved this by induction (Theorem 1.1.2); here it falls out of the division algorithm with $n = 2$. *Logic and Proof* used it in Argument A of Chapter 1 and in the proof of Logic and Proof, Theorem 2.1.3. The same uniqueness shows that no integer m has $2m = 1$, since $1 = 2 \cdot 0 + 1$ has remainder 1 and $2m = 2m + 0$ has remainder 0; this is the fact *Analysis on the Real Line*, Chapter 1 uses to show that $\mathbb{Z}$ is not a field. An integer $4k + 1 = 2(2k) + 1$ or $4k + 3 = 2(2k + 1) + 1$ is odd. With $n = 3$, every integer is $3k$, $3k + 1$ or $3k + 2$, for exactly one of the three forms.

Warning. "The remainder" is the r of the theorem, with $0 \leq r < n$. The equations $17 = 5 \cdot 4 - 3$ and $17 = 5 \cdot 2 + 7$ are true, but -3 and 7 are not remainders, and allowing them destroys uniqueness: 17 would have the three "remainders" -3, 2 and 7. Every argument above that concludes from "remainder 1" that a number is not a multiple of 2 uses the range $0 \leq r < n$, through uniqueness.

2.2.4 Lowest terms and prime factors

Logic and Proof, Chapter 2 needed one more fact about fractions, the fact (L) in the proof of Logic and Proof, Theorem 2.2.1: every rational number can be written with numerator and denominator not both even. The reason given there was that halving cannot go on for ever. Here is that reason as a proof. It supposes the claim fails, takes the least failure and derives a contradiction: a proof by **smallest counterexample**, the method of Example (Method: the least element) applied to the set of failures. Section 2.4 makes it a method of its own; here its steps are named as they occur.

Lemma 2.2.4. Lowest Terms, Up to Factors of Two

Every rational number can be written as p/q with $p \in \mathbb{Z}$, $q \in \mathbb{Z}_{>0}$, and p and q **not both** even.

Idea. A representation with both entries even can be halved. Halving makes the denominator smaller, so a least denominator cannot belong to a representation that can be halved. Well-ordering supplies the least denominator.

Proof. Suppose it fails. Fix $r \in \mathbb{Q}$, and suppose that r has no representation p/q with $p \in \mathbb{Z}$, $q \in \mathbb{Z}_{>0}$, and p and q not both even. Let

$$F \coloneqq \{q \in \mathbb{Z}_{>0} : r = p/q \text{ for some } p \in \mathbb{Z}\}.$$

Under the supposition, every $q \in F$ is the denominator of a failing representation.

Take the least failure. By the definition of $\mathbb{Q}$, $r = p/q$ for some $p \in \mathbb{Z}$ and $q \in \mathbb{Z}_{>0}$, so F is non-empty; and $F \subseteq \mathbb{Z}_{>0} \subseteq \mathbb{N}$. By Theorem 2.1.3, F has a least element m. Write $r = p/m$ with $p \in \mathbb{Z}$.

Use the supposition at m. The representation $r = p/m$ fails, so p and m are both even:

$p = 2p'$ and $m = 2m'$ with $p', m' \in \mathbb{Z}$.

Produce a smaller failure. Since $m > 0$, $m' = m/2 > 0$, so $m' \in \mathbb{Z}_{>0}$ by Proposition 2.1.2 (b). Moreover $r = 2p'/(2m') = p'/m'$, so $m' \in F$; and $m' < m' + m' = m$. So m' is an element of F smaller than its least element m, a contradiction.

Hence r has a representation of the required kind. As $r \in \mathbb{Q}$ was arbitrary, this proves the lemma.

■

This is (L), with more: the denominator can be taken positive, not merely non-zero. The proof of Logic and Proof, Theorem 2.2.1 now rests on a proved lemma. The same argument with "not both even" replaced by "no common divisor $d \geq 2$" puts every fraction in lowest terms in the full sense; that is Exercise C2. This proof is written out in full; two later exercises use the same move with less given: Exercise B2 below leaves its last step blank, and Exercise C1 of Section 2.3 leaves the last half blank.

The next result is the prime-factor fact that *Logic and Proof*, Chapter 8 used. Its proof is a strong induction from base 2; the same argument inside an RAA box is a smallest-counterexample proof, in which the least failure m gets a prime factor from its divisor a, contradicting the choice of m (compare Exercise B2).

Theorem 2.2.5. Every Integer at Least Two Has a Prime Factor

Every integer $n \geq 2$ has a prime factor.

Idea. A prime is its own prime factor. A number that is not prime has a divisor strictly between 1 and itself; that divisor is smaller, so it has a prime factor by the strong hypothesis, and divisibility passes it on.

Proof. We use Theorem 2.2.2 with $n_0 = 2$. Let $n \geq 2$ be an integer, and suppose every integer k with $2 \leq k < n$ has a prime factor.

If n is prime, then n is a prime factor of itself, since $n = 1 \cdot n$.

If n is not prime, then, as $n \geq 2$, it has a positive divisor $a \notin \{1, n\}$ (Definition 1.1.3). Write $n = ka$ with $k \in \mathbb{Z}$. Since $n > 0$ and $a > 0$, also $k > 0$, so $k \geq 1$ and $a \geq 1$ by Proposition 2.1.2 (b). Hence $a \leq ka = n$. With $a \neq 1$ and $a \neq n$ this gives $1 < a < n$, and so $2 \leq a < n$ by the discreteness clause of Proposition 2.1.2. By the hypothesis, a has a prime factor p, say $a = lp$ with $l \in \mathbb{Z}$. Then $n = ka = (kl)p$, with $kl \in \mathbb{Z}$ by Proposition 2.1.2 (a), so $p \mid n$.

In both cases n has a prime factor. By Theorem 2.2.2, every integer $n \geq 2$ has one. This proves the theorem.

■

The hypothesis was used at a, which can be far below $n - 1$: for $n = 91 = 7 \cdot 13$ it is used at 7 or at 13. Ordinary induction, which offers only $n - 1$, would have nothing to say about 91 from

90.

2.2.5 A gallery of broken inductions

An induction proof has few moving parts: a property, a base case, a step, and a citation of the right principle. Each can fail, and each failure has a place in the proof where it can be pointed at. Two questions are kept apart throughout: is the conclusion true, and does the argument prove it? Each entry below names the part that breaks.

Example. All Numbers Are Equal

Here is a "theorem" and a "proof". Find the line that fails.

"Theorem." For every integer $n \geq 1$ and all real numbers $x_1, \ldots, x_n$, we have $x_1 = x_2 = \cdots = x_n$.

"Proof." For an integer $n \geq 1$, let $P(n)$ be the statement "for all real numbers $x_1, \ldots, x_n$, all the entries of the list $x_1, \ldots, x_n$ are equal". We use Theorem 2.2.1 with $n_0 = 1$.

(1) *Base case.* A list x_1 of one number has only one entry, so all its entries are equal: $P(1)$ holds.

(2) *Step.* Let $n \geq 1$ be an integer, suppose $P(n)$, and let $x_1, \ldots, x_{n+1}$ be real numbers.

(3) The list $x_1, \ldots, x_n$ has n entries, so by $P(n)$ its entries are all equal.

(4) The list $x_2, \ldots, x_{n+1}$ has n entries, so by $P(n)$ its entries are all equal.

(5) The entry x_2 lies in both lists, so every entry of either list equals x_2.

(6) Hence $x_1 = x_2 = \cdots = x_{n+1}$, which is $P(n+1)$. By Theorem 2.2.1, $P(n)$ holds for every $n \geq 1$.

Solution. Is the conclusion true? No: the list $x_1 = 0$, $x_2 = 1$ has unequal entries, so $P(2)$ is false.

Does the argument prove it? No, and the failing line is (5) at $n = 1$. Then the two lists of lines (3) and (4) are x_1 and x_2, one entry each, and x_2 is not in the first. They share an entry exactly when the first list, $x_1, \ldots, x_n$, contains x_2, that is, when $n \geq 2$. In the terms of Logic and Proof, Example (What is not allowed), line (5) cites a "fact" that is false in the case at hand: entry (N9).

Everything else is correct. The base case (1) is true. For every $n \geq 2$ the step (2)–(6) is valid: if all lists of n reals had equal entries, so would all lists of $n+1$. So the induction fails at exactly one transition, from 1 to 2, and the valid transitions from 2 on carry nothing, because $P(2)$ is false and every later $P(n)$ with it. A counterexample to the illegal step, as opposed to the conclusion: $n = 1$, $x_1 = 0$, $x_2 = 1$, where lines (3) and (4) hold and (5) does not.

statement	true?	proved by the argument?
$P(1)$	yes	yes, line (1)
$P(1) \Rightarrow P(2)$	no	no: line (5) fails
$P(n) \Rightarrow P(n+1)$ for $n \geq 2$	yes	yes, lines (2)–(6)
$P(n)$ for every $n \geq 1$	no	no

This is the failure that *Logic and Proof*, Chapter 4's warning about $2^n \geq n^2$ foreshadowed: a step that holds only from some point on, with a gap at the first transition. A step must be proved for **every** $n \geq n_0$, and the place to look for a gap is the smallest n, where the objects the step talks about are smallest.

The other failures are quicker to state.

The missing base case. "$n = n+1$ for every $n \in \mathbb{N}$." The step is valid: if $n = n+1$, adding 1 to both sides gives $n+1 = n+2$. But $P(0)$, "$0 = 1$", is false, and so is every $P(n)$. The step is a true implication between false statements, and an induction with no true base proves nothing.

The step run backwards. Claim: $n^2 \geq 2n$ for every integer $n \geq 2$. "Step: $(n+1)^2 \geq 2(n+1)$ gives $n^2+2n+1 \geq 2n+2$, so $n^2 \geq 1$, which is true." This starts from $P(n+1)$ and ends at a true statement, so it shows only that $P(n+1)$ implies something true, which every statement does (N5). Here each line can be reversed, and written forwards ($n^2 \geq 1$, so $(n+1)^2 = n^2+2n+1 \geq 2n+2$) it is a valid step, though one that never uses $P(n)$. In general a backward chain cannot be reversed: from the false $1 = -1$, squaring gives the true $1 = 1$.

The hypothesis used out of range. A strong induction from a base n_0 may use $P(k)$ only for $n_0 \leq k < n$. A step that writes n in terms of $n-3$ needs $n-3 \geq n_0$, and for the first few n that fails. Logic and Proof, Example (Threes and fives) handled this correctly, with three base cases; the exit check C1 below is a proof that did not.

The claim too weak to carry its own step. Sometimes the statement is true and the base case holds, but the inductive step cannot be completed, because the hypothesis gives too little. The repair is to prove **more**. Section 2.3 shows a sum bounded by 2 whose own step will not go through, and which a stronger bound carries.

Warning. The induction hypothesis is "$P(n)$" for one fixed but arbitrary n: the assumption of the $\to$I box inside the $\forall$I box of the step (Logic and Proof, Definition 5.4.1). A step that begins "assume that $P(n)$ holds for every n" assumes the conclusion of the theorem, and whatever follows is circular: entry (N9) of Logic and Proof, Example (What is not allowed). The witness is a "for every n" in the assumption that binds the induction variable n itself; it should not be there. A quantifier over another variable is part of the statement and may stay: "for every k with $n_0 \leq k < n$" in strong induction, or the "for every n" inside $P(m)$ in the proof of Lemma 2.1.1 (d), where the induction is on m.

Quick check. A proof that $n^2 \leq 2^n$ for every integer $n \geq 4$ checks $n = 4$ and proves the step $2n^2 \geq (n+1)^2$ for $n \geq 3$. Is it complete? A second proof of "$n^2 \leq 2^n$ for every $n \in \mathbb{N}$" uses base 0 and the same step. Which entry of the gallery does it commit?

Solution. The first is complete: $16 \leq 16$, and the step is proved for every $n \geq 4$. The second has a true base but a step proved only from 3 on, so the transitions $0 \to 1$, $1 \to 2$, $2 \to 3$ are unproved: a step valid only from some point on, as in Example (All Numbers Are Equal). Its conclusion is false at 3 ($9 > 8$). This is *Logic and Proof*, Chapter 4's warning about $2^n \geq n^2$ (recalled at the end of Example (All Numbers Are Equal)), made precise at the level of the step.

2.2.6 Exercises

2.2.6.1 A. Check your understanding

Exercise. A1

(a) For each claim, name the form of proof that fits it most naturally (ordinary induction from 0, induction from another base, strong induction from a base with several base cases, or a smallest counterexample), and say in one clause why. Do not prove the claims. (i) $6 \mid 7^n - 1$ for every $n \in \mathbb{N}$. (ii) $2^n > n^2$ for every integer $n \geq 5$. (iii) Every integer $n \geq 12$ is $3a + 7b$ for some integers $a, b \geq 0$. (iv) There are no $m, n \in \mathbb{Z}_{>0}$ with $n^2 = 2m^2$.

(b) Negate "every integer $n \geq 2$ has a prime factor", and say what a smallest counterexample to it would be.

(c) In Example (All Numbers Are Equal), what is the smallest n for which the two lists $x_1, \ldots, x_n$ and $x_2, \ldots, x_{n+1}$ of lines (3) and (4) share an entry?

(d) *Find the error.* Here is a "proof" that $a^n = 1$ for every real $a \neq 0$ and every $n \in \mathbb{N}$; the powers a^n, $a^0 = 1$ and $a^{-1} = 1/a$ have their school meaning (Section 2.3 defines a^n for $n \in \mathbb{N}$ only, so negative exponents lie outside that definition). "Fix $a \neq 0$. Base: $a^0 = 1$. Step: let $n \in \mathbb{N}$ and suppose $a^k = 1$ for every $k \in \mathbb{N}$ with $k \leq n$. Then $a^{n+1} = a^n \cdot a^n / a^{n-1} = 1 \cdot 1/1 = 1$." The conclusion is false (take $a = 2$, $n = 1$). Which transition fails, and why?

Solution. *(a)* (i) Ordinary induction from 0: the step takes out one factor 7 and leaves a multiple of 6, as in the example $7 \mid 9^n - 2^n$ in the subsection on finding the step. (ii) Induction from base 5 (Theorem 2.2.1): the claim fails at $n = 2, 3, 4$, so it cannot start at 0, and the step $2^{n+1} = 2 \cdot 2^n > 2n^2 \geq (n+1)^2$ works for $n \geq 5$. (iii) Strong induction from base 12 with three base cases $12 = 3 \cdot 4$, $13 = 3 \cdot 2 + 7$, $14 = 7 \cdot 2$: the step reaches back three, from n to $n - 3$. (iv) A smallest counterexample: in a solution (m, n) with least n, n^2 is even, so $n = 2n'$ is even (Logic and Proof, Theorem 2.1.3), and then $m^2 = 2n'^2$, so (n', m) is a solution ($n' = n/2 > 0$) whose second entry m is smaller than n, since $n^2 = 2m^2 > m^2$ and $m, n > 0$. (Strong induction would also do; the forms are interchangeable, and the answers above name the natural fit.)

(b) The negation is: there is an integer $n \geq 2$ with no prime factor. A smallest counterexample would be an integer $m \geq 2$ with no prime factor such that every integer k with $2 \leq k < m$ has one.

(c) $n = 2$. For $n = 1$ the lists are x_1 and x_2; for $n \geq 2$ both contain x_2.

(d) The transition from 0 to 1 fails. At $n = 0$ the step writes $a^1 = a^0 \cdot a^0 / a^{-1}$ and uses $a^{-1} = 1$, which is "$P(-1)$"; but the hypothesis covers only $k \in \mathbb{N}$ with $k \leq 0$, that is, $k = 0$, and $-1 \notin \mathbb{N}$. In fact $a^{-1} = 1/a \neq 1$ unless $a = 1$. The base case $a^0 = 1$ is true, and every transition from $n \geq 1$ on is valid, since then $n - 1 \in \mathbb{N}$ and $n - 1 \leq n$, and $a^n a^n / a^{n-1} = a^{n+1}$ for $n \geq 1$. As in Example (All Numbers Are Equal), the valid transitions carry nothing, because $P(1)$ is already false.

2.2.6.2 B. Practice

Exercise. B1

Prove that $3 \mid n^3 + 2n$ for every $n \in \mathbb{N}$.

Solution. For $n \in \mathbb{N}$, let $P(n)$ be "there is $k \in \mathbb{Z}$ with $n^3 + 2n = 3k$". *Base case:* $0^3 + 2 \cdot 0 = 0 = 3 \cdot 0$. *Step:* let $n \in \mathbb{N}$ and suppose $n^3 + 2n = 3k$ with $k \in \mathbb{Z}$. Expanding the cube,

$$(n+1)^3 + 2(n+1) = (n^3 + 2n) + 3(n^2 + n + 1) = 3(k + n^2 + n + 1),$$

and $k + n^2 + n + 1 \in \mathbb{Z}$ by Proposition 2.1.2 (a). So $P(n+1)$ holds. By Logic and Proof, Axiom 4.2.1, $3 \mid n^3 + 2n$ for every $n \in \mathbb{N}$. The step is the move of Example (Method: finding $P(n)$ inside $P(n+1)$) with no power of the form a^n: the old expression plus a new piece that is visibly a multiple of 3.

Exercise. B2: Products of primes, used later

An integer is a **product of primes** if it equals $p_1 p_2 \cdots p_k$ for some $k \geq 1$ and primes $p_1, \ldots, p_k$ (a single prime counts, with $k = 1$). Here $p_1 p_2 \cdots p_k$ has its school meaning, and multiplying two such products gives the product of the joined list; Section 2.3 defines finite products (Definition 2.3.1). Here is a proof that every integer $n \geq 2$ is a product of primes, with its last step blank. *Name the move, then complete it.*

Suppose not. Then the set F of integers $n \geq 2$ that are not products of primes is non-empty and has the integer lower bound 2, so it has a least element m by Corollary 2.1.5. Since a prime is a product of primes, m is not prime; as $m \geq 2$, it has a positive divisor $a \notin \{1, m\}$, and $m = ab$ with $b \in \mathbb{Z}$. As in the proof of Theorem 2.2.5, $b > 0$ and $2 \leq a < m$. Since $a < m = ab$ and $a > 0$, we get $b > 1$, so $b \geq 2$ by the discreteness clause of Proposition 2.1.2; and since $a \geq 2$, $b < 2b \leq ab = m$. So $2 \leq a < m$ and $2 \leq b < m$, and as m is the least element of F, neither a nor b lies in F: both are products of primes.

...

Solution. The move is the **smallest counterexample**, and the blank is the contradiction: the least failure m turns out not to be a failure, because its smaller factors are not failures (compare Lemma 2.2.4, where the contradiction is a smaller element of F). Write $a = p_1 \cdots p_k$ and $b = p'_1 \cdots p'_l$ with primes p_i, p'_j. Then

$$m = ab = p_1 \cdots p_k \, p'_1 \cdots p'_l$$

is a product of primes, which contradicts $m \in F$. Hence F is empty, and every integer $n \geq 2$ is a product of primes.

Exercise. B3, used later

(a) Find the quotient and remainder of Theorem 2.2.3 for $a = 17$, $n = 5$, and for $a = -17$, $n = 5$.

(b) Prove that the square of an odd integer leaves remainder 1 on division by 8.

(c) Prove that if $2 \mid n$ and $3 \mid n$, then $6 \mid n$, for every integer n.

Hint for (c): Theorem 2.2.3, dividing by 3.

Solution. *(a)* $17 = 5 \cdot 3 + 2$, so $q = 3$, $r = 2$. And $-17 = 5 \cdot (-4) + 3$, so $q = -4$, $r = 3$; in both cases $0 \leq r < 5$, so by uniqueness these are the quotient and remainder. (Not $-17 = 5 \cdot (-3) - 2$: a remainder is never negative.)

(b) Let $x = 2k + 1$ with $k \in \mathbb{Z}$. Then $x^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$. By Theorem 2.2.3 with $n = 2$, $k = 2j$ or $k = 2j + 1$ with $j \in \mathbb{Z}$. In the first case $k(k + 1) = 2 \cdot j(2j + 1)$; in the second, $k(k + 1) = (2j + 1)(2j + 2) = 2(2j + 1)(j + 1)$. Either way $k(k + 1) = 2t$ with $t \in \mathbb{Z}$, so $x^2 = 8t + 1$. Since $0 \leq 1 < 8$, the uniqueness in Theorem 2.2.3 says that the remainder of x^2 on division by 8 is 1.

(c) Let $n = 2a$ with $a \in \mathbb{Z}$, and divide a by 3: $a = 3q + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < 3$, so $r \in \{0, 1, 2\}$ by discreteness. Then $n = 6q + 2r$. Since $3 \mid n$, say $n = 3s$ with $s \in \mathbb{Z}$, we get $2r = 3(s - 2q)$, so $3 \mid 2r$, where $2r \in \{0, 2, 4\}$. But $2 = 3 \cdot 0 + 2$ and $4 = 3 \cdot 1 + 1$ have non-zero remainders on division by 3, while a multiple $3t = 3t + 0$ has remainder 0; by uniqueness, neither 2 nor 4 is a multiple of 3. So $2r = 0$, $r = 0$, and $n = 6q$: $6 \mid n$.

Exercise. B4: Prove or disprove

Prove each true statement and refute each false one with a counterexample. Powers and finite sums have their school meaning (Section 2.3 defines them), as in the example $7 \mid 9^n - 2^n$.

(a) $3 \mid 2^{2n+1} + 1$ for every $n \in \mathbb{N}$.
(b) $2^n \geq n^3$ for every integer $n \geq 9$.
(c) $1 + 4 + 7 + \cdots + (3n + 1) = (n + 1)(3n + 2)/2$ for every $n \in \mathbb{N}$.
(d) Every integer $n \geq 10$ is $3a + 7b$ for some integers $a, b \geq 0$.
(e) $5^n \geq 4^n + 3^n$ for every integer $n \geq 2$.
(f) $n^2 + 1$ is prime for every even integer $n \geq 2$.

Solution.

(a) **True.** By Logic and Proof, Axiom 4.2.1. Base: $2^1 + 1 = 3 = 3 \cdot 1$. Step: if $2^{2n+1} + 1 = 3k$ with $k \in \mathbb{Z}$, then

$$2^{2n+3} + 1 = 4 \cdot 2^{2n+1} + 1 = 4(2^{2n+1} + 1) - 3 = 3(4k - 1),$$

and $4k - 1 \in \mathbb{Z}$.

(b) **False.** At $n = 9$: $2^9 = 512 < 729 = 9^3$. (The inequality holds from 10 on: $2^{10} = 1024 \geq 1000$, and $2n^3 \geq (n + 1)^3$ for $n \geq 10$. The claim fails only at its base.)

(c) **True.** By Logic and Proof, Axiom 4.2.1. Base $n = 0$: $1 = 1 \cdot 2/2$. Step: split off the last term. If the sum up to $3n + 1$ is $(n + 1)(3n + 2)/2$, the sum up to $3(n + 1) + 1 = 3n + 4$ is

$$\frac{(n + 1)(3n + 2)}{2} + (3n + 4) = \frac{3n^2 + 11n + 10}{2} = \frac{(n + 2)(3n + 5)}{2},$$

which is the formula at $n + 1$.

(d) **False.** Take $n = 11$. With $b = 0$ or $b = 1$ what is left, $11 - 7b$, is 11 or 4, and neither is a multiple of 3: $11 = 3 \cdot 3 + 2$ and $4 = 3 \cdot 1 + 1$ have non-zero remainders, so by the uniqueness in Theorem 2.2.3 they are not of the form $3a + 0$. With $b \geq 2$, $11 - 7b < 0$, so $a < 0$.

(e) **True.** By Theorem 2.2.1 with base 2. Base: $25 \geq 16 + 9$. Step: let $n \geq 2$ with $5^n \geq 4^n + 3^n$. Then

$$5^{n+1} = 5 \cdot 5^n \geq 5 \cdot 4^n + 5 \cdot 3^n \geq 4 \cdot 4^n + 3 \cdot 3^n = 4^{n+1} + 3^{n+1}.$$

(The step works for every n, but the inequality fails at $n = 1$, $5 < 7$, and at $n = 0$, $1 < 2$, and the claim is asserted only from 2, so the base is 2.)

(f) **False.** Take $n = 8$: $8^2 + 1 = 65 = 5 \cdot 13$, with the positive divisor $5 \notin \{1, 65\}$. For $n = 2, 4, 6$ the values 5, 17, 37 are prime: three successes, then a failure (N1).

2.2.6.3 C. Going deeper

Exercise. C1: Exit check: a flawed induction

Here is a claim and a "proof".

Claim. Every integer $n \geq 18$ is $4a + 7b$ for some integers $a, b \geq 0$.

(1) For an integer $n \geq 18$, let $P(n)$ be "$n = 4a + 7b$ for some integers $a, b \geq 0$". We use strong induction from base 18 (Theorem 2.2.2).

(2) *Base case.* $18 = 4 \cdot 1 + 7 \cdot 2$, so $P(18)$ holds.

(3) *Step.* Let $n \geq 18$ be an integer, and suppose $P(k)$ holds for every integer k with $18 \leq k \leq n$.

(4) Write $n + 1 = (n - 3) + 4$.

(5) Since $n - 3 < n$, the induction hypothesis gives $n - 3 = 4a + 7b$ with integers $a, b \geq 0$.

(6) Then $n + 1 = 4(a + 1) + 7b$, with $a + 1 \geq 0$ and $b \geq 0$, so $P(n + 1)$ holds.

(7) By Theorem 2.2.2, $P(n)$ holds for every integer $n \geq 18$.

Answer each question. (i) Is the claim true? (ii) Does the argument prove it? (iii) Which line fails, and for which n? (iv) Which rule does that line break? (v) Give a counterexample to the failing step, not merely to some conclusion. (vi) Repair the proof.

Solution. (i) The claim is **true**. Directly,

$$18 = 4 \cdot 1 + 7 \cdot 2, \quad 19 = 4 \cdot 3 + 7, \quad 20 = 4 \cdot 5, \quad 21 = 7 \cdot 3,$$

and from these four the repaired induction in (vi) reaches every larger integer.

(ii) The argument does **not** prove it, although its conclusion is true.

(iii) Line (5) fails for $n = 18$, 19 and 20. There $n - 3$ is 15, 16, 17, all below 18, and the induction hypothesis says nothing about them. For $n \geq 21$, $18 \leq n - 3 < n$, and line (5) is correct. Lines (1)–(4), (6) and (7) are correct. Line (7) needs one remark, because the step is written from n to $n + 1$ and not in the theorem's own form. At $N = 18$ the theorem's hypothesis has a vacuous "if" part, so it asks for $P(18)$ outright, which is line (2). At an integer $N \geq 19$, put $n = N - 1 \geq 18$. By the discreteness clause of Proposition 2.1.2, the

integers k with $18 \le k < N$ are exactly those with $18 \le k \le n$, so lines (3)–(6), were they valid for every $n \ge 18$, would prove the hypothesis at N.

(iv) Line (5) applies ∀E to the hypothesis "for every integer k with $18 \le k \le n$, $P(k)$" at $k = n - 3$. That is a bounded quantifier, and its elimination needs the line "$18 \le n - 3$" (Logic and Proof, Proposition 6.1.1); for $n \le 20$ that line is false. The proof checked only half of the bound, $n - 3 < n$.

(v) Run the same argument with base $14 = 7 \cdot 2$: it "proves" that every integer $n \ge 14$ is $4a+7b$. That conclusion is false at 17: with $b = 0, 1, 2$ the remainder $17-7b$ is $17, 10, 3$, none a multiple of 4, and $b \ge 3$ makes it negative. The step that breaks is line (5) at $n = 16$: it takes $P(13)$ from the hypothesis, but $13 < 14$ is outside it, and 13 is not of the form (13 and 6 are not multiples of 4). At $n = 16$ the induction hypothesis is true ($14 = 7\cdot 2$, $15 = 4\cdot 2+7$, $16 = 4 \cdot 4$), and the step concludes the false $P(17)$. So line (5) is an illegal step, not merely an unlucky one.

(vi) Take four base cases, $18, 19, 20, 21$, as in (i), and run the step only for $n \ge 21$, where $n - 3 \ge 18$. In the form of Theorem 2.2.2: for $n \in \{18, 19, 20, 21\}$, $P(n)$ holds directly; for $n \ge 22$, $n-4 \ge 18$ and $n-4 < n$, so the hypothesis gives $n-4 = 4a+7b$ and $n = 4(a+1)+7b$.

Marking scheme. (10 points) - 2: judges the conclusion **true**, with the small cases 18, 19, 20, 21 written as $4a + 7b$. - 3: identifies the failing line exactly: the appeal to the hypothesis for $n - 3$, for $n = 18, 19, 20$. - 2: states the reason as a hypothesis used outside its range (∀E at a k with $k < 18$). - 2: gives a counterexample **to the step**: the same step carrying a true statement to a false one (for example, base 14 and the failure at 17), not merely a false conclusion. - 1: gives a correct repair (four base cases, or any equivalent). Fatal errors (0 for the item): calling the conclusion false; blaming the base case.

Exercise. C2: Lowest terms, used later

Prove that every rational number can be written as p/q with $p \in \mathbb{Z}$, $q \in \mathbb{Z}_{>0}$, and no common divisor $d \ge 2$ of p and q: there is no integer $d \ge 2$ with $d \mid p$ and $d \mid q$.

Solution (Hint 1). Follow the proof of Lemma 2.2.4, step by step.

Solution (Hint 2). Suppose $r \in \mathbb{Q}$ has no such representation, and let m be the least element of $F := \{q \in \mathbb{Z}_{>0} : r = p/q \text{ for some } p \in \mathbb{Z}\}$.

Solution. Fix $r \in \mathbb{Q}$, and suppose that r has no representation of the required kind. Let F be as in Hint 2. By the definition of $\mathbb{Q}$, F is non-empty, and $F \subseteq \mathbb{Z}_{>0} \subseteq \mathbb{N}$, so by Theorem 2.1.3 it has a least element m. Write $r = p/m$ with $p \in \mathbb{Z}$.

By the supposition, this representation fails: there is an integer $d \ge 2$ with $d \mid p$ and $d \mid m$, say $p = dp'$ and $m = dm'$ with $p', m' \in \mathbb{Z}$. Since $m > 0$ and $d > 0$, $m' = m/d > 0$, so $m' \in \mathbb{Z}_{>0}$ by Proposition 2.1.2 (b). Then $r = dp'/(dm') = p'/m'$, so $m' \in F$. And $m = dm' \ge 2m' > m'$, since $d \ge 2$ and $m' > 0$. So m' is an element of F smaller than its least element, a contradiction. Hence r has a representation p/q with no common divisor

$d \geq 2$.

The statement contains Lemma 2.2.4, since $d = 2$ is one of the excluded common divisors. The only change in the proof is the size of the step down: $m' = m/d$ instead of $m/2$, and $d \geq 2$ is what makes it a step **down**.

Marking scheme. (10 points) - 2: sets up the smallest counterexample: fixes r, supposes no good representation, and defines the set of denominators. - 2: shows that set is a non-empty subset of $\mathbb{N}$ and takes its least element by Theorem 2.1.3. - 3: extracts the common divisor $d \geq 2$ and writes the reduced representation p'/m', checking $m' \in \mathbb{Z}_{>0}$. - 2: shows $m' < m$, using $d \geq 2$ and $m' > 0$. - 1: concludes, with the contradiction to the choice of m. A strong induction on the denominator earns the same points step for step. Fatal errors (0 for the step): taking a least element of a set not shown to lie in $\mathbb{N}$; dividing by d without $d \neq 0$.

Exercise. C3: Smallest, not largest

(a) Prove that a set $A \subseteq \mathbb{R}$ has at most one least element.

(b) Deduce that a claim "$P(n)$ for every $n \in \mathbb{N}$" that is false has exactly one smallest counterexample.

(c) Show that a false claim about $\mathbb{N}$ need not have a **largest** counterexample, by examining the claim "$n < 5$ for every $n \in \mathbb{N}$".

Solution. *(a)* Let m and m' be least elements of A. Since $m' \in A$ and m is least, $m \leq m'$; since $m \in A$ and m' is least, $m' \leq m$. Hence $m = m'$.

(b) The smallest counterexamples are the least elements of the set $F := \{n \in \mathbb{N} : P(n) \text{ is false}\}$. The claim is false, so F is non-empty, and Theorem 2.1.3 gives a least element. By (a), there is only one.

(c) The claim is false, and its counterexamples form $F = \{n \in \mathbb{N} : n \geq 5\}$, which is non-empty. It has no greatest element: for every $n \in F$, also $n + 1 \in \mathbb{N}$ by ($\mathbb{N}$S), and $n + 1 \geq 5$, so $n + 1 \in F$ and $n + 1 > n$. So the claim has a smallest counterexample, 5, and no largest one. Well-ordering has no upward twin in $\mathbb{N}$: a non-empty subset of $\mathbb{N}$ has a greatest element when it is bounded above (Exercise (C1: A greatest element from a least upper bound)), and not in general.

2.3 Definition by Recursion

Since school we have defined powers by two clauses: $u^0 = 1$, and $u^{n+1} = u^n u$. Sums $a_1 + \cdots + a_n$, factorials and many sequences are defined the same way: a starting value, and a rule that produces the next value from the last. *Logic and Proof*, Chapter 4 used induction to prove facts about such objects, such as $3^n \geq 2n + 1$ in Logic and Proof, Example (An inequality by induction). But induction proves facts about a function that **already exists**, and here the function is what we want to obtain. This section proves that two such clauses always define exactly one function on $\mathbb{N}$, and then uses the theorem to define sums, products and powers properly and to prove their first laws.

2.3.1 Definitions that define something

Logic and Proof, Chapter 4 met the same question for formulas. A recursive definition on formulas gives a value for each atom and a rule for each way of building a compound formula, and Logic and Proof, Theorem 4.3.4 showed that such clauses define exactly one function, because unique readability leaves no choice of clause. On $\mathbb{N}$ the clauses are simpler: one starting value at 0, and one rule for passing from n to $n+1$. What we want to prove is this.

A starting value and a rule for the next value determine exactly one sequence.

Theorem 2.3.1. Recursion Theorem

Let X be a set, let $a \in X$, and let $g\colon \mathbb{N} \times X \to X$ be a function. Then there is **exactly one** function $f\colon \mathbb{N} \to X$ such that

$$f(0) = a \quad \text{and} \quad f(n+1) = g(n, f(n)) \quad \text{for every } n \in \mathbb{N}.$$

In words: a is the starting value, and g is the rule that turns the stage n and the current value $f(n)$ into the next value. The rule may look at n as well as at $f(n)$: the factorial needs this, since $(n+1)! = (n+1)\cdot n!$ is $g(n,x) = (n+1)x$ at $x = n!$. The hypothesis that g maps into X is what lets the rule be applied again at the next stage. The conclusion has two halves: **existence** (some f obeys the two equations) and **uniqueness** (no two different functions do).

Idea. Uniqueness is an ordinary induction: two solutions agree at 0, and if they agree at n, the second equation makes them agree at $n+1$. Existence is harder, because induction cannot produce f; it can only prove statements. So we prove by induction a statement about finite pieces of f. The roadmap:

① **Uniqueness**, by induction on n.

② **Claim:** for every $n \in \mathbb{N}$ there is exactly one function on $\{0, \ldots, n\}$ obeying the two equations wherever they make sense (a **partial solution**). Its graph is the graph of the previous one with one pair added.

③ **Glue:** collect the graphs of all partial solutions in one set $\mathcal{S}$ and take the union. The partial solutions agree where they overlap, so the union is the graph of a function on all of $\mathbb{N}$, and that function obeys the equations.

Before reading on: self-explain the Claim's inductive step.

Proof. For $n \in \mathbb{N}$, the set $\{0, \ldots, n\} = \{k \in \mathbb{N} : k \leq n\}$ of Section 2.1 contains 0, since $0 \leq n$ by Lemma 2.1.1 (a). Call a function $h\colon \{0, \ldots, n\} \to X$ a **partial solution up to** n if $h(0) = a$ and $h(k+1) = g(k, h(k))$ for every $k \in \mathbb{N}$ with $k+1 \leq n$. (For such k, both k and $k+1$ lie in $\{0, \ldots, n\}$, so the equation makes sense.)

Step 1 (uniqueness). Let $f, f'\colon \mathbb{N} \to X$ both satisfy the two equations, and let $P(n)$ be "$f(n) = f'(n)$". $P(0)$ holds, since $f(0) = a = f'(0)$. If $P(n)$ holds, then

$$f(n+1) = g(n, f(n)) = g(n, f'(n)) = f'(n+1),$$

so $P(n+1)$ holds. By Logic and Proof, Axiom 4.2.1, $f(n) = f'(n)$ for every $n \in \mathbb{N}$. The two

functions have the same domain and the same codomain, so $f = f'$ by Proposition 1.5.1.

Step 2.

Claim. For every $n \in \mathbb{N}$ there is exactly one partial solution up to n.

Proof of Claim. We use Logic and Proof, Axiom 4.2.1 on n.

Base case. By Lemma 2.1.1 (a), every $k \in \mathbb{N}$ has $k \geq 0$, so $k \leq 0$ holds only for $k = 0$, and $\{0, \ldots, 0\} = \{0\}$. The graph $\{(0, a)\}$ with codomain X is a function on $\{0\}$, since $a \in X$: the input 0 has the one output a. It is a partial solution up to 0: its value at 0 is a, and the second condition is vacuous, because $k + 1 \geq 1 > 0$ for every $k \in \mathbb{N}$. Any partial solution up to 0 has value a at 0, so it equals this one by Proposition 1.5.1.

Inductive step. Let $n \in \mathbb{N}$, and suppose there is exactly one partial solution up to n; call it f_n, with graph G_n. Let

$$G_{n+1} \coloneqq G_n \cup \{(n + 1,\ g(n, f_n(n)))\}.$$

First, $\{0, \ldots, n + 1\} = \{0, \ldots, n\} \cup \{n + 1\}$: a natural number $k \leq n + 1$ is either $n + 1$ or less than $n + 1$, and then $k \leq n$, since no natural number lies strictly between n and $n + 1$ (Lemma 2.1.1 (e)). Also $n + 1 \notin \{0, \ldots, n\}$, since $n + 1 > n$.

We check the clauses of Definition 1.5.1 for G_{n+1} on $\{0, \ldots, n+1\}$ with codomain X. Every pair of G_{n+1} lies in $\{0, \ldots, n + 1\} \times X$, because g takes values in X. (Fn1): an input $k \leq n$ has the output $f_n(k)$ in G_n, and the input $n+1$ has the output $g(n, f_n(n))$. (Fn2): the pairs with first coordinate $k \leq n$ all lie in G_n, since the added pair has first coordinate $n + 1 \neq k$, and G_n satisfies (Fn2); the only pair with first coordinate $n + 1$ is the added one, since the first coordinates in G_n are at most n. So $f_{n+1} \coloneqq (G_{n+1}, X)$ is a function on $\{0, \ldots, n + 1\}$, and it agrees with f_n on $\{0, \ldots, n\}$.

It is a partial solution up to $n+1$. Its value at 0 is $f_n(0) = a$. Let $k \in \mathbb{N}$ with $k+1 \leq n+1$, so $k \leq n$. If $k < n$, then $k + 1 \leq n$ by Lemma 2.1.1 (e), and $f_{n+1}(k + 1) = f_n(k + 1) = g(k, f_n(k)) = g(k, f_{n+1}(k))$, because f_n is a partial solution. If $k = n$, then $f_{n+1}(n + 1) = g(n, f_n(n)) = g(n, f_{n+1}(n))$ by the choice of the added pair.

It is the only one. Let h be a partial solution up to $n + 1$. Its restriction $h|_{\{0,\ldots,n\}}$ (Section 1.5) is a partial solution up to n, because the conditions on it are among the conditions on h. By the induction hypothesis it is f_n. So $h(k) = f_n(k) = f_{n+1}(k)$ for $k \leq n$, and

$$h(n + 1) = g(n, h(n)) = g(n, f_n(n)) = f_{n+1}(n + 1).$$

By Proposition 1.5.1, $h = f_{n+1}$. This proves the claim.

■

For each $n \in \mathbb{N}$, let f_n be the partial solution up to n, and G_n its graph. If $m \leq n$, then $\{0, \ldots, m\} \subseteq \{0, \ldots, n\}$, and the restriction of f_n to $\{0, \ldots, m\}$ is a partial solution up to m, so by the claim it is f_m. In terms of graphs,

$$G_m = G_n \cap (\{0, \ldots, m\} \times X) \subseteq G_n \qquad (m \leq n).$$

Step 3 (existence). Let

$$\mathcal{S} \coloneqq \{G \in \mathcal{P}(\mathbb{N} \times X) : G \text{ is the graph of a partial solution up to some } n \in \mathbb{N}\},$$

a set by Definition 1.2.3 and Definition 1.3.2. By the claim, the elements of $\mathcal{S}$ are exactly the graphs G_n. Let $F \coloneqq \bigcup \mathcal{S}$ (Definition 1.3.4), so a pair lies in F if and only if it lies in some G_n; in particular $F \subseteq \mathbb{N} \times X$. We check the clauses of Definition 1.5.1 for F.

(Fn1): for $n \in \mathbb{N}$, the pair $(n, f_n(n))$ lies in $G_n \in \mathcal{S}$, hence in F.

(Fn2): let $(k, y) \in F$ and $(k, y') \in F$, say $(k, y) \in G_m$ and $(k, y') \in G_n$. If $m \leq n$, then $G_m \subseteq G_n$, so both pairs lie in G_n, and $y = y'$ because G_n satisfies (Fn2). If $n < m$, the same argument with m and n exchanged gives $y = y'$.

So $f \coloneqq (F, X)$ is a function $\mathbb{N} \to X$. For $m \geq n$, the pair $(n, f_m(n))$ lies in $G_m \subseteq F$, so $f(n) = f_m(n)$. Hence $f(0) = f_0(0) = a$, and for every $n \in \mathbb{N}$,

$$f(n+1) = f_{n+1}(n+1) = g(n, f_{n+1}(n)) = g(n, f(n)),$$

where the middle equation holds because f_{n+1} is a partial solution. This proves existence, and with Step 1, the theorem.

■

The starting value was used in both halves: Step 1 needs $f(0) = f'(0)$ as its base case, and Step 2 needs it to fix the first partial solution. The set $\mathcal{S}$ is cut out of a power set by a condition, so no family $n \mapsto f_n$ had to be formed before the union was taken. No choice is made anywhere: at every stage the claim leaves exactly one candidate. From now on, a definition of the form "$f(0) \coloneqq a$, $f(n+1) \coloneqq g(n, f(n))$" is legitimate whenever $a \in X$ and g is a function $\mathbb{N} \times X \to X$, and we say that f is **defined by recursion**.

Remark. Because the rule may depend on n, the theorem also covers constructions in which the step uses outside data indexed by n. *Analysis on the Real Line*, Chapter 1 builds closed intervals I_{n+1} from I_n and the $(n+1)$-st number of a given list in exactly this way, with no choice principle involved. The values may be sets as well as numbers. With $X = \mathcal{P}(\mathbb{N})$, $A_0 \coloneqq \mathbb{N}$ and $A_{n+1} \coloneqq A_n \setminus \{n\}$ define a sequence of sets of the kind Section 1.3 promised, and an induction that follows the same two clauses shows $A_n = \{k \in \mathbb{N} : k \geq n\}$: the base is Lemma 2.1.1 (a), and the step removes n from $\{k : k \geq n\}$, leaving $\{k : k > n\} = \{k : k \geq n+1\}$ by Lemma 2.1.1 (e).

Quick check. Name X, a and g for the sequence $1, 3, 7, 15, \ldots$, in which each term is twice the previous one plus one.

Solution. $X = \mathbb{N}$ (or $\mathbb{R}$), $a = 1$ and $g(n, x) = 2x+1$; the rule does not use n. Since $2x+1 \in \mathbb{N}$ for $x \in \mathbb{N}$ (Lemma 2.1.1 (b)), g is a function $\mathbb{N} \times X \to X$, so Theorem 2.3.1 applies. The clauses give $f(1) = 2 \cdot 1 + 1 = 3$, $f(2) = 7$, $f(3) = 15$, as listed.

2.3.2 Starting elsewhere, looking two steps back

Two variants come up constantly. Sequences are often indexed from 1, as in Section 1.5, and some recursions use the two previous values. Both reduce to the theorem.

Corollary 2.3.2. Recursion from a Base

Let n_0 be an integer, $D \coloneqq \{n \in \mathbb{Z} : n \geq n_0\}$, X a set, $a \in X$, and $g\colon D \times X \to X$ a function. Then there is exactly one function $f\colon D \to X$ with $f(n_0) = a$ and $f(n+1) = g(n, f(n))$ for every $n \in D$.

Idea. Rename the index: $k = n - n_0$ turns D into $\mathbb{N}$ and the recursion on D into one on $\mathbb{N}$, where Theorem 2.3.1 applies.

Proof. For $k \in \mathbb{N}$, the number $n_0 + k$ is an integer (Proposition 2.1.2 (a)) and $n_0 + k \geq n_0$ (Lemma 2.1.1 (a)), so it lies in D. Conversely, for $n \in D$, $n - n_0$ is an integer (Proposition 2.1.2 (a)) and ≥ 0, so $n - n_0 \in \mathbb{N}$ by Proposition 2.1.2 (b). Define $g'\colon \mathbb{N} \times X \to X$ by $g'(k, x) \coloneqq g(n_0 + k, x)$. By Theorem 2.3.1 there is exactly one $f'\colon \mathbb{N} \to X$ with $f'(0) = a$ and $f'(k+1) = g(n_0 + k, f'(k))$ for every $k \in \mathbb{N}$.

Existence. Let $t\colon D \to \mathbb{N}$, $t(n) \coloneqq n - n_0$, and $f \coloneqq f' \circ t$ (Definition 1.5.2). Then $f(n_0) = f'(0) = a$, and for $n \in D$, with $k = n - n_0$,

$$f(n+1) = f'(k+1) = g(n_0 + k, f'(k)) = g(n, f(n)).$$

Uniqueness. If $\tilde{f}\colon D \to X$ also satisfies both equations, then $k \mapsto \tilde{f}(n_0 + k)$ satisfies the equations that define f', so it is f' by the uniqueness in Theorem 2.3.1. Hence $\tilde{f}(n) = f'(n - n_0) = f(n)$ for every $n \in D$, and $\tilde{f} = f$ by Proposition 1.5.1.

■

The renaming is the move that gave induction from a base (Theorem 2.2.1). The corollary covers every sequence $(a_n)_{n \geq 1}$ given by a first term and a rule, and *Analysis on the Real Line*, Chapter 1's intervals, which are listed from 1.

Corollary 2.3.3. Two-Step Recursion

Let X be a set, $a, b \in X$, and $h\colon \mathbb{N} \times (X \times X) \to X$ a function (Definition 1.4.2); write $h(n, x, y)$ for $h(n, (x, y))$. Then there is exactly one function $f\colon \mathbb{N} \to X$ with

$$f(0) = a, \quad f(1) = b, \quad f(n+2) = h(n, f(n), f(n+1)) \quad \text{for every } n \in \mathbb{N}.$$

Idea. A rule that looks two steps back is a rule that looks one step back at **pairs**. Carry the pair $(f(n), f(n+1))$ along: the next pair is $(f(n+1), f(n+2))$, and both of its entries are computed from the current pair.

Proof. Define $G\colon \mathbb{N} \times (X \times X) \to X \times X$ by $G(n, (x, y)) \coloneqq (y, h(n, x, y))$. By Theorem 2.3.1 with the set $X \times X$ and the starting value (a, b), there is exactly one $p\colon \mathbb{N} \to X \times X$ with $p(0) = (a, b)$ and $p(n+1) = G(n, p(n))$. Write $p(n) = (p_1(n), p_2(n))$. The equation $p(n+1) =$

$(p_2(n), h(n, p_1(n), p_2(n)))$ gives, by the characteristic property of pairs (Definition 1.4.1),

$$p_1(n+1) = p_2(n), \qquad p_2(n+1) = h(n, p_1(n), p_2(n)).$$

Let $f(n) := p_1(n)$. Then $f(0) = a$, $f(1) = p_2(0) = b$, and

$$f(n+2) = p_2(n+1) = h(n, p_1(n), p_2(n)) = h(n, f(n), f(n+1)).$$

For uniqueness, let f' satisfy the three equations, and let $p'(n) := (f'(n), f'(n+1))$. Then $p'(0) = (a, b)$ and

$$p'(n+1) = (f'(n+1),\ h(n, f'(n), f'(n+1))) = G(n, p'(n)),$$

so $p' = p$ by the uniqueness in Theorem 2.3.1, and $f'(n) = p_1(n) = f(n)$ for every n. By Proposition 1.5.1, $f' = f$.

■

Quick check. Do $a_0 = 1$, $a_1 = 1$ and $a_{n+2} = a_{n+1}a_n$ define a sequence of reals? What is it?

Solution. Yes, by Corollary 2.3.3 with $X = \mathbb{R}$ and $h(n, x, y) = yx$, a function $\mathbb{N}\times(\mathbb{R}\times\mathbb{R}) \to \mathbb{R}$. Every term is 1: induct on the pair statement "$a_n = 1$ and $a_{n+1} = 1$", as in the two-step example below, after Definition 2.3.2. It holds at $n = 0$, and if it holds at n, then $a_{n+2} = 1 \cdot 1 = 1$, so it holds at $n + 1$.

2.3.3 Sums, products and powers

The symbols $\sum$ and $\prod$ are recursive definitions, and so are powers. Writing them as instances of Theorem 2.3.1 settles what they mean at the edges: the empty sum, the empty product and u^0.

Definition 2.3.1. Finite Sums and Products

Let $(a_k)_{k\geq 1}$ be a sequence of real numbers. The **sums** $\sum_{k=1}^{n} a_k$ and **products** $\prod_{k=1}^{n} a_k$, for $n \in \mathbb{N}$, are defined by recursion:

$$\sum_{k=1}^{0} a_k := 0, \quad \sum_{k=1}^{n+1} a_k := \sum_{k=1}^{n} a_k + a_{n+1},$$
$$\prod_{k=1}^{0} a_k := 1, \quad \prod_{k=1}^{n+1} a_k := \Big(\prod_{k=1}^{n} a_k\Big) a_{n+1}.$$

The **factorial** of $n \in \mathbb{N}$ is $n! := \prod_{k=1}^{n} k$. For integers $m \leq n+1$ and reals a_k given for every integer $k \geq m$,

$$\sum_{k=m}^{n} a_k := \sum_{i=1}^{n-m+1} a_{m-1+i}, \qquad \prod_{k=m}^{n} a_k := \prod_{i=1}^{n-m+1} a_{m-1+i}.$$

In words: a sum starts at 0 and adds one term at each stage; a product starts at 1 and multiplies by one term at each stage. The sum is Theorem 2.3.1 with $X = \mathbb{R}$, $a = 0$ and $g(n, x) = x + a_{n+1}$, a function $\mathbb{N} \times \mathbb{R} \to \mathbb{R}$ because $n + 1 \geq 1$ is an index of the sequence (Lemma 2.1.1 (a), (NS)); the product is $a = 1$, $g(n, x) = xa_{n+1}$. The letter k is a dummy: $\sum_{k=1}^{n} a_k$ and $\sum_{j=1}^{n} a_j$ are the same number. In the general form, $n - m + 1$ is an integer ≥ 0, hence in $\mathbb{N}$ (Proposition 2.1.2 (b)), and the terms a_{m-1+i}, for $i \geq 1$, run through $a_m, a_{m+1}, \ldots$; when $m = 1$ it gives the first form back.

The edge cases are the point of the definition. The **empty sum** is 0 and the **empty product** is 1: $\sum_{k=m}^{m-1} a_k = 0$ and $0! = 1$. These are the only values that make the recursive clause true at the first stage for every sequence, since $\sum_{k=1}^{1} a_k$ should be a_1 and $\prod_{k=1}^{1} a_k$ should be a_1. So $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$.

Three consequences are used constantly, and each is a short check from the definition.

- **Finite lists.** $\sum_{k=1}^{n} a_k$ depends only on $a_1, \ldots, a_n$. Precisely: if two sequences agree at $1, \ldots, N$, their sums up to n agree for every $n \leq N$. Induct on n with the property "if $n \leq N$, the two sums up to n are equal". The base is $0 = 0$. In the step, $n + 1 \leq N$ gives $n \leq N$, so the sums up to n agree, and the added terms a_{n+1} agree because $1 \leq n+1 \leq N$. So a finite list $a_1, \ldots, a_N$ is summed by extending it in any way, say by $a_k := 0$ for $k > N$, and the result does not depend on the extension. The same holds for products, and for the general bounds with $a_m, \ldots, a_n$.
- **Shifting the index.** For every integer p, $\sum_{k=m}^{n} a_k = \sum_{k=m+p}^{n+p} a_{k-p}$, because both sides unfold to $\sum_{i=1}^{n-m+1} a_{m-1+i}$. *Analysis on the Real Line*, Chapter 1's estimate of $y^k - x^k$ uses the shift $p = 1$.
- **Splitting off the last term.** For $m \leq n+1$, $\sum_{k=m}^{n+1} a_k = \sum_{k=m}^{n} a_k + a_{n+1}$. Unfold the left side to $\sum_{i=1}^{n-m+2} a_{m-1+i}$ and apply the recursive clause; its last term is $a_{m-1+(n-m+2)} = a_{n+1}$.

Definition 2.3.2. Powers

Let $u \in \mathbb{R}$. The **powers** u^n, for $n \in \mathbb{N}$, are defined by recursion:

$$u^0 := 1, \qquad u^{n+1} := u^n u.$$

This is Theorem 2.3.1 with $X = \mathbb{R}$, $a = 1$ and $g(n, x) = xu$. So $u^1 = u^0 u = u$, and $u^2 = uu$. The definition gives $0^0 = 1$, in line with the empty product: $u^n = \prod_{k=1}^{n} u$, since both sides obey the same two clauses and so agree by the uniqueness in Theorem 2.3.1. Only exponents in $\mathbb{N}$ are defined here; roots $a^{1/n}$ come in *Analysis on the Real Line*, Chapter 1.

A sequence that approaches $\sqrt{2}$. Let $X := (0, \infty)$ and $g(n, x) := \frac{1}{2}(x + 2/x)$. Before writing a recursion, check that g maps X into X: for $x > 0$, $2/x$ is defined and positive, so $x + 2/x > 0$, and half of it is positive. By Theorem 2.3.1, $a_0 := 2$ and $a_{n+1} := \frac{1}{2}(a_n + 2/a_n)$ define a sequence in $(0, \infty)$. Because the check was made on g, no separate induction is needed to show $a_n > 0$ before dividing by it. The first values are

$$a_0 = 2, \qquad a_1 = \tfrac{1}{2}(2 + 1) = \tfrac{3}{2}, \qquad a_2 = \tfrac{1}{2}\left(\tfrac{3}{2} + \tfrac{4}{3}\right) = \tfrac{17}{12},$$

and $(17/12)^2 = 289/144$, which exceeds 2 by $1/144$. That the sequence converges to $\sqrt{2}$ is a question for *Analysis on the Real Line*, Chapter 2, where recursively defined sequences become objects of study.

A two-step example. By Corollary 2.3.3, $a_0 = 2$, $a_1 = 3$ and $a_{n+2} = 3a_{n+1} - 2a_n$ define a unique sequence of reals ($X = \mathbb{R}$, $h(n, x, y) = 3y - 2x$), and its first values are $2, 3, 5, 9, 17$. These

are 2^n+1. To prove it, induct on the **pair** statement $Q(n)$: "$a_n = 2^n+1$ and $a_{n+1} = 2^{n+1}+1$". $Q(0)$ is $2 = 1+1$ and $3 = 2+1$. If $Q(n)$ holds, its second half is the first half of $Q(n+1)$, and

$$a_{n+2} = 3(2^{n+1}+1) - 2(2^n+1) = 2\cdot 2^{n+1} + 1 = 2^{n+2}+1,$$

where $2\cdot 2^n = 2^n\cdot 2 = 2^{n+1}$ and $2\cdot 2^{n+1} = 2^{n+1}\cdot 2 = 2^{n+2}$ by Definition 2.3.2 (and commutativity). So Logic and Proof, Axiom 4.2.1 gives $Q(n)$ for every n, and in particular $a_n = 2^n+1$. The induction carries a pair because the recursion does: the proof follows the clauses of the definition.

Warning. A recursion needs its starting values, and its rule must stay inside X. "$a_{n+2} = a_{n+1} + a_n$" alone defines nothing: $0,1,1,2,\ldots$ and $2,1,3,4,\ldots$ both obey it, and Corollary 2.3.3 asks for a_0 and a_1. And "$a_0 = 2$, $a_{n+1} = 1/(a_n - 1)$" is not a definition by recursion: $a_1 = 1$, and then a_2 would be $1/0$. The rule $x \mapsto 1/(x-1)$ is not a function from any set X containing 2 into X, since X would have to contain its value 1, where the rule is undefined.

Quick check. Compute $\prod_{k=1}^{4}(1+\frac{1}{k})$, and say why the answer is so simple.

Solution. Each factor is $1+\frac{1}{k} = \frac{k+1}{k}$, so the product is

$$\frac{2}{1}\cdot\frac{3}{2}\cdot\frac{4}{3}\cdot\frac{5}{4} = 5.$$

Each numerator cancels the next denominator: the product **telescopes**. In general $\prod_{k=1}^{n}\frac{k+1}{k} = n+1$, by induction on n: the empty product is $1 = 0+1$, and $(n+1)\cdot\frac{n+2}{n+1} = n+2$.

2.3.4 Recursion, then induction

A function defined by recursion is studied by induction, and the induction follows the clauses of the definition: the base case uses the starting value, the step uses the rule. The laws of powers are the first example. In the terms of Example (Method: finding $P(n)$ inside $P(n+1)$), the recursion says where $P(n)$ sits inside $P(n+1)$: in the last term split off, or the last factor.

Proposition 2.3.4. Laws of Powers

Let $u, v \in \mathbb{R}$ and $m, n \in \mathbb{N}$.

(a) $u^{m+n} = u^m u^n$.
(b) $(u^m)^n = u^{mn}$.
(c) $(uv)^n = u^n v^n$.
(d) If $u \in \mathbb{Z}$, then $u^n \in \mathbb{Z}$; if $u \in \mathbb{N}$, then $u^n \in \mathbb{N}$.
(e) If $u > 0$, then $u^n > 0$. If $u > 1$ and $m < n$, then $u^m < u^n$.

Idea. Each part is an induction on n from 0, with m fixed. The base case is $u^0 = 1$ in some

form, and the step peels one factor off with $u^{n+1} = u^n u$ and applies the induction hypothesis to u^n. For the second half of (e), write $n = m + j$ with $j \geq 1$ and use (a).

Proof.

(a) Fix m and induct on n. For $n = 0$: $u^{m+0} = u^m = u^m \cdot 1 = u^m u^0$. Suppose $u^{m+n} = u^m u^n$. Since $m + n \in \mathbb{N}$ (Lemma 2.1.1 (b)), Definition 2.3.2 applies at $m + n$, and

$$u^{m+(n+1)} = u^{(m+n)+1} = u^{m+n} u = u^m u^n u = u^m u^{n+1},$$

where the third equation is the induction hypothesis and the last is Definition 2.3.2. By Logic and Proof, Axiom 4.2.1, (a) holds for every n.

(b) Fix m. For $n = 0$: $(u^m)^0 = 1 = u^0 = u^{m \cdot 0}$. If $(u^m)^n = u^{mn}$, then $(u^m)^{n+1} = (u^m)^n u^m = u^{mn} u^m = u^{mn+m} = u^{m(n+1)}$, using (a) with the exponents $mn, m \in \mathbb{N}$ (Lemma 2.1.1 (b)).

(c) $(uv)^0 = 1 = 1 \cdot 1 = u^0 v^0$. If $(uv)^n = u^n v^n$, then $(uv)^{n+1} = (uv)^n uv = u^n v^n uv = (u^n u)(v^n v) = u^{n+1} v^{n+1}$.

(d) $u^0 = 1 = 0 + 1$ lies in $\mathbb{N}$ by (($\mathbb{N}$)0) and ($\mathbb{N}$S), and $\mathbb{N} \subseteq \mathbb{Z}$. If $u^n \in \mathbb{Z}$ and $u \in \mathbb{Z}$, then $u^{n+1} = u^n u \in \mathbb{Z}$ by Proposition 2.1.2 (a). For $u \in \mathbb{N}$ the same induction works with Lemma 2.1.1 (b) in place of Proposition 2.1.2.

(e) Let $u > 0$. Then $u^0 = 1 > 0$, and if $u^n > 0$, then $u^{n+1} = u^n u > 0$ as a product of positive numbers. Now let $u > 1$. First, $u^j > 1$ for every integer $j \geq 1$ (such j lies in $\mathbb{N}$ by Proposition 2.1.2 (b), so u^j is defined), by Theorem 2.2.1 with base 1: $u^1 = u > 1$, and if $u^j > 1$, then $u^{j+1} = u^j u > 1 \cdot u > 1$, multiplying $u^j > 1$ by $u > 0$. Let $m < n$. Then $j := n - m \in \mathbb{N}$ by Lemma 2.1.1 (d), and $j \neq 0$, so $j \geq 1$ by Lemma 2.1.1 (a). By (a), $u^n = u^{m+j} = u^m u^j > u^m$, multiplying $u^j > 1$ by $u^m > 0$.

■

Some instances that earlier chapters used on trust: $(t^2)^2 = t^4$ is (b) with $m = n = 2$; $2^{s+t} = 2^s 2^t$ is (a); $n \mapsto 2^n$ is strictly increasing on $\mathbb{N}$ by (e); and an integer power of an integer is an integer by (d). For $(-1)^n$: by (b), $(-1)^{2k} = ((-1)^2)^k = 1^k = 1$, where $1^k = 1$ by the induction $1^{k+1} = 1^k \cdot 1$; and $(-1)^{2k+1} = (-1)^{2k}(-1) = -1$. Every $n \in \mathbb{N}$ is $2k + r$ with $k \in \mathbb{Z}$ and $r \in \{0, 1\}$ (Theorem 2.2.3 with divisor 2, and Proposition 2.1.2 (c) for $r \leq 1$), and $k \geq 0$: if $k < 0$, then $k \leq -1$ (Proposition 2.1.2 (c)), so $n = 2k + r \leq -2 + 1 < 0$, contradicting $n \geq 0$ (Lemma 2.1.1 (a)). So $k \in \mathbb{N}$ by Proposition 2.1.2 (b), n is $2k$ or $2k + 1$, and $(-1)^n$ is 1 for even n and -1 for odd n.

The next two formulas are proved the same way; each is a recursion (the sum) followed by an induction whose step splits off the last term.

Proposition 2.3.5. Sum of the First Natural Numbers

For every $n \in \mathbb{N}$, $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Proof. For $n = 0$, both sides are 0: the left by the empty sum, the right since $0 \cdot 1 = 0$. If the formula holds for n, then by Definition 2.3.1

$$\sum_{k=1}^{n+1} k = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2},$$

which is the formula for $n+1$. By Logic and Proof, Axiom 4.2.1 it holds for every $n \in \mathbb{N}$.

■

Proposition 2.3.6. Geometric Sum

Let $r \in \mathbb{R}$ with $r \neq 1$. For every $n \in \mathbb{N}$,

$$\sum_{k=1}^{n} r^{k-1} = \frac{1 - r^n}{1 - r}.$$

Proof. The terms are defined: for $k \geq 1$, $k - 1 \in \mathbb{N}$ by Lemma 2.1.1 (c), so r^{k-1} is given by Definition 2.3.2, and the term added at stage $n+1$ is $r^{(n+1)-1} = r^n$. The right side is defined because $1 - r \neq 0$. For $n = 0$, both sides are 0, since $r^0 = 1$. If the formula holds for n, then, by Definition 2.3.1 and the induction hypothesis,

$$\begin{aligned}\sum_{k=1}^{n+1} r^{k-1} &= \frac{1 - r^n}{1 - r} + r^n = \frac{1 - r^n + r^n - r^{n+1}}{1 - r} \\ &= \frac{1 - r^{n+1}}{1 - r},\end{aligned}$$

where $r^n(1-r) = r^n - r^{n+1}$ by Definition 2.3.2. By Logic and Proof, Axiom 4.2.1 the formula holds for every $n \in \mathbb{N}$.

■

For $r = 1$ the sum is n, since every term is 1; that is the case the hypothesis excludes, where the right side would divide by 0.

The next inequality is the most used estimate of a power in analysis. Its proof shows a hypothesis doing exactly one job.

Theorem 2.3.7. Bernoulli's Inequality

Let $x \in \mathbb{R}$ with $x \geq -1$. Then $(1+x)^n \geq 1 + nx$ for every $n \in \mathbb{N}$.

Idea. Induct on n. To pass from n to $n+1$, multiply the induction hypothesis by $1 + x$; the product $(1 + nx)(1 + x) = 1 + (n+1)x + nx^2$ is at least $1 + (n+1)x$, because the extra term nx^2 is non-negative. Multiplying an inequality by $1 + x$ keeps its direction only if $1 + x \geq 0$, and that is what $x \geq -1$ says. (This is the method of Example (Method: finding $P(n)$ inside $P(n+1)$): $(1+x)^n$ is the first factor of $(1+x)^{n+1}$.)

Proof. For $n = 0$: $(1 + x)^0 = 1 \geq 1 = 1 + 0 \cdot x$. Suppose $(1 + x)^n \geq 1 + nx$. Since $x \geq -1$, we have $1 + x \geq 0$, and multiplying the induction hypothesis by $1 + x$ gives

$$\begin{aligned}(1 + x)^{n+1} &= (1 + x)^n(1 + x) \geq (1 + nx)(1 + x) \\ &= 1 + (n + 1)x + nx^2 \geq 1 + (n + 1)x,\end{aligned}$$

where the first equation is Definition 2.3.2 and the last step uses $nx^2 \geq 0$, true because $n \geq 0$ (Lemma 2.1.1 (a)) and $x^2 \geq 0$. By Logic and Proof, Axiom 4.2.1 the inequality holds for every $n \in \mathbb{N}$.

■

The hypothesis $x \geq -1$ appears in the proof once, in the sentence "since $x \geq -1$, we have $1 + x \geq 0$", and it cannot simply be dropped: for $x = -4$ and $n = 3$, $(1 + x)^3 = (-3)^3 = -27$, while $1 + 3x = -11$, and $-27 < -11$. Exercise C2 below shows that the statement can survive at some $x < -1$ even though the proof does not.

Quick check. Check Bernoulli's inequality at $x = -\frac{1}{2}$, $n = 3$, and say which line of the proof uses $x \geq -1$.

Solution. $(1 - \frac{1}{2})^3 = \frac{1}{8}$, and $1 + 3 \cdot (-\frac{1}{2}) = -\frac{1}{2}$; indeed $\frac{1}{8} \geq -\frac{1}{2}$. The hypothesis is used in the line "since $x \geq -1$, we have $1 + x \geq 0$": multiplying the induction hypothesis by $1 + x$ keeps the direction of the inequality only because $1 + x \geq 0$.

The last result of this subsection is not about a recursive definition, but its induction runs over lists, and it is the fact *Analysis on the Real Line*, Chapter 1 needs about finite sets. A maximum of a set $A \subseteq \mathbb{R}$ is a greatest element of A in the sense of Section 2.1, and a minimum is a least element. For reals $x_1, \ldots, x_n$, we write $\{x_1, \ldots, x_n\} \coloneqq \{x_k : k \in \{1, \ldots, n\}\}$.

Proposition 2.3.8. Finite Sets Have a Maximum

For every integer $n \geq 1$ and all reals $x_1, \ldots, x_n$, the set $\{x_1, \ldots, x_n\}$ has a maximum and a minimum.

Idea. Add the elements one at a time. The maximum of the longer list is the old maximum or the new element, whichever is larger, and comparing the two is all the step needs.

Proof. Let $P(n)$ be "for all reals $x_1, \ldots, x_n$, the set $\{x_1, \ldots, x_n\}$ has a maximum". We prove $P(n)$ for every $n \geq 1$ by Theorem 2.2.1 with base 1.

Base case. $\{x_1\}$ has the maximum x_1.

Inductive step. Let $n \geq 1$, suppose $P(n)$, and let $x_1, \ldots, x_{n+1}$ be reals. Since $\{1, \ldots, n + 1\} = \{1, \ldots, n\} \cup \{n + 1\}$ (Lemma 2.1.1 (e), as in the proof of Theorem 2.3.1), the set $B \coloneqq \{x_1, \ldots, x_{n+1}\}$ is $A \cup \{x_{n+1}\}$, where $A \coloneqq \{x_1, \ldots, x_n\}$. By $P(n)$, applied to the list

$x_1, \ldots, x_n$, the set A has a maximum M. By trichotomy, $x_{n+1} \le M$ or $M < x_{n+1}$.

Case 1: $x_{n+1} \le M$. Then $M \in A \subseteq B$, and every element of B is an element $a \in A$, with $a \le M$, or is $x_{n+1} \le M$. So M is a maximum of B.

Case 2: $M < x_{n+1}$. Then $x_{n+1} \in B$, and every $a \in A$ satisfies $a \le M < x_{n+1}$. So x_{n+1} is a maximum of B.

In both cases $P(n+1)$ holds. By Theorem 2.2.1, $P(n)$ holds for every $n \ge 1$.

For the minimum, apply the result to $-x_1, \ldots, -x_n$: if $-x_j$ is a maximum of $\{-x_1, \ldots, -x_n\}$, then $-x_k \le -x_j$, that is $x_j \le x_k$, for every k, so x_j is a minimum of $\{x_1, \ldots, x_n\}$.

■

The base is 1, not 0: for $n = 0$ the set is $\emptyset$, which has neither a maximum nor a minimum, since both must be elements. The proof used only order properties of $\le$: any two elements are comparable (trichotomy), $\le$ is reflexive and transitive, and $x \mapsto -x$ reverses $\le$. All of these hold in any ordered field, so the proof works word for word there; that is the setting in which *Analysis on the Real Line*, Chapter 1 uses it. Passing from a finite **set** to a list $x_1, \ldots, x_n$ that enumerates it is what "finite" means in Section 2.5.

2.3.5 When the claim is too weak to carry its step

Sometimes the statement we want is true, but it cannot be proved by induction as it stands: its inductive step does not go through. The cure looks paradoxical. We prove **more**. *Logic and Proof* met this cure (Logic and Proof, Example (Prove more to prove less)) with a sum that telescopes, where the stronger claim was an exact formula; here the sum has no closed form, and the stronger claim is an inequality with a margin.

Example. Proving more to prove anything

Prove that $\sum_{k=1}^{n} \frac{1}{k^2} < 2$ for every integer $n \ge 1$.

Solution. The direct attempt fails. Let $S_n := \sum_{k=1}^{n} 1/k^2$, so $S_{n+1} = S_n + 1/(n+1)^2$ by Definition 2.3.1. The base $S_1 = 1 < 2$ holds. For the step, all we may assume is $S_n < 2$, and that is too little: it allows $S_n = 2 - \frac{1}{2(n+1)^2}$, and then $S_n + \frac{1}{(n+1)^2} > 2$. The values of S_n never come so close to 2, but the induction hypothesis cannot know that.

Prove more. We prove $P(n)$: "$S_n \le 2 - \frac{1}{n}$" for every $n \ge 1$, by Theorem 2.2.1 with base 1. It implies the claim, since $2 - \frac{1}{n} < 2$.

Base case. $S_1 = 1 = 2 - \frac{1}{1}$.

Inductive step. Let $n \ge 1$ and suppose $S_n \le 2 - \frac{1}{n}$. Then

$$S_{n+1} = S_n + \frac{1}{(n+1)^2} \le 2 - \frac{1}{n} + \frac{1}{(n+1)^2}.$$

It remains to show $-\frac{1}{n} + \frac{1}{(n+1)^2} \le -\frac{1}{n+1}$, that is, $\frac{1}{(n+1)^2} \le \frac{1}{n} - \frac{1}{n+1} = \frac{1}{n(n+1)}$. Both denominators are positive, and $n(n+1) \le (n+1)^2$ because $n \le n+1$ and $n+1 > 0$; so the inequality holds. Hence $S_{n+1} \le 2 - \frac{1}{n+1}$, which is $P(n+1)$.

By Theorem 2.2.1, $S_n \le 2 - \frac{1}{n} < 2$ for every $n \ge 1$.

The stronger statement carries its own step because its hypothesis says **how far** below 2 the sum is, and that margin pays for the next term. When a step fails, ask what the hypothesis would need to say, and prove that instead. Exercise C3 below uses it twice over, proving two identities together because neither carries its own one-step induction.

Quick check. Would "$S_n \le 2 - \frac{1}{n+1}$" also carry its own step?

Solution. No, although the statement is true (it is weaker than $S_n \le 2 - \frac{1}{n}$). The hypothesis allows $S_n = 2 - \frac{1}{n+1}$, and then $S_{n+1} = 2 - \frac{1}{n+1} + \frac{1}{(n+1)^2} > 2 - \frac{1}{n+2}$, because $\frac{1}{(n+1)^2} > \frac{1}{(n+1)(n+2)} = \frac{1}{n+1} - \frac{1}{n+2}$ (as $(n+1)^2 < (n+1)(n+2)$). A stronger claim works only if its margin pays for the next term; this margin is too small.

2.3.6 Exercises

2.3.6.1 A. Check your understanding

Exercise. A1

These questions are about the proof of Theorem 2.3.1.

(a) Why does uniqueness need only an induction, while existence needs the claim about partial solutions?

(b) In Step 3, which property of the graphs G_n makes $\bigcup \mathcal{S}$ satisfy (Fn2), and which part of the proof supplies it?

(c) Run the construction for $X = \mathbb{R}$, $a = 1$ and $g(n, x) = (n+1)x$: write the graphs G_0, G_1, G_2. Which familiar function is f?

(d) State the idea of the proof in two sentences.

(e) Write $\sum_{k=1}^{n} a_k$ and $n!$ as instances of Theorem 2.3.1: name X, a and g for each.

Solution.

(a) Uniqueness is a statement about two functions that are **given**: it compares their values, and comparing values at $n+1$ through the values at n is an induction. Existence asks for a function that is not given. Induction proves statements and does not build objects, so the proof proves a statement (the claim) whose content is that the finite pieces exist and are unique, and then builds f from them as a union.

(b) The graphs agree where they overlap: $G_m \subseteq G_n$ for $m \le n$, more precisely $G_m = G_n \cap (\{0, \dots, m\} \times X)$. This comes from the **uniqueness** half of the claim: the restriction of f_n to $\{0, \dots, m\}$ is a partial solution up to m, so it is f_m. With it, two pairs $(k, y) \in G_m$ and $(k, y') \in G_n$ lie in the larger graph, whose (Fn2) gives $y = y'$. So it verifies (Fn2) of Definition 1.5.1 for $\bigcup \mathcal{S}$.

(c) $G_0 = \{(0, 1)\}$. Then $g(0, 1) = 1 \cdot 1 = 1$, so $G_1 = \{(0, 1), (1, 1)\}$. Then $g(1, 1) = 2 \cdot 1 = 2$, so $G_2 = \{(0, 1), (1, 1), (2, 2)\}$. The function f is $n \mapsto n!$: by Definition 2.3.1, $0! = 1$

and $(n+1)! = n!\,(n+1) = g(n, n!)$, so $n \mapsto n!$ satisfies both equations, and by the uniqueness in Theorem 2.3.1 it is f.

(d) For each n, induction shows that there is exactly one function on $\{0, \dots, n\}$ obeying the equations, and these pieces extend one another. Their union is the required function, and an induction on n shows there is no other.

(e) The sum: $X = \mathbb{R}$, $a = 0$, $g(n, x) = x + a_{n+1}$. The factorial: $X = \mathbb{R}$ (or $\mathbb{N}$), $a = 1$, $g(n, x) = (n+1)x$, as in (c).

2.3.6.2 B. Practice

Exercise. B1: Sum of cubes

Prove that $\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$ for every $n \in \mathbb{N}$.

Solution. For $n = 0$, both sides are 0 (the empty sum, and $0^2 = 0$). Suppose the formula holds for n. By Definition 2.3.1 and the induction hypothesis,

$$\sum_{k=1}^{n+1} k^3 = \frac{n^2(n+1)^2}{4} + (n+1)^3 = (n+1)^2\,\frac{n^2+4n+4}{4}$$
$$= \frac{(n+1)^2(n+2)^2}{4} = \left(\frac{(n+1)(n+2)}{2}\right)^2,$$

which is the formula for $n+1$. By Logic and Proof, Axiom 4.2.1 the formula holds for every $n \in \mathbb{N}$. (Compare Proposition 2.3.5: the sum of the first n cubes is the square of the sum of the first n numbers.)

Exercise. B2: Starting at the right place

Logic and Proof, Chapter 4 observed, in the warning after Logic and Proof, Example (An inequality by induction), that "$2^n \geq n^2$" fails at $n = 3$ and holds again from $n = 4$ on. Prove that $2^n \geq n^2$ for every integer $n \geq 4$, using Theorem 2.2.1. Say why the base must be 4 and not 3.

Solution. Let $P(n)$ be "$2^n \geq n^2$"; we use Theorem 2.2.1 with $n_0 = 4$.

Base case. $2^4 = 16 \geq 16 = 4^2$.

Inductive step. Let $n \geq 4$ and suppose $2^n \geq n^2$. Then $2^{n+1} = 2 \cdot 2^n \geq 2n^2$ by Definition 2.3.2 and the hypothesis. Moreover $2n^2 \geq (n+1)^2$, because $2n^2 - (n+1)^2 = n^2 - 2n - 1 = (n-1)^2 - 2$, and $(n-1)^2 \geq 9 > 2$ for $n \geq 4$. Hence $2^{n+1} \geq (n+1)^2$.

By Theorem 2.2.1, $2^n \geq n^2$ for every $n \geq 4$.

The base cannot be 3, because $P(3)$ is false: $2^3 = 8 < 9 = 3^2$. The step is valid from $n = 3$ on, since $(n-1)^2 - 2 \geq 2$ for $n \geq 3$, but it is useless at 3, where its hypothesis is false. At $n = 2$ the step fails ($(2-1)^2 - 2 = -1$), which is why the true $P(2)$ does not lead to $P(3)$.

Exercise. B3: A closed form

The sequence $a_0 := 0$, $a_{n+1} := 2a_n + 1$ is defined by Theorem 2.3.1. Compute its first five values, guess a formula for a_n, and prove it.

Solution. The values are $0, 1, 3, 7, 15$: one less than $1, 2, 4, 8, 16$. We prove $a_n = 2^n - 1$ for every $n \in \mathbb{N}$. For $n = 0$: $a_0 = 0 = 2^0 - 1$. If $a_n = 2^n - 1$, then

$$a_{n+1} = 2(2^n - 1) + 1 = 2^{n+1} - 1,$$

using $2 \cdot 2^n = 2^{n+1}$ (Definition 2.3.2). By Logic and Proof, Axiom 4.2.1, $a_n = 2^n - 1$ for every $n \in \mathbb{N}$. The induction follows the two clauses of the definition: the base case is the starting value, the step is the rule.

2.3.6.3 C. Going deeper

Exercise. C1: Powers of two

Prove that every $n \in \mathbb{Z}_{>0}$ can be written as $2^k q$ with $k \in \mathbb{N}$ and q odd (that is, $q = 2j + 1$ for an integer j). Below, the proof is started; the second half is blank. *Name the move, then complete it.*

> Suppose not. Then the set F of $n \in \mathbb{Z}_{>0}$ that cannot be written in this form is non-empty, and $F \subseteq \mathbb{N}$; let m be its least element. Then $m \geq 1$, and m is not odd, since otherwise $m = 2^0 m$ would be of the required form. _____

Why is the statement made for $n \geq 1$ only?

Solution. The move is the **smallest counterexample** of Section 2.2: suppose the claim fails, take the least failure by well-ordering (Theorem 2.1.3), and produce a smaller failure.

Completion. By Theorem 2.2.3 with divisor 2, every integer is even or odd; m is not odd, so $m = 2m'$ for an integer m'. Since $m > 0$, $m' = m/2 > 0$, so $m' \in \mathbb{Z}_{>0}$ (Proposition 2.1.2 (b)), and $m' < 2m' = m$. As m is the least element of F, $m' \notin F$, so $m' = 2^k q$ with $k \in \mathbb{N}$ and q odd. Then

$$m = 2 \cdot 2^k q = 2^{k+1} q$$

by Definition 2.3.2, and $k+1 \in \mathbb{N}$ by (NS). So m has the required form, contradicting $m \in F$. Hence $F = \emptyset$, and every $n \in \mathbb{Z}_{>0}$ is $2^k q$ with q odd.

The restriction to $n \geq 1$ is needed: $0 = 2^k q$ forces $q = 0$, since $2^k > 0$ (Proposition 2.3.4 (e)), and $0 = 2 \cdot 0$ is even, not odd (Theorem 2.2.3: not both). So 0 is a genuine counterexample, and in the proof it is excluded by taking $m \in \mathbb{Z}_{>0}$, which is what makes $m' > 0$.

Marking scheme. (10 points) - 2: names the move (smallest counterexample) and says that the least element m exists by well-ordering (Theorem 2.1.3). - 2: from "m is not odd" concludes $m = 2m'$ with $m' \in \mathbb{Z}$, citing even-or-odd. - 3: shows $m' \in \mathbb{Z}_{>0}$ and $m' < m$, so $m' \notin F$. - 2: writes $m = 2^{k+1} q$ with $k + 1 \in \mathbb{N}$ and reaches the contradiction. - 1: explains why $n = 0$ is excluded. Fatal errors (0 for the step): concluding $m' \notin F$ (or applying the induction hypothesis to m') without having shown both $m' < m$ and $m' \geq 1$; missing either one is fatal. A reader who restarts by Theorem 2.2.2 with base 1 earns the points for the

other steps (the induction hypothesis at m' replaces "$m' \notin F$"), but not the 2 points for naming the move.

Exercise. C2: Bernoulli beyond its hypothesis

(a) Show that $(1+x)^n \geq 1+nx$ holds for $x = -2$ and every $n \in \mathbb{N}$.

(b) Say which line of the proof of Theorem 2.3.7 fails at $x = -2$, and why the statement survives anyway.

(c) At $x = -4$, find the first n where the inequality fails, and the first n where the step "$P(n) \Rightarrow P(n+1)$" fails.

Solution.

(a) At $x = -2$ the claim is $(-1)^n \geq 1 - 2n$. By the remark after Proposition 2.3.4, $(-1)^n$ is 1 or -1. For $n = 0$ the claim reads $1 \geq 1$. For $n \geq 1$, $1 - 2n \leq -1 \leq (-1)^n$.

(b) The line "multiplying the induction hypothesis by $1+x$" fails. At $x = -2$ the multiplier is $1+x = -1 < 0$, and multiplying $(1+x)^n \geq 1+nx$ by a negative number **reverses** it: we get $(1+x)^{n+1} \leq (1+nx)(1+x)$, the wrong direction. The rest of the proof ($nx^2 \geq 0$) still holds. The statement survives because (a) proves it by a different argument, which uses the special values $(-1)^n = \pm 1$. A proof that fails does not make its conclusion false.

(c) At $x = -4$: $n = 0$ gives $1 \geq 1$; $n = 1$ gives $-3 \geq -3$; $n = 2$ gives $9 \geq -7$; $n = 3$ gives $-27 \geq -11$, false. So the first failure is $n = 3$. The step $P(n) \Rightarrow P(n+1)$ holds for $n = 0$ and $n = 1$ (both sides are true) and fails at $n = 2$, where $P(2)$ is true and $P(3)$ false.

Exercise. C3: Two identities at once

Use Corollary 2.3.3 to define the sequence $F_0 := 0$, $F_1 := 1$, $F_{n+2} := F_{n+1} + F_n$; name X, a, b and h. Then prove, for every $n \in \mathbb{N}$, the statement $P(n)$:

$$F_{2n+1} = F_n^2 + F_{n+1}^2 \quad \text{and} \quad F_{2n+2} = F_{n+1}(F_n + F_{n+2}).$$

Check $P(0)$, $P(1)$ and $P(2)$ numerically first.

Solution (Hint 1). Neither identity carries its own one-step inductive step: passing from F_{2n+1} to F_{2n+3} needs F_{2n+2}, which is the other identity. Prove both together, and use $F_n + F_{n+1} = F_{n+2}$ to merge terms.

Solution (Hint 2). In the step, start with $F_{2n+3} = F_{2n+2} + F_{2n+1}$ and substitute both halves of $P(n)$.

Solution. The definition. Corollary 2.3.3 with $X = \mathbb{R}$, $a = 0$, $b = 1$ and $h(n, x, y) = x + y$ gives exactly one sequence with $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_n + F_{n+1}$. Its first values are $0, 1, 1, 2, 3, 5, 8$.

Small cases. $P(0)$: $F_1 = 1 = 0^2 + 1^2$ and $F_2 = 1 = 1 \cdot (0 + 1)$. $P(1)$: $F_3 = 2 = 1^2 + 1^2$ and $F_4 = 3 = 1 \cdot (1 + 2)$. $P(2)$: $F_5 = 5 = 1^2 + 2^2$ and $F_6 = 8 = 2 \cdot (1 + 3)$.

Proof. We use Logic and Proof, Axiom 4.2.1. $P(0)$ was checked. Suppose $P(n)$. Using the recursion and then both halves of $P(n)$,

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

where the last two lines use $F_n + F_{n+1} = F_{n+2}$ twice. This is the first half of $P(n + 1)$. For the second half,

$$\begin{aligned} F_{2n+4} &= F_{2n+3} + F_{2n+2} \\ &= F_{n+1}^2 + F_{n+2}^2 + F_{n+1}F_n + F_{n+1}F_{n+2} \\ &= F_{n+1}(F_{n+1} + F_n) + F_{n+2}^2 + F_{n+1}F_{n+2} \\ &= F_{n+2}(2F_{n+1} + F_{n+2}) = F_{n+2}(F_{n+1} + F_{n+3}), \end{aligned}$$

using the first half of $P(n + 1)$ just proved, the second half of $P(n)$, $F_{n+1} + F_n = F_{n+2}$, and finally $F_{n+1} + F_{n+2} = F_{n+3}$. So $P(n + 1)$ holds, and by Logic and Proof, Axiom 4.2.1 $P(n)$ holds for every $n \in \mathbb{N}$.

The second identity is written with F_{n+2} rather than in the form $F_{2n} = F_n(F_{n-1} + F_{n+1})$, so that both identities make sense on all of $\mathbb{N}$ and no F_{-1} is needed. The two identities hold together, and together they carry a one-step induction that neither carries alone: this is "prove more" (Example (Proving more to prove anything)) in the form of a pair, as in the two-step example after Definition 2.3.2. (A two-step induction can prove the first identity alone; see the marking scheme.)

Marking scheme. (10 points) - 2: defines the sequence by Corollary 2.3.3, naming X, a, b and h. - 1: checks the base case $P(0)$, both halves. - 3: proves the first identity at $n + 1$ (or for all n): $F_{2n+3} = F_{n+1}^2 + F_{n+2}^2$. - 3: proves the second identity at $n + 1$ (or for all n): $F_{2n+4} = F_{n+2}(F_{n+1} + F_{n+3})$. - 1: concludes by induction (one-step or two-step), with a hypothesis that covers every value the step uses. Alternative route: 3 for proving $F_{2n+1} = F_n^2 + F_{n+1}^2$ alone by a two-step induction (via $F_{k+2} = 3F_k - F_{k-2}$ for $k \geq 2$ and the matching recursion for $F_n^2 + F_{n+1}^2$, with both bases $n = 0, 1$ checked), and 3 for deriving the second identity as $F_{2n+2} = F_{2n+3} - F_{2n+1} = F_{n+2}^2 - F_n^2 = F_{n+1}(F_n + F_{n+2})$. Fatal errors (0 for the step): inducting on one identity alone while using the other at n unproved; using the identities at $n + 1$ to prove themselves.

2.4 Contrapositive and Contradiction in Practice

Section 1.1 proved statements straight from their definitions, and Section 1.2 met the first contradiction about sets. *Logic and Proof*, Section 8.1 sorted the arguments called "by contradiction" into three faces: refuting a statement (¬I), proving the contrapositive, and genuine reductio (RAA), with the rule "use the weakest form that works, and say which one you use". This section is about choosing. Which form a proof takes is decided by the shape of the claim and by what each assumption hands over to compute with. The section proves that there are infinitely many primes and that $\sqrt[3]{2}$ is irrational, makes the smallest counterexample of Section 2.2 a method of its own, and ends with a word on existence proofs that name no witness.

2.4.1 Choosing the form

To prove "if P, then Q" there are three ways to start. Assume P and work towards Q: a direct proof (Example (Method: direct proof from a definition)). Assume $\neg Q$ and work towards $\neg P$: the contrapositive, which proves the original by Logic and Proof, Proposition 2.5.2. Or assume P and $\neg Q$ together and work towards a contradiction. A claim that is itself a negation, such as "irrational", "no solution" or "no bijection", has one natural start, face (i): assume the positive statement, reach $\bot$, and conclude the negation by ¬I. The choice is not a matter of taste. Unwind each candidate assumption by its definitions, and ask which one hands over something to compute with.

Example. A negative hypothesis

Let $n \in \mathbb{Z}$. Show that if $n^2 + n + 1$ is not divisible by 3, then n leaves remainder 0 or 2 on division by 3.

Idea (Scratch work). *Direct.* The hypothesis $3 \nmid n^2 + n + 1$ says that no integer k has $n^2 + n + 1 = 3k$. That is a "there is no", and it gives nothing to compute with: no equation, no object.

Contrapositive. The negation of "remainder 0 or remainder 2" is "remainder not 0 and not 2" (Logic and Proof, Proposition 2.5.5). The remainder lies in $\{0, 1, 2\}$ and is unique (Theorem 2.2.3), so this says: remainder 1. So the new assumption is $n = 3q+1$, an equation, and the new goal $3 \mid n^2 + n + 1$ asks for a witness, which the equation may produce.

Givens	Goal
$3 \nmid n^2 + n + 1$	the remainder of n is 0 or 2
(contrapositive) $n = 3q + 1$, $q \in \mathbb{Z}$	$3 \mid n^2 + n + 1$
$n^2 + n + 1 = 9q^2 + 9q + 3$	$n^2 + n + 1 = 3m$: $m = 3q^2 + 3q + 1$, the gap is closed

The direct start stalled at the first line; the contrapositive closed the gap in two.

Solution. We prove the contrapositive: if n does not leave remainder 0 or 2 on division by 3, then $3 \mid n^2+n+1$. Divide n by 3 (Theorem 2.2.3): $n = 3q + r$ with $q \in \mathbb{Z}$ and $r \in \{0, 1, 2\}$ (by discreteness, Proposition 2.1.2 (c)), and r is unique. By assumption $r \neq 0$ and $r \neq 2$, so $r = 1$. Then

$$n^2 + n + 1 = (9q^2 + 6q + 1) + (3q + 1) + 1 = 9q^2 + 9q + 3 = 3(3q^2 + 3q + 1),$$

and $3q^2 + 3q + 1 \in \mathbb{Z}$, so $3 \mid n^2 + n + 1$.

The contrapositive turned a "not divisible" in the hypothesis into a witness to produce, and an "or" in the conclusion into a single case to compute with. The statement is not vacuous: $n = 0$ and $n = 2$ give $n^2 + n + 1 = 1$ and 7, neither divisible by 3.

Quick check. Write the contrapositive and the negation of the statement of Example (A negative hypothesis). Which one is equivalent to it?

Solution. Contrapositive: "if n leaves remainder 1 on division by 3, then $3 \mid n^2+n+1$"; it is equivalent to the statement. Negation: "there is an integer n with $3 \nmid n^2+n+1$ that leaves remainder 1"; it is not equivalent, and it is false by the example.

The example shows the questions to ask before any proof, and they are worth fixing as a method.

Example. Method: choosing direct, contrapositive or contradiction

Template. Unwind P, Q, $\neg P$ and $\neg Q$ by their definitions. If P gives something to compute towards Q, go direct. If $\neg Q$ gives an equation, a case split or an object, and $\neg P$ is a statement you can reach, prove the contrapositive and announce it ("We prove the contrapositive"). If the claim is a negation (irrational, no solution, no bijection, no largest), assume the positive statement and derive a contradiction ($\neg$I). Otherwise assume P and $\neg Q$ together, and use both.

When to use it. Before every proof; at once when the direct attempt stalls, or when the conclusion is an "or", a "not", a "no" or "infinitely many".

The usual failure. A wrong negation: the negation of "A or B" is "not A and not B" (Logic and Proof, Proposition 2.5.5). A "contradiction" that never uses its assumption $\neg Q$, which is a direct proof in costume (Logic and Proof, Example (A direct proof in costume); for the contrapositive, Logic and Proof, Example (A contrapositive in costume)). Not saying which form is used.

Quick check. Which form, and what first sentence, for the following?

(a) For $x \in \mathbb{R}$, if $x^2 \neq x$, then $x \neq 1$.

(b) There is no integer n with $n^2 = 2$.

(c) For $f\colon X \to Y$ and $g\colon Y \to Z$, if $g \circ f$ is injective, then f is injective.

Solution. *(a)* Contrapositive: "Suppose $x = 1$; then $x^2 = 1 = x$." *(b)* Face (i), since the claim is a negation: "Suppose $n \in \mathbb{Z}$ and $n^2 = 2$." (Then $|n| \leq 1$ gives $n^2 \leq 1$, and $|n| \geq 2$ gives $n^2 \geq 4$.) *(c)* Direct, by the method of Example (Method: proving injectivity): "Let $x_1, x_2 \in X$ with $f(x_1) = f(x_2)$." Then $g(f(x_1)) = g(f(x_2))$, and injectivity of $g \circ f$ gives $x_1 = x_2$.

2.4.2 Infinitely many primes

Logic and Proof, Section 8.1 met Euclid's argument for a finite list of primes (Logic and Proof, Exercise (C1: Euclid without the contradiction)); here is a version that puts, for each n, a prime above n, and Exercise C2 turns the list argument into a bound of its own. Theorem 2.2.5 gives every integer $n \geq 2$ a prime factor. To show that the primes never run out, it is enough to build, for each n, a number all of whose prime factors exceed n. Multiplying $1, 2, \ldots, n$ together and adding 1 does it.

Theorem 2.4.1. There Are Infinitely Many Primes

For every $n \in \mathbb{N}$ there is a prime p with $p > n$.

Idea. The number $n! + 1$ leaves remainder 1 on division by every k with $2 \leq k \leq n$, so none of them divides it. Its prime factor (Theorem 2.2.5) must therefore exceed n. The last step is a face (i) argument inside the proof: suppose $p \leq n$.

Proof. *Step 1.* For every $n \in \mathbb{N}$, $n!$ is a positive integer and $k \mid n!$ for every $k \in \{1, \ldots, n\}$. We use induction on n, following the clauses of $n!$ (Definition 2.3.1). For $n = 0$, $0! = 1$, and there is no k. Suppose the claim holds for n. Then $(n+1)! = n! \cdot (n+1)$ is a positive integer. For $k \leq n$, the hypothesis gives $n! = kj$ with $j \in \mathbb{Z}$, so $(n+1)! = k \cdot j(n+1)$; and $k = n+1$ divides $(n+1)! = n! \cdot (n+1)$. Every $k \in \{1, \ldots, n+1\}$ has $k \leq n$ or $k = n+1$ (Lemma 2.1.1 (e)).

Step 2. Let $n \in \mathbb{N}$, and let $N := n! + 1$. By Step 1 and Proposition 2.1.2 (b), $n! \geq 1$, so $N \geq 2$, and N has a prime factor p (Theorem 2.2.5). Suppose $p \leq n$. Since $p \geq 2$, $p \in \{1, \ldots, n\}$, so $p \mid n!$ by Step 1. From $p \mid N$ and $p \mid n!$, $p \mid N - n! = 1$ (Example (Divisors of a combination)). So $1 = kp$ with $k \in \mathbb{Z}$; then $k > 0$, so $k \geq 1$, and $p \leq kp = 1$, against $p \geq 2$. Hence $p > n$, by trichotomy. This proves the theorem. ∎

Warning. **The proof does not say that $n! + 1$ is prime.** For $n = 4$, $n! + 1 = 25 = 5 \cdot 5$. The proof uses only that $n! + 1$ has some prime factor, and shows that every one of them exceeds n.

Quick check. Run the proof at $n = 5$: compute N and a prime $p > 5$ dividing it. Is N prime?

Solution. $N = 5! + 1 = 121 = 11 \cdot 11$, and $p = 11 > 5$. N is not prime.

Remark (Looking ahead). Section 2.5 defines infinite sets; with that definition, the set of primes is infinite.

2.4.3 An irrational number by lowest terms

Logic and Proof proved $\sqrt{2}$ irrational (Logic and Proof, Theorem 2.2.1) with the fact (L), which Lemma 2.2.4 now proves. The same lemma settles a cube root. Here $\sqrt[3]{2}$ is the real number x with $x^3 = 2$; its existence and uniqueness are school facts, as in Section 1.6.

Proposition 2.4.2. The Cube Root of 2 Is Irrational

$\sqrt[3]{2}$ is irrational.

Idea. The claim is a negation, so face (i): suppose $\sqrt[3]{2} = p/q$ in the form of Lemma 2.2.4, and show that p and q are both even. One step, "p^3 even $\Rightarrow$ p even", is itself a contrapositive.

Proof. A contrapositive first. For $p \in \mathbb{Z}$, if p^3 is even, then p is even. Suppose p is not even. Then p is odd (Theorem 1.1.2), $p = 2k + 1$ with $k \in \mathbb{Z}$, and

$$p^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$$

is odd, hence not even (Theorem 1.1.2).

The claim. Suppose $\sqrt[3]{2}$ is rational. By Lemma 2.2.4, $\sqrt[3]{2} = p/q$ with $p \in \mathbb{Z}$, $q \in \mathbb{Z}_{>0}$, and p and q not both even. Cubing, $p^3 = 2q^3$, so p^3 is even, and p is even: $p = 2s$ with $s \in \mathbb{Z}$. Then $8s^3 = 2q^3$, so $q^3 = 4s^3 = 2(2s^3)$ is even, and q is even. So p and q are both even, a contradiction. Hence $\sqrt[3]{2}$ is irrational ($\neg$I).

■

The outer frame is face (i), with no RAA: the proof refutes "$\sqrt[3]{2}$ is rational". The step inside it is face (ii), a contrapositive whose conclusion "p even" is not a negation, so it rests on Logic and Proof, Proposition 2.5.2. (It could also avoid RAA: by Theorem 1.1.2, p is even or odd, and the odd case closes by $\bot$E.) The lemma's "not both even" is the given that the contradiction breaks; without the lemma there would be nothing to contradict.

Quick check. Why does the same proof not show that $\sqrt[3]{3}$ is irrational?

Solution. $p^3 = 3q^3$ gives no parity contradiction: with q odd, p^3 is odd and p is odd, and "not both even" survives. The proof needs "no common divisor 3", which Exercise C2 of

Section 2.2 provides.

2.4.4 The smallest counterexample

Well-ordering gives the same power as strong induction, in a form that often reads more naturally. To prove a claim about every integer from n_0 on, suppose it fails somewhere. The failures form a non-empty set of integers with the integer lower bound n_0, so Corollary 2.1.5 gives a least one. Below it the claim holds. If that is enough to produce a failure that is smaller still, or to show the claim at the least failure after all, we have a contradiction.

Algorithm. To prove "$P(n)$ for every integer $n \geq n_0$" by a **smallest counterexample**:

- *Suppose it fails:* some integer $n \geq n_0$ has $P(n)$ false.
- *Take the least failure:* the set F of integers $n \geq n_0$ with $P(n)$ false is non-empty and has the integer lower bound n_0, so it has a least element m (Corollary 2.1.5; Theorem 2.1.3 when $n_0 \geq 0$, since then $F \subseteq \mathbb{N}$).
- *Use the claim below m:* $P(k)$ holds for every integer k with $n_0 \leq k < m$, since such a k is not in F.
- *Produce a contradiction:* a failure $k < m$, or $P(m)$ itself.

Then F is empty, and $P(n)$ holds for every integer $n \geq n_0$.

The method is strong induction with an RAA box drawn around it. The work done inside the box, "if $P(k)$ for every k with $n_0 \leq k < m$, then $P(m)$", is exactly the hypothesis of Theorem 2.2.2 at m; so any smallest-counterexample proof can be rewritten as a strong induction, and the reverse rewriting works too. Which one to write is a matter of which reads better. A smallest counterexample suits claims whose failure has a natural "smaller failure", like a fraction that can be reduced, or a number with a factor.

Section 2.2 used it in Lemma 2.2.4 and in the proof sketched before Theorem 2.2.5, and its Exercise B2 asks for one.

Example. Method: the smallest counterexample

Template. The four steps of the list above, opening with "Suppose not, and let m be the least integer $\geq n_0$ for which $P(m)$ fails". The least failure is Example (Method: the least element) applied to the set of failures. Worked examples: Lemma 2.2.4 (Section 2.2) and Example (Taking out the threes) below.

When to use it. A failure would give a smaller failure: a number with a factor, a fraction that can be reduced, a representation that can be shortened.

The usual failure. Not checking that the smaller object is still $\geq n_0$ (or positive), so that it lies in the set of failures. Forgetting the case in which no smaller object exists, which must be ruled out directly (in the example below, m not divisible by 3).

Example. Taking out the threes

Show that every positive integer n is $3^a \cdot b$ with $a \in \mathbb{N}$, $b \in \mathbb{Z}$ and $3 \nmid b$.

Idea (Scratch work). This is the argument of Exercise C1 of Section 2.3, with 3 in place of 2; here each step of the method is named. Suppose some positive integer has no such form, and let m be the least one. Unwind what m can be. If $3 \mid m$, say $m = 3m'$, then m' is a smaller positive integer, so it has the form, and one more factor 3 gives m the form too. If $3 \nmid m$, there is no smaller object to pass to; but then $m = 3^0 \cdot m$ already has the form, so m was not a failure at all.

Givens	Goal
m the least positive integer with no form $3^a b$, $3 \nmid b$; every k with $1 \le k < m$ has one	a contradiction
case $3 \nmid m$	$m = 3^0 \cdot m$: m has the form after all
case $m = 3m'$: $1 \le m' < m$, so $m' = 3^a b$ with $3 \nmid b$	$m = 3^{a+1} b$: m has the form; the gap is closed

Solution. Suppose not, and let F be the set of positive integers with no such form. F is a non-empty subset of $\mathbb{N}$, so it has a least element m (Theorem 2.1.3). If $3 \nmid m$, then $m = 3^0 \cdot m$ with $3 \nmid m$, so $m \notin F$, a contradiction. So $m = 3m'$ with $m' \in \mathbb{Z}$; $m' > 0$ since $m > 0$, so $m' \in \mathbb{Z}_{>0}$ (Proposition 2.1.2 (b)), and $m' < 3m' = m$. As m is least in F, $m' \notin F$: $m' = 3^a b$ with $a \in \mathbb{N}$, $b \in \mathbb{Z}$ and $3 \nmid b$. Then $m = 3^{a+1} b$ (Definition 2.3.2), so $m \notin F$, a contradiction. Hence $F = \emptyset$.

Quick check. Write 54 and 45 in the form of Example (Taking out the threes), and say why $m' \notin F$ in the proof.

Solution. $54 = 3^3 \cdot 2$ and $45 = 3^2 \cdot 5$. And m' is a positive integer smaller than the least element of F, so it cannot lie in F.

2.4.5 Existence without a witness

A proof of "there exists" by contradiction, an RAA on a statement $\exists x\, \varphi(x)$, may finish without naming any object. Theorem 2.1.3 was proved so, and the remark after its proof said what that means: the proof shows that a least element exists, not how to find one. *Logic and Proof*, Section 8.7 gave the classical example, an irrational power of an irrational number that is rational, shown to exist between two candidates without saying which one works (Logic and Proof, Theorem 8.7.1). It also gave the book's position: classical rules are allowed, and a proof that names no witness is still a proof.

The proof of Theorem 2.4.1 and the contrapositive of Example (A negative hypothesis) went the other way. The proof of Theorem 2.4.1 names its witness: a prime factor of $n! + 1$, and trying $2, 3, 4, \ldots$ in turn finds the least one. The contrapositive in Example (A negative hypothesis) turned an existence goal into an explicit witness, $m = 3q^2 + 3q + 1$. (The smallest-counterexample proof of Example (Taking out the threes) is formally an RAA, but its two cases describe how to find a and b.) A named witness says more than bare existence, and it can be checked by computation. So the advice is: when a witness is cheap, name it.

2.4.6 Exercises

2.4.6.1 A. Check your understanding

Exercise. A1

(a) Write the converse, the contrapositive and the negation of "if n is prime and $n \geq 3$, then n is odd". Which are true?

(b) Name the form you would choose and write the first sentence (no proofs): (i) $\sqrt[3]{3}$ is irrational; (ii) for $a, b \in \mathbb{Z}$, if $a^2 + b^2$ is odd, then a is even or b is even; (iii) for sets A, B, if $A \cup B = A \cap B$, then $A = B$.

(c) Run the proof of Theorem 2.4.1 at $n = 6$: find N, its least prime factor, and check that it exceeds 6.

(d) "Suppose p is the largest prime. Then $p! + 1$ has a prime factor $q > p$, a contradiction." Which face of "by contradiction" is this, and does the proof name a prime larger than p?

Solution. *(a)* Converse: if n is odd, then n is prime and $n \geq 3$. False: $9 = 3 \cdot 3$. Contrapositive: if n is even, then n is not prime or $n < 3$. It is equivalent to the statement, and true: an even $n \geq 3$ has the divisor $2 \notin \{1, n\}$. Negation: some prime $n \geq 3$ is even. False. ("Not odd" is "even" by Theorem 1.1.2.)

(b) (i) Face (i): "Suppose $\sqrt[3]{3} = p/q$ with $p \in \mathbb{Z}$, $q \in \mathbb{Z}_{>0}$ and no common divisor $d \geq 2$" (Exercise C2 of Section 2.2; "not both even" is not enough, as the last Quick check of the subsection on $\sqrt[3]{2}$ shows). (ii) Contrapositive: "Suppose a and b are both odd", the negation of "a even or b even" by Logic and Proof, Proposition 2.5.5 and Theorem 1.1.2; then a^2 and b^2 are odd (Logic and Proof, Theorem 2.4.4), and $a^2 + b^2$ is even (Example (The parity of a sum)). (iii) Direct, by Example (Method: two inclusions): "Let $x \in A$."

(c) $N = 6! + 1 = 721$. It is not divisible by 2, 3 or 5: $721 = 2 \cdot 360 + 1 = 3 \cdot 240 + 1 = 5 \cdot 144 + 1$. And $721 = 7 \cdot 103$. The least prime factor is $7 > 6$, and 721 is not prime.

(d) Face (i): it refutes "there is a largest prime". Its body names q, so it can be rewritten without contradiction: for every prime p, a prime factor of $p! + 1$ is a larger prime (Theorem 2.4.1 with $n = p$). This is the rewrite of Logic and Proof, Exercise (C1: Euclid without the contradiction), applied to $p! + 1$ in place of Euclid's product.

2.4.6.2 B. Practice

Exercise. B1: Contrapositive

Prove:

(a) for all $a, b \in \mathbb{Z}$, if $3 \nmid a + b$, then $3 \nmid a$ or $3 \nmid b$;

(b) for every $x \in \mathbb{R}$, if $x^2 > 2x + 8$, then $x > 4$ or $x < -2$.

Solution. *(a)* We prove the contrapositive: if $3 \mid a$ and $3 \mid b$, then $3 \mid a + b$; its hypothesis is the negation of "$3 \nmid a$ or $3 \nmid b$" by Logic and Proof, Proposition 2.5.5. With $a = 3k$ and $b = 3l$, $a + b = 3(k + l)$ (Example (Divisors of a combination)).

(b) We prove the contrapositive. Suppose $x \leq 4$ and $x \geq -2$ (the negation of the conclusion, by Logic and Proof, Proposition 2.5.5 and trichotomy). Then $x - 4 \leq 0$ and $x + 2 \geq 0$, so $x^2 - 2x - 8 = (x - 4)(x + 2) \leq 0$, that is, $x^2 \leq 2x + 8$.

Exercise. B2: Contradiction

Prove:

(a) there is no rational number r with $r^2 = r + 1$;

(b) there are no integers m, n with $m^2 - 8n = 5$.

Solution. *(a)* Suppose $r^2 = r + 1$, with $r = p/q$ as in Lemma 2.2.4. Multiplying by q^2, $p^2 = pq + q^2$. Two facts about products: odd times odd is odd, since $(2k + 1)(2l + 1) = 2(2kl + k + l) + 1$, and an even number times any integer is even. Since p and q are not both even, three cases remain. If p, q are odd: p^2 is odd, and $pq + q^2$ is odd plus odd, even (Example (The parity of a sum)). If p is even and q odd: p^2 is even, and $pq + q^2$ is even plus odd, odd. If p is odd and q even: p^2 is odd, and $pq + q^2$ is even. Each case equates an odd and an even integer, against Theorem 1.1.2.

(b) Suppose $m^2 = 8n + 5 = 2(4n + 2) + 1$. Then m^2 is odd, so m is odd (Logic and Proof, Theorem 2.4.4), and $m^2 = 8t + 1$ with $t \in \mathbb{Z}$ by Exercise (B3, used later) (b). So $8(t - n) = 4$, and $2(t - n) = 1$: 1 would be even, against Theorem 1.1.2.

Exercise. B3: Name the move, then complete it

Claim: $n < 2^n$ for every integer $n \geq 1$. Here is a proof with its last step blank.

Suppose not. Then the set F of integers $n \geq 1$ with $n \geq 2^n$ is non-empty and has the integer lower bound 1, so it has a least element m (Corollary 2.1.5). Since $1 < 2 = 2^1$, $m \neq 1$, so $m \geq 2$, and $m - 1$ is an integer with $1 \leq m - 1 < m$.

...

Solution. The move is the smallest counterexample (Example (Method: the smallest counterexample)), and the blank is its last step. As $m - 1 < m$, $m - 1 \notin F$: $m - 1 < 2^{m-1}$. Since $2^{m-1} \in \mathbb{N}$ (Proposition 2.3.4 (d)), discreteness gives $m \leq 2^{m-1}$. And $2^{m-1} < 2^{m-1} \cdot 2 = 2^m$ (Definition 2.3.2, with $m - 1 \in \mathbb{N}$, and $2^{m-1} > 0$ by Proposition 2.3.4 (e)). So $m < 2^m$, that is, $m \notin F$, a contradiction.

Exercise. B4: Prove or disprove

Prove each true statement; refute each false one with a concrete counterexample.

(a) For every $n \in \mathbb{Z}$: if $n^2 - 1$ is not divisible by 5, then n is divisible by 5.

(b) For every $n \in \mathbb{Z}$: if $4 \nmid n^2$, then n is odd.

(c) For every $x \in \mathbb{R}$: if x is irrational, then x^2 is irrational.

(d) For every $x \in \mathbb{R}$: if x^2 is irrational, then x is irrational.

(e) For all positive integers a, b: $a^2 - b^2 \neq 10$.

(f) For every $n \in \mathbb{N}$ there is a prime p with $n < p \leq n + 6$.

Solution.

(a) **False.** Take $n = 2$: $n^2 - 1 = 3$ is not divisible by 5, and neither is 2.

(b) **True.** We prove the contrapositive. If n is not odd, it is even (Theorem 1.1.2), $n = 2k$, and $n^2 = 4k^2$, so $4 \mid n^2$. (Its look-alike "if $4 \mid n^2$, then $4 \mid n$" is false at $n = 2$.)

(c) **False.** Take $x = \sqrt{2}$, irrational by Logic and Proof, Theorem 2.2.1: $x^2 = 2$ is rational.

(d) **True.** We prove the contrapositive: if $x = p/q$ is rational, so is $x^2 = p^2/q^2$.

(e) **True**, by contradiction (face (i)). Suppose $a^2 - b^2 = (a - b)(a + b) = 10$. Since $a + b = (a - b) + 2b$ and $2b$ is even (Theorem 1.1.2), the two factors have the same parity (Example (The parity of a sum)). If both are odd, the product is odd, since $(2k+1)(2l+1) = 2(2kl+k+l)+1$ as in B2 (a), but 10 is even. If both are even, 4 divides the product, but $10 = 4 \cdot 2 + 2$ is not a multiple of 4 (uniqueness in Theorem 2.2.3).

(f) **False.** Take $n = 89$. The numbers $90, \ldots, 95$ are not prime: 90, 92, 94 are even, $91 = 7 \cdot 13$, $93 = 3 \cdot 31$, $95 = 5 \cdot 19$. (89 is the smallest counterexample.)

Verdicts: three true, (b), (d), (e); three false.

2.4.6.3 C. Going deeper

Exercise. C1: Two proofs by contradiction

For each proof below: is the conclusion true? Is the argument valid? Name each flaw, and write a proof in the form that Example (Method: choosing direct, contrapositive or contradiction) recommends.

Proof A. Claim: if $n \in \mathbb{Z}$ is odd, then $n^2 + n$ is even. "Suppose n is odd and $n^2 + n$ is odd. Write $n = 2k + 1$. Then $n^2 + n = (2k + 1)(2k + 2) = 2(2k + 1)(k + 1)$ is even, which contradicts $n^2 + n$ odd."

Proof B. Claim: for every $n \in \mathbb{Z}$, if $n^2 \geq 10$, then $n \geq 4$ or $n \leq -4$.

(1) Suppose $n^2 \geq 10$.

(2) Suppose, for a contradiction, that $n < 4$ or $n > -4$.

(3) Say $n < 4$, so $n \leq 3$.

(4) If also $n \geq -3$, then $n^2 \leq 9 < 10$; so $n \leq -4$.

(5) So $n \leq -4$, which proves the claim.

Solution. Proof A. The conclusion is true and the argument is valid, but the assumption "$n^2 + n$ odd" is used only to clash with the result: a direct proof in costume (Logic and Proof, Example (A direct proof in costume)). Written directly: "Let $n = 2k + 1$ with $k \in \mathbb{Z}$; then $n^2 + n = 2(2k+1)(k+1)$ is even." The hypothesis is not even needed: $n^2 + n = n(n+1)$, and one of n, $n + 1$ is even.

Proof B. The conclusion is true; the argument is not a proof. Line (2) negates "$n \geq 4$ or

$n \leq -4$" wrongly, entry (N11) of Logic and Proof, Example (What is not allowed): the negation is "$n < 4$ and $n > -4$" (Logic and Proof, Proposition 2.5.5). Line (3) takes one disjunct of its own "or" and drops the other, a missing case (N7). Line (5) reaches no contradiction at all. A proof by the contrapositive: if $n < 4$ and $n > -4$, then $-3 \leq n \leq 3$ (Proposition 2.1.2 (c)), so $|n| \leq 3$ and $n^2 \leq 9 < 10$. Or by cases: if $n \geq 4$, done; if $n \leq 3$, then $n \leq -4$ by the computation of line (4).

Marking scheme. (10 points) - 2: judges A's conclusion true and its argument valid, and names the assumption it never uses. - 1: rewrites A as a direct proof. - 3: names the wrong negation in line (2) and gives the correct one (citing (N11) is optional). - 1: names the missing case (N7). - 1: notes that B reaches no contradiction. - 2: gives a correct proof of B's claim.

Exercise. C2: A bound from Euclid's list

Logic and Proof, Section 8.1 proved that for primes $p_1, \ldots, p_k$, with $k \geq 1$, the number $p_1 p_2 \cdots p_k + 1$ has a prime factor different from each p_i (Logic and Proof, Exercise (C1: Euclid without the contradiction)). Here that argument becomes a bound. Let $p_1 := 2$, and let p_{n+1} be the least prime greater than p_n; it exists by Theorem 2.4.1 and Theorem 2.1.3, and Corollary 2.3.2 makes $(p_n)_{n \geq 1}$ a sequence. So $p_2 = 3$, $p_3 = 5$.

(a) Prove that for every $n \geq 1$, every prime $q \leq p_n$ is one of $p_1, \ldots, p_n$.

(b) Prove that $p_{n+1} \leq p_1 p_2 \cdots p_n + 1$ for every $n \geq 1$.

(c) Deduce that $p_n \leq 2^{2^{n-1}}$ for every $n \geq 1$.

(d) Compute $P = p_1 \cdots p_k + 1$ and its prime factors for the lists $3, 5$ and $2, 7$. Is P prime?

Solution. *(a)* By Theorem 2.2.1 with base 1. For $n = 1$: a prime $q \leq 2$ has $q \geq 2$, so $q = 2 = p_1$. Suppose the claim for n, and let $q \leq p_{n+1}$ be prime. If $q \leq p_n$, then q is one of $p_1, \ldots, p_n$ by the hypothesis. Otherwise $q > p_n$, by trichotomy; then q is a prime greater than p_n, so $p_{n+1} \leq q$, as p_{n+1} is the least one, and $q = p_{n+1}$.

(b) Let $n \geq 1$ and $P := p_1 \cdots p_n + 1$. Each $p_i \geq 2$, so $P \geq 3$, and P has a prime factor q (Theorem 2.2.5). Suppose $q = p_i$ for some $i \leq n$. Then p_i divides $p_1 \cdots p_n$, which is p_i times the product of the other entries (school arithmetic of finite products, Definition 2.3.1), so $q \mid P - p_1 \cdots p_n = 1$ (Example (Divisors of a combination)), and $q \leq 1$ as in the proof of Theorem 2.4.1, against $q \geq 2$. So q is none of $p_1, \ldots, p_n$, and by (a) $q \not\leq p_n$: $q > p_n$. Hence $p_{n+1} \leq q$, by the choice of p_{n+1}. Finally $P = kq$ with $k \in \mathbb{Z}$, and $k > 0$ since $P, q > 0$, so $k \geq 1$ and $q \leq kq = P$.

(c) By Theorem 2.2.2 with base 1. For $n = 1$, $p_1 = 2 = 2^{2^0}$. Let $n \geq 1$, and suppose $p_k \leq 2^{2^{k-1}}$ for every k with $1 \leq k \leq n$. By (b), multiplying these n inequalities between positive numbers, Proposition 2.3.4 (a) and Proposition 2.3.6 with $r = 2$,

$$p_{n+1} \leq p_1 \cdots p_n + 1 \leq 2^{2^0 + 2^1 + \cdots + 2^{n-1}} + 1 = 2^{2^n - 1} + 1 \leq 2 \cdot 2^{2^n - 1} = 2^{2^n},$$

where the last inequality uses $1 \leq 2^{2^n - 1}$.

(d) $3 \cdot 5 + 1 = 16 = 2^4$, with prime factor 2. $2 \cdot 7 + 1 = 15 = 3 \cdot 5$, with prime factors 3 and 5. Neither P is prime; each has a prime factor off its list, and neither list is an initial segment $p_1, \ldots, p_k$, so (b) says nothing about them.

Marking scheme. (10 points) - 3: (a), with the base case and the use of leastness of p_{n+1}. - 3: (b): a prime factor q of P off the list, $q > p_n$ by (a), and $p_{n+1} \le q \le P$. - 3: (c): strong induction, the geometric sum in the exponent, and $2^{2^n-1} + 1 \le 2^{2^n}$. - 1: both computations in (d).

Exercise. C3: Challenge: primes of the form $3k + 2$

Prove that for every integer $n \ge 1$ there is a prime $p > n$ with $p = 3k + 2$ for some $k \in \mathbb{Z}$.

Hint: consider $N := 3 \cdot n! - 1$, and Exercise (B2: Products of primes, used later).

Solution. $N = 3(n! - 1) + 2 \ge 2$, since $n! \ge 1$. By Exercise (B2: Products of primes, used later), $N = q_1 \cdots q_r$ with primes q_i. Each $q_i > n$: if $q_i \le n$, then $q_i \mid n!$ (Step 1 of the proof of Theorem 2.4.1), and $q_i \mid N$ (school arithmetic of finite products, as in Exercise C2), so $q_i \mid 3 \cdot n! - N = 1$ (Example (Divisors of a combination)), which is impossible. No q_i is 3, since N leaves remainder 2 on division by 3. Dividing q_i by 3 (Theorem 2.2.3) and using discreteness, each q_i is $3t$, $3t+1$ or $3t+2$. So each q_i is $3t+1$ or $3t+2$: if $q_i = 3t$, then $3 \mid q_i$, and $q_i = 3$ since q_i is prime. If every q_i were of the form $3t + 1$, then N would be too, since $(3a + 1)(3b + 1) = 3(3ab + a + b) + 1$ and an induction on r carries this along the product; but $N = 3(n! - 1) + 2$, against the uniqueness in Theorem 2.2.3. So some q_i is $3t + 2$, and $q_i > n$.

Marking scheme. (10 points) - 2: shows $N \ge 2$ and a factorization into primes. - 2: shows each $q_i > n$ via $q_i \mid n!$. - 1: shows $q_i \ne 3$. - 2: shows each q_i is $3t + 1$ or $3t + 2$. - 2: shows a product of factors $3t + 1$ is $3t + 1$, by induction. - 1: the contradiction with remainder 2.

2.5 Equinumerous Sets and Finite Sets

Section 1.1 left a puzzle half solved: among any five lattice points, two have a lattice point as midpoint, provided that five objects in four boxes always put two in one box. That principle sounds too obvious to need proof, but it is a statement about every finite collection, and "finite" has no definition yet. Section 1.6 supplied the tool: a bijection pairs the elements of two sets one for one. This section makes "the same size" mean "there is a bijection", defines finite sets by pairing with $\{1, \ldots, n\}$, proves the pigeonhole principle and comes back to the five points, and then proves the facts about finite sets on which counting rests. Whether $\mathbb{Q}$ is larger than $\mathbb{N}$ is the question of Chapter 3.

2.5.1 Same size without counting

So far we have compared functions; now we compare sets. The everyday word is "as many as", and we can check it without knowing any numbers. Put two piles of coins on a table, and take one coin from each pile at a time, setting the two aside as a pair. If both piles run out at the same moment, they had the same number of coins. We know this before counting either pile, and a child who cannot count past ten can do it with piles of a thousand. Section 1.6 proved that the bijections are exactly the maps with a two-sided inverse (Theorem 1.6.4), and said that such a pairing is how this book says "the same size".

The pairing is a function from the first pile to the second. Different coins are paired with

different coins, so it is injective; every coin of the second pile is used, so it is surjective. Pairing makes sense for any two sets, finite or not, and that is the definition.

Same size means there is a pairing.

Definition 2.5.1. Equinumerous Sets

Let A and B be sets. We say that A and B are **equinumerous**, and write $|A| = |B|$, if **there exists** a bijection $f\colon A \to B$. In symbols,

$$|A| = |B| \iff \exists f \in B^A \quad (f \text{ is injective} \wedge f \text{ is surjective}).$$

In words: the definition asks for **one** bijection, and it does not care which. Injectivity says that no two elements of A are paired with the same element of B; surjectivity says that no element of B is left over. The statement $|A| = |B|$ is read as a whole, "A and B are equinumerous". It is a relation between two sets. We do not define an object $|A|$, "the size of A", standing alone, and a second-reading fold below explains why the obvious candidate is not available. For finite sets, the definition of a finite set below gives $|A|$ a meaning as a natural number, and the two uses agree.

Here are four examples, the degenerate one first.

- *The empty set.* The empty function $\emptyset \to \emptyset$ of Proposition 1.5.2 (a) is injective and surjective, vacuously: there are no two inputs to compare and no output to reach. So $|\emptyset| = |\emptyset|$. Conversely, if $|A| = |\emptyset|$, there is a function $A \to \emptyset$, so $A = \emptyset$ by Proposition 1.5.2 (b). The empty set is equinumerous with itself and with nothing else. This case is the test case for every statement below about sets "with n elements", at $n = 0$.
- *Three letters and three numbers.* Let a, b, c be three different letters. The function $\{a, b, c\} \to \{1, 2, 3\}$ with $a \mapsto 1$, $b \mapsto 2$, $c \mapsto 3$ sends different letters to different numbers and reaches each of $1, 2, 3$. So $|\{a, b, c\}| = |\{1, 2, 3\}|$.
- *Two intervals of different lengths.* The function $f\colon [0, 1] \to [0, 2]$, $f(x) = 2x$, has the inverse $y \mapsto y/2$, since $y/2 \in [0, 1]$ for $y \in [0, 2]$, $f(y/2) = y$ and $f(x)/2 = x$. By Theorem 1.6.4 it is a bijection, so $|[0, 1]| = |[0, 2]|$. Length and size are different things.
- *The natural numbers and the positive integers.* The function $\mathbb{N} \to \mathbb{Z}_{>0}$, $n \mapsto n + 1$, is a bijection. It is the Quick check near the end of this section, where it shows that $\mathbb{N}$ is infinite.

Quick check. Decide, from Definition 2.5.1: (a) $|\emptyset| = |\{\emptyset\}|$? (b) $|\{1, 2\}| = |\{\{1, 2\}\}|$? (c) $|\{x \in \mathbb{R} : x^2 = -1\}| = |\emptyset|$?

Solution.

(a) No. The set $\{\emptyset\}$ has the element $\emptyset$, and a function $\emptyset \to \{\emptyset\}$ has no values, so it is not surjective. (b) No. The set $\{\{1, 2\}\}$ has one element, so every function $\{1, 2\} \to \{\{1, 2\}\}$ sends 1 and 2 to it and is not injective. (c) Yes. The set $\{x \in \mathbb{R} : x^2 = -1\}$ is empty, and the empty function $\emptyset \to \emptyset$ is a bijection.

A non-example by a minimal change. Shrink $\{1, 2, 3\}$ to $\{1, 2\}$. There is no bijection $\{a, b, c\} \to \{1, 2\}$. Let g be any function $\{a, b, c\} \to \{1, 2\}$. If $g(a) = g(b)$, then g is not injective. Otherwise $g(a)$ and $g(b)$ are 1 and 2 in some order, and $g(c)$, which is 1 or 2, equals one of them.

In every case two different letters share a value. So the clause that fails is injectivity, and it fails for **every** function, which is what "not equinumerous" requires. Surjectivity can hold: $a \mapsto 1$, $b \mapsto 2$, $c \mapsto 2$ reaches both numbers.

Warning. To show that two sets are **not** equinumerous, one map is never enough. The map $x \mapsto x$ from $[0,1]$ to $[0,2]$ is not surjective, since 2 is not a value, and yet $|[0,1]| = |[0,2]|$ by the map $x \mapsto 2x$ above. "Not equinumerous" is a statement about **all** functions, $\forall f \in B^A \neg(f \text{ bijective})$, and a proof of it must deal with an arbitrary f, as the non-example did.

Why this definition. To count a set is to pair it with $\{1, \ldots, n\}$: saying "one, two, three" while pointing at the coins is a bijection from $\{1,2,3\}$ onto the pile. So the definition does not replace counting; it isolates the part of counting that still makes sense when the set is infinite. Each clause has a job. Without injectivity, the surjection $\{1,2,3\} \to \{1\}$ would make a three-element set as large as a one-element set. Without surjectivity, the inclusion $\{1\} \to \{1,2,3\}$ would do the same in the other direction.

The first result says that equinumerosity behaves like equality: reflexive, symmetric and transitive.

Proposition 2.5.1. Equinumerosity Is Reflexive, Symmetric and Transitive

For all sets A, B and C:

(a) $|A| = |A|$;
(b) if $|A| = |B|$, then $|B| = |A|$;
(c) if $|A| = |B|$ and $|B| = |C|$, then $|A| = |C|$.

Proof. *(a)* The identity id_A is injective, since $\mathrm{id}_A(x) = \mathrm{id}_A(y)$ says $x = y$, and surjective, since every $x \in A$ is $\mathrm{id}_A(x)$.

(b) Let $f\colon A \to B$ be a bijection. By Theorem 1.6.4 it has a two-sided inverse $f^{-1}\colon B \to A$, with $f^{-1} \circ f = \mathrm{id}_A$ and $f \circ f^{-1} = \mathrm{id}_B$. Read with the roles exchanged, these two equations say that f is a two-sided inverse of f^{-1} (Definition 1.6.2). So f^{-1} is a bijection $B \to A$, by Theorem 1.6.4 again.

(c) If $f\colon A \to B$ and $g\colon B \to C$ are bijections, then $g \circ f\colon A \to C$ is a bijection by Theorem 1.5.4 (c). This proves the proposition. ∎

Clauses (a)–(c) say that equinumerosity behaves like an equivalence relation: reflexive, symmetric and transitive, as equality is. We do not call it one. Chapter 4 makes "equivalence relation" precise for relations **on a set** X, subsets of $X \times X$; equinumerosity relates any two sets whatever, and there is no set of all sets for it to live on (Theorem 1.2.4). That is also why the book writes $|A| = |B|$ here and keeps the symbol $\sim$ for later.

Remark. Why not define $|A|$ as "the collection of all sets equinumerous with A"? Because that collection is in general not a set. The next paragraph proves this for $A = \{0\}$.

Take $A = \{0\}$. Every singleton $\{x\}$ is equinumerous with $\{0\}$, by $0 \mapsto x$. If the singletons formed a set $\mathcal{S}$, its union $\bigcup \mathcal{S}$ would be a set by (W3) of Section 1.2, and every object x would be an element of it, since $x \in \{x\} \in \mathcal{S}$. That is a set of which every set is an element, which Theorem 1.2.4 rules out.

2.5.2 Finite sets

Counting is pairing with $\{1, \dots, n\}$, so "finite" is defined by such a pairing. Recall from Section 2.1 that for $n \in \mathbb{N}$,

$$\{1, \dots, n\} \coloneqq \{k \in \mathbb{N} : 1 \leq k \leq n\},$$

so that $\{1, \dots, 0\} = \emptyset$, since no k has $1 \leq k \leq 0$.

Definition 2.5.2. Finite Set, Number of Elements

Let A be a set and $n \in \mathbb{N}$. We say that A **has** n **elements** if $|\{1, \dots, n\}| = |A|$, that is, if **there exists** a bijection $\varphi\colon \{1, \dots, n\} \to A$. The set A is **finite** if it has n elements for **some** $n \in \mathbb{N}$. In that case we write $|A| = n$.

In words: φ numbers the elements of A as $\varphi(1), \varphi(2), \dots, \varphi(n)$. Injectivity says that no element gets two numbers; surjectivity says that every element gets one. So a non-empty finite set is $A = \{\varphi(1), \dots, \varphi(n)\}$, a list without repetitions. By Proposition 2.5.1 (b), "A has n elements" is the same as $|A| = |\{1, \dots, n\}|$, so the notation $|A| = n$ is consistent with the relation of Definition 2.5.1.

There is a gap in the notation $|A| = n$. It presents n as **the** number of elements, but the definition only says that **some** n works. Could a set have 3 elements and also 4? It cannot, and a corollary of the pigeonhole principle below proves it. That corollary is the well-definedness step this definition needs. Until it is proved, read $|A| = n$ as "A has n elements".

Examples:

- The empty set has 0 elements: $\{1, \dots, 0\} = \emptyset$, and the empty function $\emptyset \to \emptyset$ is a bijection. Conversely, a set with 0 elements is empty, since a bijection $\emptyset \to A$ is surjective and has no values.
- $\{1, \dots, n\}$ has n elements, by $\mathrm{id}_{\{1,\dots,n\}}$.
- For $n \in \mathbb{N}$, $\{0, \dots, n\}$ has $n + 1$ elements: $k \mapsto k - 1$ maps $\{1, \dots, n + 1\}$ to $\{0, \dots, n\}$, because $k - 1 \in \mathbb{N}$ for $k \neq 0$ (Lemma 2.1.1 (c)) and $k - 1 \leq n$. It has the inverse $j \mapsto j + 1$, so it is a bijection (Theorem 1.6.4).
- The three-letter set $\{a, b, c\}$ has 3 elements, by the inverse of the bijection of the second example after Definition 2.5.1.

Quick check. How many elements does $\{n \in \mathbb{N} : 3 \leq n \leq 7\}$ have? Give the bijection.

Solution. Five, by $k \mapsto k+2$ from $\{1,\dots,5\}$: for $1 \le k \le 5$, $3 \le k+2 \le 7$. Its inverse is $m \mapsto m-2$, which lies in $\{1,\dots,5\}$ for $3 \le m \le 7$, since $m-2 \in \mathbb{N}$ by Lemma 2.1.1 (d). The two maps undo each other, so the first is a bijection (Theorem 1.6.4).

Definition 2.5.3. Infinite Set

A set A is **infinite** if it is not finite: **for every** $n \in \mathbb{N}$ there is **no** bijection $\{1,\dots,n\} \to A$.

To prove a set infinite we must rule out every n at once, and for every n every candidate bijection. Nothing so far does that, not even for $\mathbb{N}$. The tool is the pigeonhole principle, and the last theorem of this section turns it into a usable test.

Shrinking the codomain. One small device is used in the rest of this section and in Chapter 3. Let $f\colon X \to Y$ be a function, and let $C \subseteq Y$ contain every value $f(x)$. The graph of f is then a subset of $X \times C$, and with the codomain C it is a function $X \to C$ with the same values (Definition 1.5.1). We call it "f with codomain C". It is injective if and only if f is, since injectivity speaks only of values. In particular, f with codomain $f(X)$ is surjective (Definition 1.7.1). So an **injective** $f\colon X \to Y$ is a bijection $X \to f(X)$ once its codomain is shrunk, and $|X| = |f(X)|$.

2.5.3 Back to the pigeons

Section 1.1 reduced its question (Q1) to one step: five points, each with one of four parity patterns, put two points on one pattern. In the language of functions, sending each point to its pattern is a map from a five-element set to a four-element set, and the step says that it is not injective. Chapter 1 also found one function from a three-element set to a two-element set that is not injective (Example (Deciding injective and surjective) (c)), and observed without proof that none can be. Here is the general fact, for the standard sets $\{1,\dots,m\}$ and $\{1,\dots,n\}$.

Theorem 2.5.2. Pigeonhole Principle

Let $m, n \in \mathbb{N}$ with $m > n$. Then there is **no** injection $\{1,\dots,m\} \to \{1,\dots,n\}$.

Idea (Scratch work). Induct on the number n of holes. In the step there are $n+1$ holes, and we look at the last one. If no pigeon sits in hole $n+1$, all the pigeons sit in n holes, and the hypothesis applies at once. If pigeon j sits there, there is only one, by injectivity. Move pigeon j to the hole of pigeon m, and send pigeon m away. That leaves $m-1$ pigeons in n holes, still one to a hole, and $m-1 > n$. The hypothesis is used at $m-1$, not at m, so the property we induct on must say "for every m".

On scrap paper, with $n = 1$ and $m = 3$: three pigeons in two holes; if hole 2 is empty, all three sit in hole 1; if pigeon 2 sits in hole 2, move it to pigeon 3's place and send pigeon 3 away. As givens and goal, inside the step:

Givens	Goal
$P(n)$; $m > n+1$; $f\colon \{1,\dots,m\} \to \{1,\dots,n+1\}$ injective	a contradiction

Case 1: $n+1$ is no value of f	f with codomain $\{1,\dots,n\}$ is injective, $m > n$: against $P(n)$
Case 2: $f(j) = n+1$	an injection $\{1,\dots,m-1\} \to \{1,\dots,n\}$, with $m-1 > n$: $g \coloneqq f \circ \sigma$

Before reading on: self-explain the construction of the injection g in Case 2: why are its values in $\{1,\dots,n\}$, and why is it injective?

Proof. For $n \in \mathbb{N}$ let $P(n)$ be the statement

> for every $m \in \mathbb{N}$ with $m > n$, there is no injection $\{1,\dots,m\} \to \{1,\dots,n\}$.

We prove $P(n)$ for every $n \in \mathbb{N}$ by Logic and Proof, Axiom 4.2.1.

Base case $P(0)$. Let $m \in \mathbb{N}$ with $m > 0$. Then $m \geq 1$ (Lemma 2.1.1 (a)), so $1 \in \{1,\dots,m\}$ and the domain is non-empty, while $\{1,\dots,0\} = \emptyset$. By Proposition 1.5.2 (b) there is no function $\{1,\dots,m\} \to \emptyset$ at all, so there is no injection.

Inductive step. Let $n \in \mathbb{N}$ and suppose $P(n)$. Let $m \in \mathbb{N}$ with $m > n+1$, and suppose, for a contradiction, that $f\colon \{1,\dots,m\} \to \{1,\dots,n+1\}$ is injective. There are two cases.

Case 1: $n+1$ is not a value of f. For every i, $f(i) \leq n+1$ and $f(i) \neq n+1$, so $f(i) < n+1$, and $f(i) \leq n$ by Lemma 2.1.1 (e). So f with codomain $\{1,\dots,n\}$ is an injection $\{1,\dots,m\} \to \{1,\dots,n\}$, with $m > n+1 > n$. This contradicts $P(n)$.

Case 2: $f(j) = n+1$ for some $j \in \{1,\dots,m\}$. Since $m > n+1 \geq 1$, we have $m \neq 0$, so $m-1 \in \mathbb{N}$ by Lemma 2.1.1 (c); and $m-1 > n$, by subtracting 1 from $m > n+1$. Define $\sigma\colon \{1,\dots,m-1\} \to \{1,\dots,m\}$ by

$$\sigma(i) \coloneqq \begin{cases} i & \text{if } i \neq j, \\ m & \text{if } i = j. \end{cases}$$

(The second line applies only when $j \leq m-1$; if $j = m$, then $\sigma(i) = i$ for every i.) The map σ is injective: two different inputs other than j keep their different values, and if one input is j, its value is m, while the other has value $i \leq m-1 < m$. Moreover $\sigma(i) \neq j$ for every i: either $\sigma(i) = i \neq j$, or $\sigma(i) = m$, which happens only when $j \leq m-1 < m$.

Let $g \coloneqq f \circ \sigma$. It is injective by Theorem 1.5.4 (a). For every i, $\sigma(i) \neq j$, and f is injective with $f(j) = n+1$, so $g(i) = f(\sigma(i)) \neq n+1$; as in Case 1, $g(i) \in \{1,\dots,n\}$. So g with codomain $\{1,\dots,n\}$ is an injection $\{1,\dots,m-1\} \to \{1,\dots,n\}$, with $m-1 > n$. This contradicts $P(n)$, applied to the number $m-1$.

In both cases the injection f cannot exist, so $P(n+1)$ holds. By Logic and Proof, Axiom 4.2.1, $P(n)$ holds for every $n \in \mathbb{N}$. This proves the theorem.

■

The theorem is about the standard sets only, but bijections carry it to any finite sets. Part (b) below is its mirror image for surjections.

Corollary 2.5.3. Pigeonhole for Finite Sets

Let $m, n \in \mathbb{N}$, let A have m elements, and let B have n elements.

(a) If $m > n$, there is no injection $A \to B$.

(b) If $m < n$, there is no surjection $A \to B$.

Idea. For (a), the bijections of Definition 2.5.2 turn an injection $A \to B$ into an injection $\{1, \dots, m\} \to \{1, \dots, n\}$, which Theorem 2.5.2 forbids. For (b), a surjection $g\colon A \to B$ has a right inverse h, and h is an injection $B \to A$, forbidden by (a). The right inverse is built by a rule: send b to the element of A with the **smallest** number among those that g sends to b (a least element, Example (Method: the least element)).

Proof. Let $\varphi\colon \{1, \dots, m\} \to A$ and $\psi\colon \{1, \dots, n\} \to B$ be bijections (Definition 2.5.2). By Theorem 1.6.4, ψ has an inverse $\psi^{-1}\colon B \to \{1, \dots, n\}$, which is a bijection: the equations $\psi^{-1} \circ \psi = \mathrm{id}$ and $\psi \circ \psi^{-1} = \mathrm{id}$ say that ψ is a two-sided inverse of ψ^{-1} (Definition 1.6.2), so Theorem 1.6.4 applies.

(a) Suppose $m > n$ and $f\colon A \to B$ is injective. Then $\psi^{-1} \circ f \circ \varphi\colon \{1, \dots, m\} \to \{1, \dots, n\}$ is injective by Theorem 1.5.4 (a), which contradicts Theorem 2.5.2.

(b) Suppose $m < n$ and $g\colon A \to B$ is surjective. For $b \in B$ let

$$S_b := \{i \in \{1, \dots, m\} : g(\varphi(i)) = b\}.$$

It is non-empty: since g is onto, $b = g(a)$ for some $a \in A$, and $a = \varphi(i)$ for some i, since φ is onto. By Theorem 2.1.3, S_b has a least element. Define $h\colon B \to A$ by $h(b) := \varphi(\min S_b)$. Then $g(h(b)) = b$ for every $b \in B$, because $\min S_b \in S_b$. So $g \circ h = \mathrm{id}_B$: the function g is a left inverse of h, and h is injective by Theorem 1.6.1 (a). Now h is an injection from the n-element set B to the m-element set A, with $n > m$, which contradicts (a). This proves the corollary. ■

The function h in (b) is defined by a **rule**, "the least element", applied to each b at once, so its existence needs nothing beyond specification. Section 3.2 meets surjections for which no such rule is available, and there the book adds a new principle.

↻ **Second reading** · *Two loose ends from Chapter 1 and* Logic and Proof

Two special cases settle earlier loose ends. With $m = n + 1$, part (a) says that a set with n elements has no $n + 1$ different elements: there is no injection $\{1, \dots, n + 1\} \to A$. That is the second school fact that Logic and Proof, Exercise (C2: A sentence with no finite model, used later) took on trust. With $m = 3$, $n = 2$ in (a) and $m = 2$, $n = 3$ in (b), the corollary gives the two observations after Example (Deciding injective and surjective) in general.

Here is a typical use of (a). Among any three different integers, two have an even sum. Let A be a set of three different integers, and let $p\colon A \to \{0,1\}$ send each a to its remainder r on division by 2 (Theorem 2.2.3), an integer with $0 \le r < 2$; then $r \in \mathbb{N}$ by Proposition 2.1.2 (b), and $r \le 1$ by Lemma 2.1.1 (e), so $r \in \{0,1\}$. The set $\{0,1\}$ has 2 elements, so by (a), p is not injective: there are $a \neq b$ in A with the same remainder r. Writing $a = 2q + r$ and $b = 2q' + r$,

$$a + b = 2(q + q' + r),$$

which is even, since $q + q' + r \in \mathbb{Z}$ (Proposition 2.1.2 (a)). The pigeons are the integers and the holes are the remainders; the whole skill is choosing the holes.

Example. Method: the pigeonhole principle

Template. (1) Choose the pigeons, a set A whose number of elements you know, and the holes, a set B with fewer. (2) Define $p\colon A \to B$, "the hole of a pigeon", and check that its values lie in B. (3) By Corollary 2.5.3 (a), p is not injective: two different pigeons $a \neq a'$ share a hole. (4) Translate "same hole" back into the property you want.

When to use it. The claim says "among any N objects, two have ...", or "some value is taken twice", and N exceeds the number of possible values.

The usual failure. Holes for which sharing a hole does not give the property: choose the holes by what two pigeons should share. Pigeons that need not be different: a list with repeats is not a set with N elements. Claiming to know which two pigeons share a hole.

Example. Back to the five lattice points

Show that among any five different lattice points, two have a lattice point as midpoint.

Idea. The pigeons are the points and the holes are the parity patterns (Example (Method: the pigeonhole principle)).

Solution. Let A be a set of five lattice points, so A has 5 elements. Let $B := \{0,1\} \times \{0,1\}$, which has the 4 elements $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$ (number them 1 to 4). Send $(a,b) \in A$ to (r,s), where r and s are the remainders of a and b on division by 2 (Theorem 2.2.3); $r, s \in \{0,1\}$ as in the three-integers paragraph above, so the values lie in B. Since $5 > 4$, Corollary 2.5.3 (a) gives two different points $(a,b) \neq (c,d)$ in A with the same remainders. Then a and c have the same parity (Definition 1.1.1: remainder 0 means $a = 2q$, which is even, and remainder 1 means $a = 2q+1$, which is odd), and so do b and d, so their midpoint is a lattice point by Example (Same pattern, lattice midpoint). This answers (Q1) of Section 1.1: yes.

The word "different" costs nothing, since a point and itself have that point as midpoint; and the four corners of a unit square (Section 1.1) show that five cannot be lowered to four.

Quick check. Choose pigeons and holes: among any 11 different integers, two differ by a multiple of 10.

Solution. The pigeons are the 11 different integers. The holes are the remainders $0, \dots, 9$ on division by 10 (Theorem 2.2.3), a set with 10 elements. By Corollary 2.5.3 (a) two of the integers, $a \neq b$, have the same remainder r: $a = 10q + r$ and $b = 10q' + r$, so $a - b = 10(q - q')$.

The next corollary is the well-definedness promised after Definition 2.5.2.

Corollary 2.5.4. The Number of Elements Is Unique

Let A be a set and $m, n \in \mathbb{N}$. If A has m elements and A has n elements, then $m = n$.

Proof. Let $\varphi\colon \{1, \dots, m\} \to A$ and $\psi\colon \{1, \dots, n\} \to A$ be bijections. If $m > n$, then $\psi^{-1} \circ \varphi\colon \{1, \dots, m\} \to \{1, \dots, n\}$ is injective (Theorem 1.6.4, Theorem 1.5.4 (a)), which contradicts Theorem 2.5.2. Exchanging the roles of φ and ψ rules out $m < n$ in the same way. By trichotomy, $m = n$. ∎

So a finite set has exactly one number of elements, and from now on $|A| = n$ means "**the** number of elements of A is n".

2.5.4 Subsets and unions of finite sets

Three facts about finite sets are used everywhere below: the sizes of disjoint sets add, a subset is no larger than the whole, and removing one point lowers the size by one. The first uses nothing else from this section, so it comes first.

Proposition 2.5.5. Disjoint Unions

Let $m, n \in \mathbb{N}$, let A have m elements, let B have n elements, and suppose $A \cap B = \emptyset$. Then $A \cup B$ has $m + n$ elements.

Idea. Number A with $1, \dots, m$ and then carry on numbering B with $m+1, \dots, m+n$: shift the numbering of B up by m.

Proof. Let $\varphi\colon \{1, \dots, m\} \to A$ and $\psi\colon \{1, \dots, n\} \to B$ be bijections. Note $m + n \in \mathbb{N}$ by Lemma 2.1.1 (b). For $k \in \{1, \dots, m+n\}$ with $k > m$, we have $m+1 \leq k$ by Lemma 2.1.1 (e), so $k - m \in \mathbb{N}$ with $1 \leq k - m \leq n$ (Lemma 2.1.1 (d)). So we may define $\chi\colon \{1, \dots, m+n\} \to A \cup B$ by

$$\chi(k) \coloneqq \begin{cases} \varphi(k) & \text{if } k \leq m, \\ \psi(k-m) & \text{if } k > m. \end{cases}$$

Injective. Let $\chi(k) = \chi(k')$. If $k, k' \leq m$, then $\varphi(k) = \varphi(k')$ gives $k = k'$. If $k, k' > m$, then $\psi(k-m) = \psi(k'-m)$ gives $k - m = k' - m$, so $k = k'$. If $k \leq m < k'$, then $\chi(k) \in A$ and $\chi(k') \in B$, and $A \cap B = \emptyset$, so $\chi(k) \neq \chi(k')$: this case cannot occur, nor can its mirror image.

Surjective. Let $x \in A \cup B$. If $x \in A$, then $x = \varphi(i)$ with $1 \le i \le m$, and $\chi(i) = x$. If $x \in B$, then $x = \psi(j)$ with $1 \le j \le n$; put $k \coloneqq m + j$, so $m < k \le m + n$, and $\chi(k) = \psi(j) = x$.

So χ is a bijection, and $A \cup B$ has $m + n$ elements.

■

Second reading · *Why the step does not remove a point*

Now subsets. The proof is an induction on the size of the whole set, and it must be set up with care: the step peels off one element, and the obvious way to say "peel off one element" is the corollary after it, on removing a point. But that corollary is proved **from** this proposition. So the step peels off $\varphi(n+1)$ by restricting the bijection φ directly, and cites nothing proved later.

Proposition 2.5.6. Subsets of Finite Sets

Let $n \in \mathbb{N}$, let A have n elements, and let $S \subseteq A$. Then S is finite and has k elements for some $k \le n$. If $S \neq A$, then $k < n$.

Idea. Remove the last element $\varphi(n+1)$ from A. Either it is outside S, and S sits inside the smaller set; or it is in S, and S is its part in the smaller set plus one point, which Proposition 2.5.5 counts.

Proof. For $n \in \mathbb{N}$ let $P(n)$ be the statement

> for every set A with n elements and every $S \subseteq A$, the set S has k elements for some $k \le n$, and $k < n$ if $S \neq A$.

We prove $P(n)$ for every n by Logic and Proof, Axiom 4.2.1.

Base case $P(0)$. A set A with 0 elements is empty, so $S \subseteq \emptyset$ gives $S = \emptyset = A$, which has $0 \le 0$ elements; the second clause is vacuous.

Inductive step. Let $n \in \mathbb{N}$ and suppose $P(n)$. Let A have $n+1$ elements, with a bijection $\varphi\colon \{1, \dots, n+1\} \to A$, and let $S \subseteq A$. Put

$$A' \coloneqq \varphi(\{1, \dots, n\}), \qquad a \coloneqq \varphi(n+1).$$

The restriction of φ to $\{1, \dots, n\}$, with codomain A', is injective and surjective, so A' has n elements. Every element of A is $\varphi(i)$ with $i \le n$ or $i = n+1$ (Lemma 2.1.1 (e)), so $A = A' \cup \{a\}$. And $a \notin A'$: if $a = \varphi(i)$ with $i \le n$, injectivity would give $i = n+1$.

Case $a \notin S$. Then $S \subseteq A'$, and $P(n)$, applied to A' and S, shows that S has $k \le n < n+1$ elements. In this case $S \neq A$, since $a \in A \setminus S$, and indeed $k < n+1$, as required.

Case $a \in S$. Then $S = (S \cap A') \cup \{a\}$, and the union is disjoint because $a \notin A'$. By $P(n)$, applied to A' and $S \cap A' \subseteq A'$, the set $S \cap A'$ has j elements for some $j \le n$. The set $\{a\}$ has 1 element (by $1 \mapsto a$). By Proposition 2.5.5, S has $j + 1 \le n + 1$ elements. If $S \neq A$,

then $S \cap A' \neq A'$, since otherwise $S = A' \cup \{a\} = A$; so $j < n$ by $P(n)$, and $j + 1 < n + 1$.

In both cases $P(n+1)$ holds. By Logic and Proof, Axiom 4.2.1, $P(n)$ holds for every $n \in \mathbb{N}$. This proves the proposition.

■

Read contrapositively, with Corollary 2.5.4: a subset of an n-element set that itself has n elements is the whole set. (If $S \neq A$, its number of elements is $k < n$, and by uniqueness it is not n.) That is the first school fact that Logic and Proof, Exercise (C1: True in every finite model, used later) took on trust.

Quick check. A set $S \subseteq \{1, \ldots, 7\}$ has 7 elements. What is S, and which results say so?

Solution. $S = \{1, \ldots, 7\}$. If $S \neq \{1, \ldots, 7\}$, then Proposition 2.5.6 gives S some number $k < 7$ of elements, and Corollary 2.5.4 forbids S to have both k and 7 elements.

Quick check. Choose parts and sizes: among any 5 different elements of $\{1, 2\} \times \{1, 2, 3\}$, three have the same first coordinate.

Solution. Let $A \subseteq \{1, 2\} \times \{1, 2, 3\}$ have 5 elements, and let A_i be its elements with first coordinate i, for $i = 1, 2$; these are disjoint with union A, and both are finite by Proposition 2.5.6. If both had at most 2 elements, then Proposition 2.5.5 would give A at most 4 elements, contradicting Corollary 2.5.4. So some A_i has $k_i > 2$ elements, that is $k_i \geq 3$ (Lemma 2.1.1 (e)), and a bijection $\varphi\colon \{1, \ldots, k_i\} \to A_i$ gives three different elements $\varphi(1)$, $\varphi(2)$, $\varphi(3)$ of A, all with first coordinate i.

Corollary 2.5.7. Removing a Point

Let $n \in \mathbb{N}$, let A have $n + 1$ elements, and let $a \in A$. Then $A \setminus \{a\}$ has n elements.

Proof. Since $a \in A$, the set $A \setminus \{a\}$ is a proper subset of A, so by Proposition 2.5.6 it has k elements for some $k < n + 1$. Now $A = (A \setminus \{a\}) \cup \{a\}$ is a disjoint union, and $\{a\}$ has 1 element, so A has $k + 1$ elements by Proposition 2.5.5. By Corollary 2.5.4, $k + 1 = n + 1$, so $k = n$.

■

Every later induction on the number of elements uses this corollary in the same way: its step starts from an **arbitrary** set A with $n + 1$ elements, picks some $a \in A$ (there is one, since $n + 1 \geq 1$), and applies the hypothesis to $A \setminus \{a\}$, which has n elements. It never presents the set as "X with one point added" from the outset, which would prove the claim only for sets that come in that form. Here is the first such induction. Chapter 1 promised the count of subsets of

a finite set.

Proposition 2.5.8. Counting Subsets

Let $n \in \mathbb{N}$. A set with n elements has 2^n subsets: if $|A| = n$, then $|\mathcal{P}(A)| = 2^n$.

Idea. Fix one element a. Every subset either leaves a out or contains it, and adding a pairs the subsets of the first kind with those of the second. So the count doubles with each new element.

Proof. We use Logic and Proof, Axiom 4.2.1 on n. *Base case.* A set with 0 elements is $\emptyset$, and $\mathcal{P}(\emptyset) = \{\emptyset\}$ has $1 = 2^0$ element (Definition 2.3.2).

Inductive step. Let $n \in \mathbb{N}$, and suppose every set with n elements has 2^n subsets. Let A have $n+1$ elements, pick $a \in A$, and put $X := A \setminus \{a\}$. By Corollary 2.5.7, X has n elements, so $\mathcal{P}(X)$ has 2^n elements by the hypothesis (here $2^n \in \mathbb{N}$ by Proposition 2.3.4 (d), so the count makes sense; likewise $2^{n+1} \in \mathbb{N}$). Let

$$T := \{S \cup \{a\} : S \in \mathcal{P}(X)\},$$

the image of $\mathcal{P}(X)$ under $S \mapsto S \cup \{a\}$, a function $\mathcal{P}(X) \to \mathcal{P}(A)$.

$\mathcal{P}(A)$ is the disjoint union of $\mathcal{P}(X)$ and T. Every member of T contains a, and no member of $\mathcal{P}(X)$ does, since $a \notin X$; so the union is disjoint. Both sets consist of subsets of A. Conversely, let $U \subseteq A$. If $a \notin U$, then $U \subseteq X$. If $a \in U$, then $U = (U \setminus \{a\}) \cup \{a\}$ with $U \setminus \{a\} \subseteq X$, so $U \in T$.

T has 2^n elements. The map $S \mapsto S \cup \{a\}$, with codomain T, is surjective by the definition of T. It is injective: for $S \subseteq X$ we have $a \notin S$, so $(S \cup \{a\}) \setminus \{a\} = S$, and S can be read back from $S \cup \{a\}$. So it is a bijection $\mathcal{P}(X) \to T$, and composing a bijection $\{1, \dots, 2^n\} \to \mathcal{P}(X)$ with it (Theorem 1.5.4 (c)) shows that T has 2^n elements.

By Proposition 2.5.5, $\mathcal{P}(A)$ has $2^n + 2^n = 2^n \cdot 2 = 2^{n+1}$ elements (Definition 2.3.2). By Logic and Proof, Axiom 4.2.1, the claim holds for every $n \in \mathbb{N}$.

■

Second reading · *Subsets and functions to {0, 1}*

For any set Y, the map $S \mapsto \mathbf{1}_S$, with inverse $f \mapsto \{y \in Y : f(y) = 1\}$, is a bijection $\mathcal{P}(Y) \to \{0,1\}^Y$ onto the set of functions $Y \to \{0,1\}$ (the correspondence of Section 1.5 between subsets and indicator functions). Taking Y with n elements, a set with n elements also has exactly 2^n functions to $\{0,1\}$, and the two counting problems of Chapter 1 are one. Exercise C2 counts all functions between finite sets.

2.5.5 No finite set is equinumerous with a proper subset

For finite sets, “a proper part is smaller” is a theorem.

Theorem 2.5.9. A Finite Set Has No Proper Copy

Let A be a finite set and $B \subsetneq A$. Then A and B are not equinumerous: there is no bijection $A \to B$.

Proof. Let A have n elements, with a bijection $\varphi\colon \{1,\dots,n\} \to A$. By Proposition 2.5.6, B has k elements for some $k < n$, since $B \neq A$. Suppose $g\colon A \to B$ were a bijection. Then $g \circ \varphi\colon \{1,\dots,n\} \to B$ is a bijection (Theorem 1.5.4 (c)), so B also has n elements, and Corollary 2.5.4 gives $k = n$. This contradicts $k < n$. ■

Contradiction at scale. The proof never computes with g. It supposes the bijection, hands it to two theorems already proved, and lets them disagree about the number of elements of B. The claim is a negation, “no bijection”, so this is face (i), chosen by Example (Method: choosing direct, contrapositive or contradiction); but the clash is between results, not between two lines. The proofs of Theorem 2.5.2 and Corollary 2.5.4 have the same shape inside them.

Turned around, the theorem is a test for infinity: **a set that is equinumerous with a proper subset of itself is infinite.** Here is its first use. For the even natural numbers we write

$$2\mathbb{N} := \{2n : n \in \mathbb{N}\},$$

the image of $\mathbb{N}$ under $n \mapsto 2n$.

Example. Hilbert’s Hotel

A hotel has one room for every natural number, and every room is taken. A coach arrives with guests for the odd-numbered rooms: the guest in room n is asked to move to room $2n$. Show that this is a bijection $\mathbb{N} \to 2\mathbb{N}$, that $2\mathbb{N}$ is a proper subset of $\mathbb{N}$, and deduce that $\mathbb{N}$ is infinite.

Solution. Let $d\colon \mathbb{N} \to 2\mathbb{N}$, $d(n) := 2n$. Its values lie in $2\mathbb{N}$ by definition, and $2\mathbb{N} \subseteq \mathbb{N}$ by Lemma 2.1.1 (b). It is injective, since $2n = 2n'$ gives $n = n'$, and surjective, since every element of $2\mathbb{N}$ is $2n = d(n)$ for some $n \in \mathbb{N}$. So $|\mathbb{N}| = |2\mathbb{N}|$.

The inclusion is proper because $1 \notin 2\mathbb{N}$: if $n = 0$, then $2n = 0$; if $n \neq 0$, then $n \geq 1$ (Lemma 2.1.1 (a)) and $2n \geq 2$. So $2n \neq 1$ for every $n \in \mathbb{N}$.

If $\mathbb{N}$ were finite, Theorem 2.5.9 would forbid a bijection from $\mathbb{N}$ onto its proper subset $2\mathbb{N}$. So $\mathbb{N}$ is infinite. Every guest still has a room, and the odd rooms are now free.

The finite intuition “a proper part is smaller” fails for $\mathbb{N}$, and it fails exactly because $\mathbb{N}$ is infinite. Section 3.5 proves that it fails for **every** infinite set.

Warning. $A \subsetneq B$ does not make A smaller than B when B is infinite: $2\mathbb{N} \subsetneq \mathbb{N}$ and $|2\mathbb{N}| = |\mathbb{N}|$. Equinumerous is not "one is a subset of the other", in either direction.

Warning. "Finite" does not mean "bounded". The set $E \coloneqq \{1/n : n \in \mathbb{Z}_{>0}\}$ lies in $[0, 1]$, and it is infinite: $x \mapsto x/(1+x)$ sends $1/n$ to $1/(n+1)$, and it is a bijection from E onto $\{1/n : n \geq 2\}$, with inverse $y \mapsto y/(1-y)$. That set is a proper subset of E, since $1 \in E$ and $1/n \leq 1/2$ for $n \geq 2$.

Quick check. Is $n \mapsto n+1$ a bijection $\mathbb{N} \to \mathbb{N} \setminus \{0\}$? What does that show?

Solution. Yes. Its values lie in $\mathbb{N} \setminus \{0\}$, since $n + 1 \geq 1$. Its inverse is $m \mapsto m - 1$, which is defined on $\mathbb{N} \setminus \{0\}$ because $m - 1 \in \mathbb{N}$ for $m \neq 0$ (Lemma 2.1.1 (c)); the two maps undo each other, so it is a bijection by Theorem 1.6.4. So $\mathbb{N}$ is equinumerous with its proper subset $\mathbb{N} \setminus \{0\} = \mathbb{Z}_{>0}$, and by Theorem 2.5.9, $\mathbb{N}$ is infinite, a second time. In the hotel, every guest moves up one room, and room 0 is free.

Remark. By Definition 2.5.2, a non-empty finite set A with n elements is $\{x_1, \ldots, x_n\}$, with $x_k \coloneqq \varphi(k)$. So when its elements are real numbers it has a maximum and a minimum, by Proposition 2.3.8. Section 2.3 announced this passage from a finite set to a list.

Quick check. Show that the set of primes is infinite.

Solution. Suppose it is finite. It is non-empty, since 2 is prime, so it is $\{p_1, \ldots, p_n\}$ with $n \geq 1$ (Definition 2.5.2 and the remark above), and it has a maximum M (Proposition 2.3.8). By Theorem 2.4.1 there is a prime $p > M$. That prime lies in the set and exceeds its maximum, a contradiction.

Remark (Looking ahead). Chapter 4 defines equivalence relations on a set, and meets equinumerosity again as a relation that behaves like one without living on a set.

2.5.6 Exercises

2.5.6.1 A. Check your understanding

Exercise. A1

(a) Define "A is finite", and write its negation in symbols, with every quantifier shown.

(b) True or false, with a reason: a subset of an infinite set is infinite; a set that has an infinite subset is infinite.

(c) How many injections $\{1,2,3\} \to \{1,2\}$ are there?

(d) Let $f\colon A \to B$, where A and B are finite and A has more elements than B. What does the pigeonhole principle guarantee about f?

Solution.

(a) A is finite if there are $n \in \mathbb{N}$ and a bijection $\varphi\colon \{1,\dots,n\} \to A$ (Definition 2.5.2): $\exists n \in \mathbb{N}\ \exists \varphi \in A^{\{1,\dots,n\}}$ (φ injective $\wedge$ φ surjective). By Logic and Proof, Proposition 6.2.3, applied to each quantifier, and De Morgan, its negation is

$$\forall n \in \mathbb{N}\ \forall \varphi \in A^{\{1,\dots,n\}}\ (\varphi \text{ not injective} \vee \varphi \text{ not surjective}),$$

which is Definition 2.5.3.

(b) The first is false: $\emptyset \subseteq \mathbb{N}$, and $\emptyset$ is finite while $\mathbb{N}$ is infinite (Example (Hilbert's Hotel)). The second is true: if B were finite, every subset of B would be finite by Proposition 2.5.6; so a set with an infinite subset is not finite.

(c) None. By Theorem 2.5.2 with $m = 3 > 2 = n$, there is no injection $\{1,2,3\} \to \{1,2\}$.

(d) That f is not injective (Corollary 2.5.3 (a)): there are two **different** elements $a \neq a'$ of A with $f(a) = f(a')$. It does not say which two, and it says nothing when A has at most as many elements as B.

2.5.6.2 B. Practice

Exercise. B1: Moving the guests

Give explicit bijections $\mathbb{N} \to \mathbb{N} \setminus \{0,1,2\}$, $\mathbb{N} \to \{n \in \mathbb{N} : n \geq 5\}$ and $\mathbb{N} \to \{2n+1 : n \in \mathbb{N}\}$, and prove that each is a bijection by writing down its inverse.

Solution. First. For $m \in \mathbb{N}$: if $m \notin \{0,1,2\}$, then $m \geq 3$. Indeed $m \neq 0$ gives $m \geq 1$ (Lemma 2.1.1 (a)); with $m \neq 1$, $m > 1$, so $m \geq 2$ (Lemma 2.1.1 (e)); with $m \neq 2$, $m \geq 3$ likewise. Conversely every $m \geq 3$ lies outside $\{0,1,2\}$. So $\mathbb{N} \setminus \{0,1,2\} = \{m \in \mathbb{N} : m \geq 3\}$. Let $f(n) \coloneqq n+3$; then $f(n) \in \mathbb{N}$ and $f(n) \geq 3$. Let $g(m) \coloneqq m-3$ for $m \geq 3$; then $g(m) \in \mathbb{N}$ by Lemma 2.1.1 (d). Since $g(f(n)) = n$ and $f(g(m)) = m$, the map f is a bijection by Theorem 1.6.4.

Second. The same with 5 in place of 3: $n \mapsto n+5$, with inverse $m \mapsto m-5$, which lies in $\mathbb{N}$ for $m \geq 5$ by Lemma 2.1.1 (d).

Third. Let $O \coloneqq \{2n+1 : n \in \mathbb{N}\}$, the odd natural numbers, and $f(n) \coloneqq 2n+1$, which lies in O by definition. Every $m \in O$ is $2n+1$ for exactly one $n \in \mathbb{N}$: one by the definition of O, and only one since $2n+1 = 2n'+1$ gives $n = n'$. So $g(m) \coloneqq (m-1)/2$ is that n, a natural number. Then $g(f(n)) = n$ and $f(g(m)) = m$, so f is a bijection $\mathbb{N} \to O$. Each of the three sets is a proper subset of $\mathbb{N}$ equinumerous with $\mathbb{N}$, which shows again that $\mathbb{N}$ is infinite.

Exercise. B2: Choosing the holes

(a) Prove that among any 6 different integers, two have the same remainder on division by 5.

(b) Prove that among any 7 different points of $\{1,2,3\} \times \{1,2,3\}$, three lie in one row, that is, have the same first coordinate.

Hint: in (b), the rows are the holes; how many points can a row take if no row takes three?

Solution.

(a) Let A be a set of 6 integers. By Theorem 2.2.3 with divisor 5, each $a \in A$ has a unique remainder $r(a)$, an integer with $0 \leq r(a) < 5$; then $r(a) \in \mathbb{N}$ by Proposition 2.1.2 (b), and $r(a) \leq 4$ by discreteness, Proposition 2.1.2 (c), so $r(a) \in \{0,\dots,4\}$. This defines $r\colon A \to \{0,\dots,4\}$. The set $\{0,\dots,4\}$ has 5 elements (the third example after Definition 2.5.2). Since $6 > 5$, Corollary 2.5.3 (a) shows that r is not injective: there are $a \neq a'$ in A with $r(a) = r(a')$.

(b) Let $A \subseteq \{1,2,3\} \times \{1,2,3\}$ have 7 elements, and for $i = 1,2,3$ let $A_i \coloneqq \{(x,y) \in A : x = i\}$, the points of A in row i. These sets are pairwise disjoint and their union is A. Each is a subset of A, so it is finite by Proposition 2.5.6; say A_i has k_i elements. If every $k_i \leq 2$, then by Proposition 2.5.5, applied twice, $A = (A_1 \cup A_2) \cup A_3$ has $k_1 + k_2 + k_3 \leq 6$ elements, and Corollary 2.5.4 forbids A to have both that number and 7 elements. So some $k_i > 2$, that is $k_i \geq 3$ (Lemma 2.1.1 (e)); if $\varphi\colon \{1,\dots,k_i\} \to A_i$ is a bijection, then $\varphi(1), \varphi(2), \varphi(3)$ are three different points of A in row i. Seven is the least number that works: the six points with second coordinate 1 or 2 put exactly two in each row.

Exercise. B3: Finite unions

Let $n \in \mathbb{N}$, and let $A_1,\dots,A_n$ be finite sets, that is, a family $(A_i)_{i\in\{1,\dots,n\}}$ of finite sets. Prove that $\bigcup_{i\in\{1,\dots,n\}} A_i$ is finite.

Solution. For $n \in \mathbb{N}$ let $P(n)$ be "for every family $(A_i)_{i\in\{1,\dots,n\}}$ of finite sets, the union $U_n \coloneqq \bigcup_{i\in\{1,\dots,n\}} A_i$ is finite". We use Logic and Proof, Axiom 4.2.1.

Base case. For $n = 0$ the index set is $\{1,\dots,0\} = \emptyset$, and the union of the empty family is $\emptyset$ (Definition 1.3.4: no x lies in some A_i), which has 0 elements.

Step. Suppose $P(n)$, and let $(A_i)_{i\in\{1,\dots,n+1\}}$ be a family of finite sets. Since $\{1,\dots,n+1\} = \{1,\dots,n\} \cup \{n+1\}$, we have $U_{n+1} = U_n \cup A_{n+1}$, and U_n is finite by $P(n)$, applied to the first n sets; say it has p elements. Write

$$U_{n+1} = U_n \cup (A_{n+1} \setminus U_n),$$

a disjoint union. The set $A_{n+1} \setminus U_n$ is a subset of the finite set A_{n+1}, so it is finite by Proposition 2.5.6; say it has q elements. By Proposition 2.5.5, U_{n+1} has $p+q$ elements. By Logic and Proof, Axiom 4.2.1, $P(n)$ holds for every n.

The detour through $A_{n+1} \setminus U_n$ is needed because Proposition 2.5.5 is about **disjoint** sets,

and U_n and A_{n+1} may overlap.

Exercise. B4: Prove or disprove

Prove each true statement and refute each false one with a counterexample.

(a) Among any 12 different integers, two differ by a multiple of 12.

(b) Among any 3 different integers, two have an even sum.

(c) Among any 5 different lattice points of space (points of $\mathbb{Z}^3$), two have a lattice point as midpoint.

(d) If A has 8 elements and $f\colon A \to \{1,2,3,4\}$, then some value of f is taken at least 3 times.

(e) No function from the set of subsets of $\{1,2,3\}$ to $\{1,\dots,7\}$ is injective.

(f) Every injection $\{1,\dots,n\} \to \{1,\dots,n\}$ is surjective.

Solution.

(a) **False.** Take $0,1,\dots,11$. Any two of them differ by an integer d with $1 \le |d| \le 11$, which is not a multiple of 12. Thirteen integers would do, by the argument of the Quick check on 11 integers.

(b) **True.** The pigeons are the three integers and the holes are the two parities (Theorem 1.1.2), a set with 2 elements. Since $3 > 2$, two of the integers have the same parity (Corollary 2.5.3 (a)), and their sum is even (Example (The parity of a sum)).

(c) **False.** Take five of the eight points with all coordinates in $\{0,1\}$ (Exercise C3 of Section 1.1). Two different ones differ in some coordinate, where one has 0 and the other 1; the sum there is 1, so that coordinate of the midpoint is $\frac{1}{2}$.

(d) **False.** Take $A = \{1,\dots,8\}$ and $f(k) :=$ the integer part of $(k+1)/2$, with values $1,1,2,2,3,3,4,4$: each value is taken exactly twice. Nine elements would force some value three times, as in Exercise B2 (b).

(e) **True.** The set of subsets of $\{1,2,3\}$ has $2^3 = 8$ elements (Proposition 2.5.8), and $8 > 7$, so Corollary 2.5.3 (a) applies.

(f) **True.** Let f be such an injection. With its codomain shrunk to its image, f is a bijection, so $f(\{1,\dots,n\})$ has n elements. It is a subset of $\{1,\dots,n\}$, so it is all of it, by the remark after Proposition 2.5.6; that is, f is surjective.

Three are true, (b), (e) and (f), and three are false. Each true item is the method of Example (Method: the pigeonhole principle) with the holes named; each false one either has too few pigeons or holes that do not give the property.

2.5.6.3 C. Going deeper

Exercise. C1: Infinite means arbitrarily large finite pieces

Prove that a set A is infinite if and only if for every $n \in \mathbb{N}$ there is an injection $\{1,\dots,n\} \to A$. In the direction ($\Rightarrow$), say whether your proof makes infinitely many choices at once, and why.

Solution (Hint 1). For ($\Leftarrow$), suppose A has m elements and use the hypothesis at one well-chosen n. For ($\Rightarrow$), induct on n.

Solution (Hint 2). For ($\Rightarrow$): let $P(n)$ be "there is an injection $\{1,\dots,n\} \to A$"; the base case is the empty function.

Solution. ($\Leftarrow$) Suppose the condition holds and, for a contradiction, that A has m elements, with a bijection $\varphi\colon \{1,\dots,m\} \to A$. Take $n \coloneqq m+1$ and an injection $f\colon \{1,\dots,m+1\} \to A$. By Theorem 1.6.4, φ has an inverse $\varphi^{-1}\colon A \to \{1,\dots,m\}$, which is a bijection, since φ is a two-sided inverse of it (Definition 1.6.2, Theorem 1.6.4). Then $\varphi^{-1} \circ f\colon \{1,\dots,m+1\} \to \{1,\dots,m\}$ is injective (Theorem 1.5.4 (a)), which contradicts Theorem 2.5.2. So A is infinite.

($\Rightarrow$) Let A be infinite. For $n \in \mathbb{N}$ let $P(n)$ be "there is an injection $\{1,\dots,n\} \to A$". We use Logic and Proof, Axiom 4.2.1.

Base case. $\{1,\dots,0\} = \emptyset$, and the empty function $\emptyset \to A$ (Proposition 1.5.2 (a)) is injective, vacuously.

Step. Suppose $P(n)$, and let $f\colon \{1,\dots,n\} \to A$ be an injection. With its codomain shrunk to its image $F \coloneqq f(\{1,\dots,n\})$, it is a bijection, so F has n elements. Since A is infinite, $F \neq A$; and $F \subseteq A$, so there is some $a \in A \setminus F$. Define $g\colon \{1,\dots,n+1\} \to A$ by $g(k) \coloneqq f(k)$ for $k \leq n$ and $g(n+1) \coloneqq a$; this is a function because $\{1,\dots,n+1\} = \{1,\dots,n\} \cup \{n+1\}$ and $n+1 \notin \{1,\dots,n\}$ (Lemma 2.1.1 (e)). It is injective: two inputs $\leq n$ are separated by f, and $g(n+1) = a \notin F$ differs from every $g(k)$ with $k \leq n$. So $P(n+1)$ holds. By Logic and Proof, Axiom 4.2.1, $P(n)$ holds for every n.

No infinitely many choices are made. The step uses two existence statements, $P(n)$ and "$A \setminus F \neq \emptyset$", and names one witness for each: one $\exists$E each, inside the proof of the single implication $P(n) \Rightarrow P(n+1)$. Its conclusion, $P(n+1)$, is again an existence statement, so the witnesses never leave the step. Induction then gives $P(n)$ for each n **separately**: for each n **some** injection exists, and different n may use unrelated ones. Gluing the steps into one injection $\mathbb{N} \to A$, with a new point picked at every stage, would require all the picks at once, with no rule saying which point to pick. That is a different statement; Section 3.5 proves it with the principle of choice of Section 3.2.

Marking scheme. (10 points) - 2: ($\Leftarrow$) supposes A has m elements and uses the hypothesis at $n = m+1$ to contradict the pigeonhole principle (Theorem 2.5.2 or Corollary 2.5.3 (a)). - 1: ($\Rightarrow$) sets up an induction on n with the base case $n = 0$ (the empty function); a base $n = 1$ earns the point only if $n = 0$ is also covered (by the empty function). - 3: in the step, shows that the image of the given injection has n elements and is therefore not A, and takes a point outside it. - 2: extends the injection by that point and checks injectivity, including the new value against the old ones. - 2: explains that each step makes finitely many choices inside one implication, so no principle of choice is used, and that building one injection on all of $\mathbb{N}$ would be a different statement. Fatal errors (0 for the step): picking "a new point for every n" to define one function $\mathbb{N} \to A$ and calling it induction; taking a point outside the image without showing the image is not all of A.

Exercise. C2: Counting products and functions

Let $m, n \in \mathbb{N}$, let A have m elements, and let B have n elements.

(a) Prove that $A \times B$ has mn elements.

(b) Prove that the set B^A of functions $A \to B$ has n^m elements.

(c) Check your formula in (b) against Proposition 1.5.2 in the cases $m = 0$ and $m \geq 1$, $n = 0$.

Solution (Hint 1). Induct on m, with B fixed, and remove one point a from A by Corollary 2.5.7.

Solution (Hint 2). For (b), a function on A is the same as a function on $A \setminus \{a\}$ together with one value at a: consider $f \mapsto (f|_{A\setminus\{a\}}, f(a))$.

Solution.

(a) Fix B with n elements. For $m \in \mathbb{N}$ let $P(m)$ be "for every set A with m elements, $A \times B$ has mn elements" ($mn \in \mathbb{N}$ by Lemma 2.1.1 (b)). *Base case.* If A has 0 elements, then $A = \emptyset$, and $A \times B = \emptyset$, since a pair in it would need a first coordinate in $\emptyset$. It has $0 = 0 \cdot n$ elements. *Step.* Suppose $P(m)$, let A have $m + 1$ elements, pick $a \in A$, and put $A' \coloneqq A \setminus \{a\}$, which has m elements by Corollary 2.5.7. Then

$$A \times B = (A' \times B) \cup (\{a\} \times B),$$

and the union is disjoint, since first coordinates in A' differ from a (Definition 1.4.1). The first set has mn elements by $P(m)$. The map $B \to \{a\} \times B$, $b \mapsto (a, b)$, is injective by Definition 1.4.1 and surjective by Definition 1.4.2, so $\{a\} \times B$ has n elements. By Proposition 2.5.5, $A \times B$ has $mn + n = (m + 1)n$ elements. By Logic and Proof, Axiom 4.2.1, $P(m)$ holds for every m, and B was arbitrary.

(b) Fix B with n elements, and let $Q(m)$ be "for every set A with m elements, B^A has n^m elements" ($n^m \in \mathbb{N}$ by Proposition 2.3.4 (d)). *Base case.* $A = \emptyset$, and by Proposition 1.5.2 (a), $B^\emptyset$ has exactly one element, the empty function; $n^0 = 1$ (Definition 2.3.2), also when $n = 0$. *Step.* Suppose $Q(m)$, let A have $m + 1$ elements, pick $a \in A$, and let $A' \coloneqq A \setminus \{a\}$, with m elements. Define

$$R\colon B^A \to B^{A'} \times B, \qquad R(f) \coloneqq (f|_{A'}, f(a)).$$

Injective: if $R(f) = R(f')$, then f and f' agree on A' and at a, hence on $A = A' \cup \{a\}$, and they have the same domain and codomain, so $f = f'$ by Proposition 1.5.1. *Surjective:* given $(h, b) \in B^{A'} \times B$, let f have graph $G \cup \{(a, b)\}$, where G is the graph of h, and codomain B. Each $x \in A'$ has exactly one partner, its h-value, because (a, b) has first coordinate $a \notin A'$; and a has exactly one, b, because every pair of G has first coordinate in A'. So $f \in B^A$, and $R(f) = (h, b)$. Hence R is a bijection. By $Q(m)$, $B^{A'}$ has n^m elements, so by (a), applied to the sets $B^{A'}$ and B, the product $B^{A'} \times B$ has $n^m \cdot n = n^{m+1}$ elements (Definition 2.3.2). Since R is a bijection, $\left|B^A\right| = \left|B^{A'} \times B\right|$ (Definition 2.5.1), and $\left|\{1, \ldots, n^{m+1}\}\right| = \left|B^{A'} \times B\right|$. By Proposition 2.5.1 (b) and

(c), $|\{1,\dots,n^{m+1}\}| = \left|B^A\right|$, that is, B^A has n^{m+1} elements. By Logic and Proof, Axiom 4.2.1, $Q(m)$ holds for every m.

(c) For $m = 0$: $B^\emptyset$ has one element by Proposition 1.5.2 (a), and $n^0 = 1$, even for $n = 0$. For $m \geq 1$ and $n = 0$: $A \neq \emptyset$, so there is no function $A \to \emptyset$ by Proposition 1.5.2 (b), and $B^A = \emptyset$ has 0 elements; and $0^m = 0^{m-1} \cdot 0 = 0$. Both agree with (b). With $B = \{0,1\}$, (b) recovers the count 2^m of the paragraph after Proposition 2.5.8.

Marking scheme. (10 points) - 2: sets up each induction on m with B fixed, and handles $m = 0$ (the empty product; the empty function). - 2: in each step, takes an **arbitrary** A with $m+1$ elements, removes one point by Corollary 2.5.7, and applies the hypothesis to the rest. - 2: (a) splits $A \times B$ into two disjoint pieces and counts $\{a\} \times B$ by a bijection with B. - 3: (b) gives a bijection between B^A and $B^{A'} \times B$, checking injectivity (equality of functions) and surjectivity (the extended graph is a function). - 1: (c) checks both degenerate cases against Proposition 1.5.2. - Direct route for (a): composing the given bijections with a bijection $\{1,\dots,m\}\times\{1,\dots,n\} \to \{1,\dots,mn\}$, e.g. $(i,j) \mapsto (i-1)n+j$, with injectivity and surjectivity checked (for example by Theorem 2.2.3) and the case $m = 0$ or $n = 0$ handled, earns the 2 points of the (a) line and the (a) halves (1 point each) of the two induction lines. Fatal errors (0 for the step): "each of the m elements has n possible values, so n^m" with no bijection or induction; a step that applies the hypothesis to a set not shown to have m elements.

2.5.6.4 R. Review

Exercise. R1

Decide whether each function is injective and whether it is surjective. Justify your answers.

(a) $g\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $g(a,b) \coloneqq 4a + 6b$.

(b) $k\colon \mathbb{Z} \to \mathbb{Z}$, $k(n) \coloneqq 3n + 1$.

Solution. *(a)* g is neither injective nor surjective. Not surjective (Definition 1.5.4): 1 is not a value. Every value $g(a,b) = 2(2a+3b)$ is even, with $2a+3b \in \mathbb{Z}$ by Proposition 2.1.2 (a) (Definition 1.1.1), while $1 = 2 \cdot 0 + 1$ is odd, and no integer is both (Theorem 1.1.2). Not injective (Definition 1.5.3): $g(3,-2) = 12 - 12 = 0 = g(0,0)$, and $(3,-2) \neq (0,0)$, since their first coordinates differ (Definition 1.4.1). The method of Example (Method: proving surjectivity) has nothing to work with here: a witness for the value 1 would be a pair with $4a + 6b = 1$, and the parity argument shows there is none.

(b) k is injective and not surjective. Injective, by the method of Example (Method: proving injectivity): if $3n+1 = 3n'+1$, then $3n = 3n'$ and $n = n'$. Not surjective (Definition 1.5.4): 0 is not a value. If $3n+1 = 0$ for some $n \in \mathbb{Z}$, then $0 = 3n+1$ and $0 = 3\cdot 0+0$ are two divisions of 0 by 3, with remainders 1 and 0 in $\{0,1,2\}$, against the uniqueness in Theorem 2.2.3.

Exercise. R2

For a set X and a property $R(x,y)$ of two elements of X, consider the statements

$$\text{(S1)}\ \ \exists x \in X\ \forall y \in X\ \ R(x,y), \qquad \text{(S2)}\ \ \forall y \in X\ \exists x \in X\ \ R(x,y).$$

(a) Decide (S1) and (S2) for $R(x, y)$: "$x \mid y$", first with $X = \{1, \dots, 6\}$, then with $X = \{2, \dots, 6\}$.

(b) Decide (S1) and (S2) for $X = \mathbb{Z}$ and $R(x, y)$: "$x + y = 0$".

(c) Prove that (S1) implies (S2) for every X and R.

Solution. (a) For $X = \{1, \dots, 6\}$ both hold: $x = 1$ divides every y ($y = y \cdot 1$), which is (S1); and (S2) follows by (c). For $X = \{2, \dots, 6\}$, (S2) holds with $x \coloneqq y$, since $y = 1 \cdot y$. (S1) fails: its negation is $\forall x \in X\ \exists y \in X\ \ x \nmid y$ (Logic and Proof, Proposition 6.2.3), and for $x = 2$ take $y = 3$, for $x \in \{3, \dots, 6\}$ take $y = 2$, since a positive divisor of 2 is at most 2.

(b) (S2) holds: for $y \in \mathbb{Z}$, $x \coloneqq -y \in \mathbb{Z}$ has $x + y = 0$. (S1) fails: its negation is $\forall x \in \mathbb{Z}\ \exists y \in \mathbb{Z}\ \ x + y \neq 0$, and for $x \in \mathbb{Z}$ the choice $y \coloneqq 1 - x$, an integer by Proposition 2.1.2 (a), gives $x + y = 1 \neq 0$.

(c) Suppose (S1), and let $x_0 \in X$ be a witness: $R(x_0, y)$ for every $y \in X$ ($\exists$E). Let $y \in X$. Then $R(x_0, y)$, so $\exists x \in X\ R(x, y)$, with witness x_0 ($\exists$I). As y was arbitrary, (S2) holds ($\forall$I). This is Logic and Proof, Proposition 5.6.2, with bounded quantifiers. The converse fails, by (a) for $X = \{2, \dots, 6\}$ and by (b): one x for all y is more than one x for each y.

Exercise. R3

Let v and w be valuations such that every atom true under v is true under w. Prove that every formula built from atoms with $\wedge$ and $\vee$ alone (no $\neg$, $\bot$, $\to$ or $\leftrightarrow$) that is true under v is true under w. Deduce that $\neg p$ is equivalent to no such formula.

Solution. By structural induction (Logic and Proof, Theorem 4.3.1), with $P(\varphi)$: "if φ contains none of $\neg$, $\bot$, $\to$, $\leftrightarrow$ and $v(\varphi) = \mathrm{T}$, then $w(\varphi) = \mathrm{T}$". Truth values are those of Logic and Proof, Definition 4.4.2.

Atoms and $\bot$. For an atom p with $v(p) = \mathrm{T}$, $w(p) = \mathrm{T}$ by the hypothesis on v and w. The formula $\bot$ contains $\bot$, so $P(\bot)$ holds vacuously.

Step for $\neg$. $\neg\varphi$ contains $\neg$, so $P(\neg\varphi)$ holds vacuously.

Step for $(\varphi \circ \psi)$. If $\circ$ is $\to$ or $\leftrightarrow$, P holds vacuously. Otherwise, if $(\varphi \circ \psi)$ contains none of the four symbols, neither do φ and ψ, whose symbols are among its own, so $P(\varphi)$ and $P(\psi)$ apply to them. For $\circ = \wedge$: $v(\varphi \wedge \psi) = \mathrm{T}$ gives $v(\varphi) = v(\psi) = \mathrm{T}$, so $w(\varphi) = w(\psi) = \mathrm{T}$, and $w(\varphi \wedge \psi) = \mathrm{T}$. For $\circ = \vee$: $v(\varphi) = \mathrm{T}$ or $v(\psi) = \mathrm{T}$, so $w(\varphi) = \mathrm{T}$ or $w(\psi) = \mathrm{T}$, and $w(\varphi \vee \psi) = \mathrm{T}$.

The consequence. Let v be the all-F valuation and w the all-T valuation; every atom true under v (there is none) is true under w. Then $v(\neg p) = \mathrm{T}$ and $w(\neg p) = \mathrm{F}$. If φ, built with $\wedge$ and $\vee$ alone, were equivalent to $\neg p$, it would have the same value as $\neg p$ under every valuation: $v(\varphi) = \mathrm{T}$, hence $w(\varphi) = \mathrm{T}$ by the first part, against $w(\varphi) = w(\neg p) = \mathrm{F}$.

This consequence is a special case of Logic and Proof, Theorem 4.9.6 (b), which allows $\to$ as well and looks only at the all-T row; here the $\wedge/\vee$ case comes out of the stronger statement that such formulas are monotone in the valuation.

Chapter 3

Countable and Uncountable Sets

Are there more rational numbers than natural numbers? The rationals are dense, with a third between any two, while the naturals are spread out one unit apart; and yet the answer is no, because the rationals can be listed. Are there more real numbers than rationals? Yes: no list of real numbers, however cleverly it is made, contains them all. This chapter makes "more" exact, with bijections and injections in place of counting, and proves both answers. It then shows that there is no largest size at all: by Cantor's theorem, the set of subsets of any set is strictly bigger than the set itself. A second motivating question comes from school: *why does* $0.999\ldots = 1$ *need a definition at all?* The answer is in Section 3.3, where a decimal expansion is defined with finite sums only, and $0.999\ldots = 1$ becomes true by that definition. Sections 3.1–3.4 teach one method of proof each on the way: list a set, name the choices a proof makes, run a diagonal, and compare sizes by injections both ways. The last section adds, multiplies and raises sizes to powers, and finds that the plane, the sequences of natural numbers and the subsets of $\mathbb{N}$ all have exactly as many elements as the line; it teaches two more methods, encode and decode, and prove a law of sizes by a bijection.

On the way the chapter meets a principle that the rules of logic and the working rules for sets do not supply: making infinitely many arbitrary choices at once. The obvious proof that a countable union of countable sets is countable needs a list of every set of the family at the same time, and no rule produces one. The chapter states the missing principle as the axiom of choice, marks the line of each proof that uses it, and shows how often a rule (the least element, a formula) makes it unnecessary. It starts from the finite sets of Section 2.5 and the pigeonhole principle.

What you need. *Logic and Proof*, Chapters 1–8, and *Sets and Functions*, Chapters 1–2. Induction (Logic and Proof, Axiom 4.2.1) from *Logic and Proof*, Chapter 4. From *Logic and Proof*, Chapter 5, the rule $\exists$E (Logic and Proof, Definition 5.6.1): Section 3.2 shows why one use of it names one object and cannot name infinitely many. From *Logic and Proof*, Chapters 2 and 6, excluded middle (Logic and Proof, Proposition 2.5.3) and the negation of quantifiers (Logic and Proof, Proposition 6.2.1). From *Logic and Proof*, Chapter 8, the catalogue of what a proof may not do (Logic and Proof, Example (What is not allowed)). The irrationality of $\sqrt{2}$ (Logic and Proof, Theorem 2.2.1), used in one example of Section 3.1. From Chapter 1: the empty set and its uniqueness (Definition 1.2.4, Proposition 1.2.3); sets cut out by a property (Definition 1.2.3) and Russell's theorem (Theorem 1.2.4); power sets, families and their unions (Definition 1.3.2, Definition 1.3.3, Definition 1.3.4); ordered pairs and products (Definition 1.4.1, Definition 1.4.2, Proposition 1.4.1); functions, the empty function and equality of functions (Definition 1.5.1, Proposition 1.5.2, Proposition 1.5.1); injective, surjective and bijective maps and their composites (Definition 1.5.3, Definition 1.5.4, Theorem 1.5.4), with the methods for proving injectivity and surjectivity (Example (Method: proving injectivity), Example (Method: proving surjec-

tivity)); inverses (Definition 1.6.1, Theorem 1.6.4, Theorem 1.6.1, Proposition 1.6.2); images and preimages (Definition 1.7.1, Definition 1.7.2); the indicator function of a subset (Section 1.5, Example (First functions) (d)) and associativity of composition (Proposition 1.5.3). From Chapter 2: the arithmetic of $\mathbb{N}$ and $\mathbb{Z}$ (Lemma 2.1.1, Proposition 2.1.2), well-ordering (Theorem 2.1.3), induction from any base (Theorem 2.2.1), the division algorithm (Theorem 2.2.3), definition by recursion (Theorem 2.3.1), powers and sums (Definition 2.3.2, Proposition 2.3.4, Definition 2.3.1, Proposition 2.3.6), and the largest element of a finite set of numbers (Proposition 2.3.8); equinumerous, finite and infinite sets (Definition 2.5.1, Proposition 2.5.1, Definition 2.5.2, Definition 2.5.3), removing a point and the uniqueness of the number of elements (Corollary 2.5.7, Corollary 2.5.4), the pigeonhole principle (Theorem 2.5.2, Corollary 2.5.3), subsets and disjoint unions of finite sets (Proposition 2.5.6, Proposition 2.5.5), the 2^n subsets of an n-element set (Proposition 2.5.8), the number of elements of a product (Exercise (C2: Counting products and functions)), and the fact that no finite set is equinumerous with a proper subset (Theorem 2.5.9, Example (Hilbert's Hotel)); and the methods of the least element and of pigeonhole (Example (Method: the least element), Example (Method: the pigeonhole principle)). The arithmetic and order of $\mathbb{R}$ are school facts in examples, as in the earlier chapters. Section 3.3 states three school facts about decimal expansions, (D1)–(D3), and Sections 3.3, 3.4 and 3.6 use them by name without proof; Section 3.2 uses one fact from school algebra, that a non-zero polynomial of degree d has at most d real roots.

Time. About 35 hours on the core track (all of A, one B and one C per section, the exit checks); about 55 hours for everything.

3.0.1 Roadmap

- **Countable sets.** Countable as listable with repetitions allowed (empty, or the image of $\mathbb{N}$), the equivalent forms "an injection into $\mathbb{N}$" and "finite or countably infinite", closure under subsets, images, unions of two sets and finite products, and the countability of $\mathbb{N}\times\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$; the method: list a set, by a surjection from $\mathbb{N}$ or an injection into $\mathbb{N}$.
- **Countable unions and the axiom of choice.** The step in the proof for countable unions that no rule justifies, the axiom of choice that licenses it, the constructions that look like choice and are not, right inverses of surjections, countable unions of countable sets, and the countability of the algebraic numbers; the method: name each choice a proof makes.
- **Diagonal arguments: uncountable sets and Cantor's theorem.** The diagonal argument for 0–1 sequences, opening with the five-string game of Section 1.5, Cantor's theorem that no map from a set onto its power set exists, decimal expansions defined with finite sums, the uncountability of $\mathbb{R}$, and the existence of transcendental numbers; the method: the diagonal.
- **Comparing sizes: the Schröder–Bernstein theorem.** Comparing sizes by injections, its exchange with surjections at the price of choice, the Schröder–Bernstein theorem proved without choice, and every interval with more than one point equinumerous with $\mathbb{R}$; the method: injections both ways; whether any two sets are comparable is left open.
- **Infinite sets.** Every infinite set contains a countably infinite subset (a stronger use of choice), so $\mathbb{N}$ is the smallest infinite size, and a set is infinite exactly when it is equinumerous with a proper subset of itself.
- **Cardinal arithmetic.** Sums as disjoint unions, products and powers of sets compared by size; the laws $\left|X^{Y\sqcup Z}\right| = \left|X^Y \times X^Z\right|$ and $\left|(X^Y)^Z\right| = \left|X^{Y\times Z}\right|$ proved by bijections; subsets as 0–1 functions; no set of all sets, once more; and $\mathbb{R}$, $\mathbb{R}\times\mathbb{R}$, $\mathbb{N}^{\mathbb{N}}$, $\mathbb{R}^{\mathbb{N}}$ and $\mathcal{P}(\mathbb{N})$ all of one size; the methods: encode and decode, and prove a law of sizes by a bijection. The review exercises reach back across this volume and *Logic and Proof*.

3.0.2 Named moves

Each is a method box in the section named at the end of its line; the later sections use the move again.

- **List it** (Example (Method: list it)). To show a set countable, give a surjection from $\mathbb{N}$ or an injection into $\mathbb{N}$, whichever is cheaper to check; a list may repeat, and an injection only has to keep different elements apart. (Section 3.1)
- **Name the choice** (Example (Method: name the choice)). When a proof picks one object for each of infinitely many indices and no rule names it, say at that line that the axiom of choice is used; a least element or a formula is a rule, and needs no choice. (Section 3.2)
- **The diagonal** (Example (Method: the diagonal)). Given any list, build an object that differs from the n-th entry at the n-th place; it is not on the list, and since the list was arbitrary, no list contains everything. (Section 3.3)
- **Injections both ways** (Example (Method: injections both ways)). To show $|A| = |B|$, find an injection $A \to B$ and an injection $B \to A$ and invoke the Schröder–Bernstein theorem, instead of hunting for the bijection. (Section 3.4)
- **Encode and decode** (Example (Method: build a bijection by encoding and decoding)). To build a bijection, say what an element must record, write the code and the decoder, and check both round trips. (Section 3.6)
- **A law by a bijection** (Example (Method: prove a law of sizes by a bijection of sets)). To prove a law of sizes, write out an element of each side and regroup it into an element of the other side, never computing with $|\cdot|$ as if it were a number. (Section 3.6)

3.0.3 Threads

- **The five strings.** Section 1.5 plants a game: write a string of five symbols not on a given list of five. Section 3.3 opens with the rule that always works (Example (Back to the five strings)), and the same rule, run on infinitely long strings, proves that the 0–1 sequences cannot be listed (Theorem 3.3.1).
- **Russell to Cantor.** Russell's theorem (Section 1.2) built a set that disagrees with each candidate on the candidate itself; Cantor's theorem (Section 3.3, Theorem 3.3.2) is the same construction, as a theorem about sizes, and Section 3.6 proves the last clause of Russell's theorem by sizes: a set of all sets would carry a surjection onto its power set ("No set of all sets, once more").
- **Choice.** Section 1.6 could not build a right inverse of an arbitrary surjection; Section 3.2 adds the axiom of choice that does (Axiom 3.2.1, Theorem 3.2.2), Section 3.5 uses it again (Theorem 3.5.1), and Chapter 6 states its strongest everyday form, Zorn's lemma.
- **Comparability.** Section 3.4 asks whether any two sets are comparable and leaves the question open; Section 6.2 answers it.
- **Same size.** Section 2.5 defined it, Section 3.6 makes it arithmetic, and Section 4.2 names the requirement that arithmetic of sizes not depend on representatives: well-definedness.

3.0.4 Summary

Countable means listable (Definition 3.1.1), in three equivalent forms (Theorem 3.1.2). Countable sets are closed under subsets, images, finite products and, with the axiom of choice, countable unions (Theorem 3.2.3), so $\mathbb{Z}$, $\mathbb{Q}$ and the algebraic numbers are countable. The diagonal shows that the 0–1 sequences, $\mathbb{R}$ and every power set are too big to be listed (Theorem 3.3.1, Theorem 3.3.4, Theorem 3.3.2), so transcendental numbers exist. Sizes are compared by injections, and injections both ways give a bijection, without choice (Theorem 3.4.3). Every infinite set contains a copy of $\mathbb{N}$, by choice (Theorem 3.5.1), and has a proper subset of its own size

(Theorem 3.5.2).

Sizes add, multiply and exponentiate by disjoint unions, products and sets of functions, with the laws of exponents proved by bijections (Theorem 3.6.3); so $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$ and the plane, $\mathbb{N}^{\mathbb{N}}$ and $\mathbb{R}^{\mathbb{N}}$ are the size of the line (Theorem 3.6.6, Theorem 3.6.7, Theorem 3.6.8, Corollary 3.6.9).

What is open: are any two sets comparable? Chapter 6 answers it. Next, Chapter 4 studies relations, and "same size" returns there as an example.

3.0.5 Terms

- **algebraic number**: a real root of a non-zero polynomial with integer coefficients (Section 3.2, before Theorem 3.2.4).
- **at most as big as, strictly smaller**: $|A| \leq |B|$ if there is an injection $A \to B$; $|A| < |B|$ if moreover there is no bijection (Definition 3.4.1).
- **choice function**: a function c on the index set of a family with $c(i) \in A_i$ for every i (Axiom 3.2.1).
- **countable**: empty, or the image of a surjection $\mathbb{N} \to A$ (Definition 3.1.1).
- **countably infinite**: equinumerous with $\mathbb{N}$ (Definition 3.1.2).
- **decimal expansion** of $x \in [0,1]$: a digit sequence with $t_n \leq x \leq t_n + 10^{-n}$ for every $n \geq 1$, where t_n is the finite sum of the first n digits (Definition 3.3.1).
- **digit sequence**: a function from $\mathbb{Z}_{>0}$ to $\{0, 1, \ldots, 9\}$ (Definition 3.3.1).
- **disjoint union** $A \sqcup B$: the set $(A \times \{0\}) \cup (B \times \{1\})$ (Definition 3.6.1).
- **transcendental number**: a real number that is not algebraic (Section 3.3, before Corollary 3.3.5).
- **uncountable**: not countable (Definition 3.1.1).

3.1 Countable Sets

Section 2.5 made "the same size" exact and settled the finite sets. It also showed that $\mathbb{N}$ is infinite, because it is equinumerous with its proper subset $2\mathbb{N}$ (Example (Hilbert's Hotel)). The next question is which sets can be put into a list indexed by $\mathbb{N}$. *Analysis on the Real Line*, Chapter 1 already uses the word for these sets, **countable**, in its proof that the real numbers cannot be listed. This section defines it, proves three equivalent forms of it, shows that countable sets are closed under subsets, images, unions of two sets and finite products, and lists the integers and the rationals.

3.1.1 Lists

Can we list the rational numbers as $q_0, q_1, q_2, \ldots$ so that every rational number appears somewhere? Density makes it look impossible. Between any two rationals $p < q$ lies a third, $(p+q)/2$, so no rational has a next one, and a list in increasing order cannot even get from q_0 to q_1. And yet a list need not be in increasing order. It only has to reach every element at some finite position. The rationals can be listed in that sense, and so can many sets that look larger than $\mathbb{N}$.

A list indexed by $\mathbb{N}$ is a function on $\mathbb{N}$, its n-th entry being the value at n. Reaching every element is surjectivity.

Countable means listable, repetitions allowed.

Definition 3.1.1. Countable Set

A set A is **countable** if $A = \emptyset$ or **there exists** a surjection $f\colon \mathbb{N} \to A$. In the second case

$$A = f(\mathbb{N}) = \{f(0), f(1), f(2), \dots\},$$

that is, the elements of A can be listed as $x_0, x_1, x_2, \dots$, with $x_n \coloneqq f(n)$, repetitions allowed. A set that is not countable is **uncountable**. In symbols, A is countable if and only if

$$A = \emptyset \ \vee \ \exists f \in A^{\mathbb{N}} \ \ \forall a \in A \ \ \exists n \in \mathbb{N} \ \ f(n) = a.$$

In words: a non-empty set is countable when some list $x_0, x_1, x_2, \dots$ reaches every one of its elements, each at a **finite** position $n \in \mathbb{N}$. The list may repeat an element as often as it likes, and it need not follow any order. The first clause is there because there is no function at all from $\mathbb{N}$ to $\emptyset$ (Proposition 1.5.2 (b)), so the second clause can never hold for the empty set; without the first clause, $\emptyset$ would be uncountable. For a non-empty set the definition says that it is the image of some function from $\mathbb{N}$, which is how *Analysis on the Real Line*, Chapter 1 states it.

Examples, starting from the smallest:

- $\emptyset$ is countable, by the first clause.
- A non-empty finite set is countable. For three different objects a, b, c, the list $a, b, c, c, c, \dots$, that is $f(0) \coloneqq a$, $f(1) \coloneqq b$ and $f(n) \coloneqq c$ for $n \geq 2$, is a surjection $\mathbb{N} \to \{a, b, c\}$. Repetitions pad a short list out to the length of $\mathbb{N}$.
- $\mathbb{N}$ is countable: $\mathrm{id}_{\mathbb{N}}$ is a surjection.
- The set of squares $\{n^2 : n \in \mathbb{N}\}$ is countable: it is the image of $\mathbb{N}$ under $n \mapsto n^2$, and a function is a surjection onto its image (Section 2.5, "Shrinking the codomain"). In the same way $2\mathbb{N}$ is countable.

A non-example by a minimal change. The list $n \mapsto 2n$ is a list of $2\mathbb{N}$. Read it as a list of $\mathbb{N}$, keeping the rule and changing only the target set, and it fails: the clause "for every $a \in \mathbb{N}$ there is an n with $2n = a$" fails at $a = 1$. This shows that **this** list misses 1, not that $\mathbb{N}$ is uncountable; one map proves nothing about all maps (the warning after the non-example in Section 2.5). Sets that are genuinely uncountable appear in Section 3.3.

Why repetitions are allowed. Two reasons. First, finite sets are then countable with no special case: pad the list by repeating an element, as above. Second, the closure proofs below become short. A function applied to a list gives a list of the image, which may have repetitions even if the first list had none; interleaving lists of two overlapping sets repeats their common elements. If repetitions were forbidden, every such proof would need a step that deletes them. The definition puts that work in one place, the theorem on three ways to say countable below, and does it once.

Sometimes we need the stronger statement that a set has exactly the size of $\mathbb{N}$.

Definition 3.1.2. Countably Infinite Set

A set A is **countably infinite** if $|A| = |\mathbb{N}|$, that is, if there is a bijection $A \to \mathbb{N}$ (equivalently, by Proposition 2.5.1 (b), a bijection $\mathbb{N} \to A$).

So $\mathbb{N}$, $2\mathbb{N}$ and $\mathbb{Z}_{>0}$ are countably infinite (Section 2.5), and a countably infinite set is countable, since a bijection is a surjection.

Warning. In this book "countable" **includes** the finite sets and $\emptyset$. Some books use "countable" to mean "countably infinite" and say "at most countable" for our "countable". Before quoting a theorem about countable sets from elsewhere, check which convention it uses. Here, $\{0, 1\}$ is countable and is not countably infinite.

3.1.2 Subsets of the natural numbers

Every countable set will turn out to be finite or countably infinite, with nothing in between. The heart of that is a fact about subsets of $\mathbb{N}$: an infinite one can be listed in increasing order without gaps.

Lemma 3.1.1. Subsets of the Natural Numbers

Every subset $S \subseteq \mathbb{N}$ is finite or countably infinite.

Idea. If S is infinite, list it in increasing order: s_0 is the least element of S, and s_{n+1} is the least element of S above s_n. Well-ordering supplies each least element, provided the set is non-empty, and it is non-empty because S has elements beyond any bound, being infinite. Recursion turns the rule into a function. The list misses nothing: if $t \in S$ were skipped, it would lie strictly between two consecutive entries $s_{n-1} < t < s_n$, and then s_n would not be the least element of S above s_{n-1}.

Proof. If S is finite there is nothing to prove, so let S be infinite. In particular $S \neq \emptyset$.

Every $x \in \mathbb{N}$ has an element of S above it. Let $x \in \mathbb{N}$, and suppose that no $s \in S$ has $s > x$. Then $S \subseteq \{0, \dots, x\}$, a set with $x + 1$ elements (the third example after Definition 2.5.2), so S is finite by Proposition 2.5.6, a contradiction. Hence $T_x := \{s \in S : s > x\}$ is non-empty, and by Theorem 2.1.3 it has a least element.

The list. Define $g\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $g(n, x) := \min T_x$; by the previous paragraph this is defined for every $x \in \mathbb{N}$. By Theorem 2.3.1, with $X := \mathbb{N}$ and $a := \min S$ (which exists by Theorem 2.1.3), there is a function $n \mapsto s_n$ from $\mathbb{N}$ to $\mathbb{N}$ with

$$s_0 = \min S, \qquad s_{n+1} = \min\{s \in S : s > s_n\} \quad (n \in \mathbb{N}).$$

Every s_n lies in S: $s_0 \in S$, and $s_{n+1} \in T_{s_n} \subseteq S$.

Increasing. By construction $s_{n+1} > s_n$ for every n. Hence $s_m < s_n$ whenever $m < n$, by induction on n: there is no $m < 0$ (Lemma 2.1.1 (a)), and if $m < n + 1$, then $m \leq n$ (Lemma 2.1.1 (e)), so $s_m \leq s_n < s_{n+1}$, using the hypothesis when $m < n$. In particular $n \mapsto s_n$ is injective, since $m \neq n$ gives $m < n$ or $n < m$. Also $s_n \geq n$ for every n: $s_0 \geq 0$ (Lemma 2.1.1 (a)), and if $s_n \geq n$, then $s_{n+1} > s_n \geq n$, so $s_{n+1} \geq n + 1$ (Lemma 2.1.1 (e)).

Onto S. Let $t \in S$. The set $\{n \in \mathbb{N} : s_n \geq t\}$ is non-empty, since $s_t \geq t$, so it has a least element n by Theorem 2.1.3. If $n = 0$, then $s_0 = \min S \leq t$ and $s_0 \geq t$, so $s_0 = t$. If $n \neq 0$, then $n - 1 \in \mathbb{N}$ (Lemma 2.1.1 (c)), and $s_{n-1} < t$ by the minimality of n. So $t \in T_{s_{n-1}}$, and $s_n = \min T_{s_{n-1}} \leq t$. With $s_n \geq t$ this gives $s_n = t$.

So $n \mapsto s_n$, with codomain S, is a bijection $\mathbb{N} \to S$, and S is countably infinite.

■

3.1.3 Three ways to say countable

Being countable (empty or listable by $\mathbb{N}$), having an injection into $\mathbb{N}$, and being finite or the size of $\mathbb{N}$ all describe the same sets. Having the three forms side by side is what makes countability easy to prove: we may use whichever is cheapest for the set in hand.

Theorem 3.1.2. Characterizations of Countable Sets

For every set A, the following are equivalent.

(i) A is countable.

(ii) There is an injection $A \to \mathbb{N}$.

(iii) A is finite or countably infinite.

Idea. From a list to an injection: send each element to the **first** position at which it appears. From an injection to (iii): the injection makes A equinumerous with a subset of $\mathbb{N}$, and Lemma 3.1.1 sorts those. From (iii) back to a list: pad a finite list by repetition, as in the examples above.

Proof.

(i) $\Rightarrow$ (ii). If $A = \emptyset$, the empty function $\emptyset \to \mathbb{N}$ is injective, vacuously. Otherwise let $g\colon \mathbb{N} \to A$ be a surjection. For $a \in A$, the preimage $g^{-1}(\{a\}) \subseteq \mathbb{N}$ is non-empty, since g is onto, so it has a least element by Theorem 2.1.3. Define $h\colon A \to \mathbb{N}$ by

$$h(a) \coloneqq \min g^{-1}(\{a\}).$$

Then $g(h(a)) = a$ for every $a \in A$, that is, $g \circ h = \mathrm{id}_A$, so h is injective by Theorem 1.6.1 (a).

(ii) $\Rightarrow$ (iii). Let $h\colon A \to \mathbb{N}$ be injective. With its codomain shrunk to $h(A)$, it is a bijection $A \to h(A)$ (Section 2.5), so $|A| = |h(A)|$. By Lemma 3.1.1, $h(A) \subseteq \mathbb{N}$ is finite or countably infinite. If $h(A)$ has n elements, there is a bijection $\{1, \dots, n\} \to h(A)$, and following it by the inverse of $A \to h(A)$ gives a bijection $\{1, \dots, n\} \to A$ (Proposition 2.5.1 (b) for the inverse, Theorem 1.5.4 (c)); so A has n elements. If $|h(A)| = |\mathbb{N}|$, then $|A| = |\mathbb{N}|$ by Proposition 2.5.1 (c).

(iii) $\Rightarrow$ (i). If A is countably infinite, a bijection $\mathbb{N} \to A$ is a surjection. Let A be finite with n elements. If $n = 0$, then $A = \emptyset$, which is countable. If $n \geq 1$, let $\varphi\colon \{1, \dots, n\} \to A$ be a bijection and define $f\colon \mathbb{N} \to A$ by

$$f(k) \coloneqq \begin{cases} \varphi(k) & \text{if } 1 \leq k \leq n, \\ \varphi(1) & \text{if } k = 0 \text{ or } k > n. \end{cases}$$

Every $a \in A$ is $\varphi(k) = f(k)$ for some $k \in \{1, \dots, n\}$, so f is a surjection. This proves the theorem.

■

The step (i) ⇒ (ii) picks one element $h(a)$ of $g^{-1}(\{a\})$ for **every** $a \in A$ at once, and it needs no new principle for that, because there is a rule that names the element: the least one. That works because the preimages are subsets of $\mathbb{N}$, which is well-ordered. Section 3.2 meets a step that looks the same and has no such rule, and it is the point at which the book adds the axiom of choice.

Which form to use is the first decision in every countability proof:

Example. Method: list it

Template. To show A countable, give one map and check it. *(S)* A surjection onto A from $\mathbb{N}$ or a countable set: check that every $a \in A$ is a value (repetitions are free; split off $A = \emptyset$), and cite Definition 3.1.1 (or, from a countable set, the result on images proved below). *(I)* An injection of A into $\mathbb{N}$ or a countable set: check that equal values come from equal elements, and cite Theorem 3.1.2, (ii) ⇒ (i), composing if needed.

When to use it. (S) for "all objects of the form $\varphi(m, n, \dots)$": list the parameters. (I) when each element carries a code that can be read back, above all when a parametrization would leave A.

The usual failure. A list that runs through an infinite block before the next (Example (Listing the rows one after another)). An "injection" never checked to be injective.

Quick check. Which route of the method would you take for (a) the set of numbers $n^2 + 3n$ with $n \in \mathbb{N}$; (b) the set of $n \in \mathbb{N}$ with $n^2 + 1$ even?

Solution.

(a) Route (S): the set is the image of $\mathbb{N}$ under $n \mapsto n^2 + 3n$, and a function is a surjection onto its image (Section 2.5), so Definition 3.1.1 applies and nothing is left to check. (b) Route (I): the inclusion into $\mathbb{N}$ is an injection with nothing to check, so the set is countable by Theorem 3.1.2, (ii) ⇒ (i). No parametrization of the set is needed, and nobody has to work out which n qualify.

3.1.4 Closure properties

Three closure properties follow at once, each from the form of countability that suits it.

Proposition 3.1.3. Subsets of Countable Sets

Every subset of a countable set is countable.

Proof. Let B be countable and $A \subseteq B$. By Theorem 3.1.2, (i) ⇒ (ii), there is an injection $h\colon B \to \mathbb{N}$. Its restriction $h|_A\colon A \to \mathbb{N}$ is injective, since it has the same values. By (ii) ⇒ (i), A is countable. ∎

Proposition 3.1.4. Images of Countable Sets

Let A be countable and $f\colon A \to B$ a function. Then $f(A)$ is countable. In particular, if f is surjective, then B is countable.

Proof. If $A = \emptyset$, then $f(A) = \emptyset$, which is countable. Otherwise let $g\colon \mathbb{N} \to A$ be a surjection. The function f with codomain $f(A)$ is surjective (Section 2.5), so its composite with g is a surjection $\mathbb{N} \to f(A)$ by Theorem 1.5.4 (b). If f is surjective, then $f(A) = B$. ■

For unions we interleave two lists, taking the entries of the first list at the even positions and those of the second at the odd positions. That needs the fact that every natural number is even or odd, in exactly one way.

Proposition 3.1.5. Union of Two Countable Sets

If A and B are countable, then $A \cup B$ is countable.

Idea. Two lists $a_0, a_1, \ldots$ and $b_0, b_1, \ldots$ merge into one, $a_0, b_0, a_1, b_1, \ldots$: the entry at position $2q$ comes from the first list and the entry at position $2q + 1$ from the second. For this to define a function, every position must be even or odd, and not both.

Proof. If $A = \emptyset$, then $A \cup B = B$, and if $B = \emptyset$, then $A \cup B = A$; both are countable. So let $g\colon \mathbb{N} \to A$ and $h\colon \mathbb{N} \to B$ be surjections.

Claim. Every $a \in \mathbb{N}$ can be written as $a = 2q + r$ with $q \in \mathbb{N}$ and $r \in \{0, 1\}$, and the pair (q, r) is unique. In particular, no natural number is both of the form $2q$ and of the form $2q' + 1$ with $q, q' \in \mathbb{N}$.

Proof. By Theorem 2.2.3 with divisor 2, there are unique integers q, r with $a = 2q + r$ and $0 \le r < 2$. Then $r \in \mathbb{N}$ by Proposition 2.1.2 (b), and $r \le 1$ by Lemma 2.1.1 (e), so $r \in \{0, 1\}$. If $q < 0$, then $q + 1 \le 0$ by the discreteness clause Proposition 2.1.2 (c), so $q \le -1$ and $a = 2q + r \le -2 + 1 < 0$, which contradicts $a \ge 0$ (Lemma 2.1.1 (a)). So $q \ge 0$, and $q \in \mathbb{N}$ by Proposition 2.1.2 (b). Uniqueness among pairs with $q \in \mathbb{N}$ follows from uniqueness among all integer pairs. The last sentence is the uniqueness of r. ■

Define $k\colon \mathbb{N} \to A \cup B$ by

$$k(2q) \coloneqq g(q), \qquad k(2q + 1) \coloneqq h(q) \qquad (q \in \mathbb{N}).$$

By the claim, each $a \in \mathbb{N}$ falls under exactly one of the two clauses, with exactly one q, so k is a function. It is onto: an element of A is $g(q) = k(2q)$ for some q, and an element of B is $h(q) = k(2q + 1)$ for some q, where $2q$ and $2q + 1$ lie in $\mathbb{N}$ by Lemma 2.1.1 (b). So $A \cup B$ is countable. ■

If A and B overlap, the interleaved list repeats their common elements, and the definition does not mind. By induction on the number of sets, a union of finitely many countable sets is countable. A union of **infinitely** many is a different matter, and Section 3.2 is about it.

3.1.5 Pairs of natural numbers

The set $\mathbb{N} \times \mathbb{N}$ looks two-dimensional, and a first attempt to list it shows where the difficulty lies.

Example. Listing the rows one after another

Arrange $\mathbb{N} \times \mathbb{N}$ in rows, the m-th row being $(m, 0), (m, 1), (m, 2), \ldots$. Consider the "list"

$$(0,0), (0,1), (0,2), \ldots, \text{ then } (1,0), (1,1), \ldots, \text{ then } (2,0), \ldots$$

Is it a surjection $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$?

Solution. No. A list indexed by $\mathbb{N}$ gives each entry a position $n \in \mathbb{N}$. Here position n holds $(0, n)$, for every $n \in \mathbb{N}$: that already defines a function $f(n) := (0, n)$ on all of $\mathbb{N}$. No position is left for $(1, 0)$: there is no $n \in \mathbb{N}$ with $f(n) = (1, 0)$, since the first coordinate of every value is 0. The word "then" asks for positions after all the natural numbers, and there are none. So the claim that this is a list of $\mathbb{N} \times \mathbb{N}$ is false. It is a list of the first row only.

Warning. A list must give every entry a **finite** position. "First all of row 0, then all of row 1" never reaches row 1, because row 0 uses up every position. The same mistake hides in any listing that runs through an infinite block before starting the next one.

The conclusion that $\mathbb{N} \times \mathbb{N}$ is countable is nevertheless true.

Theorem 3.1.6. The Plane of Natural Numbers Is Countable

The map $p\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $p(m, n) := 2^m 3^n$, is injective. Hence $\mathbb{N} \times \mathbb{N}$ is countable.

Try it first (ten minutes): list $\mathbb{N} \times \mathbb{N}$, or inject it into $\mathbb{N}$. Which is less work to write down and check?

Idea (Scratch work). The rows-first list fails, as we saw. A list that works runs along the diagonals $m + n = 0, 1, 2, \ldots$, each of which is finite; but writing a formula for the position of (m, n) and checking that every position is used takes real work. Route (I) of Example (Method: list it) is cheaper. By Theorem 3.1.2 it is enough to **inject** $\mathbb{N} \times \mathbb{N}$ into $\mathbb{N}$, and an injection only has to be a code from which m and n can be read back. As givens and goal:

Givens	Goal
—	$\mathbb{N} \times \mathbb{N}$ countable
Theorem 3.1.2, (ii) $\Rightarrow$ (i)	an injection $p\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
$p(m, n) := 2^m 3^n$, and $2^m 3^n = 2^{m'} 3^{n'}$	$m = m'$ and $n = n'$

suppose $m > m'$ (symmetry); cancel $2^{m'}$: $2^{m-m'}3^n = 3^{n'}$	gap: an even number equals an odd one, which is impossible (the claim in the proof of Proposition 3.1.5); so $m = m'$, and then $n = n'$ because $k \mapsto 3^k$ is increasing

In 2^m3^n, the power of 2 records m and the power of 3 records n. To read them back we do not cite unique factorization into primes, which we have not proved. Parity closes the gap: cancel the smaller power of 2; if any factor 2 is left on one side, that side is even and the other is odd.

Proof. First, $p(m,n) \in \mathbb{N}$ by Proposition 2.3.4 (d) and Lemma 2.1.1 (b). Next, every power 3^k with $k \in \mathbb{N}$ is odd, that is, $3^k = 2j+1$ for some $j \in \mathbb{N}$: by Logic and Proof, Axiom 4.2.1, $3^0 = 1 = 2 \cdot 0 + 1$, and if $3^k = 2j+1$, then $3^{k+1} = 3^k \cdot 3 = 2(3j+1)+1$ (Definition 2.3.2).

Let $(m,n),(m',n') \in \mathbb{N} \times \mathbb{N}$ with $2^m3^n = 2^{m'}3^{n'}$. Suppose $m \neq m'$. The hypothesis is symmetric in the two pairs, so we may assume $m > m'$. Then $m - m' \in \mathbb{N}$ and $m - m' \geq 1$ (Lemma 2.1.1 (d), (e)), and $2^m = 2^{m'}2^{m-m'}$ by Proposition 2.3.4 (a). Canceling $2^{m'}$, which is positive by Proposition 2.3.4 (e), gives

$$2^{m-m'}3^n = 3^{n'}.$$

The left side is even: $2^{m-m'} = 2^{m-m'-1} \cdot 2$ by Definition 2.3.2, where $m - m' - 1 \in \mathbb{N}$ by Lemma 2.1.1 (c), so the left side is 2 times the natural number $2^{m-m'-1}3^n$. The right side is odd, as shown above. No natural number is both even and odd, by the uniqueness of the remainder in Theorem 2.2.3 with divisor 2 (the claim in the proof of Proposition 3.1.5). This contradiction shows $m = m'$.

Canceling 2^m now gives $3^n = 3^{n'}$. By Proposition 2.3.4 (e) with $u = 3 > 1$, $n < n'$ would give $3^n < 3^{n'}$, and $n' < n$ would give $3^{n'} < 3^n$; so $n = n'$. Hence $(m,n) = (m',n')$, and p is injective. By Theorem 3.1.2, (ii) $\Rightarrow$ (i), $\mathbb{N} \times \mathbb{N}$ is countable.

■

Alternatively, one can list $\mathbb{N} \times \mathbb{N}$ along its diagonals: first the one pair with $m+n = 0$, then the two pairs with $m+n = 1$, then the three with $m+n = 2$, and so on. Each diagonal is finite, so every pair is reached after finitely many steps, and the list never stalls on an infinite block. Some readers find this picture more convincing than the code 2^m3^n. The injection is shorter to write out and to check, which is why the proof uses it.

The theorem passes to products of any countable sets. Chapter 1 defines X^n for one set X; for several sets we first say what the product is. For an integer $k \geq 2$ and sets $A_1, \ldots, A_k$, let $U \coloneqq \bigcup_{i \in \{1,\ldots,k\}} A_i$ and

$$A_1 \times \cdots \times A_k \coloneqq \{x \in U^k : x = (x_1, \ldots, x_k) \text{ with } x_i \in A_i \text{ for every } i\},$$

the k-tuples whose i-th coordinate lies in A_i. It is a set by (W3), (W5) and (W1) of Section 1.2. For $k = 2$ it is $A_1 \times A_2$ of Definition 1.4.2, a pair being a 2-tuple, and if every A_i is the same set X, it is X^k.

Corollary 3.1.7. Products of Countable Sets

(a) If A and B are countable, then $A \times B$ is countable.

(b) Let $k \geq 2$ be an integer. If $A_1, \ldots, A_k$ are countable, then $A_1 \times \cdots \times A_k$ is countable.

Idea. For two factors, injections $A \to \mathbb{N}$ and $B \to \mathbb{N}$ turn $A \times B$ into a subset of $\mathbb{N} \times \mathbb{N}$, and the code $2^m 3^n$ does the rest. More factors are added one at a time: a $(k+1)$-tuple is a k-tuple followed by one more coordinate.

Proof. *(a)* By Theorem 3.1.2, (i) $\Rightarrow$ (ii), there are injections $i\colon A \to \mathbb{N}$ and $j\colon B \to \mathbb{N}$. The map $A \times B \to \mathbb{N} \times \mathbb{N}$, $(a, b) \mapsto (i(a), j(b))$, is injective: if $(i(a), j(b)) = (i(a'), j(b'))$, then $i(a) = i(a')$ and $j(b) = j(b')$ by Definition 1.4.1, so $a = a'$ and $b = b'$. Following it by the injection p of Theorem 3.1.6 gives an injection $A \times B \to \mathbb{N}$ (Theorem 1.5.4 (a)), and (ii) $\Rightarrow$ (i) concludes. No case split is needed: if $A = \emptyset$ or $B = \emptyset$, then $A \times B = \emptyset$ (Proposition 1.4.1), so the map $(a, b) \mapsto (i(a), j(b))$ and its composite with p are empty functions (Proposition 1.5.2 (a)), which are injective vacuously.

(b) We use Theorem 2.2.1 with $n_0 = 2$ on the statement "for all countable sets $A_1, \ldots, A_k$, the set $A_1 \times \cdots \times A_k$ is countable". *Base case* $k = 2$. This is (a). *Step.* Let $k \geq 2$, suppose the statement for k, and let $A_1, \ldots, A_{k+1}$ be countable. The map

$$((a_1, \ldots, a_k), a_{k+1}) \mapsto (a_1, \ldots, a_{k+1})$$

is a function, since a k-tuple determines its coordinates (Section 1.4), and it sends $(A_1 \times \cdots \times A_k) \times A_{k+1}$ onto $A_1 \times \cdots \times A_{k+1}$: a $(k+1)$-tuple with $x_i \in A_i$ is the image of $((x_1, \ldots, x_k), x_{k+1})$. By the hypothesis, $A_1 \times \cdots \times A_k$ is countable, so the domain is countable by (a), and the $(k+1)$-fold product is countable by Proposition 3.1.4. By Theorem 2.2.1 the statement holds for every $k \geq 2$.

■

The map in the step is in fact a bijection, by the characteristic property of tuples (Section 1.4). The proof uses that property only to see that the map is well defined, and of the map it uses only that it is onto; injectivity is never needed. Tuples of different lengths are different objects, and the book has no 1-tuples, so the corollary starts at $k = 2$; a single countable set needs no corollary.

Quick check. Let L be the set of the 26 letters a–z. Is the set of all strings of exactly 5 letters, that is L^5, countable? Which results do you use?

Solution. Yes. The set L is finite, so it is countable by Theorem 3.1.2, (iii) $\Rightarrow$ (i). The strings of length 5 are the 5-tuples of letters, $L^5 = L \times L \times L \times L \times L$, which is countable by Corollary 3.1.7 (b) with $k = 5$. (It is in fact finite, with 26^5 elements: the map in the step of the proof of Corollary 3.1.7 (b) is a bijection $L^k \times L \to L^{k+1}$ (the remark above), so Exercise (C2: Counting products and functions) (a), applied for $k = 2, 3, 4$ after $L^2 = L \times L$, counts it. Countability needs less than the count.)

All strings of every finite length together form the union of the sets L^k over k, a union of infinitely many countable sets. Section 3.2 takes up such unions.

3.1.6 The integers and the rationals

Here is the answer to the question that opened the section. Recall from Section 2.1 that $\mathbb{Z} \coloneqq \mathbb{N} \cup \{-n : n \in \mathbb{N}\}$, $\mathbb{Z}_{>0} \coloneqq \{n \in \mathbb{N} : n \neq 0\}$ and $\mathbb{Q} \coloneqq \{m/n : m \in \mathbb{Z},\ n \in \mathbb{Z}_{>0}\}$.

Theorem 3.1.8. The Integers and the Rationals Are Countable

$\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ are countable. Each of them is countably infinite.

Idea. For $\mathbb{Z}$, interleave the non-negative and the negative integers, as in Proposition 3.1.5, but with explicit lists, so that the result is a bijection: $0, -1, 1, -2, 2, -3, \ldots$. For $\mathbb{Q}$, do not try to list the fractions directly. Every rational is m/n for some pair $(m, n) \in \mathbb{Z} \times \mathbb{Z}_{>0}$, and that set of pairs is countable, so $\mathbb{Q}$ is the image of a countable set.

Proof. $\mathbb{N}$. The identity $\mathrm{id}_{\mathbb{N}}$ is a bijection $\mathbb{N} \to \mathbb{N}$.

$\mathbb{Z}$. By the claim in the proof of Proposition 3.1.5, every $n \in \mathbb{N}$ is $2k$ or $2k+1$ for exactly one $k \in \mathbb{N}$, and not both. So we may define $z \colon \mathbb{N} \to \mathbb{Z}$ by

$$z(2k) \coloneqq k, \qquad z(2k+1) \coloneqq -(k+1) \qquad (k \in \mathbb{N}),$$

which begins $z(0) = 0$, $z(1) = -1$, $z(2) = 1$, $z(3) = -2$, $z(4) = 2$. It is injective: $z(2k) = k \geq 0$, while $z(2k+1) = -(k+1) \leq -1 < 0$ (Lemma 2.1.1 (a)), so an even and an odd input never share a value; and $k = k'$ or $-(k+1) = -(k'+1)$ gives $k = k'$. It is surjective: let $m \in \mathbb{Z}$. If $m \in \mathbb{N}$, then $m = z(2m)$. Otherwise $m = -n$ with $n \in \mathbb{N}$, and $n \neq 0$, since $-0 = 0 \in \mathbb{N}$; so $n - 1 \in \mathbb{N}$ by Lemma 2.1.1 (c), and $m = -((n-1)+1) = z(2(n-1)+1)$. So z is a bijection.

$\mathbb{Q}$. The set $\mathbb{Z}_{>0} \subseteq \mathbb{N}$ is countable by Proposition 3.1.3, and $\mathbb{Z}$ is countable, so $\mathbb{Z} \times \mathbb{Z}_{>0}$ is countable by Corollary 3.1.7 (a). The map $(m, n) \mapsto m/n$ from $\mathbb{Z} \times \mathbb{Z}_{>0}$ to $\mathbb{Q}$ is defined, since $n \geq 1$ is not 0, and it is surjective by the definition of $\mathbb{Q}$. By Proposition 3.1.4, $\mathbb{Q}$ is countable. It is infinite: $\mathbb{N} \subseteq \mathbb{Q}$, since $n = n/1$, and $\mathbb{N}$ is infinite (Example (Hilbert's Hotel)), so $\mathbb{Q}$ is not finite by Proposition 2.5.6. By Theorem 3.1.2, (i) $\Rightarrow$ (iii), $\mathbb{Q}$ is countably infinite. ∎

The list of $\mathbb{Q}$ that the proof produces repeats every rational infinitely often: $1/1$, $2/2$, $3/3$, ... are all 1. The definition allows it, and that is what made the proof three lines. No line of the proof, or of the results it cites, uses the axiom of choice of Section 3.2: each surjection or injection it relies on is either given by a formula or named by a single ∃E, and the only selections made for many elements at once are least elements (Theorem 2.1.3). That $\mathbb{Q}$ can be listed is the fact *Analysis on the Real Line*, Chapter 1 quotes when it compares $\mathbb{Q}$ with $\mathbb{R}$: the rationals, dense as they are, can be listed, while *Analysis on the Real Line*, Chapter 1 shows that the reals cannot.

3.1.7 Listing in practice

Two more uses of Example (Method: list it), one by each route.

Example. Integer combinations of 1 and $\sqrt{2}$

Let $S \coloneqq \{m + n\sqrt{2} : m, n \in \mathbb{Z}\}$. Show that S is countably infinite.

Solution. Route (S). The map $\mathbb{Z} \times \mathbb{Z} \to S$, $(m, n) \mapsto m + n\sqrt{2}$, is onto by the definition of S, and $\mathbb{Z} \times \mathbb{Z}$ is countable (Theorem 3.1.8, Corollary 3.1.7 (a)). So S is countable by Proposition 3.1.4. It is infinite: $\mathbb{N} \subseteq S$ (take $n = 0$ and $m \in \mathbb{N}$), and $\mathbb{N}$ is infinite (Example (Hilbert's Hotel)), so S is not finite by Proposition 2.5.6. By Theorem 3.1.2, (i) $\Rightarrow$ (iii), S is countably infinite.

Route (I) would need an injection $S \to \mathbb{Z} \times \mathbb{Z}$, that is, that the map is injective, so that it can be inverted. If $m + n\sqrt{2} = m' + n'\sqrt{2}$ with $n \neq n'$, then $\sqrt{2} = (m - m')/(n' - n)$ would be rational, against Logic and Proof, Theorem 2.2.1; and if $n = n'$, then $m = m'$. So route (I) works here, but it costs a theorem. Route (S) never asks whether two parameter pairs give the same number.

Example. Coding the two-element subsets of $\mathbb{N}$

Let P_2 be the set of subsets of $\mathbb{N}$ with exactly two elements. Show that P_2 is countably infinite.

Solution. Route (S) from $\mathbb{N} \times \mathbb{N}$, $(m, n) \mapsto \{m, n\}$, leaves P_2 when $m = n$, the case that the box's "When to use it" sends to route (I). Route (I) needs a code from which the set can be read back, and a two-element set has a least and a largest element.

Let $S \in P_2$. By Definition 2.5.2, $S = \{s, t\}$ with $s \neq t$, and by trichotomy one of them is smaller. Write $\min S$ and $\max S$ for the smaller and the larger. They are named by a rule, so no choice is made. Define $c(S) \coloneqq 2^{\min S} 3^{\max S}$, that is, $c(S) = p(\min S, \max S)$ with p of Theorem 3.1.6. If $c(S) = c(T)$, then $(\min S, \max S) = (\min T, \max T)$, since p is injective, and so $S = \{\min S, \max S\} = T$. By Theorem 3.1.2, (ii) $\Rightarrow$ (i), P_2 is countable. It is infinite: $n \mapsto \{0, n+1\}$ is an injection $\mathbb{N} \to P_2$ (the sets differ in their larger elements), so P_2 contains a copy of $\mathbb{N}$, and a set with a subset equinumerous with $\mathbb{N}$ is not finite (Example (Hilbert's Hotel), Proposition 2.5.1, Proposition 2.5.6). By (i) $\Rightarrow$ (iii), P_2 is countably infinite.

3.1.8 Exercises

3.1.8.1 A. Check your understanding

Exercise. A1

(a) Define "A is countable", and say why the empty set is mentioned separately in the definition.

(b) True or false, with a reason: every infinite subset of $\mathbb{Q}$ is countably infinite; every

countable set is finite or equinumerous with $\mathbb{N}$.

(c) Which of the three forms (i)–(iii) of Theorem 3.1.2 is quickest to check for $\{n^2 : n \in \mathbb{N}\}$, and why?

(d) Where does the proof of (i) $\Rightarrow$ (ii) in Theorem 3.1.2 use Theorem 2.1.3, and to which set is it applied?

Solution.

(a) A is countable if $A = \emptyset$ or there is a surjection $\mathbb{N} \to A$ (Definition 3.1.1). The empty set is mentioned separately because there is no function $\mathbb{N} \to \emptyset$ at all (Proposition 1.5.2 (b)), so the surjection clause never holds for $\emptyset$.

(b) Both are true. An infinite $A \subseteq \mathbb{Q}$ is countable by Proposition 3.1.3 and Theorem 3.1.8; by Theorem 3.1.2, (i) $\Rightarrow$ (iii), it is finite or countably infinite, and it is not finite. The second statement is (i) $\Rightarrow$ (iii) itself, with "countably infinite" unfolded by Definition 3.1.2.

(c) Form (i): the set is given as the image of $\mathbb{N}$ under $n \mapsto n^2$, and a function is a surjection onto its image, so nothing is left to check. Form (ii) is almost as quick: the inclusion into $\mathbb{N}$ is injective. Form (iii) needs a bijection with $\mathbb{N}$, which costs a proof that $n \mapsto n^2$ is injective on $\mathbb{N}$.

(d) In defining $h(a) \coloneqq \min g^{-1}(\{a\})$: well-ordering is applied to the preimage $g^{-1}(\{a\}) \subseteq \mathbb{N}$, which is non-empty because g is onto. It gives every a a definite position, the first one at which a appears in the list, so no choice is needed.

3.1.8.2 B. Practice

Exercise. B1

Prove that each of the following sets is countable.

(a) $2\mathbb{N} \times \mathbb{Z}$.

(b) $\{(m, n) \in \mathbb{N} \times \mathbb{N} : m < n\}$.

(c) $\mathbb{Q} \times \mathbb{Q}$, the points of the plane with rational coordinates.

(d) The set of open intervals with rational endpoints, that is, of the sets $\{x \in \mathbb{R} : a < x < b\}$ with $a, b \in \mathbb{Q}$ and $a < b$.

Solution.

(a) $2\mathbb{N} \subseteq \mathbb{N}$ is countable by Proposition 3.1.3, and $\mathbb{Z}$ is countable by Theorem 3.1.8; so $2\mathbb{N} \times \mathbb{Z}$ is countable by Corollary 3.1.7 (a).

(b) It is a subset of $\mathbb{N} \times \mathbb{N}$, which is countable by Theorem 3.1.6, so it is countable by Proposition 3.1.3.

(c) $\mathbb{Q}$ is countable (Theorem 3.1.8), so $\mathbb{Q} \times \mathbb{Q}$ is countable by Corollary 3.1.7 (a).

(d) Let $D \coloneqq \{(a, b) \in \mathbb{Q} \times \mathbb{Q} : a < b\}$, countable by (c) and Proposition 3.1.3. Define $J \colon D \to \mathcal{P}(\mathbb{R})$ by $J(a, b) \coloneqq \{x \in \mathbb{R} : a < x < b\}$. The set of intervals in question is the image $J(D)$, so it is countable by Proposition 3.1.4. (Here $(a, b) \in D$ is an ordered

pair, and the interval it names is written in set-builder notation, so the two readings of "(a, b)" never meet.)

Exercise. B2: Putting a proof in order

The lines (i)–(ix) below include the seven lines of a proof that $2^m 3^n = 2^{m'} 3^{n'}$ implies $m = m'$ and $n = n'$, for $m, n, m', n' \in \mathbb{N}$, shuffled, together with two lines that do not belong. Write the seven lines in an order that makes a correct proof, and say why each of the other two lines fails.

(i) The left side is even, because $m - m' \geq 1$ by the supposition; the right side is odd; no natural number is both (Theorem 2.2.3, uniqueness of the remainder for divisor 2). This is a contradiction.

(ii) Suppose $2^m 3^n = 2^{m'} 3^{n'}$.

(iii) The left side is odd and the right side is even, a contradiction.

(iv) Canceling 2^m gives $3^n = 3^{n'}$.

(v) Suppose $m \neq m'$; by symmetry, say $m > m'$.

(vi) Since $k \mapsto 3^k$ is strictly increasing on $\mathbb{N}$, $n = n'$.

(vii) Since 2 and 3 are prime, unique factorization gives $m = m'$ and $n = n'$.

(viii) Canceling $2^{m'}$ gives $2^{m-m'} 3^n = 3^{n'}$.

(ix) So $m = m'$.

Solution. The order is (ii), (v), (viii), (i), (ix), (iv), (vi). No other order is admissible. Line (ii) introduces the four numbers and the equation. Lines (v), (viii) and (i) are one proof by contradiction: (v) opens it, (viii) uses the supposition $m > m'$ to cancel, and (i) closes it with a contradiction, so (ix), its conclusion, must come right after (i). Line (iv) cancels 2^m on both sides, which needs $m = m'$, so it follows (ix); and (vi) uses the equation of (iv).

Line (iii) reverses the parities. The left side $2^{m-m'} 3^n$ has a factor 2 because $m - m' \geq 1$, so it is even; the right side $3^{n'}$ is odd. A line asserting the opposite is false: for $m = 1$, $m' = 0$, $n = n' = 0$, the left side is 2 and the right side is 1.

Line (vii) would end the proof at once, but it cites unique factorization into primes, which the book has neither proved nor taken as a school fact: Section 2.2 sets it aside as a fact it does not prove or use, and the idea before Theorem 3.1.6 declines to cite it. So (vii) cites a line that is not available, (N9) of Logic and Proof, Example (What is not allowed). The theorem is true, and the conclusion of (vii) is true; the error is in the citation, which is exactly why the proof in the text goes through parity instead.

Exercise. B3: A surjection by formula

Give an explicit surjection $\mathbb{N} \to \mathbb{N} \times \{0, 1\}$ and prove that it is one. List the properties that any correct answer must have, so that a different answer can be checked against them.

Solution. By the claim in the proof of Proposition 3.1.5, every $a \in \mathbb{N}$ is $2q + r$ for exactly one pair (q, r) with $q \in \mathbb{N}$ and $r \in \{0, 1\}$. Define $s\colon \mathbb{N} \to \mathbb{N} \times \{0, 1\}$ by $s(2q + r) := (q, r)$: so $s(0) = (0, 0)$, $s(1) = (0, 1)$, $s(2) = (1, 0)$, $s(3) = (1, 1)$. The uniqueness of the pair makes s a function. It is surjective: given $(q, r) \in \mathbb{N} \times \{0, 1\}$, the number $a := 2q + r$ lies in $\mathbb{N}$ (Lemma 2.1.1 (b)), and $s(a) = (q, r)$. (It is even a bijection, by the uniqueness of the pair.)

A correct answer must:

- assign to **every** $a \in \mathbb{N}$ exactly one value, so that it is a function on all of $\mathbb{N}$;
- take its values in $\mathbb{N} \times \{0, 1\}$;
- reach every pair $(q, 0)$ **and** every pair $(q, 1)$, for every $q \in \mathbb{N}$, each at a finite position.

For instance $s'(2q) := (q, 1)$, $s'(2q + 1) := (q, 0)$ also qualifies. The rows-first attempt $a \mapsto (a, 0)$, "then" the pairs $(q, 1)$, fails the third property (Example (Listing the rows one after another)).

Exercise. B4: Prove or disprove

Prove each true statement, by a route of Example (Method: list it) where a set must be shown countable, and refute each false one with a concrete counterexample.

(a) The set of all functions $\{0, 1\} \to \mathbb{N}$ is countable.

(b) If A is countable and there is an injection $\mathbb{N} \to A$, then A is countably infinite.

(c) If $f\colon A \to B$ is an injection and B is countably infinite, then A is countably infinite.

(d) For every countable set A there is a surjection $\mathbb{N} \to A$.

(e) If A and B are countably infinite, then $A \cup B$ is countably infinite.

Solution.

(a) **True.** The map $f \mapsto (f(0), f(1))$ is injective into $\mathbb{N} \times \mathbb{N}$, since two functions on $\{0, 1\}$ with the same two values are equal (Proposition 1.5.1). Followed by p of Theorem 3.1.6 it is an injection into $\mathbb{N}$ (Theorem 1.5.4 (a)). The set is countable by Theorem 3.1.2, (ii) $\Rightarrow$ (i).

(b) **True.** Let $j\colon \mathbb{N} \to A$ be injective. Then $\mathbb{N}$ is equinumerous with $j(\mathbb{N}) \subseteq A$. If A were finite, $j(\mathbb{N})$ would be finite (Proposition 2.5.6), and so would $\mathbb{N}$ (compose the bijections), against Example (Hilbert's Hotel). So A is countable and not finite, and countably infinite by Theorem 3.1.2, (i) $\Rightarrow$ (iii).

(c) **False.** Take $A = \{0\}$, $B = \mathbb{N}$ and the inclusion: it is injective, B is countably infinite, and A is finite.

(d) **False.** $A = \emptyset$ is countable, and there is no function $\mathbb{N} \to \emptyset$ at all (Proposition 1.5.2 (b)).

(e) **True.** $A \cup B$ is countable by Proposition 3.1.5. A bijection $\mathbb{N} \to A$ followed by the inclusion $A \to A \cup B$ is an injection $\mathbb{N} \to A \cup B$ (Theorem 1.5.4 (a)), so $A \cup B$ is countably infinite by (b).

3.1.8.3 C. Going deeper

Exercise. C1: Finite subsets of the natural numbers

Let $\mathcal{F}$ be the set of all finite subsets of $\mathbb{N}$. Prove that $\mathcal{F}$ is countable, without using any result about unions of infinitely many sets.

Solution (Hint 1). Inject $\mathcal{F}$ into $\mathbb{N}$ by sending F to $S_N(F) \coloneqq \sum_{k=0}^{N} \mathbf{1}_F(k)\, 2^k$, for any N with $F \subseteq \{0, \dots, N\}$ (the value does not depend on N): the number whose binary digits are the indicator of F.

Solution (Hint 2). To prove injectivity, let m be the largest element at which two different sets $F \neq G$ differ (the largest element of $(F \setminus G) \cup (G \setminus F)$, a non-empty finite subset of $\mathbb{N}$). The terms above m are the same for F and G. Then use $\sum_{k=0}^{m-1} 2^k = 2^m - 1 < 2^m$.

Solution. The set $\mathcal{F} \subseteq \mathcal{P}(\mathbb{N})$ exists by specification. We build an injection $\sigma \colon \mathcal{F} \to \mathbb{N}$ in four steps. For $N \in \mathbb{N}$ and $F \subseteq \{0, \dots, N\}$ let

$$S_N(F) \coloneqq \sum_{k=0}^{N} \mathbf{1}_F(k)\, 2^k,$$

a finite sum as in Definition 2.3.1 (indexed from 0), where $\mathbf{1}_F \colon \mathbb{N} \to \{0, 1\}$ is the indicator function of F. Each term is 0 or 2^k, and $2^k \in \mathbb{N}$ by Proposition 2.3.4 (d). So $S_N(F) \in \mathbb{N}$, by induction on N through the recursive clause of Definition 2.3.1, using Lemma 2.1.1 (b) at each step.

Step 1: a bound. Each term is at most 2^k, so

$$0 \leq S_N(F) \leq \sum_{k=0}^{N} 2^k = 2^{N+1} - 1,$$

by Proposition 2.3.6 with $r = 2$ (shifting the index by one).

Step 2: one more term. Splitting off the last term (Section 2.3), for $F \subseteq \{0, \dots, N+1\}$,

$$S_{N+1}(F) = S_N(F \cap \{0, \dots, N\}) + \mathbf{1}_F(N+1)\, 2^{N+1}.$$

In particular, if $F \subseteq \{0, \dots, N\}$, then $S_{N+1}(F) = S_N(F)$. By induction on $N' \geq N$, $S_{N'}(F) = S_N(F)$ for every $N' \geq N$: the value does not depend on which bound N we use.

Step 3: injective for a fixed N. We prove by Logic and Proof, Axiom 4.2.1 on N: if $F, G \subseteq \{0, \dots, N\}$ and $S_N(F) = S_N(G)$, then $F = G$. For $N = 0$, F and G are $\emptyset$ or $\{0\}$, with values 0 and 1. For the step, let $F, G \subseteq \{0, \dots, N+1\}$ with $S_{N+1}(F) = S_{N+1}(G)$, and write $F' \coloneqq F \cap \{0, \dots, N\}$, $G' \coloneqq G \cap \{0, \dots, N\}$. If $N+1 \in F$ and $N+1 \notin G$, then Steps 2 and 1 give

$$S_{N+1}(F) \geq 2^{N+1} > 2^{N+1} - 1 \geq S_N(G') = S_{N+1}(G),$$

a contradiction; the case $N+1 \in G \setminus F$ is the same with F and G exchanged. So $N+1$ lies in both or in neither, the last terms in Step 2 agree, and $S_N(F') = S_N(G')$. By the hypothesis, $F' = G'$. Since $\{0, \dots, N+1\} = \{0, \dots, N\} \cup \{N+1\}$, it follows that $F = G$.

Step 4: the injection. Every $F \in \mathcal{F}$ lies in some $\{0, \dots, N\}$: if $F = \emptyset$, take $N = 0$; otherwise F is a non-empty finite set of real numbers, so it has a maximum $M \in F \subseteq \mathbb{N}$ (Proposition 2.3.8, as in the remark at the end of Section 2.5), and $F \subseteq \{0, \dots, M\}$. Define $\sigma(F) \coloneqq S_N(F)$ for any such N; by Step 2 this does not depend on N. If $\sigma(F) = \sigma(G)$, take N at least as large as a bound for F and a bound for G; then $S_N(F) = S_N(G)$, and Step 3 gives $F = G$. So σ is injective, and $\mathcal{F}$ is countable by Theorem 3.1.2, (ii) $\Rightarrow$ (i).

For example $\sigma(\emptyset) = 0$ (the empty set contributes no terms), $\sigma(\{0, 2\}) = 1 + 4 = 5$ and $\sigma(\{1, 3\}) = 2 + 8 = 10$: $\sigma(F)$ is the number whose binary numeral has a 1 exactly in the places listed in F. Step 3 is the uniqueness of binary numerals, and Step 4 uses no principle of choice: every value is given by a formula.

Marking scheme. (10 points) - 2: defines a map from the finite subsets to $\mathbb{N}$ explicitly, including the value at $\emptyset$, and checks that its values are natural numbers. - 2: makes the map well defined, either by a bound-independent definition (as in Step 2) or by summing over the elements of F listed in increasing order. - 4: proves injectivity, either by comparing the terms at the largest element at which F and G differ, using $\sum_{k=0}^{m-1} 2^k < 2^m$, or by an induction on the bound as in Step 3, or by an equivalent proved uniqueness argument for binary numerals. - 2: concludes with Theorem 3.1.2, (ii) $\Rightarrow$ (i). - Route by surjection: an explicit map $\mathbb{N} \to \mathcal{F}$ that reads off binary digits (for example, $D(n)$ is the set of $k \leq n$ for which the quotient of n by 2^k in Theorem 2.2.3 is odd) earns the same points: 2 for defining the map, 2 for checking that each value is a finite subset of $\mathbb{N}$, 4 for a proof that every $F \in \mathcal{F}$ is a value, and 2 for concluding by Definition 3.1.1. Fatal errors (0 for the step): writing $\mathcal{F}$ as the union over n of the sets of n-element subsets and citing a result on countable unions (the task excludes it); asserting injectivity, or surjectivity on the second route, "by uniqueness of binary expansions" with no proof.

Exercise. C2: Find the error

Here is a "proof" that every subset of a countable set is countable.

> Let B be countable and $A \subseteq B$. (1) If $A = \emptyset$, then A is countable by definition. (2) Otherwise $B \neq \emptyset$, so there is a surjection $g\colon \mathbb{N} \to B$. (3) Define $h\colon \mathbb{N} \to A$ by $h(n) \coloneqq g(n)$. (4) Let $a \in A$. Then $a \in B$, so $a = g(n)$ for some $n \in \mathbb{N}$, and $h(n) = a$. (5) Hence h is a surjection onto A, and A is countable.

Is the conclusion true? Does the argument prove it? If not, name the line that fails, the rule it breaks, and give a counterexample **to that line**. Then repair the proof.

Solution. The conclusion is true: it is Proposition 3.1.3. The argument does not prove it.

Line (3) fails. It does not define a function from $\mathbb{N}$ to A: Definition 1.5.1 requires, for **every** $n \in \mathbb{N}$, exactly one value **in** A, and when $g(n) \notin A$ the formula offers no value in A at all. Counterexample to line (3): $B = \mathbb{N}$, $g = \mathrm{id}_{\mathbb{N}}$, $A = \{1\}$. Then "$h(2) = g(2) = 2$", and $2 \notin A$, so h is not a function into A. Lines (1), (2) and (4) are correct, and (5) would follow if h were a function $\mathbb{N} \to A$.

Repair. In the case $A \neq \emptyset$, fix one element $a_0 \in A$ (one $\exists$E) and define

$$h(n) \coloneqq \begin{cases} g(n) & \text{if } g(n) \in A, \\ a_0 & \text{if } g(n) \notin A. \end{cases}$$

Now h is a function $\mathbb{N} \to A$, and line (4) shows that it is onto: for $a \in A$, some n has $g(n) = a \in A$, and then $h(n) = g(n) = a$. The repaired proof uses that A is non-empty, which line (1) had already split off; the flawed line ignored the elements of $B \setminus A$, and the default value a_0 is where they go. The proof in the text avoids the issue by restricting an **injection** instead, since a restriction of a function is always a function.

Marking scheme. (10 points) - 2: says the conclusion is true, citing Proposition 3.1.3 or an equivalent proof. - 3: names line (3) and the broken requirement: a function into A needs a value in A at every n (Definition 1.5.1). - 2: gives a concrete instance of the failure of line (3), with a specific n whose value leaves A. - 3: repairs the proof with a default value in A (or by restricting an injection), and checks surjectivity. Fatal errors (0 for the step): calling the conclusion false; blaming line (4) or (5); a "counterexample" that shows a subset that is not countable.

3.2 Countable Unions and the Axiom of Choice

Section 3.1 listed $\mathbb{N} \times \mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$, and showed that a union of two countable sets is countable (Proposition 3.1.5). The next question is a union of **countably many** countable sets. The natural proof is short, and it contains one step that none of the rules met so far can justify. This section isolates that step, adds the principle that licenses it, the axiom of choice, and then shows how to tell a proof that needs the axiom from one that only seems to.

3.2.1 A union of countably many lists

Let $A_0, A_1, A_2, \ldots$ be countable sets, a family $(A_n)_{n\in\mathbb{N}}$ in the sense of Definition 1.3.3. We want to prove that $\bigcup_{n\in\mathbb{N}} A_n$ is countable.

Here is the proof most people write first. List each set: $A_n = \{a_{n,0}, a_{n,1}, a_{n,2}, \ldots\}$. Put $a_{n,m}$ in row n and column m of an infinite grid. Every element of the union stands somewhere in the grid, and the grid is indexed by $\mathbb{N} \times \mathbb{N}$, which is countable (Theorem 3.1.6). So the union is the image of a countable set, and it is countable.

Every step but the first, "list each set", is a result of Section 3.1. Where do the lists come from?

3.2.2 The obstacle, rule by rule

For a non-empty A_n, "A_n is countable" says that **there exists** a surjection $\mathbb{N} \to A_n$ (Definition 3.1.1). To use it we apply $\exists$E (Logic and Proof, Definition 5.6.1): we name the object and argue inside the box of that name. One $\exists$E names **one** surjection, for **one** n.

- **Finitely many sets.** The proof of Proposition 3.1.5 used two $\exists$E's; for $A_0, \ldots, A_9$ we could nest ten boxes.
- **All $n \in \mathbb{N}$ at once.** The grid needs a list of A_n for every n, assembled into one object: a function that sends each n to a surjection $\mathbb{N} \to A_n$. A proof is a finite object. It cannot contain one $\exists$E for each of infinitely many indices, and no rule of *Logic and Proof*, Chapter 5 makes infinitely many choices in one step.

Two escape routes fail. *Recursion* (Theorem 2.3.1) defines a function on all of $\mathbb{N}$ at once, but from a rule g given in advance, each value determined by the previous one. The list of A_{n+1} is

not determined by the list of A_n, and a rule producing a list of every A_{n+1} would already be the missing object. *Induction* on k, with Proposition 3.1.5 at each step, proves "for every k, $A_0 \cup \cdots \cup A_k$ is countable" (Exercise C3 writes it out), but that is a statement about each k separately; nothing makes the lists for different k fit together.

Section 1.6 met the same wall: a right inverse of a surjection must pick a preimage of **every** point at once, and the rules could do that only for finitely many points, or when a rule names the preimage.

3.2.3 The axiom of choice

None of the working rules (W1)–(W6) of Section 1.2 forms a set out of infinitely many arbitrary picks. The principle we add is the simplest statement that does.

From any family of non-empty sets, one may pick one element from each set, all at once.

Axiom 3.2.1. Axiom of Choice

Let I be a set, and let $(A_i)_{i\in I}$ be a family of sets such that A_i is **non-empty** for **every** $i \in I$. Then **there exists** a function

$$c\colon I \to \bigcup_{i\in I} A_i \quad \text{with} \quad c(i) \in A_i \ \text{ for every } i \in I.$$

Such a function c is called a **choice function** for the family.

In symbols, with Y^X the set of functions of Section 1.5 and $U := \bigcup_{i\in I} A_i$:

$$\forall i \in I\ (A_i \neq \emptyset) \ \to\ \exists c \in U^I \ \ \forall i \in I \ \ c(i) \in A_i.$$

In words: the hypothesis says that each set of the family has an element; the conclusion says that **one** function picks an element of every A_i at the same time. The codomain, a set by (W3), only gives c somewhere to take its values. The axiom asserts that c exists and gives no recipe for it.

Its status. For finitely many indices the axiom adds nothing (proved below); for infinitely many it is a genuinely new principle. It can be neither proved nor refuted from the other axioms of set theory (Gödel, Cohen). Chapter 6 states its best-known equivalent, Zorn's lemma; *Axiomatic Set Theory* proves it equivalent to the axiom, together with the other equivalents such as the well-ordering theorem, and surveys the independence results. This book uses the axiom openly on the main line, among other places: here, for countable unions and right inverses; in Section 3.5, for infinite subsets that can be listed; in *Analysis on the Real Line*, Chapter 1, for sup approximations (the remark below); in *Measure, Integration, and Real Analysis*, Chapter 2, for the Vitali set; in the same volume, Chapter 10, through Zorn's lemma, for the Hahn–Banach theorem; and in *Functional Analysis*, Chapter 2, for Tychonoff's theorem. Each use is flagged at its line.

Remark. A corollary in *Analysis on the Real Line*, Chapter 1 gives, for each $n \geq 1$ separately, some $a_n \in A$ with $a_n > \sup A - \frac{1}{n}$: one $\exists$E per n, and no axiom. Forming the **sequence** $(a_n)_{n\geq 1}$ from these is a choice function for the family $\left(\{a \in A : a > \sup A - \frac{1}{n}\}\right)_{n\in\mathbb{Z}_{>0}}$, an instance of Axiom 3.2.1 with the countable index set $I = \mathbb{Z}_{>0}$. *Analysis on the Real Line*, Chapter 1 flags exactly this step.

Examples.

1. *The empty family.* If $I = \emptyset$, the empty function $\emptyset \to \bigcup_{i\in\emptyset} A_i = \emptyset$ (Proposition 1.5.2 (a)) is a choice function: the condition "for every $i \in \emptyset$" holds vacuously. No axiom is needed.
2. *A family with a rule.* Let $I = \mathbb{Z}_{>0}$ and $A_n := \{k \in \mathbb{N} : n \mid k,\ k \neq 0\}$, the positive multiples of n. Each A_n contains n. The rule $c(n) := n$ is a choice function, defined by specification (Definition 1.2.3); no axiom is needed.
3. *A family with no rule in sight.* Let I be the set of non-empty subsets of $\mathbb{R}$, and $A_S := S$ for $S \in I$. A choice function picks an element of every non-empty set of reals. "The least element" fails, since $(0, 1)$ has none, and no rule that works for every S is known. Here the axiom supplies what the other rules do not.

A non-example by minimal change. In Example 2, add the index $n = 0$. The positive multiples of 0 form the empty set ($0 \mid k$ means $k = 0$), so $A_0 = \emptyset$, and no function can have $c(0) \in A_0$. Only the clause "A_i is non-empty for every i" fails, and without it the conclusion is false. That is why the proofs below remove the empty sets from a family before they choose. (Dropping "all at once" instead would leave nothing beyond the hypothesis.)

3.2.4 When choice is not needed

Two kinds of construction look like choice and are not; telling them apart from a real use is the skill this section is for.

Finitely many sets. *For every finite set I and every family $(A_i)_{i\in I}$ of non-empty sets, a choice function exists, with no appeal to the axiom.* For $I = \{1, 2, 3\}$, three applications of ∃E name $a_i \in A_i$, and $\{(1, a_1), (2, a_2), (3, a_3)\}$ is the graph of a choice function. For a finite set of arbitrary size we induct on its number of elements (Definition 2.5.2). Let $P(n)$ be: "for every set I with n elements and every family $(A_i)_{i\in I}$ of non-empty sets, there is a choice function". *Base case* $P(0)$: a set with 0 elements is the image of a bijection from $\{1, \dots, 0\} = \emptyset$, so it is empty, and the empty function is a choice function (Example 1). *Inductive step:* assume $P(n)$, and let I have $n + 1$ elements. Then $I \neq \emptyset$, since a bijection $\{1, \dots, n + 1\} \to I$ has a value at 1; pick $i_0 \in I$ by ∃E. The set $I' := I \setminus \{i_0\}$ has n elements (Corollary 2.5.7), so $P(n)$ gives a choice function c' for $(A_i)_{i\in I'}$. Since $A_{i_0} \neq \emptyset$, one more ∃E names $a_0 \in A_{i_0}$. The graph of c' together with the pair (i_0, a_0), with codomain $\bigcup_{i\in I} A_i$, is a function on $I' \cup \{i_0\} = I$, because $i_0 \notin I'$; and it is a choice function. So $P(n + 1)$ holds, and Logic and Proof, Axiom 4.2.1 gives $P(n)$ for every $n \in \mathbb{N}$. Each step uses two ∃E's and no new principle; the induction says nothing about an infinite I, which has no number of elements.

A rule that picks. If one description names an element of each A_i, the choice function is defined by specification (W1), as the set of pairs (i, a) with a the element named for i. Typical rules: the **least element** of a non-empty set of natural numbers (Theorem 2.1.3); the **non-negative** square root of a positive real; in a bisection, **the left half** if it has the property in question, and otherwise the right half. The first rule is how Theorem 3.1.2 passed from a surjection $\mathbb{N} \to A$ to an injection $A \to \mathbb{N}$ with no axiom: the least preimage is named, not chosen.

Warning. **Choice is not "picking an element".** "Let $a \in A$" is a single ∃E and needs no axiom; neither does picking from ten sets. The axiom is needed only for picking **one element from each of infinitely many sets, with no rule**. A proof that says "choose" need not use it, and one that never says "choose" may: "for each n, let g_n be a list of A_n" is a use, however it is worded.

The warning is the whole method; here it is as a checklist.

Example. Method: name the choice

Template. At each line that produces an object for each of many indices at once, ask whether one rule names it for every index: a formula, "the least", "the unique", or one list fixed in advance. If so, define the function by specification; no choice is used. If not, form the family (S_i) of non-empty sets of candidates and write "**by Axiom 3.2.1** there is c with $c(i) \in S_i$" at that line, in bold.

When to use it. A proof says "for each n, let ...", builds a sequence or a family of lists, or inverts a surjection.

The usual failure. An unflagged "for each n, choose". Flagging a single ∃E, or a rule, as a use. An empty S_i left in the family (the non-example above).

Quick check. A proof says: "For each $n \in \mathbb{N}$ the set $\{k \in \mathbb{N} : k^2 > n\}$ is non-empty; choose k_n in it." Does this line need Axiom 3.2.1? Rewrite it so that it plainly does not.

Solution. No: it need not. The least element (Theorem 2.1.3) names k_n, and so does the formula $k_n := n + 1$, since $(n+1)^2 = n^2 + 2n + 1 > n$. Either rewrite defines $n \mapsto k_n$ by specification.

Example. Choice or a rule?

Which of the following needs Axiom 3.2.1?

(a) A function sending each non-empty finite set of reals to one of its elements.

(b) A function sending each open interval $\{x \in \mathbb{R} : a < x < b\}$ with $a < b$ to a rational number in it.

(c) A function sending each countably infinite subset $A \subseteq \mathbb{R}$ to a bijection $\mathbb{N} \to A$.

(d) For a given family $(A_n)_{n \in \mathbb{N}}$ of non-empty subsets of $\mathbb{Q}$, a sequence with $a_n \in A_n$ for every n.

Solution.

(a) No: $S \mapsto \max S$, which exists by Proposition 2.3.8.

(b) No, once one list of $\mathbb{Q}$ is fixed. Take a surjection $q\colon \mathbb{N} \to \mathbb{Q}$ (Theorem 3.1.8, one ∃E). Between two reals lies a rational (a school fact; *Analysis on the Real Line*, Chapter 1 proves it), so $\{n \in \mathbb{N} : a < q(n) < b\}$ is non-empty, and q of its least element (Theorem 2.1.3) is named by a rule.

(c) Yes, as far as this book is concerned. Each A has bijections $\mathbb{N} \to A$ (Definition 3.1.2), but no rule names one for an arbitrary A. The family (S_A) of sets of bijections, indexed by the countably infinite subsets of $\mathbb{R}$ (a set, by specification in $\mathcal{P}(\mathbb{R})$), consists of non-empty sets, and Axiom 3.2.1 gives the function.

(d) No: with the same fixed q, $a_n := q(\min\{k \in \mathbb{N} : q(k) \in A_n\})$; the set is non-empty

because $A_n \neq \emptyset$ and q is onto.

One fixed list turns "pick an element" into "take the first one on the list", and that is a rule.

3.2.5 Right inverses

The first consequence settles the question Section 1.6 left open. By Proposition 1.6.2, a function with a right inverse is surjective; the converse is where choice enters.

Theorem 3.2.2. Surjections Have Right Inverses

Let $f\colon X \to Y$ be a surjective function. Then f has a right inverse: there is a function $g\colon Y \to X$ with $f(g(y)) = y$ for every $y \in Y$.

Idea. A right inverse must name a preimage of every y. The preimages of the points of Y form a family of sets indexed by Y, each non-empty because f is onto. A choice function for that family is exactly a right inverse. This is the method of Example (Method: name the choice): for an arbitrary f no rule names a preimage, so the line is flagged.

Proof. For $y \in Y$, let $P_y := f^{-1}(\{y\}) = \{x \in X : f(x) = y\}$ (Definition 1.7.2). This defines a family $(P_y)_{y\in Y}$ of subsets of X, indexed by Y. Each P_y is non-empty, since f is surjective (Definition 1.5.4). **By Axiom 3.2.1** there is a function $c\colon Y \to \bigcup_{y\in Y} P_y$ with $c(y) \in P_y$ for every $y \in Y$. The union is a subset of X, so the graph of c is a subset of $Y \times X$, and with codomain X it is a function $g\colon Y \to X$ with $g(y) = c(y)$ (Definition 1.5.1). For every $y \in Y$, $g(y) \in P_y$, that is, $f(g(y)) = y$. So $f \circ g = \mathrm{id}_Y$, and g is a right inverse of f (Definition 1.6.1 (b)).

■

Together with Proposition 1.6.2: a function is surjective **if and only if** it has a right inverse. The theorem is in fact equivalent to the axiom: a right inverse of the projection $(i, a) \mapsto i$, from the set of pairs with $a \in A_i$ onto I, is a choice function in disguise.

Quick check. Let $f\colon \mathbb{Z} \to \mathbb{N}$, $f(k) := |k|$. It is surjective. Does the existence of a right inverse of f need Axiom 3.2.1?

Solution. No. Each $n \in \mathbb{N}$ has the preimage n, and also $-n$ when $n > 0$; the rule "take the non-negative one" names one of them: $g(n) := n$. Then $f(g(n)) = |n| = n$, so $g\colon \mathbb{N} \to \mathbb{Z}$ is a right inverse, defined by a formula. The axiom is needed only when no such rule is available.

3.2.6 Countable unions

Now the theorem the section opened with. The second form, with any countable index set, is the one used in practice.

Theorem 3.2.3. Countable Unions of Countable Sets

(a) Let $(A_n)_{n\in\mathbb{N}}$ be a family of sets such that A_n is countable for every $n \in \mathbb{N}$. Then $\bigcup_{n\in\mathbb{N}} A_n$ is countable.

(b) Let I be a countable set and $(A_i)_{i\in I}$ a family of sets such that A_i is countable for every $i \in I$. Then $\bigcup_{i\in I} A_i$ is countable.

Idea (Scratch work). This is the grid of the opening, with the lists supplied by the axiom. ① Throw away the empty sets: the axiom needs non-empty ones, and they add nothing to the union. ② For each remaining n, the surjections $\mathbb{N} \to A_n$ form a non-empty set; choose one from each, all at once. ③ The chosen lists turn the grid $J \times \mathbb{N}$ into a surjection onto the union, and the grid is countable by Section 3.1.

Part (b) is part (a) after renumbering the index set by a list. As givens and goal, for (a):

Givens	Goal
A_n countable for every n	$\bigcup_{n\in\mathbb{N}} A_n$ countable
$J := \{n : A_n \neq \emptyset\}$; $J \times \mathbb{N}$ countable (Corollary 3.1.7)	a surjection $F\colon J \times \mathbb{N} \to \bigcup_{n\in\mathbb{N}} A_n$
for each single $n \in J$: some surjection $\mathbb{N} \to A_n$ (one ∃E per n)	$F(n, m) :=$ (a list of A_n)(m), which needs every list at once, as one function $n \mapsto c(n)$
gap: from "for every n there is a list" to "there is one function giving a list for every n"	closed by Axiom 3.2.1 on $(S_n)_{n\in J}$, the only flagged line

Before reading on: which line uses choice, and why can ∃E *not replace it?*

Proof.

(a) Let $U := \bigcup_{n\in\mathbb{N}} A_n$ and $J := \{n \in \mathbb{N} : A_n \neq \emptyset\}$.
If $J = \emptyset$, every A_n is empty, so $U = \emptyset$, which is countable by Definition 3.1.1.
Suppose $J \neq \emptyset$. For $n \in J$, let

$$S_n := \{h \in A_n^{\mathbb{N}} : h \text{ is surjective}\},$$

the set of surjections $\mathbb{N} \to A_n$ (Definition 1.2.3, with $A_n^{\mathbb{N}}$ the set of functions of Section 1.5). Since A_n is countable and non-empty, $S_n \neq \emptyset$ (Definition 3.1.1). **By Axiom 3.2.1**, applied to the family $(S_n)_{n\in J}$, there is a function $c\colon J \to \bigcup_{n\in J} S_n$ with $c(n) \in S_n$ for every $n \in J$. This is the only line of the proof that uses the axiom.
Define $F\colon J \times \mathbb{N} \to U$ by $F(n, m) := c(n)(m)$. It takes values in U: $c(n)$ maps into $A_n \subseteq U$. It is surjective: let $x \in U$; then $x \in A_n$ for some $n \in \mathbb{N}$ (Definition 1.3.4), so $A_n \neq \emptyset$ and $n \in J$; since $c(n)$ is a surjection onto A_n, there is $m \in \mathbb{N}$ with $c(n)(m) = x$, that is, $F(n, m) = x$.
The set J is countable by Proposition 3.1.3, as a subset of $\mathbb{N}$, which is countable (the identity is a surjection). So $J \times \mathbb{N}$ is countable by Corollary 3.1.7 (a), and it is non-empty, since it contains $(n_0, 0)$ for any $n_0 \in J$. By Definition 3.1.1 there is a surjection $s\colon \mathbb{N} \to J \times \mathbb{N}$. Then $F \circ s\colon \mathbb{N} \to U$ is surjective (Theorem 1.5.4 (b)), and U is countable.

(b) Let $U := \bigcup_{i\in I} A_i$. If $I = \emptyset$, then $U = \emptyset$, which is countable. Otherwise Definition 3.1.1 gives a surjection $s\colon \mathbb{N} \to I$; fix one. For $n \in \mathbb{N}$ put $B_n := A_{s(n)}$, a countable set. Then $\bigcup_{n\in\mathbb{N}} B_n = U$. ($\subseteq$) An element of B_n lies in $A_{s(n)}$ with $s(n) \in I$. ($\supseteq$) If $x \in A_i$ with $i \in I$, then $i = s(n)$ for some $n \in \mathbb{N}$, because s is onto, and $x \in B_n$. By (a), U is countable.

■

The line in bold is the only use of the axiom. The surjections s of parts (a) and (b) are single objects, each named by one ∃E. What needed the axiom was a surjection **for every** $n \in J$ at once: ∃E supplies $c(n)$ only inside the box of a fixed n, and F needs all of them outside every such box. The set J is there because for $A_n = \emptyset$ there is no function $\mathbb{N} \to A_n$ at all (Proposition 1.5.2 (b)), so $S_n = \emptyset$. The theorem completes the closure properties of countable sets: subsets, images, finite products, countable unions.

Neither hypothesis can be dropped: Section 3.3 shows that $\mathbb{R}$ is not countable, and $\mathbb{R}$ is the union of the single set $\mathbb{R}$, and also of the countable sets $\{x\}$, $x \in \mathbb{R}$.

Warning. **The choice is of the lists, not of preimages.** A surjection $\mathbb{N} \to A$ gives least preimages by a rule (Theorem 3.1.2), but only once the surjection is **in hand**. In Theorem 3.2.3, what is missing is the surjection itself, one for each A_n, and the sets A_n need not be sets of natural numbers, so no "least" is available to name one.

3.2.7 Unions without choice

Many countable unions met in practice come with their lists, and then no axiom is used.

Example. Unions that come with their lists

(a) Show that $\mathbb{Q} = \bigcup_{n\in\mathbb{Z}_{>0}} Q_n$, where $Q_n := \{m/n : m \in \mathbb{Z}\}$, and list the union without using Axiom 3.2.1.

(b) Does the proof in Theorem 3.1.8 that $\mathbb{Q}$ is countable use Axiom 3.2.1?

Solution.

(a) By the definition $\mathbb{Q} := \{m/n : m \in \mathbb{Z},\ n \in \mathbb{Z}_{>0}\}$, a number is rational exactly when it lies in Q_n for some $n \in \mathbb{Z}_{>0}$, so the two sets are equal. Fix the bijection $z\colon \mathbb{N} \to \mathbb{Z}$ of Theorem 3.1.8 ($z(2k) = k$, $z(2k+1) = -(k+1)$). Then $k \mapsto z(k)/n$ lists Q_n, and the whole family of lists is the single function

$$L\colon \mathbb{Z}_{>0} \times \mathbb{N} \to \mathbb{Q}, \qquad L(n,k) := z(k)/n,$$

defined by specification. It is onto $\mathbb{Q}$: for m/n with $m \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$, take k with $z(k) = m$. Since $\mathbb{Z}_{>0} \times \mathbb{N}$ is countable and non-empty (Proposition 3.1.3, Corollary 3.1.7), composing L with a surjection $\mathbb{N} \to \mathbb{Z}_{>0} \times \mathbb{N}$ lists $\mathbb{Q}$. The grid is the same as in Theorem 3.2.3; the difference is that the rows were written down, not chosen.

(b) No, and its place before Axiom 3.2.1 does not settle this, since by the warning in "When choice is not needed" a proof can use the axiom without naming it; we check the lines. The maps z and $(m,n) \mapsto m/n$ are formulas. The results cited name finitely

many objects by ∃E: one injection in Proposition 3.1.3, two in Corollary 3.1.7 (a), one surjection in Proposition 3.1.4. The passage from a surjection to an injection in Theorem 3.1.2 takes the least preimage, a rule; the return from an injection to a list goes through Lemma 3.1.1, whose list is defined by recursion from least elements (Theorem 2.1.3), again a rule. No line picks from infinitely many sets without a rule.

The pattern is general: if one formula in n lists every A_n, the family of lists is a single function, and no axiom is used. Choice enters only when each A_n is known to be countable as a bare existence statement.

3.2.8 Algebraic numbers

The theorem pays off at once. A real number is called **algebraic** if it is a root of a non-zero polynomial with integer coefficients. To keep this inside what the book has defined, we speak of coefficient tuples. For $d \geq 1$ and $c = (c_0, c_1, \ldots, c_d) \in \mathbb{Z}^{d+1}$ (a $(d+1)$-tuple, entries numbered from 0), let

$$p_c(x) \coloneqq \sum_{k=0}^{d} c_k x^k \qquad (x \in \mathbb{R})$$

(Definition 2.3.1, Definition 2.3.2), and call c **non-zero** if $c_k \neq 0$ for some k. Then $x \in \mathbb{R}$ is **algebraic** if $p_c(x) = 0$ for some $d \geq 1$ and some non-zero $c \in \mathbb{Z}^{d+1}$. Constant polynomials are left out without loss, since a non-zero constant has no roots.

For example, $\sqrt{2}$ is algebraic, a root of $x^2 - 2$ ($c = (-2, 0, 1)$). Every rational m/n is algebraic, a root of $nx - m$ ($c = (-m, n)$). So is $\sqrt{2} + \sqrt{3}$, a root of $x^4 - 10x^2 + 1$.

We use one fact from school algebra, not proved here: **if $c \in \mathbb{Z}^{d+1}$ is non-zero, then p_c has at most d real roots**. (It follows from the factor theorem.) In particular the set $R(c) \coloneqq \{x \in \mathbb{R} : p_c(x) = 0\}$ is finite.

Theorem 3.2.4. The Algebraic Numbers Are Countable

The set of algebraic real numbers is countable.

Idea. Sort the polynomials by degree. For each d, the coefficient tuples form a countable set, and each polynomial contributes finitely many roots: a countable union of finite sets. Then take the union over d. Both unions are instances of Theorem 3.2.3 (b). Steps 2 and 3 are route (S) of Example (Method: list it): each union is the image of a countable grid. Step 1 only cites closure under products and subsets.

Proof. Let Alg be the set of algebraic real numbers, and for $d \geq 1$ let Z_d be the set of non-zero tuples in $\mathbb{Z}^{d+1}$.

Step 1. Let $d \geq 1$. The set $\mathbb{Z}$ is countable (Theorem 3.1.8), and $\mathbb{Z}^{d+1}$ is the product of $d+1 \geq 2$ factors all equal to $\mathbb{Z}$, so it is countable by Corollary 3.1.7 (b). Hence $Z_d \subseteq \mathbb{Z}^{d+1}$ is countable (Proposition 3.1.3).

Step 2. For $c \in Z_d$, the root set $R(c)$ is finite by the school fact above, hence countable (Theorem 3.1.2, (iii) ⇒ (i)). So $\mathrm{Alg}_d \coloneqq \bigcup_{c \in Z_d} R(c)$, the set of roots of the non-zero polynomials

of degree at most d, is countable by Theorem 3.2.3 (b), with the countable index set Z_d.

Step 3. By definition, $\text{Alg} = \bigcup_{d \in \mathbb{Z}_{>0}} \text{Alg}_d$. The index set $\mathbb{Z}_{>0} \subseteq \mathbb{N}$ is countable (Proposition 3.1.3). So Alg is countable by Theorem 3.2.3 (b).

■

The proof cites Theorem 3.2.3 twice, and so it uses Axiom 3.2.1. Here the axiom can be avoided (not proved in the text; nothing later uses it): list each finite root set in increasing order, which is a rule, and replace the two unions by one fixed enumeration of all integer coefficient tuples. Exercise C2 asks you to carry this out. The countability of Alg has a striking consequence once we know that $\mathbb{R}$ is not countable: Section 3.3 deduces that some real numbers are not algebraic.

3.2.9 Exercises

3.2.9.1 A. Check your understanding

Exercise. A1

These parts are about the proof of Theorem 3.2.3.

(a) Which line of the proof of part (a) uses Axiom 3.2.1? What are the index set I and the sets A_i of the axiom at that line?

(b) Why does the proof introduce the set J?

(c) Run the proof on $A_n := \{n, n+1\}$ for $n \in \mathbb{N}$, with the lists $c(n)(m) := n$ for odd m and $c(n)(m) := n+1$ for even m. What is J, and what is $F(3,2)$?

(d) State the idea of the proof in two sentences.

(e) Is Axiom 3.2.1 needed to show that $\bigcup_{n \in \mathbb{N}} A_n$ is countable when every A_n is a subset of $\mathbb{N}$? Justify your answer.

Solution.

(a) The line "By Axiom 3.2.1, applied to the family $(S_n)_{n \in J}$, there is a function c on J with $c(n) \in S_n$". There $I = J$, the set of indices with $A_n \neq \emptyset$, and the sets of the axiom are the S_n, the sets of surjections $\mathbb{N} \to A_n$. The axiom chooses lists, not elements of the A_n.

(b) The axiom applies only to families of **non-empty** sets. If $A_n = \emptyset$, there is no function $\mathbb{N} \to A_n$ at all (Proposition 1.5.2 (b)), so $S_n = \emptyset$, and the family $(S_n)_{n \in \mathbb{N}}$ would not qualify. Empty sets add nothing to the union, so restricting to J loses nothing.

(c) Every A_n is non-empty, so $J = \mathbb{N}$. The pair $(3,2)$ has $m = 2$ even, so $F(3,2) = c(3)(2) = 3 + 1 = 4$. (Each $c(n)$ is onto $\{n, n+1\}$: $c(n)(1) = n$ and $c(n)(0) = n+1$.)

(d) Choose, with the axiom, a list of each non-empty A_n, all at once. The lists turn the countable grid $J \times \mathbb{N}$ into a surjection onto the union, so the union is countable.

(e) No. The union is a subset of $\mathbb{N}$, so it is countable by Proposition 3.1.3. (Even the proof can run without the axiom: $h_A(m) := m$ for $m \in A$ and $h_A(m) := \min A$ otherwise (Theorem 2.1.3) is a rule that maps $\mathbb{N}$ onto any non-empty $A \subseteq \mathbb{N}$.)

3.2.9.2 B. Practice

Exercise. B1: Which constructions need choice?

Determine which of the following constructions need Axiom 3.2.1. Justify your answer.

(a) Choose a real number in each interval $(n, n+1)$, $n \in \mathbb{N}$.
(b) Choose an element of each non-empty subset of $\mathbb{N}$.
(c) Choose an element of each non-empty subset of $\mathbb{R}$.
(d) Choose one of the two square roots of each positive real number.

Solution.

(a) No. The rule $n \mapsto n + \frac{1}{2}$ names an element of each interval, since $n < n + \frac{1}{2} < n + 1$.
(b) No. The rule "the least element" names one, by Theorem 2.1.3: $S \mapsto \min S$ is a choice function, defined by specification.
(c) Yes, as far as this book is concerned. The rule "the least element" fails, since $(0, 1)$ has no least element, and no rule is known that names an element of every non-empty set of reals. A proof that needs such a function uses the axiom, and says so.
(d) No. The rule "the positive one" names one root of each $y > 0$: $y \mapsto \sqrt{y}$.

Exercise. B2: Finite sequences

Prove that the set of all finite sequences of natural numbers is countable, and say whether your proof uses Axiom 3.2.1. Here a finite sequence of length $k \in \mathbb{N}$ is a function $\{1, \dots, k\} \to \mathbb{N}$, represented by its graph, a subset of $\mathbb{Z}_{>0} \times \mathbb{N}$; the sequence of length 0 is $\emptyset$.

Hint: Theorem 2.3.1, together with one fixed surjection $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$.

Solution. Let Seq be the set of $x \in \mathcal{P}(\mathbb{Z}_{>0} \times \mathbb{N})$ such that x is the graph of a function $\{1, \dots, k\} \to \mathbb{N}$ for some $k \in \mathbb{N}$ (Definition 1.2.3, Definition 1.3.2). This k is determined by x, since $\{1, \dots, k\}$ is the set of first coordinates of x, and k is its number of elements (Corollary 2.5.4); call it the **length** of x, and let Seq_k be the set of elements of length k. So $\mathrm{Seq} = \bigcup_{k \in \mathbb{N}} \mathrm{Seq}_k$, and $\mathrm{Seq}_0 = \{\emptyset\}$.

With choice. Each Seq_k is countable (for $k \geq 2$ it is in bijection with $\mathbb{N}^k$, by $x \mapsto (x(1), \dots, x(k))$; Seq_1 with $\mathbb{N}$; Seq_0 has one element), so Theorem 3.2.3 (a) applies. This route uses Axiom 3.2.1, through the theorem.

Without choice. Fix one surjection $\sigma \colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ (Theorem 3.1.6, Definition 3.1.1; a single $\exists$E), and write $\sigma(n) = (\sigma_1(n), \sigma_2(n))$. For $x \in \mathrm{Seq}$ of length k and $m \in \mathbb{N}$, let $x \frown m \coloneqq x \cup \{(k+1, m)\}$, the sequence x with m appended; it has length $k+1$. Every $y \in \mathrm{Seq}_{k+1}$ is $x \frown m$ for x the restriction of y to $\{1, \dots, k\}$ and $m = y(k+1)$.

Let $X \coloneqq \mathrm{Seq}^{\mathbb{N}}$, the set of functions $\mathbb{N} \to \mathrm{Seq}$, let $a \in X$ be the constant function with value $\emptyset$, and define $g \colon \mathbb{N} \times X \to X$ by

$$g(k, s)(n) \coloneqq s(\sigma_1(n)) \frown \sigma_2(n).$$

By Theorem 2.3.1 there is a function $k \mapsto s_k$ from $\mathbb{N}$ to X with $s_0 = a$ and $s_{k+1}(n) = s_k(\sigma_1(n)) \frown \sigma_2(n)$ for all $k, n \in \mathbb{N}$.

Claim: for every $k \in \mathbb{N}$, s_k maps $\mathbb{N}$ onto Seq_k. By Logic and Proof, Axiom 4.2.1 on k. For $k = 0$, every value of s_0 is $\emptyset$, and $\mathrm{Seq}_0 = \{\emptyset\}$. Assume the claim for k. Each value $s_{k+1}(n) = s_k(\sigma_1(n)) \frown \sigma_2(n)$ has length $k+1$, because $s_k(\sigma_1(n))$ has length k. Let $y \in \mathrm{Seq}_{k+1}$, say $y = x \frown m$ with $x \in \mathrm{Seq}_k$. By the hypothesis there is j with $s_k(j) = x$, and since σ is onto there is n with $\sigma(n) = (j, m)$. Then $s_{k+1}(n) = s_k(j) \frown m = y$. This proves the claim.

Now $n \mapsto s_{\sigma_1(n)}(\sigma_2(n))$ maps $\mathbb{N}$ onto Seq: for $y \in \mathrm{Seq}_k$, the claim gives j with $s_k(j) = y$, and some n has $\sigma(n) = (k, j)$. So Seq is countable. One surjection was named, and the lists s_k were defined from it by recursion: no choice is used. Either route earns full credit if the use of choice is reported correctly.

Exercise. B3

A **rational point** of the plane is a point of $\mathbb{Q}\times\mathbb{Q}$. Prove that the set of lines in the plane that pass through two different rational points is countable. Does your proof use Axiom 3.2.1?

Solution. Let $D := \{(p, q) \in (\mathbb{Q} \times \mathbb{Q}) \times (\mathbb{Q} \times \mathbb{Q}) : p \neq q\}$. The set $\mathbb{Q} \times \mathbb{Q}$ is countable by Theorem 3.1.8 and Corollary 3.1.7; so is its product with itself, again by Corollary 3.1.7, and so is the subset D (Proposition 3.1.3). For $(p, q) \in D$, let $\mathrm{line}(p, q)$ be the line through p and q, as a subset of $\mathbb{R}^2$: $\mathrm{line}(p, q) := \{p + t(q - p) : t \in \mathbb{R}\}$. Two different points lie on exactly one line (school geometry), so the lines in question form the image $\mathrm{line}(D)$, countable by Proposition 3.1.4. The map line is a formula, so no choice is used.

Exercise. B4: Prove or disprove

Prove each true statement, naming each use of Axiom 3.2.1 as in Example (Method: name the choice), and refute each false one with a concrete counterexample.

(a) If A_n is finite for every $n \in \mathbb{N}$, then $\bigcup_{n\in\mathbb{N}} A_n$ is countable.
(b) If A_n is finite for every $n \in \mathbb{N}$, then $\bigcup_{n\in\mathbb{N}} A_n$ is finite.
(c) Every surjection $f : \mathbb{N} \to Y$ has a right inverse that can be defined without Axiom 3.2.1.
(d) If A_n is countable for every $n \in \mathbb{N}$, then $\bigcup_{n\in\mathbb{N}} A_n$ is countably infinite.
(e) If $A_n \neq \emptyset$ for every $n \in \mathbb{N}$ and $\bigcup_{n\in\mathbb{N}} A_n$ is finite, then $A_m \cap A_n \neq \emptyset$ for some $m \neq n$.

Solution.

(a) **True.** Finite sets are countable (Theorem 3.1.2, (iii) ⇒ (i)), and Theorem 3.2.3 (a) applies. That theorem uses Axiom 3.2.1.
(b) **False.** Take $A_n := \{n\}$: the union is $\mathbb{N}$, which is infinite (Example (Hilbert's Hotel)).
(c) **True.** For $y \in Y$, the set $f^{-1}(\{y\}) \subseteq \mathbb{N}$ is non-empty, since f is onto, so $g(y) := \min f^{-1}(\{y\})$ exists by Theorem 2.1.3. This is a rule, and $f(g(y)) = y$.
(d) **False.** Take $A_n := \{0\}$ for every n: the union is $\{0\}$, which is finite, hence not countably infinite: a bijection $\mathbb{N} \to \{0\}$ would make $\mathbb{N}$ finite (Proposition 2.5.1), against Example (Hilbert's Hotel).
(e) **True, with no axiom.** The set $U := \bigcup_{n\in\mathbb{N}} A_n$ is non-empty (it contains the elements

of A_0) and finite, say with $k \geq 1$ elements via a bijection $\varphi\colon \{1, \dots, k\} \to U$ (one ∃E). Define $c(n) := \varphi(\min\{j : \varphi(j) \in A_n\})$ (Theorem 2.1.3); the set is non-empty because $A_n \neq \emptyset$ and φ is onto. This is a rule, and $c(n) \in A_n$. If c were injective, $\mathbb{N}$ would be equinumerous with $c(\mathbb{N}) \subseteq U$, which is finite (Proposition 2.5.6). Then $\mathbb{N}$ would be finite (Proposition 2.5.1), against Example (Hilbert's Hotel). So $c(m) = c(n)$ for some $m \neq n$, and that element lies in $A_m \cap A_n$. This is the pigeonhole idea of Example (Method: the pigeonhole principle), with infinitely many pigeons.

3.2.9.3 C. Going deeper

Exercise. C1: Exit check: countable unions

Prove that if A_n is countable for every $n \in \mathbb{N}$, then so is $\bigcup_{n\in\mathbb{N}} A_n$. Point to the step of your proof that uses Axiom 3.2.1.

Solution. Let $U := \bigcup_{n\in\mathbb{N}} A_n$ and $J := \{n \in \mathbb{N} : A_n \neq \emptyset\}$. If $J = \emptyset$, then $U = \emptyset$, which is countable. Let $J \neq \emptyset$. For $n \in J$, the set S_n of surjections $\mathbb{N} \to A_n$ is non-empty (Definition 3.1.1). **By Axiom 3.2.1**, applied to $(S_n)_{n\in J}$, there is a function c on J with $c(n) \in S_n$ for every $n \in J$: a list of every A_n at once, which no finite number of ∃E's gives. This is the step that uses the axiom.

Put $F(n, m) := c(n)(m) \in A_n \subseteq U$ for $(n, m) \in J \times \mathbb{N}$. It is onto U: if $x \in U$, then $x \in A_n$ for some $n \in \mathbb{N}$ (Definition 1.3.4), so $n \in J$, and $c(n)(m) = x$ for some m, as $c(n)$ is onto A_n. Since $J \subseteq \mathbb{N}$ is countable (Proposition 3.1.3), $J \times \mathbb{N}$ is countable (Corollary 3.1.7 (a)) and non-empty, so some $s\colon \mathbb{N} \to J \times \mathbb{N}$ is onto (Definition 3.1.1), and so is $F \circ s\colon \mathbb{N} \to U$ (Theorem 1.5.4 (b)). This is the proof of Theorem 3.2.3 (a).

Marking scheme. (10 points) - 1: handles the empty sets: the case where every A_n is empty, and the restriction to the non-empty ones before choosing. - 3: obtains, by Axiom 3.2.1, a surjection onto A_n for every n simultaneously, and says at that line that the axiom is used. - 2: defines a map from a set of pairs (or another index set) to the union. - 2: shows that this map is onto the union. - 2: shows that the index set is countable and non-empty, citing the product result, and concludes. Through injections $\iota_n\colon A_n \to \mathbb{N}$: 1 for noting that they exist for every n, empty A_n included (the empty function), so nothing is discarded; 3 for choosing all ι_n by Axiom 3.2.1, flagged; 2 for $x \mapsto (n_x, \iota_{n_x}(x))$ into $\mathbb{N} \times \mathbb{N}$, with n_x the least n with $x \in A_n$ (Theorem 2.1.3); 2 for its injectivity; 2 for concluding with Theorem 3.1.6 and Theorem 3.1.2, (ii) ⇒ (i). Fatal errors (0 for the step): "for each n let f_n be a list of A_n" with no mention of choice, an unflagged infinite ∃E that no rule licenses (0 for the choice step); listing $\mathbb{N} \times \mathbb{N}$ row by row, as in Example (Listing the rows one after another) (0 for the countability step).

Exercise. C2: Algebraic numbers without choice

Prove Theorem 3.2.4 without using Axiom 3.2.1.

Solution (Hint 1). *Use Exercise (B2: Finite sequences) to obtain, without choice, one surjection from $\mathbb{N}$ onto all coefficient tuples of all lengths together.*

Solution (Hint 2). *For an algebraic r, let $n(r)$ be the least index whose tuple has r as a root; it exists by Theorem 2.1.3.*

Solution. Use the notation of Theorem 3.2.4, and let Alg be the set of algebraic numbers.

One list of all coefficient tuples. Let ZSeq be defined as Seq in Exercise (B2: Finite sequences), with $\mathbb{Z}$ in place of $\mathbb{N}$, and let $z\colon \mathbb{N} \to \mathbb{Z}$ be the bijection of Theorem 3.1.8. Sending $x \in \text{Seq}$ to the sequence $i \mapsto z(x(i))$ maps Seq onto ZSeq (use z^{-1} entrywise to find a preimage), so ZSeq is countable without choice, by that exercise and Proposition 3.1.4. Since ZSeq is non-empty (it contains $\emptyset$, the sequence of length 0), fix one surjection $\mu\colon \mathbb{N} \to \text{ZSeq}$ (Definition 3.1.1), a single $\exists$E. A sequence y of length $d+1 \geq 2$ is read as the tuple $c = (y(1), \ldots, y(d+1)) \in \mathbb{Z}^{d+1}$, and every such tuple arises; write $p_y := p_c$ and $R(y) := R(c)$. Call $n \in \mathbb{N}$ **good for** $r \in \mathbb{R}$ if $\mu(n)$ has length at least 2, is non-zero, and $p_{\mu(n)}(r) = 0$. Then r is algebraic if and only if some n is good for r, since μ is onto.

An injection, by rules. For $r \in \text{Alg}$, let $n(r)$ be the **least** $n \in \mathbb{N}$ that is good for r (Theorem 2.1.3), and let

$$\rho(r) := \text{the number of elements of } \{s \in R(\mu(n(r))) : s < r\},$$

well defined because this set is a subset of the finite set $R(\mu(n(r)))$ (Proposition 2.5.6, Corollary 2.5.4). Both are named by rules, so $r \mapsto (n(r), \rho(r))$ is a function $\text{Alg} \to \mathbb{N} \times \mathbb{N}$, defined by specification.

It is injective. Let $r, r' \in \text{Alg}$ with $n(r) = n(r')$ and $\rho(r) = \rho(r')$; call this common index n, and suppose $r \neq r'$, say $r < r'$. Both are roots of $p_{\mu(n)}$. The set $\{s \in R(\mu(n)) : s < r\}$ is a subset of $\{s \in R(\mu(n)) : s < r'\}$, and a proper one, since r lies in the second and not in the first. By Proposition 2.5.6, the first has fewer elements: $\rho(r) < \rho(r')$, a contradiction. So $r = r'$.

Following it with the injection $(m, k) \mapsto 2^m 3^k$ of Theorem 3.1.6 gives an injection $\text{Alg} \to \mathbb{N}$ (Theorem 1.5.4 (a)), so Alg is countable by Theorem 3.1.2, (ii) $\Rightarrow$ (i). Apart from the single surjection μ, every object was named by a rule, so Axiom 3.2.1 is not used.

Marking scheme. (10 points) - 3: produces, without choice, one surjection (or injection) relating $\mathbb{N}$ to the coefficient tuples of **all** degrees at once, citing Exercise (B2: Finite sequences) or an explicit coding. - 3: assigns to each algebraic number its data (an index of a polynomial and a position among its roots) by **rules**, such as a least index and a count or the increasing order of the finite root set. - 4: proves that the resulting map is injective (or a map onto Alg surjective), concludes, and says why no step uses choice. Fatal errors (0 for the step): citing Theorem 3.2.3, which uses the axiom; "for each polynomial (or each d), take a list" with no rule given.

Exercise. C3: Finite unions

(a) Prove, without Axiom 3.2.1, that for every finite set I and every family $(A_i)_{i \in I}$ of countable sets, $\bigcup_{i \in I} A_i$ is countable.

(b) Explain in two sentences why your induction does not prove Theorem 3.2.3.

Solution.

(a) We use Logic and Proof, Axiom 4.2.1 on the number of elements of I. Let $P(n)$ be: "for every set I with n elements and every family $(A_i)_{i\in I}$ of countable sets, $\bigcup_{i\in I} A_i$ is countable".
Base case. A set I with 0 elements is empty, so $\bigcup_{i\in I} A_i = \emptyset$, which is countable.
Inductive step. Assume $P(n)$, and let I have $n+1$ elements and $(A_i)_{i\in I}$ be a family of countable sets. Since $n+1 \geq 1$, $I \neq \emptyset$; pick $i_0 \in I$. Then $I' := I \setminus \{i_0\}$ has n elements (Corollary 2.5.7), so $B := \bigcup_{i\in I'} A_i$ is countable by $P(n)$, applied to the family $(A_i)_{i\in I'}$. Since $I = I' \cup \{i_0\}$, an element lies in some A_i with $i \in I$ exactly when it lies in B or in A_{i_0}, so

$$\bigcup_{i\in I} A_i = B \cup A_{i_0},$$

which is countable by Proposition 3.1.5. So $P(n+1)$ holds, and Logic and Proof, Axiom 4.2.1 gives $P(n)$ for every n. Each step makes finitely many ∃E's, so no choice is used.

(b) The induction proves the statement for each finite number n of sets, and $\mathbb{N}$ is not finite (Example (Hilbert's Hotel)), so no instance of $P(n)$ is about the family $(A_n)_{n\in\mathbb{N}}$. Writing $\bigcup_{n\in\mathbb{N}} A_n$ as the union of the finite unions $A_0 \cup \cdots \cup A_k$ does not help, since that needs a list of every finite union at once, which is a choice of infinitely many lists again.

3.3 Diagonal Arguments: Uncountable Sets and Cantor's Theorem

Every infinite set met so far has turned out to be countable: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, finite products of countable sets, countable unions of them (Theorem 3.2.3), and even the algebraic numbers (Theorem 3.2.4). Is every infinite set countable? This section shows that the answer is no, by one argument, which starts from the game of Section 1.5 and is then used three times. Given any list, it builds an object that the list misses. The argument proves that the set of 0–1 sequences is uncountable, that no set can be mapped onto the set of its subsets (Cantor's theorem), and, with decimals, that $\mathbb{R}$ is uncountable.

3.3.1 Back to the five strings

Section 1.5 left a game open: one player lists five strings of five symbols 0 or 1, and the other must write a string that is not on the list. Searching all 32 strings works; a rule is better.

Example. Back to the five strings

Find a rule that, from any list $s_1, \ldots, s_5$ of strings of five symbols 0 or 1, builds a string not on the list. Run it on 00000, 11111, 01010, 10101, 00111, and prove that it always works.

Solution. Let the new string g have, as its k-th symbol, the flip of the k-th symbol of the k-th string:

$$g(k) := 1 - s_k(k) \qquad (k = 1, \ldots, 5)$$

(strings are functions $\{1,\dots,5\} \to \{0,1\}$, Section 1.5). On the given list, the symbols $s_1(1),\dots,s_5(5)$ are $0,1,0,0,1$, so $g = 10110$. It differs from 00000 in place 1, from 11111 in place 2, from 01010 in place 3, from 10101 in place 4 and from 00111 in place 5.

For any list: for each k, $g(k) \neq s_k(k)$, since $1 - b \neq b$ for $b \in \{0,1\}$. So $g \neq s_k$ (Proposition 1.5.1), for $k = 1,\dots,5$. The k-th step looks only at the k-th string, in its own place k.

The rule never used the number 32. It used one place for each string on the list. Give the strings infinitely many places, indexed by $\mathbb{N}$, and let the list be infinite too, and the same rule still applies.

Quick check. Can the rule handle a list of six strings of five symbols? Does that contradict anything?

Solution. No. The sixth string has no sixth place to be flipped in. Nothing is contradicted: a list of 32 strings may contain every string. The rule needs as many places as strings, and in the next subsection both are indexed by $\mathbb{N}$.

3.3.2 A sequence that is not on the list

Recall from Section 1.5 that $\{0,1\}^{\mathbb{N}}$ is the set of all functions $\mathbb{N} \to \{0,1\}$: the sequences of zeros and ones, indexed from 0. These are the strings of the game with places indexed by $\mathbb{N}$. It is infinite, and it looks no bigger than $\mathbb{N} \times \mathbb{N}$, which is countable. To show that it is **not** countable we must show, by Definition 3.1.1, that it is non-empty and that **no** function $f\colon \mathbb{N} \to \{0,1\}^{\mathbb{N}}$ is onto. So we take an arbitrary list $f(0), f(1), f(2), \dots$ of sequences and look for a sequence that is not on it.

Write the list as a table: row n is the sequence $f(n)$, and the entry in row n and column k is the number $f(n)(k)$. Here is the start of one such table, with the entries in places $(0,0),(1,1),(2,2),(3,3)$ boxed:

place	0	1	2	3	4	$\cdots$
$f(0)$	$\boxed{0}$	1	0	1	0	$\cdots$
$f(1)$	1	$\boxed{1}$	1	1	1	$\cdots$
$f(2)$	0	0	$\boxed{0}$	0	0	$\cdots$
$f(3)$	1	0	0	$\boxed{1}$	1	$\cdots$
$\vdots$						
g	1	0	1	0		$\cdots$

The boxed entries run down the **diagonal** of the table. The bottom row g is the diagonal with every entry flipped: $g(n) = 1 - f(n)(n)$. It cannot be row 0, because it differs from $f(0)$ in place 0; it cannot be row 1, because it differs from $f(1)$ in place 1; and so on down the table. Nothing in this reasoning used the particular entries.

Theorem 3.3.1. The 0–1 Sequences Are Uncountable

The set $\{0,1\}^{\mathbb{N}}$ of all sequences of zeros and ones is uncountable.

Idea (Scratch work). By Definition 3.1.1, "uncountable" has two parts: the set is non-empty, and no map from $\mathbb{N}$ onto it exists. The second is a statement about **every** f, so take f arbitrary and look for a sequence it misses. As givens and goal:

Givens	Goal
$f\colon \mathbb{N} \to \{0,1\}^{\mathbb{N}}$ arbitrary	f is not onto; and $\{0,1\}^{\mathbb{N}} \neq \emptyset$
—	some $g \in \{0,1\}^{\mathbb{N}}$ with $g \neq f(n)$ for every n
$g \neq f(n)$ as soon as g and $f(n)$ differ at one place (Proposition 1.5.1)	pick the place for each n: place n, as in the game
gap: $g(n) \neq f(n)(n)$ for every n	closed by $g(n) \coloneqq 1 - f(n)(n)$

The proof writes this forwards.

Proof. Let $f\colon \mathbb{N} \to \{0,1\}^{\mathbb{N}}$ be any function. Define $g\colon \mathbb{N} \to \{0,1\}$ by

$$g(n) \coloneqq 1 - f(n)(n) \qquad (n \in \mathbb{N});$$

its values lie in $\{0,1\}$, since $1-0=1$ and $1-1=0$. So $g \in \{0,1\}^{\mathbb{N}}$. For every $n \in \mathbb{N}$, $g(n) \neq f(n)(n)$, since no $b \in \{0,1\}$ has $1-b=b$. Hence $g \neq f(n)$: if $g = f(n)$, then $g(n) = f(n)(n)$, which is false; the two functions differ at place n [=E, ¬I; Proposition 1.5.1]. So g is not a value of f, and f is not surjective. Since f was arbitrary, no function $\mathbb{N} \to \{0,1\}^{\mathbb{N}}$ is surjective. The set $\{0,1\}^{\mathbb{N}}$ is non-empty, since it contains the zero sequence. By Definition 3.1.1, $\{0,1\}^{\mathbb{N}}$ is not countable.

■

This is the move of the section.

Example. Method: the diagonal

Template. To show that no map from I onto X exists (for "uncountable": $I = \mathbb{N}$, and check $X \neq \emptyset$), let $f\colon I \to X$ be arbitrary. Build $d \in X$ whose entry at i differs from the entry of $f(i)$ at i, for every $i \in I$. Then $d \neq f(i)$ for each i, so f is not onto. Since f was arbitrary, no such map exists.

When to use it. The elements of X are themselves functions or subsets on the index set of the list: sequences, digit strings, subsets of I.

The usual failure. A d that falls outside X (a decimal ending in 9s, met below; a sequence of the wrong kind). A difference at place i that is not a real difference (two expansions of one number). Running the construction on one list only (the warning below).

Quick check. Would the unflipped diagonal, $g(n) \coloneqq f(n)(n)$, do? Test it on the list whose every entry is the zero sequence.

Solution. No. There g is the zero sequence, which is $f(0)$. The new object must differ from the n-th entry at place n, for every n.

Quick check. Run the proof on the list $f(n) \coloneqq \mathbf{1}_{\{n\}}$, the sequence with a 1 in place n and 0 elsewhere. What is g? Is it on the list?

Solution. Here $f(n)(n) = \mathbf{1}_{\{n\}}(n) = 1$ for every n, so $g(n) = 1 - 1 = 0$ for every n: g is the zero sequence. It is indeed not on the list, since every $f(n)$ has a 1 in place n.

Warning. **The diagonal object depends on the list.** "The diagonal sequence" is not one sequence: each list has its own, and a different list may well contain the g built from this one (the list $g, f(0), f(1), \dots$ does). And the conclusion "uncountable" needs the list to be **arbitrary**. Running the construction on one list, or on a few, shows only that those lists miss something; concluding "so no list works" from them is the error (N1) of Logic and Proof, Example (What is not allowed). The proof above starts from "let f be **any** function", and that is what makes its conclusion universal.

Example. A function that outgrows a list

Let $f_0, f_1, f_2, \dots$ be any list of functions $\mathbb{N} \to \mathbb{N}$. Find $g\colon \mathbb{N} \to \mathbb{N}$ such that, for every $k \in \mathbb{N}$, $g(n) > f_k(n)$ for every $n \geq k$.

Solution. Idea. The flipped diagonal beats f_n at place n only. To beat f_k from place k on, let place n beat $f_0, \dots, f_n$ at once: finitely many, so a maximum exists.

Let

$$g(n) \coloneqq \max\{f_0(n), \dots, f_n(n)\} + 1 \qquad (n \in \mathbb{N}).$$

The set is $\{x_1, \dots, x_{n+1}\}$ with $x_{k+1} \coloneqq f_k(n)$, so the maximum exists by Proposition 2.3.8; it is one of the x_j, so $g(n) \in \mathbb{N}$. For $k \in \mathbb{N}$ and $n \geq k$, $f_k(n)$ is one of the numbers in the set, so $f_k(n) \leq \max\{f_0(n), \dots, f_n(n)\} < g(n)$. The example asks more of g than a diagonal does, and each step still looks at finitely many entries at one place.

3.3.3 Back to Russell: Cantor's theorem

Section 1.2 proved Russell's theorem (Theorem 1.2.4): the set R_A disagrees with each candidate $x \in A$ about x itself, so it is not in A. Here the same disagreement becomes a theorem about sizes.

The table had a row for each $n \in \mathbb{N}$ and a column for each place $k \in \mathbb{N}$. Nothing about the diagonal needs the rows and the columns to be indexed by $\mathbb{N}$: it needs only that they are indexed by the **same** set. A subset S of a set X is a row with one entry for each $x \in X$, "in" or "out", the values of $\mathbf{1}_S$. So the argument applies to any set and the set of its subsets.

Theorem 3.3.2. Cantor's Theorem

Let X be a set. Then there is **no** surjection $X \to \mathcal{P}(X)$.

Try it first (ten minutes): given a function $f\colon X \to \mathcal{P}(X)$, which subset of X could be missed by f? Try $X = \{1, 2, 3\}$ with a function of your own first.

Idea. The first attempts look for a subset that is "too big" or "too small" to be a value, such as X itself or $\emptyset$, and fail: f may well take both values. Size is the wrong idea. A set D differs from $f(x)$ as soon as the two disagree about **one** element, and the only element we know anything about in connection with $f(x)$ is x itself. So we make D disagree with $f(x)$ at x: put x into D exactly when $x \notin f(x)$. This is the diagonal of the table, flipped. It is the method of Example (Method: the diagonal), with the rows and the places both indexed by X.

Before reading on: where is surjectivity used?

Proof. Let $f\colon X \to \mathcal{P}(X)$ be a function, and let

$$D \coloneqq \{x \in X : x \notin f(x)\},$$

a subset of X by Definition 1.2.3, so $D \in \mathcal{P}(X)$ (Definition 1.3.2). Suppose f is surjective. Then there is $d \in X$ with $f(d) = D$ (Definition 1.5.4). If $d \in D$, then $d \notin f(d)$ by the definition of D, that is, $d \notin D$, a contradiction. Hence $d \notin D$. Then $d \notin f(d)$, and since $d \in X$, the definition of D gives $d \in D$, a contradiction again. So f is not surjective. This proves the theorem. ∎

Surjectivity was used once, to obtain d; everything else holds for every function f. Read without the supposition, the proof shows that $D \neq f(x)$ for **every** $x \in X$: the two sets disagree about x. Three consequences follow.

(i) *Russell's theorem is the same argument.* In Theorem 1.2.4, the set $R_A = \{x \in A : x \notin x\}$ is the set D built from the rule $f(x) \coloneqq x$: each $x \in A$ is tested against itself. The proof that D differs from every $f(x)$ becomes the proof that R_A differs from every element of A, that is, $R_A \notin A$. (The rule $x \mapsto x$ need not map into $\mathcal{P}(A)$, but the argument never used that $f(x) \subseteq X$, only the test "$x \in f(x)$".)

(ii) *The power set is strictly bigger.* The map $x \mapsto \{x\}$ is an injection $X \to \mathcal{P}(X)$, since $\{x\} = \{y\}$ gives $x = y$. So $\mathcal{P}(X)$ has at least as many elements as X, in the sense that X is in bijection with a subset of it, and by the theorem it is not equinumerous with X, since a bijection would be a surjection. Section 3.4 names this relation: X is strictly smaller than $\mathcal{P}(X)$.

(iii) *There is no largest size.* $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, ...: each set in this sequence is strictly

bigger than the one before.

Corollary 3.3.3. The Subsets of the Naturals

The power set $\mathcal{P}(\mathbb{N})$ is uncountable.

Proof. The set $\mathcal{P}(\mathbb{N})$ is non-empty, since $\emptyset \in \mathcal{P}(\mathbb{N})$, and by Theorem 3.3.2 with $X = \mathbb{N}$ there is no surjection $\mathbb{N} \to \mathcal{P}(\mathbb{N})$. By Definition 3.1.1, $\mathcal{P}(\mathbb{N})$ is not countable. ■

The two diagonal proofs are one. By the correspondence of Section 1.5, $S \mapsto \mathbf{1}_S$ is a bijection $\mathcal{P}(\mathbb{N}) \to \{0,1\}^{\mathbb{N}}$, with inverse $b \mapsto \{n \in \mathbb{N} : b(n) = 1\}$ (Theorem 1.6.4). Given $f\colon \mathbb{N} \to \mathcal{P}(\mathbb{N})$, the sequence $g(n) = 1 - \mathbf{1}_{f(n)}(n)$ of Theorem 3.3.1 is 1 exactly when $n \notin f(n)$, so $g = \mathbf{1}_D$ for the set D of Cantor's proof.

3.3.4 Decimal expansions

The real numbers should be next. A real number in $[0,1)$ is written as a decimal $0.d_1d_2d_3\ldots$, a sequence of digits, so the diagonal suggests itself: list the numbers, write their decimals as the rows of a table, and change the diagonal digits. Two questions must be answered first. What does it **mean** that a sequence of digits is the decimal of x? And what is $0.999\ldots$? School says it equals 1, and a diagonal that produces $0.4999\ldots$ when $0.5000\ldots$ is on the list has produced a number that is on the list.

An infinite sum would answer the first question, but this book has not yet defined one. Finite sums are enough. The first n digits of x should pin x down to within 10^{-n}.

A digit sequence is a decimal of x when each of its finite truncations is within one unit of its last place below x.

Definition 3.3.1. Decimal Expansion

A **digit sequence** is a function $k \mapsto d_k$ from $\mathbb{Z}_{>0}$ to $\{0,1,\ldots,9\}$. For $n \geq 1$ let

$$t_n \coloneqq \sum_{k=1}^{n} d_k 10^{-k}$$

(Definition 2.3.1), where $10^{-k} \coloneqq (1/10)^k$ (Definition 2.3.2). The digit sequence is a **decimal expansion** of $x \in [0,1]$ if **for every** $n \geq 1$,

$$t_n \leq x \leq t_n + 10^{-n}.$$

In words: t_n is the number written with the first n digits, $0.d_1\ldots d_n$, and the condition says that x lies in the closed interval of length 10^{-n} starting at t_n, for every n. The digits are indexed from 1, so that d_k is the digit in the k-th place after the point. No infinite sum appears: every t_n is a finite sum.

Examples.

1. *Zero.* The all-zero sequence has $t_n = 0$, and $0 \leq 0 \leq 10^{-n}$; it is an expansion of 0.

2. *One half, twice.* The sequence $5, 0, 0, \ldots$ has $t_n = \frac{1}{2}$ for every $n \geq 1$, and $\frac{1}{2} \leq \frac{1}{2} \leq \frac{1}{2} + 10^{-n}$. The sequence $4, 9, 9, \ldots$ has $t_n = \frac{4}{10} + \sum_{k=2}^{n} 9 \cdot 10^{-k} = \frac{1}{2} - 10^{-n}$, by Proposition 2.3.6, so $t_n \leq \frac{1}{2} \leq t_n + 10^{-n} = \frac{1}{2}$. Both are expansions of $\frac{1}{2}$.
3. *One.* The all-nine sequence has $t_n = \sum_{k=1}^{n} 9 \cdot 10^{-k} = 1 - 10^{-n}$ (Proposition 2.3.6), so $t_n \leq 1 \leq t_n + 10^{-n} = 1$: it is an expansion of 1.

A non-example by minimal change. Keep the sequence $5, 0, 0, \ldots$ and move x from $\frac{1}{2}$ to 0.51. The inequalities still hold for $n = 1$ ($0.5 \leq 0.51 \leq 0.6$) and for $n = 2$ ($0.50 \leq 0.51 \leq 0.51$), and they fail at $n = 3$: $0.51 > 0.500 + 0.001$. So $5, 0, 0, \ldots$ is not an expansion of 0.51; the clause "for every $n \geq 1$" is what fails.

Why this definition. Both inequalities are non-strict. With a strict right inequality, $x < t_n + 10^{-n}$, the all-nine sequence would be an expansion of no number at all: it would need $x < 1$ together with $1 - 10^{-n} \leq x$ for every n, and no real number satisfies both, by the Archimedean property (a school fact; *Analysis on the Real Line*, Chapter 1 proves it). The non-strict form is what makes $0.999\ldots = 1$ true, and true **by the definition**: the inequalities for $x = 1$ are checked in Example 3, and no other number satisfies them, since $1 - 10^{-n} \leq x \leq 1$ for every n forces $x = 1$, again by the Archimedean property (this is the uniqueness half of (D2) below). Example 2 shows that the price is two expansions for some numbers.

What this book does not prove are the facts that make expansions behave as school says. We state them once and use them in this section and the next, always by name.

(D1) Every $x \in [0, 1)$ has a decimal expansion that does **not** end in all 9s.

(D2) Every digit sequence is a decimal expansion of **exactly one** $x \in [0, 1]$.

(D3) If two **different** digit sequences are expansions of the same x, then one of them ends in all 9s and the other ends in all 0s.

Here a digit sequence **ends in all 9s** if there is $N \geq 1$ with $d_k = 9$ for every $k \geq N$, and likewise for 0s. By the uniqueness in (D2), we may write $x = 0.d_1 d_2 d_3 \ldots$ for "x is the number of which $d_1, d_2, d_3, \ldots$ is an expansion". So $0.4999\ldots = 0.5000\ldots = \frac{1}{2}$, as in (D3).

Neither (D1) nor (D2) follows from what we have so far. (D3) does, by a finite computation at the first place where the two sequences differ (Theorem 2.1.3, Proposition 2.3.6); we state it with the others to quote it by name. The **existence** half of (D2), that some x satisfies all the inequalities at once, is where the completeness of $\mathbb{R}$ hides, and *Analysis on the Real Line*, Chapter 1 takes completeness as an axiom. The **uniqueness** half of (D2) and the "not ending in all 9s" of (D1) rest on the Archimedean property: two numbers x, x' with $|x - x'| \leq 10^{-n}$ for every n must be equal, which *Analysis on the Real Line*, Chapter 1 also proves. Until then we use them as school facts, and each use names the fact it uses.

One consequence is used below. *A digit sequence with no digit* 0 *and no digit* 9 *is the* ***only*** *expansion of its number.* Indeed, by (D3) a second expansion of the same number would force one of the two to end in all 9s and the other in all 0s; the given sequence ends in neither, since it has no 9s and no 0s at all.

3.3.5 The real numbers are uncountable

With the facts in hand, the diagonal runs on digits. Two precautions are built in. Each number on the list gets its expansion by a **rule**, so that no choosing is needed. And the new digits avoid 0 and 9, so that the new number has only one expansion.

Theorem 3.3.4. The Reals Are Uncountable, by Decimals

The interval $[0, 1)$ is uncountable. Hence $\mathbb{R}$ is uncountable.

Idea. Take an arbitrary list of numbers in $[0, 1)$, write each as its expansion with no tail of 9s, and change the n-th digit of the n-th number to 4 or 5. The resulting digit sequence is an expansion of some y, by (D2). If y were the n-th number, it would have two different expansions, one with no 0s or 9s, against (D3).

Proof. Let $f\colon \mathbb{N} \to [0, 1)$ be any function. For $n \geq 1$ let $x_n := f(n-1)$, so that the list $x_1, x_2, x_3, \ldots$ has the same values as f.

For each $n \geq 1$, x_n has an expansion not ending in all 9s, by (D1), and only one: by (D3), two different such expansions would include one ending in all 9s. Let $(d_{n,k})_{k\geq 1}$ be this expansion. It is named by a rule, "the expansion of x_n not ending in all 9s", so no choice is involved. Define a digit sequence by

$$e_n := \begin{cases} 5 & \text{if } d_{n,n} \neq 5, \\ 4 & \text{if } d_{n,n} = 5, \end{cases} \qquad (n \geq 1).$$

Then $e_n \neq d_{n,n}$ for every $n \geq 1$. By (D2), there is $y \in [0, 1]$ of which $(e_k)_{k\geq 1}$ is an expansion. Its first truncation is $t_1 = e_1/10 \in \{0.4, 0.5\}$, so $0.4 \leq t_1 \leq y \leq t_1 + 0.1 \leq 0.6$, and in particular $y \in [0, 1)$.

Let $n \geq 1$, and suppose $y = x_n$. Then (e_k) and $(d_{n,k})$ are both expansions of y, and they are different, since they differ in place n. But (e_k) has no digit 0 and no digit 9, so by the consequence of (D3) stated above it is the **only** expansion of y, a contradiction. So $y \neq x_n$ for every $n \geq 1$, and y is not a value of f. Since f was arbitrary, no function $\mathbb{N} \to [0, 1)$ is surjective; and $[0, 1)$ is non-empty, since it contains 0. By Definition 3.1.1, $[0, 1)$ is not countable.

Finally, if $\mathbb{R}$ were countable, its subset $[0, 1)$ would be countable by Proposition 3.1.3. So $\mathbb{R}$ is uncountable.

■

Why the digits 4 and 5. The first rule that comes to mind is $e_n := 9 - d_{n,n}$, which also changes every diagonal digit. Run it on the list $x_1 = \frac{1}{2}$, $x_n = 0$ for $n \geq 2$ (that is, $f(0) = \frac{1}{2}$ and $f(n) = 0$ for $n \geq 1$). The expansions are $0.5000\ldots$ and $0.000\ldots$, so $d_{1,1} = 5$ and $d_{n,n} = 0$ for $n \geq 2$. The naive rule produces $e_1 = 4$ and $e_n = 9$ for $n \geq 2$: the sequence $0.4999\ldots$, which is an expansion of $\frac{1}{2} = x_1$ by Example 2. The new digit sequence differs from every row, and its number is on the list. The rule with 4 and 5, on the same list, gives $0.4555\ldots = \frac{41}{90}$, which is on no row. Avoiding 0 and 9 is exactly what the last paragraph of the proof uses.

Analysis on the Real Line, Chapter 1 proves that $\mathbb{R}$ is uncountable again, with no decimals at all, directly from its least upper bound axiom; that proof needs none of (D1)–(D3).

3.3.6 Transcendental numbers

A real number that is not algebraic is called **transcendental**. Section 3.2 showed that the set Alg of algebraic numbers is countable (Theorem 3.2.4).

Corollary 3.3.5. Transcendental Numbers Exist

The set $\mathbb{R} \setminus \text{Alg}$ of transcendental numbers is uncountable. In particular, there is a real number that is not algebraic.

Proof. By excluded middle (Logic and Proof, Proposition 2.5.3), every real number is in Alg or not, so $\mathbb{R} = \text{Alg} \cup (\mathbb{R} \setminus \text{Alg})$. Suppose $\mathbb{R} \setminus \text{Alg}$ is countable. Since Alg is countable by Theorem 3.2.4, $\mathbb{R}$ is countable by Proposition 3.1.5, contradicting Theorem 3.3.4. So $\mathbb{R} \setminus \text{Alg}$ is uncountable. In particular $\mathbb{R} \setminus \text{Alg} \neq \emptyset$, since $\emptyset$ is countable (Definition 3.1.1). So not every x satisfies $x \notin \mathbb{R} \setminus \text{Alg}$: otherwise $\mathbb{R} \setminus \text{Alg}$ would be an empty set (Definition 1.2.4), hence equal to $\emptyset$ (Proposition 1.2.3). By the classical law Logic and Proof, Proposition 6.2.1 (a) and $\neg\neg$E, some x lies in $\mathbb{R} \setminus \text{Alg}$; this x is a real number that is not algebraic. This last passage, from "not empty" to "has an element", is a classical step (*Logic and Proof*, Section 8.7). ■

Remark. The proof names no transcendental number: it shows that the set of them is too large to be countable, hence not empty. Its classical steps are the split of $\mathbb{R}$ into Alg and its complement (excluded middle) and the last one, from "not empty" to "has an element". Compare the classical proof of Logic and Proof, Theorem 8.7.1 in *Logic and Proof*, Section 8.7, which also names no witness (unlike Logic and Proof, Proposition 8.7.2, which does). Proving that a particular number, such as π, is transcendental is a different and much harder matter.

3.3.7 Exercises

3.3.7.1 A. Check your understanding

Exercise. A1

These parts are about the proof of Theorem 3.3.2.

(a) Where in the proof is the surjectivity of f used, and what does it supply?

(b) Run the proof on $X = \{1, 2, 3\}$ and $f(1) = \{1, 2\}$, $f(2) = \emptyset$, $f(3) = \{1, 3\}$. What is D? Is D a value of f?

(c) State the idea of the proof in two sentences.

(d) Why does the same argument not show that there is no surjection $X \to X$?

Solution.

(a) It is used once, right after D is defined: surjectivity supplies an element $d \in X$ with

$f(d) = D$. The two cases $d \in D$ and $d \notin D$ are then both refuted. Everything before that line holds for every function f.

(b) Test each x against $f(x)$: $1 \in f(1)$, so $1 \notin D$; $2 \notin f(2) = \emptyset$, so $2 \in D$; $3 \in f(3)$, so $3 \notin D$. Hence $D = \{2\}$. It is not a value of f: the values are $\{1, 2\}$, $\emptyset$, $\{1, 3\}$, and D differs from $f(x)$ about x in each case ($1 \in f(1) \setminus D$, $2 \in D \setminus f(2)$, $3 \in f(3) \setminus D$).

(c) Build the set D of those x that are not in their own image $f(x)$. Then D disagrees with every $f(x)$ about the element x, so it is not a value of f.

(d) The set D is a **subset** of X, so it is a candidate value only for a function into $\mathcal{P}(X)$. For $f\colon X \to X$, the argument (where the test $x \in f(x)$ makes sense at all) shows that D is not a value of f, but D need not be an element of X, so nothing contradicts surjectivity. Indeed id_X is a surjection $X \to X$; with $f = \mathrm{id}_X$ the argument is Russell's, and shows only that $D = R_X$ is not an element of X (Theorem 1.2.4).

3.3.7.2 B. Practice

Exercise. B1: A faded diagonal

Let $\mathbb{N}^{\mathbb{N}}$ be the set of all functions $\mathbb{N} \to \mathbb{N}$. Here is a proof that $\mathbb{N}^{\mathbb{N}}$ is uncountable, with its last step left blank. *Name the move, then complete it.*

> Let $f\colon \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$ be any function, and write $f_n := f(n)$, so that $f_0, f_1, f_2, \ldots$ is a list of elements of $\mathbb{N}^{\mathbb{N}}$. Define $g\colon \mathbb{N} \to \mathbb{N}$ by $g(n) := f_n(n) + 1$. (Last step: _____.) Since f was arbitrary, no function $\mathbb{N} \to \mathbb{N}^{\mathbb{N}}$ is surjective, and as $\mathbb{N}^{\mathbb{N}}$ is non-empty (it contains the zero function), $\mathbb{N}^{\mathbb{N}}$ is not countable.

Solution. The move is **the diagonal**: g is built to disagree with the list's n-th entry in place n. The last step: for every $n \in \mathbb{N}$, $g(n) = f_n(n) + 1 \neq f_n(n)$, so $g \neq f_n$ by Proposition 1.5.1 (two equal functions agree at n). Hence g is not on the list: g is an element of $\mathbb{N}^{\mathbb{N}}$ (its values $f_n(n) + 1$ are natural numbers) that is not a value of f, and f is not surjective.

Exercise. B2

Prove that the set of **infinite** subsets of $\mathbb{N}$ is uncountable.

Solution. Let $\mathcal{F}$ be the set of finite subsets of $\mathbb{N}$ and $\mathcal{I}$ the set of infinite ones, both subsets of $\mathcal{P}(\mathbb{N})$ defined by specification. By excluded middle (Logic and Proof, Proposition 2.5.3), every subset of $\mathbb{N}$ is finite or not finite, that is, finite or infinite (Definition 2.5.3), so $\mathcal{P}(\mathbb{N}) = \mathcal{F} \cup \mathcal{I}$. The set $\mathcal{F}$ is countable by Exercise (C1: Finite subsets of the natural numbers). If $\mathcal{I}$ were countable, $\mathcal{P}(\mathbb{N})$ would be countable by Proposition 3.1.5, contradicting Corollary 3.3.3. So $\mathcal{I}$ is uncountable.

Exercise. B3: Expansions of three numbers

For each of $x = \frac{1}{3}, \frac{1}{2}, 1$, find **all** decimal expansions of x, checking the inequalities of Definition 3.3.1 for each one you give, and say which of (D1)–(D3) each case illustrates.

Solution. We use Proposition 2.3.6 with $r = \frac{1}{10}$, after taking the constant factor $\frac{1}{10}$ out of the sum: $\sum_{k=1}^{n} 10^{-k} = \frac{1}{10}\sum_{k=1}^{n}(\frac{1}{10})^{k-1} = \frac{1}{10} \cdot \frac{1-10^{-n}}{9/10} = \frac{1}{9}(1-10^{-n})$.

$x = \frac{1}{3}$. The all-three sequence has $t_n = \frac{3}{9}(1-10^{-n}) = \frac{1}{3} - \frac{1}{3}10^{-n}$, so $t_n \le \frac{1}{3} \le t_n + 10^{-n}$. It is an expansion, and it does not end in all 9s, as (D1) promises. It ends in neither 9s nor 0s, so by (D3) no other expansion of $\frac{1}{3}$ exists. Answer: $0.333\ldots$ only.

$x = \frac{1}{2}$. Example 2 after Definition 3.3.1 checks that $0.5000\ldots$ and $0.4999\ldots$ are expansions. There are no others: if three different expansions existed, two of them would both end in all 9s or both not; but by (D3), of two different expansions of one number, one ends in all 9s and the other in all 0s, and a sequence ending in all 0s does not end in all 9s (from some place on, its digits would be both 0 and 9). Answer: exactly these two, which illustrate (D3); the first is the one (D1) promises.

$x = 1$. The all-nine sequence is an expansion (Example 3). Conversely, let (d_k) be an expansion of 1, and suppose $d_m \le 8$ for some m. Since every digit is at most 9, $t_m \le \sum_{k=1}^{m} 9 \cdot 10^{-k} - 10^{-m} = 1 - 2 \cdot 10^{-m}$, so $t_m + 10^{-m} \le 1 - 10^{-m} < 1$, against the definition. So every digit is 9. Answer: $0.999\ldots$ only. The all-nine sequence is an expansion of 1, an instance of the existence half of (D2). Here (D3) has no second expansion to compare. The case also shows why (D1) is stated for $[0, 1)$ only: the one expansion of 1 ends in all 9s.

Exercise. B4: Prove or disprove

Prove each true statement, and show each false one false.

(a) The set of periodic 0–1 sequences, those $a \in \{0,1\}^{\mathbb{N}}$ with some $p \ge 1$ such that $a(n+p) = a(n)$ for every $n \in \mathbb{N}$, is uncountable.

(b) The set of 0–1 sequences with no two consecutive 1s is uncountable.

(c) For every set X there is no injection $\mathcal{P}(X) \to X$.

(d) If X is infinite, there is no surjection $X \to X \times X$.

(e) The set of all functions $\mathbb{Z} \to \{0,1\}$ is uncountable.

Solution.

(a) **False:** the set is countable. For $p \in \mathbb{Z}_{>0}$ let P_p be the set of sequences a with $a(n+p) = a(n)$ for every $n \in \mathbb{N}$. For $a \in P_p$, $a(qp+r) = a(r)$ for all $q \in \mathbb{N}$ and $0 \le r < p$, by induction on q. Every $n \in \mathbb{N}$ is $qp + r$ for such q and r (Theorem 2.2.3; $q \ge 0$ since $n \ge 0$ and $r < p$). So a is determined by $a(0), \ldots, a(p-1)$, and $a \mapsto a|_{\{0,\ldots,p-1\}}$ is an injection of P_p into the set of functions $\{0,\ldots,p-1\} \to \{0,1\}$, which is finite, with 2^p elements (Proposition 2.5.8, through indicator functions). A finite set injects into $\mathbb{N}$ (Theorem 3.1.2, (iii) $\Rightarrow$ (ii)); composing, P_p injects into $\mathbb{N}$, so P_p is countable ((ii) $\Rightarrow$ (i)). The set of periodic sequences is $\bigcup_{p \in \mathbb{Z}_{>0}} P_p$, countable by Theorem 3.2.3 (b), since $\mathbb{Z}_{>0} \subseteq \mathbb{N}$ is countable (Proposition 3.1.3). Choice is not needed here, although the proof of the cited theorem uses Axiom 3.2.1 in general: the lists are given by a formula. Let $w_{p,k}$ $(k < 2^p)$ be the k-th pattern $\{0,\ldots,p-1\} \to \{0,1\}$ in binary

order, put $w_{p,k} \coloneqq w_{p,2^p-1}$ for $k \geq 2^p$, and let $L(p,k)$ be the sequence $n \mapsto w_{p,k}(r)$, r the remainder of n on division by p. Then L maps $\mathbb{Z}_{>0} \times \mathbb{N}$ onto the set of periodic sequences, and composing it with a surjection $\mathbb{N} \to \mathbb{Z}_{>0} \times \mathbb{N}$, as in Example (Unions that come with their lists), lists them without Axiom 3.2.1. The diagonal fails here because the flipped diagonal of a list of periodic sequences need not be periodic: the first usual failure of Example (Method: the diagonal).

(b) **True.** Send $b \in \{0,1\}^{\mathbb{N}}$ to the sequence a with $a(2n) \coloneqq b(n)$ and $a(2n+1) \coloneqq 0$. Every odd place of a is 0, and of two consecutive places one is odd, so a has no two consecutive 1s. The map is injective, since b is read back from the even places (Proposition 1.5.1). If the set were countable, composing with an injection of it into $\mathbb{N}$ (Theorem 3.1.2, (i) $\Rightarrow$ (ii)) would give an injection $\{0,1\}^{\mathbb{N}} \to \mathbb{N}$, so $\{0,1\}^{\mathbb{N}}$ would be countable ((ii) $\Rightarrow$ (i)), against Theorem 3.3.1.

(c) **True.** Let $i\colon \mathcal{P}(X) \to X$ be injective. Since $\emptyset \in \mathcal{P}(X)$, the domain is non-empty, so i has a left inverse $r\colon X \to \mathcal{P}(X)$ (Theorem 1.6.1 (b)). The equation $r \circ i = \mathrm{id}_{\mathcal{P}(X)}$ says that i is a right inverse of r, so r is surjective (Proposition 1.6.2), against Theorem 3.3.2.

(d) **False.** Take $X = \mathbb{N}$. The set $\mathbb{N} \times \mathbb{N}$ is countable (Theorem 3.1.6) and non-empty, so Definition 3.1.1 gives a surjection $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$.

(e) **True.** Restriction $a \mapsto a|_{\mathbb{N}}$ maps $\{0,1\}^{\mathbb{Z}}$ onto $\{0,1\}^{\mathbb{N}}$: a given $b \in \{0,1\}^{\mathbb{N}}$ is the restriction of its extension by 0 on the negative integers. If $\{0,1\}^{\mathbb{Z}}$ were countable, its image $\{0,1\}^{\mathbb{N}}$ would be countable (Proposition 3.1.4), against Theorem 3.3.1.

3.3.7.3 C. Going deeper

Exercise. C1: Exit check: Cantor

Prove Theorem 3.3.2: for every set X, there is no surjection $X \to \mathcal{P}(X)$. Deduce that $\mathcal{P}(\mathbb{N})$ is uncountable.

Solution. Let $f\colon X \to \mathcal{P}(X)$ be a function, and let $D \coloneqq \{x \in X : x \notin f(x)\}$, a subset of X, so $D \in \mathcal{P}(X)$. Suppose f is surjective. Then $D = f(d)$ for some $d \in X$. If $d \in D$, then $d \notin f(d) = D$ by the definition of D, a contradiction; so $d \notin D$. But then $d \notin f(d)$ and $d \in X$, so $d \in D$ by the definition of D, a contradiction. Hence f is not surjective, and since f was arbitrary, no surjection $X \to \mathcal{P}(X)$ exists.

For $X = \mathbb{N}$: by Definition 3.1.1, $\mathcal{P}(\mathbb{N})$ is countable only if it is empty or there is a surjection $\mathbb{N} \to \mathcal{P}(\mathbb{N})$. It is not empty, since $\emptyset \in \mathcal{P}(\mathbb{N})$, and the theorem excludes the surjection. So $\mathcal{P}(\mathbb{N})$ is uncountable.

Marking scheme. (10 points) - 2: takes an arbitrary $f\colon X \to \mathcal{P}(X)$ and either assumes it onto, towards a contradiction, or sets out to show that it misses a set. - 3: defines $D = \{x \in X : x \notin f(x)\}$ and notes that it is a subset of X. - 2: uses surjectivity to obtain d with $f(d) = D$ (or, in the direct form, fixes an arbitrary x). - 2: refutes both cases, $d \in D$ and $d \notin D$ (or shows that D and $f(x)$ disagree about x). - 1: the deduction for $\mathcal{P}(\mathbb{N})$, handling both clauses of "countable": non-empty, and no surjection from $\mathbb{N}$. The direct form ("$D \neq f(x)$ for every x, since they disagree about x") earns the same points: 2 for the arbitrary f, 3 for D, 4 for the disagreement at every x, 1 for the deduction. Fatal errors (0 for the step): $D = \{x \in X : x \in f(x)\}$ (it may well be a value of f); checking the claim for one particular f and concluding for all, as in (N1) of Logic and Proof, Example (What is not allowed) (0 for the first step).

Exercise. C2: Permutations of the naturals

Prove that the set of all bijections $\mathbb{N} \to \mathbb{N}$ is uncountable.

Solution (Hint 1). *Consider the bijections that only swap* $2n$ *and* $2n+1$*, for some of the* $n \in \mathbb{N}$*, and fix every other number.*

Solution (Hint 2). *Such bijections correspond to* $\{0,1\}^{\mathbb{N}}$*: the* n*-th entry says whether the pair* $2n, 2n+1$ *is swapped.*

Solution. Every $m \in \mathbb{N}$ is $2q + r$ for exactly one pair (q, r) with $q \in \mathbb{N}$ and $r \in \{0,1\}$ (Theorem 2.2.3 with divisor 2, the quotient lying in $\mathbb{N}$ as in the proof of Proposition 3.1.5). For $b \in \{0,1\}^{\mathbb{N}}$ define $\pi_b \colon \mathbb{N} \to \mathbb{N}$ by

$$\pi_b(2q+r) \coloneqq \begin{cases} 2q+r & \text{if } b(q) = 0, \\ 2q+1-r & \text{if } b(q) = 1, \end{cases}$$

so π_b swaps $2q$ and $2q+1$ when $b(q) = 1$ and fixes them otherwise. It maps each pair $\{2q, 2q+1\}$ to itself, and applying it twice returns every number to its place, so $\pi_b \circ \pi_b = \mathrm{id}_{\mathbb{N}}$, and π_b is a bijection by Theorem 1.6.4.

Let B be the set of bijections $\mathbb{N} \to \mathbb{N}$; it is non-empty, since $\mathrm{id}_{\mathbb{N}} \in B$. Let $f \colon \mathbb{N} \to B$ be any function, and write $f_n \coloneqq f(n)$. Define $b \in \{0,1\}^{\mathbb{N}}$ by $b(n) \coloneqq 1$ if $f_n(2n) = 2n$, and $b(n) \coloneqq 0$ otherwise, and let $\pi \coloneqq \pi_b \in B$. For every $n \in \mathbb{N}$, $\pi(2n) \neq f_n(2n)$: if $f_n(2n) = 2n$, then $b(n) = 1$ and $\pi(2n) = 2n+1$; if $f_n(2n) \neq 2n$, then $b(n) = 0$ and $\pi(2n) = 2n$. So $\pi \neq f_n$ for every n (Proposition 1.5.1), and f is not surjective. Since f was arbitrary and $B \neq \emptyset$, B is uncountable (Definition 3.1.1).

This is the diagonal again, with the n-th entry tested at the place $2n$. Alternatively, $b \mapsto \pi_b$ is an injection $\{0,1\}^{\mathbb{N}} \to B$, since $\pi_b(2q)$ is $2q$ or $2q+1$ according to $b(q)$; if B were countable, composing with an injection $B \to \mathbb{N}$ (Theorem 3.1.2) would make $\{0,1\}^{\mathbb{N}}$ countable, against Theorem 3.3.1.

Marking scheme. (10 points) - 3: defines, for each $b \in \{0,1\}^{\mathbb{N}}$ (or each set of pairs), the bijection that swaps $2n$ and $2n+1$ exactly when $b(n) = 1$, and proves it is a bijection. - 4: given an arbitrary list of bijections, defines b from the n-th entry's value at a place belonging to the n-th pair, and shows that the resulting bijection differs from the n-th entry; or shows that $b \mapsto \pi_b$ is injective. - 3: concludes, with the non-emptiness of the set of bijections or through Theorem 3.3.1 and the closure properties of countable sets. Fatal errors (0 for the step): the plain diagonal $g(n) \coloneqq f_n(n) + 1$, which is not a bijection; a "bijection" that moves numbers between different pairs without checking that it stays one-to-one and onto.

3.4 Comparing Sizes: the Schröder–Bernstein Theorem

We have $(0,1) \subseteq [0,1] \subseteq \mathbb{R}$. Are the three sets the same size? Section 2.5 made "same size" mean "there is a bijection", and for these sets a bijection is fiddly to write down: $[0,1]$ has two endpoints that $(0,1)$ lacks, and $\mathbb{R}$ is unbounded. An **injection**, on the other hand, is easy in both directions: the inclusion goes one way, and squeezing $[0,1]$ into the middle of $(0,1)$ goes the other. This section turns injections into a way of comparing sizes, and proves the theorem that makes the comparison useful: injections both ways give a bijection.

3.4.1 Comparing sizes with injections

An injection $A \to B$ places a copy of A inside B: distinct elements of A go to distinct elements of B, so B has room for all of A. For finite sets this is the pigeonhole principle read the other way round (Corollary 2.5.3). It deserves a name for all sets.

A is at most as big as B when A fits into B without collisions.

Definition 3.4.1. Comparing Sizes

Let A and B be sets. We write $|A| \leq |B|$, and say that A **is at most as big as** B, if **there exists** an injection $A \to B$. We write $|A| < |B|$, and say that A **is strictly smaller than** B, if $|A| \leq |B|$ and **not** $|A| = |B|$: there is an injection $A \to B$, and there is **no** bijection $A \to B$.

In words: "$\leq$" asks for one injection, of our choosing. "$<$" asks for an injection **and** rules out every bijection, which is a statement about all functions $A \to B$ at once. As with $|A| = |B|$ in Section 2.5 (Definition 2.5.1), the symbols $|A| \leq |B|$ and $|A| < |B|$ are **relations between the sets** A and B. No object $|A|$ is defined for an infinite set, and nothing here compares two numbers.

Examples.

- *Subsets.* If $A \subseteq B$, the inclusion $a \mapsto a$ is an injection $A \to B$, so $|A| \leq |B|$. In particular $|(0,1)| \leq |[0,1]| \leq |\mathbb{R}|$.
- *The degenerate case.* For every set B, $|\emptyset| \leq |B|$: the empty function $\emptyset \to B$ (Proposition 1.5.2 (a)) is injective, vacuously, since there are no $x_1, x_2 \in \emptyset$ to test.
- *Finite sets.* Let A have m elements and B have n elements (Definition 2.5.2). Then $|A| \leq |B|$ exactly when $m \leq n$. If $m \leq n$, take bijections $\varphi\colon \{1,\dots,m\} \to A$ and $\psi\colon \{1,\dots,n\} \to B$; the inclusion $\iota\colon \{1,\dots,m\} \to \{1,\dots,n\}$ is injective, so $\psi \circ \iota \circ \varphi^{-1}\colon A \to B$ is injective by Theorem 1.5.4 (a), φ^{-1} being a bijection (Theorem 1.6.4). If $m > n$, there is no injection $A \to B$ by Corollary 2.5.3 (a). So the relation agrees with the count of elements, which is why it is allowed to borrow the symbol $\leq$.
- *Countable sets.* By Theorem 3.1.2, (i) $\iff$ (ii), a set A is countable if and only if $|A| \leq |\mathbb{N}|$. "Countable" means "at most as big as $\mathbb{N}$".
- *Power sets.* For every set X, $|X| < |\mathcal{P}(X)|$. The map $x \mapsto \{x\}$ is an injection $X \to \mathcal{P}(X)$, since $\{x_1\} = \{x_2\}$ gives $x_1 \in \{x_2\}$, so $x_1 = x_2$. And there is no bijection $X \to \mathcal{P}(X)$, because by Theorem 3.3.2 there is not even a surjection. In particular $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$.

Non-example by minimal change. Replace "injection" by "function" in the definition. Then any set would be "at most as big as" any non-empty set, by a constant map: $\mathbb{R} \to \{0\}$ would

put $\mathbb{R}$ below a one-element set. The clause that carries the meaning is "no two elements collide".

Warning. $|A| < |B|$ does **not** mean "there is an injection $A \to B$ that is not a bijection". The map $n \mapsto n+1$ is an injection $\mathbb{N} \to \mathbb{N}$ that misses 0, and yet $|\mathbb{N}| = |\mathbb{N}|$. For infinite sets one injection that fails to be onto proves nothing about strictness; $|A| < |B|$ needs **every** map $A \to B$ to fail to be a bijection, which is why Cantor's theorem, a statement about every $f\colon X \to \mathcal{P}(X)$, is the source of our strict inequalities.

The relation behaves like an order in two of the three ways. The third is the content of this section's theorem.

Proposition 3.4.1. Comparing Sizes Is Reflexive and Transitive

For all sets A, B, C:

(a) $|A| \leq |A|$;
(b) if $|A| \leq |B|$ and $|B| \leq |C|$, then $|A| \leq |C|$.

Proof.

(a) The identity id_A is injective, since $\mathrm{id}_A(x_1) = \mathrm{id}_A(x_2)$ says $x_1 = x_2$.
(b) Let $f\colon A \to B$ and $g\colon B \to C$ be injections. Then $g \circ f\colon A \to C$ is injective by Theorem 1.5.4 (a). This proves the proposition.

■

As with equinumerosity (Section 2.5, after Proposition 2.5.1), comparing sizes is reflexive and transitive (Proposition 3.4.1), but we do not call it an order: there is no set of all sets for it to be a relation on (Theorem 1.2.4). And the clause one would expect next, the analogue of $x \leq y \leq x \Rightarrow x = y$ for numbers, would say "if $|A| \leq |B|$ and $|B| \leq |A|$, then $A = B$", which is false: $|\mathbb{N}| \leq |2\mathbb{N}|$ and $|2\mathbb{N}| \leq |\mathbb{N}|$, while $2\mathbb{N} \neq \mathbb{N}$. The right replacement for "$A = B$" is "$|A| = |B|$". That is the Schröder–Bernstein Theorem below.

Before it, one more way to read $\leq$. A countable set was defined by a surjection from $\mathbb{N}$, and Theorem 3.1.2 turned that into an injection into $\mathbb{N}$. The same exchange works for all sets, with one exception and one price.

Proposition 3.4.2. Injections and Surjections

Let A and B be sets with $A \neq \emptyset$. Then $|A| \leq |B|$ if and only if there is a surjection $B \to A$.

Proof. ($\Rightarrow$) Let $f\colon A \to B$ be an injection. Since $A \neq \emptyset$, Theorem 1.6.1 (b) gives a left inverse $g\colon B \to A$, so $g \circ f = \mathrm{id}_A$. This says that f is a right inverse of g (Definition 1.6.1), so g is surjective by Proposition 1.6.2.

($\Leftarrow$) Let $g\colon B \to A$ be a surjection. By Theorem 3.2.2, g has a right inverse $h\colon A \to B$, so $g \circ h = \mathrm{id}_A$; **this step uses Axiom 3.2.1**, through Theorem 3.2.2. Then g is a left inverse of h, so h is injective by Theorem 1.6.1 (a). Hence $|A| \leq |B|$. This proves the proposition.

■

The hypothesis $A \neq \emptyset$ is needed for ($\Rightarrow$) only. For $A = \emptyset$ and $B = \{b\}$, the empty function is an injection $\emptyset \to \{b\}$, but there is no function $\{b\} \to \emptyset$ at all (Proposition 1.5.2 (b)), let alone a surjection. The proof shows where the hypothesis enters: a left inverse $g\colon B \to A$ must send b somewhere in A. The choice in ($\Leftarrow$) is genuine in general, but not for $B = \mathbb{N}$: a surjection from $\mathbb{N}$ has least preimages, a rule, which is how Theorem 3.1.2 went from (i) to (ii) without the axiom.

Quick check. Is $\left|\{0,1\}^{\mathbb{N}}\right| \leq |\mathcal{P}(\mathbb{N})|$? Give an injection, and say whether your answer needed Proposition 3.4.2.

Solution. Yes. Send a sequence $a \in \{0,1\}^{\mathbb{N}}$ to the set $\{n \in \mathbb{N} : a(n) = 1\}$. If two sequences give the same set, they take the value 1 at the same places, and so the value 0 at the same places too; hence they are equal (Proposition 1.5.1), and the map is injective. No appeal to Proposition 3.4.2 is needed: the definition asks for an injection, and we wrote one down. (The map is in fact a bijection, with inverse $S \mapsto \mathbf{1}_S$; this is the correspondence of Section 1.5, recalled after Corollary 3.3.3.)

3.4.2 The Schröder–Bernstein Theorem

Here is the replacement for antisymmetry. To show two sets are the same size, it is enough to fit each into the other.

Theorem 3.4.3. Schröder–Bernstein Theorem

Let A and B be sets. If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

Idea. Let $f\colon A \to B$ and $g\colon B \to A$ be the two injections. We want a bijection $h\colon A \to B$, and at each $a \in A$ there are two candidates: go forward, $h(a) = f(a)$, or go back along g: let $h(a)$ be the unique b with $g(b) = a$. Going back is possible only for $a \in g(B)$. So a point of A **not hit by** g must be sent forward by f. Then the point $f(a) \in B$ is used up, and $g(f(a))$ must not go back to it, or h would collide; so $g(f(a))$ must also be sent forward, and then $g(f(g(f(a))))$, and so on along the chain. Everything reached this way goes forward; everything else goes back.

Step roadmap.

① Build the set $C \subseteq A$ of points that are forced forward: $C_0 := A \setminus g(B)$, $C_{n+1} := g(f(C_n))$, $C := \bigcup_{n\in\mathbb{N}} C_n$.

② Define $h(a) := f(a)$ on C, and let $h(a)$ be the unique b with $g(b) = a$ off C.

③ Show h is injective; the only case with content is one point of each kind.

④ Show h is onto: for $b \in B$, look at $g(b)$ and ask whether it lies in C.

Before reading on: in step ④, why is $g(b) \notin C_0$, and what does that buy?

Proof. Let $f\colon A \to B$ and $g\colon B \to A$ be injections.

Step 1. By Theorem 2.3.1, applied with the set $\mathcal{P}(A)$, the starting value $A \setminus g(B) \in \mathcal{P}(A)$ and the function $(n, S) \mapsto g(f(S))$ from $\mathbb{N} \times \mathcal{P}(A)$ to $\mathcal{P}(A)$, there are sets $C_n \subseteq A$, for $n \in \mathbb{N}$, with

$$C_0 = A \setminus g(B), \qquad C_{n+1} = g(f(C_n)) \quad \text{for every } n \in \mathbb{N}.$$

Here $f(C_n) \subseteq B$ and $g(f(C_n)) \subseteq A$ are images (Definition 1.7.1). Let $C \coloneqq \bigcup_{n\in\mathbb{N}} C_n \subseteq A$ (Definition 1.3.4). Two facts about C will be used.

(F1) If $a \in C$, then $g(f(a)) \in C$. Indeed $a \in C_n$ for some $n \in \mathbb{N}$; then $f(a) \in f(C_n)$, so $g(f(a)) \in g(f(C_n)) = C_{n+1} \subseteq C$.

(F2) If $a \in A \setminus C$, there is **exactly one** $b \in B$ with $g(b) = a$. It exists because $a \notin C_0 = A \setminus g(B)$ and $a \in A$, so $a \in g(B)$. It is unique because g is injective.

Step 2. Define $h\colon A \to B$ by

$$h(a) \coloneqq \begin{cases} f(a) & \text{if } a \in C, \\ \text{the unique } b \in B \text{ with } g(b) = a & \text{if } a \notin C. \end{cases}$$

Each $a \in A$ falls under exactly one case, and in each case the value exists and is unique (in the second case by (F2)), so h is a function. Note that $g(h(a)) = a$ whenever $a \notin C$.

Step 3.

Claim. h is injective.

Proof of Claim. Let $a, a' \in A$ with $h(a) = h(a')$.

Case 1: $a, a' \in C$. Then $f(a) = f(a')$, and $a = a'$ because f is injective.

Case 2: $a, a' \notin C$. Then $a = g(h(a)) = g(h(a')) = a'$.

Case 3: $a \in C$ *and* $a' \notin C$. Then $h(a') = h(a) = f(a)$, so $a' = g(h(a')) = g(f(a))$. By (F1), $g(f(a)) \in C$, so $a' \in C$, a contradiction. So this case does not occur.

The case $a \notin C$, $a' \in C$ is Case 3 with the roles of a and a' swapped. Hence $a = a'$ in every case that occurs.

■

Step 4.

Claim. h is surjective.

Proof of Claim. Let $b \in B$, and consider $g(b) \in A$.

Case 1: $g(b) \notin C$. Then $h(g(b))$ is the unique element of B whose image under g is $g(b)$, and b is such an element. So $h(g(b)) = b$.

Case 2: $g(b) \in C$. Then $g(b) \in C_n$ for some $n \in \mathbb{N}$. Since $g(b) \in g(B)$, we have $g(b) \notin A \setminus g(B) = C_0$, so $n \neq 0$. By Lemma 2.1.1 (c), $k \coloneqq n - 1 \in \mathbb{N}$, and $g(b) \in C_{k+1} = g(f(C_k))$.

By Definition 1.7.1 there is $b' \in f(C_k)$ with $g(b') = g(b)$, and then $a \in C_k$ with $f(a) = b'$. As g is injective, $b = b' = f(a)$. Since $a \in C_k \subseteq C$, $h(a) = f(a) = b$.

In both cases b is a value of h.

■

By the two claims, $h\colon A \to B$ is a bijection, so $|A| = |B|$. This proves the theorem.

■

The answer to the prompt: $g(b)$ is a value of g, and C_0 consists exactly of the points of A that are **not** values of g. That is what pushes the index n of Case 2 up to at least 1, so that $g(b)$ has a predecessor $a \in C_{n-1}$ in its chain, and b is reached by f from that predecessor.

Every value of h is given by a rule, so the proof makes **no use of Axiom 3.2.1**: Step 1 is a recursion with an explicit step, and Step 2 picks the unique preimage, where there is nothing to choose. The case split "$a \in C$ or $a \notin C$" is an instance of excluded middle, the classical step discussed in *Logic and Proof*, Section 8.7; nothing in the proof decides which case holds for a given a, and nothing needs to.

Each hypothesis is used. Without the injection g, the conclusion fails: $\mathbb{N} \to \mathcal{P}(\mathbb{N})$, $n \mapsto \{n\}$, is an injection, and $|\mathbb{N}| \neq |\mathcal{P}(\mathbb{N})|$ by Theorem 3.3.2. In the proof, injectivity of f is used once, in Case 1 of Step 3, and injectivity of g twice, in (F2) and in Case 2 of Step 4.

In practice the theorem is used as a method.

Example. Method: injections both ways

Template. To show $|A| = |B|$, write an injection $f\colon A \to B$ and an injection $g\colon B \to A$, check each one separately, and cite Theorem 3.4.3. Often one map is an inclusion and the other squeezes B into a part of A. Do not hunt for the bijection: the theorem builds it.

When to use it. A and B differ by "a little" (endpoints, a countable piece, a factor), so that a bijection would need cases; or A sits inside B, and B fits back into A.

The usual failure. Two injections in the same direction. One injection that is not onto, read as strictness or as a bijection (the warnings after Definition 3.4.1 and after Example (The real line and its intervals)). A squeeze whose values leave the target: $x \mapsto x/2$ sends $[0,1]$ into $[0, \frac{1}{2}]$ and hits $0 \notin (0,1)$.

Quick check. Show $|[0,1] \cup \{5\}| = |[0,1]|$ by the method.

Solution. The inclusion $[0,1] \to [0,1] \cup \{5\}$ is injective. In the other direction, send $x \in [0,1]$ to $x/2$ and 5 to 1. Since $5 \notin [0,1]$, the two clauses define a function into $[0,1]$. It is injective: two points of $[0,1]$ with $x/2 = y/2$ are equal, and the image $x/2$ of a point of $[0,1]$ is never 1, the image of 5, since $x/2 \leq \frac{1}{2} < 1$. By Theorem 3.4.3 the sets are equinumerous.

3.4.3 Intervals of real numbers

The theorem's first use is the question of the opening frame.

Example. The closed and the open unit interval

Show that $|[0,1]| = |(0,1)|$: first with Theorem 3.4.3, then by writing down a bijection.

Solution. With the theorem. Planned as in Example (Method: injections both ways):

Givens	Goal
$(0,1) \subseteq [0,1]$	$\lvert[0,1]\rvert = \lvert(0,1)\rvert$
the inclusion $(0,1) \to [0,1]$, injective	an injection $[0,1] \to (0,1)$
gap: squeeze $[0,1]$ into a closed interval inside $(0,1)$	$u(x) \coloneqq x/2 + 1/4$, with values in $[\frac{1}{4}, \frac{3}{4}]$

The inclusion $(0,1) \to [0,1]$ is an injection. In the other direction let $u(x) \coloneqq x/2 + 1/4$ for $x \in [0,1]$. If $0 \le x \le 1$, then $1/4 \le u(x) \le 3/4$, so $u(x) \in (0,1)$, and u is a function $[0,1] \to (0,1)$. It is injective: $x/2 + 1/4 = y/2 + 1/4$ gives $x = y$. By Theorem 3.4.3, $|[0,1]| = |(0,1)|$.

A bijection. The two extra points 0 and 1 are absorbed by a Hilbert's hotel (Example (Hilbert's Hotel)) run on the points $1, \frac{1}{2}, \frac{1}{3}, \ldots$. Define $\varphi\colon [0,1] \to (0,1)$ by

$$\varphi(x) \coloneqq \begin{cases} \frac{1}{2} & \text{if } x = 0, \\ \frac{1}{n+2} & \text{if } x = \frac{1}{n} \text{ for some } n \in \mathbb{Z}_{>0}, \\ x & \text{otherwise.} \end{cases}$$

The cases do not overlap, since $\frac{1}{n} \neq 0$, and in the second case $n = 1/x$ is determined by x; so φ is a function, with values in $(0,1)$: the value is $\frac{1}{2}$, or $\frac{1}{n+2} \in (0, \frac{1}{3}]$, or, in the last case, x with $x \neq 0$ and $x \neq 1 = \frac{1}{1}$, so $0 < x < 1$. Let $H \coloneqq \{0\} \cup \{\frac{1}{n} : n \in \mathbb{Z}_{>0}\} = \{0, 1, \frac{1}{2}, \frac{1}{3}, \ldots\}$ and $H' \coloneqq \{\frac{1}{m} : m \in \mathbb{Z}_{>0},\ m \ge 2\} = \{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\}$. Then φ maps H onto H': $0 \mapsto \frac{1}{2}$, and $\frac{1}{n} \mapsto \frac{1}{n+2}$ runs through $\frac{1}{3}, \frac{1}{4}, \ldots$. It is injective on H, since $\frac{1}{n+2} = \frac{1}{n'+2}$ forces $n = n'$, and $\frac{1}{n+2} \le \frac{1}{3} < \frac{1}{2}$. Off H it is the identity of $[0,1] \setminus H = (0,1) \setminus H'$. Since

$$[0,1] = H \cup ([0,1] \setminus H), \qquad (0,1) = H' \cup ((0,1) \setminus H'),$$

both unions disjoint, φ is a bijection, and $|[0,1]| = |(0,1)|$. For instance $\varphi(1) = \frac{1}{3}$, $\varphi(\frac{1}{2}) = \frac{1}{4}$, $\varphi(\frac{3}{4}) = \frac{3}{4}$.

The first route took two lines and the second took a paragraph. That is the point of the theorem: we never had to find φ.

The second interval computation turns an unbounded set into a bounded one.

Example. The real line and its intervals

Show that $x \mapsto x/(1+|x|)$ is a bijection $\mathbb{R} \to (-1,1)$. Deduce that every open interval (c,d)

with $c < d$ is equinumerous with $\mathbb{R}$, and then that every interval with more than one point is.

Solution. The bijection. Let $s(x) := x/(1+|x|)$ for $x \in \mathbb{R}$; the denominator is at least 1, so $s(x)$ is defined, and $|s(x)| = |x|/(1+|x|) < 1$, so $s(x) \in (-1,1)$. For $y \in (-1,1)$ let $t(y) := y/(1-|y|)$; here $1-|y| > 0$. We check that t is a two-sided inverse. For $x \in \mathbb{R}$, $|s(x)| = |x|/(1+|x|)$, so

$$1-|s(x)| = \frac{1}{1+|x|}, \qquad t(s(x)) = \frac{x}{1+|x|}\cdot(1+|x|) = x.$$

For $y \in (-1,1)$, $|t(y)| = |y|/(1-|y|)$, so

$$1+|t(y)| = \frac{1}{1-|y|}, \qquad s(t(y)) = \frac{y}{1-|y|}\cdot(1-|y|) = y.$$

By Theorem 1.6.4, s is a bijection $\mathbb{R} \to (-1,1)$. For example $s(1) = \frac{1}{2}$ and $s(-3) = -\frac{3}{4}$.

Open intervals. The map $y \mapsto (y+1)/2$ is a bijection $(-1,1) \to (0,1)$, with inverse $u \mapsto 2u-1$. For $c < d$, the map $u \mapsto c + (d-c)u$ is a bijection $(0,1) \to (c,d)$, with inverse $v \mapsto (v-c)/(d-c)$, since $d-c > 0$. Composing the three bijections (Theorem 1.5.4 (c)) gives a bijection $\mathbb{R} \to (c,d)$, so $|(c,d)| = |\mathbb{R}|$.

Every interval with more than one point. Let I be an interval (bounded or not, with or without its endpoints) containing two points $c < d$. An interval contains every number between two of its points, so $(c,d) \subseteq I \subseteq \mathbb{R}$. The inclusion is an injection $(c,d) \to I$. In the other direction, let $\beta\colon \mathbb{R} \to (c,d)$ be the bijection just built; then β restricted to I is an injection $I \to (c,d)$. By the method of Example (Method: injections both ways) (Theorem 3.4.3), $|I| = |(c,d)|$, and $|(c,d)| = |\mathbb{R}|$, so $|I| = |\mathbb{R}|$ by Proposition 2.5.1. This covers $[0,1]$, $[0,1)$, $(0,\infty)$, $[5,\infty)$ and $\mathbb{R}$ itself at once.

In particular every interval with more than one point is uncountable: it is equinumerous with $\mathbb{R}$, which is uncountable by Theorem 3.3.4, and a set equinumerous with a countable set is countable (compose a surjection from $\mathbb{N}$ with the bijection, Proposition 3.1.4).

Warning. Injections both ways do not make either injection a bijection. On $\mathbb{N}$, $n \mapsto 2n$ is an injection $\mathbb{N} \to \mathbb{N}$ in both directions, and it is not onto: 1 is never a value. Theorem 3.4.3 builds a **new** map h out of f and g; it says nothing about f or g themselves. In Example (The closed and the open unit interval), $u(x) = x/2+1/4$ misses $\frac{9}{10} \in (0,1)$, and the bijection is a different map.

Quick check. Give an injection $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$ and an injection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$. What does Theorem 3.4.3 conclude?

Solution. $n \mapsto (n,1)$ is injective, by the characteristic property of pairs (Definition 1.4.1). $(m,n) \mapsto 2^m 3^n$ is injective, as shown in the proof of Theorem 3.1.6. So $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$, and

$\mathbb{N}\times\mathbb{N}$ is countably infinite (Definition 3.1.2). Section 3.1 showed only that $\mathbb{N}\times\mathbb{N}$ is countable; the theorem gives a bijection with $\mathbb{N}$ directly, with no listing at all.

Remark (Looking ahead). The method needs an injection each way. Are any two sets comparable, that is, is $|A| \le |B|$ or $|B| \le |A|$ for all A and B? Building an injection one element at a time does not settle it: a recursion indexed by $\mathbb{N}$ reaches only countably many elements, so it cannot exhaust an uncountable set. Section 6.2 proves that the answer is yes, by Zorn's lemma, a principle equivalent to Axiom 3.2.1. Nothing in this chapter needs comparability.

3.4.4 Exercises

3.4.4.1 A. Check your understanding

Exercise. A1

These parts are about the proof of Theorem 3.4.3.

(a) In Step 4, Case 2, why is $g(b) \notin C_0$, and what would go wrong without it?

(b) Run the construction for $A = B = \mathbb{N}$ and $f(n) = g(n) = 2n$. Compute C_0, C_1 and C, and the values $h(0), h(1), h(2), h(3), h(4)$.

(c) Where is the injectivity of f used?

(d) Give the idea of the proof in two sentences.

Solution.

(a) $C_0 = A \setminus g(B)$ consists of the points that are not values of g, and $g(b)$ is a value of g. Without it the index n with $g(b) \in C_n$ could be 0, and then there would be no C_{n-1} to find a predecessor a in, so no $a \in C$ with $f(a) = b$.

(b) $g(\mathbb{N}) = 2\mathbb{N}$, so $C_0 = \mathbb{N} \setminus 2\mathbb{N}$ is the set of odd numbers. $C_1 = g(f(C_0)) = \{4q : q \text{ odd}\} = \{4, 12, 20, \dots\}$. In general $C_{n+1} = \{4c : c \in C_n\}$, so $C_n = \{4^n q : q \text{ odd}\}$ by induction on n, and C is the set of numbers $4^k q$ with $k \in \mathbb{N}$ and q odd. Now:
- $0 \notin C$, since $4^k q \neq 0$ for odd q ($4^k > 0$ and $q \ge 1$). So $h(0)$ is the b with $2b = 0$: $h(0) = 0$, a fixed point.
- $1 \in C_0$, so $h(1) = f(1) = 2$.
- $2 \notin C$: for $k = 0$, 2 is not odd; for $k \ge 1$, $4^k q \ge 4 > 2$. So $h(2)$ is the b with $2b = 2$: $h(2) = 1$.
- $3 \in C_0$, so $h(3) = 6$.
- $4 = 4^1 \cdot 1 \in C_1$, so $h(4) = f(4) = 8$.

(c) In Step 3, Case 1: from $f(a) = f(a')$ with $a, a' \in C$ it concludes $a = a'$.

(d) Points of A that g does not reach must be sent forward by f, and so must everything reached from them by repeating $g \circ f$; this is the set C. Every other point of A is a value of g and is sent back to its unique preimage, and the two halves fit together into a bijection.

3.4.4.2 B. Practice

Exercise. B1: Injections both ways

Prove each of the following by giving an injection in each direction and applying Theorem 3.4.3.

(a) $|[0,1]| = |\mathbb{R}|$.
(b) $|\mathbb{N}| = |\mathbb{N} \times \mathbb{Z}|$.
(c) $|(0,1) \cup (2,3)| = |(0,1)|$.

Solution.

(a) The inclusion $[0,1] \to \mathbb{R}$ is injective. In the other direction, $x \mapsto (x/(1+|x|)+1)/2$ is a bijection $\mathbb{R} \to (0,1)$ by Example (The real line and its intervals), so it is an injection $\mathbb{R} \to [0,1]$, as $(0,1) \subseteq [0,1]$.

(b) $n \mapsto (n,0)$ is an injection $\mathbb{N} \to \mathbb{N} \times \mathbb{Z}$, by the characteristic property of pairs (Definition 1.4.1). In the other direction, let $j\colon \mathbb{Z} \to \mathbb{N}$ be $j(k) \coloneqq 2k$ for $k \geq 0$ and $j(k) \coloneqq -2k-1$ for $k < 0$. Its values are in $\mathbb{N}$, even for $k \geq 0$ and odd for $k < 0$; since no natural number is both even and odd (Theorem 2.2.3, uniqueness), $j(k) = j(k')$ forces k and k' to have the same sign, and then $k = k'$. So j is injective, and so is $(m,k) \mapsto (m, j(k))$. Following it by the injection $(m,n) \mapsto 2^m 3^n$ from the proof of Theorem 3.1.6 gives an injection $\mathbb{N} \times \mathbb{Z} \to \mathbb{N}$ (Theorem 1.5.4 (a)).

(c) The inclusion $(0,1) \to (0,1) \cup (2,3)$ is injective. The map $x \mapsto x/4$ is injective and sends $(0,1) \cup (2,3)$ into $(0, \frac{1}{4}) \cup (\frac{1}{2}, \frac{3}{4}) \subseteq (0,1)$.

Hence, by Theorem 3.4.3, the three equalities hold.

Exercise. B2: A proper subset of the same size

Give an example of sets $A \subsetneq B \subseteq \mathbb{R}$ with $|A| = |B|$, such that A is uncountable and $B \setminus A$ is uncountable. Check each property, and list the properties any answer must have.

Solution. An answer must have: (1) $A \subseteq B \subseteq \mathbb{R}$; (2) $A \neq B$; (3) a bijection $A \to B$, or injections both ways; (4) A uncountable; (5) $B \setminus A$ uncountable. (Then B is uncountable too, since it contains A, by Proposition 3.1.3.)

Example: $A = (0,1)$, $B = (0,3)$. (1) and (2): $(0,1) \subseteq (0,3)$ and $2 \in B \setminus A$. (3): $x \mapsto 3x$ is a bijection $(0,1) \to (0,3)$, with inverse $y \mapsto y/3$. (4) and (5): A and $B \setminus A = [1,3)$ are intervals with more than one point, hence equinumerous with $\mathbb{R}$ by Example (The real line and its intervals), hence uncountable, as shown after it.

Another correct answer: $A = (0,1)$, $B = \mathbb{R}$, with $B \setminus A \supseteq (1,2)$ uncountable. Any answer can be checked against (1)–(5).

Exercise. B3: Interleaving two sequences

Prove that $\left|\{0,1\}^{\mathbb{N}} \times \{0,1\}^{\mathbb{N}}\right| = \left|\{0,1\}^{\mathbb{N}}\right|$ by an explicit bijection.

Hint: put one sequence in the even places and the other in the odd places.

Solution. Every $m \in \mathbb{N}$ is $2n$ or $2n+1$ for exactly one $n \in \mathbb{N}$, and not both (Theorem 2.2.3 with divisor 2, the quotient in $\mathbb{N}$, as in the proof of Proposition 3.1.5). So for $a, b \in \{0,1\}^{\mathbb{N}}$ we may define $c = \Phi(a,b) \in \{0,1\}^{\mathbb{N}}$ by

$$c(2n) \coloneqq a(n), \qquad c(2n+1) \coloneqq b(n) \qquad (n \in \mathbb{N}).$$

Define $\Psi\colon \{0,1\}^{\mathbb{N}} \to \{0,1\}^{\mathbb{N}} \times \{0,1\}^{\mathbb{N}}$ by $\Psi(c) \coloneqq (a,b)$ with $a(n) \coloneqq c(2n)$ and $b(n) \coloneqq c(2n+1)$. Then $\Psi(\Phi(a,b)) = (a,b)$: its coordinates $n \mapsto c(2n) = a(n)$ and $n \mapsto c(2n+1) = b(n)$ are a and b by Proposition 1.5.1, so the pairs are equal (Definition 1.4.1). And $\Phi(\Psi(c))$ agrees with c at every even place $2n$ and every odd place $2n+1$, which are all the places, so $\Phi(\Psi(c)) = c$ (Proposition 1.5.1). By Theorem 1.6.4, Φ is a bijection.

Exercise. B4: Prove or disprove

Prove each true statement and refute each false one with a counterexample. Here A, B, C are sets.

(a) $|\mathbb{Z}| < |\mathbb{Q}|$.

(b) If $|A| < |B|$ and $|B| \le |C|$, then $|A| < |C|$.

(c) If $|A| \le |B|$ and B is countable, then A is countable.

(d) $\left|\{0,1\}^{\mathbb{N}}\right| = \left|\mathbb{N}^{\mathbb{N}}\right|$, where $\mathbb{N}^{\mathbb{N}}$ is the set of functions $\mathbb{N} \to \mathbb{N}$.

(e) If $A \subseteq B$ and $|B| \le |A|$, then $|A| = |B|$.

Solution.

(a) False. Both sets are countably infinite (Theorem 3.1.8), so $|\mathbb{Z}| = |\mathbb{N}| = |\mathbb{Q}|$ by Proposition 2.5.1, and there is a bijection $\mathbb{Z} \to \mathbb{Q}$. So "not $|\mathbb{Z}| = |\mathbb{Q}|$" fails.

(b) True. First, $|A| \le |C|$ by Proposition 3.4.1 (b). Suppose, for a contradiction, that there is a bijection $\varphi\colon A \to C$, and let $k\colon B \to C$ be an injection. Then $\varphi^{-1} \circ k\colon B \to A$ is injective (Theorem 1.5.4 (a); φ^{-1} is a bijection by Theorem 1.6.4), so $|B| \le |A|$. With $|A| \le |B|$, Theorem 3.4.3 gives $|A| = |B|$, against $|A| < |B|$. So there is no bijection $A \to C$, and $|A| < |C|$.

(c) True. Let $f\colon A \to B$ be an injection. As B is countable, there is an injection $j\colon B \to \mathbb{N}$ (Theorem 3.1.2, (i) $\Rightarrow$ (ii)). The composite $j \circ f\colon A \to \mathbb{N}$ is injective (Theorem 1.5.4 (a)), so A is countable by (ii) $\Rightarrow$ (i).

(d) True, by the method of Example (Method: injections both ways). *Into* $\mathbb{N}^{\mathbb{N}}$*:* send $a \in \{0,1\}^{\mathbb{N}}$ to the same rule read with codomain $\mathbb{N}$. Two sequences with the same image have the same values, so they are equal (Proposition 1.5.1). *Back:* in three injective steps.

- $f \mapsto G_f$, the graph of f, is an injection $\mathbb{N}^{\mathbb{N}} \to \mathcal{P}(\mathbb{N} \times \mathbb{N})$: equal graphs give equal values, so equal functions (Proposition 1.5.1).
- With the injection $p(m,n) \coloneqq 2^m 3^n$ from the proof of Theorem 3.1.6, $S \mapsto p(S)$ is an injection $\mathcal{P}(\mathbb{N} \times \mathbb{N}) \to \mathcal{P}(\mathbb{N})$. If $p(S) = p(T)$ and $x \in S$, then $p(x) \in p(T)$, so

$p(x) = p(y)$ for some $y \in T$, and $x = y \in T$. So $S \subseteq T$, and $T \subseteq S$ in the same way.

- $S \mapsto \mathbf{1}_S$ is an injection $\mathcal{P}(\mathbb{N}) \to \{0,1\}^{\mathbb{N}}$: $\mathbf{1}_S = \mathbf{1}_T$ says that $n \in S$ exactly when $n \in T$.

The composite of the three is an injection $\mathbb{N}^{\mathbb{N}} \to \{0,1\}^{\mathbb{N}}$ (Proposition 3.4.1 (b)), and Theorem 3.4.3 gives the equality.

(e) True. The inclusion $A \to B$ gives $|A| \leq |B|$, and Theorem 3.4.3 applies.

3.4.4.3 C. Going deeper

Exercise. C1: The real line and the subsets of $\mathbb{N}$

Prove that $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$, using the decimal facts (D1)–(D3) of Section 3.3.

(a) For $x \in [0,1)$ let $d_1 d_2 \ldots$ be its decimal expansion that does not end in all 9s, and let $E(x) := \{10k + d_k : k \in \mathbb{Z}_{>0}\}$. Show that E is a well-defined injection $[0,1) \to \mathcal{P}(\mathbb{N})$.

(b) For $S \subseteq \mathbb{N}$ let y_S be the number with decimal expansion $0.e_1 e_2 e_3 \ldots$, where $e_{k+1} := 1$ if $k \in S$ and $e_{k+1} := 2$ if $k \notin S$, for $k \in \mathbb{N}$. Show that $S \mapsto y_S$ is a well-defined injection $\mathcal{P}(\mathbb{N}) \to [0,1)$.

(c) Conclude.

Solution (Hint 1). The tools are the decimal facts (D1)–(D3), and Theorem 2.2.3 with divisor 10 for reading digits back out of $E(x)$.

Solution (Hint 2). Begin (a) with: "By (D1), x has an expansion that does not end in all 9s, and by (D3) it has only one."

Solution.

(a) *Well defined.* By (D1), x has an expansion not ending in all 9s. It has only one: if two different expansions of x both failed to end in all 9s, (D3) would make one of them end in all 9s. So $d_1 d_2 \ldots$ is determined by x, and $E(x) \subseteq \mathbb{N}$ because $10k + d_k \in \mathbb{N}$.
Injective. By Theorem 2.2.3 with divisor 10, the number $10j + d_j$, with $0 \leq d_j \leq 9$, has quotient j and remainder d_j, and these are unique. So for each $k \geq 1$, the only element of $E(x)$ with quotient k is $10k + d_k$, and $E(x)$ determines every digit d_k. If $E(x) = E(x')$, then x and x' have the same expansion $d_1 d_2 \ldots$, and by the uniqueness half of (D2) a digit sequence is an expansion of exactly one number; so $x = x'$.

(b) *Well defined.* By (D2), the digit sequence $e_1 e_2 \ldots$ is an expansion of exactly one $y_S \in [0,1]$. With $t_1 = e_1/10$ as in Definition 3.3.1, $y_S \leq t_1 + \frac{1}{10} \leq \frac{2}{10} + \frac{1}{10} = \frac{3}{10}$, so $y_S \in [0,1)$.
Injective. Let $S \neq S'$, say $k \in S \setminus S'$ or $k \in S' \setminus S$. Then the two digit sequences differ at place $k+1$. Neither contains a 0 or a 9, so neither ends in all 9s or in all 0s. If $y_S = y_{S'}$, the number would have two different expansions, and by (D3) one would end in all 9s, which is false. So $y_S \neq y_{S'}$. The index shift e_{k+1} is there so that whether $0 \in S$ is recorded too, in the first digit.

(c) By (a), (b) and Theorem 3.4.3, $|[0,1)| = |\mathcal{P}(\mathbb{N})|$. By Example (The real line and

its intervals), $[0,1)$, an interval with more than one point, has $|[0,1)| = |\mathbb{R}|$. By Proposition 2.5.1, $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.

Marking scheme. (10 points) - 2: shows the expansion in (a) is unique, citing (D1) and (D3), so E is a function. - 2: shows E is injective: the set determines each digit, and one digit sequence names one number (D2). - 2: shows y_S exists, is unique and lies in $[0,1)$. - 2: shows $S \mapsto y_S$ is injective, using that the digits avoid 0 and 9 and (D3). - 2: applies Theorem 3.4.3 and passes from $[0,1)$ to $\mathbb{R}$ with a cited bijection or injections both ways. Fatal errors (0 for the step): treating "the expansion of x" as unique without (D1) and (D3); concluding $y_S \neq y_{S'}$ from different digit sequences without ruling out the $0.4999\ldots = 0.5$ case.

Exercise. C2: Find the error

Here is a proof that $|[0,1]| = |(0,1)|$.

> *Proof.* (1) Let $u\colon [0,1] \to (0,1)$, $u(x) := x/2 + 1/4$. For $0 \le x \le 1$ we have $1/4 \le u(x) \le 3/4$, so u does map into $(0,1)$. (2) If $u(x) = u(y)$, then $x/2 = y/2$, so $x = y$; hence u is injective. (3) The inclusion $\iota\colon (0,1) \to [0,1]$ is injective. (4) So there are injections in both directions between $[0,1]$ and $(0,1)$. (5) Therefore u is a bijection, and $|[0,1]| = |(0,1)|$.

Is the conclusion true? Does the argument prove it? If not, name the line that fails, say why, and give a counterexample to the step it takes.

Solution. The conclusion is true: Example (The closed and the open unit interval) proves it twice.

The argument does not prove it. Lines (1)–(4) are correct. Line (5) fails: it infers that a particular injection is a bijection from the existence of injections both ways. The step cites a general "fact", that injections both ways make a given injection a bijection. That fact is neither proved nor a school fact, and it is false, so the line cites nothing: entry (N9) of Logic and Proof, Example (What is not allowed). And u is in fact not onto: $\frac{9}{10} \in (0,1)$ is not a value, since every value lies in $[\frac{1}{4}, \frac{3}{4}]$.

Counterexample to the step. Take $A = B = \mathbb{N}$ and $f = g = (n \mapsto 2n)$. These are injections both ways, and the step would conclude that $n \mapsto 2n$ is a bijection $\mathbb{N} \to \mathbb{N}$; but 1 is not a value.

Repair. Replace line (5) by: "By Theorem 3.4.3, $|[0,1]| = |(0,1)|$." The theorem produces a bijection, but a different one, built from both u and ι.

3.5 Infinite Sets

Section 3.4 compared sizes with injections. Here we ask where $\mathbb{N}$ sits in that comparison. Every infinite set we have met contains a copy of $\mathbb{N}$, and it is tempting to say that this must always happen by picking new elements one at a time; this section makes that picking exact. It turns out to need Axiom 3.2.1 again, this time applied to a family with one set for each non-empty subset of the given set, and it gives two results: $\mathbb{N}$ is the smallest infinite size, and a set is infinite

exactly when it is the same size as a proper part of itself.

3.5.1 Every infinite set contains a copy of the natural numbers

The question has a goal theorem: we want to show that an infinite set X has a countably infinite subset, that is, a subset equinumerous with $\mathbb{N}$ (Definition 3.1.2). Equivalently, we want an injection $\mathbb{N} \to X$: its image is then such a subset.

Theorem 3.5.1. Infinite Sets Contain a Countably Infinite Subset

Every infinite set X has a countably infinite subset. Equivalently, there is an injection $\mathbb{N} \to X$.

Idea. The natural attempt picks $x_0 \in X$, then $x_1 \in X \setminus \{x_0\}$, then $x_2 \in X \setminus \{x_0, x_1\}$, and so on. Each pick is possible, because a finite set cannot exhaust the infinite X, and each single pick is one $\exists$E. But "and so on" is a definition by recursion, and Theorem 2.3.1 needs a **function** g that says, once and for all, which new element to take after any finite stage. That function must pick an element from every non-empty set of the form $X \setminus F$ at once, with no rule for doing so when X is arbitrary. So we let Axiom 3.2.1 supply a choice function c on all non-empty subsets of X first, and then the recursion is an ordinary one, with c as its rule.

Proof. Let X be infinite. The family $(S)_{S \in \mathcal{P}(X) \setminus \{\emptyset\}}$, indexed by the non-empty subsets of X with each index as its own member, consists of non-empty sets, and its union is X: every index is a subset of X, and each $x \in X$ lies in the index $\{x\}$. **By Axiom 3.2.1** there is a function $c \colon \mathcal{P}(X) \setminus \{\emptyset\} \to X$ with

$$c(S) \in S \quad \text{for every non-empty } S \subseteq X.$$

This is the one line of the proof that uses the axiom.

Define $g \colon \mathbb{N} \times \mathcal{P}(X) \to \mathcal{P}(X)$ by $g(n, F) \coloneqq F \cup \{c(X \setminus F)\}$ if $F \neq X$, and $g(n, F) \coloneqq F$ if $F = X$. In the first case $X \setminus F$ is non-empty, so $c(X \setminus F)$ is defined; so g is a function. By Theorem 2.3.1, applied with the set $\mathcal{P}(X)$, the starting value $\emptyset$ and this g, there are sets $F_n \subseteq X$, for $n \in \mathbb{N}$, with $F_0 = \emptyset$ and $F_{n+1} = g(n, F_n)$.

We show by induction (Logic and Proof, Axiom 4.2.1) that F_n **has exactly** n **elements, for every** $n \in \mathbb{N}$. For $n = 0$, $F_0 = \emptyset$ has 0 elements (Definition 2.5.2). Suppose F_n has n elements. Then F_n is finite and X is not, so $F_n \neq X$, and $F_{n+1} = F_n \cup \{c(X \setminus F_n)\}$ with $c(X \setminus F_n) \in X \setminus F_n$. This is a union of disjoint sets with n elements and 1 element, so F_{n+1} has $n + 1$ elements by Proposition 2.5.5.

In particular $F_n \neq X$ for every $n \in \mathbb{N}$, so we may define

$$x_n \coloneqq c(X \setminus F_n) \in X \setminus F_n, \qquad \text{and then} \qquad F_{n+1} = F_n \cup \{x_n\}.$$

Hence $F_n \subseteq F_{n+1}$ for every n, and by induction on k, $F_m \subseteq F_{m+k}$ for all $m, k \in \mathbb{N}$.

Now let $m, n \in \mathbb{N}$ with $m < n$. Then $x_m \in F_{m+1} \subseteq F_n$, because $m + 1 \leq n$ (Lemma 2.1.1 (e)), so $k := n - (m + 1) \in \mathbb{N}$ (Lemma 2.1.1 (d)) and $F_{m+1} \subseteq F_{(m+1)+k} = F_n$; and $x_n \notin F_n$. So $x_m \neq x_n$. Hence $n \mapsto x_n$ is an injection $\mathbb{N} \to X$. Its image $\{x_n : n \in \mathbb{N}\} \subseteq X$ is equinumerous with $\mathbb{N}$, since $n \mapsto x_n$ is a bijection from $\mathbb{N}$ onto it. This proves the theorem.

■

The proof shows where the axiom enters and why one ∃E per step is not enough: ∃E names one element for one set, while the recursion needs g as a single function defined on every stage at once. Each F_n is then determined by c; the only arbitrary thing is c itself.

A non-example by a minimal change. Run the same construction on the finite set $X = \{a, b\}$, with $a \neq b$. The choice function c and the recursion still make sense, since g is defined on every $F \subseteq X$. But $F_1 = \{c(X)\}$ has one element, F_2 adds the other, so $F_2 = X$, and from then on g leaves F_n unchanged. So $x_2 = c(X \setminus F_2) = c(\emptyset)$ is not defined. The step that fails is "F_n is finite and X is not, so $F_n \neq X$", exactly where the hypothesis that X is infinite is used.

Remark. Compare *Analysis on the Real Line*, Chapter 1's proof that the real numbers cannot be listed. There, a given list is used to build nested closed intervals, and each interval is obtained from the previous one by an explicit rule (keep an outer third that misses the next point of the list), so no choice principle is involved. Here X is an arbitrary infinite set, and there is no rule available for picking an element of an arbitrary non-empty subset of it; the choice function **is** the rule.

For a particular X a rule may exist: for $X \subseteq \mathbb{N}$, "the least element" is one (Theorem 2.1.3), and then the proof needs no axiom. That the theorem cannot be proved in general from the other rules of set formation alone is a result of set theory; we state it without proof, and nothing depends on it.

3.5.2 Consequences: the smallest infinite size

The theorem says $|\mathbb{N}| \leq |X|$ for every infinite X (Definition 3.4.1). Three consequences follow at once.

- $\mathbb{N}$ **is the smallest infinite size.** If X is infinite and $|X| \leq |\mathbb{N}|$, then $|X| = |\mathbb{N}|$, by Theorem 3.4.3 and the theorem. So no infinite set is strictly smaller than $\mathbb{N}$.
- **Countable sets are exactly the sets of size at most** $|\mathbb{N}|$, by Theorem 3.1.2, (i) $\iff$ (ii). Combining with the first point: a countable set is finite or equinumerous with $\mathbb{N}$, which Theorem 3.1.2 (iii) already said.
- **An uncountable set is strictly bigger than** $\mathbb{N}$**.** If X is uncountable, then X is infinite (a finite set is countable, by Theorem 3.1.2), so $|\mathbb{N}| \leq |X|$; and $|\mathbb{N}| = |X|$ would make X countable. So $|\mathbb{N}| < |X|$. For example $|\mathbb{N}| < |\mathbb{R}|$, since $\mathbb{R}$ is uncountable (Theorem 3.3.4).

Warning. "Infinite" and "uncountable" are different words. $\mathbb{Q}$ is infinite (it contains $\mathbb{N}$, which is infinite by Example (Hilbert's Hotel), and a subset of a finite set is finite, by Proposition 2.5.6) and countable (Theorem 3.1.8). Likewise "X contains a copy of $\mathbb{N}$" is not "X is equinumerous with $\mathbb{N}$": $\mathbb{R}$ contains $\mathbb{N}$, and $|\mathbb{N}| < |\mathbb{R}|$ (as above).

Quick check. Let X be uncountable. Is $X \setminus \{x\}$ uncountable for every $x \in X$? Why must X have an element at all?

Solution. $X \neq \emptyset$, because $\emptyset$ is countable by Definition 3.1.1. For $x \in X$, if $X \setminus \{x\}$ were countable, then $X = (X \setminus \{x\}) \cup \{x\}$ would be a union of two countable sets, countable by Proposition 3.1.5. So $X \setminus \{x\}$ is uncountable.

3.5.3 Infinite sets are the same size as a proper part

Section 2.5 proved that a finite set is never equinumerous with a proper subset (Theorem 2.5.9), and Example (Hilbert's Hotel) showed $\mathbb{N}$ doing exactly that. With Theorem 3.5.1, the hotel can be built inside any infinite set: run it on the copy of $\mathbb{N}$, and leave everything else alone.

Theorem 3.5.2. Infinite Sets and Proper Subsets

A set X is infinite if and only if $|X| = |Y|$ for some proper subset $Y \subsetneq X$.

Idea. One direction is already done: Section 2.5 showed that finite sets have no proper subset of their own size. For the other, take the copy $x_0, x_1, x_2, \ldots$ of $\mathbb{N}$ inside X and move every guest one room up, $x_n \mapsto x_{n+1}$, as $n \mapsto n+1$ does in the Quick check after Example (Hilbert's Hotel). Room x_0 is vacated, and every point outside the copy stays where it is.

Proof. ($\Leftarrow$) This is the contrapositive of Theorem 2.5.9: a finite set is not equinumerous with any proper subset, so a set that is equinumerous with one is not finite.

($\Rightarrow$) Let X be infinite. By Theorem 3.5.1 there is an injection $n \mapsto x_n$ from $\mathbb{N}$ to X; let $S \coloneqq \{x_n : n \in \mathbb{N}\}$. Each element of S is x_n for exactly one $n \in \mathbb{N}$, by injectivity. Define $h\colon X \to X \setminus \{x_0\}$ by

$$h(x) \coloneqq \begin{cases} x_{n+1} & \text{if } x = x_n \text{ with } n \in \mathbb{N}, \\ x & \text{if } x \notin S. \end{cases}$$

This is a function into $X \setminus \{x_0\}$: $x_{n+1} \neq x_0$ because $n+1 \neq 0$, and an $x \notin S$ is not x_0.

h is injective. Two points of S: $x_{m+1} = x_{n+1}$ gives $m+1 = n+1$, so $m = n$. Two points outside S: h is the identity there. One of each: $h(x_n) = x_{n+1} \in S$, while $h(x) = x \notin S$, so the values differ.

h is onto $X \setminus \{x_0\}$. Let $y \in X \setminus \{x_0\}$. If $y \notin S$, then $y = h(y)$. If $y \in S$, then $y = x_m$ with $m \neq 0$, so $n \coloneqq m - 1 \in \mathbb{N}$ (Lemma 2.1.1 (c)) and $y = x_{n+1} = h(x_n)$.

So h is a bijection, and $Y \coloneqq X \setminus \{x_0\}$ is a proper subset of X, as $x_0 \in X \setminus Y$, with $|X| = |Y|$. This proves the theorem.

■

Together with Section 2.5, this gives a characterization of "infinite" that never mentions $\mathbb{N}$ or counting: a set is infinite precisely when some proper part of it is as big as the whole. The finite intuition "a part is smaller than the whole" is exactly the property that separates finite sets from infinite ones. The direction ($\Rightarrow$) used Axiom 3.2.1, through Theorem 3.5.1; the direction ($\Leftarrow$) did not.

Quick check. Name a proper subset of $\mathbb{R}$ that is equinumerous with $\mathbb{R}$, and give a bijection.

Solution. $(-1, 1)$, with the bijection $x \mapsto x/(1 + |x|)$ of Example (The real line and its intervals). (Any interval with more than one point other than $\mathbb{R}$ itself works, by the same example.) No choice is needed for $\mathbb{R}$: the bijection is a formula.

3.5.4 Exercises

3.5.4.1 A. Check your understanding

Exercise. A1

(a) Where does the proof of Theorem 3.5.1 use Axiom 3.2.1? Why is one $\exists$E per step not enough?

(b) True or false, with a reason: every infinite subset of $\mathbb{R}$ contains a countably infinite subset; every uncountable set contains an uncountable proper subset.

(c) Write down the bijection $X \to X \setminus \{x_0\}$ of the proof of Theorem 3.5.2 for $X = \mathbb{Z}$ and $x_n = n$ for $n \in \mathbb{N}$.

(d) For $X = \mathbb{N}$, is choice needed to find a countably infinite subset?

Solution.

(a) At the line "By Axiom 3.2.1 there is a function c with $c(S) \in S$ for every non-empty $S \subseteq X$." One $\exists$E names one element of one non-empty set; that would give x_0, then x_1, and any finite number of steps. But Theorem 2.3.1 needs the step as a **function** g, defined once for every stage F at once, before the sequence exists. Defining g means picking an element of $X \setminus F$ for every such F simultaneously, and that is what the axiom provides.

(b) Both are true. The first is Theorem 3.5.1 applied to the infinite subset. For the second, let X be uncountable; then $X \neq \emptyset$, and for $x \in X$, $X \setminus \{x\}$ is an uncountable proper subset, by the Quick check after the warning above.

(c) $h(n) = n + 1$ for $n \in \mathbb{N}$, and $h(k) = k$ for $k < 0$. It maps $\mathbb{Z}$ onto $\mathbb{Z} \setminus \{0\}$: a positive m is $h(m - 1)$, and a negative k is $h(k)$.

(d) No. $\mathbb{N}$ itself is countably infinite, via $\mathrm{id}_{\mathbb{N}}$. (More generally, an infinite $X \subseteq \mathbb{N}$ can be listed in increasing order by Lemma 3.1.1, a rule.)

3.5.4.2 B. Practice

Exercise. B1: Removing finitely many points

Let X be infinite and let $F \subseteq X$ be finite. Prove that $|X \setminus F| = |X|$.

Solution. First, $X \setminus F$ is infinite: otherwise $X = (X \setminus F) \cup F$ would be a union of two disjoint finite sets, finite by Proposition 2.5.5.

By Theorem 3.5.1 applied to $X \setminus F$ (this uses Axiom 3.2.1), there is an injection $n \mapsto s_n$ from $\mathbb{N}$ to $X \setminus F$; let $S \coloneqq \{s_n : n \in \mathbb{N}\}$. Let F have k elements, and let $\varphi\colon \{1, \dots, k\} \to F$ be a bijection (Definition 2.5.2). No two of $X \setminus (F \cup S)$, F and S meet, and together they make up X; and $X \setminus F$ is the union of the disjoint sets $X \setminus (F \cup S)$ and S. Define $h\colon X \to X \setminus F$ by

$$h(x) \coloneqq \begin{cases} x & \text{if } x \notin F \cup S, \\ s_{i-1} & \text{if } x = \varphi(i),\ i \in \{1, \dots, k\}, \\ s_{n+k} & \text{if } x = s_n,\ n \in \mathbb{N}. \end{cases}$$

Each x falls under one case, with one i or one n, since φ and $n \mapsto s_n$ are injective. The second case sends F bijectively onto $\{s_0, \dots, s_{k-1}\}$, and the third sends S bijectively onto $\{s_m : m \geq k\}$; these two image sets are disjoint and together make up S. The first case is the identity on $X \setminus (F \cup S)$. So h is a bijection, and $|X \setminus F| = |X|$. (For $k = 0$, $F = \emptyset$ and h is the identity.)

Exercise. B2: Absorbing a countable set

Let X be infinite, and let C be countable with $C \cap X = \emptyset$. Prove that $|X \cup C| = |X|$.

Hint: absorb C into a countably infinite subset of X.

Solution. By Theorem 3.5.1 (using Axiom 3.2.1) there is a countably infinite $S \subseteq X$. The set $S \cup C$ is countable by Proposition 3.1.5, and infinite, because it contains S (a subset of a finite set is finite, Proposition 2.5.6), which is infinite: if $\varphi\colon \{1, \dots, k\} \to S$ were a bijection and $\beta\colon \mathbb{N} \to S$ is a bijection given by the theorem, then $\beta^{-1} \circ \varphi$ would be a bijection $\{1, \dots, k\} \to \mathbb{N}$ (Proposition 2.5.1, Theorem 1.5.4), against Example (Hilbert's Hotel). By Theorem 3.1.2 (iii), $S \cup C$ is countably infinite. So $|S \cup C| = |\mathbb{N}| = |S|$, and Proposition 2.5.1 gives a bijection $\psi\colon S \cup C \to S$.

Now $X \cup C$ is the union of the disjoint sets $X \setminus S$ and $S \cup C$ (disjoint because $C \cap X = \emptyset$), and X is the union of the disjoint sets $X \setminus S$ and S. Define $h\colon X \cup C \to X$ by $h(x) \coloneqq x$ for $x \in X \setminus S$ and $h(x) \coloneqq \psi(x)$ for $x \in S \cup C$. It is a bijection on each piece, onto the corresponding piece, so it is a bijection, and $|X \cup C| = |X|$.

Exercise. B3: A big hole

Give an example of an infinite set X and a proper subset $Y \subsetneq X$ with $|Y| = |X|$ and $X \setminus Y$ infinite. Check each property, and list the properties any answer must have.

Solution. An answer must have: (1) $Y \subseteq X$; (2) $Y \neq X$; (3) a bijection $X \to Y$, or injections both ways; (4) X infinite; (5) $X \setminus Y$ infinite. (The hole $X \setminus Y$ in the proof of Theorem 3.5.2 was the single point x_0; this asks for more.)

Example: $X = \mathbb{N}$, $Y = 2\mathbb{N}$. (1), (2): $2\mathbb{N} \subseteq \mathbb{N}$ and $1 \notin 2\mathbb{N}$. (3): $n \mapsto 2n$ is a bijection $\mathbb{N} \to 2\mathbb{N}$ (Example (Hilbert's Hotel)). (4): $\mathbb{N}$ is infinite (Example (Hilbert's Hotel)). (5): $X \setminus Y$ is the set of odd numbers (every $m \in \mathbb{N}$ is even or odd, not both, by Theorem 2.2.3), and $n \mapsto 2n+1$ is a bijection from $\mathbb{N}$ onto it; if it were finite, $\mathbb{N}$ would be finite too (compose with a bijection from $\{1, \dots, k\}$, Theorem 1.5.4), which it is not.

Another correct answer: $X = \mathbb{R}$, $Y = (0, \infty)$. (1), (2): $(0, \infty) \subseteq \mathbb{R}$ and $0 \notin (0, \infty)$. (3): Example (The real line and its intervals). (4), (5): $n \mapsto -n$ is a bijection from $\mathbb{N}$ onto $\{-n : n \in \mathbb{N}\}$, so this set is infinite, as in (5) above. It lies inside $X \setminus Y = (-\infty, 0] \subseteq \mathbb{R}$, so by Proposition 2.5.6 neither $(-\infty, 0]$ nor $\mathbb{R}$ is finite.

3.5.4.3 C. Going deeper

Exercise. C1: Increasing functions

A function $f : \mathbb{N} \to \mathbb{N}$ is **strictly increasing** if $f(m) < f(n)$ whenever $m < n$. Let I be the set of strictly increasing functions $\mathbb{N} \to \mathbb{N}$. Prove that I is uncountable.

Below, the proof is started; the second half is blank. *Name the move, then complete it.*

> Let $n \mapsto f_n$ be any function from $\mathbb{N}$ to I. By Theorem 2.3.1, applied with the set $\mathbb{N}$, the starting value $f_0(0)+1$ and the function $(n, x) \mapsto \max\{x, f_{n+1}(n+1)\}+1$ from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$ (a step that depends on n), there is a function $g : \mathbb{N} \to \mathbb{N}$ with
>
> $$g(0) = f_0(0) + 1, \qquad g(n+1) = \max\{g(n), f_{n+1}(n+1)\} + 1.$$
>
> _____

Solution (Hint 1). Two things must be shown about g: that it lies in I, and that it differs from each f_n somewhere. Where?

Solution (Hint 2). The second half begins: "For every $n \in \mathbb{N}$, $g(n+1) \geq g(n) + 1 > g(n)$."

Solution. The move is **the diagonal**: given any list, build an object that differs from the n-th entry at the n-th place. Here the object must also stay inside I, which is why $g(n+1)$ is pushed above $g(n)$ as well as above $f_{n+1}(n+1)$.

Completion. For every $n \in \mathbb{N}$, $g(n+1) = \max\{g(n), f_{n+1}(n+1)\}+1 \geq g(n)+1 > g(n)$. From this, $g(m) < g(n)$ whenever $m < n$, by induction on n (Theorem 2.2.1 with base $m+1$): $g(m) < g(m+1)$, and $g(m) < g(n) < g(n+1)$. So $g \in I$.

Next, $g(n) > f_n(n)$ for every $n \in \mathbb{N}$: for $n = 0$, $g(0) = f_0(0) + 1$; for $n = k+1$, $g(k+1) \geq f_{k+1}(k+1) + 1$. So $g(n) \neq f_n(n)$, and hence $g \neq f_n$, for every $n \in \mathbb{N}$. So $g \in I$ is not a value of $n \mapsto f_n$, and no function $\mathbb{N} \to I$ is onto. Since $I \neq \emptyset$ (it contains $\mathrm{id}_{\mathbb{N}}$), I is not countable.

Marking scheme. (10 points) - 1: names the diagonal move. - 4: shows g is strictly increasing: 2 for the step $g(n) < g(n+1)$ for every n, and 2 for the passage to all $m < n$. - 3: shows $g(n) > f_n(n)$ for every n, treating $n = 0$ and $n = k+1$ separately, and concludes $g \neq f_n$. - 2: concludes that no function $\mathbb{N} \to I$ is onto and, noting $I \neq \emptyset$ ($\mathrm{id}_{\mathbb{N}} \in I$), that I is not countable. Fatal errors (0 for the part concerned): taking $g(n) < g(n+1)$ alone as strict increase, with no passage to all $m < n$; inferring $g \neq f_n$ without exhibiting a point where they differ, or exhibiting one only for $n \geq 1$.

The max in g is needed: the plain diagonal $g(n) := f_n(n) + 1$ need not be strictly increasing (for $f_0(n) = 5 + n$ and $f_1(n) = n$, it gives $g(0) = 6 > g(1) = 2$).

Exercise. C2: The irrationals

Deduce from Exercise (B2: Absorbing a countable set) that $|\mathbb{R} \setminus \mathbb{Q}| = |\mathbb{R}|$.

Solution. The set $\mathbb{R} \setminus \mathbb{Q}$ is uncountable: otherwise $\mathbb{R} = (\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q}$ would be a union of two countable sets (Theorem 3.1.8), countable by Proposition 3.1.5, against Theorem 3.3.4. An uncountable set is infinite, since finite sets are countable (Theorem 3.1.2). Now apply Exercise (B2: Absorbing a countable set) with $X := \mathbb{R} \setminus \mathbb{Q}$ and $C := \mathbb{Q}$, which is countable and disjoint from X: $|(\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q}| = |\mathbb{R} \setminus \mathbb{Q}|$, and the left side is $|\mathbb{R}|$.

3.6 Cardinal Arithmetic

Section 2.5 counted finite sets, and Section 2.3 proved the laws of powers $m^{n+k} = m^n m^k$ and $(m^n)^k = m^{nk}$ by induction (Proposition 2.3.4). For finite sets these numbers count functions: Y^X has m^n elements when Y has m and X has n (Section 1.5, before Example (All functions between two small sets)). This section asks what is left of that arithmetic when the sets are infinite and all we have are bijections.

3.6.1 The plane and the line

A square has two dimensions and a segment has one. Surely the plane $\mathbb{R} \times \mathbb{R}$ has more points than the line? The injection $x \mapsto (x, 0)$ gives $|\mathbb{R}| \leq |\mathbb{R} \times \mathbb{R}|$, and it seems that the other half of the plane should be left over.

A second question. Is $\mathbb{N}^{\mathbb{N}}$, the set of sequences of natural numbers, bigger than $\mathbb{R}$? A real number in $[0, 1)$ is only a sequence of digits below 10, while a sequence in $\mathbb{N}^{\mathbb{N}}$ may use any natural number at every place, so $\mathbb{N}^{\mathbb{N}}$ looks bigger.

Guess both answers before reading on. The plane is a product, $\mathbb{N}^{\mathbb{N}}$ is a power, and the line will turn out to be a power too: a power of 2.

3.6.2 Adding sizes: disjoint unions

For finite sets that do not meet, Section 2.5 added sizes by taking the union (Proposition 2.5.5). So define the sum of two sets as their union? With $A = B = \{0\}$ we want two elements, and $A \cup B = \{0\}$ has one. The union counts the shared element once. The cure is to tag every element with the name of the set it came from, so that the two copies cannot overlap.

A disjoint union keeps a labeled copy of each set, so nothing is counted twice.

Definition 3.6.1. Disjoint Union

Let A and B be sets. Their **disjoint union** is

$$A \sqcup B := (A \times \{0\}) \cup (B \times \{1\}).$$

The maps $\iota_A \colon A \to A \sqcup B$, $\iota_A(a) := (a, 0)$, and $\iota_B \colon B \to A \sqcup B$, $\iota_B(b) := (b, 1)$, are the **inclusions**.

In words: every element of $A \sqcup B$ is $(a, 0)$ with $a \in A$ or $(b, 1)$ with $b \in B$, and **not both**, since $(a, 0) = (b, 1)$ would give $0 = 1$ by the characteristic property of pairs (Definition 1.4.1). By the same property each inclusion is injective, the two images are disjoint, and together they make up $A \sqcup B$. So a function on $A \sqcup B$ may be defined by giving its values on the two tagged parts separately: these are the two cases that cannot overlap, as in the proof of Proposition 3.1.5.

Example. Two copies of $\mathbb{N}$

Show that $|\mathbb{N} \sqcup \mathbb{N}| = |\mathbb{N}|$.

Solution. This is the merging of two lists from the proof of Proposition 3.1.5, now as a bijection. Let $e(n, 0) := 2n$ and $e(n, 1) := 2n + 1$, for $n \in \mathbb{N}$; by the unwinding above this defines $e \colon \mathbb{N} \sqcup \mathbb{N} \to \mathbb{N}$. For the decoder, let $d(m) := (q, r)$, where $m = 2q + r$ with $q \in \mathbb{N}$ and $r \in \{0, 1\}$; the pair exists and is unique by the claim in that proof, and $(q, r) \in \mathbb{N} \sqcup \mathbb{N}$. Then $d(e(n, r)) = (n, r)$ by the uniqueness, and $e(d(m)) = 2q + r = m$. By Theorem 1.6.4, e is a bijection.

This is the first encoding of the section: e writes a pair as one number, and d reads it back. The method box comes with the next one.

Quick check.

(a) With $a \neq b$, list the elements of $\{a, b\} \sqcup \{a\}$ and of $\{a, b\} \cup \{a\}$. (b) What is $\emptyset \sqcup B$? (c) If $A \cap B = \emptyset$, give a bijection $A \cup B \to A \sqcup B$.

Solution.

(a) $\{a, b\} \sqcup \{a\} = \{(a, 0), (b, 0), (a, 1)\}$, three elements; $\{a, b\} \cup \{a\} = \{a, b\}$, two. (b) $\emptyset \sqcup B = B \times \{1\}$, since $\emptyset \times \{0\} = \emptyset$; and $b \mapsto (b, 1)$ is a bijection $B \to \emptyset \sqcup B$. (c) Send x to $(x, 0)$ if $x \in A$ and to $(x, 1)$ if $x \in B$. The cases do not overlap, since $A \cap B = \emptyset$, so this is a function. Its inverse sends $(a, 0) \mapsto a$ and $(b, 1) \mapsto b$.

Warning. **No subtraction.** For numbers, $m + k = n + k$ gives $m = n$. For sets, $|\{0\} \sqcup \mathbb{N}| = |\emptyset \sqcup \mathbb{N}|$ although $|\{0\}| \neq |\emptyset|$: the map sending $(0, 0) \mapsto 0$ and $(n, 1) \mapsto n + 1$ is a bijection

$\{0\} \sqcup \mathbb{N} \to \mathbb{N}$, and $(n, 1) \mapsto n$ is a bijection $\emptyset \sqcup \mathbb{N} \to \mathbb{N}$ (Exercise B4 (a) has the details). Every law below is proved by a bijection, never borrowed from the numbers.

3.6.3 Multiplying, raising to powers, and comparing

Products $A \times B$ (Definition 1.4.2) and sets of functions Y^X (Section 1.5) are the other two operations. If A has m elements and B has n, then $A \times B$ has mn elements and B^A has n^m, as Exercise C2 of Section 2.5 counts. The base is written on the line and the exponent is the domain: Y^X is the set of functions **from** X **to** Y.

Before any law, we check that the three operations see only sizes.

Proposition 3.6.1. Sums, Products and Powers Respect Size

Let A, A', B, B' be sets with $|A| = |A'|$ and $|B| = |B'|$. Then

(a) $|A \sqcup B| = |A' \sqcup B'|$;
(b) $|A \times B| = |A' \times B'|$;
(c) $\left|A^B\right| = \left|A'^{B'}\right|$.

Idea. Carry each element across along the bijections: on each tagged part for (a), on each coordinate for (b), and for (c) by composing a function with the bijections on both sides. The inverses carry everything back.

Proof. Let $\alpha\colon A \to A'$ and $\beta\colon B \to B'$ be bijections, with two-sided inverses α^{-1} and β^{-1} (Theorem 1.6.4).

(a) Send $(a, 0) \mapsto (\alpha(a), 0)$ and $(b, 1) \mapsto (\beta(b), 1)$; this is a function by the two-part rule after Definition 3.6.1. The same rule with α^{-1} and β^{-1} undoes it on each part, so it is a two-sided inverse.

(b) Send $(a, b) \mapsto (\alpha(a), \beta(b))$. The map $(a', b') \mapsto (\alpha^{-1}(a'), \beta^{-1}(b'))$ is a two-sided inverse, by Definition 1.4.1.

(c) For $f \in A^B$, the composite $\alpha \circ f \circ \beta^{-1}$ is a function $B' \to A'$. Let $\Theta(f) \coloneqq \alpha \circ f \circ \beta^{-1}$ and $\Lambda(g) \coloneqq \alpha^{-1} \circ g \circ \beta$ for $g \in A'^{B'}$. By Proposition 1.5.3 and $\alpha^{-1} \circ \alpha = \mathrm{id}_A$, $\beta^{-1} \circ \beta = \mathrm{id}_B$,

$$\Lambda(\Theta(f)) = (\alpha^{-1} \circ \alpha) \circ f \circ (\beta^{-1} \circ \beta) = f,$$

and $\Theta(\Lambda(g)) = g$ in the same way. In each part, Theorem 1.6.4 gives a bijection.

■

Remark. The proposition lets us replace either set by an equinumerous one without changing the size of the result. An answer computed from representatives must not depend on which representatives we used. Compare "send p/q to p" in Section 1.5 (Example (Relations that

are not functions)), which fails exactly this test.

The comparison $\leq$ of Definition 3.4.1 is respected as well, with one exception.

Proposition 3.6.2. Monotonicity

Let A, A', B, B' be sets with $|A| \leq |A'|$ and $|B| \leq |B'|$. Then

(a) $|A \sqcup B| \leq |A' \sqcup B'|$;
(b) $|A \times B| \leq |A' \times B'|$;
(c) if $A' \neq \emptyset$, then $\left|A^B\right| \leq \left|A'^{B'}\right|$.

Idea. Carry the injections across, as in the previous proof. For powers, a function on B must be extended to all of B', and the extension needs a value to put on the points that B does not reach.

Proof. Let $u\colon A \to A'$ and $v\colon B \to B'$ be injections. (a), (b): the maps of the previous proof with u, v in place of α, β are injective, by Definition 1.4.1.

(c) Fix $a_0 \in A'$. For $f \in A^B$ define $F(f)\colon B' \to A'$ by

$$F(f)(b') := \begin{cases} u(f(b)) & \text{if } b' = v(b) \text{ for some } b \in B, \\ a_0 & \text{if } b' \notin v(B). \end{cases}$$

In the first case b is unique, since v is injective, so $F(f)$ is a function. If $F(f) = F(g)$, then for every $b \in B$,

$$u(f(b)) = F(f)(v(b)) = F(g)(v(b)) = u(g(b)),$$

so $f(b) = g(b)$, since u is injective. Hence $f = g$ (Proposition 1.5.1), and F is an injection $A^B \to A'^{B'}$.

■

A non-example by minimal change. Drop "$A' \neq \emptyset$" from (c), and take $A = A' = \emptyset$, $B = \emptyset$, $B' = \{0\}$. Then $|B| \leq |B'|$, but $\emptyset^\emptyset$ has one element, the empty function (Proposition 1.5.2), while $\emptyset^{\{0\}} = \emptyset$; there is no injection from a one-element set into $\emptyset$. The proof used a_0 exactly once, and here there is no a_0. (If $A' = \emptyset$, then $A = \emptyset$ too, since a function into $\emptyset$ has empty domain.)

Quick check. Where does the proof of (c) use that v is injective? Where does it use that u is injective?

Solution. Injectivity of v makes $F(f)$ a function: the point b with $v(b) = b'$ must be unique. Injectivity of u makes F injective: $u(f(b)) = u(g(b))$ must give $f(b) = g(b)$.

3.6.4 Encoding: the diagonals of $\mathbb{N} \times \mathbb{N}$

Section 3.1 showed $\mathbb{N} \times \mathbb{N}$ countable by an injection. At the scratch work for Theorem 3.1.6 it set aside the list along the diagonals, because writing a formula for the position of (m, n) and checking that every position is used takes real work. The Quick check before 3.4's Looking-ahead remark got $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ from Theorem 3.4.3 without ever seeing a bijection. Here is the work, done.

For $s \in \mathbb{N}$, the **triangular number** $\tau_s \coloneqq \sum_{i=1}^{s} i$ (Definition 2.3.1) has $\tau_0 = 0$ and $\tau_{s+1} = \tau_s + s + 1$. It counts the points on the diagonals $m + n = 0, 1, \ldots, s - 1$, which hold $1, 2, \ldots, s$ points.

Example. The diagonal pairing of $\mathbb{N} \times \mathbb{N}$ with $\mathbb{N}$

Show that $\pi(m, n) \coloneqq \tau_{m+n} + n$ is a bijection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

Idea (Scratch work). What must the code record? Which diagonal the point is on, $s = m+n$, and its place on that diagonal, $n \in \{0, \ldots, s\}$; from s and n we read back $m = s - n$. The diagonals before diagonal s hold $1 + 2 + \cdots + s = \tau_s$ points, so the code counts them and adds the place. Small values: diagonal 0 gives 0; diagonal 1 gives $1, 2$; diagonal 2 gives $3, 4, 5$. The decoder must find, for each k, the diagonal it falls on.

Givens	Goal
$(m, n) \in \mathbb{N} \times \mathbb{N}$	$\pi(m, n) \in \mathbb{N}$
$k \in \mathbb{N}$	exactly one (m, n) with $\tau_{m+n} + n = k$
gap	every $k \in \mathbb{N}$ is $\tau_s + n$ with $s, n \in \mathbb{N}$, $n \leq s$, in exactly one way

Existence by induction on k: stepping from k to $k+1$ moves one place along the diagonal, or, at its end, to the start of the next one. Uniqueness: diagonal s fills the block $\tau_s, \ldots, \tau_s + s$, just below τ_{s+1}, so different diagonals give different numbers.

Solution.

Claim. For every $k \in \mathbb{N}$ there are $s, n \in \mathbb{N}$ with $n \leq s$ and $k = \tau_s + n$, and the pair (s, n) is unique.

Proof. Existence, by Theorem 2.2.1 from 0. First, $0 = \tau_0 + 0$. Suppose $k = \tau_s + n$ with $n \leq s$. If $n < s$, then $k + 1 = \tau_s + (n + 1)$ with $n + 1 \leq s$. If $n = s$, then $k + 1 = \tau_s + s + 1 = \tau_{s+1} + 0$.

Uniqueness. First, $\tau_{j+1} = \tau_j + j + 1 > \tau_j$ for every j, so if $s < s'$, then $\tau_{s+1} \leq \tau_{s'}$, by Theorem 2.2.1 on s' from $s+1$. Now let $\tau_s + n = \tau_{s'} + n'$ with $n \leq s$ and $n' \leq s'$, and suppose $s \neq s'$; by symmetry $s < s'$. Then

$$\tau_s + n \leq \tau_s + s < \tau_{s+1} \leq \tau_{s'} \leq \tau_{s'} + n',$$

a contradiction. So $s = s'$, and then $n = n'$.

■

The bijection. $\pi(m,n) \in \mathbb{N}$, since $\tau_{m+n} \in \mathbb{N}$, by Theorem 2.2.1 on s from $\tau_0 = 0$ and $\tau_{s+1} = \tau_s + s + 1$ with Lemma 2.1.1 (b). For $k \in \mathbb{N}$, write $k = \tau_s + n$ by the claim and set $\delta(k) := (s-n, n)$, where $s - n \in \mathbb{N}$ because $n \leq s$ (Lemma 2.1.1 (d)); the uniqueness in the claim makes δ a function. Then $\pi(\delta(k)) = \tau_{(s-n)+n} + n = \tau_s + n = k$. And $\delta(\pi(m,n)) = (m,n)$, by the uniqueness applied to $k = \tau_{m+n} + n$, where $s = m+n \geq n$. By Theorem 1.6.4, π is a bijection.

A table of the first values: $\pi(0,0) = 0$, $\pi(1,0) = 1$, $\pi(0,1) = 2$, $\pi(2,0) = 3$, $\pi(1,1) = 4$, $\pi(0,2) = 5$. Decoding 11: $\tau_4 = 10 \leq 11 < 15 = \tau_5$, so $11 = \tau_4 + 1$ and $\delta(11) = (3,1)$.

Example. Method: build a bijection by encoding and decoding

Template. (1) Say what an element of the source must record for nothing to be lost. (2) Choose a code: a rule sending each element to an element of the target, and check that it lands there. (3) Write the decoder: a rule reading an element of the source back from each element of the target, and check that it is a function, with exactly one answer for each input. (4) Check both round trips and cite Theorem 1.6.4.

When to use it. The two sets carry the same information arranged differently: two numbers in one, a pair of sequences in one sequence, a function of two variables as a function with function values.

The usual failure. Checking one round trip only: $\delta \circ \pi = \mathrm{id}$ alone shows only that π is injective (Theorem 1.6.1). A decoder that is not a function, with two readings of one code or none (the interleaving of decimals, later in this section). If the decoder works on part of the target only, keep the injection and use Example (Method: injections both ways).

Warning. An injective code is not yet a bijection. The code $2^m 3^n$ of Theorem 3.1.6 is injective, but 5 is not a value, and no decoder is defined at 5. Step (3) of the method, a decoder defined on the **whole** target, is what makes π a bijection.

Quick check. Compute $\pi(3,2)$ and $\delta(47)$.

Solution. $\pi(3,2) = \tau_5 + 2 = 15 + 2 = 17$. For 47: $\tau_9 = 45 \leq 47 < 55 = \tau_{10}$, so $47 = \tau_9 + 2$, and $\delta(47) = (9-2, 2) = (7,2)$. Check: $\pi(7,2) = \tau_9 + 2 = 47$.

3.6.5 The laws of exponents, for all sets

For numbers, $m^{n+k} = m^n m^k$ and $(m^n)^k = m^{nk}$. Read through the sets these numbers count, each law says that two sets of functions are the same size, and for sets we must find the bijection.

Theorem 3.6.3. Laws of Cardinal Arithmetic

For all sets A, B, C, X, Y, Z:

(a) $|A \sqcup B| = |B \sqcup A|$, $|(A \sqcup B) \sqcup C| = |A \sqcup (B \sqcup C)|$, $|A \times B| = |B \times A|$ and $|(A \times B) \times C| = |A \times (B \times C)|$;

(b) $|A \times (B \sqcup C)| = |(A \times B) \sqcup (A \times C)|$;

(c) $X^{\emptyset}$ has exactly one element, and $\left|X^{\{0\}}\right| = |X|$;

(d) $\left|X^{Y \sqcup Z}\right| = \left|X^Y \times X^Z\right|$;

(e) $\left|(X \times Y)^Z\right| = \left|X^Z \times Y^Z\right|$;

(f) $\left|(X^Y)^Z\right| = \left|X^{Y \times Z}\right|$.

Idea (Scratch work). For (d): what is an element of each side? On the left, a function h defined on the tagged copies of Y and Z. On the right, a pair (f, g) with $f\colon Y \to X$ and $g\colon Z \to X$. A function on two disjoint pieces is the same thing as a function on each piece. So cut h into its two pieces by composing with the inclusions, and glue a pair back together piece by piece.

Givens	Goal
$h \in X^{Y \sqcup Z}$	an element of $X^Y \times X^Z$: $(h \circ \iota_Y, h \circ \iota_Z)$
$(f, g) \in X^Y \times X^Z$	one h with $h \circ \iota_Y = f$ and $h \circ \iota_Z = g$
gap	$h(y, 0) \coloneqq f(y)$, $h(z, 1) \coloneqq g(z)$ is a function: the parts do not overlap (after Definition 3.6.1)

Proof.

(d) Let $\Phi(h) \coloneqq (h \circ \iota_Y, h \circ \iota_Z)$ for $h \in X^{Y \sqcup Z}$. For $(f, g) \in X^Y \times X^Z$, let $\Psi(f, g)$ be the function $h\colon Y \sqcup Z \to X$ with

$$h(y, 0) \coloneqq f(y), \qquad h(z, 1) \coloneqq g(z) \qquad (y \in Y,\ z \in Z).$$

This is a function, because every element of $Y \sqcup Z$ has exactly one of the two forms. Then $\Phi(\Psi(f, g)) = (f, g)$: for $y \in Y$, $h(\iota_Y(y)) = h(y, 0) = f(y)$, so $h \circ \iota_Y = f$ by Proposition 1.5.1, and likewise $h \circ \iota_Z = g$; the pairs are equal by Definition 1.4.1. And $\Psi(\Phi(h)) = h$: the two functions agree at every $(y, 0)$ and every $(z, 1)$, which are all the points of $Y \sqcup Z$, so they are equal by Proposition 1.5.1. By Theorem 1.6.4, Φ is a bijection.

(e) For $g \in (X^Y)^Z$, each $g(z)$ is a function $Y \to X$. Let $\Phi(g)\colon Y \times Z \to X$, $\Phi(g)(y, z) \coloneqq g(z)(y)$. For $h \in X^{Y \times Z}$ and $z \in Z$, the rule $y \mapsto h(y, z)$ is an element of X^Y; let $\Psi(h)\colon Z \to X^Y$ send z to it. Then

$$\Phi(\Psi(h))(y, z) = \Psi(h)(z)(y) = h(y, z)$$

for all (y, z), so $\Phi(\Psi(h)) = h$. And $\Psi(\Phi(g))(z)$ is the function $y \mapsto g(z)(y)$, which is $g(z)$; so $\Psi(\Phi(g)) = g$. Here Proposition 1.5.1 is used twice: first for functions on Y, then for functions on Z. By Theorem 1.6.4, Φ is a bijection.

The remaining parts are proved by the same kind of regrouping; the maps are in the fold below.

■

Second reading · *The other laws*

Each map below has the stated inverse, and each round trip is one line of Proposition 1.5.1 and Definition 1.4.1. As a sample, the associativity of $\sqcup$ has three cases, one for each form of element; on $((b,1),0)$ the map gives $((b,0),1)$, and the inverse, reading the tag 1 outside and the tag 0 inside, returns $((b,1),0)$.

(a) $A \sqcup B \to B \sqcup A$: $(a,0) \mapsto (a,1)$, $(b,1) \mapsto (b,0)$; it is its own inverse, with the roles of A and B exchanged. $(A \sqcup B) \sqcup C \to A \sqcup (B \sqcup C)$: $((a,0),0) \mapsto (a,0)$, $((b,1),0) \mapsto ((b,0),1)$, $(c,1) \mapsto ((c,1),1)$; the three forms of the source do not overlap, and the inverse reads the three forms of the target back. $A \times B \to B \times A$: $(a,b) \mapsto (b,a)$. $(A \times B) \times C \to A \times (B \times C)$: $((a,b),c) \mapsto (a,(b,c))$, with inverse $(a,(b,c)) \mapsto ((a,b),c)$.

(b) $A \times (B \sqcup C) \to (A \times B) \sqcup (A \times C)$: $(a,(b,0)) \mapsto ((a,b),0)$ and $(a,(c,1)) \mapsto ((a,c),1)$; the inverse moves the tag back inside.

(c) $X^{\emptyset} = \{(\emptyset, X)\}$, the empty function, by Proposition 1.5.2 (a). The map $f \mapsto f(0)$ is a bijection $X^{\{0\}} \to X$, with inverse sending x to the function $0 \mapsto x$.

(d) Let $p_1(x,y) \coloneqq x$ and $p_2(x,y) \coloneqq y$ on $X \times Y$. The map $h \mapsto (p_1 \circ h, p_2 \circ h)$ from $(X \times Y)^Z$ to $X^Z \times Y^Z$ has the inverse $(f,g) \mapsto (z \mapsto (f(z), g(z)))$.

Law (f) is called **currying**: a function of two variables becomes a function whose values are functions. For finite sets with m, n and k elements, the theorem gives back $m^{n+k} = m^n m^k$ and $(m^n)^k = m^{nk}$ with no induction in sight; the induction has moved into the counting of Section 2.5. Nothing in the proof used finiteness.

Example. Method: prove a law of sizes by a bijection of sets

Template. (1) Write out what an element of each side is: a tagged element, a pair, a function, a function with function values. (2) Find the map that only regroups: compose with the inclusions, pair the coordinates, or curry. (3) Write the reverse regrouping. (4) Check both round trips with Proposition 1.5.1 and Definition 1.4.1, and cite Theorem 1.6.4.

When to use it. A law familiar from numbers, such as $m^{n+k} = m^n m^k$, is claimed for sets of any size; or a size is to be computed by rewriting a set step by step.

The usual failure. Computing with symbols, as in "$|X|^{|Y|+|Z|} = |X|^{|Y|}\,|X|^{|Z|}$", when no number $|X|$ exists and the step is the law itself: (N9) of Logic and Proof, Example (What is not allowed). Dropping the tags: with $\cup$ in place of $\sqcup$ the law fails: for $X = \{0,1\}$ and $Y = Z = \{0\}$, $X^{Y \cup Z}$ has 2 elements and $X^Y \times X^Z$ has 4 (Exercise B4 (b)).

Quick check. Let $X = \{0,1\}$, $Y = \{a\}$ and $Z = \{b,c\}$. How many elements has each side of (d)? Let $h(a,0) = 1$, $h(b,1) = 0$, $h(c,1) = 1$. What is $\Phi(h)$?

Solution. $Y \sqcup Z = \{(a,0),(b,1),(c,1)\}$ has three elements, and a function from it to $\{0,1\}$ is fixed by three values, each 0 or 1: $2 \cdot 2 \cdot 2 = 8$ functions. On the right, X^Y has 2 elements and X^Z has 4, so the product has $2 \cdot 4 = 8$. And $\Phi(h) = (f,g)$ with $f(a) = 1$, $g(b) = 0$, $g(c) = 1$.

3.6.6 Subsets are 0–1 functions

Section 1.5 stated, for every set, that subsets and 0–1 functions match, and gave both maps: send f to $\{x : f(x) = 1\}$ and A to $\mathbf{1}_A$. Here are the two round trips, which make 2 a base like any other.

Theorem 3.6.4. Subsets and 0–1 Functions

For every set X, the map $A \mapsto \mathbf{1}_A$ is a bijection $\mathcal{P}(X) \to \{0,1\}^X$, with inverse $f \mapsto \{x \in X : f(x) = 1\}$. In particular $|\mathcal{P}(X)| = \left|\{0,1\}^X\right|$.

Proof. For $A \subseteq X$, $\mathbf{1}_A \in \{0,1\}^X$ (Example (First functions) (d)), and $\{x \in X : \mathbf{1}_A(x) = 1\} = A$ by the definition of $\mathbf{1}_A$. For $f \in \{0,1\}^X$, let $S \coloneqq \{x \in X : f(x) = 1\}$. For $x \in S$, $\mathbf{1}_S(x) = 1 = f(x)$. For $x \in X \setminus S$, $f(x) \neq 1$, so $f(x) = 0 = \mathbf{1}_S(x)$. So $\mathbf{1}_S = f$ (Proposition 1.5.1). By Theorem 1.6.4, $A \mapsto \mathbf{1}_A$ is a bijection. ■

Section 2.5 (the fold after Proposition 2.5.8), Section 3.3 (after Corollary 3.3.3) and Section 3.4 (the Quick check after Proposition 3.4.2) quoted this correspondence; it is now a theorem to cite.

Corollary 3.6.5. No Set Is the Size of Its 0–1 Functions

For every set X, $|X| < \left|\{0,1\}^X\right|$.

Idea. One injection is easy; for strictness, move a bijection over to $\mathcal{P}(X)$ with the theorem just proved, where Cantor's theorem forbids it.

Proof. The map $x \mapsto \mathbf{1}_{\{x\}}$ is injective, since $\mathbf{1}_{\{x\}}$ takes the value 1 at x only; so $|X| \leq \left|\{0,1\}^X\right|$. A bijection $X \to \{0,1\}^X$, followed by the inverse of the bijection of Theorem 3.6.4, would be a bijection $X \to \mathcal{P}(X)$ (Theorem 1.5.4 (c)), in particular a surjection, against Theorem 3.3.2. ■

So $\mathbb{N}$, $\{0,1\}^{\mathbb{N}}$, $\{0,1\}^{\{0,1\}^{\mathbb{N}}}$, ... grow strictly at each step, and there is no largest size.

3.6.7 No set of all sets, once more

Section 3.3 (consequence (i) after Theorem 3.3.2) saw that Russell's argument is Cantor's, with the rule $f(x) = x$ and R_A in the role of D. What is new here is a proof **by sizes** of the last clause of Theorem 1.2.4: there is no set of which every set is an element.

Suppose U were such a set. Every subset of U is a set, hence an element of U, so $\mathcal{P}(U) \subseteq U$. Define $f\colon U \to \mathcal{P}(U)$ by $f(u) := u$ if $u \in \mathcal{P}(U)$, and $f(u) := \emptyset$ otherwise. It is onto: each $S \in \mathcal{P}(U)$ lies in U, and $f(S) = S$. This contradicts Theorem 3.3.2.

Cantor's set for this f, $D = \{u \in U : u \notin f(u)\}$, agrees with $R_U = \{u \in U : u \notin u\}$ on $\mathcal{P}(U)$, and contains every $u \in U \setminus \mathcal{P}(U)$, since $u \notin \emptyset$. The unrestricted collection $\{x : x \notin x\}$ is never formed.

3.6.8 The size of the line

The hook asked about $\mathbb{R} \times \mathbb{R}$; first $\mathbb{R}$ itself. A real number in $[0, 1)$ is a digit sequence, a function $\mathbb{Z}_{>0} \to \{0, \dots, 9\}$. So $\mathbb{R}$ should be a power, and that power should be a power of 2.

Theorem 3.6.6. The Line Is a Power of Two

$|\mathbb{R}| = \left|\{0,1\}^{\mathbb{N}}\right| = |\mathcal{P}(\mathbb{N})|$.

Idea. Injections both ways (Example (Method: injections both ways)). Into the 0–1 sequences, the digits are encoded and the laws do the bookkeeping. Out of them, a 0–1 sequence is read as decimal digits 0 and 1, which contain no 9.

Proof. Let $T := \{0, 1, \dots, 9\}$ and $W := T^{\mathbb{Z}_{>0}}$, the set of digit sequences (Definition 3.3.1).

$|[0,1)| \le |W|$. This is the step of the proof of Theorem 3.3.4. Send x to its expansion not ending in all 9s: one exists by (D1), and only one by (D3), so the rule is a function and no choice is made. It is injective, since a digit sequence is an expansion of only one number, by (D2).

$|W| \le \left|\{0,1\}^{\mathbb{N}}\right|$. The map $n \mapsto n + 1$ is a bijection $\mathbb{N} \to \mathbb{Z}_{>0}$ (inverse $m \mapsto m - 1$, Lemma 2.1.1 (c)), so $|W| = \left|T^{\mathbb{N}}\right|$ (Proposition 3.6.1 (c)). The map $j \mapsto \mathbf{1}_{\{j\}}$ injects T into $\{0,1\}^T$, so $\left|T^{\mathbb{N}}\right| \le \left|(\{0,1\}^T)^{\mathbb{N}}\right|$ (Proposition 3.6.2 (c), as $\{0,1\}^T \neq \emptyset$), and this is $\left|\{0,1\}^{T \times \mathbb{N}}\right|$ by Theorem 3.6.3 (f). A pair (j, n) is recorded by one number, by the method of Example (Method: build a bijection by encoding and decoding): the code $(j, n) \mapsto 10n + j$ is a bijection $T \times \mathbb{N} \to \mathbb{N}$, whose decoder takes quotient and remainder on division by 10 (Theorem 2.2.3, with the quotient in $\mathbb{N}$ as in the claim in the proof of Proposition 3.1.5). So $\left|\{0,1\}^{T \times \mathbb{N}}\right| = \left|\{0,1\}^{\mathbb{N}}\right|$ (Proposition 3.6.1 (c)). Composing the maps gives an injection $W \to \{0,1\}^{\mathbb{N}}$ (Theorem 1.5.4 (a)).

$\left|\{0,1\}^{\mathbb{N}}\right| \le |[0,1)|$. For $b \in \{0,1\}^{\mathbb{N}}$, let $c_{k+1} := b(k)$ for $k \in \mathbb{N}$: a digit sequence with digits 0 and 1 only. By (D2) it is an expansion of exactly one $y_b \in [0,1]$, and $y_b \le t_1 + \frac{1}{10} \le \frac{2}{10}$ by Definition 3.3.1 at $n = 1$, so $y_b \in [0,1)$. If $b \neq b'$, the two digit sequences differ. If also

$y_b = y_{b'}$, they would be two different expansions of one number, and by (D3) one of them would end in all 9s; but neither contains a 9. So $y_b \neq y_{b'}$, and $b \mapsto y_b$ is injective.

Conclusion. By Proposition 3.4.1 (b) and Theorem 3.4.3, $|[0,1)| = \left|\{0,1\}^{\mathbb{N}}\right|$. By Example (The real line and its intervals), $|[0,1)| = |\mathbb{R}|$, and by Theorem 3.6.4, $\left|\{0,1\}^{\mathbb{N}}\right| = |\mathcal{P}(\mathbb{N})|$. Chaining with Proposition 2.5.1 proves the theorem.

■

The first step is the one of Exercise C1 of Section 3.4. What is new is the middle step, where the laws reduce the bookkeeping to the one-line code $(j,n) \mapsto 10n + j$ in place of the set $E(x)$ of that exercise, and the last, where the digits 0 and 1 suffice because (D3) needs only that no 9 appears. Neither step needed binary expansions of real numbers.

Remark (Notation in other books). Many books treat sizes as objects, called **cardinal numbers**, and write $\aleph_0$ for the size of $\mathbb{N}$ and $2^{\aleph_0}$, or $\mathfrak{c}$, for the size of $\mathbb{R}$. Making a size into an object needs more set theory than this book uses (Section 2.5, the fold after Proposition 2.5.1). Here "$|A| = 2^{\aleph_0}$" can be read only as shorthand for $|A| = \left|\{0,1\}^{\mathbb{N}}\right|$. Whether some subset of $\mathbb{R}$ is strictly bigger than $\mathbb{N}$ and strictly smaller than $\mathbb{R}$ is the **continuum hypothesis**; it is known to be neither provable nor refutable from the usual axioms of set theory, if those axioms are consistent.

Quick check. Which step of the proof of Theorem 3.6.6 uses the axiom of choice?

Solution. None. The expansion of x is picked by a rule ("the one not ending in all 9s"), every other map is a formula, and Theorem 3.4.3 was proved without choice (Section 3.4).

3.6.9 Back to the plane

Example. Interleaving digits

The natural map $[0,1) \times [0,1) \to [0,1)$ interleaves digits. If $x = 0.a_1a_2\ldots$ and $y = 0.b_1b_2\ldots$, with the expansions not ending in all 9s, let

$$F(x,y) \coloneqq 0.a_1b_1a_2b_2\ldots;$$

the inverse splits the digits of z into the odd and the even places. Is F a bijection?

Solution. F is a function into $[0,1)$. The expansions of x and y are fixed by the rule, as in the last proof. Let c be the interleaved sequence: $c_{2k-1} \coloneqq a_k$, $c_{2k} \coloneqq b_k$. It has infinitely many places that are not 9 (those of a), so it does not end in all 9s, and by (D2) it is an expansion of exactly one $z \in [0,1]$. To see $z < 1$, let n be the first place with $c_n \leq 8$ (Theorem 2.1.3).

Every earlier digit is 9, so by Proposition 2.3.6

$$t_n \le (1 - 10^{-(n-1)}) + 8 \cdot 10^{-n} = 1 - 2 \cdot 10^{-n},$$

and $z \le t_n + 10^{-n} \le 1 - 10^{-n} < 1$.

F is injective. If $F(x, y) = F(x', y') = z$, both interleaved sequences are expansions of z and neither ends in all 9s, so by (D3) they are equal. Then $a = a'$ and $b = b'$, and $x = x'$, $y = y'$ by (D2).

F is not onto. Take $z = \frac{1}{11} = 0.090909\ldots$. The truncations at even places are $t_{2j} = \frac{9}{99}(1 - 100^{-j}) = \frac{1}{11} - \frac{1}{11}100^{-j}$ (Proposition 2.3.6 with $r = \frac{1}{100}$), and the inequalities of Definition 3.3.1 hold at every place. This expansion has no tail of 0s and no tail of 9s, so by (D3) it is the only expansion of $\frac{1}{11}$. A preimage (x, y) would need $b = 9, 9, 9, \ldots$; but b was the expansion of y not ending in all 9s.

The splitting "inverse" named "the $y \in [0, 1)$ whose expansion is $999\ldots$" without checking that such a y exists: that is (N14) of Logic and Proof, Example (What is not allowed). So the direct route gives an injection and no bijection. The injection is enough (Example (Method: injections both ways)), and the laws give a bijection with no digit-fiddling.

Theorem 3.6.7. The Plane Is the Size of the Line

$|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$.

Idea. By the method of Example (Method: prove a law of sizes by a bijection of sets): replace $\mathbb{R}$ by $\{0, 1\}^{\mathbb{N}}$ and rewrite the plane step by step.

Proof. By Theorem 3.6.6 and Proposition 3.6.1 (b), $|\mathbb{R} \times \mathbb{R}| = \left|\{0, 1\}^{\mathbb{N}} \times \{0, 1\}^{\mathbb{N}}\right|$. By Theorem 3.6.3 (d), this is $\left|\{0, 1\}^{\mathbb{N} \sqcup \mathbb{N}}\right|$. By Example (Two copies of $\mathbb{N}$) and Proposition 3.6.1 (c), this is $\left|\{0, 1\}^{\mathbb{N}}\right|$, which is $|\mathbb{R}|$ by Theorem 3.6.6. Chaining with Proposition 2.5.1 proves the theorem.

■

Read through the maps, the composite on 0–1 sequences sends (a, b) to the sequence with $a(n)$ at place $2n$ and $b(n)$ at place $2n + 1$: the interleaving of Exercise B3 of Section 3.4. The trouble with decimals has gone because 0–1 sequences, unlike numbers, have no double expansions. That price is paid once, in the proof of Theorem 3.6.6.

Theorem 3.6.8. Sequences of Natural Numbers

$\left|\mathbb{N}^{\mathbb{N}}\right| = |\mathbb{R}|$.

Idea. By the method of Example (Method: prove a law of sizes by a bijection of sets), with injections both ways: a 0–1 sequence is already a sequence of natural numbers, and a natural number is recorded by a 0–1 sequence.

Proof. Send $b \in \{0,1\}^{\mathbb{N}}$ to the same rule with codomain $\mathbb{N}$. This map is injective: two sequences with the same image have the same value at every point, so they are equal (Proposition 1.5.1). In the other direction, $n \mapsto \mathbf{1}_{\{n\}}$ is an injection $\mathbb{N} \to \{0,1\}^{\mathbb{N}}$, so $\left|\mathbb{N}^{\mathbb{N}}\right| \leq \left|(\{0,1\}^{\mathbb{N}})^{\mathbb{N}}\right|$ (Proposition 3.6.2 (c), as $\{0,1\}^{\mathbb{N}} \neq \emptyset$). This is $\left|\{0,1\}^{\mathbb{N}\times\mathbb{N}}\right|$ (Theorem 3.6.3 (f)), and that is $\left|\{0,1\}^{\mathbb{N}}\right|$ by Example (The diagonal pairing of $\mathbb{N} \times \mathbb{N}$ with $\mathbb{N}$) and Proposition 3.6.1 (c). By Proposition 3.4.1 (b) and Theorem 3.4.3, $\left|\mathbb{N}^{\mathbb{N}}\right| = \left|\{0,1\}^{\mathbb{N}}\right|$, which is $|\mathbb{R}|$ by Theorem 3.6.6.

■

Exercise B4 (d) of Section 3.4 reached the equality $\left|\mathbb{N}^{\mathbb{N}}\right| = \left|\{0,1\}^{\mathbb{N}}\right|$ through graphs and $\mathcal{P}(\mathbb{N} \times \mathbb{N})$.

Corollary 3.6.9. Sequences of Real Numbers

$\left|\mathbb{R}^{\mathbb{N}}\right| = |\mathbb{R}|$.

Proof. In one chain,

$$\begin{aligned}\left|\mathbb{R}^{\mathbb{N}}\right| &= \left|(\{0,1\}^{\mathbb{N}})^{\mathbb{N}}\right| = \left|\{0,1\}^{\mathbb{N}\times\mathbb{N}}\right| \\ &= \left|\{0,1\}^{\mathbb{N}}\right| = |\mathbb{R}|\,,\end{aligned}$$

by Proposition 3.6.1 (c) with Theorem 3.6.6, then Theorem 3.6.3 (f), then Example (The diagonal pairing of $\mathbb{N} \times \mathbb{N}$ with $\mathbb{N}$) with Proposition 3.6.1 (c), and Theorem 3.6.6 again, chained by Proposition 2.5.1. No further appeal to Theorem 3.4.3 is needed beyond the one inside Theorem 3.6.6.

■

So both guesses of the hook were wrong. The plane is no bigger than the line, and $\mathbb{N}^{\mathbb{N}}$ is no bigger either. For every infinite set X it is in fact true that $|X \times X| = |X|$ and $|X \sqcup X| = |X|$; in general these cannot be proved without the axiom of choice (the first is equivalent to it), and this book does not prove them.

Quick check. Show that $\left|\mathbb{R}^{\mathbb{N}} \times \mathbb{R}\right| = |\mathbb{R}|$.

Solution. By Corollary 3.6.9 and Proposition 3.6.1 (b), $\left|\mathbb{R}^{\mathbb{N}} \times \mathbb{R}\right| = |\mathbb{R} \times \mathbb{R}|$, which is $|\mathbb{R}|$ by Theorem 3.6.7; chain with Proposition 2.5.1.

Remark (Looking ahead). Respecting size, Proposition 3.6.1, is an instance of a requirement that Section 4.2 names: a rule stated through representatives must give the same answer for all of them. There it is called well-definedness, and it is what makes functions on quotient sets possible.

3.6.10 Exercises

3.6.10.1 A. Check your understanding

Exercise. A1

(a) True or false, for every set A: $|\emptyset \sqcup A| = |A|$; $\emptyset \times A = \emptyset$; $A^{\emptyset}$ has exactly one element; $\emptyset^{A} = \emptyset$.

(b) Under the bijection of Theorem 3.6.3 (f) with $X = Y = \{0, 1\}$ and $Z = \{0\}$, which element of $(X^{Y})^{Z}$ corresponds to $h(y, z) \coloneqq y$?

(c) Give an injection $\mathbb{R} \sqcup \mathbb{N} \to \mathbb{R}$.

(d) The proof of Theorem 3.6.6 reads a 0–1 sequence as decimal digits 0 and 1. Which other pairs of digits give an injection into $[0, 1)$ in the same way? Why does the pair 0 and 9 not follow from (D3) alone?

Solution.

(a) True: $\emptyset \sqcup A = A \times \{1\}$, and $(a, 1) \mapsto a$ is a bijection onto A. True: no pair has a first coordinate in $\emptyset$. True, by Proposition 1.5.2 (a). False: for $A = \emptyset$, $\emptyset^{\emptyset}$ has one element, the empty function; the claim holds for every non-empty A, by Proposition 1.5.2 (b).

(b) The g with $g(0) = \mathrm{id}_{\{0,1\}}$, since $g(0)(y) = h(y, 0) = y$ for both $y \in \{0, 1\}$.

(c) Send $(x, 0) \mapsto x/(1 + |x|)$, which lies in $(-1, 1)$ (Example (The real line and its intervals)), and $(n, 1) \mapsto n + 1 \geq 1$. Each part is injective (the first is a bijection onto $(-1, 1)$, the second cancels the 1), and the values of the two parts are disjoint, so the map is injective.

(d) Any pair that misses 9 works unchanged: a sequence with no 9s cannot end in all 9s, so (D3) rules out two different expansions of one number, and the first digit is at most 8, so $y_b \leq \frac{8}{10} + \frac{1}{10} < 1$. Any pair that misses 0 gives an injection too, since a sequence with no 0s cannot end in all 0s; but if the pair contains 9, the sequence of all 9s goes to 1, so the target must be widened to $[0, 1]$, which Example (The real line and its intervals) also covers. (The digits 1 and 2, used in Exercise C1 of Section 3.4, miss both.) With the digits 0 and 9, one sequence could end in all 9s and another in all 0s, which is exactly the situation (D3) allows; so (D3) alone does not decide whether $b \mapsto y_b$ is injective, and a further computation at the first differing place would be needed.

3.6.10.2 B. Practice

Exercise. B1: Encodings

Prove each equality by an explicit bijection and its inverse.

(a) $|\mathbb{N} \times \{0,1,2\}| = |\mathbb{N}|$.

(b) $\left|\{0,1\}^{\mathbb{N}}\right| = \left|\{0,1,2,3\}^{\mathbb{N}}\right|$.

(c) $|\mathbb{N} \times \mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, using the pairing π of Example (The diagonal pairing of $\mathbb{N} \times \mathbb{N}$ with $\mathbb{N}$) twice, with an explicit decoder.

Solution.

(a) Send $(n, r) \mapsto 3n + r$. The inverse sends m to (q, r), the quotient and remainder of m on division by 3 (Theorem 2.2.3, with $q \in \mathbb{N}$ as in the claim in the proof of Proposition 3.1.5). Both round trips follow from the uniqueness in the division algorithm.

(b) For $c \in \{0,1\}^{\mathbb{N}}$ let $\Phi(c)(n) := 2c(2n) + c(2n+1) \in \{0,1,2,3\}$. For the inverse, given $d \in \{0,1,2,3\}^{\mathbb{N}}$, write $d(n) = 2q_n + r_n$ with $q_n, r_n \in \{0,1\}$ (division by 2, unique), and set $c(2n) := q_n$, $c(2n+1) := r_n$. This defines c on all of $\mathbb{N}$, since each $m \in \mathbb{N}$ is $2n$ or $2n+1$ for exactly one n. The round trips follow from the two uniqueness statements and Proposition 1.5.1.

(c) Let $E(m, n, k) := \pi(\pi(m, n), k)$. The decoder sends k' to (m, n, k), where $\delta(k') = (j, k)$ and $\delta(j) = (m, n)$. The round trips follow from $\delta \circ \pi = \mathrm{id}$ and $\pi \circ \delta = \mathrm{id}$, each used twice, together with the characteristic property of triples (the paragraph after the proof of Corollary 3.1.7). For example, $E(1,0,1) = \pi(\pi(1,0),1) = \pi(1,1) = 4$.

Exercise. B2: More laws

By the method of Example (Method: prove a law of sizes by a bijection of sets), prove for all sets A, B, X:

(a) $|\mathcal{P}(A \sqcup B)| = |\mathcal{P}(A) \times \mathcal{P}(B)|$;

(b) $\left|X^{\{0,1\}}\right| = |X \times X|$.

Solution.

(a) Directly: send $S \mapsto (\{a \in A : (a,0) \in S\}, \{b \in B : (b,1) \in S\})$, with inverse $(S_1, S_2) \mapsto (S_1 \times \{0\}) \cup (S_2 \times \{1\})$. The round trips hold because every element of $A \sqcup B$ is $(a,0)$ or $(b,1)$, and not both (after Definition 3.6.1). Or by laws: $|\mathcal{P}(A \sqcup B)| = \left|\{0,1\}^{A \sqcup B}\right|$ by Theorem 3.6.4, which is $\left|\{0,1\}^A \times \{0,1\}^B\right|$ by Theorem 3.6.3 (d), which is $|\mathcal{P}(A) \times \mathcal{P}(B)|$ by Theorem 3.6.4 twice with Proposition 3.6.1 (b).

(b) Send $f \mapsto (f(0), f(1))$, with inverse sending (x, x') to the function $0 \mapsto x$, $1 \mapsto x'$. Or from (c) and (d) of Theorem 3.6.3, since $\{0,1\}$ is the same size as $\{0\} \sqcup \{0\}$, by $0 \mapsto (0,0)$, $1 \mapsto (0,1)$.

Exercise. B3: Sets the size of the line, used later

Prove:

(a) $|\mathbb{N} \times \mathbb{R}| = |\mathbb{R}|$;

(b) $|\mathbb{R} \sqcup \mathbb{R}| = |\mathbb{R}|$;

(c) $\left|\mathbb{R}^k\right| = |\mathbb{R}|$ for every integer $k \geq 2$.

Solution.

(a) $x \mapsto (0, x)$ injects $\mathbb{R}$ into $\mathbb{N} \times \mathbb{R}$. In the other direction, $\mathbb{N} \times \mathbb{R} \subseteq \mathbb{R} \times \mathbb{R}$, so the inclusion followed by a bijection $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$ (Theorem 3.6.7) is an injection $\mathbb{N} \times \mathbb{R} \to \mathbb{R}$. Apply Theorem 3.4.3.

(b) Unwinding Definition 3.6.1, $\mathbb{R} \sqcup \mathbb{R} = (\mathbb{R} \times \{0\}) \cup (\mathbb{R} \times \{1\}) = \mathbb{R} \times \{0, 1\}$, a subset of $\mathbb{R} \times \mathbb{R}$; so it injects into $\mathbb{R}$ as in (a). And $x \mapsto (x, 0)$ injects $\mathbb{R}$ into $\mathbb{R} \sqcup \mathbb{R}$. Apply Theorem 3.4.3.

(c) By Theorem 2.2.1 with $n_0 = 2$. The base case $k = 2$ is Theorem 3.6.7. Step: the map $((x_1, \ldots, x_k), x_{k+1}) \mapsto (x_1, \ldots, x_{k+1})$ is a bijection $\mathbb{R}^k \times \mathbb{R} \to \mathbb{R}^{k+1}$, by the characteristic property of tuples (the paragraph after the proof of Corollary 3.1.7). So

$$\left|\mathbb{R}^{k+1}\right| = \left|\mathbb{R}^k \times \mathbb{R}\right| = |\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|,$$

by the hypothesis with Proposition 3.6.1 (b), then Theorem 3.6.7, chained by Proposition 2.5.1. (The book has no 1-tuples and defines X^k for $k \geq 2$ only, so the induction starts at 2.)

Exercise. B4: Prove or disprove

Prove each true statement and refute each false one with a counterexample. Here A, B, C, X, Y, Y', Z are sets.

(a) If $|A \sqcup C| = |B \sqcup C|$, then $|A| = |B|$.

(b) $\left|X^{Y \cup Z}\right| = \left|X^Y \times X^Z\right|$.

(c) If $|Y| \leq |Y'|$, then $\left|X^Y\right| \leq \left|X^{Y'}\right|$.

(d) $\left|\mathbb{N}^{\{0,1\}}\right| = \left|\{0, 1\}^{\mathbb{N}}\right|$.

(e) If $|A| < |B|$ and $C \neq \emptyset$, then $|A \times C| < |B \times C|$.

(f) There is a set X with $\left|\{0, 1\}^X\right| \leq |X|$.

Solution.

(a) False. Take $A = \{0\}$, $B = \emptyset$, $C = \mathbb{N}$. The map $(0, 0) \mapsto 0$, $(n, 1) \mapsto n + 1$ is a bijection $\{0\} \sqcup \mathbb{N} \to \mathbb{N}$, with inverse $0 \mapsto (0, 0)$ and $m \mapsto (m - 1, 1)$ for $m \geq 1$ (Lemma 2.1.1 (c)). And $(n, 1) \mapsto n$ is a bijection $\emptyset \sqcup \mathbb{N} = \mathbb{N} \times \{1\} \to \mathbb{N}$. So both sides are the size of $\mathbb{N}$, while $|\{0\}| \neq |\emptyset|$.

(b) False. Take $X = \{0, 1\}$ and $Y = Z = \{0\}$. Then $Y \cup Z = \{0\}$, and $X^{Y \cup Z}$ has 2 elements, while $X^Y \times X^Z$ has $2 \cdot 2 = 4$. Finite sets with different numbers of elements are not equinumerous (Corollary 2.5.4). The statement is true when $Y \cap Z = \emptyset$, by Quick check 1 (c) with Proposition 3.6.1 (c), and Theorem 3.6.3 (d).

(c) False. Take $X = \emptyset$, $Y = \emptyset$, $Y' = \{0\}$: this is the non-example after Proposition 3.6.2. It is true when $X \neq \emptyset$, by Proposition 3.6.2 (c).

(d) False. The map $f \mapsto (f(0), f(1))$ is a bijection $\mathbb{N}^{\{0,1\}} \to \mathbb{N} \times \mathbb{N}$, with inverse sending

(m, n) to the function $0 \mapsto m$, $1 \mapsto n$. Since $\mathbb{N} \times \mathbb{N}$ is countable (Theorem 3.1.6), there is an injection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ (Theorem 3.1.2), and so an injection $\mathbb{N}^{\{0,1\}} \to \mathbb{N}$ (Theorem 1.5.4 (a)). If $\mathbb{N}^{\{0,1\}}$ were the same size as $\{0,1\}^{\mathbb{N}}$, composing would inject $\{0,1\}^{\mathbb{N}}$ into $\mathbb{N}$, making it countable (Theorem 3.1.2), against Theorem 3.3.1. Base and exponent do not commute.

(e) False. Take $A = \{0\}$, $B = \{0,1\}$, $C = \mathbb{N}$; then $|A| < |B|$ (Corollary 2.5.4 for "no bijection"). But $|\{0\} \times \mathbb{N}| = |\mathbb{N}|$, by $(0, n) \mapsto n$, and $|\{0,1\} \times \mathbb{N}| = |\mathbb{N}|$: the map $(r, n) \mapsto (n, r)$ is a bijection $\{0,1\} \times \mathbb{N} \to \mathbb{N} \sqcup \mathbb{N}$, and Example (Two copies of $\mathbb{N}$) finishes.

(f) False. For every X, $x \mapsto \mathbf{1}_{\{x\}}$ gives $|X| \leq \left|\{0,1\}^X\right|$, so $\left|\{0,1\}^X\right| \leq |X|$ would give $|X| = \left|\{0,1\}^X\right|$ by Theorem 3.4.3, against Corollary 3.6.5.

3.6.10.3 C. Going deeper

Exercise. C1: Functions from the line to the line

Prove that $\left|\mathbb{R}^{\mathbb{R}}\right| = |\mathcal{P}(\mathbb{R})|$. Deduce that there is no surjection $\mathbb{R} \to \mathbb{R}^{\mathbb{R}}$.

Solution (Hint 1). Replace the base $\mathbb{R}$ by $\{0,1\}^{\mathbb{N}}$, then curry.

Solution (Hint 2). You will need $|\mathbb{N} \times \mathbb{R}| = |\mathbb{R}|$.

Solution. Let $\beta \colon \mathbb{R} \to \{0,1\}^{\mathbb{N}}$ be a bijection (Theorem 3.6.6). Then

$$\begin{aligned} \left|\mathbb{R}^{\mathbb{R}}\right| &= \left|(\{0,1\}^{\mathbb{N}})^{\mathbb{R}}\right| = \left|\{0,1\}^{\mathbb{N} \times \mathbb{R}}\right| \\ &= \left|\{0,1\}^{\mathbb{R}}\right| = |\mathcal{P}(\mathbb{R})|, \end{aligned}$$

by Proposition 3.6.1 (c) with β and $\mathrm{id}_{\mathbb{R}}$; then Theorem 3.6.3 (f) with $Y = \mathbb{N}$, $Z = \mathbb{R}$; then Exercise (B3: Sets the size of the line, used later) (a) with Proposition 3.6.1 (c), now in the exponent; then Theorem 3.6.4; chained by Proposition 2.5.1.

For the second part, let $\Theta \colon \mathbb{R}^{\mathbb{R}} \to \mathcal{P}(\mathbb{R})$ be a bijection. If $s \colon \mathbb{R} \to \mathbb{R}^{\mathbb{R}}$ were onto, then $\Theta \circ s \colon \mathbb{R} \to \mathcal{P}(\mathbb{R})$ would be onto (Theorem 1.5.4 (b)), against Theorem 3.3.2. Since $x \mapsto c_x$, where $c_x(t) \coloneqq x$ for all t, is an injection $\mathbb{R} \to \mathbb{R}^{\mathbb{R}}$ (evaluate at 0), and a bijection would be a surjection, $|\mathbb{R}| < \left|\mathbb{R}^{\mathbb{R}}\right|$ (Definition 3.4.1): there are more functions $\mathbb{R} \to \mathbb{R}$ than real numbers.

Marking scheme. (10 points) - 2: replaces the base $\mathbb{R}$ by $\{0,1\}^{\mathbb{N}}$, citing the bijection and Proposition 3.6.1 (c). - 3: applies currying in the right direction: $(X^Y)^Z$ with $Y = \mathbb{N}$, $Z = \mathbb{R}$, to reach $\{0,1\}^{\mathbb{N} \times \mathbb{R}}$. - 2: uses $|\mathbb{N} \times \mathbb{R}| = |\mathbb{R}|$ together with respecting size in the exponent. - 1: passes from $\{0,1\}^{\mathbb{R}}$ to $\mathcal{P}(\mathbb{R})$. - 2: rules out a surjection by composing with the bijection and citing Theorem 3.3.2. Any other complete route (for example graphs into $\mathcal{P}(\mathbb{R} \times \mathbb{R})$, an injection $\mathcal{P}(\mathbb{R}) \to \mathbb{R}^{\mathbb{R}}$ and Theorem 3.4.3) earns the 8 points of the first part, split between the two injections. Fatal errors (0 for the step): computing with symbols as if sizes were numbers ("$\mathfrak{c}^{\mathfrak{c}} = 2^{\aleph_0 \mathfrak{c}}$") with no bijection behind each step.

Exercise. C2: Find the error

Claim: $\{0,1\}^{\mathbb{N}}$ is countable.

> *Proof.* Send b to the natural number $N(b) := \sum_k b(k)2^k$. Different sequences have different binary digits, so N is injective, and an injection into $\mathbb{N}$ makes a set countable (Theorem 3.1.2).

Is the conclusion true? Where does the argument fail? What does it prove?

Solution. The conclusion is false: $\{0,1\}^{\mathbb{N}}$ is uncountable (Theorem 3.3.1).

The error is in the first line. $N(b)$ is named before it is shown to exist: (N14) of Logic and Proof, Example (What is not allowed). The sum is infinite whenever b has infinitely many 1s, and Section 2.3 defines only finite sums (Definition 2.3.1); no natural number is "$1+2+4+\cdots$". The all-1 sequence is a witness: it has no value under N.

What survives. On the sequences that are eventually 0, the sum is finite ($\sum_{k<K} b(k)2^k$ for any K past the last 1), and N is defined there. It is injective once the uniqueness of binary digits is proved, which Exercise R1 below does not do (R1 gives existence only). The countability of that set follows anyway, with no binary digits: changing the codomain from $\{0,1\}$ to $\mathbb{N}$ injects it into the set of eventually zero functions $\mathbb{N} \to \mathbb{N}$ of Exercise (R4), at the end of this section, which is countable; compose with an injection of that set into $\mathbb{N}$ (Theorem 3.1.2, Theorem 1.5.4 (a)).

Marking scheme. (10 points) - 2: says the conclusion is false, citing Theorem 3.3.1. - 3: names the failing step, an infinite sum named as a natural number, with (N14). - 2: gives a witness, such as the all-1 sequence. - 2: says what the argument does prove: the eventually zero sequences form a countable set. - 1: flags that the injectivity of N on them needs the uniqueness of binary digits, which is not proved. Fatal errors (0 for the step): calling the conclusion true; locating the error in "an injection into $\mathbb{N}$ makes a set countable", which is correct.

Exercise. C3: Rearrangements of $\mathbb{N}$

Let B be the set of bijections $\mathbb{N} \to \mathbb{N}$. Exercise C2 of Section 3.3 showed that B is uncountable. Prove that it has exactly the size of $\mathbb{R}$: $|B| = |\mathbb{R}|$.

Solution. Up. Every bijection $\mathbb{N} \to \mathbb{N}$ is a function $\mathbb{N} \to \mathbb{N}$, so $B \subseteq \mathbb{N}^{\mathbb{N}}$, and the inclusion followed by a bijection $\mathbb{N}^{\mathbb{N}} \to \mathbb{R}$ (Theorem 3.6.8) is an injection $B \to \mathbb{R}$.

Down. For $b \in \{0,1\}^{\mathbb{N}}$, let $\sigma_b \colon \mathbb{N} \to \mathbb{N}$ swap $2n$ and $2n+1$ when $b(n) = 1$, and fix them when $b(n) = 0$; this is a function, since each $m \in \mathbb{N}$ is $2n$ or $2n+1$ for exactly one n. It is its own inverse, so $\sigma_b \in B$ (Theorem 1.6.4). The map $b \mapsto \sigma_b$ is injective, since $b(n) = 1$ exactly when $\sigma_b(2n) = 2n+1$. This is the construction of Exercise (C2: Permutations of the naturals).

Composing the *Up* injection with a bijection $\mathbb{R} \to \{0,1\}^{\mathbb{N}}$ (Theorem 3.6.6) gives $|B| \leq \left|\{0,1\}^{\mathbb{N}}\right|$ (Proposition 3.4.1 (b)); by Theorem 3.4.3, $|B| = \left|\{0,1\}^{\mathbb{N}}\right|$, and this is $|\mathbb{R}|$ by Theorem 3.6.6.

Marking scheme. (10 points) - 3: shows $|B| \leq |\mathbb{R}|$, through $B \subseteq \mathbb{N}^{\mathbb{N}}$ and Theorem 3.6.8. - 3: defines σ_b and shows that it is a bijection of $\mathbb{N}$. - 2: shows that $b \mapsto \sigma_b$ is injective, by reading $b(n)$ off $\sigma_b(2n)$. - 2: concludes by Theorem 3.4.3 and Theorem 3.6.6. Fatal errors (0 for the step): concluding $|B| = |\mathbb{R}|$ from "B is uncountable and $B \subseteq \mathbb{N}^{\mathbb{N}}$" alone, with no injection from a set the size of $\mathbb{R}$ into B.

3.6.10.4 R. Review

Exercise. R1

Prove that every integer $n \geq 1$ is a sum of distinct powers of 2: there are an integer $r \geq 1$ and natural numbers $k_1 > k_2 > \cdots > k_r$ with $n = 2^{k_1} + 2^{k_2} + \cdots + 2^{k_r}$.

Solution. We use Theorem 2.2.2 with $n_0 = 1$. Let $n \geq 1$, and suppose every integer m with $1 \leq m < n$ is such a sum.

The largest power of 2 not above n. The set $T := \{k \in \mathbb{N} : 2^k > n\}$ is non-empty, since $2^n \geq 1 + n > n$ by Theorem 2.3.7 with $x = 1$. By Theorem 2.1.3 it has a least element m (the method of Example (Method: the least element)). Since $2^0 = 1 \leq n$, $0 \notin T$, so $m \geq 1$, and $K := m - 1 \in \mathbb{N}$ (Lemma 2.1.1 (c)). As $K < m$, $K \notin T$; so

$$2^K \leq n < 2^{K+1}.$$

The step. Let $s := n - 2^K$, so $0 \leq s < 2^{K+1} - 2^K = 2^K$. If $s = 0$, then $n = 2^K$, a sum with $r = 1$. If $s \geq 1$, then $s < n$, because $2^K \geq 1$. By the hypothesis, $s = 2^{k_1} + \cdots + 2^{k_r}$ with $k_1 > \cdots > k_r$. Each $2^{k_i} \leq s < 2^K$, so $k_i < K$ (if $k_i \geq K$, then $2^{k_i} \geq 2^K$ by Proposition 2.3.4 (e)). Hence

$$n = 2^K + 2^{k_1} + \cdots + 2^{k_r}, \qquad K > k_1 > \cdots > k_r,$$

a sum of distinct powers of 2. By Theorem 2.2.2, every $n \geq 1$ is such a sum. For example $13 = 2^3 + 2^2 + 2^0$.

The base 1 is the right one: 0 is not a sum of one or more powers of 2, since each power is positive.

Exercise. R2

Show that $\forall x\, \exists y\, R(x, y) \nvdash \exists y\, \forall x\, R(x, y)$ by a counter-model whose domain is $\mathbb{N}$. Say in words what the two sentences say when $R(x, y)$ is read as "$x < y$".

Solution. Let $\mathfrak{M}$ have domain $\mathbb{N}$ and $R^{\mathfrak{M}} := \{(d, e) \in \mathbb{N} \times \mathbb{N} : d < e\}$. Both formulas are sentences, so no assignment matters.

The premise is true. $\forall x\, \exists y\, (x < y)$ says "every natural number has a larger one". For each $d \in \mathbb{N}$, $e := d + 1 \in \mathbb{N}$ has $d < e$.

The conclusion is false. $\exists y\, \forall x\, (x < y)$ says "some natural number is larger than every natural number". For any $e \in \mathbb{N}$, the choice $d := e$ gives $d < e$ false, so no e works.

So $\mathfrak{M}$ is a counter-model, and $\forall x\, \exists y\, R(x, y) \not\models \exists y\, \forall x\, R(x, y)$. By the soundness statement of

Logic and Proof, Section 7.2 (the subsection "From counter-models to non-derivability"), a counter-model shows non-derivability: $\forall x\, \exists y\, R(x,y) \nvdash \exists y\, \forall x\, R(x,y)$.

This is the converse of Logic and Proof, Proposition 5.6.2 with the variables renamed and the two places of R exchanged (read $R(x,y)$ as $R(y,x)$), and the counter-model is the one of Logic and Proof, Example (The swap of $\exists$ and $\forall$): there the domain was $\mathbb{Z}$ and R was read as $>$; with the roles of the variables exchanged, R read as $<$ and the domain cut down to $\mathbb{N}$, the same witnesses work, as checked above. In the premise the larger number y is chosen after x and depends on it; the conclusion asks for one y in advance.

Exercise. R3

For an integer $n \geq 1$, how many truth functions with n inputs are there? Prove your answer.

Solution. There are 2^{2^n}. A truth function with n inputs (Logic and Proof, Definition 4.4.4) assigns a truth value to each row $(a_1, \ldots, a_n)$; read a row as the function $i \mapsto a_i$ on $\{1, \ldots, n\}$, and let L be the set of rows.

There are 2^n rows. The map sending a row to $\{i \in \{1, \ldots, n\} : a_i = \mathrm{T}\}$ is a bijection $L \to \mathcal{P}(\{1, \ldots, n\})$ (injective and surjective by Example (Method: proving injectivity) and Example (Method: proving surjectivity)): a row is determined by the places where it is T, and every set of places arises: given $A \subseteq \{1, \ldots, n\}$, the row with $a_i = \mathrm{T}$ for $i \in A$ and $a_i = \mathrm{F}$ otherwise maps to A, and two rows with the same T-places agree at every i, since each a_i is T or F. Since $\{1, \ldots, n\}$ has n elements, Proposition 2.5.8 gives 2^n subsets, so L has 2^n elements (compose the bijections).

There are 2^{2^n} truth functions. In the same way, a truth function f is determined by the set $\{\rho \in L : f(\rho) = \mathrm{T}\} \subseteq L$, and every subset of L arises (the same two checks, with $f \mapsto \{\rho : f(\rho) = \mathrm{T}\}$ in place of the row map); so the truth functions are in bijection with $\mathcal{P}(L)$, which has 2^{2^n} elements by Proposition 2.5.8 again. For $n = 1, 2, 3$ this gives $4, 16, 256$.

Exercise. R4

A function $f\colon \mathbb{N} \to \mathbb{N}$ is **eventually zero** if there is $N \in \mathbb{N}$ with $f(n) = 0$ for every $n \geq N$. Is the set of eventually zero functions countable?

Solution. Yes. The tool is a **countable union of countable sets**. For $N \in \mathbb{N}$ let Z_N be the set of $f\colon \mathbb{N} \to \mathbb{N}$ with $f(n) = 0$ for every $n \geq N$; the set of eventually zero functions is $Z := \bigcup_{N \in \mathbb{N}} Z_N$. Each Z_N is countable:

- Z_0 has one element, the zero function, so it is countable.
- For $N = 1$, $f \mapsto f(0)$ is a bijection $Z_1 \to \mathbb{N}$: a function in Z_1 is determined by its value at 0, and every value occurs.
- For $N \geq 2$, $f \mapsto (f(0), \ldots, f(N-1))$ is a bijection $Z_N \to \mathbb{N} \times \cdots \times \mathbb{N}$ (N factors), by the same reasoning and the characteristic property of tuples; the product is countable by Corollary 3.1.7, and so is Z_N (compose a surjection $\mathbb{N} \to \mathbb{N} \times \cdots \times \mathbb{N}$ with the inverse bijection, Proposition 3.1.4).

By Theorem 3.2.3, Z is countable. (That theorem uses Axiom 3.2.1; here it could be avoided, since each Z_N comes with an explicit listing, but the question did not ask for that.)

Why the look-alike fails. A diagonal argument, as in Theorem 3.3.1, builds from a list $f_0, f_1, \ldots$ of eventually zero functions the function $g(n) := f_n(n) + 1$. It differs from every f_n, but $g(n) \geq 1$ for every n, so g is **not** eventually zero: it is not in Z, and nothing is contradicted. A diagonal argument proves uncountability only when the diagonal object stays inside the set; this is the usual failure named in Example (Method: the diagonal).

Chapter 4

Relations: Equivalence and Order

This chapter is about relations. When is "the same" a legitimate way to identify different things, as a clock identifies 2 with 14, or a function identifies two points with the same value? And what does "larger" mean when not everything can be compared, as with sets under inclusion or natural numbers under divisibility? The motivating problem: *in what sense is "*$9 + 5 = 2$ *on a clock" a true statement?* The answer is an equivalence relation, the partition it cuts its set into, and a check that arithmetic on the pieces does not depend on which integer names a piece. For orders the answer is that "largest" splits into two notions, greatest and maximal, which agree only when every two elements are comparable. The last section reaches least upper bounds in a general partially ordered set (*Analysis on the Real Line*, Chapter 1's supremum is the case of $\leq$ on $\mathbb{R}$, and its axiom says that such suprema exist) and closes with well-ordered sets, the order-theoretic name for what Section 2.1 proved about $\mathbb{N}$.

Two methods of proof are new. Section 4.1 decides a property of a relation by a proof for all elements or by one witness against it, and records the verdicts in a table. Section 4.2 checks that a definition made through a representative does not depend on the representative: the check called well-definedness, promised in Section 1.5. Section 4.3 uses the methods of Chapters 1 and 2 without new scaffolding.

What you need. *Logic and Proof*, Chapters 1–8, and *Sets and Functions*, Chapters 1–3. From *Logic and Proof*: the rules for "there exists" (Logic and Proof, Definition 5.6.1), equality (Logic and Proof, Definition 5.7.1, Logic and Proof, Proposition 5.7.1), negating bounded quantifiers and implications (Logic and Proof, Proposition 6.2.3, Logic and Proof, Proposition 6.2.2), De Morgan and double negation (Logic and Proof, Proposition 2.5.5, Logic and Proof, Proposition 2.5.1), the catalogue of what a proof may not do (Logic and Proof, Example (What is not allowed)), squares and order (Logic and Proof, Theorem 2.4.5), and induction (Logic and Proof, Axiom 4.2.1). From Chapter 1: subsets, set equality and sets cut out by a property (Definition 1.2.2, Definition 1.2.1, Definition 1.2.3, Proposition 1.2.3, Proposition 1.2.1, Proposition 1.2.2); power sets and unions of families (Definition 1.3.2, Definition 1.3.4); ordered pairs and relations as sets of pairs (Definition 1.4.1, Definition 1.4.3); functions, their equality, and rules that are not functions (Definition 1.5.1, Proposition 1.5.1, Example (Relations that are not functions)); surjections and two-sided inverses (Definition 1.5.4, Theorem 1.6.4); preimages (Definition 1.7.2, Proposition 1.7.5); Russell's theorem (Theorem 1.2.4); divisibility and parity (Definition 1.1.2, Proposition 1.1.1, Theorem 1.1.2); and the methods direct proof, cases, counterexample, double inclusion, uniqueness, injectivity and construct-and-verify (Example (Method: direct proof from a definition), Example (Method: proof by cases), Example (Method: disproof by counterexample, proof by example), Example (Method: two inclusions), Example (Method: existence and uniqueness), Example (Method: proving injectivity), Example (Method: construct and verify)). From Chapter 2: well-ordering and the least-element method

(Theorem 2.1.3, Corollary 2.1.5, Example (Method: the least element)); the arithmetic of the integers (Proposition 2.1.2, Lemma 2.1.1); induction from a base (Theorem 2.2.1); the division algorithm and prime factors (Theorem 2.2.3, Theorem 2.2.5); powers (Definition 2.3.2, Proposition 2.3.4); finite maxima (Proposition 2.3.8); choosing between direct proof, contrapositive and contradiction (Example (Method: choosing direct, contrapositive or contradiction)); equinumerous, finite and infinite sets (Definition 2.5.1, Proposition 2.5.1, Corollary 2.5.4, Definition 2.5.2, Definition 2.5.3, Proposition 2.5.6, Example (Hilbert's Hotel)). From Chapter 3: images of countable sets and the countability of $\mathbb{Z}$ (Proposition 3.1.4, Theorem 3.1.8), for one review exercise, and the axiom of choice (Axiom 3.2.1), for one remark. The arithmetic and order of $\mathbb{R}$ are school facts, as before.

Time. About 20 hours on the core track (all of A, one B and one C per section, the exit check 4.2 C1); about 25 hours for everything.

4.0.1 Roadmap

- **Properties of relations.** Reflexive, symmetric, antisymmetric and transitive; deciding each one by a proof for all elements or by a single witness, with the verdicts collected in a table of eight relations; divisibility as the relation whose antisymmetry depends on the set.
- **Equivalence relations and partitions.** Relations that behave like equality, the proof that their classes partition the set and that every partition arises from exactly one of them (a correspondence proved in both directions), the integers modulo n, sizes of subsets as a last example, and the method for checking that a definition on classes is well defined.
- **Partial orders, maximal and greatest elements.** Relations that behave like $\leq$, greatest elements against maximal ones and when the two agree, uniqueness from antisymmetry, least upper bounds in a partially ordered set, and well-ordered sets.

4.0.2 Named moves

The first two are method boxes; Chapters 1–3's boxes are cited where they are used.

- **Prove or disprove each property** (Example (Method: proving or disproving a property of a relation)). A property that holds is a "for all": take arbitrary related elements and unwind. A property that fails needs one witness: an element, a pair or a triple. (Section 4.1)
- **Well-definedness** (Example (Method: checking that a definition on classes is well defined)). For a rule that reads a representative, take two representatives of one class and show that the outputs agree. (Section 4.2)
- **Classes from a relation, a relation from classes.** Pass between an equivalence relation and its partition, whichever description makes the next step easier.
- **Uniqueness by antisymmetry.** Two candidates, each below the other, are equal: the method of Example (Method: existence and uniqueness) with (PO2) closing the gap. (Section 4.3)

4.0.3 Threads

- **Same size.** The bijections of Section 1.6 say when two sets have the same size; Section 2.5 makes this a definition (Definition 2.5.1); Section 4.2 meets it as an equivalence relation on the subsets of one set (Example (Same size, revisited)), and explains why it is not one on all sets.
- **The clock.** The arithmetic of $\mathbb{Z}/n$ in Section 4.2 returns in *Number Systems: From* $\mathbb{N}$ *to*

$\mathbb{R}$, Section 3.4, where $\mathbb{Z}/n$ becomes a ring.
- **Maximal elements and chains.** Section 4.3 ends by asking when a partially ordered set must have a maximal element; Chapter 6 answers with Zorn's lemma.

4.0.4 Summary

A relation on a set may be reflexive, symmetric, antisymmetric or transitive (Definition 4.1.1); each property is proved for all elements or refuted by one witness. The relations with the first, second and fourth are the equivalence relations (Definition 4.2.1); their classes partition the set (Theorem 4.2.1), and every partition comes from exactly one of them (Theorem 4.2.2). Congruence modulo n gives $\mathbb{Z}/n = \{[0], \ldots, [n-1]\}$ (Proposition 4.2.4), whose sum and product are well defined (Proposition 4.2.5), while some rules on classes are not functions at all (Example (A rule on classes that is not a function)). The relations with the first, third and fourth are the partial orders (Definition 4.3.1). A greatest element is unique (Proposition 4.3.1) and maximal, and the converse needs totality (Proposition 4.3.2); a supremum is the least upper bound (Definition 4.3.5), and under divisibility it is the least common multiple (Example (The supremum under divisibility is the least common multiple)).

What is open: in a partially ordered set where every chain has an upper bound, must there be a maximal element? Nothing proved so far decides it. Chapter 6 states the principle that does, Zorn's lemma, and puts it to work. Next, Chapter 5 uses quotient sets and well-definedness to build functions: every function factors through the quotient by "same value".

4.0.5 Terms

- **antisymmetric**: $x \mathrel{R} y$ and $y \mathrel{R} x$ give $x = y$ (Definition 4.1.1).
- **block**: one of the sets of a partition (Definition 4.2.3).
- **bounded**: bounded above and below, that is, with an upper and a lower bound (Definition 4.3.2).
- **comparable**: $x \preceq y$ or $y \preceq x$ (Definition 4.3.1).
- **congruent modulo** n: $a \equiv b \pmod{n}$, that is, $n \mid a - b$ (Definition 4.2.5).
- **equivalence class**: $[a] = \{x \in X : x \sim a\}$ (Definition 4.2.2).
- **equivalence relation**: reflexive, symmetric and transitive (Definition 4.2.1).
- **greatest element**: an element of A above every element of A (Definition 4.3.3).
- **infimum**: a greatest lower bound (Definition 4.3.5).
- **least element**: an element of A below every element of A (Definition 4.3.3).
- **lower bound**: an element of X below every element of A (Definition 4.3.2).
- **maximal element**: an element of A with nothing in A strictly above it (Definition 4.3.4).
- **minimal element**: an element of A with nothing in A strictly below it (Definition 4.3.4).
- **partially ordered set**: a set with a reflexive, antisymmetric and transitive relation (Definition 4.3.1).
- **partition**: a set of non-empty, pairwise disjoint subsets whose union is the whole set (Definition 4.2.3).
- **quotient map**: $x \mapsto [x]$, from X onto $X/\sim$ (Definition 4.2.4).
- **quotient set**: the set $X/\sim$ of all equivalence classes (Definition 4.2.4).
- **reflexive**: $x \mathrel{R} x$ for every $x \in X$ (Definition 4.1.1).
- **representative**: an element of a class, which names the class (Definition 4.2.2).
- **strict part**: $x \prec y$, that is, $x \preceq y$ and $x \neq y$ (Definition 4.3.1).
- **supremum**: a least upper bound (Definition 4.3.5).
- **symmetric**: $x \mathrel{R} y$ gives $y \mathrel{R} x$ (Definition 4.1.1).
- **total**: every two elements are comparable (Definition 4.3.1).
- **transitive**: $x \mathrel{R} y$ and $y \mathrel{R} z$ give $x \mathrel{R} z$ (Definition 4.1.1).

- **upper bound**: an element of X above every element of A (Definition 4.3.2).
- **well defined**: a rule on classes whose output does not depend on the representative (Example (Method: checking that a definition on classes is well defined)).
- **well-ordered set**: a partially ordered set whose order is total and in which every non-empty subset has a least element (Definition 4.3.6).

4.1 Properties of Relations

Chapter 1 made relations into sets: a relation on a set X is a subset $R \subseteq X \times X$, and $x\ R\ y$ means $(x, y) \in R$ (Definition 1.4.3). It named the properties that make a relation an order or an equivalence and left them to this chapter. Equality, $\leq$, inclusion $\subseteq$, divisibility $|$, and "leaves the same remainder on division by 3" are all relations, and they behave alike in some ways and differently in others. This section names four properties that sort them, proves the ones that divisibility has, and collects witnesses for every failure. Each property is decided by the same method: a proof for all elements when it holds, one witness when it fails. Sections 4.2 and 4.3 then study the two combinations that matter most.

4.1.1 Four properties

Start from equality. Every x equals itself; if $x = y$, then $y = x$; and if $x = y$ and $y = z$, then $x = z$. The relation $\leq$ on $\mathbb{R}$ keeps the first and third of these and loses the second, but it has a substitute: $x \leq y$ and $y \leq x$ together force $x = y$. Each of these is a property a relation may or may not have.

Each property is one rule for what the relation must contain, given what it already contains.

Definition 4.1.1. Properties of a Relation

Let X be a set and R a relation on X. Then R is

- **reflexive on** X if $x\ R\ x$ for **every** $x \in X$:

$$\forall x \in X \quad x\ R\ x;$$

- **symmetric** if $x\ R\ y$ implies $y\ R\ x$, for all $x, y \in X$:

$$\forall x \in X\ \forall y \in X \quad (x\ R\ y \to y\ R\ x);$$

- **antisymmetric** if $x\ R\ y$ and $y\ R\ x$ together imply $x = y$, for all $x, y \in X$:

$$\forall x \in X\ \forall y \in X \quad \big((x\ R\ y \wedge y\ R\ x) \to x = y\big);$$

- **transitive** if $x\ R\ y$ and $y\ R\ z$ together imply $x\ R\ z$, for all $x, y, z \in X$:

$$\forall x \in X\ \forall y \in X\ \forall z \in X \quad \big((x\ R\ y \wedge y\ R\ z) \to x\ R\ z\big).$$

In words: reflexive says every element is related to itself. Symmetric says the relation can be read backwards: whenever it relates x to y, it also relates y to x. Antisymmetric says it can be read both ways only between an element and itself. Transitive says two steps can always be replaced by one.

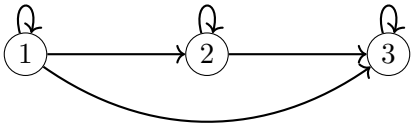
Three of the four are implications, so a relation has them unless some related pair (or triple)

makes the conclusion false: for symmetry and transitivity a pair is missing from R, and for antisymmetry two different elements are related both ways. Negating with Logic and Proof, Proposition 6.2.3 and Logic and Proof, Proposition 6.2.2 turns each failure into a **witness**:

$$\begin{aligned}
\text{not reflexive:} &\quad \exists x \in X \;\; \neg(x \; R \; x), \\
\text{not symmetric:} &\quad \exists x \in X \; \exists y \in X \;\; (x \; R \; y \wedge \neg(y \; R \; x)), \\
\text{not antisymmetric:} &\quad \exists x \in X \; \exists y \in X \;\; ((x \; R \; y \wedge y \; R \; x) \wedge x \neq y), \\
\text{not transitive:} &\quad \exists x \in X \; \exists y \in X \; \exists z \in X \;\; ((x \; R \; y \wedge y \; R \; z) \wedge \neg(x \; R \; z)).
\end{aligned}$$

So "not symmetric" is shown by **one** pair related in one direction only, and "not transitive" by one triple. A single witness settles a failure; a success needs an argument for all elements.

Reading a relation as a picture. Draw the elements of X as points and an arrow from x to y whenever $x \; R \; y$. The relation $\leq$ on $\{1, 2, 3\}$ is $\{(1, 1), (2, 2), (3, 3), (1, 2), (1, 3), (2, 3)\}$:



Reflexive means a loop at every point. Symmetric means every arrow has a return arrow. Antisymmetric means no two **different** points are joined in both directions. Transitive means every path of two arrows has a direct arrow from its start to its end. In the picture there are loops everywhere, no return arrows, and the two-arrow path $1 \to 2 \to 3$ has its shortcut $1 \to 3$; so $\leq$ on $\{1, 2, 3\}$ is reflexive, antisymmetric and transitive, and not symmetric, with witness the pair $(1, 2)$. A path may also return to its start: $x \to y \to x$. Transitivity then demands the loop at x. That case is the source of the warning below.

Why "reflexive on X". The other three properties mention elements only when they are related, so they depend on the set R alone. Reflexivity depends on X too. The relation $\{(0, 0)\}$ is reflexive on $\{0\}$, and the same set of pairs, viewed as a relation on $\{0, 1\}$, is not reflexive on $\{0, 1\}$, with witness 1. That is why the definition names the set.

4.1.2 Prove or disprove, property by property

A relation given by a formula has each property or not, and nothing tells us in advance which. So the first step is to test small elements and guess; the second is a proof if the guess is "yes", and a witness, checked clause by clause, if it is "no".

Example. Deciding four properties

On $\mathbb{Z}$, let $x \; R \; y$ mean $7 \mid 3x + 4y$. Decide which of the four properties of Definition 4.1.1 R has.

Idea (Scratch work). Test small elements first. $1 \; R \; 1$, since $3+4 = 7$. Also $0 \; R \; 7$ ($0+28 = 28$) and $7 \; R \; 0$ ($21 + 0 = 21$), with $0 \neq 7$: antisymmetry fails, and the pair $0, 7$ is the witness. Reflexivity looks true in general: $3x + 4x = 7x$. Symmetry is the one to plan, since the coefficients swap places.

Givens	Goal
$x \mathrel{R} y$	$y \mathrel{R} x$
$3x + 4y = 7k$, with $k \in \mathbb{Z}$	$3y + 4x = 7m$ for some $m \in \mathbb{Z}$: find m
$3x + 4y = 7k$	$(3y + 4x) + (3x + 4y) = 7x + 7y$, so
	$3y + 4x = 7(x + y - k)$: try $m = x + y - k$

The last row closes the gap: the two expressions add up to a multiple of 7, because $3+4 = 7$. Transitivity goes the same way: adding the givens $3x + 4y = 7k$ and $3y + 4z = 7l$ gives $3x + 7y + 4z$, and the middle term is a multiple of 7.

Solution. Reflexive. For $x \in \mathbb{Z}$, $3x + 4x = 7x$ with $x \in \mathbb{Z}$, so $7 \mid 3x + 4x$.

Symmetric. Let $x \mathrel{R} y$, say $3x + 4y = 7k$ with $k \in \mathbb{Z}$. Then $3y + 4x = 7(x + y) - (3x + 4y) = 7(x + y - k)$, and $x + y - k \in \mathbb{Z}$ by Proposition 2.1.2 (a), so $y \mathrel{R} x$.

Transitive. Let $x \mathrel{R} y$ and $y \mathrel{R} z$, say $3x + 4y = 7k$ and $3y + 4z = 7l$ with $k, l \in \mathbb{Z}$. Adding, $3x + 7y + 4z = 7(k + l)$, so $3x + 4z = 7(k + l - y)$, with $k + l - y \in \mathbb{Z}$ (Proposition 2.1.2 (a)), and $x \mathrel{R} z$.

Not antisymmetric. $3 \cdot 0 + 4 \cdot 7 = 28 = 7 \cdot 4$ and $3 \cdot 7 + 4 \cdot 0 = 21 = 7 \cdot 3$, so $0 \mathrel{R} 7$ and $7 \mathrel{R} 0$, while $0 \neq 7$.

reflexive	symmetric	antisymmetric	transitive
yes	yes	no: $0, 7$	yes

Three verdicts needed a proof about all integers, and one needed a single pair: that asymmetry of effort is the method.

Example. Method: proving or disproving a property of a relation

Template. To prove a property, write it as the "for all" it is (Definition 4.1.1), take arbitrary elements satisfying its hypothesis, unwind the relation's definition and rewind the conclusion (Example (Method: direct proof from a definition)). To disprove it, exhibit one witness of the negated form and check each clause (Example (Method: disproof by counterexample, proof by example)). Record the verdicts in a table, each "no" with its witness.

When to use it. A relation is given by a formula, a list or a picture, and the question is which properties it has: whether it is an equivalence relation, or a partial order.

The usual failure. "Proving" a property from one example; refuting antisymmetry with a pair related one way only, which refutes symmetry instead; a witness for "not reflexive" that is not in X.

Quick check. On $\mathbb{Z}$, let $x \mathrel{S} y$ mean $7 \mid 3x + 5y$. Is S reflexive? Is it symmetric?

Solution. Neither. Not reflexive: $1 \; S \; 1$ would need $7 \mid 8$, and $8 = 7k$ fails for every integer k: if $k \leq 1$, then $7k \leq 7$; if $k > 1$, then $k \geq 2$ by Proposition 2.1.2 (c), and $7k \geq 14$. Not symmetric: $1 \; S \; 5$, since $3 + 25 = 28 = 7 \cdot 4$, but $5 \; S \; 1$ fails, since $15 + 5 = 20$ and $14 < 20 < 21$, and no multiple of 7 lies strictly between $7 \cdot 2$ and $7 \cdot 3$, as no integer lies strictly between 2 and 3 (Proposition 2.1.2 (c)). With $3 + 5 = 8$, the coefficients no longer add up to a multiple of 7, and the trick of the scratch work is gone.

4.1.3 Divisibility

Divisibility shows that the same rule can give an antisymmetric relation on one set and not on a larger one, because the larger set brings in more pairs: $\mid$ on $\mathbb{Z}$ contains both $(2, -2)$ and $(-2, 2)$, which $\mid$ on $\mathbb{N}$ does not. Recall Definition 1.1.2: for integers a, b, $a \mid b$ means $b = ka$ for some $k \in \mathbb{Z}$.

Proposition 4.1.1. Divisibility on the Natural Numbers

The relation $\mid$ is reflexive, antisymmetric and transitive on $\mathbb{N}$. On $\mathbb{Z}$ it is reflexive and transitive, and **not** antisymmetric.

Idea. Reflexivity and transitivity are one line each from Definition 1.1.2. For antisymmetry, $b = ka$ and $a = lb$ give $a = lka$. If $a \neq 0$, this forces $kl = 1$, and for **positive** integers that means $k = l = 1$. On $\mathbb{N}$ the multipliers are positive, so $b = a$; on $\mathbb{Z}$ they may both be -1. (The method of Example (Method: proving or disproving a property of a relation): three proofs for $\mathbb{N}$ and one witness for $\mathbb{Z}$.)

Proof. Reflexive. For every integer a, $a = 1 \cdot a$, so $a \mid a$.

Transitive. This is Proposition 1.1.1.

These two arguments work for all integers, so on $\mathbb{N}$ and on $\mathbb{Z}$.

Antisymmetric on $\mathbb{N}$. Let $a, b \in \mathbb{N}$ with $a \mid b$ and $b \mid a$, say $b = ka$ and $a = lb$ with $k, l \in \mathbb{Z}$.

Case 1: $a = 0$ or $b = 0$. If $a = 0$, then $b = k \cdot 0 = 0$; if $b = 0$, then $a = l \cdot 0 = 0$. Either way $a = b$.

Case 2: $a \neq 0$ and $b \neq 0$. By Lemma 2.1.1 (a), $a \geq 1$ and $b \geq 1$, so both are positive. Since $ka = b > 0$ and $a > 0$, we have $k > 0$ (if $k \leq 0$, then $ka \leq 0$); likewise $l > 0$. By Proposition 2.1.2 (b), $k, l \in \mathbb{Z}_{>0} = \{n \in \mathbb{N} : n \geq 1\}$, so $k \geq 1$ and $l \geq 1$. Now $a = lb = lka$, and $a \neq 0$, so $kl = 1$. If $k > 1$, then multiplying by $l > 0$ gives $kl > l \geq 1$, contradicting $kl = 1$. So $k \leq 1$, hence $k = 1$, and $b = a$.

Not antisymmetric on $\mathbb{Z}$. $-2 = (-1) \cdot 2$ and $2 = (-1) \cdot (-2)$, so $2 \mid -2$ and $-2 \mid 2$, but $2 \neq -2$.

■

The failure on $\mathbb{Z}$ is a non-example by minimal change: enlarging the set from $\mathbb{N}$ to $\mathbb{Z}$ keeps

reflexivity and transitivity, and antisymmetry fails exactly because an integer and its negative divide each other. Two facts about $(\mathbb{N}, |)$ will matter in Section 4.3: every $a \in \mathbb{N}$ divides 0, since $0 = 0 \cdot a$, and 1 divides every a, since $a = a \cdot 1$. In the divisibility relation, 0 sits above everything and 1 below everything.

4.1.4 A table of examples

Here are eight relations checked against the four properties. Each "no" comes with its witness, which is how a failure is proved; each "yes" is a one-line argument given after the table. The table is the method of Example (Method: proving or disproving a property of a relation) run eight times: thirty-two verdicts, nine of them refuted by a witness.

Example. Eight relations, four properties

Decide which of the four properties each relation has: $=$, $\leq$ and $<$ on $\mathbb{R}$; $\subseteq$ on $\mathcal{P}(X)$ for a set X with at least one element; $|$ on $\mathbb{N}$ and on $\mathbb{Z}$; "$x - y \in \mathbb{Z}$" on $\mathbb{R}$; and the empty relation $\emptyset$ on a set X with at least one element.

Solution.

Relation	reflexive	symmetric	antisymmetric	transitive
$=$ on $\mathbb{R}$	yes	yes	yes	yes
$\leq$ on $\mathbb{R}$	yes	no: $0, 1$	yes	yes
$<$ on $\mathbb{R}$	no: 0	no: $0, 1$	yes	yes
$\subseteq$ on $\mathcal{P}(X)$	yes	no: $\emptyset, X$	yes	yes
$\mid$ on $\mathbb{N}$	yes	no: $1, 2$	yes	yes
$\mid$ on $\mathbb{Z}$	yes	no: $1, 2$	no: $2, -2$	yes
$x - y \in \mathbb{Z}$ on $\mathbb{R}$	yes	yes	no: $0, 1$	yes
$\emptyset$ on X	no: any x	yes	yes	yes

The witnesses. $0 \leq 1$ and not $1 \leq 0$; $0 < 1$ and not $1 < 0$; not $0 < 0$. $\emptyset \subseteq X$, since the empty set is a subset of every set (Section 1.2, after Proposition 1.2.3), and $X \not\subseteq \emptyset$, since X has an element and $\emptyset$ has none. $1 \mid 2$, and $2 \nmid 1$: $1 = 2k$ would give $0 < k < 1$, and no integer lies there (Proposition 2.1.2 (c)). The pair $2, -2$ is from Proposition 4.1.1. For $x - y \in \mathbb{Z}$: $0 - 1 = -1$ and $1 - 0 = 1$ are integers, and $0 \neq 1$. For $\emptyset$: no x has $(x, x) \in \emptyset$.

The "yes" entries. Equality is reflexive by =I (Logic and Proof, Definition 5.7.1), symmetric and transitive by Logic and Proof, Proposition 5.7.1, and antisymmetric because its conclusion $x = y$ is one of its hypotheses. For $\leq$ and $<$, antisymmetry and transitivity are order facts about $\mathbb{R}$, and $\leq$ is reflexive because $x = x$ gives $x \leq x$; for $<$, antisymmetry holds **vacuously**, since $x < y$ and $y < x$ never hold together. For $\subseteq$, reflexivity is immediate from Definition 1.2.2, transitivity is Proposition 1.2.2, and antisymmetry is Proposition 1.2.1. For $|$, see Proposition 4.1.1. For $x - y \in \mathbb{Z}$: $x - x = 0 \in \mathbb{Z}$; $y - x = -(x - y)$; and $x - z = (x - y) + (y - z)$; these are integers by Proposition 2.1.2 (a). The empty relation is symmetric, antisymmetric and transitive vacuously: each property is an implication whose hypothesis requires a pair in $\emptyset$.

Three degenerate cases are worth a sentence each, because each shows a property holding for a

reason other than the one we expect.

- The **empty relation** on a non-empty X has every property except reflexivity, all vacuously. It is the standard witness that the three implication properties do not imply reflexivity.
- The **full relation** $X \times X$ relates everything to everything. It is reflexive, symmetric and transitive; it is antisymmetric only if X has at most one element.
- If $X = \emptyset$, then $\mathcal{P}(X) = \{\emptyset\}$, and $\subseteq$ on it is $\{(\emptyset, \emptyset)\}$: with only one element, it is **symmetric**. The non-emptiness of X in the table is what the witness $\emptyset, X$ needs.

Quick check. On the set $\{2, 3, 4, \dots\}$ of integers ≥ 2, let $x\ C\ y$ mean "x and y have a common prime factor", that is, some prime p divides both. Which of the four properties does C have?

Solution. Reflexive: every integer $x \geq 2$ has a prime factor p (Theorem 2.2.5), and p divides x and x. Symmetric: the condition "$p \mid x$ and $p \mid y$" does not depend on the order of x and y. Not antisymmetric: $2\ C\ 4$ and $4\ C\ 2$ (both divisible by 2), and $2 \neq 4$. Not transitive: $2\ C\ 6$ (common factor 2) and $6\ C\ 3$ (common factor 3), but 2 and 3 have no common prime factor, since 2 is prime (Section 1.1, after Definition 1.1.3), so a prime dividing 2, being a positive divisor of 2 other than 1, is 2; and $2 \nmid 3$: $3 = 2k$ would give $1 < k < 2$, and no integer lies there (Proposition 2.1.2 (c)). Sharing a factor with a middle element does not pass along, because the shared factor may change.

Warning. **A false theorem: "symmetric and transitive imply reflexive."** The "proof": let $x \in X$, and take y with $x\ R\ y$; by symmetry $y\ R\ x$, and by transitivity $x\ R\ x$. The conclusion is false: the empty relation on $\{1\}$ is symmetric and transitive (vacuously) and not reflexive, with witness 1. The illegal step, "take y with $x\ R\ y$", is an $\exists$E (Logic and Proof, Definition 5.6.1) on $\exists y \in X\ x\ R\ y$, which was never derived and need not be true: (N9) of Logic and Proof, Example (What is not allowed) (Exercise C2 gives the correct version).

Remark. "Antisymmetric" is not "not symmetric". Equality is both symmetric and antisymmetric. And $\{(1,2), (2,1), (2,3)\}$ on $\{1, 2, 3\}$ is neither: it is not symmetric, since $2\ R\ 3$ and not $3\ R\ 2$; and it is not antisymmetric, since $1\ R\ 2$, $2\ R\ 1$ and $1 \neq 2$.

Two combinations of the properties organize the rest of the chapter. A relation that is reflexive, symmetric and transitive behaves like equality; Section 4.2 calls it an **equivalence relation** and shows that it cuts X into classes. A relation that is reflexive, antisymmetric and transitive behaves like $\leq$; Section 4.3 calls it a **partial order**; inclusion on $\mathcal{P}(X)$ and divisibility on $\mathbb{N}$ are examples that are not comparisons of sizes.

4.1.5 Exercises

4.1.5.1 A. Check your understanding

Exercise. A1

(a) State in symbols what it means for a relation R on X to be antisymmetric, and write its negation in symbols.

(b) True or false, with a witness: every antisymmetric relation fails to be symmetric.

(c) Which of the four properties does the relation "$|x - y| \leq 1$" have on $\mathbb{R}$?

(d) Let $X = \{p, q\}$ with $p \neq q$. How many relations on X are reflexive on X?

(e) To show that a relation is **not** transitive, what must you produce? To show that it **is**, what do you assume?

Solution.

(a) $\forall x \in X\ \forall y \in X\ ((x\ R\ y \wedge y\ R\ x) \to x = y)$. Its negation, by Logic and Proof, Proposition 6.2.3 and Logic and Proof, Proposition 6.2.2: $\exists x \in X\ \exists y \in X\ ((x\ R\ y \wedge y\ R\ x) \wedge x \neq y)$.

(b) False. Equality on any set is antisymmetric and symmetric. So is the empty relation (vacuously).

(c) Reflexive: $|x-x| = 0 \leq 1$. Symmetric: $|y-x| = |x-y|$. Not antisymmetric: $|0-1| \leq 1$ both ways and $0 \neq 1$. Not transitive: $|0 - 1| \leq 1$ and $|1 - 2| \leq 1$, but $|0 - 2| = 2 > 1$. "Close to" does not pass along a chain, because small differences add up.

(d) Four. A reflexive relation must contain (p, p) and (q, q). The other two pairs of $X \times X$, (p, q) and (q, p), may each be in or out, independently, which gives $2 \cdot 2 = 4$ relations: $\{(p, p), (q, q)\}$ together with one of $\emptyset$, $\{(p, q)\}$, $\{(q, p)\}$, $\{(p, q), (q, p)\}$.

(e) Elements x, y, z (not necessarily distinct) with $x\ R\ y$, $y\ R\ z$ and not $x\ R\ z$ (the witness form of Definition 4.1.1). To show transitivity, assume arbitrary $x, y, z \in X$ with $x\ R\ y$ and $y\ R\ z$, and derive $x\ R\ z$ (Example (Method: proving or disproving a property of a relation)).

4.1.5.2 B. Practice

Exercise. B1: Five relations

For each relation, determine which of the four properties it has. Justify your answer, with a witness for each failure.

(a) On $\mathbb{N} \times \mathbb{N}$: $(a, b)\ E\ (c, d)$ if and only if $a + d = b + c$.

(b) On $\mathbb{R}$: $x\ S\ y$ if and only if $x^2 = y^2$.

(c) On the set $\mathbb{R}^{\mathbb{R}}$ of functions $\mathbb{R} \to \mathbb{R}$: $f\ L\ g$ if and only if $f(x) \leq g(x)$ for every $x \in \mathbb{R}$.

(d) On $\mathbb{R}$: $x\ P\ y$ if and only if $xy > 0$.

(e) On $\mathbb{Z}$: $x\ N\ y$ if and only if $y = x + 1$.

Solution.

(a) Reflexive: $a + b = b + a$. Symmetric: $a + d = b + c$ gives $c + b = d + a$. Transitive: from $a + d = b + c$ and $c + f = d + e$, adding gives $a + d + c + f = b + c + d + e$, and canceling $c + d$ gives $a + f = b + e$. Not antisymmetric: $(0, 0)\ E\ (1, 1)$ both ways, and $(0, 0) \neq (1, 1)$. (The pairs (a, b) and (c, d) are related exactly when $a - b = c - d$; *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 2 builds $\mathbb{Z}$ from the classes of this relation.)

(b) Reflexive, symmetric and transitive, because "$x^2 = y^2$" is equality of the values x^2 and y^2, and equality has those three properties. Not antisymmetric: $1^2 = (-1)^2$ and $1 \neq -1$.

(c) Reflexive: $f(x) \leq f(x)$. Transitive: $f(x) \leq g(x) \leq h(x)$ at each x. Antisymmetric: if $f \; L \; g$ and $g \; L \; f$, then $f(x) = g(x)$ for every x, and $f = g$ by Proposition 1.5.1 (same domain and codomain). Not symmetric: the constant functions 0 and 1 satisfy $0 \; L \; 1$ and not $1 \; L \; 0$. In addition, two functions need not be comparable: for $f(x) = x$ and the constant 0, neither $f \; L \; 0$ (fails at $x = 1$) nor $0 \; L \; f$ (fails at $x = -1$).

(d) Symmetric: $xy = yx$. Transitive: if $xy > 0$ and $yz > 0$, then $(xy)(yz) = xz\,y^2 > 0$, and $y^2 > 0$ (since $y \neq 0$, as $xy \neq 0$), so $xz > 0$. **Not reflexive:** $0 \cdot 0 = 0$, so 0 is not related to itself. Not antisymmetric: $1 \; P \; 2$ and $2 \; P \; 1$ (both products are $2 > 0$), and $1 \neq 2$. This is the planted case: P is symmetric and transitive, yet not reflexive on $\mathbb{R}$, exactly at the one element related to nothing. On $\mathbb{R} \setminus \{0\}$ it is reflexive. Compare the warning before these exercises.

(e) Not reflexive: $0 \neq 0 + 1$. Not symmetric: $0 \; N \; 1$ and not $1 \; N \; 0$ ($0 \neq 2$). Not transitive: $0 \; N \; 1$ and $1 \; N \; 2$, and not $0 \; N \; 2$. Antisymmetric, vacuously: $x \; N \; y$ and $y \; N \; x$ would give $y = x + 1$ and $x = y + 1 = x + 2$, which is impossible, so no pair satisfies the hypothesis.

Exercise. B2: Example generation

Give an example of a relation on $\{1, 2, 3\}$ that is reflexive and transitive, but neither symmetric nor antisymmetric. Check each property. Then list the properties that every correct answer must have.

Solution. One answer:

$$R = \{(1,1), (2,2), (3,3), (1,2), (2,1), (1,3), (2,3)\}.$$

Reflexive: the three loops are in R. Not symmetric: $1 \; R \; 3$ and not $3 \; R \; 1$. Not antisymmetric: $1 \; R \; 2$, $2 \; R \; 1$ and $1 \neq 2$. Transitive: we check every two-step path $x \; R \; y \; R \; z$ with $x \neq y$ and $y \neq z$ (a step along a loop changes nothing). They are $1 \to 2 \to 1$, $1 \to 2 \to 3$, $2 \to 1 \to 2$ and $2 \to 1 \to 3$, and their shortcuts $(1,1)$, $(1,3)$, $(2,2)$, $(2,3)$ are all in R. Element 3 has no arrow out except its loop, so no other path exists.

Every correct answer must: - contain the three pairs $(1,1)$, $(2,2)$, $(3,3)$; - contain two different elements related **both** ways (to fail antisymmetry); - contain a pair related **one** way only (to fail symmetry); - contain the shortcut of every two-arrow path.

The second and fourth items together force more: if $a \; R \; b$, $b \; R \; a$ and $b \; R \; c$, transitivity puts $a \; R \; c$ in. First, there is only one two-way pair: two of them, say $\{a, b\}$ and $\{b, c\}$, give $a \; R \; c$ and $c \; R \; a$ by transitivity, so R is the full relation, which is symmetric. Call the two-way pair $\{a, b\}$ and the third element c. Every arrow between a and b is two-way, so a one-way arrow must have c at one end, and one such arrow is never enough: transitivity relates c to the other element of the pair too, in the same direction. For example, $\{(1,1), (2,2), (3,3), (1,2), (2,1), (3,1)\}$ fails transitivity, since $3 \; R \; 1 \; R \; 2$ and not $3 \; R \; 2$. If $c \; R \; a$, then $c \; R \; a \; R \; b$ gives $c \; R \; b$, and neither $a \; R \; c$ nor $b \; R \; c$ can hold, since that would make a second two-way pair; so both arrows point out of c. Likewise $a \; R \; c$ forces $b \; R \; c$, and both arrows point into c. Conversely, each of these six relations is a correct answer. Those

with c above the pair are the answer above with the elements renamed. Those with c below are obtained from them by reversing every arrow, which keeps the loops, the two-way pair and the one-way arrows, and keeps transitivity: a path $z \to y \to x$ of the reversed relation is the reverse of a path $x \to y \to z$, and the reverse of its shortcut (x, z) is (z, x). So $\{1, 2, 3\}$ carries exactly six correct answers: one for each choice of the two-way pair (three choices) and of whether the third element lies above the pair or below it (two choices); the answer above has 3 above the pair $\{1, 2\}$.

Exercise. B3: Intersections and unions

Let R and S be transitive relations on a set X. Prove that $R \cap S$ is transitive. Show by an example on $\{1, 2, 3\}$ that $R \cup S$ need not be transitive.

Solution. Let $x, y, z \in X$ with $(x, y) \in R \cap S$ and $(y, z) \in R \cap S$. Then $(x, y), (y, z) \in R$, so $(x, z) \in R$ because R is transitive; likewise $(x, z) \in S$. Hence $(x, z) \in R \cap S$.

For the union, let $R = \{(1, 2)\}$ and $S = \{(2, 3)\}$. Each is transitive, vacuously: in R a two-step path would need a pair starting at 2, and there is none; in S one would need a pair ending at 2. But $R \cup S = \{(1, 2), (2, 3)\}$ contains $(1, 2)$ and $(2, 3)$ and not $(1, 3)$, so it is not transitive. The intersection keeps both relations' shortcuts; the union creates paths that neither relation contains, so neither supplies their shortcuts.

Exercise. B4: Prove or disprove

Prove or disprove each statement. Here R and S are relations on a set X, and R^{-1} is the inverse relation (Definition 1.4.3).

(a) If R is reflexive on X and transitive, then $R \cap R^{-1}$ is an equivalence relation on X (reflexive on X, symmetric and transitive).

(b) If R and S are symmetric, then $R \cup S$ is symmetric.

(c) If R and S are antisymmetric, then $R \cup S$ is antisymmetric.

(d) If R is transitive, then R^{-1} is transitive.

(e) On $\mathbb{N}$, the relation "$x + y$ is a multiple of 3" is transitive.

Solution.

(a) True. Write $E \coloneqq R \cap R^{-1}$; so $(x, y) \in E$ means $x \mathrel{R} y$ and $y \mathrel{R} x$. *Reflexive.* For $x \in X$, $x \mathrel{R} x$ by reflexivity, so $(x, x) \in E$. *Symmetric.* The definition of E is symmetric in x and y. *Transitive.* Let $(x, y), (y, z) \in E$. From $x \mathrel{R} y$ and $y \mathrel{R} z$, transitivity gives $x \mathrel{R} z$; from $z \mathrel{R} y$ and $y \mathrel{R} x$, it gives $z \mathrel{R} x$. So $(x, z) \in E$.

(b) True. If $(x, y) \in R \cup S$, say $(x, y) \in R$, then $(y, x) \in R$ by symmetry of R, so $(y, x) \in R \cup S$; likewise if $(x, y) \in S$.

(c) False. On $X = \{1, 2\}$, $R = \{(1, 2)\}$ and $S = \{(2, 1)\}$ are antisymmetric (vacuously: neither relates two elements both ways), but $R \cup S$ contains $(1, 2)$ and $(2, 1)$, and $1 \neq 2$.

(d) True. Let $x \mathrel{R^{-1}} y$ and $y \mathrel{R^{-1}} z$, that is, $y \mathrel{R} x$ and $z \mathrel{R} y$. By transitivity of R, from $z \mathrel{R} y$ and $y \mathrel{R} x$, $z \mathrel{R} x$, that is, $x \mathrel{R^{-1}} z$.

(e) False. Take $x = 1$, $y = 2$, $z = 1$: $1 + 2 = 3$ and $2 + 1 = 3$ are multiples of 3, but $1 + 1 = 2$ is not: $2 = 3k$ fails for every integer k, since $k \leq 0$ gives $3k \leq 0$, and $k > 0$ gives $k \geq 1$ by Proposition 2.1.2 (c), hence $3k \geq 3$. (A triple with $x = z$ is allowed: transitivity quantifies over all x, y, z.)

4.1.5.3 C. Going deeper

Exercise. C1: Properties as equations between sets

Let R be a relation on X, let R^{-1} be its inverse relation (Definition 1.4.3), and let $\Delta_X \coloneqq \{(x, x) : x \in X\}$ be the diagonal.

(a) Prove that R is symmetric if and only if $R = R^{-1}$, and that R is antisymmetric if and only if $R \cap R^{-1} \subseteq \Delta_X$.

(b) Deduce that a relation that is both symmetric and antisymmetric satisfies $R \subseteq \Delta_X$. Is every subset of Δ_X both symmetric and antisymmetric?

Solution. Recall that $(x, y) \in R^{-1}$ if and only if $(y, x) \in R$.

(a) *Symmetric.* ($\Rightarrow$) Let R be symmetric. If $(x, y) \in R$, then $(y, x) \in R$, that is, $(x, y) \in R^{-1}$; so $R \subseteq R^{-1}$. If $(x, y) \in R^{-1}$, then $(y, x) \in R$, so $(x, y) \in R$ by symmetry; so $R^{-1} \subseteq R$. By Proposition 1.2.1, $R = R^{-1}$. ($\Leftarrow$) If $R = R^{-1}$ and $x \; R \; y$, then $(x, y) \in R^{-1}$, so $(y, x) \in R$.
Antisymmetric. A pair (x, y) lies in $R \cap R^{-1}$ exactly when $x \; R \; y$ and $y \; R \; x$, and it lies in Δ_X exactly when $x = y$ (by the characteristic property of pairs, Definition 1.4.1). So "$R \cap R^{-1} \subseteq \Delta_X$" says: for all $x, y \in X$, if $x \; R \; y$ and $y \; R \; x$, then $x = y$. That is antisymmetry, word for word.

(b) If R is symmetric and antisymmetric, then by (a), $R = R \cap R = R \cap R^{-1} \subseteq \Delta_X$. Conversely, every $R \subseteq \Delta_X$ is symmetric (each of its pairs is (x, x), which is its own reverse) and antisymmetric ($x \; R \; y$ already forces $x = y$). So the relations with both properties are exactly the subsets of the diagonal; equality, Δ_X itself, is the largest of them, and $\emptyset$ the smallest.

Exercise. C2: What symmetry and transitivity do give

Let R be a symmetric and transitive relation on X, and let $D \coloneqq \{x \in X : \exists y \in X \;\; x \; R \; y\}$ be its domain. Prove that $R \subseteq D \times D$ and that R, as a relation on D, is reflexive on D, symmetric and transitive.

Solution. $R \subseteq D \times D$. Let $(x, y) \in R$. Then $x \in D$, with witness y. By symmetry $y \; R \; x$, so $y \in D$, with witness x. Hence $(x, y) \in D \times D$.

Reflexive on D. Let $x \in D$. By the definition of D there is $y \in X$ with $x \; R \; y$; fix one (an $\exists$E, legitimate now, because $x \in D$ is exactly the statement $\exists y \in X \; x \; R \; y$). By symmetry $y \; R \; x$, and by transitivity, from $x \; R \; y$ and $y \; R \; x$, $x \; R \; x$.

Symmetric and transitive on D. These are implications about related elements, and every related pair lies in $D \times D$; so they hold on D because they hold on X.

This is the correct version of the false theorem in the warning: its argument proves reflexivity exactly on the set of elements for which "take y with $x\ R\ y$" is available. Elements outside D are related to nothing, and there reflexivity fails. In the language of Section 4.2, R is an equivalence relation on D.

Marking scheme. (10 points) - 2: shows $R \subseteq D \times D$, using symmetry to put the second coordinate in D. - 4: for reflexivity on D, obtains y with $x\ R\ y$ **from** $x \in D$, and says why this step is now legitimate. - 2: applies symmetry and then transitivity, in that order, to get $x\ R\ x$. - 2: explains why symmetry and transitivity restrict to D. Fatal errors (0 for the step): taking y with $x\ R\ y$ for an arbitrary $x \in X$ rather than $x \in D$ (the error of the warning); applying transitivity to $x\ R\ y$ and $x\ R\ y$.

4.2 Equivalence Relations and Partitions

Section 4.1 sorted relations by four properties: reflexive, symmetric, antisymmetric and transitive (Definition 4.1.1). This section studies the relations that have the first, second and fourth. They are the relations that say two things are "the same" in some respect, and each of them cuts its set into disjoint pieces of mutually "same" elements. We prove that the pieces always form a partition, and that every partition arises from exactly one such relation. Then we build the integers modulo n, and meet the check that every definition on pieces needs: that it does not depend on which element names the piece. Section 1.5 promised that check for functions defined on classes; here it is, with a method for making it.

4.2.1 Arithmetic on a clock

On a twelve-hour clock, five hours after nine o'clock it is two o'clock. People say "$9 + 5 = 2$ on a clock", and nobody is confused. Read as a statement about integers, it is false: $9 + 5 = 14$. So what is it a statement about?

The clock does not distinguish 2 from 14, or from 26 or -10: all of them put the hand in the same place. Two integers name the same hour when they differ by a multiple of 12. The sentence "$9 + 5 = 2$" is then about hours, and an hour is not one integer but a whole collection of them, $\{\ldots, -10, 2, 14, 26, \ldots\}$. The addition adds collections: take any integer from the first, any from the second, add them, and see which collection the sum lands in.

Two things have to be checked before this is mathematics. First, "differ by a multiple of 12" must behave like "is the same as": it must cut the integers into separate collections, and no integer may land in two of them. Second, the answer must not depend on the choice: if we take 21 for "nine" and -7 for "five", the sum 14 must still name two o'clock. It does, since $21 + (-7) = 14$. The first check is the theory of equivalence relations and partitions. The second is called **well-definedness**, and it comes at the end of the section.

4.2.2 Equivalence relations

Equality has three properties that every argument with "=" uses silently: $x = x$; if $x = y$, then $y = x$; and if $x = y$ and $y = z$, then $x = z$ (Logic and Proof, Proposition 5.7.1). They are exactly what lets us replace a thing by an equal thing, as often as we like, in either direction. "Same hour on the clock", "same remainder on division by 3" and "same absolute value" all have the same three properties, although none of them is equality. They deserve a common name.

An equivalence relation declares things the same in a way that behaves like equality.

Definition 4.2.1. Equivalence Relation

Let X be a set. An **equivalence relation on** X is a relation $\sim$ on X (Definition 1.4.3) that is reflexive, symmetric and transitive on X (Definition 4.1.1):

(Eq1) **for every** $x \in X$, $x \sim x$;

(Eq2) **for all** $x, y \in X$, if $x \sim y$, then $y \sim x$;

(Eq3) **for all** $x, y, z \in X$, if $x \sim y$ and $y \sim z$, then $x \sim z$.

When $x \sim y$, we say that x is **equivalent** to y (under $\sim$).

In words: (Eq1) says everything is the same as itself. (Eq2) says "the same" has no direction: if x counts as the same as y, then y counts as the same as x. (Eq3) says sameness passes along a chain: two things that are each the same as a third are linked through it. In symbols, (Eq1)–(Eq3) are

$$\forall x \in X \;\; x \sim x, \qquad \forall x, y \in X \;\; (x \sim y \to y \sim x),$$

$$\forall x, y, z \in X \;\; \big((x \sim y \wedge y \sim z) \to x \sim z\big).$$

The symbol $\sim$ is a letter for a relation, like R in Section 4.1; it is written between its arguments because it is read like $=$. Nothing needs checking for well-definedness: the definition names a property of a set of pairs.

Example. Four equivalence relations

Check (Eq1)–(Eq3) for each relation.

(a) Equality on any set X: $x \sim y$ if and only if $x = y$.

(b) The relation $X \times X$ on a set X, which relates every x to every y.

(c) "Same absolute value" on $\mathbb{R}$: $x \sim y$ if and only if $|x| = |y|$.

(d) The empty relation $\emptyset$ on the empty set.

Solution.

(a) (Eq1)–(Eq3) are the three properties of equality recalled above: $x = x$ is =I, and symmetry and transitivity are Logic and Proof, Proposition 5.7.1.

(b) Every pair (x, y) with $x, y \in X$ lies in $X \times X$, so each of (Eq1)–(Eq3) has a conclusion of the form $(u, v) \in X \times X$ with $u, v \in X$, and that conclusion is true. This is the coarsest sameness: everything is the same as everything.

(c) Each of (Eq1)–(Eq3) for $\sim$ is the same property for equality, applied to the numbers $|x|, |y|, |z|$. For instance, (Eq3): if $|x| = |y|$ and $|y| = |z|$, then $|x| = |z|$ by transitivity of $=$. Here $3 \sim -3$, and $3 \not\sim 2$.

(d) Each of (Eq1)–(Eq3) begins "for every element of X", and $X = \emptyset$ has none, so all three hold vacuously. The empty relation **is** an equivalence relation on $\emptyset$.

Part (c) is an instance of a pattern that returns later in this section, with the fibers of a function: "$x \sim y$ when some quantity attached to x equals the same quantity attached to y". Any such relation inherits (Eq1)–(Eq3) from equality.

Second reading · *The degenerate case and a non-example*

Part (d) is the degenerate case, and it is worth keeping: it says that the definition makes no demand on an empty set, so the theorems below hold for $X = \emptyset$ without a separate case. On a **non-empty** set the empty relation is not an equivalence relation: (Eq1) fails at any element x, since $(x, x) \notin \emptyset$. The same set of pairs passes on one set and fails on another, because (Eq1) speaks about every element of X.

A non-example by minimal change. On $\mathbb{R}$, let $x \sim y$ mean $x - y \in \mathbb{Z}$, and let $x \; R \; y$ mean $x - y \in \mathbb{N}$. The first is an equivalence relation, as an example later in this section checks. The second changes one letter. It is still reflexive, since $x - x = 0 \in \mathbb{N}$ by (($\mathbb{N}$)0), and still transitive: if $x - y \in \mathbb{N}$ and $y - z \in \mathbb{N}$, then $x - z = (x - y) + (y - z) \in \mathbb{N}$ by Lemma 2.1.1 (b). But it is not symmetric: $1 \; R \; 0$, since $1 - 0 = 1 \in \mathbb{N}$, while $0 - 1 = -1$, and $-1 \notin \mathbb{N}$ because every natural number is ≥ 0 (Lemma 2.1.1 (a)). The clause that fails is (Eq2). The relation R is the order $y \leq x$ restricted to pairs at integer distance; it has a direction, and sameness has none.

Second reading · *Why these three clauses*

Why these three clauses. Each clause has a job, and each failure has a witness.

- Drop (Eq1), and an element may be the same as nothing at all. On $\{1\}$, the empty relation is symmetric and transitive (Section 4.1's warning), and 1 is related to nothing; it would sit in no piece of the cutting.
- Drop (Eq2), and the pieces overlap. The relation $\leq$ on $\{1, 2\}$ is reflexive and transitive; the set of elements below 2 is $\{1, 2\}$, the set below 1 is $\{1\}$, and the two share 1 without being equal.
- Drop (Eq3), and sameness leaks. "$|x - y| \leq 1$" on $\mathbb{R}$ is reflexive and symmetric, and 0 is related to 1, 1 to 2, 2 to 3, and so on, while 0 is not related to 2. Every integer is linked to every other through a chain of steps of length 1, though few are related directly.

The name comes from "equal value": equivalent elements are equal in whatever respect the relation measures.

Warning. An equivalence relation is an equivalence relation **on a named set**. The relation $\{(1, 1), (2, 2)\}$ is equality on $\{1, 2\}$, an equivalence relation; on $\{1, 2, 3\}$ it is the same set of pairs and not an equivalence relation, since $(3, 3)$ is missing and (Eq1) fails at 3. Before checking (Eq1), name the set.

The payoff is the object the clock was after: the collection of everything that counts as the same as a given element.

4.2.3 Equivalence classes

An equivalence class is everything that counts as the same as one element.

Definition 4.2.2. Equivalence Class

Let $\sim$ be an equivalence relation on a set X, and let $a \in X$. The **equivalence class** of a is

$$[a] \coloneqq \{x \in X : x \sim a\}.$$

When the relation must be named, we write $[a]_{\sim}$. Any element of a class is called a **representative** of it.

The class is a subset of X, by specification (Definition 1.2.3). Its definition fixes the order of the letters as $x \sim a$; by (Eq2) the order does not matter, and $x \in [a]$ holds exactly when $a \sim x$.

For the four relations of Example (Four equivalence relations): under equality, $[a] = \{a\}$; under $X \times X$, $[a] = X$ for every $a \in X$; under "same absolute value", $[3] = \{-3, 3\}$ and $[0] = \{0\}$; and on the empty set there are no elements and so no classes.

Quick check. On $\{1, 2, \ldots, 30\}$, let $x \sim y$ mean that x and y have the same last digit. List the classes. How many are there, and how many elements has each?

Solution. The classes are $\{1, 11, 21\}$, $\{2, 12, 22\}$, $\ldots$, $\{9, 19, 29\}$ and $\{10, 20, 30\}$: ten classes, three elements each. Each class is the class of any of its elements; for instance $[11] = [21] = [1]$.

The quick check shows the features the theorem below proves in general: every class is non-empty, no number is in two classes, and every number is in one. A family of subsets with these three features has a name.

Definition 4.2.3. Partition

Let X be a set. A **partition** of X is a set $\mathcal{P}$ of subsets of X, called **blocks**, such that

(P1) every block is **non-empty**: $P \neq \emptyset$ for every $P \in \mathcal{P}$;
(P2) the blocks are **pairwise disjoint**: for all $P, Q \in \mathcal{P}$, if $P \neq Q$, then $P \cap Q = \emptyset$;
(P3) the blocks cover X: $\bigcup \mathcal{P} = X$.

Here $\bigcup \mathcal{P}$ is the union of the set of sets $\mathcal{P}$ (Definition 1.3.4): the set of points lying in some block. Since every block is a subset of X, the union is always a subset of X, and (P3) says that every $x \in X$ lies in **some** block. With (P2), it lies in **exactly one**: if $x \in P$ and $x \in Q$, then $P \cap Q \neq \emptyset$, so $P = Q$.

Examples: $\{\{1, 2\}, \{3\}\}$ is a partition of $\{1, 2, 3\}$. For a non-empty X, $\{X\}$ is a partition with one block, and $\{\{x\} : x \in X\}$ is one with a block for each point. The even and the odd integers form a partition of $\mathbb{Z}$ with two blocks, because every integer is even or odd and not both (Theorem 1.1.2). For $X = \emptyset$, the empty set of blocks $\mathcal{P} = \emptyset$ is a partition: (P1) and (P2) are vacuous, and $\bigcup \emptyset = \emptyset$.

Second reading · *Non-examples by minimal change*

Non-examples by minimal change. $\{\{1,2\},\{2,3\}\}$ covers $\{1,2,3\}$ and its sets are non-empty, but 2 lies in both, so (P2) fails. $\{\{1,2\},\{3\},\emptyset\}$ satisfies (P2) and (P3), and fails (P1). Without (P1), "the block containing x" would still be unique, but a partition could carry useless empty blocks, and the correspondence with equivalence relations below would break, since no class is empty.

A partition is a set of subsets of X. So is the set of all classes of an equivalence relation, and it gets its own name.

Definition 4.2.4. Quotient Set

Let $\sim$ be an equivalence relation on a set X. The **quotient set** of X by $\sim$ is the set of all equivalence classes,

$$X/\!\sim \coloneqq \{C \in \mathcal{P}(X) : C = [a] \text{ for some } a \in X\}.$$

The **quotient map** is $q\colon X \to X/\!\sim$, $q(a) \coloneqq [a]$.

The quotient set is a set by specification inside $\mathcal{P}(X)$ (Definition 1.2.3, Definition 1.3.2), and it is often written $\{[a] : a \in X\}$. The quotient map is a function by Definition 1.5.1: each $a \in X$ has the value $[a]$, which lies in $X/\!\sim$, and only that value. It is **surjective**: an element of $X/\!\sim$ is $[a]$ for some $a \in X$, and then it is $q(a)$ (Definition 1.5.4). The quotient map forgets everything about a except which class it lies in, and that is the point of it. Read "$X/\!\sim$" as "X with equivalent elements identified".

4.2.4 The classes form a partition

Here is the theorem the clock needs. It also says exactly when two names give the same class.

Theorem 4.2.1. Equivalence Classes Partition the Set

Let $\sim$ be an equivalence relation on a set X.

(a) For every $a \in X$, $a \in [a]$; in particular every class is non-empty.
(b) For all $a, b \in X$, $[a] = [b]$ **if and only if** $a \sim b$.
(c) For all $a, b \in X$, if $[a] \cap [b] \neq \emptyset$, then $[a] = [b]$.
(d) The quotient set $X/\!\sim$ is a partition of X.

Idea. Each property of $\sim$ does one job. Reflexivity puts a in its own class, which gives (a) and the covering. For (b), a class is determined by any one of its elements: if $a \sim b$, then anything the same as a is the same as b, by transitivity, and the reverse needs symmetry first. For (c), a common element c of two classes has $c \sim a$ and $c \sim b$; symmetry turns the first around, transitivity joins the two, and (b) finishes. Then (d) is (a), (c) and the covering, read against the three clauses of Definition 4.2.3. (b) is a double inclusion (Example (Method: two inclusions)).

Before reading on: which property of $\sim$ does each line use?

Proof. *(a)* Let $a \in X$. By (Eq1), $a \sim a$, so $a \in [a]$ by Definition 4.2.2. Hence $[a] \neq \emptyset$.

(b) ($\Rightarrow$) Suppose $[a] = [b]$. By (a), $a \in [a] = [b]$, so $a \sim b$.

($\Leftarrow$) Suppose $a \sim b$. ($\subseteq$) Let $x \in [a]$, so $x \sim a$. With $a \sim b$, (Eq3) gives $x \sim b$, so $x \in [b]$. ($\supseteq$) Let $x \in [b]$, so $x \sim b$. By (Eq2) applied to $a \sim b$, $b \sim a$; with $x \sim b$, (Eq3) gives $x \sim a$, so $x \in [a]$. Hence $[a] = [b]$ by Proposition 1.2.1.

(c) Suppose $[a] \cap [b] \neq \emptyset$, and let $c \in [a] \cap [b]$. Then $c \sim a$ and $c \sim b$. By (Eq2), $a \sim c$; with $c \sim b$, (Eq3) gives $a \sim b$. By (b), $[a] = [b]$.

(d) We check the clauses of Definition 4.2.3 for $\mathcal{P} := X/\!\sim$, a set of subsets of X by Definition 4.2.4.

(P1) Every element of $X/\!\sim$ is $[a]$ for some $a \in X$, and is non-empty by (a).

(P2) Let $C, D \in X/\!\sim$ with $C \neq D$, say $C = [a]$ and $D = [b]$. If $C \cap D \neq \emptyset$, then $C = D$ by (c), which is false. Hence $C \cap D = \emptyset$.

(P3) Every class is a subset of X, so $\bigcup X/\!\sim \subseteq X$. Conversely, let $x \in X$. Then $x \in [x]$ by (a), and $[x] \in X/\!\sim$, so $x \in \bigcup X/\!\sim$. Hence $\bigcup X/\!\sim = X$ by Proposition 1.2.1.

This proves the theorem. ∎

Part (b) is the rule we will use most. It turns a statement about classes, $[a] = [b]$, into a statement about elements, $a \sim b$, and back. On the clock: $[14] = [2]$ because $14 - 2 = 12$ is a multiple of 12. Part (c) says that two classes are either equal or disjoint; there is no third possibility.

Second reading · *When the quotient map is injective, and what $\leq$ lacked*

By (b), the quotient map q of Definition 4.2.4 has $q(a) = q(b)$ exactly when $a \sim b$. So q is injective only when every class has a single element: two different elements x, y of one class $[c]$ have $[x] = [c] = [y]$ by (b), so $q(x) = q(y)$. That is what the relations of "Why these three clauses" lacked: for $\leq$, the sets $[2] = \{1, 2\}$ and $[1] = \{1\}$ given by the formula of Definition 4.2.2 overlap and differ, and with $a = 2$, $b = 1$, $c = 1$ the line of (c) that fails is the one that uses (Eq2) (Exercise A1(c)).

Warning. A class has many names. In the quick check, [1], [11] and [21] are one set, and nothing about that set prefers 1. So any argument or definition that starts from "$[a]$" and then uses a itself (its size, its sign, its last digit) must be shown not to depend on which representative was chosen. "The smallest element of $[a]$" makes sense for the last-digit classes;

"$[a+1]$" as a function of the class $[a]$ needs a proof, which the section supplies for congruences under "Operations on classes".

4.2.5 Every partition comes from one equivalence relation

The theorem turns an equivalence relation into a partition. The reverse is just as natural: given the blocks, call two points "the same" when they lie in a common block.

Theorem 4.2.2. Partitions and Equivalence Relations Correspond

Let X be a set.

(a) Let $\mathcal{P}$ be a partition of X. For $x, y \in X$, let $x \sim_{\mathcal{P}} y$ mean that there is a block $P \in \mathcal{P}$ with $x \in P$ and $y \in P$. Then $\sim_{\mathcal{P}}$ is an equivalence relation on X, and its classes are the blocks: $X/\sim_{\mathcal{P}} = \mathcal{P}$.

(b) Let $\sim$ be an equivalence relation on X. Then $\sim_{X/\sim}$, the relation of (a) for the partition $X/\sim$, is $\sim$ itself.

(c) Hence every partition of X is the quotient set of **exactly one** equivalence relation on X, namely $\sim_{\mathcal{P}}$.

Idea. For (a), (Eq1) and (Eq2) are immediate from (P3) and the symmetry of "lie in a common block". The real work is (Eq3): x, y lie in one block and y, z in another, and we need one block holding x and z. The two blocks share y, so (P2) makes them equal. The classes are the blocks because each point lies in exactly one block. Then (b) is Theorem 4.2.1 (b) in disguise, and (c) puts (a) and (b) together.

Proof. *(a)* (Eq1) Let $x \in X$. By (P3), $x \in \bigcup \mathcal{P}$, so $x \in P$ for some $P \in \mathcal{P}$; this block contains x and x, so $x \sim_{\mathcal{P}} x$. (Eq2) If a block contains x and y, it contains y and x. (Eq3) Let $x \sim_{\mathcal{P}} y$ and $y \sim_{\mathcal{P}} z$. Take a block P with $x, y \in P$, and a block Q with $y, z \in Q$. Then $y \in P \cap Q$, so $P \cap Q \neq \emptyset$, and $P = Q$ by (P2). Hence $x, z \in P$, and $x \sim_{\mathcal{P}} z$.

Now the classes. Let $x \in X$, and let P be a block with $x \in P$ (one exists by (P3)). We show $[x] = P$, the class taken under $\sim_{\mathcal{P}}$. ($\subseteq$) Let $y \in [x]$, so $y \sim_{\mathcal{P}} x$: some block Q contains y and x. Then $x \in P \cap Q$, so $Q = P$ by (P2), and $y \in P$. ($\supseteq$) Let $y \in P$. Then P contains y and x, so $y \sim_{\mathcal{P}} x$, and $y \in [x]$.

So every class is a block: $[x]$ is the block containing x. Conversely, every block P is nonempty by (P1); for any $x \in P$, the argument just given shows $P = [x]$. Hence $X/\sim_{\mathcal{P}} = \mathcal{P}$, each inclusion being one of the last two sentences.

(b) Both relations are subsets of $X \times X$, so we show that they contain the same pairs (Definition 1.2.1). Let $x, y \in X$. If $x \sim y$, then the class $[y] \in X/\sim$ contains y by Theorem 4.2.1 (a) and, by Definition 4.2.2, x; so $x \sim_{X/\sim} y$. Conversely, if $x \sim_{X/\sim} y$, some class $[a]$ contains x and y, so $x \sim a$ and $y \sim a$. By (Eq2), $a \sim y$, and by (Eq3), $x \sim y$.

(c) By (a), $\mathcal{P}$ is the quotient set of $\sim_{\mathcal{P}}$. Suppose $\mathcal{P} = X/\sim$ for an equivalence relation $\sim$. Then, by (b), $\sim$ is $\sim_{X/\sim}$, the relation of (a) for the partition $X/\sim = \mathcal{P}$; that is, $\sim$ is $\sim_{\mathcal{P}}$. So

there is exactly one such relation. This proves the theorem.

■

So the two passages undo each other. Going from $\sim$ to $X/\sim$ and back gives $\sim$ again, by (b); going from $\mathcal{P}$ to $\sim_{\mathcal{P}}$ and back gives $\mathcal{P}$ again, by (a). An equivalence relation and a partition are two descriptions of one structure: the relation says which pairs are the same, and the partition lists the piles. This is the move *classes from a relation, a relation from classes*, and we choose whichever description makes the next step easier.

A correspondence, proved both ways. Put this in the language of Section 1.6. Write $\mathrm{Eq}(X)$ for the set of equivalence relations on X (a subset of $\mathcal{P}(X \times X)$) and $\mathrm{Part}(X)$ for the set of partitions (a subset of $\mathcal{P}(\mathcal{P}(X))$). Together with Theorem 4.2.1, the theorem gives two functions, $\Phi\colon \mathrm{Eq}(X) \to \mathrm{Part}(X)$, $\Phi(\sim) \coloneqq X/\sim$ (a partition by Theorem 4.2.1), and $\Psi\colon \mathrm{Part}(X) \to \mathrm{Eq}(X)$, $\Psi(\mathcal{P}) \coloneqq \sim_{\mathcal{P}}$ (an equivalence relation by part (a)). Part (a) says $\Phi \circ \Psi = \mathrm{id}_{\mathrm{Part}(X)}$, and part (b) says $\Psi \circ \Phi = \mathrm{id}_{\mathrm{Eq}(X)}$. So each is the other's two-sided inverse, and both are bijections (Theorem 1.6.4): the method of Example (Method: construct and verify), with both composites checked. To count the equivalence relations on a finite set, count its partitions.

Quick check. How many equivalence relations on $\{1, 2, 3, 4\}$ have exactly two classes?

Solution. Seven. By the correspondence, count partitions into two blocks. Either one block is a singleton and the other has three elements, and the singleton can be chosen in four ways; or both blocks are pairs, and the pair containing 1 is fixed by its second element, chosen in three ways. So $4 + 3 = 7$.

The transitivity step in (a) is where (P2) does its real work (the classes part uses it again, the same way), and it is the step that a hasty proof skips. If the blocks were allowed to overlap, as in the cover $\{\{1, 2\}, \{2, 3\}\}$ of $\{1, 2, 3\}$, then "lie in a common set" would relate 1 to 2 and 2 to 3 but not 1 to 3.

4.2.6 Congruence modulo n

Back to the clock, with any number of hours. The divisibility notation $d \mid m$, "there is $k \in \mathbb{Z}$ with $m = kd$", is Definition 1.1.2.

Definition 4.2.5. Congruence Modulo n

Let $n \in \mathbb{Z}_{>0}$. Integers a and b are **congruent modulo** n, written $a \equiv b \pmod{n}$, if $n \mid a - b$, that is, if $a - b = kn$ for some $k \in \mathbb{Z}$.

So $14 \equiv 2 \pmod{12}$, since $14 - 2 = 1 \cdot 12$; $-10 \equiv 2 \pmod{12}$, since $-10 - 2 = (-1) \cdot 12$; and $7 \not\equiv 2 \pmod{12}$, since 5 is not a multiple of 12 (the multiples $12k$ are 0 for $k = 0$, at least 12 for $k \geq 1$ and at most -12 for $k \leq -1$, by discreteness, Proposition 2.1.2 (c)). The symbol $\equiv$ here always carries its modulus, so it does not clash with the semantic equivalence $\varphi \equiv \psi$ of *Logic and Proof*, Chapter 4.

Second reading · *Why $n \geq 1$*

Why $n \geq 1$? The condition makes sense for $n = 0$, but it says nothing new: $0 \mid a - b$ means $a - b = k \cdot 0 = 0$, so "congruence modulo 0" is equality on $\mathbb{Z}$. Its classes would be the singletons $\{a\}$, a copy of $\mathbb{Z}$ and not $\mathbb{Z}$ itself, and the count of classes proved below would fail. Excluding $n = 0$ keeps that count exact.

Proposition 4.2.3. Congruence Is an Equivalence Relation

For every $n \in \mathbb{Z}_{>0}$, congruence modulo n is an equivalence relation on $\mathbb{Z}$.

Proof. (Eq1) $a - a = 0 = 0 \cdot n$, and $0 \in \mathbb{Z}$. (Eq2) If $a - b = kn$ with $k \in \mathbb{Z}$, then $b - a = (-k)n$, and $-k = 0 - k \in \mathbb{Z}$ by Proposition 2.1.2 (a). (Eq3) If $a - b = kn$ and $b - c = ln$ with $k, l \in \mathbb{Z}$, then $a - c = (a - b) + (b - c) = (k + l)n$, and $k + l \in \mathbb{Z}$ by Proposition 2.1.2 (a). ■

The quotient set is written $\mathbb{Z}/n$, "the integers modulo n". Its elements are the **residue classes** $[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\} = \{a + kn : k \in \mathbb{Z}\}$; the second form holds because $x \equiv a$ means $x - a = kn$, that is, $x = a + kn$. When two moduli are in play we write $[a]_n$ for the class of a in $\mathbb{Z}/n$. For example, $[2]_{12} = \{\ldots, -22, -10, 2, 14, 26, \ldots\}$, the integers that name two o'clock.

How many classes are there? The clock has twelve positions, and the division algorithm says why: each integer has exactly one remainder among $0, 1, \ldots, 11$.

Proposition 4.2.4. The Integers Modulo n

Let $n \in \mathbb{Z}_{>0}$. For every $a \in \mathbb{Z}$ there is **exactly one** $r \in \{0, \ldots, n - 1\}$ with $[a] = [r]$ in $\mathbb{Z}/n$, namely the remainder of a on division by n. Hence

$$\mathbb{Z}/n = \{[0], [1], \ldots, [n - 1]\},$$

and the n classes listed are pairwise different.

Here $n - 1 \in \mathbb{N}$ by Lemma 2.1.1 (c), since $n \neq 0$, so $\{0, \ldots, n - 1\}$ is the set of Section 2.1.

Proof. Let $a \in \mathbb{Z}$. By Theorem 2.2.3 there are $q, r \in \mathbb{Z}$ with $a = qn + r$ and $0 \leq r < n$. Since $r \geq 0$, $r \in \mathbb{N}$ (Proposition 2.1.2 (b)); since $r < n$, $r + 1 \leq n$ by discreteness (Proposition 2.1.2 (c)), so $r \leq n - 1$. Hence $r \in \{0, \ldots, n - 1\}$. Also $a - r = qn$, so $a \equiv r \pmod{n}$, and $[a] = [r]$ by Theorem 4.2.1 (b).

For uniqueness, let $r, s \in \{0, \ldots, n - 1\}$ with $[a] = [r]$ and $[a] = [s]$. Then $[r] = [s]$, so $r \equiv s \pmod{n}$ by Theorem 4.2.1 (b): $r - s = kn$ for some $k \in \mathbb{Z}$. So the integer r can be written both as $r = 0 \cdot n + r$ and as $r = kn + s$, and both remainders r and s satisfy $0 \leq r, s < n$. By the uniqueness in Theorem 2.2.3, $s = r$.

Finally, every element of $\mathbb{Z}/n$ is $[a]$ for some $a \in \mathbb{Z}$, hence equal to one of $[0], \ldots, [n - 1]$;

and if $[r] = [s]$ with $r, s \in \{0, \dots, n-1\}$, the uniqueness just proved, applied to $a = r$, gives $r = s$. This proves the proposition.

■

So $\mathbb{Z}/12$ has exactly the twelve classes $[0], \dots, [11]$, one for each position of the hand. (The clock face writes 12 where we write $[0]$, and $[12] = [0]$.) The uniqueness also gives a test that is often quicker than the definition: $a \equiv b \pmod{n}$ **if and only if** a and b leave the same remainder on division by n. Indeed, if $a \equiv b$, then $[a] = [b]$, and the one r with $[a] = [r]$ is also the one with $[b] = [r]$; conversely, if both leave the remainder r, then $[a] = [r] = [b]$. With $n = 2$, the two classes of $\mathbb{Z}/2$ are the even integers $[0]$ and the odd integers $[1]$: the partition of $\mathbb{Z}$ into evens and odds is the quotient set of congruence modulo 2.

4.2.7 Two more sources of equivalence relations

Congruence is one way to manufacture an equivalence relation. Here is the most general way, and a second example on the real line that later chapters return to.

Example. The fibers of a function

Let $f\colon X \to Y$ be a function, and for $x, y \in X$ let $x \sim_f y$ mean $f(x) = f(y)$. Show that $\sim_f$ is an equivalence relation on X, and describe its classes. Then show that every equivalence relation $\sim$ on X is of this form, for a suitable function.

Solution. (Eq1)–(Eq3) for $\sim_f$ are the properties of equality applied to the values $f(x), f(y), f(z)$, exactly as in Example (Four equivalence relations) (c): $f(x) = f(x)$; $f(x) = f(y)$ gives $f(y) = f(x)$; and $f(x) = f(y)$, $f(y) = f(z)$ give $f(x) = f(z)$ (Logic and Proof, Proposition 5.7.1).

The class of $a \in X$ is

$$[a] = \{x \in X : f(x) = f(a)\} = f^{-1}(\{f(a)\}),$$

the preimage of the one-point set $\{f(a)\}$ (Definition 1.7.2). Such a preimage $f^{-1}(\{y\})$ is called the **fiber** of f over y. So the classes of $\sim_f$ are the fibers over the points y of the range $f(X)$. A fiber over a point outside the range is empty, and is not a class: (P1) is what excludes it.

For the converse, let $\sim$ be an equivalence relation on X, and take for f the quotient map $q\colon X \to X/\!\sim$ of Definition 4.2.4. Then, for $x, y \in X$,

$$x \sim_q y \iff q(x) = q(y) \iff [x] = [y] \iff x \sim y,$$

where the last step is Theorem 4.2.1 (b). So $\sim_q$ and $\sim$ contain the same pairs, and are equal (Definition 1.2.1).

Two instances. For $f(x) = |x|$ on $\mathbb{R}$, $\sim_f$ is "same absolute value", and the fiber over 3 is the class $\{-3, 3\}$. For the map $\mathbb{Z} \to \{0, 1, 2\}$ sending each integer to its remainder on division by 3 (a function by the uniqueness in Theorem 2.2.3), $\sim_f$ is congruence modulo 3, by the remainder test above. The example says that "the same in some respect" always means "equal value of

some function": an equivalence relation is the same thing as a function, up to the names of its values.

Example. The reals modulo the integers

On $\mathbb{R}$, let $x \sim y$ mean $x - y \in \mathbb{Z}$. Show that $\sim$ is an equivalence relation. Find the classes of 0, of $\frac{1}{2}$ and of $\sqrt{2}$, and show that these three classes are different.

Solution. An equivalence relation. (Eq1) $x - x = 0 \in \mathbb{Z}$. (Eq2) If $x - y \in \mathbb{Z}$, then $y - x = 0 - (x - y) \in \mathbb{Z}$, by Proposition 2.1.2 (a). (Eq3) If $x - y \in \mathbb{Z}$ and $y - z \in \mathbb{Z}$, then $x - z = (x - y) + (y - z) \in \mathbb{Z}$, by Proposition 2.1.2 (a).

The classes. $[0] = \{x \in \mathbb{R} : x - 0 \in \mathbb{Z}\} = \mathbb{Z}$. Next, $x \in [\frac{1}{2}]$ means $x - \frac{1}{2} = k$ for some $k \in \mathbb{Z}$, so

$$[\tfrac{1}{2}] = \{k + \tfrac{1}{2} : k \in \mathbb{Z}\} = \{\dots, -\tfrac{3}{2}, -\tfrac{1}{2}, \tfrac{1}{2}, \tfrac{3}{2}, \dots\},$$

and in the same way $[\sqrt{2}] = \{\sqrt{2} + k : k \in \mathbb{Z}\} = \{\dots, \sqrt{2} - 1, \sqrt{2}, \sqrt{2} + 1, \dots\}$.

Three different classes. By Theorem 4.2.1 (b), two classes $[x]$ and $[y]$ are equal exactly when $x - y \in \mathbb{Z}$. A real number t with $0 < t < 1$ is not an integer: if it were, discreteness (Proposition 2.1.2 (c)) applied to $0 < t$ would give $1 \leq t$. Now $\frac{1}{2} - 0 = \frac{1}{2}$ lies strictly between 0 and 1, so $[\frac{1}{2}] \neq [0]$. Since $\sqrt{2} \geq 0$ and $(\sqrt{2})^2 = 2$, Logic and Proof, Theorem 2.4.5 rules out $\sqrt{2} \leq 1$ (it would give $2 \leq 1$) and $2 \leq \sqrt{2}$ (it would give $4 \leq 2$), so $1 < \sqrt{2} < 2$, and $0 < \sqrt{2} - 1 < 1$; then $\sqrt{2} - 1 \notin \mathbb{Z}$, and therefore $\sqrt{2} - 0 \notin \mathbb{Z}$ (else $\sqrt{2} - 1$ would be a difference of integers), so $[\sqrt{2}] \neq [0]$. Finally, in the same way $\sqrt{2} \leq \frac{1}{2}$ would give $2 \leq \frac{1}{4}$, and $\frac{3}{2} \leq \sqrt{2}$ would give $\frac{9}{4} \leq 2$, so $\frac{1}{2} < \sqrt{2} < \frac{3}{2}$, and $0 < \sqrt{2} - \frac{1}{2} < 1$, and $[\sqrt{2}] \neq [\frac{1}{2}]$.

Picture each class as one point of a circle of circumference 1: the real line is wound around it, and two numbers land on the same point when they differ by an integer. Each class has exactly one representative in $[0, 1)$: the class of $\sqrt{2}$ meets $[0, 1)$ in $\sqrt{2} - 1$, for instance. Proving this for every class needs the integer part of a real number, which *Analysis on the Real Line*, Chapter 1 constructs; we do not use it here.

↻ **Second reading** · *A set with no length*

With $\mathbb{Q}$ in place of $\mathbb{Z}$, the relation "$x - y \in \mathbb{Q}$" is again an equivalence relation on $\mathbb{R}$, and choosing one point from each of its classes is how *Measure and Integration*, Chapter 1 builds a set of real numbers that has no length.

4.2.8 Operations on classes

Now the second check of the clock. To add hours we want to define

$$[a] + [b] \coloneqq [a + b] \qquad \text{in } \mathbb{Z}/n.$$

The right-hand side is computed from the representatives a and b. If another pair of representatives of the same two classes gave a different class, the "definition" would assign two answers to one input, and Definition 1.5.1 forbids that: a function gives each input **exactly one** value.

So the definition is legitimate only if the answer does not depend on the representatives. That property is called **well-definedness**, and it was met in Section 1.5, where "write a rational number as p/q, then send it to its numerator p" failed to be a function (Example (Relations that are not functions)).

Proposition 4.2.5. Congruence Respects Sums and Products

Let $n \in \mathbb{Z}_{>0}$ and $a, a', b, b' \in \mathbb{Z}$. If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then

$$a + b \equiv a' + b' \pmod{n} \qquad \text{and} \qquad ab \equiv a'b' \pmod{n}.$$

Hence the operations $[a] + [b] \coloneqq [a + b]$ and $[a][b] \coloneqq [ab]$ on $\mathbb{Z}/n$ are **well defined**.

Idea (Scratch work). The rule $[a] + [b] \coloneqq [a + b]$ reads representatives. So take two representatives of each class, a, a' and b, b', and compare the outputs. By Theorem 4.2.1 (b), equal classes means congruent representatives, and a congruence unwinds to a "there exists" (Definition 4.2.5): name the multipliers, with different names.

Givens	Goal
$[a] = [a']$, $[b] = [b']$	$[a + b] = [a' + b']$ and $[ab] = [a'b']$
$a - a' = kn$, $b - b' = ln$, with $k, l \in \mathbb{Z}$	$(a + b) - (a' + b') = mn$ and $ab - a'b' = m'n$ for some $m, m' \in \mathbb{Z}$
the same	sum: $(a - a') + (b - b') = (k + l)n$, done; product: $ab - a'b'$ changes both factors at once, and neither given appears
the same	$ab - a'b' = (ab - ab') + (ab' - a'b') = a(b - b') + (a - a')b'$: change one factor at a time

The last row closes the gap: each bracket is a given times an integer, so $m' = al + kb'$. The proof writes this forwards.

Proof. Write $a - a' = kn$ and $b - b' = ln$ with $k, l \in \mathbb{Z}$. Then

$$(a + b) - (a' + b') = (a - a') + (b - b') = (k + l)n,$$

and $k + l \in \mathbb{Z}$ by Proposition 2.1.2 (a). For the product,

$$\begin{aligned} ab - a'b' &= a(b - b') + (a - a')b' \\ &= (al + kb')n, \end{aligned}$$

and $al + kb' \in \mathbb{Z}$ by Proposition 2.1.2 (a). This proves both congruences.

For well-definedness, suppose $[a] = [a']$ and $[b] = [b']$. By Theorem 4.2.1 (b), $a \equiv a'$ and $b \equiv b'$, so $a + b \equiv a' + b'$ and $ab \equiv a'b'$ by what was just proved, and $[a + b] = [a' + b']$ and $[ab] = [a'b']$, again by Theorem 4.2.1 (b). So the class assigned to the pair of classes $([a], [b])$ is the same whichever representatives are used.

■

In the language of Definition 1.5.1: the addition of $\mathbb{Z}/n$ is the function $\mathbb{Z}/n \times \mathbb{Z}/n \to \mathbb{Z}/n$ whose graph is the set of all pairs $(([a],[b]),[a+b])$ with $a, b \in \mathbb{Z}$. Clause (Fn1) holds because every element of $\mathbb{Z}/n$ is a class $[a]$; clause (Fn2) is the proposition. The clock sentence of the opening is now a true statement: in $\mathbb{Z}/12$,

$$[9] + [5] = [14] = [2],$$

the first equality by the definition of $+$, the second because $14 - 2 = 12$. And $[21] + [-7] = [14] = [2]$ as well, as the proposition guarantees.

Example. Method: checking that a definition on classes is well defined

Template. For a rule on $X/\sim$ that reads a representative a: (1) take two representatives of one class, $a \sim a'$ (Theorem 4.2.1 (b)); (2) unwind $a \sim a'$, naming any witness; (3) show the outputs equal in the codomain's sense (as classes, if it is a quotient set); (4) every class has a representative, and its value lies in the codomain (Fn1); (1)–(3) make the value unique (Fn2). To refute, give one pair $a \sim a'$ with different outputs.

When to use it. A definition picks one name for something that has many: operations on $\mathbb{Z}/n$, maps out of a quotient set, "write r as p/q", the size of a finite set.

The usual failure. Checking one pair only; proving the converse, which is injectivity (Example (Method: proving injectivity)); comparing classes as elements; an output outside the codomain.

Quick check. Which rules define a function: (a) $\mathbb{Z}/6 \to \mathbb{Z}$, $[a] \mapsto a^2$; (b) $\mathbb{Z}/6 \to \mathbb{Z}/3$, $[a]_6 \mapsto [a^2]_3$?

Solution.

(a) No: $[0] = [6]$, but $0^2 = 0 \neq 36 = 6^2$, and the codomain $\mathbb{Z}$ compares elements, not classes. (b) Yes: if $a - a' = 6k$ with $k \in \mathbb{Z}$, then $a^2 - a'^2 = (a-a')(a+a') = 3 \cdot 2k(a+a')$, and $2k(a+a') \in \mathbb{Z}$ (Proposition 2.1.2 (a)), so $[a^2]_3 = [a'^2]_3$.

Well-definedness can fail, and the next example shows a failure next to a success, with the minimal change between them.

Example. A rule on classes that is not a function

Decide whether each rule defines a function: (a) $F\colon \mathbb{Z}/6 \to \mathbb{Z}/4$, $F([a]_6) \coloneqq [a]_4$; (b) $G\colon \mathbb{Z}/6 \to \mathbb{Z}/3$, $G([a]_6) \coloneqq [a]_3$.

Solution.

(a) No. The class $[0]_6$ is also $[6]_6$, since $6 - 0 = 1 \cdot 6$. Read with the representative 0, the rule gives $[0]_4$; read with 6, it gives $[6]_4 = [2]_4$, since $6 - 2 = 1 \cdot 4$. And $[0]_4 \neq [2]_4$, since

$2 - 0 = 2$ is not a multiple of 4 ($0 < 2 < 4$, and the multiples of 4 are 0, at least 4, or at most -4). So one input receives two values, and (Fn2) of Definition 1.5.1 fails.

(b) Yes. If $[a]_6 = [a']_6$, then $a - a' = 6k$ for some $k \in \mathbb{Z}$ (Theorem 4.2.1 (b)), so $a - a' = 3(2k)$ with $2k \in \mathbb{Z}$ (Proposition 2.1.2 (a)), and $[a]_3 = [a']_3$. The value does not depend on the representative. What made it work is $3 \mid 6$: a multiple of 6 is a multiple of 3, while a multiple of 6, such as 6 itself, need not be a multiple of 4.

That is the method of Example (Method: checking that a definition on classes is well defined), applied once with success and once with failure.

The check is not special to congruences. Section 2.5 met it for the number of elements of a finite set.

Example. Same size, revisited

Let X be a set, and for $A, B \in \mathcal{P}(X)$ let $A \approx B$ mean $|A| = |B|$ (Definition 2.5.1). (a) Show that $\approx$ is an equivalence relation on $\mathcal{P}(X)$. (b) For $X = \{1, 2, 3\}$, list the classes. (c) For $X = \{1, 2, 3\}$, show that the rule sending the class of A to the number of elements of A is a well-defined function $\mathcal{P}(X)/\!\approx \to \{0, 1, 2, 3\}$.

Solution.

(a) (Eq1)–(Eq3) are Proposition 2.5.1 (a)–(c), read for subsets of X.

(b) Every subset of $\{1, 2, 3\}$ is finite with $0, 1, 2$ or 3 elements (Proposition 2.5.6, since $\{1, 2, 3\}$ has 3 elements; or list the eight subsets). Two subsets with the same number m of elements are equivalent: $|\{1, \ldots, m\}| = |A|$ and $|\{1, \ldots, m\}| = |B|$ give $|A| = |B|$ by Proposition 2.5.1 (b) and (c). Two with different numbers are not, by (c) below. So the classes are $\{\emptyset\}$, $\{\{1\}, \{2\}, \{3\}\}$, $\{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$ and $\{\{1, 2, 3\}\}$.

(c) By the method of Example (Method: checking that a definition on classes is well defined): let $A \approx A'$, and let A have m elements and A' have m'. From $|A| = |A'|$ we get $|A'| = |A|$ (Proposition 2.5.1 (b)); with $|\{1, \ldots, m'\}| = |A'|$, part (c) of that proposition gives that A has m' elements as well, so $m = m'$ by Corollary 2.5.4. Each class has a representative, its number lies in $\{0, 1, 2, 3\}$ by part (b) of this example, and all its representatives give the same number.

Part (c) rests on the well-definedness step of Section 2.5 (Corollary 2.5.4: one set, one number) and adds a second: one class, one number. And the relation lives on $\mathcal{P}(X)$, a set: for equinumerosity between arbitrary sets there is no set of all sets for it to be a relation on (Theorem 1.2.4), which is why Section 2.5 said only that it behaves like an equivalence relation.

Remark (Looking ahead). The clock does not stop here. *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Section 3.4 builds $\mathbb{Z}/n$ again, on the constructed integers, as a quotient ring: the check of Proposition 4.2.5 is made once for every ideal, and the sum and product obey the laws of a ring.

4.2.9 Exercises

4.2.9.1 A. Check your understanding

Exercise. A1

Parts (a)–(d) are about Theorem 4.2.1 and its proof.

(a) Which property of $\sim$ is used to show that every class is non-empty, and which properties are used to show that two overlapping classes are equal?

(b) Run the proof of part (c) for congruence modulo 3, with $a = 4$, $b = 10$ and the common element $c = 7$: write each line with its numbers.

(c) On $\{1, 2, 3\}$, let $x \sim y$ mean $x \leq y$, and define $[a]$ by the formula of Definition 4.2.2. Show that $[2]$ and $[1]$ overlap without being equal, and name the line of the proof of part (c) that fails, with $a = 2$, $b = 1$.

(d) Give the idea of the proof of part (c) in two sentences.

(e) How many classes has the relation $x^2 = y^2$ on $\{-2, -1, 0, 1, 2\}$? List them.

(f) To show that a rule $[a] \mapsto \ldots$ on $\mathbb{Z}/n$ is well defined, what do you assume and what do you show?

Solution.

(a) Non-emptiness uses only reflexivity (Eq1): $a \sim a$ puts a in $[a]$. Overlapping classes are equal by symmetry (Eq2), which turns $c \sim a$ into $a \sim c$, and transitivity (Eq3), which joins $a \sim c$ and $c \sim b$; the final step, part (b), uses (Eq2) and (Eq3) again.

(b) Since $7 - 4 = 3$, $7 \equiv 4 \pmod 3$, so $7 \in [4]$; since $7 - 10 = -3$, $7 \equiv 10 \pmod 3$, so $7 \in [10]$. By (Eq2), $4 \equiv 7$ (indeed $4 - 7 = -3$). By (Eq3), $4 \equiv 10$ (indeed $4 - 10 = -6 = (-2) \cdot 3$). By part (b), $[4] = [10]$.

(c) $[2] = \{x : x \leq 2\} = \{1, 2\}$ and $[1] = \{x : x \leq 1\} = \{1\}$. They share 1 and differ. In the proof of (c), take $c = 1$: $c \leq 2$ and $c \leq 1$ hold. The next line, "by (Eq2), $a \sim c$", would need $2 \leq 1$, which is false: $\leq$ is not symmetric, and that line fails.

(d) A common element of two classes is equivalent to both representatives, so symmetry and transitivity make the two representatives equivalent. Equivalent representatives have the same class, because each class is determined by any one of its elements.

(e) Three: $\{0\}$, $\{-1, 1\}$ and $\{-2, 2\}$. This is the relation $\sim_f$ of Example (The fibers of a function) for $f(x) = x^2$, whose values on the set are 0, 1, 4, one class for each value.

(f) Assume $[a] = [a']$, that is, $a \equiv a' \pmod n$, for arbitrary $a, a' \in \mathbb{Z}$; show that the rule's outputs for a and for a' are equal (Example (Method: checking that a definition on classes is well defined)).

4.2.9.2 B. Practice

Exercise. B1: Fractions as classes

(a) On $\mathbb{Z} \times \mathbb{Z}_{>0}$, let $(a, b) \sim (c, d)$ mean $ad = bc$. Prove that $\sim$ is an equivalence relation, and describe the class of $(1, 2)$.

(b) On $\mathbb{Z} \times \mathbb{N}$, let $(a, b)\ R\ (c, d)$ again mean $ad = bc$. Determine which of (Eq1)–(Eq3)

hold. Justify your answer.

Solution.

(a) (Eq1) $ab = ba$. (Eq2) If $ad = bc$, then $cb = da$. (Eq3) Let $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, so $ad = bc$ and $cf = de$. Multiply the first equation by f and use the second: $adf = bcf = bde$. So $d(af - be) = 0$. Since $d \in \mathbb{Z}_{>0}$, $d \neq 0$, and we may cancel d: $af = be$, that is, $(a, b) \sim (e, f)$. The hypothesis $d \neq 0$ on the **middle** pair is used here and nowhere else.
The class of $(1, 2)$ is $\{(c, d) \in \mathbb{Z} \times \mathbb{Z}_{>0} : d = 2c\}$. Since $d > 0$, $c = d/2 > 0$, so $c \in \mathbb{Z}_{>0}$ (Proposition 2.1.2 (b)), and the class is $\{(k, 2k) : k \in \mathbb{Z}_{>0}\} = \{(1, 2), (2, 4), (3, 6), \dots\}$: the ways of writing $\frac{1}{2}$ as a fraction. Each class is "one rational number"; *Number Systems: From* $\mathbb{N}$ *to* $\mathbb{R}$, Chapter 2 builds $\mathbb{Q}$ as this quotient set.

(b) (Eq1) and (Eq2) hold, by the same two lines as in (a), which did not use $b, d \neq 0$. (Eq3) fails: $(1, 1)\ R\ (0, 0)$, since $1 \cdot 0 = 1 \cdot 0$, and $(0, 0)\ R\ (2, 1)$, since $0 \cdot 1 = 0 \cdot 2$; but $(1, 1)\ \not R\ (2, 1)$, since $1 \cdot 1 \neq 1 \cdot 2$. The pair $(0, 0)$ is related to every pair, so it links any two; this is exactly the cancellation of (a) failing for $d = 0$.

Exercise. B2: Computing in Z/7

In $\mathbb{Z}/7$, compute $[3] + [5]$ and $[3][5]$, each written as $[r]$ with $r \in \{0, \dots, 6\}$. Then prove that $a \equiv b \pmod{n}$ implies $a^k \equiv b^k \pmod{n}$ for every $k \in \mathbb{N}$, and use it to find the remainder of 3^{100} on division by 7. *Hint:* $3^6 = 729$.

Solution. $[3] + [5] = [8] = [1]$, since $8 - 1 = 7$; and $[3][5] = [15] = [1]$, since $15 - 1 = 2 \cdot 7$.

Powers. Let $n \in \mathbb{Z}_{>0}$, $a, b \in \mathbb{Z}$ with $a \equiv b \pmod{n}$. By Proposition 2.3.4 (d), a^k and b^k are integers. We prove $a^k \equiv b^k$ by induction on $k \in \mathbb{N}$ (Logic and Proof, Axiom 4.2.1). Base: $a^0 = 1 = b^0$, and $1 \equiv 1$ by (Eq1). Step: suppose $a^k \equiv b^k$. By Definition 2.3.2, $a^{k+1} = a^k a$ and $b^{k+1} = b^k b$; the product clause of Proposition 4.2.5, applied to $a^k \equiv b^k$ and $a \equiv b$, gives $a^k a \equiv b^k b$.

The remainder. By Proposition 2.3.4, $3^{100} = 3^{96} \cdot 3^4 = (3^6)^{16} \cdot 3^4$. Now $729 = 104 \cdot 7 + 1$, so $3^6 \equiv 1 \pmod{7}$, and by the power fact, $(3^6)^{16} \equiv 1^{16} = 1$. Also $3^4 = 81 = 11 \cdot 7 + 4$, so $3^4 \equiv 4$. By Proposition 4.2.5, $3^{100} \equiv 1 \cdot 4 = 4 \pmod{7}$. Since $0 \leq 4 < 7$, the remainder of 3^{100} on division by 7 is 4 (Proposition 4.2.4), and $[3^{100}] = [4]$ in $\mathbb{Z}/7$. Here $1^{16} = 1$ is itself an induction: $1^0 = 1$, and $1^{k+1} = 1^k \cdot 1 = 1$.

Exercise. B3: Which rules are well defined?

Determine which of the following rules define a function. Justify your answer.

(a) $\mathbb{Z}/n \to \mathbb{Z}/n$, $[a]_n \mapsto [a^2]_n$, for a fixed $n \in \mathbb{Z}_{>0}$.
(b) $\mathbb{Z}/5 \to \mathbb{Z}/10$, $[a]_5 \mapsto [a]_{10}$.
(c) $\mathbb{Z}/10 \to \mathbb{Z}/5$, $[a]_{10} \mapsto [a]_5$.

Solution. The check in each case: take $[a] = [a']$, that is, $a \equiv a'$, and decide whether the outputs agree (Example (Method: checking that a definition on classes is well defined)).

(a) Yes. If $a \equiv a' \pmod{n}$, the product clause of Proposition 4.2.5, applied to $a \equiv a'$ twice, gives $a \cdot a \equiv a' \cdot a'$, so $[a^2]_n = [a'^2]_n$.

(b) No. $[0]_5 = [5]_5$, since $5 - 0 = 5$. But $[0]_{10} \neq [5]_{10}$, since $5 - 0 = 5$ is not a multiple of 10 ($0 < 5 < 10$, and the multiples of 10 are 0, at least 10, or at most -10; Proposition 2.1.2 (c)). The input $[0]_5$ would get two values.

(c) Yes. If $a - a' = 10k$ with $k \in \mathbb{Z}$, then $a - a' = 5(2k)$ with $2k \in \mathbb{Z}$ (Proposition 2.1.2 (a)), so $[a]_5 = [a']_5$. The difference from (b) is the direction: $5 \mid 10$, so a multiple of 10 is a multiple of 5, not conversely.

Exercise. B4: Prove or disprove

Prove or disprove: each rule defines a function.

(a) $\mathbb{Z}/6 \times \mathbb{Z}/6 \to \mathbb{Z}/6$, $([a], [b]) \mapsto [a - 2b]$.

(b) $\mathbb{Z}/4 \to \mathbb{Z}/8$, $[a]_4 \mapsto [2a]_8$.

(c) On $\mathbb{R}$, with $x \sim y$ meaning $x - y \in \mathbb{Z}$ (Example (The reals modulo the integers)), the rule $\mathbb{R}/\sim \to \mathbb{R}/\sim$, $[x] \mapsto [x^2]$.

(d) On $\mathbb{Z} \times \mathbb{Z}_{>0}$, with $(a, b) \sim (c, d)$ meaning $ad = bc$ (an equivalence relation by Exercise B1 (a)), the rule $[(a, b)] \mapsto [(a + b, b)]$, from the quotient set to itself.

(e) With the same relation, the rule $[(a, b)] \mapsto [(a + 1, b + 1)]$.

Solution.

(a) True. Two representatives of each argument: $a - a' = 6k$ and $b - b' = 6l$ with $k, l \in \mathbb{Z}$. Then $(a - 2b) - (a' - 2b') = 6(k - 2l)$, so $[a - 2b] = [a' - 2b']$. (The method runs once per argument.)

(b) True. If $a - a' = 4k$, then $2a - 2a' = 8k$, so $[2a]_8 = [2a']_8$. (Compare B3 (b), where $[a]_5 \mapsto [a]_{10}$ failed: doubling the representative doubles the difference.)

(c) False. $[\frac{1}{3}] = [\frac{4}{3}]$, since $\frac{4}{3} - \frac{1}{3} = 1$. But $(\frac{4}{3})^2 - (\frac{1}{3})^2 = \frac{16}{9} - \frac{1}{9} = \frac{5}{3}$, and $\frac{5}{3} \notin \mathbb{Z}$: $0 < \frac{5}{3} - 1 = \frac{2}{3} < 1$, and no integer lies strictly between 0 and 1 (Proposition 2.1.2 (c)), so $\frac{5}{3} - 1 \notin \mathbb{Z}$, hence $\frac{5}{3} \notin \mathbb{Z}$ (else $\frac{5}{3} - 1 \in \mathbb{Z}$ by Proposition 2.1.2 (a)). So $[\frac{1}{9}] \neq [\frac{16}{9}]$ by Theorem 4.2.1 (b): one class, two values.

(d) True. Let $(a, b) \sim (c, d)$, so $ad = bc$. Then $(a + b)d = ad + bd = bc + bd = b(c + d)$, so $(a + b, b) \sim (c + d, d)$; and $b, d \in \mathbb{Z}_{>0}$, so the outputs lie in $\mathbb{Z} \times \mathbb{Z}_{>0}$.

(e) False. $(1, 2) \sim (2, 4)$, since $1 \cdot 4 = 2 \cdot 2$. The outputs are $(2, 3)$ and $(3, 5)$, and $2 \cdot 5 = 10 \neq 9 = 3 \cdot 3$, so $(2, 3) \not\sim (3, 5)$. (Reading the classes as fractions: (d) adds 1, and (e) adds 1 to numerator and denominator, which depends on how the fraction is written.)

4.2.9.3 C. Going deeper

Exercise. C1: Exit check: classes partition

Let $\sim$ be an equivalence relation on a set X. Prove that the equivalence classes of $\sim$ form

a partition of X, and that for all $a, b \in X$, $[a] = [b]$ if and only if $a \sim b$. Write the proof without looking at the text, naming the property of $\sim$ behind each step.

Solution. Non-empty. For $a \in X$, reflexivity gives $a \sim a$, so $a \in [a]$, and $[a] \neq \emptyset$.

Cover. Every class is a subset of X by definition. Every $x \in X$ lies in the class $[x]$, as just shown. So the union of all classes is X.

$[a] = [b] \iff a \sim b$. ($\Rightarrow$) $a \in [a] = [b]$, so $a \sim b$. ($\Leftarrow$) Let $a \sim b$. If $x \in [a]$, then $x \sim a$ and $a \sim b$, so $x \sim b$ by transitivity: $[a] \subseteq [b]$. By symmetry $b \sim a$; if $x \in [b]$, then $x \sim b$ and $b \sim a$ give $x \sim a$ by transitivity: $[b] \subseteq [a]$. So $[a] = [b]$.

Disjoint or equal. Let $[a] \cap [b] \neq \emptyset$, with a common element c. Then $c \sim a$ and $c \sim b$. By symmetry $a \sim c$, and by transitivity $a \sim b$. By the previous paragraph, $[a] = [b]$. Hence two different classes are disjoint.

The three paragraphs on non-emptiness, covering and disjointness are the three clauses of Definition 4.2.3, so the set of classes $X/\sim$ is a partition of X. (This is Theorem 4.2.1.)

Marking scheme. (10 points)

- 2: each class is non-empty, by reflexivity.
- 1: every element lies in some class (its own), so the classes cover X.
- 4: overlapping classes are equal: a common element c with $c \sim a$ and $c \sim b$; symmetry to reverse one of them; transitivity to link a and b; both inclusions (or the equivalence $[a] = [b] \iff a \sim b$) to conclude equality.
- 2: $[a] = [b] \iff a \sim b$, both directions.
- 1: the conclusion names the three conditions of a partition.

A proof that shows "overlapping classes are equal" by proving $[a] \subseteq [c] \subseteq [b]$ and back directly from the definition earns the 4 points for that step if each use of symmetry and transitivity is named. So does a proof that, from $c \sim a$ and $c \sim b$, applies the ($\Leftarrow$) direction of $[a] = [b] \iff a \sim b$ twice to get $[a] = [c] = [b]$, provided that equivalence was proved independently of this step, with symmetry and transitivity named. Fatal errors (0 for the step): applying transitivity to $a \sim c$ and $b \sim c$ without reversing one by symmetry; showing only $[a] \subseteq [b]$ and concluding $[a] = [b]$.

Exercise. C2: Find the error

A student proves part of Theorem 4.2.2. Let $\mathcal{P}$ be a partition of X, and let $x \sim y$ mean that x and y lie in a common block of $\mathcal{P}$.

> *Claim.* $\sim$ is transitive. *Proof.* (1) Let $x, y, z \in X$ with $x \sim y$ and $y \sim z$. (2) Since $x \sim y$, there is a block $P \in \mathcal{P}$ with $x \in P$ and $y \in P$. (3) Since $y \sim z$, y and z lie in a common block, and that block is P, so $z \in P$. (4) Hence x and z both lie in P, and $x \sim z$.

(a) Is the claim true?

(b) Which line fails, and which rule does it break?

(c) Give a counterexample to the failing step, and repair the proof.

Solution.

(a) The claim is true: it is the transitivity step (Eq3) in the proof of Theorem 4.2.2 (a).

(b) Line (3) fails. "y and z lie in a common block" is an existential statement, and to use it the proof must name its witness by ∃E, with a **new** name. Line (3) gives the second witness the name P, already in use for the witness of line (2): this is entry (N4) of Logic and Proof, Example (What is not allowed), reusing one witness name for two ∃E's (Logic and Proof, Definition 5.6.1). The tell is that the proof never uses (P2), the disjointness of the blocks; and without (P2) the claim is false, as (c) shows.

(c) A counterexample to the step needs blocks that overlap, since for a partition the step's conclusion happens to be true. Take the cover $\{\{1,2\},\{2,3\}\}$ of $\{1,2,3\}$, which is not a partition, with $x=1$, $y=2$, $z=3$. Then $1 \sim 2$ with $P=\{1,2\}$, and $2 \sim 3$ through $\{2,3\}$; line (3) concludes $3 \in \{1,2\}$, which is false, and the argument "proves" $1 \sim 3$, although no set of the cover contains 1 and 3.

Repair: replace (3) and (4) by "Since $y \sim z$, there is a block $Q \in \mathcal{P}$ with $y \in Q$ and $z \in Q$. Then $y \in P \cap Q$, so $P \cap Q \neq \emptyset$, and $P = Q$ by (P2). Hence $x \in P$ and $z \in P$, so $x \sim z$."

4.3 Partial Orders, Maximal and Greatest Elements

Section 4.2 studied the relations that behave like equality. This section studies the ones that behave like $\leq$: reflexive and transitive like an equivalence relation, but antisymmetric instead of symmetric, so that they have a direction. For numbers, "the largest element of a set" is clear. For sets under $\subseteq$, or for natural numbers under divisibility, two elements can be **incomparable**, neither below the other, and "largest" splits into two different notions. We separate them, prove what links them, and then take a first look at least upper bounds. That is the vocabulary *Analysis on the Real Line*, Chapter 1 needs for the supremum.

4.3.1 Partial orders

Section 4.1 found three relations with the same three properties: $\leq$ on $\mathbb{R}$, $\subseteq$ on $\mathcal{P}(X)$ (Example (Eight relations, four properties)), and $\mid$ on $\mathbb{N}$ (Proposition 4.1.1). Each is reflexive, antisymmetric and transitive. Each says "below" in its own sense: smaller, contained in, a divisor of. What they share is what "being below" needs, and it deserves a name, so that a fact proved once holds for all three.

A partial order says which elements lie below which, without requiring every two to be comparable.

Definition 4.3.1. Partial Order

Let X be a set. A **partial order on** X is a relation $\preceq$ on X that is reflexive, antisymmetric and transitive on X (Definition 4.1.1):

(PO1) **for every** $x \in X$, $x \preceq x$;

(PO2) **for all** $x, y \in X$, if $x \preceq y$ and $y \preceq x$, then $x = y$;

(PO3) **for all** $x, y, z \in X$, if $x \preceq y$ and $y \preceq z$, then $x \preceq z$.

The pair $(X, \preceq)$ is a **partially ordered set**. Elements $x, y \in X$ are **comparable** if $x \preceq y$ or $y \preceq x$. The partial order is **total** if **every** two elements of X are comparable. The **strict part** of $\preceq$ is the relation $\prec$ on X given by

$$x \prec y \iff x \preceq y \text{ and } x \neq y.$$

We also write $y \succeq x$ for $x \preceq y$.

In words: (PO1) everything is below itself. (PO2) is the clause that gives an order its direction: two elements below each other are the same element, so "below" cannot run both ways between different things. (PO3) lets "below" pass along a chain. "Total" adds that any two elements can be compared; "partial" is the word for not requiring it. The symbol $\preceq$ is a letter for an arbitrary partial order, chosen so that $\leq$ keeps its meaning on numbers.

The strict part is irreflexive and transitive. No x has $x \prec x$, since that would need $x \neq x$. If $x \prec y$ and $y \prec z$, then $x \preceq z$ by (PO3); and $x \neq z$, because $x = z$ would give $x \preceq y$ and $y \preceq x$, hence $x = y$ by (PO2), contradicting $x \neq y$. So $x \prec z$.

Examples.

- $(\mathbb{R}, \leq)$ is a partially ordered set, and it is total: for real numbers $x \leq y$ or $y \leq x$. Its strict part is $<$. The same holds for $(\mathbb{N}, \leq)$ and $(\mathbb{Z}, \leq)$, since restricting a total order to a subset keeps all four properties: each is a statement about all elements, and holds in particular for the elements of the subset.
- $(\mathbb{N}, |)$ is a partially ordered set by Proposition 4.1.1, and it is not total: $2 \nmid 3$ and $3 \nmid 2$, so 2 and 3 are incomparable.
- $(\mathcal{P}(X), \subseteq)$ is a partially ordered set; the example after this list decides when it is total.
- Degenerate cases: equality on any set X is a partial order, in which no two **different** elements are comparable; and the empty relation is a partial order on $\emptyset$, vacuously.

Non-examples by minimal change. Divisibility on $\mathbb{Z}$ is reflexive and transitive, but not antisymmetric: $2 \mid -2$ and $-2 \mid 2$, and $2 \neq -2$ (Proposition 4.1.1). Passing from $\mathbb{N}$ to $\mathbb{Z}$ loses exactly (PO2). The relation $<$ on $\mathbb{R}$ is antisymmetric (vacuously: $x < y$ and $y < x$ never both hold) and transitive, but not reflexive, since $0 < 0$ fails. It is the strict part of $\leq$, not a partial order.

Why these clauses. Without (PO2), two different elements could each be below the other, and "the largest element" of a set could fail to be unique; the uniqueness proof in the next subsection uses (PO2) and nothing else. A relation that keeps (PO1) and (PO3) and drops (PO2) is often called a preorder; $|$ on $\mathbb{Z}$ is one. Totality is left out because the important examples, $\subseteq$ and $|$, do not have it, and much of the interest lies in what changes without it.

Example. Inclusion is a partial order, rarely total

Let X be a set. Show that $\subseteq$ is a partial order on $\mathcal{P}(X)$, and that it is total if and only if X has at most one element.

Solution. A partial order. (PO1) $A \subseteq A$ for every set A. (PO2) If $A \subseteq B$ and $B \subseteq A$, then $A = B$ by Proposition 1.2.1. (PO3) is Proposition 1.2.2. (These are the entries of Example (Eight relations, four properties).)

Total exactly when X has at most one element. Suppose X has two different elements $a \neq b$. Then $\{a\}, \{b\} \in \mathcal{P}(X)$, and $\{a\} \not\subseteq \{b\}$, since $a \in \{a\}$ and $a \notin \{b\}$; likewise $\{b\} \not\subseteq \{a\}$. So

$\{a\}$ and $\{b\}$ are incomparable, and $\subseteq$ is not total. For $X = \{1, 2\}$, the incomparable pair is $\{1\}$, $\{2\}$.

Conversely, suppose any two elements of X are equal. Let $A \subseteq X$. If $A \neq \emptyset$, take $a \in A$; then every $x \in X$ equals a, so $x \in A$, and $A = X$. So every subset of X is $\emptyset$ or X. Any two of these are comparable, since $\emptyset \subseteq X$ (Section 1.2, after Proposition 1.2.3) and each is a subset of itself. So $\subseteq$ is total on $\mathcal{P}(X)$.

Warning. In a partial order, "$x \preceq y$ fails" does **not** give "$y \prec x$". In $(\mathcal{P}(\{1, 2\}), \subseteq)$, $\{1\} \not\subseteq \{2\}$, and $\{2\} \subsetneq \{1\}$ is false too: the two are incomparable. The habit from numbers, "not $\leq$ means $>$", is the totality of $\leq$ on $\mathbb{R}$, and it must not be carried into a partial order.

4.3.2 Bounds, greatest and maximal elements

From now on, $(X, \preceq)$ is a partially ordered set and $A \subseteq X$. The bounds come first, because both kinds of "largest" are measured against them.

Definition 4.3.2. Upper and Lower Bounds

An element $u \in X$ is an **upper bound** of A if $a \preceq u$ for every $a \in A$, and a **lower bound** of A if $u \preceq a$ for every $a \in A$. The set A is **bounded above** if it has an upper bound in X, **bounded below** if it has a lower bound in X, and **bounded** if both.

An upper bound lives in X and need not belong to A: in $(\mathbb{R}, \leq)$, 5 is an upper bound of $[0, 1]$. Every element of X is an upper bound of $\emptyset$, vacuously. In $(\mathbb{N}, |)$, an upper bound of $\{4, 6\}$ is a common multiple of 4 and 6, such as 12, 24 or 0.

Now the two notions of "largest". The first is the familiar one: an element of the set that is above everything in the set. The second asks less: an element with nothing in the set strictly above it.

Definition 4.3.3. Greatest and Least Elements

An element g is a **greatest element** of A if $g \in A$ and $a \preceq g$ for **every** $a \in A$. An element l is a **least element** of A if $l \in A$ and $l \preceq a$ for every $a \in A$.

Definition 4.3.4. Maximal and Minimal Elements

An element m is a **maximal element** of A if $m \in A$ and there is **no** $a \in A$ with $m \prec a$. An element m is a **minimal element** of A if $m \in A$ and there is no $a \in A$ with $a \prec m$.

In words: a greatest element is an upper bound of A that belongs to A. A maximal element is one that cannot be beaten inside A, which is weaker: an element can be unbeaten simply because it is incomparable with its rivals. In symbols the difference is where the negation sits:

$$g \text{ greatest:} \quad g \in A \wedge \forall a \in A \;\; a \preceq g,$$
$$m \text{ maximal:} \quad m \in A \wedge \neg\exists a \in A \;\; m \prec a.$$

By Logic and Proof, Proposition 6.2.3 (b), $\neg\exists a \in A \;\; m \prec a$ is $\forall a \in A \;\; \neg(m \prec a)$, and $\neg(m \prec a)$

says that $m \preceq a$ implies $m = a$. So "maximal" reads: everything in A that is above m **is** m. "Greatest" reads: everything in A is below g. The first only forbids elements above; the second demands that every element be compared.

For numbers the two coincide. In $(\mathbb{R}, \leq)$, the set $\{1, 4, 9\}$ has greatest element 9, its only maximal element, and least element 1. The interval $[0, 1)$ has least element 0 and neither a greatest nor a maximal element: for each $a \in [0, 1)$, the number $(a + 1)/2$ lies in $[0, 1)$ and is strictly above a. A one-point set $\{x\}$ has x as greatest, least, maximal and minimal element, and $\emptyset$ has none of the four, since each definition requires an element of A.

The first result explains the article in "**the** greatest element".

Proposition 4.3.1. Greatest and Least Elements Are Unique

A subset A of a partially ordered set has at most one greatest element and at most one least element.

Idea. The method of Example (Method: existence and uniqueness), uniqueness half: take two greatest elements, about which nothing else is assumed. Each is in A, so each is below the other, and (PO2) closes the gap.

Proof. Let g and g' be greatest elements of A. Since $g' \in A$ and g is greatest, $g' \preceq g$; since $g \in A$ and g' is greatest, $g \preceq g'$. By (PO2), $g = g'$. For least elements the same argument applies with the inequalities reversed.

■

So we may speak of **the** greatest element and **the** least element of A when they exist. In $(\mathbb{R}, \leq)$, the greatest element of a set is its maximum, $\max A$, and the least element its minimum, $\min A$. This settles a point left open in Section 1.5: the least $q_0 \in \mathbb{Z}_{>0}$ with $rq_0 \in \mathbb{Z}$ in Example (Relations that are not functions) exists by Theorem 2.1.3: the set of such q lies in $\mathbb{Z}_{>0} \subseteq \mathbb{N}$, and it is non-empty, since writing $r = p/q$ with $q \in \mathbb{Z}_{>0}$ (as the solution of (b) there notes) gives $rq = p \in \mathbb{Z}$. It is unique by the least-element half of the proposition, so the rule there names one value.

Quick check. Divisibility on $\mathbb{Z}$ is reflexive and transitive but not antisymmetric, so it is not a partial order. Read the formula of Definition 4.3.3 in $(\mathbb{Z}, |)$ anyway, and run the proof of Proposition 4.3.1 for $A = \{2, -2\}$: which elements of A satisfy the formula, and which line of the proof fails?

Solution. Both: $2 \mid 2$, $-2 \mid 2$ ($2 = (-1)(-2)$), $2 \mid -2$ and $-2 \mid -2$. Every line of the proof goes through except the last, "By (PO2), $g = g'$": $2 \mid -2$ and $-2 \mid 2$, yet $2 \neq -2$.

The second result compares the two notions.

Proposition 4.3.2. Greatest and Maximal Elements

Let $(X, \preceq)$ be a partially ordered set and $A \subseteq X$.

(a) A greatest element of A is a maximal element of A.

(b) If $\preceq$ is total, then a maximal element of A is a greatest element of A.

The same holds for least and minimal elements.

Idea. For (a), anything strictly above the greatest element would also be below it, and antisymmetry forbids that. For (b), a maximal element m must be compared with each $a \in A$, and totality says it can be: either $a \preceq m$, as wanted, or $m \preceq a$, and then maximality forces $a = m$. Part (a) proves a negative claim, "no element strictly above", so it starts by supposing one (Example (Method: choosing direct, contrapositive or contradiction)); part (b) is a proof by cases on the two outcomes of comparability (Example (Method: proof by cases)).

Proof. *(a)* Let g be a greatest element of A. Then $g \in A$. Suppose some $a \in A$ has $g \prec a$, so $g \preceq a$ and $g \neq a$. Since g is greatest, $a \preceq g$. By (PO2), $a = g$, contradicting $g \neq a$. So no such a exists, and g is maximal.

(b) Let $\preceq$ be total and m a maximal element of A, and let $a \in A$. By totality, $a \preceq m$ or $m \preceq a$. *Case 1:* $a \preceq m$. This is what we want. *Case 2:* $m \preceq a$. If $m \neq a$, then $m \prec a$ with $a \in A$, which maximality excludes. So $m = a$, and $a \preceq m$ by (PO1). In either case $a \preceq m$. Since $a \in A$ was arbitrary and $m \in A$, m is a greatest element.

For least and minimal elements, apply (a) and (b) to the partial order $\succeq$: its greatest and maximal elements are the least and minimal elements for $\preceq$, and it is total when $\preceq$ is. (That $\succeq$ satisfies (PO1)–(PO3), and is total when $\preceq$ is, comes from reading those clauses with the two variables exchanged. Its strict part is $x \succ y \iff y \prec x$, since $x \neq y$ is symmetric in x and y. So "no $a \in A$ with $m \succ a$" is "no $a \in A$ with $a \prec m$", and "$a \succeq l$ for every $a \in A$" is "$l \preceq a$ for every $a \in A$".)

■

Part (b) uses totality once, in the case split of its second sentence, and the case split is where it fails without it. The proof of Proposition 2.3.8 in Section 2.3 compares two elements at a time and keeps the larger. Its maximum half uses nothing about $\leq$ on $\mathbb{R}$ beyond reflexivity, transitivity and the comparability of any two elements, so it works word for word in any totally ordered set. The minimum half passes to $-x_1, \ldots, -x_n$, which needs an ordered field; in a totally ordered set, apply the maximum half to the reverse order $\succeq$ instead, which is total by the last paragraph of the proof above. In particular the whole proposition holds in any ordered field, which is how *Analysis on the Real Line*, Chapter 1 reads it.

Without totality, (b) fails, and maximal elements need not be greatest. Each failure is shown by a counterexample (Example (Method: disproof by counterexample, proof by example)).

Example. Maximal elements that are not greatest

Find the maximal elements of each set, and decide whether it has a greatest element: (a) $A = \{2, 3, 4, 5, 6\}$ in $(\mathbb{N}, |)$; (b) $\mathcal{B} = \{\{1\}, \{2\}\}$ in $(\mathcal{P}(\{1, 2\}), \subseteq)$.

Solution.

(a) Within A, the only strict divisibilities are $2 \mid 4$, $2 \mid 6$ and $3 \mid 6$. So $2 \prec 4$ and $3 \prec 6$, and 2, 3 are not maximal. Nothing in A is strictly above 4, 5 or 6: every element of A is positive, and a positive multiple kn of $n \in \{4, 5, 6\}$ other than n has $k > 0$ and $k \neq 1$, so $k \geq 2$ (Proposition 2.1.2 (c)), and then $kn \geq 2n \geq 8$, while every element of A is at most 6. So the maximal elements are 4, 5 and 6.
There is no greatest element. By Proposition 4.3.2 (a), a greatest element would be maximal, so it would be 4, 5 or 6. But $5 \nmid 4$, $4 \nmid 5$ and $4 \nmid 6$, so none of the three is above every element of A.

(b) $\{1\}$ and $\{2\}$ are incomparable (Example (Inclusion is a partial order, rarely total)), so neither is strictly above the other: both are maximal. Neither is greatest, since neither contains the other.

In (a), the minimal elements are 2, 3 and 5, and there is no least element either. The example is the minimal change from $\{1, 2, 3, 4, 5, 6\}$, which has the least element 1 and still no greatest.

Warning. "Maximal" is not "greatest". A set can have many maximal elements and no greatest, as in Example (Maximal elements that are not greatest); and a set can have no maximal element at all: $\mathbb{N}$ under $\leq$, where $n + 1 \in \mathbb{N}$ (by (NS)) is strictly above n. The answer also depends on the order, not just on the set: under divisibility, $\mathbb{N}$ **has** a greatest element, 0, since every $a \in \mathbb{N}$ divides $0 = 0 \cdot a$.

Quick check. In $\mathcal{P}(\{1, 2, 3\}) \setminus \{\{1, 2, 3\}\}$, ordered by $\subseteq$, name the maximal elements. Is there a greatest element?

Solution. The maximal elements are the three two-element sets $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$: the only subset of $\{1, 2, 3\}$ strictly containing a two-element set is $\{1, 2, 3\}$, which was removed, and every set with at most one element lies strictly inside some two-element set. There is no greatest element: it would be maximal (Proposition 4.3.2 (a)), hence a two-element set, and no two-element set contains the other two.

4.3.3 Least upper bounds, a first look

Here is the notion that the rest of the book is built on. When a set has no greatest element, its upper bounds may still have a least one, and that element plays the part of "the top of the set" from outside.

The supremum is the best upper bound: the least element of the set of upper bounds.

Definition 4.3.5. Supremum and Infimum

Let $(X, \preceq)$ be a partially ordered set and $A \subseteq X$. An element $s \in X$ is a **least upper bound**, or **supremum**, of A in X if

(S1) s is an upper bound of A, and

(S2) $s \preceq u$ for **every** upper bound u of A.

An element $i \in X$ is a **greatest lower bound**, or **infimum**, of A in X if i is a lower bound of A and $u \preceq i$ for every lower bound u of A.

In other words, a supremum of A is a least element of the set of upper bounds of A, and an infimum a greatest element of the set of lower bounds. By Proposition 4.3.1, applied to those sets, each is **unique** when it exists, and we write $\sup A$ and $\inf A$. The words "in X" matter: the upper bounds are taken in X, and enlarging or shrinking X can create or destroy a supremum. The definition also carries no promise that $\sup A$ exists, or that it belongs to A.

Two quick consequences. If A has a greatest element g, then $g = \sup A$: g is an upper bound, and every upper bound u has $g \preceq u$ because $g \in A$. And a supremum that belongs to A is a greatest element of A, by (S1). So a supremum is a greatest element exactly when it lies in the set; the new cases are the ones where it lies outside.

Suprema of sets. In $(\mathcal{P}(X), \subseteq)$, let $A, B \subseteq X$. Then $\sup\{A, B\} = A \cup B$. (S1): $A \subseteq A \cup B$ and $B \subseteq A \cup B$, and $A \cup B \in \mathcal{P}(X)$. (S2): let $C \in \mathcal{P}(X)$ be an upper bound, so $A \subseteq C$ and $B \subseteq C$; every element of $A \cup B$ lies in A or in B, hence in C, so $A \cup B \subseteq C$. The supremum $A \cup B$ belongs to $\{A, B\}$ only when one of the two sets contains the other; for $\{\{1\}, \{2\}\}$ it is $\{1, 2\}$, which is not in the set. Exercise B1 extends this to every family of subsets, and adds the infimum.

Suprema under divisibility. In $(\mathbb{N}, |)$, an upper bound of $\{a, b\}$ is a common multiple of a and b. The least upper bound turns out to be the least common multiple, and proving that it is **least in the divisibility order**, not merely the smallest number, is a job for the division algorithm and for the least-element method (Example (Method: the least element)): the least common multiple is a least element, and a smaller common multiple would contradict it.

Example. The supremum under divisibility is the least common multiple

Let $a, b \in \mathbb{N}$. Find $\sup\{a, b\}$ in $(\mathbb{N}, |)$. Deduce that an integer divisible by 2 and by 3 is divisible by 6.

Solution. *Case* $a, b \in \mathbb{Z}_{>0}$. Let $M := \{m \in \mathbb{Z}_{>0} : a \mid m \text{ and } b \mid m\}$, the positive common multiples. It is non-empty: $ab \in \mathbb{N}$ by Lemma 2.1.1 (b), $ab > 0$ as a product of positive numbers, so $ab \in \mathbb{Z}_{>0}$ (Proposition 2.1.2 (b)), and $ab = b \cdot a = a \cdot b$ is a multiple of both. Since $M \subseteq \mathbb{Z}_{>0} \subseteq \mathbb{N}$, M has a least element L (Theorem 2.1.3), the **least common multiple** of a and b.

We show that L divides **every** integer common multiple c of a and b. By Theorem 2.2.3, $c = qL + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < L$. Write $c = as$, $L = at$ with $s, t \in \mathbb{Z}$; then $r = c - qL = a(s - qt)$ with $s - qt \in \mathbb{Z}$ (Proposition 2.1.2 (a)), so $a \mid r$, and in the same way $b \mid r$. If $r > 0$, then $r \in \mathbb{Z}_{>0}$ (Proposition 2.1.2 (b)), so $r \in M$ and $r < L$, contradicting the choice of L. Hence $r = 0$, and $c = qL$: $L \mid c$. The argument never used $c \geq 0$.

Now $L = \sup\{a, b\}$. (S1): $a \mid L$ and $b \mid L$, since $L \in M$. (S2): an upper bound $c \in \mathbb{N}$ of $\{a, b\}$ is a common multiple, so $L \mid c$ by the previous paragraph.

Case $a = 0$ or $b = 0$. Say $a = 0$. An upper bound c has $0 \mid c$, that is, $c = k \cdot 0 = 0$ for some $k \in \mathbb{Z}$. And 0 is an upper bound, since $n \mid 0 = 0 \cdot n$ for every $n \in \mathbb{N}$. So 0 is the only upper bound, and $\sup\{a, b\} = 0$, the greatest element of $(\mathbb{N}, |)$.

The instance. For $a = 2$, $b = 3$: $6 \in M$, and none of $1, 2, 3, 4, 5$ is a multiple of both 2 and 3 ($1, 3, 5$ are odd, and $2, 4$ lie strictly between consecutive multiples of 3). So $L = 6$, and every integer n with $2 \mid n$ and $3 \mid n$ has $6 \mid n$, by the second paragraph with $c = n$.

The instance gives a second proof, through the least common multiple, of the fact that Section 1.3 used as a school fact and Section 2.2 proved in Exercise B3 (c) (Exercise (B3, used later)): an integer divisible by 2 and by 3 is divisible by 6. It also shows the two orders on $\mathbb{N}$ disagreeing: $\sup\{4, 6\}$ is 12 under divisibility and 6 under $\leq$.

A supremum that does not exist. In $(\mathbb{Q}, \leq)$, the set $\{x \in \mathbb{Q} : x > 0,\ x^2 < 2\}$ is non-empty and bounded above (by 2, for instance: a rational $x > 2$ has $x^2 > 4$). It has **no** least upper bound in $\mathbb{Q}$. We do not prove this here. *Analysis on the Real Line*, Chapter 1 proves it, and then takes the existence of suprema in $\mathbb{R}$ as its axiom: the supremum of *Analysis on the Real Line*, Chapter 1, defined in an ordered field, is Definition 4.3.5 for the order $\leq$ of that field; *Analysis on the Real Line*, Chapter 1 uses it in $\mathbb{Q}$ and in $\mathbb{R}$. The ambient set decides: the same set has a supremum in $(\mathbb{R}, \leq)$, namely $\sqrt{2}$.

4.3.4 Well-ordered sets

Section 2.1 proved that every non-empty subset of $\mathbb{N}$ has a least element (Theorem 2.1.3). In the language of this section, that is a property of the partially ordered set $(\mathbb{N}, \leq)$, and it has a name.

Definition 4.3.6. Well-Ordered Set

A partially ordered set $(X, \preceq)$ is **well-ordered**, and $\preceq$ is a **well-order** on X, if $\preceq$ is total and every **non-empty** subset of X has a least element.

$(\mathbb{N}, \leq)$ is well-ordered: $\leq$ is total, and Theorem 2.1.3 supplies the least elements. $(\mathbb{Z}, \leq)$ is not: $\mathbb{Z}$ itself has no least element, since for every $n \in \mathbb{Z}$ also $n - 1 \in \mathbb{Z}$ (Proposition 2.1.2 (a)) and $n - 1 < n$. Nor is the set of positive rationals, which has no least element ($q/2 < q$). The word "non-empty" is needed because $\emptyset$ has no least element in any order. Totality is in fact automatic: any two elements x, y form a non-empty set $\{x, y\}$, whose least element is below the other one. Upper bounds work too: in $(\mathbb{N}, \leq)$ a non-empty set bounded above has a greatest element (Corollary 2.1.5). Exercise C1 gives a well-ordered set that does not look like $\mathbb{N}$.

Remark. In a general partially ordered set, one may ask: if every **chain** (a subset on which $\preceq$ is total) has an upper bound, must there be a maximal element? For a non-empty partially ordered set the answer "yes" is Zorn's lemma, and it cannot be proved from what we have: it is equivalent to the axiom of choice, which Section 3.2 states (Axiom 3.2.1). Chapter 6 states Zorn's lemma and uses it, and *Axiomatic Set Theory*, Chapter 4 proves it equivalent to the axiom of choice, together with the other equivalents, among them the claim that every set has a well-order.

4.3.5 Exercises

4.3.5.1 A. Check your understanding

Exercise. A1

(a) Let $(X, \preceq)$ be a partially ordered set and $A \subseteq X$. Write "g is a greatest element of A" and "m is a maximal element of A" in symbols, and negate each.

(b) True or false, with a witness: every finite non-empty subset of a partially ordered set has a greatest element.

(c) Find $\sup\{4, 6\}$ in $(\mathbb{N}, |)$ and in $(\mathbb{N}, \leq)$.

(d) On $\mathbb{N} \times \mathbb{N}$, the **lexicographic order** is $(a, b) \preceq (c, d)$ if $a < c$, or $a = c$ and $b \leq d$. Given that it is a partial order, is it total?

Solution.

(a) g greatest: $g \in A \wedge \forall a \in A \;\; a \preceq g$. Its negation, by Logic and Proof, Proposition 2.5.5 and Logic and Proof, Proposition 6.2.3 (a): $g \notin A \vee \exists a \in A \;\; \neg(a \preceq g)$.
m maximal: $m \in A \wedge \neg\exists a \in A \;\; m \prec a$. Its negation: $m \notin A \vee \exists a \in A \;\; m \prec a$, by Logic and Proof, Proposition 2.5.5 and Logic and Proof, Proposition 2.5.1. In words: g fails to be greatest if some element of A is **not below** it; m fails to be maximal if some element of A is **strictly above** it. The first failure can happen through incomparability; the second cannot.

(b) False. In $(\mathcal{P}(\{1, 2\}), \subseteq)$, the set $\{\{1\}, \{2\}\}$ is finite and non-empty and has no greatest element (Example (Maximal elements that are not greatest) (b)). What is true is that it has a **maximal** element: it can be listed as $\{x_1, \ldots, x_n\}$, which is what "finite" means (Definition 2.5.2, Section 2.5), so it has one by Exercise R4.

(c) Under divisibility, $\sup\{4, 6\} = 12$, the least common multiple (Example (The supremum under divisibility is the least common multiple)): 12 is a common multiple, and none of $1, \ldots, 11$ is (the positive multiples of 6 below 12 are just 6, and $4 \nmid 6$). Under $\leq$, $\sup\{4, 6\} = 6$, the greatest element.

(d) Yes. Let $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$. If $a < c$, then $(a, b) \preceq (c, d)$; if $c < a$, then $(c, d) \preceq (a, b)$; if $a = c$, then $b \leq d$ or $d \leq b$, by totality of $\leq$, and the pairs are comparable. By trichotomy these cases cover everything.

4.3.5.2 B. Practice

Exercise. B1: Suprema of families of sets

Let X be a set and $(A_i)_{i \in I}$ a family of subsets of X. In $(\mathcal{P}(X), \subseteq)$, prove that the set $\{A_i : i \in I\}$ has supremum $\bigcup_{i \in I} A_i$ and infimum $\bigcap_{i \in I} A_i$, the intersection taken in X. What are they when $I = \emptyset$?

Solution. Write $U := \bigcup_{i \in I} A_i$ and $N := \bigcap_{i \in I} A_i$ (Definition 1.3.4). Both are subsets of X, so they lie in $\mathcal{P}(X)$.

Supremum. (S1) For each $i \in I$, every element of A_i lies in U, so $A_i \subseteq U$. (S2) Let $C \in \mathcal{P}(X)$ be an upper bound: $A_i \subseteq C$ for every $i \in I$. Let $x \in U$. Then $x \in A_i$ for some $i \in I$; name

it i. Since $A_i \subseteq C$, $x \in C$. So $U \subseteq C$.

Infimum. N is a lower bound: for each $i \in I$, every $x \in N$ lies in A_i, so $N \subseteq A_i$. Let $D \in \mathcal{P}(X)$ be a lower bound: $D \subseteq A_i$ for every i. Let $x \in D$. Then $x \in X$, and $x \in A_i$ for every $i \in I$, so $x \in N$. Hence $D \subseteq N$.

Empty index set. If $I = \emptyset$, then $U = \emptyset$ and $N = X$, since an intersection in X of no sets is X. This agrees with the definitions: every element of $\mathcal{P}(X)$ is an upper bound of the empty set, and the least of them is $\emptyset$; every element is a lower bound, and the greatest is X. The arguments above cover this case, since their "for every i" clauses hold vacuously.

Exercise. B2: Two maximal elements and a least one

Give an example of a partially ordered set that has exactly two maximal elements and a least element, and check each property. Then list the properties that every answer must have.

Solution. An example. $X = \{\emptyset, \{1\}, \{2\}\}$ ordered by $\subseteq$. It is a partial order, as a subset of $(\mathcal{P}(\{1,2\}), \subseteq)$. The least element is $\emptyset$, since $\emptyset \subseteq A$ for every $A \in X$ (Section 1.2, after Proposition 1.2.3). The maximal elements are $\{1\}$ and $\{2\}$: neither is strictly contained in an element of X. And $\emptyset$ is not maximal, since $\emptyset \subsetneq \{1\}$. So there are exactly two. Another answer: $\{1, 2, 3\}$ under divisibility, with least element 1 and maximal elements 2, 3.

What every answer must have. Let l be the least element and $m_1 \neq m_2$ the maximal elements.

- m_1 and m_2 are incomparable: if $m_1 \preceq m_2$, then $m_1 \prec m_2$, since $m_1 \neq m_2$, and m_1 would not be maximal; symmetrically for $m_2 \preceq m_1$.
- So the order is not total, and there is no greatest element: a greatest element g would have $m_1 \preceq g$, and maximality of m_1 gives $m_1 = g$; likewise $m_2 = g$, contradicting $m_1 \neq m_2$.
- l, m_1, m_2 are three different elements: if $l = m_1$, then $m_1 = l \preceq m_2$, which the first point excludes; likewise $l \neq m_2$.

So an answer has at least three elements and two incomparable maximal ones above a common least element. A candidate failing any of these is not an answer.

Exercise. B3: Minimal is least in a total order

Let $(X, \preceq)$ be a totally ordered set and $A \subseteq X$. Prove that a minimal element of A is a least element of A, by applying Proposition 4.3.2 (b) to the reverse order $\succeq$. Check each fact about $\succeq$ that you use.

Solution. The reverse order. $\succeq$ is the relation $x \succeq y \iff y \preceq x$. (PO1): $x \preceq x$, so $x \succeq x$. (PO2): if $x \succeq y$ and $y \succeq x$, then $y \preceq x$ and $x \preceq y$, so $x = y$. (PO3): if $x \succeq y$ and $y \succeq z$, then $z \preceq y$ and $y \preceq x$, so $z \preceq x$, that is, $x \succeq z$. Totality: for $x, y \in X$, $x \preceq y$ or $y \preceq x$, that is, $y \succeq x$ or $x \succeq y$. Its strict part is $x \succ y \iff y \prec x$, since $x \neq y$ is symmetric in x, y.

Translating. In the order $\succeq$, "x lies below y" is written $x \succeq y$, and "strictly below" is $x \succ y$. Now m is minimal for $\preceq$: $m \in A$ and no $a \in A$ has $a \prec m$, that is, no $a \in A$ has $m \succ a$.

That is exactly "m is maximal for $\succeq$". Likewise "l is greatest for $\succeq$" says $l \in A$ and $a \succeq l$ for every $a \in A$, that is, $l \preceq a$ for every $a \in A$: "l is least for $\preceq$".

Conclusion. Let m be minimal in A for $\preceq$. Then m is maximal in A for the total order $\succeq$, so it is greatest for $\succeq$ by Proposition 4.3.2 (b), hence least for $\preceq$.

4.3.5.3 C. Going deeper

Exercise. C1: A well-order that is not like N

Let $\preceq$ be the lexicographic order on $\mathbb{N} \times \mathbb{N}$ of Exercise A1 (d).

(a) Prove that $\preceq$ is a partial order.

(b) Prove that $(\mathbb{N} \times \mathbb{N}, \preceq)$ is well-ordered.

(c) Show that $(1, n) \prec (2, 1)$ for every $n \in \mathbb{N}$, and that these elements $(1, n)$ are pairwise different. In $(\mathbb{N}, \leq)$, which elements lie strictly below a given $k \in \mathbb{N}$? Deduce that infinitely many elements lie strictly below $(2, 1)$.

Solution.

(a) (PO1) $a = a$ and $b \leq b$, so $(a, b) \preceq (a, b)$. (PO2) Let $(a, b) \preceq (c, d)$ and $(c, d) \preceq (a, b)$. If $a < c$, the second relation needs $c < a$ or $c = a$, both impossible; likewise $c < a$ is impossible. So $a = c$ by trichotomy, and then $b \leq d$ and $d \leq b$ give $b = d$. (PO3) Let $(a, b) \preceq (c, d) \preceq (e, f)$. If $a < c$ or $c < e$, then $a < e$, since in each case the other comparison is $\leq$; so $(a, b) \preceq (e, f)$. Otherwise $a = c = e$ and $b \leq d \leq f$, so again $(a, b) \preceq (e, f)$.

(b) Totality is A1 (d). Let $S \subseteq \mathbb{N} \times \mathbb{N}$ be non-empty. The set $F := \{a \in \mathbb{N} : (a, b) \in S \text{ for some } b \in \mathbb{N}\}$ of first coordinates is non-empty, so it has a least element a_0 (Theorem 2.1.3). The set $G := \{b \in \mathbb{N} : (a_0, b) \in S\}$ is non-empty, since $a_0 \in F$, so it has a least element b_0. Then $(a_0, b_0) \in S$. Let $(a, b) \in S$. Then $a \in F$, so $a_0 \leq a$. If $a_0 < a$, then $(a_0, b_0) \preceq (a, b)$. If $a_0 = a$, then $b \in G$, so $b_0 \leq b$, and again $(a_0, b_0) \preceq (a, b)$. So (a_0, b_0) is the least element of S.

(c) For $n \in \mathbb{N}$, $1 < 2$ gives $(1, n) \preceq (2, 1)$, and $(1, n) \neq (2, 1)$ since $1 \neq 2$; so $(1, n) \prec (2, 1)$. For $n \neq n'$, $(1, n) \neq (1, n')$ by the characteristic property of pairs. So one element, $(2, 1)$, has an element $(1, n)$ strictly below it for each of the natural numbers n, all different. In $(\mathbb{N}, \leq)$, the elements strictly below k are exactly $0, 1, \ldots, k-1$ (none when $k = 0$), by Lemma 2.1.1 (a), (c) and (e): they form a list ending at $k - 1$. So a well-ordered set need not look like $\mathbb{N}$: here one element has a strictly smaller element for every natural number.

Let S be the set of elements strictly below $(2, 1)$, and $B := \{(1, n) : n \in \mathbb{N}\} \subseteq S$. The map $\mathbb{N} \to B$, $n \mapsto (1, n)$, is injective (just shown) and surjective, so $|\mathbb{N}| = |B|$. Suppose S were finite. Then B would have k elements for some k (Proposition 2.5.6), and $|\{1, \ldots, k\}| = |B| = |\mathbb{N}|$ (Proposition 2.5.1 (b), (c)) would make $\mathbb{N}$ finite (Definition 2.5.2); but $\mathbb{N}$ is infinite (Example (Hilbert's Hotel)). So S is infinite (Definition 2.5.3).

Exercise. C2: Infima and suprema under divisibility

Work in $(\mathbb{N}, |)$. Let $a, b \in \mathbb{N}$, not both 0, and let d be the least element of

$$D := \{ka + lb : k, l \in \mathbb{Z}\} \cap \mathbb{Z}_{>0}.$$

(a) Explain why d exists.

(b) Prove that $d \mid a$ and $d \mid b$.

(c) Prove that every common divisor $c \in \mathbb{N}$ of a and b divides d, and conclude that $d = \inf\{a, b\}$.

(d) Decide whether every non-empty subset of $\mathbb{N}$ has a supremum in $(\mathbb{N}, |)$. Then decide the same question for $(\mathbb{Z}_{>0}, |)$.

Solution (Hint 1). For (b), apply the division algorithm to a and d.

Solution (Hint 2). Write $a = qd + r$ with $0 \leq r < d$, and write $d = k_0 a + l_0 b$.

Solution.

(a) $D \subseteq \mathbb{Z}_{>0} \subseteq \mathbb{N}$. It is non-empty: if $a \neq 0$, then $a = 1 \cdot a + 0 \cdot b$ and $a \in \mathbb{Z}_{>0}$, so $a \in D$; otherwise $b \neq 0$ and $b \in D$ likewise. So D has a least element by Theorem 2.1.3, unique by Proposition 4.3.1.

(b) Write $d = k_0 a + l_0 b$ with $k_0, l_0 \in \mathbb{Z}$. Since $d \in \mathbb{Z}_{>0}$, Theorem 2.2.3 gives $a = qd + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < d$. Then

$$r = a - qd = (1 - qk_0)a + (-ql_0)b,$$

with integer coefficients (Proposition 2.1.2 (a)). If $r > 0$, then $r \in \mathbb{Z}_{>0}$, so $r \in D$ and $r < d$, contradicting the choice of d. Hence $r = 0$, and $a = qd$: $d \mid a$. The same argument with b in place of a gives $d \mid b$.

(c) Let $c \in \mathbb{N}$ with $c \mid a$ and $c \mid b$: $a = cs$, $b = ct$ with $s, t \in \mathbb{Z}$. Then $d = k_0 cs + l_0 ct = c(k_0 s + l_0 t)$, so $c \mid d$. In $(\mathbb{N}, |)$, the lower bounds of $\{a, b\}$ are the common divisors in $\mathbb{N}$. By (b), d is one; by (c), every lower bound c has $c \mid d$. So d is the greatest lower bound: $d = \inf\{a, b\}$.

(d) *In $(\mathbb{N}, |)$: yes.* Let $T \subseteq \mathbb{N}$ be non-empty. An upper bound of T is a common multiple $c \in \mathbb{N}$ of all elements of T, and 0 is one, since $t \mid 0 = 0 \cdot t$ for every t.

Case 1: T has a positive common multiple. The positive common multiples form a non-empty subset of $\mathbb{N}$, so they have a least element L (Theorem 2.1.3). It is an upper bound. Let $c \in \mathbb{N}$ be any upper bound. By Theorem 2.2.3, $c = qL + r$ with $0 \leq r < L$. For each $t \in T$, $t \mid c$ and $t \mid L$, so $t \mid r = c - qL$ (as in Example (The supremum under divisibility is the least common multiple)). If $r > 0$, then r is a positive common multiple smaller than L, which is impossible. So $r = 0$ and $L \mid c$. Hence $\sup T = L$. This is the argument of Example (The supremum under divisibility is the least common multiple), which never used that the set had two elements.

Case 2: T has no positive common multiple. Then 0 is its only upper bound, and $\sup T = 0$, the least element of $\{0\}$. This case includes every T containing 0, since $0 \mid c$ forces $c = 0$.

In $(\mathbb{Z}_{>0}, |)$: no. (It is a partial order, as the restriction of one.) Take $T = \mathbb{Z}_{>0}$. An upper bound would be some $c \in \mathbb{Z}_{>0}$ with $t \mid c$ for every $t \in \mathbb{Z}_{>0}$, in particular $(c+1) \mid c$: $c = k(c+1)$ with $k \in \mathbb{Z}$. Since $c > 0$ and $c + 1 > 0$, $k > 0$ (if $k \leq 0$, then $k(c+1) \leq 0$), so $k \geq 1$ (Proposition 2.1.2 (b)), and $c = k(c+1) \geq c + 1$, which is impossible. So T has no upper bound in $\mathbb{Z}_{>0}$, and no supremum. Removing 0 removed the element that bounded everything.

Marking scheme. (10 points)

- 1: (a) D is non-empty (exhibits a or b in it) and $D \subseteq \mathbb{N}$, so well-ordering applies.
- 3: (b) the division algorithm with divisor $d \geq 1$; the remainder is again of the form $ka + lb$; minimality of d forces $r = 0$.
- 2: (c) a common divisor divides d, and the conclusion $d = \inf\{a, b\}$ checks both clauses of an infimum.
- 3: (d) for $\mathbb{N}$: 0 is always an upper bound; with a positive common multiple, the least one divides every upper bound (division algorithm again); without one, the supremum is 0.
- 1: (d) for $\mathbb{Z}_{>0}$: a set with no upper bound, with proof.

Fatal errors (0 for the step): concluding $d \mid a$ from $d \leq a$; in (d), taking the numerically smallest upper bound and not checking that it **divides** every upper bound; treating inf as the minimum under $\leq$.

4.3.5.4 R. Review

Exercise. R1

Let $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 + 4x$. Compute $f([-3, 1])$ and $f^{-1}([-3, 0])$. Then compute $f(\mathbb{R})$, and check that $f(f^{-1}([-5, 0])) = [-5, 0] \cap f(\mathbb{R})$ by computing both sides.

Solution. Complete the square: $f(x) = (x + 2)^2 - 4$. We use, as school facts, that squares are non-negative and that every $y \geq 0$ has a square root $\sqrt{y} \geq 0$, and, by Logic and Proof, Theorem 2.4.5, that for $s, t \geq 0$, $s \leq t$ exactly when $s^2 \leq t^2$.

$f([-3, 1]) = [-4, 5]$. ($\subseteq$) If $-3 \leq x \leq 1$, then $-1 \leq x+2 \leq 3$, so $|x+2| \leq 3$, $0 \leq (x+2)^2 \leq 9$, and $-4 \leq f(x) \leq 5$. ($\supseteq$) For $-4 \leq y \leq 5$, take $x := -2 + \sqrt{y+4}$. Then $0 \leq \sqrt{y+4} \leq 3$, so $x \in [-2, 1] \subseteq [-3, 1]$, and $f(x) = (y + 4) - 4 = y$.

$f^{-1}([-3, 0]) = [-4, -3] \cup [-1, 0]$. For $x \in \mathbb{R}$: $-3 \leq f(x) \leq 0 \iff 1 \leq (x+2)^2 \leq 4 \iff 1 \leq |x+2| \leq 2$, and splitting by the sign of $x+2$, this holds exactly when $x+2 \in [-2, -1] \cup [1, 2]$, that is, $x \in [-4, -3] \cup [-1, 0]$.

$f(\mathbb{R}) = [-4, \infty)$, by the argument for $f([-3, 1])$: $f(x) \geq -4$ always, and $y \geq -4$ is $f(-2 + \sqrt{y+4})$.

The check. $f^{-1}([-5, 0]) = \{x : (x + 2)^2 \leq 4\} = [-4, 0]$, since $(x + 2)^2 - 4 \geq -4 > -5$ always. Then $f([-4, 0]) = [-4, 0]$, by the first computation's method ($x + 2 \in [-2, 2]$, so $(x + 2)^2 \in [0, 4]$, and each value is attained). On the other side, $[-5, 0] \cap [-4, \infty) = [-4, 0]$. Both sides are $[-4, 0]$, as Proposition 1.7.5 (b) predicts: the round trip removes exactly the part $[-5, -4)$ of $[-5, 0]$ that f never reaches.

Exercise. R2

Write in symbols, with bounded quantifiers, the statement "every element of A has an element of A strictly above it", for a set $A \subseteq \mathbb{R}$ ordered by $\leq$. Write its negation with no $\neg$ in front of a quantifier, and decide which of the two holds for $A = \mathbb{N}$ and for $A = \{1, \dots, 5\}$.

Solution. The statement is $\forall a \in A\ \exists b \in A\ \ a < b$. By Logic and Proof, Proposition 6.2.3 (a) and then (b), its negation is

$$\exists a \in A\ \forall b \in A\ \ \neg(a < b),$$

and since $\leq$ is total on $\mathbb{R}$, $\neg(a < b)$ is $b \leq a$: the negation is $\exists a \in A\ \forall b \in A\ \ b \leq a$, "$A$ has a greatest element". Passing the $\neg$ through the quantifiers turns each $\forall$ into $\exists$ and each $\exists$ into $\forall$, and leaves the bounds $a \in A$, $b \in A$ untouched; negating the bound instead is entry (N11) of Logic and Proof, Example (What is not allowed).

For $A = \mathbb{N}$ the statement holds: for $a \in \mathbb{N}$, $b := a + 1 \in \mathbb{N}$ by (NS), and $a < a + 1$. For $A = \{1, \dots, 5\}$ the negation holds, with $a = 5$: every $b \in A$ has $b \leq 5$.

Exercise. R3

Let X be a countable set and $\sim$ an equivalence relation on X. Prove that $X/\!\sim$ is countable. Give an example with X countable, not finite, and $X/\!\sim$ finite.

Solution. The quotient map $q\colon X \to X/\!\sim$, $q(a) = [a]$, is surjective (Definition 4.2.4 and the paragraph after it). By Proposition 3.1.4, the image of a countable set under a function is countable, and here the image is all of $X/\!\sim$. Example: $X = \mathbb{Z}$, countable by Theorem 3.1.8, and not finite, since it contains $\mathbb{N}$, which is infinite (Example (Hilbert's Hotel), Proposition 2.5.6), with congruence modulo 2: $\mathbb{Z}/2 = \{[0], [1]\}$ (Proposition 4.2.4) has two elements.

Exercise. R4

Let $(X, \preceq)$ be a partially ordered set, let $n \geq 1$ be an integer, and let $x_1, \dots, x_n \in X$. Show that the set $\{x_1, \dots, x_n\}$ has a maximal element.

Solution. *The tool* is induction from base 1 (Theorem 2.2.1 with $n_0 = 1$), in the shape of Proposition 2.3.8: add one element at a time and keep track of a maximal element. Let $P(n)$ say: for all $x_1, \dots, x_n \in X$, the set $\{x_1, \dots, x_n\}$ has a maximal element.

Base. $\{x_1\}$: no element a of it has $x_1 \prec a$, since the only candidate is x_1 and $x_1 \prec x_1$ never holds. So x_1 is maximal.

Step. Let $n \geq 1$, assume $P(n)$, and let $x_1, \dots, x_{n+1} \in X$. Put $A := \{x_1, \dots, x_n\}$ and $A' := \{x_1, \dots, x_{n+1}\}$, where, as in Section 2.3, $\{x_1, \dots, x_n\} := \{x_k : k \in \{1, \dots, n\}\}$, now for elements of X. Since $\{1, \dots, n+1\} = \{1, \dots, n\} \cup \{n+1\}$ (Lemma 2.1.1 (e), as in the proof of Proposition 2.3.8), $A' = A \cup \{x_{n+1}\}$. By $P(n)$, A has a maximal element m.

Case 1: $m \prec x_{n+1}$ fails. Then m is maximal in A': $m \in A'$; no $a \in A$ has $m \prec a$, by maximality in A; and $a = x_{n+1}$ is excluded by the case.

Case 2: $m \prec x_{n+1}$. Then x_{n+1} is maximal in A'. Suppose $x_{n+1} \prec a$ with $a \in A'$. Then $a \neq x_{n+1}$, so $a \in A$; and $m \prec x_{n+1} \prec a$ gives $m \prec a$, since the strict part of a partial order is transitive. This contradicts the maximality of m in A.

In either case A' has a maximal element, so $P(n+1)$ holds, and Theorem 2.2.1 gives $P(n)$ for every $n \geq 1$.

The look-alikes. "Take the greatest element" fails, because a finite set need not have one (Example (Maximal elements that are not greatest)). "Take the largest, as in Proposition 2.3.8" fails for the same reason: that proof keeps the larger of M and x_{n+1}, which needs the two to be comparable; here Case 1 covers incomparable elements by keeping m. "Take x_n, the last one" confuses the order of the list with the order $\preceq$: nothing makes x_n large.

Chapter 5

Building Functions

Chapter 1 made a function a set of pairs, and Chapter 4 cut sets into classes. This chapter builds new functions from old ones: cut a function down to a smaller domain, extend it, glue several together, factor it through the quotient by "has the same value", combine functions by an operation, and apply one function again and again. The motivating problem: *shuffle a deck of twelve cards by a fixed rule and repeat the shuffle; must the deck come back to its starting order, and after how many shuffles?* The answer is in Section 5.4, and it comes from the orbits of a permutation, which are the classes of an equivalence relation. Along the way, the subsets of a set turn out to be functions with values 0 and 1, and a function turns out to be a quotient map, followed by a bijection between its fibers and its image, followed by an inclusion.

Each section teaches one method of proof. Section 5.1 defines a function by pieces and checks that the pieces agree where they overlap. Section 5.2 defines a function on a quotient by a rule on representatives and checks that the rule is constant on classes, which is the well-definedness check of Section 4.2 turned into a theorem. Section 5.3 proves that two objects are equal by computing one expression in two ways. Section 5.4 follows a point under repeated application of a map until the sequence repeats. The operations of Section 5.3 and the permutations of Section 5.4 are the first examples of the structures that *Algebraic Preliminaries* studies, and this chapter proves facts that book can cite.

What you need. *Logic and Proof*, Chapters 1–8, and *Sets and Functions*, Chapters 1–4 and Section 3.6. From *Logic and Proof*: induction (Logic and Proof, Axiom 4.2.1), squares and order (Logic and Proof, Theorem 2.4.5) and the catalogue of what a proof may not do (Logic and Proof, Example (What is not allowed)). From Chapter 1: equality of sets and subsets (Definition 1.2.1, Definition 1.2.2), the operations on sets, families and the laws of set algebra (Definition 1.3.1, Definition 1.3.4, Theorem 1.3.1), the method of uniqueness (Example (Method: existence and uniqueness)), and divisibility is transitive (Proposition 1.1.1); functions, the empty function, equality of functions and what is not a function (Definition 1.5.1, Proposition 1.5.2, Proposition 1.5.1, Example (First functions), Example (Relations that are not functions)); injective, surjective and bijective maps and composition (Definition 1.5.3, Definition 1.5.4, Definition 1.5.5, Definition 1.5.2, Proposition 1.5.3, Theorem 1.5.4); inverses (Definition 1.6.2, Proposition 1.6.3, Theorem 1.6.4, Exercise (B2: The inverse of a composite)); images and preimages (Definition 1.7.1, Definition 1.7.2, Theorem 1.7.3, Theorem 1.7.4). From Chapter 2: the integers are closed under the operations (Proposition 2.1.2), well-ordering and induction (Theorem 2.1.3, Theorem 2.2.1), the division algorithm (Theorem 2.2.3), definition by recursion, powers and sums (Theorem 2.3.1, Definition 2.3.2, Definition 2.3.1), and finite sets: equinumerous and finite sets, the uniqueness of the number of elements and the pigeonhole principle (Definition 2.5.1, Definition 2.5.2, Corollary 2.5.4, Corollary 2.5.3), subsets and disjoint unions of finite sets (Proposition 2.5.6, Proposition 2.5.5), and Hilbert's hotel (Example

(Hilbert's Hotel)). From Chapter 3: the default-value repair in the find-the-error exercise on subsets of countable sets (Exercise (C2: Find the error)), the axiom of choice and right inverses of surjections (Axiom 3.2.1, Theorem 3.2.2), the diagonal (Theorem 3.3.1, Theorem 3.3.2, Exercise (C2: Permutations of the naturals)), the Schröder–Bernstein theorem (Theorem 3.4.3), and, from Section 3.6, subsets as 0–1 functions (Theorem 3.6.4, Corollary 3.6.5). From Chapter 4: relations and their properties (Example (Method: proving or disproving a property of a relation)), equivalence relations, classes, partitions and quotient sets (Definition 4.2.1, Definition 4.2.2, Definition 4.2.3, Definition 4.2.4, Theorem 4.2.1), congruence (Definition 4.2.5, Proposition 4.2.5, Proposition 4.2.4), the fibers of a function as classes (Example (The fibers of a function)), the check that a definition does not depend on the representative (Example (Method: checking that a definition on classes is well defined)), the reals modulo the integers and equal-size subsets as quotients (Example (The reals modulo the integers), Example (Same size, revisited)), a quotient built from fractions (Exercise (B1: Fractions as classes)), and the least common multiple as an order example (Example (The supremum under divisibility is the least common multiple)). The arithmetic and order of $\mathbb{R}$ are school facts in examples, as in the earlier chapters.

Time. About 25 hours on the core track (all of A, one B and one C per section, the exit checks); about 35 hours for everything.

5.0.1 Roadmap

- **Restriction, extension and gluing.** Restriction to a subset, extension, the inclusion map; a function defined on the pieces of a cover is one function exactly when the pieces agree on the overlaps; indicator functions, with the set operations as arithmetic of indicators and the subsets of X as the functions $X \to \{0,1\}$; the method: define a function by gluing.
- **Fibers and the canonical factorization.** The fibers of a function partition its domain, and every function is a quotient map, then a bijection onto its image, then an inclusion; a function constant on classes factors through the quotient in exactly one way; the method: define a function on a quotient.
- **Binary operations.** An operation on a set, closure, associativity, commutativity, identities and inverses, with the uniqueness proofs; the operations on the set of functions Y^X defined pointwise, and composition as an operation on X^X; an operation that is constant on classes descends to the quotient; the method: compute one expression in two ways.
- **Permutations and iteration.** The permutations of a set and their composites and inverses, iterates by recursion, orbits as the classes of an equivalence relation, fixed points, the decomposition of a permutation of a finite set into disjoint cycles, the number of shuffles after which a deck returns, and the eventually periodic orbits of a self-map of a finite set; the method: follow an orbit.

5.0.2 Named moves

Each is a method box in the section named at the end of its line; later sections, and the later chapters of this volume, use the move again. The first four below are this chapter's; the last bullet names three earlier moves reused here as tools: Chapter 4's well-definedness, Chapter 1's uniqueness and Chapter 2's pigeonhole principle.

- **Define a function by gluing** (Example (Method: define a function by gluing)). Name the pieces, check that they cover the domain, check that the formulas agree on each overlap, and conclude by the gluing theorem; prove injectivity across pieces too, not only inside each piece. (Section 5.1)

- **Define a function on a quotient** (Example (Method: define a function on a quotient)). Write the function on X that the rule computes from a representative, check that it is constant on classes, and conclude that the induced function exists, is unique, and agrees with the rule. (Section 5.2)
- **Compute one expression in two ways** (Example (Method: compute one expression in two ways)). To equate two objects known only through equations, reduce both to one expression and cite a hypothesis at each step. (Section 5.3)
- **Follow an orbit** (Example (Method: follow an orbit)). List the forward orbit of a point, use the pigeonhole principle to find a repeat in a finite set, take the first repeat, and carry the repeat through the structure of the map. (Section 5.4)
- **Well-definedness** (Example (Method: checking that a definition on classes is well defined)), from Section 4.2, is step 2 of the quotient box, and **uniqueness** (Example (Method: existence and uniqueness)), from Section 1.4, is the shape of the uniqueness proofs in Section 5.3. The **pigeonhole principle** (Corollary 2.5.3) is step 2 of the orbit box.

5.0.3 Threads

- **Same value, same class.** Section 4.2 observed that the fibers of a function are the classes of an equivalence relation (Example (The fibers of a function)). Section 5.2 turns the observation into a factorization theorem (Theorem 5.2.2), and Section 5.3 runs the same well-definedness check on pairs of classes to define an operation on a quotient (Proposition 5.3.6).
- **Subsets are functions.** Section 1.5 introduced the indicator of a subset, Section 3.6 proved that $A \mapsto \mathbf{1}_A$ is a bijection (Theorem 3.6.4), and Section 5.1 makes it a calculus: intersections and complements of subsets are products and differences of indicators, and the indicator of a union is $\mathbf{1}_A+\mathbf{1}_B-\mathbf{1}_A\mathbf{1}_B$ (a sum when the sets are disjoint) (Proposition 5.1.3).
- **Inverses.** Section 1.6 showed that a function has at most one inverse. Section 5.3 shows that an element has at most one inverse for any associative operation with an identity (Proposition 5.3.2), of which composition of bijections is the case, and Section 5.4 puts this to work on the set of permutations.
- **Orbits.** The classes of "can be reached from" are the orbits of a permutation (Theorem 5.4.3), and each is a cycle (Proposition 5.4.4). The same idea, without invertibility, gives tails and cycles for an arbitrary self-map of a finite set (Proposition 5.4.7).

5.0.4 Summary

A function can be restricted to a subset, extended, and glued from functions on the pieces of a cover that agree on the overlaps (Theorem 5.1.2). Subsets of X correspond to indicator functions, and the set operations become arithmetic (Proposition 5.1.3). The fibers of a function partition its domain (Proposition 5.2.1), and every function factors as a quotient map, a bijection and an inclusion (Theorem 5.2.2); a function that is constant on the classes of an equivalence relation factors through the quotient in exactly one way (Theorem 5.2.3). The identity of an associative operation and the inverse of an element are unique (Proposition 5.3.1, Proposition 5.3.2), pointwise operations on Y^X inherit the properties of the operation on Y (Proposition 5.3.4), and an operation that respects an equivalence relation descends to the quotient (Proposition 5.3.6). The permutations of a set are closed under composition and inverses (Proposition 5.4.1), the orbits of a permutation partition the set (Theorem 5.4.3), and a permutation of a finite set is a product of disjoint cycles (Theorem 5.4.5), so some power of it is the identity (Corollary 5.4.6).

What is open: Zorn's lemma, in Chapter 6. The permutations of a set with composition are the first example of the structures that *Algebraic Preliminaries*, Chapter 2 will study. Next, Chapter 6 states and uses Zorn's lemma.

5.0.5 Terms

- **associative, commutative**: properties of an operation $*$ with $(x * y) * z = x * (y * z)$, respectively $x * y = y * x$, for all x, y, z (Definition 5.3.2).
- **binary operation** on a set X: a function $X \times X \to X$; the operation is **closed** on a subset A if $x * y \in A$ for all $x, y \in A$ (Definition 5.3.1).
- **cycle**: the permutation $(x_1\ x_2\ \cdots\ x_k)$ that sends $x_j \mapsto x_{j+1}$, $x_k \mapsto x_1$ and fixes every other point; **disjoint cycles** have disjoint sets of entries (Definition 5.4.4).
- **extension, restriction**: g extends $f\colon A \to Y$ if $g|_A = f$; $f|_A$ is the function f with its domain cut down to A (Definition 5.1.1).
- **fiber** of a function $f\colon X \to Y$ over y: the set $\{x \in X : f(x) = y\}$ (Example (The fibers of a function), Proposition 5.2.1).
- **fixed point** of $f\colon X \to X$: a point with $f(x) = x$ (Definition 5.4.3).
- **identity** (left, right, two-sided) of an operation; **inverse** of an element and **invertible** element (Definition 5.3.2).
- **inclusion map** $\iota_A\colon A \to X$, $a \mapsto a$ (Definition 5.1.1).
- **indicator function** $\mathbf{1}_A\colon X \to \{0, 1\}$ of $A \subseteq X$: 1 on A, 0 off A (Definition 5.1.2).
- **iterate** f^n: the n-th composite of a self-map f, by recursion; for a permutation, also σ^{-n} (Definition 5.4.2).
- **orbit** of x under a permutation σ: $\{\sigma^k(x) : k \in \mathbb{Z}\}$; its **length** is its number of elements (Proposition 5.4.4); the **forward orbit** of x under any self-map is $\{f^n(x) : n \in \mathbb{N}\}$ (Definition 5.4.3).
- **permutation** of X: a bijection $X \to X$; S_X is the set of them (Definition 5.4.1).
- **symmetric difference** $A \triangle B$: the elements in exactly one of A and B (Section 5.1, before Proposition 5.1.3).

5.1 Restriction, Extension and Gluing

Chapter 1 made a function a graph with a codomain, and Chapter 4 cut sets into classes. This chapter builds new functions out of old ones. Here we take the three simplest constructions: cutting a function down to a smaller domain, enlarging its domain, and assembling one function from pieces defined on parts of the domain. The last of these is behind every definition "by cases", and the section ends with the functions that take only the values 0 and 1, with which an equation between sets becomes a computation with numbers.

5.1.1 A function in two pieces

The proof of the Schröder–Bernstein theorem (Theorem 3.4.3) defined its bijection h by one formula on a set C and by another off C, and then said: each a falls under exactly one case, and in each case the value exists and is unique, so h is a function. That sentence carried the whole definition. It is worth asking what it really needed.

Here is a familiar definition by cases:

$$|x| = \begin{cases} x & \text{if } x \geq 0, \\ -x & \text{if } x \leq 0. \end{cases}$$

This time a point falls under **both** cases: $0 \geq 0$ and $0 \leq 0$. So the sentence from Schröder–Bernstein does not apply. Is $|\cdot|$ still a function? Most readers would say yes at once, because

both formulas give 0 at 0. Now try

$$r(x) = \begin{cases} x & \text{if } x \geq 0, \\ x+1 & \text{if } x \leq 0. \end{cases}$$

At 0 the first line gives 0 and the second gives 1. The "rule" offers two values at one input, and by (Fn2) of Definition 1.5.1 it is not a function.

So whether "one formula on this piece, another on that piece" defines a function depends on two things: whether the pieces leave any point out, and what the formulas do where the pieces meet. *Before reading on: write down the condition on two formulas, on two pieces, that makes the definition a function.* The gluing theorem below answers this, for any number of pieces.

5.1.2 Restriction and extension

Section 1.5 cut a function down: the restriction of $f\colon X \to Y$ to a subset $A \subseteq X$ keeps the pairs of f whose input lies in A. The reverse question is just as natural. A function is known on part of a set, say $g(x) = 1/x$ on $(0, 1]$; can it be **extended** to a larger set, and in how many ways?

A restriction forgets part of the domain; an extension fills in the part that was missing.

Definition 5.1.1. Restriction, Extension, Inclusion

Let X and Y be sets and $A \subseteq X$.

(a) For $f\colon X \to Y$, the **restriction** of f to A is the function $f|_A\colon A \to Y$, $f|_A(a) \coloneqq f(a)$, as in Section 1.5.

(b) For $g\colon A \to Y$, an **extension** of g to X is **a** function $f\colon X \to Y$ with $f|_A = g$.

(c) The **inclusion map** of A into X is $\iota_A\colon A \to X$, $\iota_A(a) \coloneqq a$.

In words: the restriction keeps the codomain and forgets the inputs outside A. An extension is any function on the larger set that agrees with g at every point of A; by Proposition 1.5.1, $f|_A = g$ says exactly that $f(a) = g(a)$ for every $a \in A$, since both functions have domain A and codomain Y. The inclusion map is the identity of A with its codomain enlarged to X; it is not id_A unless $A = X$, because the codomains differ.

The article in (b) is "**a**", not "the", and the naive expectation that an extension is determined by g fails at once. The function $g\colon (0, 1] \to \mathbb{R}$, $g(x) = 1/x$, has an extension to $[0, 1]$ for every choice of a value at 0: sending 0 to 0 and sending 0 to 5 give two different extensions, since they differ at 0. The formula $1/x$ suggests no value at all there. Nor need an extension keep a property that g has. Let $a \neq b$, and let $g\colon \{1, 2\} \to \{a, b\}$ send $1 \mapsto a$ and $2 \mapsto b$, a bijection. An extension to $\{1, 2, 3\}$ with codomain $\{a, b\}$ is a function from a set of three elements to a set of two, and by Corollary 2.5.3 (a) no such function is injective. So the bijection g has extensions, but no injective one.

Restriction, by contrast, is predictable. The next proposition lists what it does.

Proposition 5.1.1. Restrictions

Let $f\colon X \to Y$ be a function and $B \subseteq A \subseteq X$.

(a) $f|_A = f \circ \iota_A$.

(b) $(f|_A)|_B = f|_B$.

(c) For every function $g\colon Y \to Z$, $(g \circ f)|_A = g \circ (f|_A)$.
(d) If f is injective, then so is $f|_A$.
(e) $f|_A(B) = f(B)$.

Idea. Parts (a)–(c) are equations between functions, so we compare domains, codomains and values. Parts (d) and (e) only unwind Definition 1.5.3 and Definition 1.7.1, using $f|_A(a) = f(a)$.

Proof. For (a)–(c) we use Proposition 1.5.1: in each part both sides have the same domain and codomain, and we compare values.

(a) Both sides are functions $A \to Y$ (Definition 1.5.2). For $a \in A$, $(f \circ \iota_A)(a) = f(\iota_A(a)) = f(a) = f|_A(a)$.
(b) Both sides are functions $B \to Y$. For $b \in B$, $(f|_A)|_B(b) = f|_A(b) = f(b) = f|_B(b)$, where the middle step uses $b \in A$.
(c) Both sides are functions $A \to Z$. For $a \in A$, $(g \circ f)|_A(a) = g(f(a)) = g(f|_A(a)) = (g \circ (f|_A))(a)$.
(d) Let $a, a' \in A$ with $f|_A(a) = f|_A(a')$. Then $f(a) = f(a')$, so $a = a'$ because f is injective (Definition 1.5.3).
(e) By Definition 1.7.1, $f|_A(B) = \{f|_A(b) : b \in B\} = \{f(b) : b \in B\} = f(B)$, since $f|_A(b) = f(b)$ for every $b \in B \subseteq A$.

■

Part (e) with $B = A$ says that the restriction has the same image as f on A: $f|_A(A) = f(A)$. Part (d) has no partner for surjectivity, and the next check asks why.

Quick check. Is a restriction of a surjection always surjective?

Solution. No. The function $f\colon \mathbb{R} \to [0, \infty)$, $f(x) = x^2$, is surjective (every $t \geq 0$ is $(\sqrt{t})^2$). Its restriction $f|_{[1,2]}\colon [1, 2] \to [0, \infty)$ has image $f([1, 2]) = [1, 4]$, so 0 is not a value. The restriction keeps the codomain while the domain shrinks, so it can lose surjectivity. It can also gain injectivity: $f|_{[0,\infty)}$ is injective, although f is not.

5.1.3 Gluing

Restriction takes a function apart: it hands us the pieces $f|_{A_i}$ on the parts A_i of the domain. Gluing is the reverse. We are given functions on the parts and want one function on the whole set. The hook named the two ways this can go wrong: a point may lie in no part, and a point may lie in two parts whose formulas disagree there. Only the second failure appeared there; the first is easy to picture.

Theorem 5.1.2. Gluing Functions

Let $(A_i)_{i\in I}$ be a family of subsets of a set X with $\bigcup_{i\in I} A_i = X$, and let $(f_i)_{i\in I}$ be a family of functions $f_i\colon A_i \to Y$. Suppose the f_i **agree on overlaps**:

$$f_i(x) = f_j(x) \quad \text{for all } i, j \in I \text{ and every } x \in A_i \cap A_j.$$

Then there is **exactly one** function $f\colon X \to Y$ with $f|_{A_i} = f_i$ for every $i \in I$.

Idea (Scratch work). A function is a graph satisfying (Fn1) and (Fn2), together with a codomain (Definition 1.5.1). We must produce a graph, and the only graphs in sight are the graphs G_i of the f_i. The obvious candidate is their union. The plan, as givens and goal:

Givens	Goal
graphs $G_i \subseteq A_i \times Y$, each with (Fn1) and (Fn2) on A_i; $\bigcup_i A_i = X$; agreement on overlaps	a function $f\colon X \to Y$ whose restriction to each A_i is f_i, and only one
$G \coloneqq \bigcup_i G_i \subseteq X \times Y$	(Fn1) and (Fn2) for G on X
$x \in X$, so $x \in A_i$ for some i (the cover)	(Fn1): $(x, f_i(x)) \in G_i \subseteq G$
$(x, y) \in G_i$, $(x, y') \in G_j$; so $y = f_i(x)$, $y' = f_j(x)$ and $x \in A_i \cap A_j$	(Fn2): $y = y'$; this is the gap, and agreement on overlaps closes it

In the existence part each hypothesis has one job: the cover gives (Fn1), agreement gives (Fn2). Uniqueness is easier: two functions with the right restrictions both take the value $f_i(x)$ at a point $x \in A_i$.

Proof. For each $i \in I$, let $G_i \subseteq A_i \times Y$ be the graph of f_i, and let $G \coloneqq \bigcup_{i\in I} G_i$ (Definition 1.3.4). Since $A_i \subseteq X$, each $G_i \subseteq X \times Y$, so $G \subseteq X \times Y$.

(Fn1). Let $x \in X$. Since $\bigcup_{i\in I} A_i = X$, there is $i \in I$ with $x \in A_i$. Then $(x, f_i(x)) \in G_i \subseteq G$.

(Fn2). Let $(x, y) \in G$ and $(x, y') \in G$. Then $(x, y) \in G_i$ and $(x, y') \in G_j$ for some $i, j \in I$. Since $G_i \subseteq A_i \times Y$ and $G_j \subseteq A_j \times Y$, we have $x \in A_i \cap A_j$, and by $(**)$ of Section 1.5, $y = f_i(x)$ and $y' = f_j(x)$. Agreement on overlaps gives $y = y'$.

So $f \coloneqq (G, Y)$ is a function $X \to Y$. Let $i \in I$. Both $f|_{A_i}$ and f_i are functions $A_i \to Y$, and for $x \in A_i$ we have $(x, f_i(x)) \in G$, so $f(x) = f_i(x)$ by $(**)$; that is, $f|_{A_i}(x) = f_i(x)$. By Proposition 1.5.1, $f|_{A_i} = f_i$.

Uniqueness. Let $g\colon X \to Y$ also satisfy $g|_{A_i} = f_i$ for every $i \in I$. Let $x \in X$, and choose i with $x \in A_i$. Then $g(x) = g|_{A_i}(x) = f_i(x) = f|_{A_i}(x) = f(x)$. By Proposition 1.5.1, $g = f$. This proves the theorem.

■

In the existence part, the proof used the cover only for (Fn1) and agreement only for (Fn2). Each hypothesis is needed. If a point x lies in no A_i, the union graph has no pair with first coordinate x, and (Fn1) fails; the theorem fails too: for $X = Y = \{0, 1\}$, $A_1 = \{0\}$ and $f_1(0) = 0$, both

ways of choosing the value at 1 give a function f with $f|_{A_1} = f_1$, so "exactly one" fails. The rule r of the hook shows two pieces that cover $\mathbb{R}$ and disagree at 0, where (Fn2) fails.

The theorem is used so often that its use deserves a template. Step (4) below is the one most often forgotten.

Example. Method: define a function by gluing

Template. (1) Name the pieces and check that they cover the domain. (2) For each two pieces, find the overlap and check that the formulas agree on it; disjoint pieces need nothing. (3) Conclude by Theorem 5.1.2. (4) Prove further properties piece by piece **and across pieces**: for injectivity, compare a value from one piece with a value from another.

When to use it. Definitions by cases, piecewise formulas, a default value off a subset, constructions such as Schröder–Bernstein's.

The usual failure. Checking the cover and forgetting the overlaps (a boundary point lies in two pieces); checking injectivity inside each piece only.

Example. Piecewise definitions are gluings

Decide whether each definition glues to a function $\mathbb{R} \to \mathbb{R}$.

(a) x on $[0, \infty)$ and $-x$ on $(-\infty, 0]$.
(b) x on $[0, \infty)$ and $x + 1$ on $(-\infty, 0]$.
(c) x on $[0, \infty)$ and $x + 1$ on $(-\infty, 0)$. If it glues, is the result injective?

Solution.

(a) Step (1): the pieces cover $\mathbb{R}$, since every real number is ≥ 0 or ≤ 0. Step (2): the overlap is $\{0\}$, where the formulas give 0 and $-0 = 0$. They agree, so by Theorem 5.1.2 there is exactly one function with these restrictions: the absolute value $|\cdot|$.

(b) The pieces cover $\mathbb{R}$ and overlap in $\{0\}$, where the values are 0 and 1. Agreement fails, so the hypothesis of Theorem 5.1.2 fails; and no function can have both restrictions, since its value at 0 would be 0 and 1. This is the rule r of the hook, which is not a function.

(c) A minimal change to (b): the second piece loses the point 0. Now the pieces are disjoint and still cover $\mathbb{R}$, so step (2) has nothing to check, and they glue to a function $k\colon \mathbb{R} \to \mathbb{R}$. Inside each piece k is injective ($x = x'$ and $x+1 = x'+1$ each force $x = x'$). Across the pieces, step (4) finds a collision: $k(\frac{1}{2}) = \frac{1}{2}$ and $k(-\frac{1}{2}) = -\frac{1}{2} + 1 = \frac{1}{2}$. So k is not injective.

Back to Schröder–Bernstein. In the proof of Theorem 3.4.3, the pieces were C and $A \setminus C$: disjoint, and covering A. So the definition of h is a gluing, with nothing to check in step (2), and "each a falls under exactly one case" is steps (1) and (2) at once: the pieces cover A, and there is no overlap to check. The proof's Case 3 of injectivity, one point in C and one outside, is step (4)'s comparison across pieces; Cases 1 and 2 are the checks inside each piece.

Default values. Let $A \subseteq X$, $g\colon A \to Y$ and $y_0 \in Y$. "Take g on A and the value y_0 on $X \setminus A$" glues g with the constant function $X \setminus A \to Y$ with value y_0: the pieces A and $X \setminus A$ are disjoint

and cover X. The "Repair" in the solution of Section 3.1's Exercise (C2: Find the error) was a default-value definition of this kind, with the default a_0 on the inputs that had no value of the right kind. The indicator functions of the next subsection are default-value definitions too.

Warning. A boundary point usually lies in two pieces. "x^2 on $(-\infty, 1]$, $3x$ on $[1, \infty)$" covers $\mathbb{R}$, and each formula is a function on its piece, but at 1 the values are 1 and 3, so nothing glues. Check every overlap, not just the cover.

Quick check. Glue x^2 on $(-\infty, 1]$ and $2x - 1$ on $[1, \infty)$. Does it glue? Is the result injective?

Solution. The pieces cover $\mathbb{R}$ and overlap in $\{1\}$, where $1^2 = 1 = 2 \cdot 1 - 1$; so the definitions glue to a function $f\colon \mathbb{R} \to \mathbb{R}$. It is not injective, and the failure is inside the first piece: $f(-1) = 1 = f(1)$.

5.1.4 Indicator functions

A subset A of X can be described by a function that answers, for each $x \in X$, the question "is x in A?" with 1 for yes and 0 for no. Section 1.5 met this function in Example (First functions) (d). It now gets its own label, because it turns statements about sets into arithmetic.

Definition 5.1.2. Indicator Function

Let X be a set and $A \subseteq X$. The **indicator function** of A is $\mathbf{1}_A\colon X \to \{0, 1\}$,

$$\mathbf{1}_A(x) := \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } x \in X \setminus A. \end{cases}$$

It is a default-value definition: the constant 1 on A glued with the constant 0 on $X \setminus A$, over a disjoint cover of X. The function depends on X as well as on A, since X is its domain; throughout this subsection one set X is fixed and every set named is a subset of it. Two small cases: $\mathbf{1}_X$ is the constant function 1, and $\mathbf{1}_\emptyset$ is the constant function 0.

Section 3.6 proved that $A \mapsto \mathbf{1}_A$ is a bijection $\mathcal{P}(X) \to \{0, 1\}^X$, with inverse $f \mapsto \{x \in X : f(x) = 1\} = f^{-1}(\{1\})$ (Theorem 3.6.4). Only one consequence is needed here, and it can be read off directly: A is recovered from its indicator as the set of points where the value is 1. So

$$\mathbf{1}_A = \mathbf{1}_B \quad \text{implies} \quad A = B.$$

This is what lets a computation with indicators prove an equation between sets: show that the two sides have the same indicator, and they are equal.

To compute, we need to know what the set operations do to indicators. Besides the operations of Definition 1.3.1 we use one more. The **symmetric difference** of A and B is

$$A \triangle B := (A \setminus B) \cup (B \setminus A),$$

the set of points that lie in exactly one of A and B.

Proposition 5.1.3. Set Operations as Arithmetic of Indicators

Let $A, B \subseteq X$. For every $x \in X$, write $u \coloneqq \mathbf{1}_A(x)$ and $v \coloneqq \mathbf{1}_B(x)$. Then:

(a) $\mathbf{1}_{A\cap B}(x) = uv$;
(b) $\mathbf{1}_{X\setminus A}(x) = 1 - u$;
(c) $\mathbf{1}_{A\cup B}(x) = u + v - uv$;
(d) $\mathbf{1}_{A\triangle B}(x) = u + v - 2uv$;
(e) $A \subseteq B$ if and only if $\mathbf{1}_A(x) \leq \mathbf{1}_B(x)$ for **every** $x \in X$.

Idea. For (a), (b) and (d), membership of x in the left-hand set is decided by which of $x \in A$, $x \in B$ hold: four cases, one table. Part (c) need not be tabled at all: De Morgan turns a union into a complement of an intersection, and (a), (b) compute that.

Proof. Fix $x \in X$. By Definition 5.1.2, $u = 1$ if $x \in A$ and $u = 0$ otherwise, and likewise for v and B.

(a), (b), (d). There are four cases, and in each we read membership from Definition 1.3.1 and the definition of $\triangle$:

$x \in A$?	$x \in B$?	u	v	$x \in A\cap B$?	uv	$x \in X \setminus A$?	$1-u$	$x \in A\triangle B$?	$u+v-2uv$
yes	yes	1	1	yes	1	no	0	no	0
yes	no	1	0	no	0	no	0	yes	1
no	yes	0	1	no	0	yes	1	yes	1
no	no	0	0	no	0	yes	1	no	0

In every row, the number in each formula column is 1 exactly when the membership column before it says yes, and 0 otherwise. That is (a), (b) and (d).

(c) By Theorem 1.3.1 (d) with X in the place of A, $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$. Applying (a) to the sets $X \setminus A$ and $X \setminus B$, whose indicators at x are $1 - u$ and $1 - v$ by (b), gives $\mathbf{1}_{X\setminus(A\cup B)}(x) = (1 - u)(1 - v)$. Applying (b) to the set $A \cup B \subseteq X$,

$$\mathbf{1}_{A\cup B}(x) = 1 - \mathbf{1}_{X\setminus(A\cup B)}(x) = 1 - (1 - u)(1 - v) = u + v - uv.$$

(d) ($\Rightarrow$) Suppose $A \subseteq B$ and let $x \in X$. If $\mathbf{1}_A(x) = 1$, then $x \in A$, so $x \in B$ and $\mathbf{1}_B(x) = 1$. If $\mathbf{1}_A(x) = 0$, then $\mathbf{1}_A(x) \leq \mathbf{1}_B(x)$ since $\mathbf{1}_B(x) \in \{0, 1\}$. ($\Leftarrow$) Suppose the inequality holds at every point, and let $x \in A$. Then $1 = \mathbf{1}_A(x) \leq \mathbf{1}_B(x) \leq 1$, so $\mathbf{1}_B(x) = 1$ and $x \in B$. By Definition 1.2.2, $A \subseteq B$.

■

Part (e) says the only pattern of values that $A \subseteq B$ forbids is $u = 1$, $v = 0$: a point of A outside B.

Quick check. Express $\mathbf{1}_{A\setminus B}(x)$ in terms of $u = \mathbf{1}_A(x)$ and $v = \mathbf{1}_B(x)$.

Solution. By Definition 1.3.1, $A \setminus B = A \cap (X \setminus B)$, since both consist of the points of A not in B. By (a) and (b), $\mathbf{1}_{A\setminus B}(x) = u(1-v) = u - uv$. Check on the row $u = 1$, $v = 0$: the value is 1, and indeed such an x lies in $A \setminus B$.

Compute with indicators. To prove an equation $L = R$ between sets built from subsets A, B, C of X, fix $x \in X$, write u, v, w for the values of $\mathbf{1}_A, \mathbf{1}_B, \mathbf{1}_C$ at x, and translate each side into a polynomial in u, v, w by Proposition 5.1.3. Simplify both, using $u^2 = u$, $v^2 = v$, $w^2 = w$, which hold because $0^2 = 0$ and $1^2 = 1$. If the two polynomials agree for all values in $\{0, 1\}$, then $\mathbf{1}_L = \mathbf{1}_R$, and $L = R$ because a set is recovered from its indicator. The method replaces a case analysis on memberships by algebra, and it pays most when the case analysis is long.

Example. Symmetric difference is associative

Show that $(A \triangle B) \triangle C = A \triangle (B \triangle C)$ for all $A, B, C \subseteq X$.

Solution. Fix $x \in X$ and let u, v, w be the values of $\mathbf{1}_A, \mathbf{1}_B, \mathbf{1}_C$ at x. By Proposition 5.1.3 (d), $\mathbf{1}_{A\triangle B}(x) = u + v - 2uv$. Applying (d) again, to the sets $A \triangle B$ and C,

$$\begin{aligned}\mathbf{1}_{(A\triangle B)\triangle C}(x) &= (u + v - 2uv) + w - 2(u + v - 2uv)w \\ &= u + v + w - 2uv - 2uw - 2vw + 4uvw.\end{aligned}$$

The final expression does not change when u, v, w are permuted. The right-hand side gives $u + (v + w - 2vw) - 2u(v + w - 2vw)$, which expands to the same expression. So the two sets have the same indicator, and they are equal.

The common value is 1 exactly when an odd number of u, v, w equal 1: with one of them equal to 1 it is 1, with two it is $2 - 2 = 0$, with three $3 - 6 + 4 = 1$. So both sides are the set of points lying in an odd number of A, B, C. An element chase would split into eight cases, one for each pattern of memberships; the indicator computation did all eight at once.

Cantor, re-read. The set $D = \{x \in X : x \notin f(x)\}$ in the proof of Theorem 3.3.2 has indicator $\mathbf{1}_D(x) = 1 - \mathbf{1}_{f(x)}(x)$: it is the flipped diagonal of the proof of Theorem 3.3.1 in Section 3.3, and Section 3.3, after Theorem 3.3.2, already joined the two arguments for $X = \mathbb{N}$. Exercise C3 runs the argument for an arbitrary set, with 0–1 functions first and subsets second.

Quick check. Let $X = \{1, 2, 3, 4\}$, $A = \{1, 2\}$ and $B = \{2, 3\}$. List the values $\mathbf{1}_{A\triangle B}(1), \ldots, \mathbf{1}_{A\triangle B}(4)$, first from the formula $u + v - 2uv$ and then from the definition of $\triangle$.

Solution. The values of $\mathbf{1}_A$ are $(1, 1, 0, 0)$ and those of $\mathbf{1}_B$ are $(0, 1, 1, 0)$. The formula gives $1 + 0 - 0 = 1$, $1 + 1 - 2 = 0$, $0 + 1 - 0 = 1$, 0: the list $(1, 0, 1, 0)$. From the definition, $A \triangle B = \{1\} \cup \{3\} = \{1, 3\}$, whose indicator is the same list.

5.1.5 Exercises

5.1.5.1 A. Check your understanding

Exercise. A1

(a) Let $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$. What is the image of $f|_{[-1,2]}$?

(b) Let a, b, c be distinct and let $g\colon \{1,2\} \to \{a,b\}$ send $1 \mapsto a$, $2 \mapsto b$. Does g have an injective extension to $\{1,2,3\}$ with codomain $\{a,b\}$? With codomain $\{a,b,c\}$?

(c) Let $A \subseteq X$ and $g\colon A \to Y$. Show that g has an extension to X if and only if $A = X$ or $Y \neq \emptyset$.

(d) For $X = \{1,2,3,4\}$, write $\mathbf{1}_{\{1,3\}}$ as the list of its values at $1,2,3,4$, and name the subset of X whose indicator has the values $(0,1,1,0)$.

Solution.

(a) By Proposition 5.1.1 (e), the image is $f([-1,2])$. For $x \in [-1,2]$, $0 \leq x^2 \leq 4$; conversely each $t \in [0,4]$ is $(\sqrt{t})^2$ with $\sqrt{t} \in [0,2]$. So the image is $[0,4]$.

(b) No: a function from a set of three elements to a set of two elements is not injective, by Corollary 2.5.3 (a). Yes: send $3 \mapsto c$; the three values a, b, c are distinct, so the extension is injective.

(c) ($\Leftarrow$) If $A = X$, then g is an extension of itself, since $g|_X = g$. If $Y \neq \emptyset$, choose $y_0 \in Y$ and glue g with the constant function $X \setminus A \to Y$ with value y_0: the pieces A and $X \setminus A$ are disjoint and cover X, so Theorem 5.1.2 gives $f\colon X \to Y$ with $f|_A = g$. ($\Rightarrow$) Suppose $A \neq X$ and $Y = \emptyset$. Since $A \subseteq X$ and $A \neq X$, some $x_0 \in X$ is not in A; so X is non-empty, and by Proposition 1.5.2 (b) there is no function $X \to \emptyset$, let alone an extension of g. By contraposition, an extension forces $A = X$ or $Y \neq \emptyset$.

(d) $(1,0,1,0)$; the subset $\{2,3\}$, the set of points where the value is 1.

5.1.5.2 B. Practice

Exercise. B1: Three pieces

Let $f_1(x) = -x$ on $(-\infty,-1]$, $f_2(x) = x^2$ on $[-1,1]$ and $f_3(x) = x$ on $[1,\infty)$, each with codomain $\mathbb{R}$. Show that they glue to a function $f\colon \mathbb{R} \to \mathbb{R}$. Find $f(\mathbb{R})$ and $f^{-1}(\{\frac{1}{4}\})$, and decide whether f is injective.

Solution. The three intervals cover $\mathbb{R}$. The overlaps are $(-\infty,-1] \cap [-1,1] = \{-1\}$, where $f_1(-1) = 1 = f_2(-1)$; $[-1,1] \cap [1,\infty) = \{1\}$, where $f_2(1) = 1 = f_3(1)$; and $(-\infty,-1] \cap [1,\infty) = \emptyset$. So the pieces agree on overlaps and glue, by Theorem 5.1.2.

Since $\mathbb{R}$ is the union of the three pieces, Theorem 1.7.3 gives $f(\mathbb{R})$ as the union of the images of the pieces, and by Proposition 5.1.1 (e) the image of a piece is the image of the corresponding f_i. These are $f_1((-\infty,-1]) = [1,\infty)$, $f_2([-1,1]) = [0,1]$ and $f_3([1,\infty)) = [1,\infty)$. Hence $f(\mathbb{R}) = [0,\infty)$.

On the first and third pieces every value is ≥ 1, so a solution of $f(x) = \frac{1}{4}$ lies in $[-1,1]$, where it solves $x^2 = \frac{1}{4}$. Hence $f^{-1}(\{\frac{1}{4}\}) = \{-\frac{1}{2}, \frac{1}{2}\}$. Two different points have the same

value, so f is not injective.

Exercise. B2: Injective across pieces

Let $f\colon X \to Y$ and $X = A \cup B$. Prove that f is injective if and only if $f|_A$ and $f|_B$ are injective and $f(A) \cap f(B) = f(A \cap B)$.

Solution. ($\Rightarrow$) The restrictions are injective by Proposition 5.1.1 (d), and $f(A) \cap f(B) = f(A \cap B)$ by Theorem 1.7.4 (b), since f is injective.

($\Leftarrow$) Let $x, x' \in X$ with $f(x) = f(x')$. If both lie in A, then $f|_A(x) = f|_A(x')$ and $x = x'$ since $f|_A$ is injective; likewise if both lie in B. Otherwise, since $X = A \cup B$, one lies in A and the other in B; by symmetry say $x \in A$ and $x' \in B$. Then $y := f(x) = f(x')$ lies in $f(A) \cap f(B) = f(A \cap B)$, so $y = f(z)$ for some $z \in A \cap B$ (Definition 1.7.1). Now $x, z \in A$ with $f|_A(x) = y = f|_A(z)$, so $x = z$; and $x', z \in B$ with $f|_B(x') = f|_B(z)$, so $x' = z$. Hence $x = x'$, and f is injective.

Exercise. B3: By indicators

Let $A, B, C \subseteq X$. Prove by computing with indicators:

(a) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
(b) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

Solution. Fix $x \in X$ and write u, v, w for the values of $\mathbf{1}_A, \mathbf{1}_B, \mathbf{1}_C$ at x. For any $S \subseteq X$, $A \setminus S = A \cap (X \setminus S)$, so Proposition 5.1.3 (a), (b) give $\mathbf{1}_{A \setminus S}(x) = u(1 - \mathbf{1}_S(x))$.

(a) By Proposition 5.1.3 (c), $\mathbf{1}_{B \cup C}(x) = v + w - vw$, so the left side has indicator value $u(1 - v - w + vw) = u(1 - v)(1 - w)$. The right side has, by Proposition 5.1.3 (a), $u(1 - v) \cdot u(1 - w) = u^2(1 - v)(1 - w) = u(1 - v)(1 - w)$, using $u^2 = u$. The indicators agree at every x, so the sets are equal.

(b) By Proposition 5.1.3 (a) and (d), the left side has $u(v + w - 2vw) = uv + uw - 2uvw$. The sets $A \cap B$ and $A \cap C$ have indicator values uv and uw, so by Proposition 5.1.3 (d) the right side has $uv + uw - 2(uv)(uw) = uv + uw - 2u^2vw = uv + uw - 2uvw$. The indicators agree, so the sets are equal.

Exercise. B4: Prove or disprove

Prove each true statement and refute each false one with a counterexample.

(a) If $X = A \cup B$ with $A \cap B = \emptyset$, and $f\colon A \to Y$, $g\colon B \to Y$ are functions, then there is exactly one $h\colon X \to Y$ with $h|_A = f$ and $h|_B = g$.
(b) If $f\colon X \to Y$, $X = A \cup B$, and $f|_A$ and $f|_B$ are injective, then f is injective.
(c) If $f\colon X \to Y$ and $f|_A\colon A \to Y$ is surjective for some $A \subseteq X$, then f is surjective.
(d) The definition $h(x) = x$ for $x \in \mathbb{Q}$, $h(x) = 2x$ for $x \in \mathbb{R} \setminus \mathbb{Q}$ gives a bijection $h\colon \mathbb{R} \to \mathbb{R}$.

(e) Gluing x on $[0,1]$ and $2-x$ on $[1,2]$ gives an injective function $[0,2] \to \mathbb{R}$.

Solution.

(a) True. The family A, B covers X, and the only overlap $A \cap B$ is empty, so agreement holds vacuously. By Theorem 5.1.2 there is exactly one such h.

(b) False. Let $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, $A = [0,\infty)$ and $B = (-\infty, 0]$. Then $X = A \cup B$, and both restrictions are injective (on each piece, $x^2 = x'^2$ with x, x' of the same sign gives $x = x'$), but $f(1) = 1 = f(-1)$. The collision is across the pieces.

(c) True. Let $y \in Y$. Since $f|_A$ is surjective, $y = f|_A(a) = f(a)$ for some $a \in A \subseteq X$. So y is a value of f.

(d) True. The pieces $\mathbb{Q}$ and $\mathbb{R} \setminus \mathbb{Q}$ are disjoint and cover $\mathbb{R}$, so h is a function by Theorem 5.1.2. *Injective.* Inside the pieces: $x = x'$ and $2x = 2x'$ each give $x = x'$. Across the pieces: if $x \in \mathbb{Q}$, $x' \notin \mathbb{Q}$ and $h(x) = h(x')$, then $x = 2x'$, so $x' = x/2 \in \mathbb{Q}$, a contradiction. *Surjective.* A rational y is $h(y)$. An irrational y is $h(y/2)$: here $y/2 \notin \mathbb{Q}$, since otherwise $y = 2 \cdot (y/2) \in \mathbb{Q}$.

(e) False. The pieces agree at the overlap $\{1\}$ (both give 1), so they glue to a function f; but $f(\frac{1}{2}) = \frac{1}{2} = 2 - \frac{3}{2} = f(\frac{3}{2})$.

5.1.5.3 C. Going deeper

Exercise. C1: Counting extensions

Let $A \subseteq X$ and $g\colon A \to Y$, and let E be the set of all extensions of g to X. Show that $f \mapsto f|_{X \setminus A}$ is a bijection from E to $Y^{X \setminus A}$.

Solution. Write $\rho(f) \coloneqq f|_{X \setminus A}$, a function $E \to Y^{X \setminus A}$. For $k \in Y^{X \setminus A}$, the pieces A and $X \setminus A$ are disjoint and cover X, so by Theorem 5.1.2 there is exactly one $\gamma(k)\colon X \to Y$ with $\gamma(k)|_A = g$ and $\gamma(k)|_{X \setminus A} = k$. In particular $\gamma(k) \in E$, so $\gamma\colon Y^{X \setminus A} \to E$.

Round trip on $Y^{X \setminus A}$. $\rho(\gamma(k)) = \gamma(k)|_{X \setminus A} = k$, by the choice of $\gamma(k)$.

Round trip on E. Let $f \in E$. Both f and $\gamma(\rho(f))$ restrict to g on A and to $f|_{X \setminus A}$ on $X \setminus A$. By the uniqueness in Theorem 5.1.2, $\gamma(\rho(f)) = f$.

So γ is a two-sided inverse of ρ, and ρ is a bijection by Theorem 1.6.4. In words: an extension of g is the same thing as an arbitrary choice of values off A. For finite sets this counts the extensions: if $X \setminus A$ has m elements and Y has n, there are as many extensions as functions from an m-element set to an n-element set.

Marking scheme. (10 points) - 3: defines γ by gluing, checking the pieces cover and are disjoint. - 2: $\rho(\gamma(k)) = k$. - 3: $\gamma(\rho(f)) = f$ by uniqueness in Theorem 5.1.2. - 2: concludes that ρ is a bijection.

Exercise. C2: Find the error

Here is a proposed proof of the existence part of Theorem 5.1.2. "Given $x \in X$, pick i with

$x \in A_i$, and set $f(x) \coloneqq f_i(x)$. Then $f|_{A_i} = f_i$ for every $i \in I$." Which hypothesis of the theorem is never used? Where does the argument fail, and which check is missing? Is the conclusion true?

Solution. The conclusion is true: it is Theorem 5.1.2. The argument does not prove it.

Agreement on overlaps is never used. The failure is in the definition of f: the rule reads a chosen index i from the set $\{i \in I : x \in A_i\}$, and it defines a function only if the value $f_i(x)$ does not depend on which such i is picked. That is the well-definedness check of Example (Method: checking that a definition on classes is well defined), with "an index i with $x \in A_i$" in the role of a representative; it is exactly agreement on overlaps. Without it, the second sentence fails too: at a point $x \in A_i \cap A_j$ where i was picked, $f|_{A_j}(x) = f_i(x)$, which need not equal $f_j(x)$. Example (Piecewise definitions are gluings) (b) at $x = 0$ is a case: picking the first piece gives $f(0) = 0$, and then $f|_{(-\infty,0]}$ is not $x \mapsto x + 1$, which has the value 1 at 0.

Marking scheme. (10 points) - 3: names agreement on overlaps as the unused hypothesis. - 4: locates the failure either in the definition of f (the value depends on the choice of i, so a well-definedness check is missing) or in the claim $f|_{A_j} = f_j$ at a point of $A_i \cap A_j$ where another index was picked, and says that agreement on overlaps is what is missing. - 3: gives a concrete case where the choice matters and $f|_{A_j} = f_j$ fails. Fatal errors (0 for the step): claiming the conclusion is false; locating the error in the cover (every x does lie in some A_i).

Exercise. C3: Cantor through indicators

Let X be a set and $g\colon X \to \{0,1\}^X$ a function. Define $d\colon X \to \{0,1\}$ by $d(x) \coloneqq 1 - g(x)(x)$.

(a) Prove that d is not a value of g.

(b) Deduce Theorem 3.3.2. *Hint: for $f\colon X \to \mathcal{P}(X)$, use $g(x) \coloneqq \mathbf{1}_{f(x)}$.*

Solution.

(a) Since $g(x)(x) \in \{0,1\}$, also $d(x) \in \{0,1\}$, so $d \in \{0,1\}^X$. Suppose $d = g(a)$ for some $a \in X$. Then $d(a) = g(a)(a)$, and by the definition of d, $d(a) = 1 - g(a)(a)$. Hence $2g(a)(a) = 1$, which is impossible for $g(a)(a) \in \{0,1\}$. So d is not a value of g.

(b) Let $f\colon X \to \mathcal{P}(X)$ be a function, and put $g(x) \coloneqq \mathbf{1}_{f(x)} \in \{0,1\}^X$. Let $D \coloneqq \{x \in X : d(x) = 1\}$. Since d takes only the values 0 and 1, $\mathbf{1}_D = d$. If $D = f(a)$ for some $a \in X$, then $g(a) = \mathbf{1}_{f(a)} = \mathbf{1}_D = d$, against (a). So D is not a value of f, and f is not surjective. Unwinding, $d(x) = 1$ exactly when $\mathbf{1}_{f(x)}(x) = 0$, so $D = \{x \in X : x \notin f(x)\}$, the set of the proof in Section 3.3.

Marking scheme. (10 points) - 1: checks that $d \in \{0,1\}^X$. - 4: assumes $d = g(a)$ and reaches the contradiction $2g(a)(a) = 1$. - 4: shows $\mathbf{1}_D = d$ and transfers the argument to f via $g(x) = \mathbf{1}_{f(x)}$. - 1: concludes that f is not surjective.

Section 3.6's Corollary 3.6.5 went the other way, from Cantor's theorem to 0–1 functions; here the argument about 0–1 functions comes first, and the statement about subsets follows from it.

5.2 Fibers and the Canonical Factorization

Section 4.2 cut a set into classes, and Section 5.1 cut functions down and glued them together. This section joins the two threads. Every function sorts its domain into piles by value, the fibers, and we prove that the piles carry all the information the function has, apart from the names of the values: every function is a quotient map, then a bijection, then an inclusion. Read in reverse, the same argument says exactly which functions on a set pass to a function on a quotient set, and gives a method for defining one.

5.2.1 Functions on the clock

Section 4.2 built the clock $\mathbb{Z}/12$, whose elements are the twelve hours $[0], [1], \ldots, [11]$. Some questions about an integer are really questions about its hour. "Is a even?" is one: 14 and 2 name the same hour, and both are even; 13 and 1 name the same hour, and both are odd. In general, let $g\colon \mathbb{Z} \to Y$ be a function with

$$g(a) = g(a') \quad \text{whenever } 12 \mid a - a',$$

so that g takes one value on each class modulo 12. Then g "is" a function of the hour: to compute it at an hour, pick any integer naming that hour and apply g. The condition is stated for all pairs in one class at once. A condition such as $g(a+12) = g(a)$ for every a says the same thing in the end, but getting from it to $g(a+12k) = g(a)$ for every $k \in \mathbb{Z}$ takes an induction in each direction.

Other functions are not functions of the hour. "Is a positive?" gives different answers at 2 and at -10, which name the same hour, so no function on $\mathbb{Z}/12$ can answer it.

There is a second way into the same idea, from the side of an arbitrary function. A function $f\colon X \to Y$ sorts its domain: put two points in one pile when f gives them the same value. Section 4.2 met these piles as the classes of the relation $\sim_f$ (Example (The fibers of a function)). So every function produces a quotient set of its domain.

Two questions organize the section.

- **(Q1)** Given an equivalence relation $\sim$ on X, when does a function on X pass to a function on $X/\!\sim$, and is the function it passes to unique?
- **(Q2)** What does a function look like once its domain has been sorted by value?

We answer (Q2) first, because its answer contains the answer to (Q1).

5.2.2 The fibers of a function

Recall the relation of Example (The fibers of a function). For $f\colon X \to Y$ and $x, x' \in X$, $x \sim_f x'$ means $f(x) = f(x')$. It is an equivalence relation on X, and the class of $a \in X$ is the **fiber** of f over $f(a)$,

$$[a] = \{x \in X : f(x) = f(a)\} = f^{-1}(\{f(a)\}),$$

a preimage in the sense of Definition 1.7.2. A fiber over a point of Y that f never takes is empty, and so is not a class.

The fibers of a function are the piles it sorts its domain into, one pile for each value it takes.

Proposition 5.2.1. The Fibers of a Function

Let $f\colon X \to Y$ be a function.

(a) The fibers $f^{-1}(\{y\})$ over the points $y \in f(X)$ are exactly the classes of $\sim_f$, and they form a partition of X.

(b) The rule $y \mapsto f^{-1}(\{y\})$ is a bijection $f(X) \to X/\!\sim_f$. Hence $|f(X)| = |X/\!\sim_f|$.

Idea. Part (a) is already proved: Example (The fibers of a function) identified the classes with the fibers, and Theorem 4.2.1 says the classes partition X. For (b), a fiber over a value is a class, so the rule lands in $X/\!\sim_f$; every class is the fiber over the value at its representative, which is surjectivity; and two different values have different fibers, because a point of the first fiber is not in the second.

Proof. *(a)* Let $y \in f(X)$, say $y = f(a)$ with $a \in X$ (Definition 1.7.1). Then $f^{-1}(\{y\}) = f^{-1}(\{f(a)\}) = [a]$, by the computation in Example (The fibers of a function); so each such fiber is a class. Conversely, each class is $[a]$ for some $a \in X$, and $[a] = f^{-1}(\{f(a)\})$ with $f(a) \in f(X)$. So the fibers over the points of $f(X)$ are the elements of $X/\!\sim_f$, and these form a partition of X by Theorem 4.2.1 (d).

(b) By (a), each $y \in f(X)$ is sent to an element of $X/\!\sim_f$, and to only one, so the rule is a function $\Phi\colon f(X) \to X/\!\sim_f$ (Definition 1.5.1). It is surjective: an element of $X/\!\sim_f$ is $[a]$ for some $a \in X$, and $[a] = \Phi(f(a))$ by (a). It is injective: let $y, y' \in f(X)$ with $y \neq y'$, and write $y = f(a)$ with $a \in X$. Then $a \in f^{-1}(\{y\})$, while $a \notin f^{-1}(\{y'\})$ because $f(a) = y \neq y'$. So $\Phi(y) \neq \Phi(y')$, and different values have different fibers. Hence Φ is a bijection (Definition 1.5.5), and $|f(X)| = |X/\!\sim_f|$ by Definition 2.5.1.

■

So a function takes exactly as many values as it has fibers, in the sense of equinumerosity: the values and the piles can be paired off. The partition remembers which points share a value, and forgets only what the values are called.

Quick check. List the classes of $\sim_f$ for $f(n) = n^2 - 2n$ on $\{-1, 0, 1, 2, 3\}$, and match each class with its value.

Solution. The values are $f(-1) = 3$, $f(0) = 0$, $f(1) = -1$, $f(2) = 0$, $f(3) = 3$. So the classes are $\{-1, 3\}$ (value 3), $\{0, 2\}$ (value 0) and $\{1\}$ (value -1): three classes for the three values in $f(X) = \{-1, 0, 3\}$.

The proposition explains a computation of Section 4.2. In Example (Same size, revisited), the subsets of $\{1, 2, 3\}$ were sorted by "same number of elements". That relation is $\sim_f$ for the function $f\colon \mathcal{P}(\{1, 2, 3\}) \to \{0, 1, 2, 3\}$ sending each subset to its number of elements, a function by Proposition 2.5.6 (every subset has some number of elements, at most 3) and Corollary 2.5.4 (only one). Its four fibers are $\{\emptyset\}$, the three singletons, the three pairs, and $\{\{1, 2, 3\}\}$, and

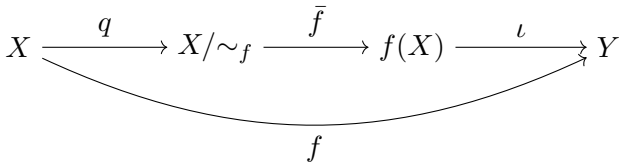
its image is all of $\{0, 1, 2, 3\}$. Part (c) of that example, the well-defined map from classes to numbers, is the bijection of (b) read backwards.

Quick check. List the fibers of $f\colon \{1, \ldots, 6\} \to \{0, 1, 2\}$, where $f(n)$ is the remainder of n on division by 3.

Solution. $f^{-1}(\{0\}) = \{3, 6\}$, $f^{-1}(\{1\}) = \{1, 4\}$, $f^{-1}(\{2\}) = \{2, 5\}$. Three fibers, three values; every value is taken, so $f(X)$ is the whole codomain.

5.2.3 Every function factors

Now (Q2). The quotient map $q\colon X \to X/\!\sim_f$, $q(x) = [x]$ (Definition 4.2.4), sends each point to its fiber. The bijection of Proposition 5.2.1 (b) goes from values to fibers; turn it around, and it sends the fiber $[x]$ to the value $f(x)$. Finally, a value of f lies in the image $f(X)$, and the **inclusion map** $\iota\colon f(X) \to Y$, $\iota(y) = y$ (Definition 5.1.1), puts it back into the codomain. Composed, the three maps take x to $[x]$, to $f(x)$, to $f(x)$. That is f.



Theorem 5.2.2. Canonical Factorization

Let $f\colon X \to Y$ be a function, let $q\colon X \to X/\!\sim_f$ be the quotient map, and let $\iota\colon f(X) \to Y$ be the inclusion map. There is **exactly one** function $\bar{f}\colon X/\!\sim_f \to f(X)$ with

$$f = \iota \circ \bar{f} \circ q.$$

It is given by $\bar{f}([x]) = f(x)$, and it is a **bijection**.

Idea (Scratch work). The only candidate is forced. If $\iota(\bar{f}(q(x))) = f(x)$, then $\bar{f}([x]) = f(x)$, since ι changes no value. So uniqueness costs nothing, and the work is to show that the forced rule is a function and a bijection. The rule $[x] \mapsto f(x)$ reads a representative, so the first check is well-definedness, by the method of Example (Method: checking that a definition on classes is well defined). The twist is in the table's third row: injectivity is the well-definedness line read backwards.

Givens	Goal
$[x] = [x'] \iff x \sim_f x'$ (Theorem 4.2.1 (b)), and $x \sim_f x' \iff f(x) = f(x')$	$\bar{f}$ a function, bijective, $f = \iota \circ \bar{f} \circ q$, unique
$[x] = [x']$	$f(x) = f(x')$: one class, one value, (Fn2), well defined
$f(x) = f(x')$	$[x] = [x']$: injective, the same equivalence read right to left

$y \in f(X)$, so $y = f(a)$ with $a \in X$ $\qquad$ $y = \bar{f}([a])$: surjective

Uniqueness: q is onto, so every class is $[x]$ for some x; a second $\bar{f}'$ with $\iota \circ \bar{f}' \circ q = f$ has $\bar{f}'([x]) = f(x)$ at every class. The proof writes this forwards.

Proof. A function. Every element of $X/\!\sim_f$ is $[x]$ for some $x \in X$, and $f(x) \in f(X)$ by Definition 1.7.1; this gives (Fn1). Let $[x] = [x']$. By Theorem 4.2.1 (b), $x \sim_f x'$, that is, $f(x) = f(x')$. So all representatives of one class give one value, which is (Fn2), and $\bar{f}([x]) \coloneqq f(x)$ defines a function $\bar{f}\colon X/\!\sim_f \to f(X)$ (Definition 1.5.1).

Injective. Let $\bar{f}([x]) = \bar{f}([x'])$, that is, $f(x) = f(x')$. Then $x \sim_f x'$, and $[x] = [x']$ by Theorem 4.2.1 (b).

Surjective. Let $y \in f(X)$. By Definition 1.7.1 there is $a \in X$ with $f(a) = y$, and then $\bar{f}([a]) = f(a) = y$.

The factorization. Both f and $\iota \circ \bar{f} \circ q$ have domain X and codomain Y, and for every $x \in X$,

$$(\iota \circ \bar{f} \circ q)(x) = \iota(\bar{f}([x])) = \iota(f(x)) = f(x),$$

by Definition 1.5.2. Hence $f = \iota \circ \bar{f} \circ q$ by Proposition 1.5.1.

Uniqueness. Let $\bar{f}'\colon X/\!\sim_f \to f(X)$ satisfy $f = \iota \circ \bar{f}' \circ q$. Every element of $X/\!\sim_f$ is $[x] = q(x)$ for some $x \in X$, and

$$\bar{f}'([x]) = \iota(\bar{f}'(q(x))) = f(x) = \bar{f}([x]),$$

where the first equality holds because ι sends each point to itself. The two functions have the same domain and codomain, so $\bar{f}' = \bar{f}$ by Proposition 1.5.1. This proves the theorem. ∎

Read the factorization from left to right: every function is a **surjection** (q, onto by Definition 4.2.4), followed by a **bijection** ($\bar{f}$), followed by an **injection** (ι, which sends each point to itself, so different points stay different). All the identifying is done by q, all the renaming by $\bar{f}$, and all the enlarging of the target by ι. The two properties of Section 1.5 sit at the two ends. The function f is injective exactly when q is: if f is injective and $q(x) = q(x')$, then $x \sim_f x'$ by Theorem 4.2.1 (b), so $f(x) = f(x')$ and $x = x'$; if q is injective and $f(x) = f(x')$, then $x \sim_f x'$, so $q(x) = q(x')$ by Theorem 4.2.1 (b), and $x = x'$. And f is surjective exactly when $f(X) = Y$, that is, when $\iota = \mathrm{id}_Y$.

Warning. The middle map is a bijection onto the **image**, not onto the codomain. With target Y, the rule $[x] \mapsto f(x)$ is still a well-defined injection, but it is surjective only when f is. For $f(x) = x^2$ on $\mathbb{R}$, the rule $[x] \mapsto x^2$ maps the classes $\{-x, x\}$ onto $[0, \infty)$ and reaches no negative number of the codomain $\mathbb{R}$.

The factorization also explains a failure from Section 1.5.

Example. Fractions as classes

Let $f\colon \mathbb{Z} \times \mathbb{Z}_{>0} \to \mathbb{Q}$, $f(a,b) \coloneqq a/b$. Describe $\sim_f$, the three maps of Theorem 5.2.2, and decide whether "send a/b to its numerator a" passes through q.

Solution. The relation. $(a,b) \sim_f (c,d)$ means $a/b = c/d$, and since $b, d \neq 0$ this holds exactly when $ad = bc$, by the arithmetic of fractions. It is the relation of Exercise B1 in Section 4.2 (Exercise (B1: Fractions as classes)), now seen as the fiber relation of a function; that it is an equivalence relation is also immediate from Example (The fibers of a function). The class of $(1,2)$ is the fiber over $\frac{1}{2}$: the pairs $(1,2), (2,4), (3,6), \ldots$, all the ways of writing one half as a fraction.

The three maps. The quotient map q sends a pair to its class, "the fraction a/b up to rewriting". The map $\bar{f}$ sends a class to the rational number its pairs all name. And f is onto $\mathbb{Q}$, since every rational number is a/b for some $a \in \mathbb{Z}$ and $b \in \mathbb{Z}_{>0}$; so $f(X) = \mathbb{Q}$ and $\iota = \mathrm{id}_{\mathbb{Q}}$. By Theorem 5.2.2, $\bar{f}$ is a bijection from the set of classes onto $\mathbb{Q}$: a rational number "is" a class of fractions, and nothing is lost by identifying the two.

The numerator. Let $p(a,b) \coloneqq a$. If p were $g \circ q$ for some function g on the classes, then $(a,b) \sim_f (c,d)$ would force $p(a,b) = g([(a,b)]) = g([(c,d)]) = p(c,d)$. But $(1,2) \sim_f (2,4)$, since $1 \cdot 4 = 2 \cdot 2$, while $p(1,2) = 1 \neq 2 = p(2,4)$. So p does not pass through q, and no function on the classes, hence none on $\mathbb{Q}$, sends each fraction to its numerator. This is the failure of Example (Relations that are not functions) (b), located: the numerator is a function of the pair, not of its fiber.

Quick check. In Example (Fractions as classes), which of q, $\bar{f}$, ι are injective, and which are surjective?

Solution. q is surjective, and not injective, since $q(1,2) = q(2,4)$. $\bar{f}$ is both, by Theorem 5.2.2. ι is injective, as every inclusion is; here it is $\mathrm{id}_{\mathbb{Q}}$, so it is also surjective.

5.2.4 Functions out of a quotient

Now (Q1). The canonical factorization built a function on the classes of $\sim_f$ from f itself. Nothing in its first step needed the relation to come from f: what made $[x] \mapsto f(x)$ a function was only that equivalent points have equal values. So the same argument works for any equivalence relation, as long as the function is constant on its classes.

Theorem 5.2.3. Functions out of a Quotient

Let $\sim$ be an equivalence relation on a set X, let $q\colon X \to X/\!\sim$ be its quotient map, and let $g\colon X \to Z$ be a function.

(a) There is a function $\bar{g}\colon X/\!\sim \to Z$ with $\bar{g} \circ q = g$ **if and only if** g is **constant on classes**: for all $x, x' \in X$, if $x \sim x'$, then $g(x) = g(x')$. In that case $\bar{g}$ is unique, and $\bar{g}([x]) = g(x)$.

(b) Suppose g is constant on classes. Then $\bar{g}$ is injective **if and only if**, for all $x, x' \in X$, $g(x) = g(x')$ implies $x \sim x'$.

(c) Suppose g is constant on classes. Then $\bar{g}$ is surjective **if and only if** g is surjective.

Idea. This is the argument of Theorem 5.2.2 with $\sim$ in place of $\sim_f$ (Example (Method: checking that a definition on classes is well defined) for the existence, q onto for the uniqueness). The new part is the forward direction of (a): if $\bar{g}$ exists, equivalent points have one class, so $g = \bar{g} \circ q$ gives them one value. For (b) and (c), translate statements about classes into statements about representatives with Theorem 4.2.1 (b).

Proof. *(a)* ($\Rightarrow$) Suppose $\bar{g} \circ q = g$, and let $x \sim x'$. Then $q(x) = [x] = [x'] = q(x')$ by Theorem 4.2.1 (b), so

$$g(x) = \bar{g}(q(x)) = \bar{g}(q(x')) = g(x').$$

($\Leftarrow$) Suppose g is constant on classes. Every element of $X/\!\sim$ is $[x]$ for some $x \in X$, with $g(x) \in Z$, which is (Fn1). If $[x] = [x']$, then $x \sim x'$ by Theorem 4.2.1 (b), so $g(x) = g(x')$, which is (Fn2). Hence $\bar{g}([x]) \coloneqq g(x)$ defines a function $\bar{g}\colon X/\!\sim \to Z$ (Definition 1.5.1). Both $\bar{g} \circ q$ and g have domain X and codomain Z, and $(\bar{g} \circ q)(x) = \bar{g}([x]) = g(x)$ for every $x \in X$, so $\bar{g} \circ q = g$ by Proposition 1.5.1.

Uniqueness. If $h\colon X/\!\sim \to Z$ also satisfies $h \circ q = g$, then each element of $X/\!\sim$ is $q(x)$ for some $x \in X$, since q is onto (Definition 4.2.4), and $h(q(x)) = g(x) = \bar{g}(q(x))$. So $h = \bar{g}$ by Proposition 1.5.1.

(b) By Definition 1.5.3, $\bar{g}$ is injective when $\bar{g}(C) = \bar{g}(D)$ implies $C = D$ for all $C, D \in X/\!\sim$. Every class is $[x]$ for some $x \in X$, and $\bar{g}([x]) = g(x)$; so the condition reads: for all $x, x' \in X$, $g(x) = g(x')$ implies $[x] = [x']$. By Theorem 4.2.1 (b), $[x] = [x']$ is $x \sim x'$.

(c) By Definition 1.5.4, $\bar{g}$ is surjective when every $z \in Z$ is $\bar{g}(C)$ for some class C. Since every class is $[x]$ for some $x \in X$, and $\bar{g}([x]) = g(x)$, this says that every $z \in Z$ is $g(x)$ for some $x \in X$: that g is surjective.

■

The canonical factorization is the case where $\sim$ is $\sim_f$, with g the function $X \to f(X)$, $x \mapsto f(x)$. That g is constant on the classes of $\sim_f$ by the definition of $\sim_f$; the converse condition of (b) holds for the same reason, so $\bar{g}$ is injective; and g is onto $f(X)$ by Definition 1.7.1, so $\bar{g}$ is surjective by (c). The map $\bar{g}$ is $\bar{f}$.

Warning. "Constant on classes" runs from equivalence to equal values: $x \sim x' \Rightarrow g(x) = g(x')$. Its converse, $g(x) = g(x') \Rightarrow x \sim x'$, is the injectivity condition of (b), and checking it instead proves nothing about existence. For congruence modulo 12 and $g(a) = [a]_{24}$, the converse holds, since $24 \mid a - a'$ gives $12 \mid a - a'$; but $0 \equiv 12 \pmod{12}$ while $[0]_{24} \neq [12]_{24}$, so "$[a]_{12} \mapsto [a]_{24}$" is not a function.

The theorem turns the check of Example (Method: checking that a definition on classes is well defined) into a complete method: it says what the check buys, and how to read off injectivity

and surjectivity afterwards.

Example. Method: define a function on a quotient

Template. (1) Write the function g on X that the rule computes from a representative. (2) Check that g is constant on classes (Example (Method: checking that a definition on classes is well defined)). (3) Conclude by Theorem 5.2.3: $\bar{g}$ exists, is unique, and $\bar{g} \circ q = g$. (4) Read injectivity of $\bar{g}$ as "equal values force equivalence", and surjectivity of $\bar{g}$ as surjectivity of g.

When to use it. Maps out of $\mathbb{Z}/n$, out of classes of fractions, out of any "the same in some respect".

The usual failure. Proving (4)'s converse condition instead of (2); a g not defined on all of X; running the check for a map **into** a quotient, which needs none: compose with q.

Here is the method three times, twice on the clock and once on $\mathbb{Z}/2$. As in Section 4.2, the subscript in $[a]_n$ names the modulus: it is the class of a in $\mathbb{Z}/n$.

Example. Maps out of the clock

(a) Let $r\colon \mathbb{Z} \to \{0,1\}$ send each integer to its remainder on division by 2. Show that "$[a]_{12} \mapsto r(a)$" is a function $\mathbb{Z}/12 \to \{0,1\}$, and decide whether it is injective and whether it is surjective.

(b) Do the same for "$[a]_2 \mapsto r(a)$", from $\mathbb{Z}/2$.

(c) Show that "$[a]_{12} \mapsto [a+1]_{12}$" is a bijection $t\colon \mathbb{Z}/12 \to \mathbb{Z}/12$.

Solution. The remainder $r(a)$ is well defined by the uniqueness in Theorem 2.2.3. We use the remainder test of Section 4.2, after Proposition 4.2.4: $a \equiv a' \pmod{n}$ if and only if a and a' leave the same remainder on division by n.

(a) *Step (1).* The rule computes $r(a)$ from the representative a, so $g = r$. *Step (2).* Let $a \equiv a' \pmod{12}$, so $a - a' = 12k$ with $k \in \mathbb{Z}$. Then $a - a' = 2(6k)$ with $6k \in \mathbb{Z}$, so $a \equiv a' \pmod{2}$, and $r(a) = r(a')$ by the remainder test. *Step (3).* By Theorem 5.2.3 (a), $\bar{r}([a]_{12}) \coloneqq r(a)$ is a function $\mathbb{Z}/12 \to \{0,1\}$: "is the hour even?" is a question about the hour. *Step (4).* It is surjective by Theorem 5.2.3 (c), since $r(0) = 0$ and $r(1) = 1$. It is not injective, by part (b) of the theorem: $r(0) = r(2)$, but $0 \not\equiv 2 \pmod{12}$, since $2 - 0 = 2$ lies strictly between 0 and 12 and so is not a multiple of 12 (Proposition 2.1.2 (c)). So $\bar{r}([0]_{12}) = \bar{r}([2]_{12})$ with $[0]_{12} \neq [2]_{12}$.

(b) *Step (2).* If $a \equiv a' \pmod{2}$, then $r(a) = r(a')$ by the remainder test. *Step (4).* Conversely, $r(a) = r(a')$ gives $a \equiv a' \pmod{2}$, again by the remainder test, so the induced map $\mathbb{Z}/2 \to \{0,1\}$ is injective by Theorem 5.2.3 (b), and surjective by part (c), as in (a). It is a bijection: the two classes of $\mathbb{Z}/2$ are the even and the odd integers, matched with the remainders 0 and 1.

(c) *Steps (1)–(3).* Here $g(a) \coloneqq [a+1]_{12}$, a function $\mathbb{Z} \to \mathbb{Z}/12$. If $a - a' = 12k$, then $(a+1) - (a'+1) = a - a' = 12k$, so $[a+1]_{12} = [a'+1]_{12}$ (Theorem 4.2.1 (b)). So $t([a]_{12}) \coloneqq [a+1]_{12}$ is a function $\mathbb{Z}/12 \to \mathbb{Z}/12$, the **tick** of the clock. *A bijection.* In the same way, $(a-1) - (a'-1) = a - a'$, so $s([a]_{12}) \coloneqq [a-1]_{12}$ is a function $\mathbb{Z}/12 \to \mathbb{Z}/12$. For every $a \in \mathbb{Z}$, $s(t([a])) = s([a+1]) = [a]$ and $t(s([a])) = t([a-1]) = [a]$; so $s \circ t$

and $t \circ s$ are the identity of $\mathbb{Z}/12$ (Proposition 1.5.1), and t is a bijection with inverse s (Theorem 1.6.4).

In (c) the codomain is itself a quotient set, and the check compared outputs as classes. In (a) and (b) the codomain is $\{0, 1\}$, and outputs were compared as numbers. Step (2) of the method is the same check in both cases; only the meaning of "equal outputs" changes with the codomain.

Second reading · *Surjections are quotient maps, and choosing representatives*

If $f\colon X \to Y$ is onto, then $\iota = \mathrm{id}_Y$, and Theorem 5.2.2 reads $f = \bar{f} \circ q$ with $\bar{f}\colon X/\!\sim_f \to Y$ a bijection. So every surjection is a quotient map up to renaming the classes: to give an onto map out of X is to give an equivalence relation on X and names for its classes. In the other direction, q itself is onto, so it has a right inverse $c\colon X/\!\sim \to X$ by Theorem 3.2.2, which uses Axiom 3.2.1. Then $q(c(C)) = C$, that is, $c(C) \in C$ for every class C: a right inverse of a quotient map is a choice of one representative from each class. For $\mathbb{Z}/n$ no axiom is needed, since the remainder picks one, $c([a]) :=$ the remainder of a on division by n (Proposition 4.2.4).

Quick check. Is the rule $[a]_{10} \mapsto [a]_5$ a well-defined function $\mathbb{Z}/10 \to \mathbb{Z}/5$? Is it injective? Is it surjective?

Solution. Take $g\colon \mathbb{Z} \to \mathbb{Z}/5$, $g(a) = [a]_5$. *Well defined:* yes. If $a - a' = 10k$ with $k \in \mathbb{Z}$, then $a - a' = 5(2k)$, so $g(a) = g(a')$ (this was Exercise B3 (c) of Section 4.2). *Injective:* no. $g(0) = [0]_5 = [5]_5 = g(5)$, but $0 \not\equiv 5 \pmod{10}$, since $0 < 5 < 10$; by Theorem 5.2.3 (b), the classes $[0]_{10} \neq [5]_{10}$ have one image. *Surjective:* yes, by (c), because g is the quotient map of congruence modulo 5, which is onto.

Remark (Looking ahead). Later in this chapter, in the section on permutations and iteration, the tick t of Example (Maps out of the clock) is applied again and again; its iterates carry each hour once round the whole clock.

5.2.5 Exercises

5.2.5.1 A. Check your understanding

Exercise. A1

(a) For $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 - 1$, find the fibers over 3, over -1 and over -2. Which of them are classes of $\sim_f$?

(b) Let $f\colon \{a, b, c, d\} \to \{1, 2, 3\}$ send a and c to 1, and b and d to 3. Write down $X/\!\sim_f$, $f(X)$, $\bar{f}$ and ι of Theorem 5.2.2.

(c) Which of the functions $a \mapsto [a]_2$, $a \mapsto [a]_8$ and $a \mapsto [a^2]_8$, from $\mathbb{Z}$, are constant on the

classes of congruence modulo 4?

Solution.

(a) $x^2 - 1 = 3$ means $x^2 = 4$, so the fiber over 3 is $\{-2, 2\}$. $x^2 - 1 = -1$ means $x^2 = 0$, so the fiber over -1 is $\{0\}$. $x^2 - 1 = -2$ would need $x^2 = -1$, and no real square is negative, so the fiber over -2 is $\emptyset$. The first two are classes, since $3 = f(2)$ and $-1 = f(0)$ lie in $f(\mathbb{R})$; the empty fiber is not a class, because $-2 \notin f(\mathbb{R})$ and every class is non-empty (Theorem 4.2.1 (a)).

(b) The fibers over the values are $\{a, c\}$ and $\{b, d\}$, so $X/\!\sim_f = \{\{a, c\}, \{b, d\}\}$. The image is $f(X) = \{1, 3\}$. The bijection is $\bar{f}(\{a, c\}) = 1$, $\bar{f}(\{b, d\}) = 3$, and $\iota\colon \{1, 3\} \to \{1, 2, 3\}$ sends $1 \mapsto 1$ and $3 \mapsto 3$. The value 2 is in the codomain but outside the image, which is why ι is not surjective.

(c) Let $a' = a+4k$ with $k \in \mathbb{Z}$, the general element of the class of a modulo 4. $a \mapsto [a]_2$: yes, since $a' - a = 4k = 2(2k)$. $a \mapsto [a]_8$: no. $0 \equiv 4 \pmod 4$, but $[0]_8 \neq [4]_8$, since $4 - 0 = 4$ lies strictly between 0 and 8. $a \mapsto [a^2]_8$: yes, since $a'^2 - a^2 = 8ak + 16k^2 = 8(ak + 2k^2)$, with $ak + 2k^2 \in \mathbb{Z}$.

5.2.5.2 B. Practice

Exercise. B1: The absolute value, factored

Let $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = |x|$. Describe the classes of $\sim_f$, the image $f(\mathbb{R})$ and the bijection $\bar{f}$. Then show that $[x] \mapsto x^2$ is a well-defined injective function $\mathbb{R}/\!\sim_f \to \mathbb{R}$.

Solution. The pieces. $|x| = |x'|$ holds exactly when $x' = x$ or $x' = -x$, so the class of x is $\{-x, x\}$, which is $\{0\}$ for $x = 0$. Every value $|x|$ is ≥ 0, and every $t \geq 0$ is $|t|$, so $f(\mathbb{R}) = [0, \infty)$. The bijection of Theorem 5.2.2 is $\bar{f}(\{-x, x\}) = |x|$, from the set of classes onto $[0, \infty)$.

Well defined. Let $g(x) := x^2$. Since $x^2 = |x|^2$, $x \sim_f x'$ gives $x^2 = |x|^2 = |x'|^2 = x'^2$. So g is constant on classes, and $[x] \mapsto x^2$ is a function by Theorem 5.2.3 (a).

Injective. Let $x^2 = x'^2$. Then $|x|^2 = |x'|^2$ with $|x|, |x'| \geq 0$, and Logic and Proof, Theorem 2.4.5, applied in both orders, gives $|x| \leq |x'|$ and $|x'| \leq |x|$. So $|x| = |x'|$, that is, $x \sim_f x'$. By Theorem 5.2.3 (b), the induced function is injective. (It is not surjective onto $\mathbb{R}$: no class goes to -1.)

Exercise. B2: Same fibers

Let $f\colon X \to Y$ and $g\colon X \to Z$ be functions. Prove that $\sim_f = \sim_g$ if and only if there is a bijection $h\colon f(X) \to g(X)$ with $g(x) = h(f(x))$ for every $x \in X$.

Solution. ($\Leftarrow$) Let h be such a bijection, and let $x, x' \in X$. If $f(x) = f(x')$, then $g(x) = h(f(x)) = h(f(x')) = g(x')$. If $g(x) = g(x')$, then $h(f(x)) = h(f(x'))$, and $f(x) = f(x')$ because h is injective. So $x \sim_f x' \iff x \sim_g x'$: the two relations contain the same pairs, and are equal (Definition 1.2.1).

($\Rightarrow$) Suppose $\sim_f = \sim_g$; write $\sim$ for both, so the two quotient sets are one set $X/\!\sim$. By Theorem 5.2.2 there are bijections $\bar{f}\colon X/\!\sim \to f(X)$ and $\bar{g}\colon X/\!\sim \to g(X)$ with $\bar{f}([x]) = f(x)$ and $\bar{g}([x]) = g(x)$. The inverse $\bar{f}^{-1}\colon f(X) \to X/\!\sim$ is a bijection (Definition 1.6.2, Theorem 1.6.4), so $h := \bar{g} \circ \bar{f}^{-1}\colon f(X) \to g(X)$ is a bijection by Theorem 1.5.4 (c). For every $x \in X$, $\bar{f}^{-1}(f(x)) = [x]$, since $\bar{f}([x]) = f(x)$; so $h(f(x)) = \bar{g}([x]) = g(x)$.

Exercise. B3: A coarser relation

Let $\sim$ and $\approx$ be equivalence relations on a set X such that $x \sim x'$ implies $x \approx x'$. Show that $[x]_\sim \mapsto [x]_\approx$ is a well-defined surjection $X/\!\sim \to X/\!\approx$. Give the instance $\mathbb{Z}/12 \to \mathbb{Z}/4$.

Solution. Apply Theorem 5.2.3 to the relation $\sim$ and to $g := q_\approx\colon X \to X/\!\approx$, the quotient map of $\approx$. It is constant on $\sim$-classes: if $x \sim x'$, then $x \approx x'$ by hypothesis, so $[x]_\approx = [x']_\approx$ by Theorem 4.2.1 (b). By part (a), $[x]_\sim \mapsto [x]_\approx$ is a function, and by part (c) it is surjective, since $q_\approx$ is onto (Definition 4.2.4).

For $\mathbb{Z}/12 \to \mathbb{Z}/4$, the hypothesis is: $12 \mid a - a'$ implies $4 \mid a - a'$. This holds by Proposition 1.1.1, since $4 \mid 12$ ($12 = 3 \cdot 4$). So $[a]_{12} \mapsto [a]_4$ is a well-defined surjection: each hour is sent to its position within a block of four hours (0, 4 and 8 go to $[0]_4$).

Exercise. B4: Prove or disprove

Prove or disprove each statement.

(a) If $g\colon X \to Z$ is constant on the classes of an equivalence relation $\sim$ on X and g is surjective, then $\bar{g}\colon X/\!\sim \to Z$ is a bijection.

(b) For every function $f\colon X \to Y$, $|f(X)| = |X/\!\sim_f|$.

(c) If $f\colon X \to Y$ is injective, then the quotient map $X \to X/\!\sim_f$ is a bijection.

(d) The rule $[a]_4 \mapsto [3a]_{12}$ is a bijection $\mathbb{Z}/4 \to \mathbb{Z}/12$.

(e) If $f, g\colon X \to Y$ satisfy $\sim_f = \sim_g$, then $f = g$.

Solution.

(a) **False.** Let $X = \{1, 2\}$, let $\sim$ be equality, and let $g\colon X \to \{0\}$ be the constant function. It is constant on classes (every function is, for equality) and surjective. But $\bar{g}([1]) = 0 = \bar{g}([2])$ with $[1] = \{1\} \neq \{2\} = [2]$, so $\bar{g}$ is not injective. Surjectivity of g gives surjectivity of $\bar{g}$ only, by Theorem 5.2.3 (c).

(b) **True.** This is Proposition 5.2.1 (b).

(c) **True.** If $x \sim_f x'$, then $f(x) = f(x')$, so $x = x'$ by injectivity; hence $[x] = \{x\}$ for every x. The quotient map q is injective: $q(x) = q(x')$ gives $x \sim_f x'$ by Theorem 4.2.1 (b), so $x = x'$. And q is onto by Definition 4.2.4.

(d) **False.** Let $g(a) := [3a]_{12}$. It is constant on classes modulo 4: if $a - a' = 4k$, then $3a - 3a' = 12k$. The induced map is injective by Theorem 5.2.3 (b): if $[3a]_{12} = [3a']_{12}$, then $3(a - a') = 12k$ for some $k \in \mathbb{Z}$, so $a - a' = 4k$ after cancelling 3. But it is not surjective, so by part (c) of the theorem, look for a class that g misses. If $[1]_{12} = [3a]_{12}$, then $1 - 3a = 12k$ for some $k \in \mathbb{Z}$, so $1 = 3(a + 4k)$ and $3 \mid 1$. That is impossible:

$1 = 0 \cdot 3 + 1$ with $0 \leq 1 < 3$, so by the uniqueness in Theorem 2.2.3 the remainder of 1 on division by 3 is 1, not 0. So $[1]_{12}$ is missed.

(e) **False.** Take $X = Y = \mathbb{R}$, $f = \mathrm{id}_{\mathbb{R}}$ and $g(x) = 2x$. Both are injective, so $\sim_f$ and $\sim_g$ are both equality on $\mathbb{R}$, but $f(1) = 1 \neq 2 = g(1)$. Equal fiber relations make the functions differ only by a renaming of values, which is Exercise B2.

5.2.5.3 C. Going deeper

Exercise. C1: Equal fibers

Let $k, m, n \in \mathbb{N}$, let X be a set with n elements, and let $f\colon X \to \{1, \ldots, k\}$ be a function such that the fiber $f^{-1}(\{i\})$ has exactly m elements for every $i \in \{1, \ldots, k\}$. Prove that $n = km$.

Solution. For $k \in \mathbb{N}$, let $P(k)$ be the statement: for every $n \in \mathbb{N}$, every set X with n elements, and every $f\colon X \to \{1, \ldots, k\}$ all of whose fibers over $1, \ldots, k$ have m elements, $n = km$. We prove $P(k)$ for every k by Logic and Proof, Axiom 4.2.1, with m fixed.

Base case $P(0)$. Here $\{1, \ldots, 0\} = \emptyset$, so f is a function $X \to \emptyset$, and $X = \emptyset$ by Proposition 1.5.2 (b). Then $n = 0$: for $n \geq 1$, a bijection $\{1, \ldots, n\} \to \emptyset$ would give 1 a value in $\emptyset$. So $n = 0 = 0 \cdot m$.

Inductive step. Suppose $P(k)$, and let X have n elements and $f\colon X \to \{1, \ldots, k+1\}$ have every fiber of m elements. Put $X' \coloneqq f^{-1}(\{1, \ldots, k\})$ and $F \coloneqq f^{-1}(\{k+1\})$. Every $x \in X$ has $f(x) \leq k$ or $f(x) = k+1$, and not both, so $X = X' \cup F$ and $X' \cap F = \emptyset$. By Proposition 2.5.6, X' has j elements for some $j \in \mathbb{N}$. Let $f'\colon X' \to \{1, \ldots, k\}$, $f'(x) \coloneqq f(x)$; this is a function, because $f(x) \in \{1, \ldots, k\}$ for $x \in X'$. For $i \leq k$, its fiber is $f'^{-1}(\{i\}) = \{x \in X' : f(x) = i\} = f^{-1}(\{i\})$, since every x with $f(x) = i$ lies in X'; so it has m elements. By $P(k)$, $j = km$. The fiber F has m elements by hypothesis, so Proposition 2.5.5 gives that $X = X' \cup F$ has $km + m = (k+1)m$ elements. Since X also has n elements, $n = (k+1)m$ by Corollary 2.5.4. This proves $P(k+1)$.

The statement says that a function whose fibers all have one size cuts X into equal piles, so the size of X is the number of piles times the pile size. With fibers of different sizes the same induction gives the sum of the fiber sizes.

Marking scheme. (10 points)

- 2: states the induction hypothesis with X and f quantified inside it.
- 2: the base case $k = 0$: $X = \emptyset$ and $n = 0$.
- 3: the step: X' and F are disjoint with union X, the fibers of f' are fibers of f, and $j = km$.
- 3: the conclusion by Proposition 2.5.5 and Corollary 2.5.4.

Fatal errors (0 for the step): induction with X fixed; applying $P(k)$ to a function whose fibers were not shown to have m elements.

Exercise. C2: Find the error

A student proves the uniqueness clause of Theorem 5.2.3 (a) as follows.

(1) Suppose $\bar{g}\colon X/\!\sim \to Z$ and $h\colon X/\!\sim \to Z$ both satisfy $\bar{g}\circ q = g$ and $h\circ q = g$. (2) Then $\bar{g}\circ q = h\circ q$. (3) The quotient map q is injective, so q can be cancelled on the right, and $\bar{g} = h$.

Is the conclusion true? Which line fails, and why? Give a counterexample to the failing step, and repair the proof.

Solution. The conclusion is true: it is the uniqueness clause, proved in the text. Lines (1) and (2) are correct. Line (3) fails twice. First, q is injective only when every class is a single point (the second reading after Theorem 4.2.1), which the theorem does not assume. Second, even for an injective map p, $u\circ p = v\circ p$ need not give $u = v$.

Counterexample to the step. For congruence modulo 12 on $\mathbb{Z}$, $q(0) = [0] = [12] = q(12)$ with $0 \neq 12$, so q is not injective, and the claim "q is injective" is false in the very case the clock needs. *Counterexample to the inference.* The inclusion $\iota\colon \{0\} \to \{0,1\}$ is injective; let $u = \mathrm{id}_{\{0,1\}}$ and v be the constant function 0. Then $u\circ\iota = v\circ\iota$ but $u \neq v$.

Repair. What cancels q on the right is that q is **onto**. Replace (3) by: "Let $C \in X/\!\sim$. Since q is surjective (Definition 4.2.4), $C = q(x)$ for some $x \in X$, and then $\bar{g}(C) = \bar{g}(q(x)) = h(q(x)) = h(C)$ by (2). The two functions have the same domain and codomain, so $\bar{g} = h$ by Proposition 1.5.1." Injectivity of q would let one cancel q on the **left**, in $q\circ u = q\circ v$, which is a different situation.

Marking scheme. (10 points)

- 2: says the conclusion is true.
- 3: identifies line (3), and says either that q need not be injective or that injectivity does not license cancelling on the right (surjectivity does).
- 2: gives a concrete non-injective quotient map, such as $q(0) = q(12)$ modulo 12.
- 3: repairs the proof by surjectivity of q: every class is $q(x)$, where both functions take the value $g(x)$.

Fatal errors (0 for the step): calling the conclusion false; a repair that assumes classes are singletons.

Exercise. C3: Exit check: depends only on f

Let $f\colon X \to Y$ and $g\colon X \to Z$ be functions such that, for all $x, x' \in X$, $f(x) = f(x')$ implies $g(x) = g(x')$.

(a) Prove that there is exactly one function $h\colon f(X) \to Z$ with $g(x) = h(f(x))$ for every $x \in X$.

(b) For $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, decide whether $g(x) = x^4$ and whether $g(x) = x^3$ are of the form $h\circ f$ for some function $h\colon f(\mathbb{R}) \to \mathbb{R}$.

Solution.

(a) *Existence.* The hypothesis says that g is constant on the classes of $\sim_f$. By Theorem 5.2.3 (a), there is a function $\bar{g}\colon X/\!\sim_f \to Z$ with $\bar{g}([x]) = g(x)$. By Theorem 5.2.2, $\bar{f}\colon X/\!\sim_f \to f(X)$, $\bar{f}([x]) = f(x)$, is a bijection, so it has an inverse $\bar{f}^{-1}\colon f(X) \to X/\!\sim_f$

(Theorem 1.6.4), and $\bar{f}^{-1}(f(x)) = [x]$ for every $x \in X$. Put $h \coloneqq \bar{g} \circ \bar{f}^{-1}$. Then, for every $x \in X$,

$$h(f(x)) = \bar{g}(\bar{f}^{-1}(f(x))) = \bar{g}([x]) = g(x).$$

Uniqueness. Let $h, h' \colon f(X) \to Z$ both satisfy the condition. Let $y \in f(X)$; by Definition 1.7.1, $y = f(x)$ for some $x \in X$. Then $h(y) = g(x) = h'(y)$. The two functions have the same domain and codomain, so $h = h'$ by Proposition 1.5.1.

(b) $g(x) = x^4$ is of this form: $x^4 = (x^2)^2$, so $h(t) \coloneqq t^2$ on $f(\mathbb{R})$ works, and by (a) it is the only such h. $g(x) = x^3$ is not: if $x^3 = h(x^2)$ for every x, then $1 = 1^3 = h(1) = h((-1)^2) = (-1)^3 = -1$, which is false. The hypothesis of (a) fails at the pair $1, -1$: $f(1) = f(-1)$, while $g(1) \neq g(-1)$.

Marking scheme. (10 points)

- 2: recognizes the hypothesis as "g is constant on the classes of $\sim_f$" and obtains $\bar{g}$ with $\bar{g}([x]) = g(x)$ (or defines $h(f(x)) \coloneqq g(x)$ directly and checks it is well defined).
- 2: uses the bijection $\bar{f}$ onto $f(X)$, or an equivalent argument, so that h is defined at **every** point of $f(X)$ and only there.
- 2: verifies $h(f(x)) = g(x)$ for every x.
- 2: uniqueness, using that every point of $f(X)$ is a value $f(x)$.
- 2: part (b): $h(t) = t^2$ for x^4; the witness pair $1, -1$ for x^3.

A direct proof that defines $h(y) \coloneqq g(x)$ for any x with $f(x) = y$ earns the first two steps if it checks that the value does not depend on the choice of x (that is the hypothesis) and that every $y \in f(X)$ has such an x. Fatal errors (0 for the step): defining h on all of Y without a value for points outside $f(X)$; proving the converse implication $g(x) = g(x') \Rightarrow f(x) = f(x')$ instead of using the hypothesis.

5.3 Binary Operations

Sections 5.1 and 5.2 built new functions from old ones by cutting, gluing and factoring. This section looks at functions of a special shape: functions that take two elements of a set and return a third element of the same set, such as $+$ on $\mathbb{Z}$, $\cup$ on $\mathcal{P}(X)$ and $\circ$ on the functions from a set to itself. We name the properties such an operation may have, one at a time, and ask what each property buys on its own. The central answers, uniqueness of identities and of inverses, are short proofs by one method, computing a single expression in two ways; the rest are proved by checking candidates. All of them work at once for numbers, for sets, for functions and for the hours of the clock.

5.3.1 Brackets

Nobody writes brackets in $2 + 3 + 4$: whether we add $2 + 3$ first or $3 + 4$ first, the answer is 9. Subtraction is different. Reading $2 - 3 - 4$ from the left gives $(2 - 3) - 4 = -5$, and from the right gives $2 - (3 - 4) = 3$. Powers behave like subtraction: $2^{(3^2)} = 2^9 = 512$, while $(2^3)^2 = 8^2 = 64$. School arithmetic settles this by convention (subtraction from the left, towers of powers from the top), and a convention is needed exactly because the bracketing changes the answer.

The same questions arise far from numbers. For subsets of a set X, is $(A \cup B) \cup C$ the same set as $A \cup (B \cup C)$? For functions from X to itself, is $h \circ (g \circ f)$ the same function as $(h \circ g) \circ f$? On the clock $\mathbb{Z}/12$ of Section 4.2, is there an hour that changes nothing when added, as 0 does for integers, and can every hour be undone?

Each of these questions asks whether some rule of arithmetic holds for some way of combining two things into a third. The aim of this section is to separate the rules and to find out what each rule gives on its own. Here is a test question to keep in mind: can a set with an operation have two different elements that both behave like 0? For $+$ on $\mathbb{Z}$ the answer seems obvious, but the reason is not; the answer comes in the subsection "One identity, one inverse".

5.3.2 Operations

The first thing to fix is what counts as a way of combining two things. Two natural candidates fail. Subtraction on $\mathbb{N}$ takes the pair $(2,3) \in \mathbb{N} \times \mathbb{N}$ to -1, which is not in $\mathbb{N}$. Division on $\mathbb{R}$ has no value at all at the pair $(1,0)$. The first fails because a value leaves the set; the second fails because a pair has no value. A way of combining must give **every** pair a value, and the value must lie **in the set**. Those are the two halves of being a function with domain $X \times X$ and codomain X (Definition 1.5.1).

An operation on a set combines any two of its elements into a third element of the same set.

Definition 5.3.1. Binary Operation

Let X be a set. A **binary operation** on X, or an **operation** on X, is a function

$$*\colon X \times X \to X.$$

Its value at (x, y) is written $x * y$ rather than $*(x, y)$.

A subset $A \subseteq X$ is **closed** under $*$ if $a * b \in A$ **for all** $a, b \in A$.

In words: the definition asks for a function, so each pair (x, y) of elements of X, in this order, has **exactly one** value, and that value lies in X. The order matters, since (x, y) and (y, x) are different pairs and may have different values; $2 - 3 \neq 3 - 2$. The letter $*$ is a name for the operation, like f for a function. In examples it is replaced by a familiar symbol, $+$, $\cdot$, $\cup$, $\circ$.

If A is closed under $*$, then the restriction of $*$ to $A \times A$, with codomain A, is an operation on A: restriction to a subset of the domain (Definition 5.1.1) gives a function $A \times A \to X$, and closure says its values lie in A, so A may serve as the codomain. We keep the symbol $*$ for the restricted operation.

Example. Operations

Decide which of the following are operations on the set named, and which subsets named are closed.

(a) $+$, $\cdot$ and $-$ on $\mathbb{Z}$; the average $x * y := (x + y)/2$ and max on $\mathbb{R}$.
(b) $\cup$, $\cap$ and the symmetric difference $\triangle$ of Section 5.1 on $\mathcal{P}(X)$.
(c) Composition $\circ$ on X^X, the set of all functions $X \to X$.
(d) $[a] + [b] := [a + b]$ and $[a][b] := [ab]$ on $\mathbb{Z}/n$, for $n \in \mathbb{Z}_{>0}$.
(e) Division $(x, y) \mapsto x/y$ on $\mathbb{R} \setminus \{0\}$; and the subset $\mathbb{Z}_{>0}$ of $\mathbb{Z}$, under $+$ and under $-$.

Solution.

(a) Each rule gives every pair of integers one integer, and every pair of reals one real, so

each is an operation. The average is an operation on $\mathbb{R}$ but not on $\mathbb{Z}$: $(0+1)/2 \notin \mathbb{Z}$.

(b) For $A, B \subseteq X$, the sets $A \cup B$, $A \cap B$ and $A \triangle B$ are again subsets of X (Definition 1.3.1), so each is an operation on $\mathcal{P}(X)$.

(c) For $f, g \in X^X$, the composite $g \circ f$ is a function $X \to X$ (Definition 1.5.2), so $(g, f) \mapsto g \circ f$ is an operation on X^X.

(d) Both rules read representatives of classes; Proposition 4.2.5 proved that they are well defined, that is, that each pair of classes gets exactly one class. So both are operations on $\mathbb{Z}/n$.

(e) If $x, y \neq 0$, then x/y is defined and $x/y \neq 0$, so division is an operation on $\mathbb{R} \setminus \{0\}$. The positive integers are closed under $+$, since a sum of positive integers is positive. They are not closed under $-$: $1, 2 \in \mathbb{Z}_{>0}$, and $1 - 2 = -1 \notin \mathbb{Z}_{>0}$.

Part (d) is the reason this section returns to quotients at its end: an operation on classes is a rule on representatives together with a proof of well-definedness. Part (e) shows that a rule that fails on one set may succeed on a smaller one; the pairs that caused trouble for division, those with second entry 0, have been removed.

Quick check. Is $(A, B) \mapsto A \setminus B$ an operation on $\mathcal{P}(X)$? Are the even integers closed under $+$? The odd integers?

Solution. Yes: for $A, B \subseteq X$, $A \setminus B \subseteq A \subseteq X$, so the value lies in $\mathcal{P}(X)$. Yes: $2k+2l = 2(k+l)$. No: 1 is odd and $1+1=2$ is not.

5.3.3 Properties

The questions of the hook are now questions about an operation $*$ on a set X. Each asks whether an equation holds for every choice of elements, or whether some element has a special behavior.

Definition 5.3.2. Associative, Commutative, Identity, Inverse

Let $*$ be an operation on a set X.

(a) $*$ is **associative** if $(x * y) * z = x * (y * z)$ **for all** $x, y, z \in X$.

(b) $*$ is **commutative** if $x * y = y * x$ **for all** $x, y \in X$.

(c) An element $e \in X$ is a **left identity** of $*$ if $e * x = x$ **for every** $x \in X$; a **right identity** if $x * e = x$ **for every** $x \in X$; and an **identity** if it is both.

(d) Suppose $*$ has an identity e, and let $x \in X$. An element $y \in X$ is an **inverse** of x if $x * y = e$ **and** $y * x = e$. The element x is **invertible** if it has an inverse.

In words: associativity says brackets may be moved; commutativity says the two inputs may be swapped. A left or right identity is an element that changes nothing, from the side named; an identity must change nothing from **both** sides and must do so for **every** element. An inverse of x undoes x, again from both sides, and it is defined only relative to an identity. Clause (d) says "an inverse", not "the inverse": nothing in the definition says there is only one.

For $+$ on $\mathbb{Z}$, all four hold: $+$ is associative and commutative, 0 is an identity, and $-x$ is an

inverse of x. For $\cdot$ on $\mathbb{Z}$, 1 is an identity, and only 1 and -1 are invertible. For $\cup$ on $\mathcal{P}(X)$, $\emptyset$ is an identity, since $\emptyset \cup A = A = A \cup \emptyset$.

Deciding whether an operation has a property is the work of Section 4.1's method for relations (Example (Method: proving or disproving a property of a relation)): a property that says "for all" is proved by taking arbitrary elements, and a failure needs one witness, checked. For an identity the quantifiers are the other way round, "there is an e such that for every x", so a proof names one e and checks it against every x, and a refutation must show that **every** candidate e fails at some x.

Example. A right identity that is not an identity

Decide whether subtraction on $\mathbb{Z}$ is associative, and find its left and right identities.

Solution. Not associative. The triple $2, 3, 4$ of the hook is a witness: $(2-3)-4 = -5$ and $2-(3-4) = 3$.

A right identity. For every $x \in \mathbb{Z}$, $x - 0 = x$, so 0 is a right identity.

Not a left identity. $0 - 1 = -1 \neq 1$, so 0 fails at $x = 1$.

No left identity at all. Suppose e is a left identity, so $e - x = x$ for every $x \in \mathbb{Z}$. At $x = 0$ this gives $e = 0$; at $x = 1$ it gives $e - 1 = 1$, so $e = 2$. Then $0 = 2$, which is false. So no integer is a left identity, and subtraction has no identity.

The refutation of "there is a left identity" did not test candidates one by one. It assumed a left identity e, used the hypothesis "for every x" at two well-chosen values of x, and reached two incompatible values for e.

Quick check. Is the average $x * y \coloneqq (x + y)/2$ on $\mathbb{R}$ associative? Is it commutative? Has it an identity?

Solution. Not associative: $(0 * 0) * 4 = 0 * 4 = 2$, while $0 * (0 * 4) = 0 * 2 = 1$. Commutative: $(x + y)/2 = (y + x)/2$. No identity: if $(e + x)/2 = x$ for every x, then $e = x$ for every $x \in \mathbb{R}$, so $e = 0$ and $e = 1$, which is false.

Quick check. Consider max on $\mathbb{N}$ and max on $\mathbb{Z}$. Is each associative? Commutative? Has it an identity?

Solution. Both are associative, since $\max(\max(x, y), z)$ and $\max(x, \max(y, z))$ are both the largest of x, y, z, and both are commutative. On $\mathbb{N}$, 0 is an identity: $\max(0, x) = x = \max(x, 0)$ since $x \geq 0$. On $\mathbb{Z}$ there is none: an identity e would need $\max(e, e - 1) = e - 1$, but $\max(e, e - 1) = e$. The same rule, on a larger set, loses its identity.

5.3.4 One identity, one inverse

Back to the test question of the hook. An operation may have several left identities: for $x*y := y$ on a set with two elements, every element is a left identity (Exercise A1 (c)). But an element that is an identity from both sides is never shared.

Proposition 5.3.1. An Identity Is Unique

Let $*$ be an operation on a set X. If e is a left identity and e' is a right identity of $*$, then $e = e'$. In particular, $*$ has at most one identity.

Idea (Scratch work). Two candidates, so this is the uniqueness half of Example (Method: existence and uniqueness): two names, about which we know only the defining equations, to be shown equal. The givens are equations about products; the goal mentions no product at all. The gap is to find one product that both givens can simplify.

Givens	Goal
$e * x = x$ for every $x \in X$; $x * e' = x$ for every $x \in X$	$e = e'$
the givens speak about products; the goal about two elements	one product that each given simplifies
the product $e * e'$: the first given at $x = e'$ makes it e'; the second at $x = e$ makes it e	$e = e * e' = e'$

The last row closes the gap: the product $e * e'$, with one candidate on each side, is the expression both givens can reach.

Proof. Since e' is a right identity, the case $x = e$ of its defining equation gives $e * e' = e$. Since e is a left identity, the case $x = e'$ gives $e * e' = e'$. Hence $e = e * e' = e'$.

If e and e' are both identities, then e is a left identity and e' a right identity, so $e = e'$. This proves the proposition.

■

Neither associativity nor commutativity was used: the proof applies two hypotheses once each, to the single product $e*e'$. So the answer to the test question is no, for every operation whatsoever. Because of the proposition, we may speak of **the** identity of $*$ when there is one.

The proof is an instance of a move that runs through this section and the next.

Example. Method: compute one expression in two ways

Template. To prove $a = b$ when a and b are known only through equations: (1) find one expression m that the equations about a reduce to a, and the equations about b reduce to b; (2) write the chain $a = \cdots = m = \cdots = b$, citing a hypothesis at each "=".

When to use it. Uniqueness of identities and of inverses, cancellation, and any goal equating two objects given by equations.

The usual failure. Assuming $a = b$ somewhere in the chain (entry (N9) of Logic and Proof, Example (What is not allowed)); using associativity or commutativity that was not given; a bracket moved silently.

Inverses are the second test of the method. Here associativity is needed, and the proof shows exactly where.

Proposition 5.3.2. Inverses Are Unique for an Associative Operation

Let $*$ be an associative operation on a set X with identity e, and let $x \in X$. If $y * x = e$ and $x * z = e$, then $y = z$. In particular, x has at most one inverse.

Idea. As in Example (Method: compute one expression in two ways). The expression is $m = (y * x) * z$, which is also $y * (x * z)$ by associativity: bracketed as written it is $e * z = z$, and regrouped it is $y * e = y$. Associativity is exactly the license to read it both ways.

Proof. Using that e is an identity, then $x * z = e$, then associativity, then $y * x = e$, and finally that e is an identity again:

$$y = y * e = y * (x * z) = (y * x) * z = e * z = z.$$

If y and z are both inverses of x, then in particular $y * x = e$ and $x * z = e$, so $y = z$. This proves the proposition.

■

For an associative operation with identity, the inverse of an invertible x is therefore unique, and we write it x^{-1}. For an operation written $+$, the inverse is written $-x$ instead. The proposition is a little stronger than uniqueness: an element x with some y such that $y * x = e$ and some z such that $x * z = e$ has $y = z$, and then y is an inverse of x, so x is invertible. This is the same computation as Proposition 1.6.3 for functions, now done for any associative operation.

Without associativity the conclusion can fail, and a three-element table shows it.

Example. Without associativity, two inverses

Let $X = \{e, a, b\}$ with three different elements, and define $*$ by the table below: the entry in row u and column v is $u * v$.

$*$	e	a	b
e	e	a	b
a	a	e	e
b	b	e	e

Show that $*$ is a commutative operation with identity e, that a has two different inverses, and that $*$ is not associative.

Solution. The table gives each of the nine pairs exactly one value in X, so $*$ is an operation on X. The table is symmetric about its diagonal, which says $u * v = v * u$ for all u, v: $*$ is commutative. The row and the column of e repeat the headings, so $e * u = u = u * e$ for every u: e is the identity.

Since $a * a = e$, the element a is an inverse of itself; since $a * b = e = b * a$, the element b is another inverse of a, and $a \neq b$.

Finally, $(a * a) * b = e * b = b$, while $a * (a * b) = a * e = a$. These differ, so $*$ is not associative.

The last line is Proposition 5.3.2's chain, run on $y = a$, $x = a$, $z = b$, breaking at the one step that used associativity.

With uniqueness in hand, the rules that school algebra uses for inverses of numbers can be proved for any associative operation. The method for each is the same: name a candidate, check it on both sides, and let uniqueness do the rest.

Proposition 5.3.3. Inverses of Products

Let $*$ be an associative operation on a set X with identity e.

(a) e is invertible, and $e^{-1} = e$.
(b) If x is invertible, then so is x^{-1}, and $(x^{-1})^{-1} = x$.
(c) If x and y are invertible, then so is $x * y$, and $(x * y)^{-1} = y^{-1} * x^{-1}$.

Idea. Each part names a candidate and checks it, which is the existence half of Example (Method: existence and uniqueness); uniqueness was proved once and for all in Proposition 5.3.2. For (c) the candidate is found by asking what undoes $x * y$: first remove y, then x.

Proof. In each part we show that the candidate is an inverse by checking both equations of Definition 5.3.2 (d); then it is **the** inverse by Proposition 5.3.2.

(a) $e * e = e$, since e is an identity, and this one equation is both required equations.

(b) The two equations $x * x^{-1} = e$ and $x^{-1} * x = e$, which say that x^{-1} is an inverse of x, also say that x is an inverse of x^{-1}.

(c) Using associativity twice to regroup, then the defining equation of y^{-1}, the identity, and the defining equation of x^{-1}:

$$\begin{aligned}(x * y) * (y^{-1} * x^{-1}) &= x * (y * (y^{-1} * x^{-1})) = x * ((y * y^{-1}) * x^{-1}) \\ &= x * (e * x^{-1}) = x * x^{-1} = e.\end{aligned}$$

In the same way, $(y^{-1} * x^{-1}) * (x * y) = y^{-1} * (x^{-1} * (x * y)) = y^{-1} * ((x^{-1} * x) * y) = y^{-1} * (e * y) = y^{-1} * y = e$. This proves the proposition.

■

In (c) the order reverses: to undo "first x, then y", one undoes y first. The display moved brackets one step at a time; Exercise C1 shows that for four factors every bracketing gives the same element.

Quick check. Which elements of $\mathcal{P}(X)$ are invertible under $\cup$? Which are invertible under $\triangle$?

Solution. Both operations have identity $\emptyset$: $A \cup \emptyset = A$, and $A \triangle \emptyset = (A \setminus \emptyset) \cup (\emptyset \setminus A) = A$ and $\emptyset \triangle A = (\emptyset \setminus A) \cup (A \setminus \emptyset) = A$. Under $\cup$, if $A \cup B = \emptyset$, then $A \subseteq A \cup B = \emptyset$, so $A = \emptyset$: only $\emptyset$ is invertible. Under $\triangle$, $A \triangle A = (A \setminus A) \cup (A \setminus A) = \emptyset$, so every A is invertible and is its own inverse.

5.3.5 Operations on functions

An operation on a set Y gives an operation on every set of functions into Y, by combining values point by point. This is how $f + g$ and $f \cdot g$ are defined for real functions, and it carries each property of the operation on Y over to the functions.

Proposition 5.3.4. Pointwise Operations

Let $*$ be an operation on a set Y, and let X be a set. For $f, g \in Y^X$, define $f * g \colon X \to Y$ by

$$(f * g)(x) := f(x) * g(x) \qquad (x \in X).$$

This is an operation on Y^X, the **pointwise** operation, and:

(a) if $*$ is associative, or commutative, on Y, then so is the pointwise operation on Y^X;
(b) if e is an identity of $*$, then the constant function $c_e \colon X \to Y$, $x \mapsto e$, is an identity of the pointwise operation;
(c) if $*$ is associative with identity e, then $f \in Y^X$ is invertible if and only if every value $f(x)$ is invertible in Y, and then the inverse of f is $x \mapsto f(x)^{-1}$.

Idea. An equation between functions is checked value by value (Proposition 1.5.1), and at the point x each law for the pointwise operation is the same law for $*$, applied to the values $f(x)$, $g(x)$, $h(x)$.

Proof. For $x \in X$, the value $f(x) * g(x)$ is one element of Y, so $f * g$ is a function $X \to Y$, and $(f, g) \mapsto f * g$ is an operation on Y^X. Each equation below is between functions $X \to Y$, so by Proposition 1.5.1 it suffices to compare values at an arbitrary $x \in X$.

(a) By the definition, used twice on each side, and associativity in Y,

$$((f * g) * h)(x) = (f(x) * g(x)) * h(x) = f(x) * (g(x) * h(x)) = (f * (g * h))(x).$$

Likewise $(f * g)(x) = f(x) * g(x) = g(x) * f(x) = (g * f)(x)$ when $*$ is commutative.

(b) $(c_e * f)(x) = e * f(x) = f(x)$ and $(f * c_e)(x) = f(x) * e = f(x)$.

(c) ($\Rightarrow$) Let g be an inverse of f, so $f * g = c_e = g * f$, the identity being c_e by (b) and Proposition 5.3.1. Evaluating at x gives $f(x) * g(x) = e = g(x) * f(x)$, so $g(x)$ is an inverse of $f(x)$. ($\Leftarrow$) If every $f(x)$ is invertible, its inverse $f(x)^{-1}$ is unique (Proposition 5.3.2), so $g(x) \coloneqq f(x)^{-1}$ defines a function $g\colon X \to Y$. Then $(f * g)(x) = f(x) * f(x)^{-1} = e = c_e(x)$, and likewise $(g * f)(x) = e$, so g is an inverse of f. The pointwise operation is associative by (a), so this inverse is the only one, by Proposition 5.3.2. This proves the proposition.

■

Part (c) needs every value to be invertible, not just most of them. On $\mathbb{R}^{\mathbb{R}}$ with pointwise $\cdot$, the identity is the constant c_1; the function $x \mapsto x$ is not invertible, because its value at 0 has no multiplicative inverse, although every other value has one.

Warning (Iterate or product?). On $\mathbb{R}^{\mathbb{R}}$ the symbol f^2 could mean two different functions: the pointwise product $x \mapsto f(x) \cdot f(x)$, or the composite $f \circ f$. For $f(x) = x + 1$ the first is $x \mapsto (x+1)^2$ and the second is $x \mapsto x + 2$. In this book f^n always means the n-th iterate, f composed with itself n times, defined in Section 5.4. A pointwise product is written $f \cdot g$, and a pointwise power is written out, $x \mapsto f(x)^n$. For the same reason f^{-1} standing alone always means the inverse function, while $f^{-1}(B)$ for a set B is still the preimage of Definition 1.7.2, defined for every f; the inverse of f under pointwise $\cdot$, when it exists, is written $x \mapsto 1/f(x)$.

Indicators are a first instance. The set $\{0, 1\}$ is closed under multiplication of numbers, so $\cdot$ is an operation on $\{0, 1\}$, and pointwise multiplication is an operation on $\{0, 1\}^X$. By Proposition 5.1.3 (a), $\mathbf{1}_A \cdot \mathbf{1}_B = \mathbf{1}_{A \cap B}$: on indicators, the pointwise product **is** intersection. The identity of pointwise $\cdot$ is the constant function c_1, which is $\mathbf{1}_X$, matching $X \cap A = A$ for $A \subseteq X$.

The second instance is composition. On X^X, any two functions can be composed in either order, and composition is an operation (Example (Operations) (c)).

Proposition 5.3.5. Composition on X^X

Let X be a set. Composition $(g, f) \mapsto g \circ f$ is an associative operation on X^X with identity id_X. An element $f \in X^X$ is invertible under $\circ$ if and only if f is bijective, and then its inverse under $\circ$ is the inverse function f^{-1}. If X has two different elements, then $\circ$ is not commutative on X^X.

Proof. Associativity and $f \circ \mathrm{id}_X = f = \mathrm{id}_X \circ f$ are Proposition 1.5.3, with all four sets equal to X. Under $\circ$, an inverse of f in the sense of Definition 5.3.2 (d) is a $g \in X^X$ with $f \circ g = \mathrm{id}_X = g \circ f$, which is exactly a two-sided inverse of f in the sense of Definition 1.6.2. By Theorem 1.6.4, f has one if and only if f is bijective, and it is then the inverse function f^{-1}, which is unique by Proposition 1.6.3.

Now let $a, b \in X$ with $a \neq b$, and let $c_a, c_b \in X^X$ be the constant functions with values a and b. For every $x \in X$, $(c_a \circ c_b)(x) = c_a(b) = a$ and $(c_b \circ c_a)(x) = c_b(a) = b$. So $c_a \circ c_b = c_a$ and $c_b \circ c_a = c_b$, and these differ, since their values at a differ (Proposition 1.5.1). This proves the proposition.

■

So the invertible elements of X^X under composition are exactly the bijections from X to itself, the subject of Section 5.4. For them, Proposition 5.3.3 (c) says $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. That rule appeared as Exercise B2 of Section 1.6 (Exercise (B2: The inverse of a composite)); here it is proved once, for every associative operation, and the rule for bijections of a set to itself is one case of it (Exercise B2 of Section 1.6 allows three different sets).

Quick check. In $\mathbb{R}^{\mathbb{R}}$, find the inverse of $f(x) = 2x + 1$ under composition, and its inverse under pointwise $+$.

Solution. Under $\circ$: $g(x) = (x - 1)/2$, since $f(g(x)) = (x - 1) + 1 = x$ and $g(f(x)) = (2x + 1 - 1)/2 = x$. Under pointwise $+$, whose identity is the constant c_0: $x \mapsto -2x - 1$, since $(2x + 1) + (-2x - 1) = 0$. The two inverses are different functions; "the inverse" always names its operation.

5.3.6 Operations on a quotient

The clock adds hours, and Section 4.2 checked that the addition is well defined (Proposition 4.2.5). Every operation that respects an equivalence relation passes to the quotient in the same way, and it takes its properties with it.

Proposition 5.3.6. Operations on a Quotient

Let $*$ be an operation on a set X, and let $\sim$ be an equivalence relation on X such that, for all $x, x', y, y' \in X$,

$$x \sim x' \text{ and } y \sim y' \quad \Longrightarrow \quad x * y \sim x' * y'.$$

Then $[x] * [y] := [x * y]$ is a well-defined operation on $X/\!\sim$, and the quotient map satisfies $q(x * y) = q(x) * q(y)$. Moreover:

(a) if $*$ is associative, or commutative, then so is the operation on $X/\!\sim$;

(b) if e is an identity of $*$, then $[e]$ is an identity of the operation on $X/\!\sim$;

(c) if y is an inverse of x, then $[y]$ is an inverse of $[x]$.

Idea. As in Example (Method: define a function on a quotient), the rule computes a value from representatives, so the one thing to check is that the value does not depend on them (Example (Method: checking that a definition on classes is well defined)); here there are two representatives to change, and the hypothesis on $\sim$ handles both at once. Each law then holds for classes because it holds for representatives, and every class has one.

Proof. Well defined. Every class is $[x]$ for some $x \in X$ (Definition 4.2.4), so the rule gives every pair of classes a value, and the value $[x * y]$ lies in $X/\!\sim$. Let $[x] = [x']$ and $[y] = [y']$. By Theorem 4.2.1 (b), $x \sim x'$ and $y \sim y'$, so $x * y \sim x' * y'$ by hypothesis, and $[x * y] = [x' * y']$

by Theorem 4.2.1 (b) again. So the value does not depend on the representatives, and $*$ is an operation on $X/\sim$. The equation $q(x*y) = [x*y] = [x]*[y] = q(x)*q(y)$ is the definition.

(a) Let three classes be given, with representatives x, y, z. Applying the definition twice on each side and associativity in X,

$$([x] * [y]) * [z] = [(x * y) * z] = [x * (y * z)] = [x] * ([y] * [z]).$$

Likewise $[x] * [y] = [x * y] = [y * x] = [y] * [x]$ when $*$ is commutative.

(b) $[e] * [x] = [e * x] = [x]$ and $[x] * [e] = [x * e] = [x]$, for every class $[x]$.

(c) $[x] * [y] = [x * y] = [e]$ and $[y] * [x] = [y * x] = [e]$, and $[e]$ is the identity by (b). This proves the proposition.

■

The hypothesis on $\sim$ is the whole content: it says that $*$ does not see the difference between equivalent elements. For $\mathbb{Z}$ with congruence modulo n, it is exactly Proposition 4.2.5, for $+$ and for $\cdot$. So $\mathbb{Z}/n$ inherits from $\mathbb{Z}$: addition is associative and commutative with identity $[0]$, every class $[a]$ has the inverse $[-a]$ and we write $-[a] = [-a]$, and multiplication is associative and commutative with identity $[1]$. On the clock, $[9] + [3] = [12] = [0]$, so $-[9] = [3]$: the hour that undoes nine hours is three hours.

Part (c) goes one way only. The quotient can have inverses that X lacks: in $\mathbb{Z}/3$, $[2][2] = [4] = [1]$, so $[2]$ is invertible under multiplication, while no integer y has $2y = 1$, since 1 is odd.

5.3.7 Exercises

5.3.7.1 A. Check your understanding

Exercise. A1

(a) Which of the following are operations: subtraction on $\mathbb{N}$; subtraction on $\mathbb{Z}$; $(x, y) \mapsto x/y$ on $\mathbb{R} \setminus \{0\}$; $(x, y) \mapsto x/y$ on $\mathbb{Z} \setminus \{0\}$?

(b) Write the table of $+$ on $\mathbb{Z}/3 = \{[0], [1], [2]\}$. Find the identity and the inverse of each class.

(c) Let X be a set with at least two elements, and let $x * y := y$. Find all left identities and all right identities of $*$.

(d) State the template of the method of computing one expression in two ways, and say which expression it computes in the proof of Proposition 5.3.2.

Solution.

(a) Subtraction on $\mathbb{N}$: no, $2 - 3 = -1 \notin \mathbb{N}$. Subtraction on $\mathbb{Z}$: yes. Division on $\mathbb{R} \setminus \{0\}$: yes, since x/y is defined and non-zero for $x, y \neq 0$. Division on $\mathbb{Z} \setminus \{0\}$: no, $1/2 \notin \mathbb{Z}$.

(b) By the rule $[a] + [b] = [a + b]$, reducing with Proposition 4.2.4 ($[3] = [0]$, $[4] = [1]$):

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$

[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

The row and column of [0] repeat the headings, so [0] is the identity. Reading off the entries [0]: $-[0]=[0]$, $-[1]=[2]$, $-[2]=[1]$.

(c) Every $e \in X$ is a left identity, since $e*y=y$ for every y. No element is a right identity: for $e \in X$, pick $x \in X$ with $x \neq e$ (there is one, since X has at least two elements); then $x*e=e \neq x$. So left identities need not be unique when there is no right identity; Proposition 5.3.1 needs one of each.

(d) To prove $a=b$ for objects known only through equations, find one expression that the equations about a reduce to a and those about b reduce to b, and write $a=\cdots=m=\cdots=b$ with a reason at each step (Example (Method: compute one expression in two ways)). In Proposition 5.3.2 the expression is $(y*x)*z$, which equals z as written and, regrouped as $y*(x*z)$, equals y.

5.3.7.2 B. Practice

Exercise. B1: Deciding properties

On $\mathbb{R}$, let $x*y \coloneqq x+y-xy$. Determine whether $*$ is associative and whether it is commutative, find its identity, and find which elements are invertible, with their inverses. Justify your answer.

Solution. Associative. Expanding both sides,

$$\begin{aligned}(x*y)*z &= (x+y-xy)+z-(x+y-xy)z\\ &= x+y+z-xy-xz-yz+xyz,\\ x*(y*z) &= x+(y+z-yz)-x(y+z-yz)\\ &= x+y+z-xy-xz-yz+xyz.\end{aligned}$$

The two results agree, so $*$ is associative. (Both are unchanged by any rearrangement of x,y,z.)

Commutative. $x+y-xy=y+x-yx$.

Identity. $0*x=0+x-0=x$, and $x*0=x$ by commutativity; so 0 is the identity, unique by Proposition 5.3.1.

Inverses. We need y with $x+y-xy=0$ (the other side follows by commutativity), that is, $y(1-x)=-x$. If $x \neq 1$, this has the solution $y=x/(x-1)$: indeed $x+\frac{x}{x-1}-\frac{x^2}{x-1}=\frac{x(x-1)+x-x^2}{x-1}=0$. If $x=1$, then $1*y=1+y-y=1\neq 0$ for every y, so 1 has no inverse. So every $x \neq 1$ is invertible, with inverse $x/(x-1)$ under $*$, and 1 is not.

A remark. $1-x*y=(1-x)(1-y)$. For $u,v \in \{0,1\}$, $u*v=u+v-uv$ is the indicator rule for a union, Proposition 5.1.3 (c): $\mathbf{1}_{A\cup B}(x)=\mathbf{1}_A(x)*\mathbf{1}_B(x)$.

Exercise. B2: Every square is the identity

Let $*$ be an associative operation on a set X with identity e, such that $x * x = e$ for every $x \in X$. Prove that $*$ is commutative. Check the hypothesis for $\triangle$ on $\mathcal{P}(X)$.

Solution. Let $x \in X$. The equation $x * x = e$ says that x is an inverse of itself, from both sides; by Proposition 5.3.2, $x^{-1} = x$. Now let $x, y \in X$. By the hypothesis applied to $x * y$, and by Proposition 5.3.3 (c),

$$x * y = (x * y)^{-1} = y^{-1} * x^{-1} = y * x.$$

For $\triangle$: it is associative (Example (Symmetric difference is associative)) with identity $\emptyset$, and $A \triangle A = \emptyset$ for every $A \subseteq X$ (the Quick check after Proposition 5.3.3). So $\triangle$ is commutative, which can also be read off its definition, since $(A \setminus B) \cup (B \setminus A)$ is symmetric in A and B.

Exercise. B3: Two kinds of inverse

In $\mathbb{R}^{\mathbb{R}}$, find, if they exist, the inverses of $f(x) = x^3 + 1$ under composition and under pointwise $+$, and the inverses of $g(x) = x^2$ under composition and under pointwise $\cdot$. Justify each answer.

Solution. *f under $\circ$.* Let $h(x) := \sqrt[3]{x - 1}$, the real cube root. Then $f(h(x)) = (x-1)+1 = x$ and $h(f(x)) = \sqrt[3]{x^3} = x$, so h is the inverse (Proposition 5.3.5).

f under $+$. The identity is c_0, and $x \mapsto -x^3 - 1$ is the inverse: $(x^3 + 1) + (-x^3 - 1) = 0$ at every x (Proposition 5.3.4 (c)).

g under $\circ$. None: $g(1) = 1 = g(-1)$, so g is not injective, hence not bijective, hence not invertible under $\circ$ by Proposition 5.3.5.

g under $\cdot$. None: the value $g(0) = 0$ has no inverse under multiplication of reals ($0 \cdot y = 0 \neq 1$), so by Proposition 5.3.4 (c) g is not invertible.

Exercise. B4: Prove or disprove

Prove or disprove each statement. Throughout, $*$ is an operation on a set X.

(a) Every left identity of $*$ equals every right identity of $*$.

(b) $*$ has at most one left identity.

(c) If $*$ is associative with identity, x is invertible and $x * y = x * z$, then $y = z$.

(d) If $*$ is associative with identity e and $x * y = e$, then $y * x = e$.

(e) A commutative operation with an identity is associative.

Solution.

(a) True. This is Proposition 5.3.1.

(b) False. For $x * y := y$ on $X = \{1, 2\}$, both 1 and 2 are left identities, as in Exercise A1 (c).

(c) True, by computing $(x^{-1} * x) * y$, regrouped as $x^{-1} * (x * y)$, in two ways (Example (Method: compute one expression in two ways)), with associativity at the second and fourth steps:

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

(d) False. Take $X = \mathbb{N}^{\mathbb{N}}$ under composition, associative with identity $\mathrm{id}_{\mathbb{N}}$ (Proposition 5.3.5). Let $s(n) := n + 1$, and $p(n) := n - 1$ for $n \geq 1$, $p(0) := 0$: the successor map of Section 1.6 and a left inverse of it. Then $p \circ s = \mathrm{id}_{\mathbb{N}}$, since $p(n + 1) = n$. But $(s \circ p)(0) = s(0) = 1 \neq 0$, so $s \circ p \neq \mathrm{id}_{\mathbb{N}}$. With $x = p$ and $y = s$, $x \circ y = e$ and $y \circ x \neq e$.

(e) False. The operation of Example (Without associativity, two inverses) is commutative with identity e, and not associative.

5.3.7.3 C. Going deeper

Exercise. C1: Four factors

Let $*$ be an associative operation on a set X, and let $a, b, c, d \in X$. Writing uv for $u * v$, show that the five bracketings

$$((ab)c)d, \quad (a(bc))d, \quad (ab)(cd), \quad a((bc)d), \quad a(b(cd))$$

are all equal.

Solution. We show that each equals $((ab)c)d$. Each step is one use of associativity, $(xy)z = x(yz)$, with x, y, z chosen as stated.

- $(a(bc))d = ((ab)c)d$: associativity with $x = a$, $y = b$, $z = c$ gives $a(bc) = (ab)c$, and then both sides are that element times d.
- $(ab)(cd) = ((ab)c)d$: associativity with $x = ab$, $y = c$, $z = d$.
- $a((bc)d) = (a(bc))d$: associativity with $x = a$, $y = bc$, $z = d$; and $(a(bc))d = ((ab)c)d$ by the first item.
- $a(b(cd)) = (ab)(cd)$: associativity with $x = a$, $y = b$, $z = cd$; and $(ab)(cd) = ((ab)c)d$ by the second item.

So all five bracketings are equal. That every bracketing of any finite number of factors gives the same element is true as well; its proof is an induction on the number of factors, not carried out here, and this chapter regroups longer composites only by repeated use of the three-factor law.

Exercise. C2: Find the error

Let $*$ be an operation on a set X with identity e. A student argues:

> (1) Let y and z be inverses of x. (2) Then $x*y = e$ and $x*z = e$, so $x*y = x*z$. (3) Cancelling x on the left, $y = z$. (4) Hence an element has at most one inverse.

(a) Which line fails, and which hypothesis does it hide?

(b) Show that without that hypothesis the step of the failing line is false.

Solution.

(a) Line (3) fails. "Cancelling x" is the statement of Exercise B4 (c), which holds when $*$ is associative and x is invertible; its proof regroups $x^{-1} * (x * y)$ as $(x^{-1} * x) * y$, and that is associativity. The statement here does not assume associativity, so line (3) cites a fact that is not available: entry (N9) of Logic and Proof, Example (What is not allowed). Lines (1) and (2) are correct, and with associativity added the argument becomes a correct proof of Proposition 5.3.2.

(b) In Example (Without associativity, two inverses), which has an identity and is not associative, $a * a = e = a * b$, so $a * a = a * b$, and yet $a \neq b$. Cancelling a on the left is false there, and so is the conclusion (4): a has the two inverses a and b.

Marking scheme. (10 points)

- 3: names line (3) as the step that fails.
- 3: names associativity as the hidden hypothesis, and says where cancellation uses it.
- 4: gives an operation with identity, not associative, and an **invertible** element x with $x * y = x * z$ and $y \neq z$ (for instance y, z two inverses of x), each equation checked.

A different counterexample to cancellation earns the 4 points if its table is given and the failure of associativity is shown. Fatal errors (0 for the step): naming line (2) or line (4); a counterexample that is associative, or that has no identity, or whose element x is not invertible.

Exercise. C3: Transport by a bijection

Let $\varphi\colon X \to Y$ be a bijection, and let $*$ be an operation on Y. For $x, x' \in X$, define

$$x \star x' := \varphi^{-1}(\varphi(x) * \varphi(x')).$$

(a) Show that $\star$ is an operation on X with $\varphi(x \star x') = \varphi(x) * \varphi(x')$ for all $x, x' \in X$.

(b) Show that $\star$ is associative if and only if $*$ is.

(c) Compute $\star$ for $X = Y = \mathbb{R}$, $\varphi(x) = 1 - x$ and $* = \cdot$.

Solution.

(a) The inverse function $\varphi^{-1}\colon Y \to X$ exists by Theorem 1.6.4, so the right-hand side is one element of X for each pair, and $\star$ is an operation on X. Applying φ and using $\varphi \circ \varphi^{-1} = \mathrm{id}_Y$ (Definition 1.6.2) gives $\varphi(x \star x') = \varphi(x) * \varphi(x')$.

(b) ($\Leftarrow$) Let $*$ be associative and $x, y, z \in X$. By (a), applied twice on each side,

$$\varphi((x \star y) \star z) = (\varphi(x) * \varphi(y)) * \varphi(z) = \varphi(x) * (\varphi(y) * \varphi(z)) = \varphi(x \star (y \star z)),$$

and φ is injective, so $(x \star y) \star z = x \star (y \star z)$. ($\Rightarrow$) Let $\star$ be associative and $u, v, w \in Y$. Since φ is surjective, $u = \varphi(x)$, $v = \varphi(y)$, $w = \varphi(z)$ for some $x, y, z \in X$, and the same display read from the outside in gives $(u*v)*w = \varphi((x\star y)\star z) = \varphi(x\star(y\star z)) = u*(v*w)$.

(c) $\varphi \circ \varphi = \mathrm{id}_{\mathbb{R}}$, since $1-(1-x)=x$, so $\varphi^{-1}=\varphi$ (Definition 1.6.2). Hence

$$x \star x' = 1-(1-x)(1-x') = x + x' - xx',$$

the operation of Exercise B1. Its identity $0=\varphi(1)$ and its one non-invertible element $1=\varphi(0)$ are the images of the identity 1 and of the non-invertible 0 of multiplication.

5.4 Permutations and Iteration

Sections 5.1–5.3 built new functions from old ones: by cutting a domain down, by gluing pieces together, by passing to a quotient, and by combining two functions with an operation. This section does the simplest thing that can be done with a function whose codomain is its own domain: it applies the function again, and again. For a bijection, going forwards and backwards sorts the set into orbits, and on a finite set each orbit is a cycle. We prove that a bijection of a finite set, repeated often enough, gives back the identity, and we say after how many steps. Then we see what is left of this when the map is not a bijection.

5.4.1 Shuffling twelve cards

Lay twelve cards in a row and number the positions $0, 1, \ldots, 11$. Cut the row into three piles of four: positions 0–3, positions 4–7, positions 8–11. Now deal them back: take the first card of each pile in turn, then the second card of each pile, and so on. The new row holds the cards from the old positions

$$0,\ 4,\ 8,\ 1,\ 5,\ 9,\ 2,\ 6,\ 10,\ 3,\ 7,\ 11,$$

in that order. So the card that was at position 4 is now at position 1, and the card that was at position 1 is now at position 3.

The card at old position i moves to the new position $\sigma(i)$, where

$$\sigma(i) = \begin{cases} 3i & \text{if } 0 \le i \le 3, \\ 3i-11 & \text{if } 4 \le i \le 7, \\ 3i-22 & \text{if } 8 \le i \le 11. \end{cases}$$

Check one card from each pile: card 2 lands at 6, card 5 at $15-11=4$, card 10 at $30-22=8$, as the row above says. The three pieces $\{0,\ldots,3\}$, $\{4,\ldots,7\}$, $\{8,\ldots,11\}$ are disjoint and cover the positions, so σ is a gluing with nothing to check on overlaps (Example (Method: define a function by gluing)).

Now shuffle again by the same rule. After two shuffles the card from position i is at $\sigma(\sigma(i))$. Follow card 1 through the shuffles: it goes to 3, then 9, then $27-22=5$, then $15-11=4$, then $12-11=1$. Card 2 goes to 6, 7, 10, 8, and back to 2. Cards 0 and 11 never move. These are $1+1+5+5=12$ cards, every card of the deck, and each is back in its place after five shuffles. The deck is in its starting order.

Was that luck? Three questions organize the section. Does **every** shuffle of a finite deck, repeated, bring the deck back? After how many shuffles? And what is left of the answer when the rule is not a shuffle, for instance when it sends two positions to one?

5.4.2 Permutations and iterates

A shuffle sends every position to a position, sends no two positions to the same one, and fills every position. That is a bijection from the set of positions to itself.

Definition 5.4.1. Permutation

Let X be a set. A **permutation** of X is a bijection $\sigma\colon X \to X$. The set of all permutations of X is written S_X; it is a subset of X^X, the set of all functions $X \to X$.

For a finite set, a function $X \to X$ can be written as a **two-line table**: the elements of X in the top row, and under each element its image. For instance,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

is the function on $\{1,2,3\}$ with $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$. It is a table, not a matrix: nothing is multiplied. Such a function is a permutation exactly when its bottom row lists every element of X once: "every element appears" is surjectivity, and "no element twice" is injectivity. The hook's shuffle is the table with top row $0,\dots,11$ and bottom row $0,3,6,9,1,4,7,10,2,5,8,11$. The two permutations of $\{1,2\}$ are the identity and the swap $1 \mapsto 2$, $2 \mapsto 1$.

Section 5.3 made composition an operation on X^X (Proposition 5.3.5). The permutations are closed under it, and they keep everything that operation has.

Proposition 5.4.1. Permutations under Composition

Let X be a set.

(a) If $\sigma, \tau \in S_X$, then $\sigma \circ \tau \in S_X$.
(b) $\mathrm{id}_X \in S_X$.
(c) If $\sigma \in S_X$, then $\sigma^{-1} \in S_X$, and $\sigma \circ \sigma^{-1} = \mathrm{id}_X = \sigma^{-1} \circ \sigma$.

Hence S_X is closed under $\circ$, and $\circ$ is an associative operation on S_X with identity id_X, in which every element σ is invertible, with inverse σ^{-1}.

Proof.

(a) is Theorem 1.5.4 (c). (b) $\mathrm{id}_X \circ \mathrm{id}_X = \mathrm{id}_X$, so id_X is a two-sided inverse of itself, and it is bijective by Theorem 1.6.4. (c) Since σ is bijective, it has the inverse σ^{-1} with $\sigma^{-1} \circ \sigma = \mathrm{id}_X$ and $\sigma \circ \sigma^{-1} = \mathrm{id}_X$ (Theorem 1.6.4, Definition 1.6.2). Read the other way round, the same two equations say that σ is a two-sided inverse of σ^{-1}, so σ^{-1} is bijective by Theorem 1.6.4.

By (a), S_X is closed under $\circ$, so $\circ$ restricted to $S_X \times S_X$ is an operation on S_X (Definition 5.3.1). Associativity holds on all of X^X (Proposition 5.3.5), so in particular on S_X; id_X lies in S_X by (b) and is an identity there; and by (c) each $\sigma \in S_X$ has an inverse σ^{-1} that lies in S_X.

■

So everything Section 5.3 proved for an associative operation with an identity applies to S_X.

For instance, Proposition 5.3.3 (c) gives $(\sigma \circ \tau)^{-1} = \tau^{-1} \circ \sigma^{-1}$: undo the second shuffle first.

Composing a function with itself needs only that its codomain is its domain; bijectivity is not needed. Shuffling twice is $\sigma \circ \sigma$, and "apply f a total of n times" is a definition by recursion.

Definition 5.4.2. Iterates

Let X be a set and $f\colon X \to X$. The **iterates** $f^n\colon X \to X$, for $n \in \mathbb{N}$, are defined by

$$f^0 := \mathrm{id}_X, \qquad f^{n+1} := f \circ f^n.$$

For $\sigma \in S_X$ and $n \in \mathbb{N}$, we also set $\sigma^{-n} := (\sigma^{-1})^n$.

The definition is an instance of Theorem 2.3.1, applied to the set X^X with the starting value id_X and the step $g\colon \mathbb{N} \times X^X \to X^X$, $g(n, h) := f \circ h$: there is exactly one sequence $n \mapsto f^n$ in X^X with these two properties. Unwinding, $f^1 = f \circ \mathrm{id}_X = f$, $f^2 = f \circ f$, $f^3 = f \circ (f \circ f)$, and $f^n(x)$ is "apply f to x, n times". For a permutation the two clauses do not clash: $\sigma^{-0} = (\sigma^{-1})^0 = \mathrm{id}_X = \sigma^0$, and $(\sigma^{-1})^1 = \sigma^{-1}$ is the inverse function. So σ^k has one meaning for every $k \in \mathbb{Z}$. As Section 5.3 warned, f^n is always an iterate in this book, never the pointwise power $x \mapsto f(x)^n$.

The definition adds one f at a time, on the left. The first thing to prove is that blocks of f's can be moved around as the notation suggests.

Proposition 5.4.2. Laws of Iterates

Let X be a set, $f\colon X \to X$, and $m, n \in \mathbb{N}$.

(a) $f^{m+n} = f^m \circ f^n$.

(b) $(f^m)^n = f^{mn}$.

(c) If $\sigma \in S_X$, then $\sigma^k \in S_X$ for every $k \in \mathbb{Z}$; $\sigma^n \circ \sigma^{-n} = \mathrm{id}_X = \sigma^{-n} \circ \sigma^n$; and $\sigma^{k+l} = \sigma^k \circ \sigma^l$ for all $k, l \in \mathbb{Z}$.

Idea. Each law is an equation between iterates, and the definition only tells us how to peel one f off the left. So we induct on the exponent that appears first, peel one f, and use the induction hypothesis on what is left. For (c) the new feature is the sign: σ^{-n} undoes σ^n, and a mixed sum $k + l$ is handled by canceling the overlap.

Proof.

(a) Fix n and induct on m (Logic and Proof, Axiom 4.2.1). For $m = 0$, $f^{0+n} = f^n = \mathrm{id}_X \circ f^n = f^0 \circ f^n$ by Proposition 1.5.3. Suppose $f^{m+n} = f^m \circ f^n$. Then, by Definition 5.4.2, the induction hypothesis and Proposition 1.5.3,

$$f^{(m+1)+n} = f \circ f^{m+n} = f \circ (f^m \circ f^n) = (f \circ f^m) \circ f^n = f^{m+1} \circ f^n.$$

(b) Induct on n. For $n = 0$, $(f^m)^0 = \mathrm{id}_X = f^0 = f^{m \cdot 0}$. If $(f^m)^n = f^{mn}$, then $(f^m)^{n+1} = f^m \circ (f^m)^n = f^m \circ f^{mn} = f^{m+mn}$ by (a), and $m + mn = m(n + 1)$.

(c) First, $\sigma^n \in S_X$ for $n \in \mathbb{N}$, by induction: $\sigma^0 = \mathrm{id}_X \in S_X$, and $\sigma^{n+1} = \sigma \circ \sigma^n \in S_X$ by Proposition 5.4.1 (a). Since $\sigma^{-1} \in S_X$ (Proposition 5.4.1 (c)), the same induction gives $\sigma^{-n} = (\sigma^{-1})^n \in S_X$. So $\sigma^k \in S_X$ for every $k \in \mathbb{Z}$.

Next, $\sigma^n \circ \sigma^{-n} = \mathrm{id}_X$, by induction on n. For $n = 0$ both factors are id_X. If it holds for n, then $\sigma^{n+1} = \sigma^n \circ \sigma$ by (a) with the exponents n and 1, and $\sigma^{-(n+1)} = \sigma^{-1} \circ \sigma^{-n}$ by Definition 5.4.2, so

$$\sigma^{n+1} \circ \sigma^{-(n+1)} = \sigma^n \circ (\sigma \circ \sigma^{-1}) \circ \sigma^{-n} = \sigma^n \circ \sigma^{-n} = \mathrm{id}_X,$$

by Proposition 1.5.3 and Proposition 5.4.1 (c). The equation $\sigma^{-n} \circ \sigma^n = \mathrm{id}_X$ is the same induction with the roles of σ and σ^{-1} exchanged.

Finally, $\sigma^{k+l} = \sigma^k \circ \sigma^l$. When $k, l \geq 0$ this is (a). When $k, l \leq 0$, it is (a) for the map σ^{-1} with the exponents $-k$ and $-l$. The cases with k and l of opposite signs reduce to these two by canceling, as the second reading below shows.

■

Second reading · *The mixed signs in (c)*

Let k and l have opposite signs. All equalities below use Proposition 1.5.3, the cases of (c) already proved, and $\sigma^n \circ \sigma^{-n} = \mathrm{id}_X = \sigma^{-n} \circ \sigma^n$ for $n \in \mathbb{N}$.

Case $k \geq 0$, $l = -b$ with $b > 0$. If $k \geq b$, then $\sigma^k = \sigma^{k-b} \circ \sigma^b$ by (a), so $\sigma^k \circ \sigma^{-b} = \sigma^{k-b} \circ (\sigma^b \circ \sigma^{-b}) = \sigma^{k-b}$. If $k < b$, then $\sigma^{-b} = \sigma^{-k} \circ \sigma^{-(b-k)}$ by (a) for σ^{-1}, so $\sigma^k \circ \sigma^{-b} = (\sigma^k \circ \sigma^{-k}) \circ \sigma^{-(b-k)} = \sigma^{k-b}$. In both cases $\sigma^k \circ \sigma^l = \sigma^{k+l}$.

Case $k = -a$ with $a > 0$, $l \geq 0$. If $l \geq a$, then $\sigma^l = \sigma^a \circ \sigma^{l-a}$ by (a), so $\sigma^{-a} \circ \sigma^l = (\sigma^{-a} \circ \sigma^a) \circ \sigma^{l-a} = \sigma^{l-a}$. If $l < a$, then $\sigma^{-a} = \sigma^{-(a-l)} \circ \sigma^{-l}$ by (a) for σ^{-1}, so $\sigma^{-a} \circ \sigma^l = \sigma^{-(a-l)} \circ (\sigma^{-l} \circ \sigma^l) = \sigma^{l-a}$. Again $\sigma^k \circ \sigma^l = \sigma^{k+l}$.

In particular σ^{-n} is the inverse of σ^n, by the middle clause of (c) and Definition 1.6.2: shuffling backwards n times undoes shuffling forwards n times.

Quick check. For $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x + 3$, find f^n and prove your answer.

Solution. $f^n(x) = x + 3n$. By induction on n: $f^0(x) = x = x + 3 \cdot 0$; and if $f^n(x) = x + 3n$, then $f^{n+1}(x) = f(f^n(x)) = (x + 3n) + 3 = x + 3(n + 1)$ by Definition 5.4.2. Here f^n is not the power $(x + 3)^n$.

5.4.3 Orbits

In the hook, the cards fell into sets that move among themselves: $\{1, 3, 9, 5, 4\}$, $\{2, 6, 7, 10, 8\}$, $\{0\}$ and $\{11\}$. The natural guess for "in the same set" is "one card reaches the other": $y = f^n(x)$ for some $n \in \mathbb{N}$. This relation is reflexive ($n = 0$) and transitive (add the exponents, Proposition 5.4.2 (a)). It is not symmetric. For $f\colon \mathbb{N} \to \mathbb{N}$, $f(n) = n + 1$, the point 0 reaches $1 = f(0)$, but 1 never reaches 0, since $f^n(1) = 1 + n \geq 1$. So reachability does not cut a set into pieces. For a permutation the repair is to allow negative exponents: walk backwards as well as forwards.

The orbit of a point is everywhere a permutation can take it, forwards or backwards.

Definition 5.4.3. Orbit, Forward Orbit, Fixed Point

Let X be a set and $\sigma \in S_X$. For $x, y \in X$, let $x \sim_\sigma y$ mean that $y = \sigma^k(x)$ for **some** $k \in \mathbb{Z}$. The **orbit** of x under σ is

$$O_\sigma(x) := \{\sigma^k(x) : k \in \mathbb{Z}\}.$$

For an arbitrary function $f\colon X \to X$, the **forward orbit** of x is $\{f^n(x) : n \in \mathbb{N}\}$. A **fixed point** of f is an $x \in X$ with $f(x) = x$.

In words: the orbit collects every point reached from x by applying σ or σ^{-1} any number of times; the forward orbit uses f only, so it makes sense for every self-map. For a permutation, the forward orbit of x is contained in $O_\sigma(x)$, since $\mathbb{N} \subseteq \mathbb{Z}$; on a finite set the two are equal, as the next subsection proves. A fixed point is a point the map does not move, the sense in which Section 3.4 called 0 a fixed point of a bijection. For the hook's shuffle, $O_\sigma(1) = \{1, 3, 9, 5, 4\}$: since $\sigma^5(1) = 1$, the negative powers give nothing new ($\sigma^{-1}(1) = \sigma^4(1)$, and so on; Proposition 5.4.4 proves this in general), and 0 and 11 are the fixed points.

Warning. Forward orbits need not cut a set into pieces. For $f(n) = n + 1$ on $\mathbb{N}$, the forward orbit of 0 is $\mathbb{N}$ and that of 1 is $\{n \in \mathbb{N} : n \geq 1\}$: they overlap and are not equal. Only orbits of a **permutation**, with k running over $\mathbb{Z}$, are guaranteed to be disjoint or equal.

The guarantee is the next theorem: $\sim_\sigma$ is an equivalence relation, and the orbits are its classes.

Theorem 5.4.3. The Orbits of a Permutation Partition the Set

Let X be a set and $\sigma \in S_X$. Then $\sim_\sigma$ is an equivalence relation on X, and the class of each $x \in X$ is $O_\sigma(x)$. Hence the orbits of σ form a partition of X. Moreover, x is a fixed point of σ if and only if $O_\sigma(x) = \{x\}$.

Proof. We check (Eq1)–(Eq3) of Definition 4.2.1, using Proposition 5.4.2 (c) throughout. (Eq1): $x = \sigma^0(x)$, so $x \sim_\sigma x$. (Eq2): if $y = \sigma^k(x)$, then $\sigma^{-k}(y) = \sigma^{-k}(\sigma^k(x)) = \sigma^{-k+k}(x) = \sigma^0(x) = x$, so $y \sim_\sigma x$. (Eq3): if $y = \sigma^k(x)$ and $z = \sigma^l(y)$, then $z = \sigma^l(\sigma^k(x)) = \sigma^{l+k}(x)$ and $l + k \in \mathbb{Z}$, so $x \sim_\sigma z$.

The class of x is $\{y \in X : y \sim_\sigma x\}$ (Definition 4.2.2), which by (Eq2) is $\{y \in X : x \sim_\sigma y\} = \{\sigma^k(x) : k \in \mathbb{Z}\} = O_\sigma(x)$. By Theorem 4.2.1 (d), the classes form a partition of X.

If $O_\sigma(x) = \{x\}$, then $\sigma(x) = \sigma^1(x) \in O_\sigma(x)$, so $\sigma(x) = x$. Conversely, let $\sigma(x) = x$. Then $\sigma^n(x) = x$ for every $n \in \mathbb{N}$, by induction: $\sigma^{n+1}(x) = \sigma(\sigma^n(x)) = \sigma(x) = x$. Also $\sigma^{-1}(x) = \sigma^{-1}(\sigma(x)) = x$, so x is a fixed point of σ^{-1}, and the same induction gives $\sigma^{-n}(x) = (\sigma^{-1})^n(x) = x$. Hence $\sigma^k(x) = x$ for every $k \in \mathbb{Z}$, and $O_\sigma(x) = \{x\}$.

■

The theorem answers the hook's first observation: the cards always fall into sets that move among themselves, because the orbits are the classes of an equivalence relation, and each card lies in exactly one class.

Quick check. Find the orbits of $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$.

Solution. From 1: $1 \mapsto 3 \mapsto 1$, so $O_\sigma(1) = \{1, 3\}$ (going backwards, $\sigma^{-1}(1) = 3$, gives nothing new). From 2: $2 \mapsto 5 \mapsto 4 \mapsto 2$, so $O_\sigma(2) = \{2, 5, 4\}$. These two orbits are disjoint and cover $\{1, \dots, 5\}$, as Theorem 5.4.3 says they must; σ has no fixed point.

5.4.4 Following an orbit

In the hook, card 1 came back after five shuffles and card 0 after one. On a finite set this always happens, and the first return controls everything else about the orbit.

Proposition 5.4.4. Following an Orbit

Let X be a finite set, $\sigma \in S_X$, and $x \in X$. Then there is a **least** integer $k \geq 1$ with $\sigma^k(x) = x$. For this k:

(a) the points $x, \sigma(x), \dots, \sigma^{k-1}(x)$ are distinct;
(b) $O_\sigma(x) = \{x, \sigma(x), \dots, \sigma^{k-1}(x)\}$, so $O_\sigma(x)$ has exactly k elements;
(c) for every $m \in \mathbb{Z}$, $\sigma^m(x) = x$ if and only if $k \mid m$.

The number k is the **length** of the orbit $O_\sigma(x)$.

Idea (Scratch work). The set is finite and the forward orbit $x, \sigma(x), \sigma^2(x), \dots$ is an infinite list, so the list must repeat. A repeat is not yet a return to x: we need to cancel the front of it, and that is where injectivity comes in.

Givens	Goal
X has n elements; σ bijective	some $k \geq 1$ with $\sigma^k(x) = x$
the $n+1$ points $\sigma^0(x), \dots, \sigma^n(x)$	two of them equal: $m \mapsto \sigma^{m-1}(x)$ on $\{1, \dots, n+1\}$ is not injective (Corollary 2.5.3 (a))
$\sigma^i(x) = \sigma^j(x)$ with $0 \leq i < j \leq n$; $\sigma^j = \sigma^i \circ \sigma^{j-i}$	cancel σ^i, which is injective (Proposition 5.4.2 (c)): $k = j - i$ works
a non-empty set of such k	a least one (Theorem 2.1.3)

Once there is a least return time, (a) is minimality again, and (c) is division with remainder: m full rounds plus a part of a round.

Proof. Let X have n elements. The set $\{1, \dots, n+1\}$ has $n+1$ elements, so the function $\{1, \dots, n+1\} \to X$, $m \mapsto \sigma^{m-1}(x)$, is not injective (Corollary 2.5.3 (a)). So there are integers $0 \leq i < j \leq n$ with $\sigma^i(x) = \sigma^j(x)$. By Proposition 5.4.2 (c), $\sigma^j = \sigma^i \circ \sigma^{j-i}$, so $\sigma^i(\sigma^{j-i}(x)) = \sigma^i(x)$, and since $\sigma^i \in S_X$ is injective, $\sigma^{j-i}(x) = x$. Hence the set $K := \{k \in$

$\mathbb{N} : k \geq 1$ and $\sigma^k(x) = x\}$ contains $j - i$, and by Theorem 2.1.3 it has a least element k.

(a) Suppose $\sigma^i(x) = \sigma^j(x)$ with $0 \leq i < j < k$. As above, $\sigma^{j-i}(x) = x$, with $1 \leq j - i < k$, so $j - i \in K$, against the choice of k. So the k points are distinct.

(b) First, $\sigma^{qk}(x) = x$ for every $q \in \mathbb{Z}$. For $q \geq 0$, by induction on q: $\sigma^0(x) = x$, and $\sigma^{(q+1)k}(x) = \sigma^k(\sigma^{qk}(x)) = \sigma^k(x) = x$ by Proposition 5.4.2 (c). For $q < 0$, $-q > 0$, so $\sigma^{-qk}(x) = x$ by the case just proved, and $\sigma^{qk}(x) = \sigma^{qk}(\sigma^{-qk}(x)) = \sigma^0(x) = x$. Now let $m \in \mathbb{Z}$, and write $m = qk + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < k$ (Theorem 2.2.3). Then

$$\sigma^m(x) = \sigma^r(\sigma^{qk}(x)) = \sigma^r(x).$$

If $r = 0$, this is x. If $1 \leq r < k$, then $\sigma^r(x) \neq x$, since otherwise $r \in K$ and $r < k$. So $\sigma^m(x) = x$ if and only if $r = 0$. By the uniqueness in Theorem 2.2.3, $r = 0$ holds exactly when $m = q'k$ for some $q' \in \mathbb{Z}$, that is, when $k \mid m$.

(c) The display shows that every point $\sigma^m(x)$ of the orbit is one of $\sigma^0(x), \ldots, \sigma^{k-1}(x)$; conversely each of these lies in the orbit. By (a), $\{1, \ldots, k\} \to O_\sigma(x)$, $j \mapsto \sigma^{j-1}(x)$, is injective, and it is onto by what was just shown; so $O_\sigma(x)$ has k elements (Definition 2.5.2).

■

Two things to take from the proof. The forward orbit already contains $x, \sigma(x), \ldots, \sigma^{k-1}(x)$, so on a finite set it equals the orbit: walking forwards reaches every point that walking backwards does. And in the existence of a return, the hypothesis "σ is a permutation" was used once, in the cancellation of σ^i; the rest of the proof needs negative powers only because the orbit is defined with them. The last subsection shows what goes wrong without it. The argument is a method in its own right.

Example. Method: follow an orbit

Template. (1) List the forward orbit $x, f(x), f^2(x), \ldots$. (2) On a finite set of n elements, two of the first $n+1$ terms are equal (Corollary 2.5.3). (3) Take the first repeat, or the least return time (Theorem 2.1.3). (4) Carry the repeat with the map's structure: cancel if the map is injective; push forward with $f^{l+1} = f \circ f^l$ always.

When to use it. Repeated application of one map on a finite set: shuffles, the tick of a clock, maps on $\mathbb{Z}/n$.

The usual failure. Speaking of "the first repeat" without proving that a repeat exists; canceling a map that is not injective, which forgets the tail before the cycle.

Now the hook, in full.

Example. The three-pile shuffle

Let σ be the shuffle of twelve cards in three piles of four. Show that σ is a permutation of $\{0, \ldots, 11\}$, find its orbits and their lengths, and find the least $N \geq 1$ with $\sigma^N = \mathrm{id}$.

Solution. A formula. Write $i = 4p + r$ with $0 \leq r < 4$ (Theorem 2.2.3); for $0 \leq i \leq 11$, $p \in \{0, 1, 2\}$ is the pile and r the place in it. The card is dealt in round r (counting from 0),

after the p cards of that round from the earlier piles, so $\sigma(i) = 3r + p$; the three cases of the hook are $p = 0, 1, 2$.

A permutation. Every $j \in \{0, \dots, 11\}$ is $3r + p$ for exactly one pair with $0 \le p < 3$, by Theorem 2.2.3, and then $0 \le r \le 3$, because $-3 < j - p = 3r \le 11$. So $3r + p \mapsto 4p + r$ is a function $\{0, \dots, 11\} \to \{0, \dots, 11\}$, and it undoes σ on both sides. By Theorem 1.6.4, $\sigma \in S_X$ for $X = \{0, \dots, 11\}$.

Arithmetic modulo 11. $3i - \sigma(i) = 12p + 3r - 3r - p = 11p$, so $\sigma(i) \equiv 3i \pmod{11}$. For $i \le 10$, $\sigma(i) \neq 11$, since $3r + p = 11$ forces $r = 3$, $p = 2$, that is $i = 11$. So for $i \le 10$, $3i = 11p + \sigma(i)$ with $0 \le \sigma(i) < 11$, and $\sigma(i)$ is the remainder of $3i$ on division by 11 by the uniqueness in Theorem 2.2.3; and $\sigma(11) = 11$.

Orbits. Follow each orbit (Example (Method: follow an orbit)), reducing modulo 11:

$$1 \mapsto 3 \mapsto 9 \mapsto 5 \mapsto 4 \mapsto 1 \quad (27 \equiv 5,\ 15 \equiv 4,\ 12 \equiv 1),$$
$$2 \mapsto 6 \mapsto 7 \mapsto 10 \mapsto 8 \mapsto 2 \quad (18 \equiv 7,\ 21 \equiv 10,\ 30 \equiv 8,\ 24 \equiv 2),$$

and 0, 11 are fixed. The orbits are $\{0\}$, $\{11\}$, $\{1, 3, 9, 5, 4\}$, $\{2, 6, 7, 10, 8\}$, of lengths $1, 1, 5, 5$.

The return. Each length divides 5, so $\sigma^5(x) = x$ for every x by Proposition 5.4.4 (c), and $\sigma^5 = \mathrm{id}$ by Proposition 1.5.1. For $1 \le N < 5$, $5 \nmid N$, so $\sigma^N(1) \neq 1$ by the same part (c). Hence $N = 5$. The arithmetic agrees: $3^5 = 243 = 22 \cdot 11 + 1$, so five shuffles multiply every position below 11 by 1 modulo 11.

Quick check. Let $t\colon \mathbb{Z}/12 \to \mathbb{Z}/12$, $[a] \mapsto [a + 1]$, be the tick of Example (Maps out of the clock). What is the length of the orbit of $[1]$ under t? And under $[a] \mapsto [a + 3]$?

Solution. By induction, $t^m([1]) = [1 + m]$ for $m \in \mathbb{N}$, and $[1 + m] = [1]$ exactly when $12 \mid m$ (Theorem 4.2.1 (b), Definition 4.2.5). The least $m \ge 1$ is 12: the orbit is all of $\mathbb{Z}/12$, of length 12. The map $[a] \mapsto [a + 3]$ is well defined as the tick is $((a + 3) - (a' + 3) = a - a')$, and is a permutation with inverse $[a] \mapsto [a - 3]$. From $[1]$: $[1], [4], [7], [10], [13] = [1]$. The orbit is $\{[1], [4], [7], [10]\}$, of length 4.

5.4.5 Cycles

The hook's shuffle moves $1, 3, 9, 5, 4$ round in a ring, moves $2, 6, 7, 10, 8$ round in another ring, and leaves everything else alone. A permutation that moves one ring and nothing else deserves a name and a notation.

Definition 5.4.4. Cycle

Let X be a set, $k \ge 2$, and $x_1, \dots, x_k \in X$ **distinct**. The **cycle** $(x_1\ x_2\ \cdots\ x_k)$ is the function $X \to X$ that sends $x_j \mapsto x_{j+1}$ for $1 \le j < k$, sends $x_k \mapsto x_1$, and sends every other point of X to itself. Two cycles are **disjoint** if their sets of entries are disjoint.

The cycle is defined by gluing (Example (Method: define a function by gluing)): the pieces $\{x_1, \dots, x_k\}$ and its complement are disjoint and cover X, so there are no overlaps to check. On

the first piece the rule reads the index j of a point, and distinctness makes that index unique. On the second piece the rule is the identity. A cycle is a permutation: $(x_k \ \cdots \ x_2 \ x_1)$ sends $x_{j+1} \mapsto x_j$ and $x_1 \mapsto x_k$, so composing it with $(x_1 \ \cdots \ x_k)$ in either order fixes each x_j, and it fixes each point off the entries since both factors do. By Theorem 1.6.4 the cycle is bijective, with inverse the reversed cycle. The same cycle has k names: $(1\ 3\ 9\ 5\ 4) = (3\ 9\ 5\ 4\ 1)$, since both send each entry to the next one round the ring.

The theorem below says that every permutation of a finite set is built from its orbits in this way: one cycle for each orbit with at least two points. Before stating it, note that such orbits are finitely many. Let X have n elements via a bijection $\varphi\colon \{1,\dots,n\} \to X$. Send each orbit O to the least i with $\varphi(i) \in O$ (Theorem 2.1.3). Distinct orbits are disjoint (Theorem 5.4.3), so they get distinct indices, and the orbits are in bijection with a subset of $\{1,\dots,n\}$, which is finite (Proposition 2.5.6).

Theorem 5.4.5. Cycle Decomposition

Let X be a finite set and $\sigma \in S_X$. Let $O_1,\dots,O_r$ be the distinct orbits of σ with at least two elements, choose $x_i \in O_i$, let k_i be the number of elements of O_i (so $|O_i| = k_i$), and let

$$\gamma_i \coloneqq (x_i \ \ \sigma(x_i) \ \ \cdots \ \ \sigma^{k_i-1}(x_i)).$$

Then $\gamma_1,\dots,\gamma_r$ are pairwise disjoint cycles, $\gamma_i \circ \gamma_j = \gamma_j \circ \gamma_i$ for all i, j, and

$$\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_r,$$

bracketed from the left; if $r = 0$, this says $\sigma = \mathrm{id}_X$.

Idea. Both sides are functions on X, so we compare values (Proposition 1.5.1). A point of O_i is moved by γ_i exactly as σ moves it, and is left alone by every other γ_j. So composing the cycles one at a time, the composite agrees with σ on more and more orbits; an induction on the number of cycles composed makes that precise.

Proof. By Proposition 5.4.4, $O_i = \{x_i, \sigma(x_i), \dots, \sigma^{k_i-1}(x_i)\}$ and these $k_i \geq 2$ points are distinct, so γ_i is a cycle whose set of entries is O_i. Distinct orbits are disjoint (Theorem 5.4.3), so the cycles are pairwise disjoint.

The key value. Let $y \in O_i$, say $y = \sigma^m(x_i)$ with $0 \leq m < k_i$. If $m < k_i - 1$, then $\gamma_i(y) = \sigma^{m+1}(x_i) = \sigma(y)$ by Definition 5.4.2. If $m = k_i - 1$, then $\gamma_i(y) = x_i = \sigma^{k_i}(x_i) = \sigma(y)$. So $\gamma_i(y) = \sigma(y)$ for every $y \in O_i$; and $\sigma(y) = \sigma^{m+1}(x_i) \in O_i$. For $j \neq i$, γ_j fixes every point of O_i, since $O_i \cap O_j = \emptyset$.

Define $\delta^{(0)} \coloneqq \mathrm{id}_X$ and $\delta^{(j)} \coloneqq \delta^{(j-1)} \circ \gamma_j$ for $1 \leq j \leq r$, by recursion (Theorem 2.3.1, with $\gamma_j \coloneqq \mathrm{id}_X$ for $j > r$). So $\delta^{(r)}$ is the composite of the theorem, bracketed from the left. Let $U_j \coloneqq O_1 \cup \cdots \cup O_j$. We prove by induction on $j \leq r$:

$$\delta^{(j)}(y) = \sigma(y) \ \text{ for } y \in U_j, \qquad \delta^{(j)}(y) = y \ \text{ for } y \in X \setminus U_j.$$

For $j = 0$, $U_0 = \emptyset$ and $\delta^{(0)} = \mathrm{id}_X$. Suppose the claim holds for $j-1$, and let $y \in X$. If $y \in O_j$, then $\gamma_j(y) = \sigma(y) \in O_j$, and O_j is disjoint from U_{j-1}, so $\delta^{(j)}(y) = \delta^{(j-1)}(\sigma(y)) = \sigma(y)$. If $y \notin O_j$, then $\gamma_j(y) = y$, so $\delta^{(j)}(y) = \delta^{(j-1)}(y)$; and since $y \notin O_j$, $y \in U_j$ exactly when $y \in U_{j-1}$. In both cases the claim holds for j.

For $j = r$: a point y outside U_r lies in an orbit with fewer than two elements, so $O_\sigma(y) = \{y\}$ and $\sigma(y) = y$ (Theorem 5.4.3). Hence $\delta^{(r)}(y) = \sigma(y)$ for every $y \in X$, and $\delta^{(r)} = \sigma$ by Proposition 1.5.1. That disjoint cycles commute is a check of values at a point of O_i, of O_j, and of neither, which the second reading below carries out.

■

Second reading · *Disjoint cycles commute*

Let $i \neq j$ and $y \in X$. If $y \in O_i$, then $\gamma_j(y) = y$, so $\gamma_i(\gamma_j(y)) = \gamma_i(y) = \sigma(y)$; and $\gamma_i(y) = \sigma(y) \in O_i$ is fixed by γ_j, so $\gamma_j(\gamma_i(y)) = \sigma(y)$. If $y \in O_j$, the same two lines with i and j exchanged give $\sigma(y)$ on both sides. If y lies in neither, both cycles fix it, and both composites give y. So $\gamma_i \circ \gamma_j = \gamma_j \circ \gamma_i$ by Proposition 1.5.1. For $i = j$ there is nothing to prove.

From now on we write $\gamma\delta$ for $\gamma \circ \delta$, the right factor applied first, the convention of *Algebraic Preliminaries*, Chapter 2. Two examples. The three-pile shuffle of Example (The three-pile shuffle) is

$$\sigma = (1\ 3\ 9\ 5\ 4)(2\ 6\ 7\ 10\ 8),$$

and the two factors may be written in either order. The tick of Example (Maps out of the clock) has one orbit, all of $\mathbb{Z}/12$, with $t^m([0]) = [m]$, so it is the single cycle $([0]\ [1]\ \cdots\ [11])$.

The decomposition answers the hook's second question. A permutation of a finite set comes back to the identity, and the orbit lengths say when.

Corollary 5.4.6. Some Power Is the Identity

Let X be a finite set and $\sigma \in S_X$. For an integer $N \geq 1$, $\sigma^N = \mathrm{id}_X$ if and only if the length of every orbit of σ divides N. There is such an N.

Proof. By Proposition 1.5.1, $\sigma^N = \mathrm{id}_X$ means $\sigma^N(x) = x$ for every $x \in X$, and by Proposition 5.4.4 (c) that holds exactly when the length k_x of $O_\sigma(x)$ divides N for every x. This proves the equivalence.

For existence, let X have n elements, and let $\varphi\colon \{1, \ldots, n\} \to X$ be a bijection (Definition 2.5.2), and let $N := \prod_{i=1}^{n} k_{\varphi(i)}$ (Definition 2.3.1). Each factor is an integer ≥ 1, so N is an integer ≥ 1. Write $P_j := \prod_{i=1}^{j} k_{\varphi(i)}$. For a fixed $i \leq n$, $k_{\varphi(i)} \mid P_j$ for every j with $i \leq j \leq n$, by induction on j: $P_i = P_{i-1}\, k_{\varphi(i)}$, and $P_j \mid P_{j+1} = P_j\, k_{\varphi(j+1)}$, so Proposition 1.1.1 carries the divisibility from P_j to P_{j+1}. Hence $k_x \mid P_n = N$ for every $x = \varphi(i) \in X$, and $\sigma^N = \mathrm{id}_X$ by the first part.

■

The **least** such N is the least positive common multiple of the orbit lengths: by the corollary, N works exactly when it is a common multiple of all of them. For two distinct lengths a and b, that least common multiple is the one found in Example (The supremum under divisibility is the least common multiple). For the three-pile shuffle the lengths are $1, 1, 5, 5$, and the answer is 5, as the hook found by hand.

Quick check. Decompose $[a] \mapsto [5a]$ on $\mathbb{Z}/12$ into disjoint cycles.

Solution. The map is well defined by Proposition 4.2.5. Applying it twice gives $[25a] = [a]$, since $25 \equiv 1 \pmod{12}$, so it is its own inverse and a permutation. Following orbits: $[1] \mapsto [5] \mapsto [25] = [1]$; $[2] \mapsto [10] \mapsto [50] = [2]$; $[4] \mapsto [20] = [8] \mapsto [40] = [4]$; $[7] \mapsto [35] = [11] \mapsto [55] = [7]$; and $[0], [3], [6], [9]$ are fixed ($15 \equiv 3$, $30 \equiv 6$, $45 \equiv 9$). So the map is ([1] [5])([2] [10])([4] [8])([7] [11]).

5.4.6 Maps that are not permutations

The last question of the hook: what if the rule sends two positions to one? Then there is no inverse, orbits in the sense of Definition 5.4.3 are not defined, and Proposition 5.4.4's cancellation is not available. Forward orbits still exist, and on a finite set they still repeat. What changes is that the repeat need not involve the starting point.

Proposition 5.4.7. Forward Orbits of a Self-Map of a Finite Set

Let X be a set with n elements, $f\colon X \to X$, and $x \in X$. There are integers $m \geq 0$ and $p \geq 1$ with $m + p \leq n$ such that

$$f^{l+p}(x) = f^{l}(x) \quad \text{for every integer } l \geq m.$$

Idea. This is Example (Method: follow an orbit) with step (4) done without canceling: the pigeonhole repeat $f^{i}(x) = f^{j}(x)$ cannot be pulled back to x, but it can be pushed forward, one application of f at a time.

Proof. As in the proof of Proposition 5.4.4, Corollary 2.5.3 (a) gives integers $0 \leq i < j \leq n$ with $f^{i}(x) = f^{j}(x)$. Let $m := i$ and $p := j - i \geq 1$; then $m + p = j \leq n$. We prove $f^{l+p}(x) = f^{l}(x)$ by induction on $l \geq m$ (Theorem 2.2.1). For $l = m$ it is $f^{j}(x) = f^{i}(x)$. If it holds for l, then by Definition 5.4.2

$$f^{l+1+p}(x) = f(f^{l+p}(x)) = f(f^{l}(x)) = f^{l+1}(x).$$

■

The forward orbit of x is thus a **tail** $x, f(x), \ldots, f^{m-1}(x)$ followed by a **cycle** that repeats with period p. For a permutation the tail can be taken empty: $m = 0$ and $p = k$, the length of $O_{\sigma}(x)$, work, by Proposition 5.4.4 (c). Without injectivity it need not be.

Example. Squaring on an eleven-hour clock

Let $s\colon \mathbb{Z}/11 \to \mathbb{Z}/11$, $s([a]) := [a^2]$. Show that s is well defined, follow the forward orbit of $[2]$, and find m and p. Does $[2]$ ever come back?

Solution. *Well defined.* If $a \equiv a' \pmod{11}$, then $a \cdot a \equiv a' \cdot a'$ by the product clause of Proposition 4.2.5: the rule $a \mapsto [a^2]$ is constant on classes (Example (Method: define a function on a quotient)).

The orbit. Squaring and reducing modulo 11:

$$[2] \mapsto [4] \mapsto [16] = [5] \mapsto [25] = [3] \mapsto [9] \mapsto [81] = [4],$$

using $16 - 11 = 5$, $25 - 22 = 3$, $81 - 77 = 4$. So $s^5([2]) = [4] = s^1([2])$, with $s^1([2]), \dots, s^4([2])$ distinct: the tail is $[2]$, and the cycle is $[4], [5], [3], [9]$, so $m = 1$ and $p = 4$.

No return. The set $C = \{[4], [5], [3], [9]\}$ contains $s([2]) = [4]$, and the computation above shows that s maps C into C ($[4] \mapsto [5] \mapsto [3] \mapsto [9] \mapsto [4]$). So by induction on $l \geq 1$ (Theorem 2.2.1, Definition 5.4.2), every $s^l([2])$ with $l \geq 1$ lies in C, and none of them is $[2]$. This is the tail-and-cycle shape that Proposition 5.4.7 predicts. The reason is the failure of injectivity: $s([2]) = [4] = s([9])$, with $[2] \neq [9]$. The point $[4]$ has two arrows coming in, from $[2]$ and from $[9]$; the cycle comes back to $[4]$ through $[9]$, and never needs $[2]$ again.

The example is the usual failure of Example (Method: follow an orbit) in action: from $s([2]) = s([9])$ one may not cancel s to conclude $[2] = [9]$.

Quick check. Follow the forward orbit of $[0]$ under $[a] \mapsto [a^2 + 1]$ on $\mathbb{Z}/7$, and find m and p.

Solution. $[0] \mapsto [1] \mapsto [2] \mapsto [5] \mapsto [26] = [5]$, since $26 - 21 = 5$. The tail is $[0], [1], [2]$, so $m = 3$, and $[5]$ is a fixed point, so $p = 1$.

Remark (Looking ahead). *Algebraic Preliminaries*, Chapter 2 gives a name, group, to a set with an associative operation that has an identity and inverses, as $\circ$ on S_X does by Proposition 5.4.1, and studies S_X among its examples.

5.4.7 Exercises

5.4.7.1 A. Check your understanding

Exercise. A1

(a) For $\sigma = (1\ 4)(2\ 3\ 5)$ on $\{1, \dots, 5\}$, write the two-line tables of σ, σ^{-1} and σ^2.

(b) Let $f\colon \{1, \dots, 5\} \to \{1, \dots, 5\}$ send $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 4$, $4 \mapsto 2$, $5 \mapsto 5$. Find m and p as in Proposition 5.4.7 for $x = 1$, with m as small as possible.

(c) How many fixed points has the three-pile shuffle of twelve cards?

Solution.

(a) Applying the right factor first, σ sends $1 \mapsto 4$, $2 \mapsto 3$, $3 \mapsto 5$, $4 \mapsto 1$, $5 \mapsto 2$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}, \quad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix}, \quad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}.$$

The table of σ^{-1} is that of σ read from bottom to top; $\sigma^{-1} = (1\ 4)(2\ 5\ 3)$ and $\sigma^2 = (2\ 5\ 3)$, since the swap $(1\ 4)$ applied twice is the identity.

(b) The forward orbit is $1, 2, 3, 4, 2, \ldots$: $f^4(1) = 2 = f^1(1)$, with $f^0(1), \ldots, f^3(1)$ distinct. So $m = 1$, $p = 3$ work. And $m = 0$ is impossible: f maps $\{2, 3, 4\}$ into itself and $f(1) = 2$, so by induction $f^l(1) \in \{2, 3, 4\}$ for every $l \geq 1$, and $f^p(1) \neq 1 = f^0(1)$ for every $p \geq 1$.

(c) Two: positions 0 and 11 (Example (The three-pile shuffle)).

5.4.7.2 B. Practice

Exercise. B1: Doubling on nine hours

Let $d\colon \mathbb{Z}/9 \to \mathbb{Z}/9$, $d([a]) \coloneqq [2a]$. Show that d is a permutation, decompose it into disjoint cycles, and find the least $N \geq 1$ with $d^N = \mathrm{id}$.

Solution. d is well defined by Proposition 4.2.5, and so is $e([a]) \coloneqq [5a]$. Since $10 \equiv 1 \pmod 9$, $e(d([a])) = [10a] = [a]$ and $d(e([a])) = [a]$, so d is bijective with inverse e (Theorem 1.6.4). Following orbits (Example (Method: follow an orbit)):

$$[1] \mapsto [2] \mapsto [4] \mapsto [8] \mapsto [16] = [7] \mapsto [14] = [5] \mapsto [10] = [1],$$

$[3] \mapsto [6] \mapsto [12] = [3]$, and $[0]$ is fixed. So

$$d = ([1]\ [2]\ [4]\ [8]\ [7]\ [5])([3]\ [6]),$$

with orbit lengths $6, 2, 1$. By Corollary 5.4.6, $d^N = \mathrm{id}$ exactly when $6 \mid N$, $2 \mid N$ and $1 \mid N$, that is, when $6 \mid N$ (since $2 \mid 6$, Proposition 1.1.1). The least such $N \geq 1$ is 6.

Exercise. B2: Iterates commute

Let $f, g\colon X \to X$. Prove that $f^{n+1} = f^n \circ f$ for every $n \in \mathbb{N}$, and that if $f \circ g = g \circ f$, then $f^n \circ g = g \circ f^n$ for every $n \in \mathbb{N}$.

Solution. The first equation is Proposition 5.4.2 (a) with the exponents n and 1, since $f^1 = f$. For the second, induct on n. For $n = 0$, $\mathrm{id}_X \circ g = g = g \circ \mathrm{id}_X$ (Proposition 1.5.3). If $f^n \circ g = g \circ f^n$, then, by Definition 5.4.2 and Proposition 1.5.3,

$$f^{n+1} \circ g = f \circ (f^n \circ g) = f \circ (g \circ f^n) = (f \circ g) \circ f^n = (g \circ f) \circ f^n = g \circ f^{n+1}.$$

Exercise. B3: Orbits are invariant

Let $\sigma \in S_X$ and $x \in X$. Prove that $\sigma(O_\sigma(x)) = O_\sigma(x)$.

Solution. ($\subseteq$) A point of $\sigma(O_\sigma(x))$ is $\sigma(\sigma^k(x)) = \sigma^{k+1}(x)$ for some $k \in \mathbb{Z}$ (Definition 1.7.1, Proposition 5.4.2 (c)), and $k+1 \in \mathbb{Z}$. ($\supseteq$) For $k \in \mathbb{Z}$, $\sigma^k(x) = \sigma(\sigma^{k-1}(x))$ by Proposition 5.4.2 (c), and $\sigma^{k-1}(x) \in O_\sigma(x)$.

Exercise. B4: Prove or disprove

Prove or disprove each statement.

(a) If X is finite and $f\colon X \to X$ is injective, then every $x \in X$ has $f^k(x) = x$ for some $k \geq 1$.

(b) If $f\colon X \to X$ and $f^N = \mathrm{id}_X$ for some $N \geq 1$, then f is a permutation.

(c) Every function from a finite non-empty set to itself has a fixed point.

(d) Every orbit of a permutation is finite.

(e) If X is finite and every orbit of $\sigma \in S_X$ has length 1 or 2, then $\sigma \circ \sigma = \mathrm{id}_X$.

Solution.

(a) True. The proof of Proposition 5.4.4 used only that σ^i is injective. Here f^i is injective for every $i \in \mathbb{N}$, by induction with Theorem 1.5.4 (a) ($f^0 = \mathrm{id}_X$, $f^{i+1} = f \circ f^i$). So pigeonhole gives $f^i(x) = f^j(x)$ with $i < j$; by Proposition 5.4.2 (a), $f^j = f^i \circ f^{j-i}$, and canceling f^i gives $f^{j-i}(x) = x$, with $j - i \geq 1$.

(b) True. By Proposition 5.4.2 (a), $f \circ f^{N-1} = f^N = \mathrm{id}_X$ and $f^{N-1} \circ f = f^{(N-1)+1} = \mathrm{id}_X$. So f^{N-1} is a two-sided inverse of f, and f is bijective by Theorem 1.6.4.

(c) False. The swap of $\{0, 1\}$, $0 \mapsto 1$, $1 \mapsto 0$, moves both points.

(d) False. $\sigma\colon \mathbb{Z} \to \mathbb{Z}$, $\sigma(n) = n+1$, is a permutation with inverse $n \mapsto n-1$, and $\sigma^k(0) = k$ for every $k \in \mathbb{Z}$ (induction in each direction), so $O_\sigma(0) = \mathbb{Z}$. This is not finite: it contains $\mathbb{N}$, which is infinite (Example (Hilbert's Hotel), Proposition 2.5.6).

(e) True. Each orbit length k_x divides 2, so $\sigma^2(x) = x$ by Proposition 5.4.4 (c), for every x; and $\sigma^2 = \sigma \circ \sigma$ by Definition 5.4.2. So $\sigma \circ \sigma = \mathrm{id}_X$ by Proposition 1.5.1.

5.4.7.3 C. Going deeper

Exercise. C1: Exit check: fifteen cards

Fifteen cards lie at positions $0, \ldots, 14$. Cut them into three piles of five and deal them back in turn, as in the hook, so that

$$\sigma(i) = \begin{cases} 3i & \text{if } 0 \leq i \leq 4, \\ 3i - 14 & \text{if } 5 \leq i \leq 9, \\ 3i - 28 & \text{if } 10 \leq i \leq 14. \end{cases}$$

Show that σ is a permutation, decompose it into disjoint cycles, and find the least $N \geq 1$ with $\sigma^N = \mathrm{id}$.

Solution. A permutation. The three pieces have images $\{0,3,6,9,12\}$, $\{1,4,7,10,13\}$ and $\{2,5,8,11,14\}$: the positions with remainder 0, 1, 2 on division by 3. Each piece is injective ($3i - c = 3i' - c$ gives $i = i'$), and the images are disjoint and cover $\{0,\dots,14\}$ by Theorem 2.2.3. So two different cards in one piece land in different places, two cards in different pieces land in different images, and every position is hit: σ is bijective. (This is the cross-piece check of Example (Method: define a function by gluing).)

Arithmetic modulo 14. Write $i = 5p + r$ with $0 \le r < 5$; the card lands at $\sigma(i) = 3r + p$, and $3i - \sigma(i) = 15p - p = 14p$, so $\sigma(i) \equiv 3i \pmod{14}$. Since $3r + p = 14$ only for $r = 4$, $p = 2$, that is $i = 14$, σ maps $\{0,\dots,13\}$ into itself, with $\sigma(i)$ the remainder of $3i$ on division by 14, and $\sigma(14) = 14$. By induction and Proposition 4.2.5, $\sigma^k(i) \equiv 3^k i \pmod{14}$ for $i \le 13$.

Cycles. 0, 7 ($21 \equiv 7$) and 14 are fixed. Following orbits (Example (Method: follow an orbit)):

$$1 \mapsto 3 \mapsto 9 \mapsto 13 \mapsto 11 \mapsto 5 \mapsto 1 \quad (27 \equiv 13,\ 39 \equiv 11,\ 33 \equiv 5,\ 15 \equiv 1),$$
$$2 \mapsto 6 \mapsto 4 \mapsto 12 \mapsto 8 \mapsto 10 \mapsto 2 \quad (18 \equiv 4,\ 36 \equiv 8,\ 24 \equiv 10,\ 30 \equiv 2).$$

These account for $3 + 6 + 6 = 15$ positions, so $\sigma = (1\ 3\ 9\ 13\ 11\ 5)(2\ 6\ 4\ 12\ 8\ 10)$ by Theorem 5.4.5.

The return. The orbit lengths are $1, 1, 1, 6, 6$. By Corollary 5.4.6, $\sigma^N = \mathrm{id}$ exactly when $6 \mid N$; the least $N \ge 1$ is 6. Check: $3^6 = 729 = 52 \cdot 14 + 1$, so six shuffles multiply every position below 14 by 1 modulo 14.

Marking scheme. (10 points) - 2: proves σ bijective, including the check across pieces (or by an explicit inverse). - 2: reduces σ to multiplication by 3 modulo 14 on $\{0,\dots,13\}$ with 14 fixed, or follows the orbits directly from the three formulas. - 3: finds the two 6-cycles and the fixed points $0, 7, 14$, with the arithmetic shown. - 3: concludes $N = 6$ and shows that no smaller N works, either from the orbit lengths by Corollary 5.4.6 or directly ($3^6 \equiv 1 \pmod{14}$ and $\sigma^k(1) \ne 1$ for $1 \le k \le 5$). Fatal errors (0 for the step): claiming bijectivity from injectivity of each piece alone; taking N as the sum, rather than a common multiple, of the orbit lengths.

Exercise. C2: Find the error

Here is a claim and a proof.

Claim. For every function f from a finite set X to itself and every $x \in X$, there is $k \ge 1$ with $f^k(x) = x$.

Proof. By pigeonhole, $f^i(x) = f^j(x)$ for some $i < j$. Apply f^{-i} to both sides: $x = f^{j-i}(x)$. Take $k = j - i$.

Is the claim true? Find the line that fails, say why, and state what the argument does prove.

Solution. The claim is false. The line that fails is "apply f^{-i}": f^{-i} is defined only for a permutation (Definition 5.4.2), and the claim is about every self-map. A counterexample to that step, and to the claim, is Example (Squaring on an eleven-hour clock) with $x = [2]$: $s^1([2]) = s^5([2]) = [4]$, but no $s^k([2])$ with $k \ge 1$ is $[2]$. The correct conclusion from the pigeonhole repeat is Proposition 5.4.7: after a tail, the forward orbit is periodic. For a permutation, or more generally an injective f (B4 (a)), the cancellation is legitimate and the

claim holds.

Marking scheme. (10 points) - 3: says the claim is false, with a counterexample. - 4: names the failing line, "apply f^{-i}", and the reason: f need not be invertible, or even injective. - 3: states the correct conclusion (tail then cycle, Proposition 5.4.7), or the extra hypothesis under which the proof is right. Fatal errors (0 for the step): accepting the proof because the claim holds for permutations; objecting to the pigeonhole step, which is correct.

Exercise. C3: Each point, its own clock

Let X be a finite set and $\sigma \in S_X$. Show that the length of $O_\sigma(x)$ is the same for all points x of one orbit. Show also that if σ has exactly two orbits, then the number of elements of X is the sum of their lengths.

Solution. Let $y \in O_\sigma(x)$. Then $x \sim_\sigma y$, so $O_\sigma(y) = O_\sigma(x)$ by Theorem 5.4.3 and Theorem 4.2.1 (b). By Proposition 5.4.4 (b), the length of an orbit is its number of elements, so the length at y is the number of elements of $O_\sigma(y) = O_\sigma(x)$, which is the length at x.

If σ has exactly two orbits O and O', they are disjoint and their union is X (Theorem 5.4.3, Definition 4.2.3). By Proposition 5.4.4 (b), O and O' have as many elements as their lengths k and k', so $X = O \cup O'$ has $k + k'$ elements by Proposition 2.5.5.

5.4.7.4 R. Review

Exercise. R1

On $\mathbb{R}$, let $x \sim y$ mean $x - y \in \mathbb{Z}$. Show that $[x] \mapsto [2x]$ is a well-defined surjection $\mathbb{R}/\!\sim \to \mathbb{R}/\!\sim$ that is not injective.

Solution. Here $\sim$ is the equivalence relation of Example (The reals modulo the integers). Let $g\colon \mathbb{R} \to \mathbb{R}/\!\sim$, $g(x) := [2x]$. If $x \sim x'$, then $2x - 2x' = 2(x - x') \in \mathbb{Z}$, so g is constant on classes, and Theorem 5.2.3 (a) gives the function $[x] \mapsto [2x]$ (Example (Method: define a function on a quotient)). It is onto: every class $[y]$ is the image of $[y/2]$. It is not injective: $[0] \mapsto [0]$ and $[\frac{1}{2}] \mapsto [1] = [0]$, while $[0] \neq [\frac{1}{2}]$ by Example (The reals modulo the integers). The method is the well-definedness check of Section 4.2 (Example (Method: checking that a definition on classes is well defined)).

Exercise. R2

Let $\varphi\colon X \to Y$ be a bijection. Show that $\sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$ is a bijection from S_X to S_Y, and that x is a fixed point of σ if and only if $\varphi(x)$ is a fixed point of $\varphi \circ \sigma \circ \varphi^{-1}$.

Solution. For $\sigma \in S_X$, $\varphi \circ \sigma \circ \varphi^{-1}\colon Y \to Y$ is a composite of bijections (φ^{-1} is bijective by Theorem 1.6.4, since φ is a two-sided inverse of it, Definition 1.6.2), so it lies in S_Y (Theorem 1.5.4 (c)); so the rule is a function $c\colon S_X \to S_Y$. In the same way $d(\tau) := \varphi^{-1} \circ \tau \circ \varphi$

defines $d\colon S_Y \to S_X$. By Proposition 1.5.3 and $\varphi^{-1}\circ\varphi = \mathrm{id}_X$, $\varphi\circ\varphi^{-1} = \mathrm{id}_Y$ (Definition 1.6.2),

$$d(c(\sigma)) = \varphi^{-1}\circ((\varphi\circ\sigma)\circ\varphi^{-1})\circ\varphi = (\varphi^{-1}\circ(\varphi\circ\sigma))\circ(\varphi^{-1}\circ\varphi) = ((\varphi^{-1}\circ\varphi)\circ\sigma)\circ\mathrm{id}_X = \sigma,$$

with Proposition 1.5.3 at each regrouping, and likewise $c(d(\tau)) = \tau$. So c has a two-sided inverse and is bijective (Theorem 1.6.4). For the fixed points,

$$c(\sigma)(\varphi(x)) = \varphi(\sigma(\varphi^{-1}(\varphi(x)))) = \varphi(\sigma(x)),$$

which equals $\varphi(x)$ if and only if $\sigma(x) = x$, since φ is injective. The tools are the composites and inverses of Sections 1.5 and 1.6. (Section 3.3's Exercise (C2: Permutations of the naturals) used bijections of $\mathbb{N}$ for a different purpose.)

Exercise. R3

Let $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = 2x + 1$. Prove that $f^n(x) = 2^n x + 2^n - 1$ for every $n \in \mathbb{N}$ and $x \in \mathbb{R}$.

Solution. By induction on n (Logic and Proof, Axiom 4.2.1), with the powers of Definition 2.3.2. For $n = 0$: $f^0(x) = x = 1\cdot x + 1 - 1$. If $f^n(x) = 2^n x + 2^n - 1$, then by Definition 5.4.2

$$f^{n+1}(x) = 2(2^n x + 2^n - 1) + 1 = 2^{n+1}x + 2^{n+1} - 1,$$

since $2\cdot 2^n = 2^n\cdot 2 = 2^{n+1}$. The method is the induction of Section 2.2 on a sequence defined by recursion (Theorem 2.3.1).

Exercise. R4

Let $f\colon X \to Y$, $A \subseteq X$ and $B \subseteq Y$. Show that $(f|_A)^{-1}(B) = A \cap f^{-1}(B)$.

Solution. For every a, by Definition 1.7.2 applied to $f|_A\colon A \to Y$ and to f, and $f|_A(a) = f(a)$ for $a \in A$ (Definition 5.1.1),

$$a \in (f|_A)^{-1}(B) \iff a \in A \wedge f(a) \in B \iff a \in A \cap f^{-1}(B),$$

where the second step uses $A \subseteq X$. The two sets have the same elements, so they are equal. This is the element-chasing of Section 1.7 applied to a function built in Section 5.1. The tool is the preimage definition (Definition 1.7.2), tested pointwise. The look-alike tools fail: image rules such as Proposition 5.1.1 compare images, not preimages, and $f(A \cap C)$ can be strictly smaller than $f(A) \cap f(C)$; and $(f|_A)^{-1}$ here is a preimage, not an inverse function, which $f|_A$ need not have.

Chapter 6

Zorn's Lemma

Some objects are built one piece at a time: an injection one pair at a time, a set of representatives one class at a time, a total order one comparison at a time. When the pieces can be listed, induction finishes the job, one step for each natural number. When they cannot, as for the elements of $\mathbb{R}$, the words "and so on" stand in for a step that is never given, and that is not a proof. Zorn's lemma is the principle that replaces them. *If every unfinished partial object can be enlarged, and every growing chain of partial objects has a partial object above it, then there is one that cannot be enlarged, and it is complete.*

The chapter states the lemma and says why it is not proved here: it is equivalent to the axiom of choice of Chapter 3, and this volume proves only the half that gives choice. It turns the lemma into a single method of proof, the maximality template, and runs the template four times. The third run settles the question Section 3.4 left open: any two sets are comparable in size.

What you need. *Logic and Proof*, Chapters 1–8, in particular the rule ∃E (Logic and Proof, Definition 5.6.1) and the catalogue of what is not allowed (Logic and Proof, Example (What is not allowed)), above all (N13), "an 'and so on' needs its step". From this volume: Section 4.3 on orders (Definition 4.3.1, Example (Inclusion is a partial order, rarely total), Definition 4.3.2, Definition 4.3.3, Definition 4.3.4, Proposition 4.3.2, Example (Maximal elements that are not greatest), Proposition 4.3.1); Section 4.2 on equivalence relations (Definition 4.2.1, Definition 4.2.2, Theorem 4.2.1, Example (The reals modulo the integers)); Chapter 3 on sizes and choice (Axiom 3.2.1, Section 3.2's method box Example (Method: name the choice), Definition 3.4.1, Theorem 3.4.3, Proposition 3.4.2, Proposition 3.1.4, Proposition 3.1.5, Theorem 3.3.4); Section 2.5 on finite sets (Proposition 2.5.6, Example (Hilbert's Hotel), Proposition 2.5.5, Corollary 2.5.3, Proposition 2.5.1); Sections 2.1–2.2 (Theorem 2.1.3, Theorem 2.2.1); Chapter 1 (Definition 1.1.2, Definition 1.4.3, Definition 1.5.1). Proof methods: proof by contradiction (Example (Method: choosing direct, contrapositive or contradiction), Chapter 2) and disproof by counterexample (Example (Method: disproof by counterexample, proof by example), Chapter 1).

Time. About 10 hours on the core track (all of A, one B and one C per section, the exit checks); about 15 hours for everything.

6.0.1 Roadmap

- **Chains and Zorn's lemma.** A pair-by-pair matching that cannot finish; chains in a partially ordered set, and why finitely many elements of the union of a chain of sets lie in one member; Zorn's lemma, why each hypothesis is needed, and why it is stated and not proved; the axiom of choice from Zorn's lemma, as the first run of the maximality template; a set of representatives for any equivalence relation.

- **Using Zorn's lemma.** Any two sets are comparable, so sizes satisfy trichotomy; every partial order extends to a total order, one added comparison at a time; and, in an optional last subsection, how the same template gives every vector space a basis (*Linear Algebra*, Section 1.8).

6.0.2 Named moves

- **The maximality template** (Example (Method: the maximality template)). Partial objects ordered by extension; the union of a chain is again a partial object, since each defining condition mentions finitely many elements and these lie in one member of the chain (Lemma 6.1.1); Zorn's lemma gives a maximal one; a maximal one is complete, since a missing piece would give a strictly larger partial object. (Section 6.1)

6.0.3 Threads

- **Comparing sizes.** Section 3.4 asked whether any two sets are comparable. Section 6.1 opens with a pair-by-pair matching that does not finish, and Section 6.2 finishes it with Zorn's lemma (Theorem 6.2.1).
- **Choice.** Chapter 3 stated the axiom of choice. Section 6.1 derives it from Zorn's lemma (Theorem 6.1.3), and *Axiomatic Set Theory*, Chapter 4 proves the converse.

6.0.4 Summary

A chain is a subset of a partially ordered set on which the order is total (Definition 6.1.1), and finitely many elements of the union of a chain of sets lie in one member (Lemma 6.1.1). Zorn's lemma (Theorem 6.1.2): a non-empty partially ordered set in which every non-empty chain has an upper bound has a maximal element, usually one of many and not a greatest one. It is stated without proof; it implies the axiom of choice (Theorem 6.1.3), and the converse belongs to *Axiomatic Set Theory*, Chapter 4. The maximality template (Example (Method: the maximality template)) gives a set of representatives for any equivalence relation (Example (A set of representatives)), shows that any two sets are comparable in size (Theorem 6.2.1), so that exactly one of $|A| < |B|$, $|A| = |B|$, $|B| < |A|$ holds (Corollary 6.2.2), and extends every partial order to a total order (Theorem 6.2.4), by adding one comparison at a time (Lemma 6.2.3).

Every object built in this chapter is shown to exist and none is written down: no formula is known for a set of representatives of $\mathbb{R}$ modulo $\mathbb{Q}$, for an injection between two arbitrary sets, or for a total order containing $\subseteq$ on $\mathcal{P}(\mathbb{R})$. Where a formula exists, as for divisibility on $\mathbb{N}$ (Example (A total order containing divisibility)), it is the better proof.

6.0.5 Terms

- **chain**: a subset in which any two elements are comparable (Definition 6.1.1).
- **linear extension**: a total order containing a given partial order; "linear order" is a synonym of "total order" (Theorem 6.2.4).
- **maximality template**: partial objects, unions of chains, Zorn's lemma, completeness of a maximal object (Example (Method: the maximality template)).
- **partial choice function**: a set of pairs (i, x) with $x \in A_i$, at most one for each index (Theorem 6.1.3).
- **partial matching**: a relation $G \subseteq A \times B$ in which each element of A and of B occurs in at most one pair (Theorem 6.2.1).
- **set of representatives**: a set meeting every equivalence class in exactly one element

(Example (A set of representatives)).

- **Zorn's lemma**: a non-empty partially ordered set in which every non-empty chain has an upper bound has a maximal element (Theorem 6.1.2).

6.1 Chains and Zorn's Lemma

Section 3.4 proved that injections both ways give a bijection, and left open whether, for any two sets, at least one injection exists. Section 4.3 ended with a question about partially ordered sets: if every chain has an upper bound, must there be a maximal element? One principle answers both questions. This section states it, Zorn's lemma, which answers the second question; explains why this volume does not prove it; and turns it into a method of proof, the maximality template, with two first uses. Section 6.2 uses the template to answer the first question.

6.1.1 Matching two sets, one pair at a time

Let A and B be sets, and suppose we want an injection from one of them into the other, in either direction. A natural plan is to **match** elements in pairs. Pick $a_0 \in A$ and $b_0 \in B$ and pair them. Then pick $a_1 \in A \setminus \{a_0\}$ and $b_1 \in B \setminus \{b_0\}$ and pair those. Continue until one side is used up. If A runs out first, every element of A has a partner, different elements have different partners, and the pairs form the graph of an injection $A \to B$. If B runs out first, the same pairs read backwards form an injection $B \to A$.

For finite sets the plan works, because each step uses one more element of each side, and a finite set is used up after as many steps as it has elements (Section 2.5). Take $A = \{1, 2, 3\}$ and $B = \{x, y\}$. Pair 1 with x, then 2 with y. Now B is used up, and reading the pairs backwards gives $x \mapsto 1$, $y \mapsto 2$, an injection $B \to A$.

For $A = B = \mathbb{R}$ the plan breaks down. Suppose we have made one step for each natural number. The elements of A used so far are $a_0, a_1, a_2, \ldots$, the image of the function $n \mapsto a_n$ on $\mathbb{N}$, so they form a countable set (Proposition 3.1.4). But $\mathbb{R}$ is uncountable (Theorem 3.3.4), so A is not used up; neither is B. The instruction "continue until one side is used up" has no last step, and the words "and so on" stand in for a step that is never stated: (N13) of Logic and Proof, Example (What is not allowed), "an 'and so on' needs its step". (The infinitely many unnamed choices of a_n and b_n are a second problem, the one Section 3.2 met.)

Still, the attempt gets two things right, and they are the thesis of this section:

Every unfinished matching can be enlarged by one more pair, and a growing family of matchings, put together, is again a matching.

The first half is plain: if neither side is used up, an unused a and an unused b make one more pair. The rest of the section makes "growing family" exact and supplies a principle that turns these two facts into a finished matching. We return to the matching in Section 6.2.

6.1.2 Chains

Look at the matchings the plan produces, each a set of pairs. Of any two of them, one was built from the other by adding pairs, so one is a subset of the other: under $\subseteq$, any two are comparable. That is what "growing family" means, and it makes sense in any partially ordered set.

Definition 6.1.1. Chain

Let $(X, \preceq)$ be a partially ordered set. A subset $C \subseteq X$ is a **chain** if **any two** elements of C are comparable: for all $x, y \in C$, $x \preceq y$ or $y \preceq x$.

So a chain is a subset on which $\preceq$ is total (Definition 4.3.1); in a totally ordered set, every subset is a chain.

Examples.

- In $(\mathbb{N}, |)$, the set $\{1, 2, 4, 8, \dots\} = \{2^n : n \in \mathbb{N}\}$ is a chain: for $m \leq n$, $2^n = 2^{n-m} \cdot 2^m$, so $2^m \mid 2^n$. The set $\{2, 3\}$ is not, since $2 \nmid 3$ and $3 \nmid 2$.
- In $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$, the set $\{\emptyset, \{2\}, \{2, 3\}\}$ is a chain.
- Degenerate cases: $\emptyset$ is a chain, vacuously, and so is every one-element set $\{x\}$, by (PO1).

Quick check. Decide: (a) Is $\{\{1\}, \{1, 2\}, \{3\}\}$ a chain in $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$? (b) Is $\{0, 1, 5, 25\}$ a chain in $(\mathbb{N}, |)$? (c) Is $\{3, 6, 0\}$? (d) In $(\mathbb{R}, \leq)$, which subsets are chains?

Solution.

(a) No: $\{1, 2\} \not\subseteq \{3\}$ and $\{3\} \not\subseteq \{1, 2\}$.

(b) Yes. 1 divides every natural number, $25 = 5 \cdot 5$, and every natural number a divides $0 = 0 \cdot a$; so any two of the four are comparable.

(c) Yes: $6 = 2 \cdot 3$, and $3 \mid 0$, $6 \mid 0$.

(d) All of them, since $\leq$ is total on $\mathbb{R}$.

Why do chains matter for the matching? Take two pairs from the union of a growing family of matchings. Each pair comes from some matching of the family, and the two matchings are comparable, so both pairs lie in the larger of the two. Any condition that speaks about two pairs at a time can then be checked inside one matching. The same works for any finite number of elements, and that is the content of the next lemma.

The lemma speaks about a set of sets ordered by $\subseteq$. That is always a partially ordered set: each member of a set of sets $\mathcal{S}$ is a subset of $\bigcup \mathcal{S}$, and $\subseteq$ is a partial order on $\mathcal{P}(\bigcup \mathcal{S})$ (Example (Inclusion is a partial order, rarely total)), which stays one when restricted to the subset $\mathcal{S}$, since (PO1)–(PO3) are statements about all elements.

Lemma 6.1.1. Finitely Many Members of a Chain

(a) Let C be a chain in a partially ordered set $(X, \preceq)$, let $n \geq 1$ and $x_1, \dots, x_n \in C$. Then some x_k satisfies $x_j \preceq x_k$ for $j = 1, \dots, n$.

(b) Let $\mathcal{S}$ be a set of sets, partially ordered by $\subseteq$, and $\mathcal{C} \subseteq \mathcal{S}$ a chain. Then $C \subseteq \bigcup \mathcal{C}$ for every $C \in \mathcal{C}$; and if $n \geq 1$ and $z_1, \dots, z_n \in \bigcup \mathcal{C}$, then some single $C \in \mathcal{C}$ contains all of $z_1, \dots, z_n$.

Proof. (a) By induction on n (Theorem 2.2.1 with $n_0 = 1$). For $n = 1$, take $k = 1$: $x_1 \preceq x_1$ by (PO1). For the step, let $x_1, \dots, x_{n+1} \in C$, and by the induction hypothesis let x_k with

$k \le n$ be above $x_1, \dots, x_n$. Since C is a chain, $x_{n+1} \preceq x_k$ or $x_k \preceq x_{n+1}$. In the first case x_k is above all $n+1$ elements. In the second, x_{n+1} is: $x_j \preceq x_k \preceq x_{n+1}$ gives $x_j \preceq x_{n+1}$ by (PO3) for $j \le n$, and $x_{n+1} \preceq x_{n+1}$ by (PO1).

(b) The first claim is the definition of the union. For the second, induct on n (Theorem 2.2.1 with $n_0 = 1$). For $n = 1$: $z_1 \in \bigcup \mathcal{C}$ means that $z_1 \in C$ for some $C \in \mathcal{C}$, and one use of ∃E (Logic and Proof, Definition 5.6.1) names such a C. For the step, by the induction hypothesis some $C' \in \mathcal{C}$ contains $z_1, \dots, z_n$, and one use of ∃E gives $C'' \in \mathcal{C}$ with $z_{n+1} \in C''$. Since $\mathcal{C}$ is a chain, $C' \subseteq C''$ or $C'' \subseteq C'$, and the larger of the two contains all of $z_1, \dots, z_{n+1}$.

■

Each step of the induction in (b) makes one use of ∃E, so no choice is involved. Writing "use ∃E n times" instead would be the "and so on" that (N13) flags; the induction is what supplies its step.

Quick check.

(a) Is there a chain of subsets of $\mathbb{N}$, none of whose members contains both 0 and 1, whose union contains both? (b) Is there such a family of subsets that is not a chain?

Solution.

(a) No. If 0 and 1 lie in the union of a chain, then by Lemma 6.1.1 (b) with $n = 2$ some member contains both.

(b) Yes: $\{\{0\}, \{1\}\}$ has union $\{0, 1\}$, and neither member contains both. This is exactly what "chain" rules out.

6.1.3 Zorn's lemma

Return to the question of Section 4.3: in a partially ordered set in which every chain has an upper bound, is there a maximal element? A naive attempt: start at any p_0. If p_0 is not maximal, there is $p_1 \succ p_0$; if p_1 is not maximal, there is $p_2 \succ p_1$; and so on. The p_n form a chain, which has an upper bound u; if u is not maximal, continue above u, and so on. Each single step is legitimate. But the chain $p_0 \prec p_1 \prec \cdots$ may have an upper bound that is again not maximal, the next chain may too, and "continue past every such bound" is neither a finite process nor one indexed by $\mathbb{N}$. It is (N13) once more: the "and so on" has no step. Instead of a proof, there is a principle, stated as its own result.

Theorem 6.1.2. Zorn's Lemma

Let $(P, \preceq)$ be a **non-empty** partially ordered set in which **every non-empty chain** has an upper bound in P. Then P has a maximal element.

We do not prove Theorem 6.1.2. It cannot be proved from the rules of logic and the working rules for sets of Chapter 1 alone: it is equivalent to the axiom of choice (Axiom 3.2.1), which, as Section 3.2 records, can be neither proved nor refuted from the other axioms. One half of the equivalence, that Zorn's lemma implies the axiom of choice, is the first application below

(Theorem 6.1.3). The other half, which builds a maximal element from a choice function, is proved in *Axiomatic Set Theory*, Chapter 4, together with the other equivalents. As with the axiom, we use the lemma openly and cite it at each use. Zorn (1935) put the principle in this form, which suits algebra, where the objects to be built are sets ordered by inclusion.

Why each hypothesis is needed. Each of three small examples breaks one hypothesis and has no maximal element.

- $(\mathbb{N}, \leq)$ is non-empty and total, and has no maximal element, since $n < n + 1$. The chain hypothesis fails: the chain $\mathbb{N}$ has no upper bound in $\mathbb{N}$.
- The empty partially ordered set satisfies the chain hypothesis vacuously, since it has no non-empty chain, and it has no maximal element. "Non-empty" is needed.
- The set of finite subsets of $\mathbb{N}$, ordered by $\subseteq$, is non-empty, as $\emptyset$ belongs to it, and has no maximal element. For finite F, $\mathbb{N}$ is not a subset of F, since a subset of a finite set is finite (Proposition 2.5.6) and $\mathbb{N}$ is infinite (Example (Hilbert's Hotel)); for $m \in \mathbb{N} \setminus F$, the set $F \cup \{m\}$ is finite (Proposition 2.5.5) and strictly larger. By the contrapositive of Zorn's lemma, some non-empty chain has no upper bound in this set, and here one is visible: $\{\{0, 1, \ldots, n-1\} : n \in \mathbb{N}\}$, that is, $\emptyset, \{0\}, \{0, 1\}, \ldots$. An upper bound would be a finite set containing every natural number, hence containing $\mathbb{N}$, which is impossible.

Warning. **Maximal, not greatest, and not unique.** Zorn's lemma produces **a** maximal element, by no formula, and says nothing about how many there are. By Proposition 4.3.2 a greatest element would be maximal, but the converse fails (Example (Maximal elements that are not greatest)). In the applications below there are usually many maximal objects and no greatest one; a proof that treats "the" maximal element as unique, or as above everything, has gone wrong.

Quick check. Let $P = \{\{1\}, \{2\}, \{1, 3\}\}$, ordered by $\subseteq$. List the chains with at least two elements; check that every non-empty chain has an upper bound in P; name the maximal elements.

Solution. The only comparable pair of different elements is $\{1\} \subseteq \{1, 3\}$, so the only chain with at least two elements is $\{\{1\}, \{1, 3\}\}$, with upper bound $\{1, 3\}$. A one-element chain $\{p\}$ has the upper bound p. The maximal elements are $\{2\}$ and $\{1, 3\}$: two of them, as the warning says, and no greatest element.

Remark (Every chain, or every non-empty chain). Some books ask for an upper bound of **every** chain, the empty one included. An upper bound of $\emptyset$ is any element of P (Definition 4.3.2), so that form contains "$P \neq \emptyset$" as a special case. The two forms say the same thing.

6.1.4 The maximality template

Zorn's lemma is almost always used in one pattern. Its first use proves the half of the equivalence with the axiom of choice that this volume can prove.

Theorem 6.1.3. Zorn's Lemma Gives Choice

Assume Theorem 6.1.2. Let I be a set and $(A_i)_{i\in I}$ a family of **non-empty** sets. Then there is a function $c\colon I \to \bigcup_{i\in I} A_i$ with $c(i) \in A_i$ for every $i \in I$.

This is the conclusion of Axiom 3.2.1, so the axiom follows from Zorn's lemma.

Idea (Scratch work). A choice function can be built one index at a time, like the matching of the first subsection. Call a set of pairs (i, x) with $x \in A_i$, at most one pair for each i, a **partial choice function**: it is a graph (Definition 1.5.1) defined on part of I. Order these by $\subseteq$: the larger of two comparable ones agrees with the smaller and is defined at more indices. Write $U \coloneqq \bigcup_{i\in I} A_i$.

Givens	Goal
$A_i \neq \emptyset$ for each $i \in I$	$c\colon I \to U$ with $c(i) \in A_i$ for all i
P: the $G \subseteq I \times U$ with (C1) $(i, x) \in G \Rightarrow x \in A_i$ and (C2) $(i, x), (i, y) \in G \Rightarrow x = y$; order $\subseteq$	Zorn's hypotheses: $P \neq \emptyset$, and each non-empty chain has an upper bound in P
$\emptyset \in P$; for a chain $\mathcal{C}$, try $\bigcup\mathcal{C}$: (C1) and (C2) mention at most two pairs (Lemma 6.1.1)	a maximal $M \in P$ is defined at every $i \in I$
M maximal; suppose i_0 is missed	$M \cup \{(i_0, x_0)\} \in P$, strictly larger: a contradiction

The last row is a proof by contradiction (Example (Method: choosing direct, contrapositive or contradiction)): a missed index gives a larger partial object. Choosing $x_0 \in A_{i_0}$ is **one** use of $\exists$E, which Section 3.2 showed is always allowed; Zorn's lemma does the infinitely many.

Proof. Let U and P be as in the table. Then $P \subseteq \mathcal{P}(I \times U)$ is a set, partially ordered by $\subseteq$.

P is non-empty: $\emptyset$ satisfies (C1) and (C2) vacuously.

Chains have upper bounds: let $\mathcal{C} \subseteq P$ be a non-empty chain and $H \coloneqq \bigcup\mathcal{C} \subseteq I \times U$. If $(i, x) \in H$, it lies in some $G \in \mathcal{C}$, so $x \in A_i$ by (C1) for G. If $(i, x), (i, y) \in H$, some $G \in \mathcal{C}$ contains both (Lemma 6.1.1 (b) with $n = 2$), so $x = y$ by (C2) for G. So $H \in P$, and $G \subseteq H$ for every $G \in \mathcal{C}$: H is an upper bound of $\mathcal{C}$ in P.

Zorn: by Theorem 6.1.2, P has a maximal element M.

M is defined everywhere: suppose some $i_0 \in I$ has no pair $(i_0, x) \in M$. Since $A_{i_0} \neq \emptyset$, take $x_0 \in A_{i_0}$, and let $M' \coloneqq M \cup \{(i_0, x_0)\}$. Then $M' \subseteq I \times U$, since $i_0 \in I$ and $x_0 \in A_{i_0} \subseteq U$; M' satisfies (C1), and it satisfies (C2), because the only pair of M' with first coordinate i_0 is (i_0, x_0). So $M' \in P$, $M \subseteq M'$, and $M \neq M'$, as $(i_0, x_0) \notin M$; this contradicts the maximality of M. Hence for every $i \in I$ there is a pair $(i, x) \in M$, and by (C2) exactly one. By Definition 1.5.1, M is the graph of a function $c\colon I \to U$, and $c(i) \in A_i$ by (C1).

■

If $I = \emptyset$, then $P = \{\emptyset\}$, and the proof produces the empty function, which is correct. Of the

proof's four steps, only the last is about choice functions; the first three run the same way in every use of the lemma, and that is worth recording.

Example. Method: the maximality template

Template. To show that a complete object exists: (1) **partial objects:** let P be the set of partial objects, of which the complete ones are the finished case, ordered by $\subseteq$ (extension); check $P \neq \emptyset$, usually with the empty or the given starting object. (2) **chains:** for a non-empty chain $\mathcal{C} \subseteq P$, show $\bigcup \mathcal{C} \in P$; each defining condition mentions finitely many elements, which lie in one member (Lemma 6.1.1). (3) **Zorn:** P has a maximal element M (Theorem 6.1.2). (4) **complete:** suppose M is not complete; use the missing piece to build a strictly larger partial object, a contradiction.

When to use it. The object can be built piece by piece, each condition on it checks finitely many pieces at a time, and the pieces cannot be listed.

The usual failure. The union of a chain is not a partial object, because a condition mentions infinitely many pieces ("finite", "countable"); step (4) builds an object that is not strictly larger, or not in P; and treating M as the greatest or the only complete object.

The second use runs the template with a shorter plan.

Example. A set of representatives

Let $\sim$ be an equivalence relation on a set X. Show that there is a set $S \subseteq X$ that meets every equivalence class in exactly one element.

Idea (Scratch work). By the method of Example (Method: the maximality template). A partial object should be a set that meets each class **at most** once, so that the complete ones meet each class exactly once. "At most once" reads: $s \sim t$ implies $s = t$, a condition on two elements at a time, so step (2) works. For step (4), a class $[x]$ that is missed gives the larger set $S \cup \{x\}$, and no choice is needed, since x is already in hand.

Solution. Let P be the set of $S \subseteq X$ such that for all $s, t \in S$, $s \sim t$ implies $s = t$; order it by $\subseteq$. Then $\emptyset \in P$. For a non-empty chain $\mathcal{C} \subseteq P$, any two elements s, t of $\bigcup \mathcal{C}$ lie in one member (Lemma 6.1.1 (b)), so $s \sim t$ gives $s = t$: $\bigcup \mathcal{C} \in P$, an upper bound of $\mathcal{C}$. By Theorem 6.1.2, take a maximal $M \in P$.

Suppose some class $[x]$ (Definition 4.2.2) contains no element of M. Then $x \notin M$, since $x \in [x]$ by (Eq1). And $M \cup \{x\} \in P$: let $s, t \in M \cup \{x\}$ with $s \sim t$. If both lie in M, then $s = t$. If $s = x$ and $t \in M$, then $t \sim x$ by (Eq2), so $t \in [x] \cap M$, which is impossible; the case $t = x$, $s \in M$ is the same with the letters exchanged; and if $s = t = x$, there is nothing to show. So $M \subsetneq M \cup \{x\}$ in P, contradicting maximality. Hence M meets every class, and by the condition defining P in at most one element: $S \coloneqq M$ works.

The axiom of choice gives the same set in one line, by choosing one element from each class; the template's advantage shows when the pieces interact, as in Section 6.2. On $\mathbb{R}$, the relation $x \sim y \iff x - y \in \mathbb{Q}$ is an equivalence relation (Section 4.2, after Example (The reals modulo

the integers)). A set of representatives for it inside $[0,1]$ is a set of real numbers that *Measure and Integration*, Chapter 1 shows has no length, and no formula for one is known.

Quick check. Let $X = \mathbb{Z}$ and $m \sim n \iff m - n$ is even. Describe the partial objects of Example (A set of representatives) that have two elements, and the maximal ones.

Solution. They are the sets $\{e, o\}$ with e even and o odd: two even or two odd integers are related, since their difference is even, so a partial object holds at most one of each parity. Conversely, $\{e, o\}$ is a partial object: with $e = 2a$ and $o = 2b + 1$, $e - o = 2(a - b - 1) + 1$ is odd, hence not even (no integer is both, Theorem 1.1.2), so $e \not\sim o$. These are exactly the maximal elements, since any third integer has the parity of e or of o (every integer is even or odd, Theorem 1.1.2), and $\emptyset$ and the one-element sets are not maximal, since each lies strictly inside some $\{e, o\}$. There are many maximal elements, such as $\{0, 1\}$ and $\{4, -7\}$, and no greatest one.

Warning. **Check that the union is a partial object.** Here is an almost-correct proof that $\mathbb{N}$ has a maximal finite subset. "Let P be the set of finite subsets of $\mathbb{N}$, ordered by $\subseteq$. A chain has its union as an upper bound. By Zorn's lemma, P has a maximal element." The conclusion is false, by the third example after Theorem 6.1.2. The failing line is the second: the union is an upper bound in $\mathcal{P}(\mathbb{N})$, but it need not be finite, so it need not lie in P. "Finite" is a condition on all the elements at once, and Lemma 6.1.1 handles only finitely many.

Section 6.2 applies the template twice more, first to the matching that opened this section.

6.1.5 Exercises

6.1.5.1 A. Check your understanding

Exercise. A1

These questions are about the proof of Theorem 6.1.3.

(a) Where is "$A_i \neq \emptyset$" used, and which step fails without it?

(b) Why does the chain step need Lemma 6.1.1 only for $n = 2$?

(c) Run the proof on $I = \{1, 2\}$, $A_1 = \{0\}$, $A_2 = \{5, 6\}$: list P, name its maximal elements, and decide whether P has a greatest element.

(d) Which of the two hypotheses of Theorem 6.1.2 does the empty partially ordered set satisfy?

Solution.

(a) In the last step: $x_0 \in A_{i_0}$ exists only because $A_{i_0} \neq \emptyset$. Without it, M could miss i_0 and still be maximal, and indeed no choice function exists if some A_i is empty.

(b) Condition (C1) mentions one pair and (C2) mentions two; no condition defining P

mentions more.

(c) $U = \{0, 5, 6\}$, and

$$P = \{\emptyset, \{(1,0)\}, \{(2,5)\}, \{(2,6)\}, \{(1,0),(2,5)\}, \{(1,0),(2,6)\}\}.$$

The maximal elements are the last two, each the graph of a choice function. There is no greatest element: the two maximal elements are incomparable, and a greatest element would be maximal (Proposition 4.3.2 (a)), so it would be one of them and contain the other.

(d) The chain hypothesis, vacuously; not non-emptiness.

6.1.5.2 B. Practice

Exercise. B1: Maximal chains

Let $(X, \preceq)$ be a partially ordered set and $C_0 \subseteq X$ a chain. Prove that there is a chain $C \supseteq C_0$ that is **maximal**: no chain contains C properly.

Solution (Hint). The partial objects are the chains containing C_0.

Solution. Let P be the set of chains $C \subseteq X$ with $C_0 \subseteq C$, ordered by $\subseteq$; then $C_0 \in P$. Let $\mathcal{K} \subseteq P$ be a non-empty chain and $H := \bigcup \mathcal{K}$. Then $H \supseteq C_0$, since $\mathcal{K}$ has a member and each member contains C_0. Any $x, y \in H$ lie in one member $K \in \mathcal{K}$ (Lemma 6.1.1 (b)), which is a chain, so x and y are comparable. So $H \in P$, and it is an upper bound of $\mathcal{K}$. By Theorem 6.1.2, P has a maximal element C. If a chain $D \supsetneq C$ existed, then $D \supseteq C_0$, so $D \in P$ and $C \subsetneq D$, contradicting maximality. So C is a maximal chain containing C_0.

Exercise. B2: Name the move, then complete it

Here is the frame of a proof that for every set $\mathcal{F}$ of non-empty sets there is a subfamily $\mathcal{D} \subseteq \mathcal{F}$ of pairwise disjoint sets such that every member of $\mathcal{F}$ meets some member of $\mathcal{D}$.

> Let P be the set of subfamilies $\mathcal{E} \subseteq \mathcal{F}$ whose members are pairwise disjoint ($E \cap E' = \emptyset$ for $E \neq E'$ in $\mathcal{E}$), ordered by $\subseteq$. Then $\emptyset \in P$. For a non-empty chain of such subfamilies, two members $E \neq E'$ of its union lie in one subfamily of the chain, so $E \cap E' = \emptyset$; the union lies in P and is an upper bound. By Zorn's lemma, P has a maximal element $\mathcal{D}$.
>
> $\vdots$
>
> ... Hence every member of $\mathcal{F}$ meets some member of $\mathcal{D}$.

Name the move, then complete it.

Solution. The move is step (4) of Example (Method: the maximality template): a missing piece gives a strictly larger partial object. Suppose $F \in \mathcal{F}$ meets no member of $\mathcal{D}$. Then $F \notin \mathcal{D}$: otherwise F would meet itself, as $F \cap F = F \neq \emptyset$. And $\mathcal{D} \cup \{F\}$ is pairwise disjoint,

since $F \cap D = \emptyset$ for every $D \in \mathcal{D}$ by assumption. So $\mathcal{D} \subsetneq \mathcal{D} \cup \{F\} \in P$, against the maximality of $\mathcal{D}$. The check $F \notin \mathcal{D}$ is what makes the new family strictly larger, the failure the method box warns about. Hence every member of $\mathcal{F}$ meets some member of $\mathcal{D}$.

Exercise. B3: A small poset of partial injections

Let $A = \{1, 2\}$ and $B = \{b\}$. List the relations $G \subseteq A \times B$ in which each element of A and each element of B occurs in at most one pair, ordered by $\subseteq$. Name the maximal elements. For each, is every element of A paired? Every element of B?

Solution. They are $\emptyset$, $\{(1, b)\}$ and $\{(2, b)\}$; the only other subset of $A \times B$, $\{(1, b), (2, b)\}$, fails because b occurs twice. The maximal elements are $\{(1, b)\}$ and $\{(2, b)\}$. Neither pairs every element of A; each pairs every element of B, and read backwards it is an injection $B \to A$. (Section 6.2 shows that this always happens: a maximal partial injection uses up one side.)

Exercise. B4: Prove or disprove

Prove each true statement and refute each false one.

(a) If every chain of a non-empty partially ordered set P has an upper bound in P, then P has a greatest element.

(b) Every non-empty finite partially ordered set has a maximal element.

(c) The set of subsets of $\mathbb{N}$ that contain no two consecutive numbers, ordered by $\subseteq$, has a greatest element.

(d) If P is a non-empty partially ordered set in which every non-empty chain has an upper bound, then every $p \in P$ lies below some maximal element of P.

(e) The set of countable subsets of $\mathbb{R}$, ordered by $\subseteq$, has a maximal element.

Hint for (d): apply Zorn's lemma to the elements above p.

Solution.

(a) False. Take $P = \{\{1\}, \{2\}\}$ under $\subseteq$. Its chains are $\emptyset$, $\{\{1\}\}$ and $\{\{2\}\}$, each with an upper bound in P. But P has no greatest element, since $\{1\}$ and $\{2\}$ are incomparable.

(b) True. Let P be non-empty and finite, and let C be a non-empty chain of P. Then C is finite (Proposition 2.5.6); list it as $x_1, \ldots, x_n$ with $n \geq 1$. By Lemma 6.1.1 (a), one x_k is above all of them, an upper bound of C in P. By Theorem 6.1.2, P has a maximal element. (Section 4.3, Exercise R4 proves this without Zorn's lemma, by induction.)

(c) False. The set E of even numbers and the set O of odd numbers both contain no two consecutive numbers. A greatest element G would contain E and O, so $0, 1 \in G$, which are consecutive. (In fact E and O are both maximal: adding any $n \notin E$ to E puts n and $n + 1$ in it (n is odd by Theorem 1.1.2, so $n + 1$ is even), and adding any $n \notin O$ to O does the same. So Zorn's lemma, if applied here, gives a maximal element, never a greatest one, as the warning after Theorem 6.1.2 says.)

(d) True. Let $p \in P$, and let $Q := \{q \in P : p \preceq q\}$, ordered by $\preceq$; then $p \in Q$. A non-empty chain $\mathcal{K}$ of Q is a chain of P, so it has an upper bound $u \in P$; for any $c \in \mathcal{K}$, $p \preceq c \preceq u$,

so $u \in Q$ by (PO3). By Theorem 6.1.2, Q has a maximal element m, and $p \preceq m$. If $m \prec q$ for some $q \in P$, then $p \preceq q$ by (PO3), so $q \in Q$, against the maximality of m in Q. So m is maximal in P.

(e) False. Let $C \subseteq \mathbb{R}$ be countable. Then $C \neq \mathbb{R}$, since $\mathbb{R}$ is uncountable (Theorem 3.3.4); for $x \in \mathbb{R} \setminus C$, the set $C \cup \{x\}$ is countable (Proposition 3.1.5) and strictly larger. So no countable set is maximal. (By the contrapositive of Zorn's lemma, some non-empty chain of countable sets has no countable upper bound; the answer does not need one.)

6.1.5.3 C. Going deeper

Exercise. C1: Find the error

Claim: every chain C_0 of a partially ordered set X lies in a maximal chain.

"Proof": Let P be the set of chains containing C_0, ordered by $\subseteq$; then $C_0 \in P$. Let $\mathcal{K}$ be a non-empty chain in P. Every $K \in \mathcal{K}$ is a subset of $\bigcup \mathcal{K}$, so $\bigcup \mathcal{K}$ is an upper bound of $\mathcal{K}$. By Zorn's lemma, P has a maximal element C. A chain containing C contains C_0, so it lies in P; hence C is a maximal chain.

Is the conclusion true? Does the argument prove it?

Solution. The conclusion is true: it is Exercise B1.

The argument does not prove it. It never checks that $\bigcup \mathcal{K}$ **is a chain**, that is, that it lies in P; the upper bound in Theorem 6.1.2 must belong to P. The step's general form, "the union of a chain of partial objects lies in P", is false: among the finite subsets of $\mathbb{N}$, the chain $\{\{0, \dots, n-1\} : n \in \mathbb{N}\}$ has union $\mathbb{N}$, which is not finite (the warning before these exercises). Here the conclusion of the step happens to be true, which is exactly why it must be proved, not assumed. The repair is the chain step of B1: two elements of $\bigcup \mathcal{K}$ lie in one member $K \in \mathcal{K}$ (Lemma 6.1.1 (b)), which is a chain, so they are comparable.

Marking scheme. (10 points) - 2: the conclusion is true, with B1 cited. - 3: the missing check named: $\bigcup \mathcal{K} \in P$. - 3: a counterexample to the general inference "the union of a chain of partial objects lies in P" (in any partially ordered set), with the remark that here the step's conclusion is true but unproved. - 2: the repair via Lemma 6.1.1. Fatal errors (0 for the step): calling the conclusion false; "repairing" the proof by assuming that a union of chains is always a chain.

Exercise. C2: Exit check: when no choice is needed

(a) Let $\sim$ be an equivalence relation on $\mathbb{N}$. Without Zorn's lemma or the axiom of choice, give a set S meeting every class exactly once, and prove that it does.

(b) Do the same for an equivalence relation on a set X with an injection $j \colon X \to \mathbb{N}$.

(c) Which ingredient of Example (A set of representatives) does your answer to (a) make unnecessary, and why?

Solution (Hint 1). Each class is a non-empty set of natural numbers. Which element of it can be named without choosing?

Solution.

(a) Let $S \coloneqq \{m_x : x \in \mathbb{N}\}$, where m_x is the least element of $[x]$. It exists by Theorem 2.1.3, since $[x] \subseteq \mathbb{N}$ contains x and so is non-empty, and it is unique (Proposition 4.3.1), so the rule names one value. *Every class is met:* $m_x \in [x] \cap S$. *At most once:* let $m_x, m_y \in S$ lie in the same class $[z]$. Then $m_x \in [x] \cap [z]$, so $[x] = [z]$, and likewise $[y] = [z]$, since different classes are disjoint (Theorem 4.2.1). So $[x] = [y]$, these classes have the same least element, and $m_x = m_y$. Hence S meets each class $[x]$ in m_x and nowhere else.

(b) For $x \in X$, the set $j([x]) \subseteq \mathbb{N}$ is non-empty, so it has a least element k_x (Theorem 2.1.3), and since j is injective exactly one $s_x \in [x]$ has $j(s_x) = k_x$. Let $S \coloneqq \{s_x : x \in X\}$. The argument of (a) applies word for word, with s_x for m_x: equal classes give equal k_x, hence equal s_x.

(c) Zorn's lemma, that is, the whole argument with P, chains and a maximal M: a rule names each representative, so nothing needs to be chosen (Example (Method: name the choice)).

Marking scheme. (10 points) - 3: (a) each class has a well-defined representative (well-ordering, and the rule names one value). - 3: (a) every class met, and met at most once (justified). - 2: (b) the least value of j, and injectivity naming one element. - 2: (c) Zorn's lemma named as the unnecessary ingredient, because a rule names each representative. Fatal errors (0 for the step): "choose an element of each class" in (a) or (b), which is the axiom of choice.

6.2 Using Zorn's Lemma

Section 6.1 turned Zorn's lemma into a four-step template. This section uses it twice. The first use finishes the matching that opened Section 6.1 and answers the question Section 3.4 left open: any two sets are comparable in size. The second extends any partial order to a total one, the infinite form of putting tasks in an order that respects their prerequisites. An optional last subsection shows the same template in linear algebra.

6.2.1 Back to comparing sizes

Section 3.4 defined $|A| \leq |B|$ as the existence of an injection $A \to B$ (Definition 3.4.1) and proved that injections both ways give a bijection (Theorem 3.4.3). It left open whether at least one of the two injections always exists. Section 6.1 tried to build one by matching elements pair by pair, and the attempt got two things right: an unfinished matching can be enlarged by one pair, and a growing family of matchings, put together, is again a matching. Those are steps (4) and (2) of the maximality template (Example (Method: the maximality template)), and Zorn's lemma supplies the rest.

Theorem 6.2.1. Any Two Sets Are Comparable

For all sets A and B, $|A| \leq |B|$ or $|B| \leq |A|$.

Idea. By the method of Example (Method: the maximality template). The partial objects are the partial matchings: relations $G \subseteq A \times B$ in which each element of A and each element of B occurs in at most one pair. The union of a chain of them is one, since each condition

mentions two pairs at a time. A maximal matching uses up A or B, since otherwise one more pair fits; read in the right direction, it is an injection.

Proof. Let P be the set of relations $G \subseteq A \times B$ such that

- (M1) if $(a, b), (a, b') \in G$, then $b = b'$;
- (M2) if $(a, b), (a', b) \in G$, then $a = a'$;

ordered by $\subseteq$. It is a set of subsets of $A \times B$, so $\subseteq$ is a partial order on it.

Partial objects. $\emptyset \in P$, since (M1) and (M2) hold vacuously; so $P \neq \emptyset$.

Chains. Let $\mathcal{C} \subseteq P$ be a non-empty chain and $H \coloneqq \bigcup \mathcal{C} \subseteq A \times B$. Any two pairs of H lie in a single member $G \in \mathcal{C}$ (Lemma 6.1.1 (b), with $n = 2$). So if $(a, b), (a, b') \in H$, then $b = b'$ by (M1) for G; and (M2) for H follows in the same way. Hence $H \in P$, and $G \subseteq H$ for every $G \in \mathcal{C}$: H is an upper bound of $\mathcal{C}$ in P.

Zorn. By Theorem 6.1.2, P has a maximal element M.

M uses up a side. Suppose some $a_0 \in A$ occurs in no pair of M, and some $b_0 \in B$ occurs in no pair of M. Then $M' \coloneqq M \cup \{(a_0, b_0)\}$ satisfies (M1) and (M2), because the new pair shares no coordinate with a pair of M. So $M' \in P$, $M \subseteq M'$, and $M \neq M'$, since $(a_0, b_0) \notin M$. This contradicts the maximality of M. Hence every $a \in A$ occurs in a pair of M, or every $b \in B$ does.

Case 1: every $a \in A$ occurs. By (M1) it occurs in exactly one pair, so M is the graph of a function $f \colon A \to B$ (Definition 1.5.1). If $f(a) = f(a') = b$, then $(a, b), (a', b) \in M$, so $a = a'$ by (M2): f is injective, and $|A| \leq |B|$.

Case 2: every $b \in B$ occurs. Consider the inverse relation $M^{-1} = \{(b, a) : (a, b) \in M\} \subseteq B \times A$ (Definition 1.4.3). Every $b \in B$ occurs as a first coordinate of M^{-1}, and by (M2) in exactly one pair; so M^{-1} is the graph of a function $g \colon B \to A$. By (M1), $g(b) = g(b') = a$ gives $b = b'$: g is injective, and $|B| \leq |A|$.

■

Section 6.1's "continue until one side is used up" has become step (4): a maximal matching cannot be continued, and so a side is used up. The words "and so on" never appear.

Corollary 6.2.2. Trichotomy for Sizes

For all sets A and B, exactly one of $|A| < |B|$, $|A| = |B|$, $|B| < |A|$ holds.

Proof. At least one. By Theorem 6.2.1, $|A| \leq |B|$ or $|B| \leq |A|$. In the first case, either $|A| = |B|$, or not, and then $|A| < |B|$ by Definition 3.4.1. The second case gives $|B| = |A|$, hence $|A| = |B|$ (Proposition 2.5.1 (b)), or $|B| < |A|$.

At most one. $|A| < |B|$ excludes $|A| = |B|$ by Definition 3.4.1. $|B| < |A|$ excludes $|B| = |A|$, and therefore $|A| = |B|$, by symmetry (Proposition 2.5.1 (b)). Finally, $|A| < |B|$ and $|B| < |A|$ together give injections $A \to B$ and $B \to A$, so $|A| = |B|$ by Theorem 3.4.3, contradicting $|A| < |B|$.

■

Comparability is itself equivalent to the axiom of choice, a fact proved in *Axiomatic Set Theory*, Chapter 4: this book needed choice for it, and no proof can avoid it.

Quick check. Run the proof of Theorem 6.2.1 on $A = \{1, 2, 3\}$ and $B = \{x, y\}$: describe the maximal elements of P, and say which case of the proof occurs.

Solution. A partial matching has at most two pairs, since each of x, y occurs at most once. The maximal elements are the six two-pair matchings $\{(a, x), (a', y)\}$ with $a \neq a'$ in A (three choices of a, then two of a'). A matching with fewer pairs is not maximal: it leaves some element of A and some element of B unpaired, and one more pair fits. No maximal M pairs every element of A: that would be an injection $A \to B$, impossible by Corollary 2.5.3 (a). So Case 2 occurs every time: M^{-1} is an injection $B \to A$. This is the finite example of Section 6.1, where the matching $(1, x)$, $(2, y)$ ran out of B.

A maximal matching tells us which side is used up, not that the sizes differ. For $A = B = \mathbb{N}$, the identity $\{(n, n) : n \in \mathbb{N}\}$ is a maximal matching that uses up both sides. So is $\{(n, n+1) : n \in \mathbb{N}\}$: it pairs every element of A, and although $0 \in B$ is unpaired, no element of A is left to pair it with. That matching is an injection and not a bijection, although $|\mathbb{N}| = |\mathbb{N}|$. The proof only promises an injection, and that is all it delivers.

6.2.2 Extending a partial order

Suppose a project consists of tasks, and some tasks must be done before others. Write $u \preceq v$ when task u must come no later than task v: either $u = v$, or u must be finished before v can start, directly or through a sequence of prerequisites. Counting each task as coming no later than itself makes $\preceq$ reflexive; passing prerequisites along makes it transitive; and no two different tasks can each be required before the other, or nothing could ever start. So $\preceq$ is a partial order. A **schedule** puts the tasks in one line, and it respects the prerequisites when its order, a total order, contains $\preceq$.

For finitely many tasks there is a procedure: pick a task with no unfinished prerequisite, do it, and repeat. Here is a small case. Five tasks, survey S, financing F, design D, permit P and building B, with four prerequisites:

$$S \text{ before } D, \qquad F \text{ before } D, \qquad D \text{ before } B, \qquad F \text{ before } P.$$

The order they generate consists of the five pairs (t, t), the four given pairs, and the two pairs (S, B) and (F, B) that the prerequisites pass along through D: eleven pairs in all. At the start, S and F have no prerequisites. Picking S, then F, leaves D and P free; picking D, then P, frees B. That gives the schedule

$$S,\ F,\ D,\ P,\ B.$$

Picking F first instead, then P, then S, then D, then B, gives a second schedule

$$F,\ P,\ S,\ D,\ B.$$

Each contains all eleven pairs: in both lists S and F come before D, D before B, F before P, and hence S and F before B. So schedules are not unique (there are seven in all), and the

procedure needs the tasks in hand, one free task at a time, until none is left. For an infinite set with no list there is no last step, and the maximality template does the work instead. Its engine is a single move: two incomparable elements can be made comparable without breaking anything.

A partial order on X is a relation on X, a subset of $X \times X$ (Definition 1.4.3), so it makes sense to say that one partial order is contained in another.

Lemma 6.2.3. Adding One Comparison

Let $\preceq$ be a partial order on a set X, and let $a, b \in X$ be incomparable. Let

$$R := \preceq \cup \{(x, y) \in X \times X : x \preceq a \text{ and } b \preceq y\}.$$

Then R is a partial order on X, $\preceq \subseteq R$, and $(a, b) \in R \setminus \preceq$.

Idea. R puts everything below a below everything above b. A new pair can break antisymmetry or transitivity only by producing $b \preceq a$, and incomparability forbids that.

Proof. Call a pair (x, y) **new** if $x \preceq a$ and $b \preceq y$, and **old** if $x \preceq y$. Every pair of R is old or new. The pair (a, b) is new, since $a \preceq a$ and $b \preceq b$ by (PO1), and it is not old, since a and b are incomparable. By the definition of R, $\preceq \subseteq R$.

(PO1): $x \preceq x$ for every $x \in X$, and $\preceq \subseteq R$.

(PO2): let $x \mathrel{R} y$ and $y \mathrel{R} x$. If both pairs are old, $x = y$ by (PO2) for $\preceq$. If (x, y) is new and (y, x) old, then $b \preceq y \preceq x \preceq a$, so $b \preceq a$ by (PO3), which incomparability excludes. If (x, y) is old and (y, x) new, then $b \preceq x \preceq y \preceq a$, excluded in the same way. If both are new, then $b \preceq x$ (from (y, x)) and $x \preceq a$ (from (x, y)), so again $b \preceq a$. Only the first case can occur, and it gives $x = y$.

(PO3): let $x \mathrel{R} y$ and $y \mathrel{R} z$. If both pairs are old, $x \preceq z$ by (PO3). If (x, y) is old and (y, z) new, then $x \preceq y \preceq a$ and $b \preceq z$, so (x, z) is new. If (x, y) is new and (y, z) old, then $x \preceq a$ and $b \preceq y \preceq z$, so (x, z) is new. If both are new, $x \preceq a$ and $b \preceq z$ directly. In every case $x \mathrel{R} z$.

■

Quick check. Apply Lemma 6.2.3 to $\subseteq$ on $\mathcal{P}(\{1, 2\})$ with $a = \{1\}$ and $b = \{2\}$. Which pairs does R add to $\subseteq$?

Solution. A new pair (x, y) needs $x \subseteq \{1\}$ and $\{2\} \subseteq y$: $x \in \{\emptyset, \{1\}\}$ and $y \in \{\{2\}, \{1, 2\}\}$. Of these four pairs, all but $(\{1\}, \{2\})$ already belong to $\subseteq$. So R adds exactly one pair, and it is the total order $\emptyset, \{1\}, \{2\}, \{1, 2\}$.

The lemma adds one comparison. The template adds them all at once.

Theorem 6.2.4. Every Partial Order Extends to a Total Order

Let $\preceq$ be a partial order on a set X. Then there is a total order T on X with $\preceq \subseteq T$.

This book's word is "total" (Definition 4.3.1); "linear order" is a common synonym, and T is then called a linear extension of $\preceq$.

Idea. By the method of Example (Method: the maximality template). The partial objects are the partial orders on X containing $\preceq$. The union of a chain of them is one, since (PO2) and (PO3) each mention two pairs. A maximal one is total, because Lemma 6.2.3 enlarges any partial order that has an incomparable pair.

Proof. Let P be the set of partial orders R on X with $\preceq \subseteq R$, a set of subsets of $X \times X$, ordered by $\subseteq$. Then $\preceq \in P$, so $P \neq \emptyset$.

Let $\mathcal{C} \subseteq P$ be a non-empty chain and $H := \bigcup \mathcal{C} \subseteq X \times X$. Since $\mathcal{C}$ has a member, and that member contains $\preceq$, so does H; in particular (PO1) holds for H. If $(x, y), (y, x) \in H$, some single $R_0 \in \mathcal{C}$ contains both (Lemma 6.1.1 (b)), so $x = y$ by (PO2) for R_0. If $(x, y), (y, z) \in H$, some $R_0 \in \mathcal{C}$ contains both, so $(x, z) \in R_0 \subseteq H$ by (PO3) for R_0. Hence $H \in P$, and it is an upper bound of $\mathcal{C}$.

By Theorem 6.1.2, P has a maximal element T. Suppose T is not total, and let $a, b \in X$ be incomparable for T. By Lemma 6.2.3, applied to T, there is a partial order R on X with $T \subseteq R$ and $T \neq R$. Since $\preceq \subseteq T \subseteq R$, $R \in P$, contradicting the maximality of T. So T is total.

■

Warning. **One comparison at a time.** It is tempting to skip Zorn's lemma and settle every incomparable pair at once, each in some direction. That can fail. Take equality on $X = \{1, 2, 3\}$, where no two different elements are comparable, and decide the three pairs as 1 before 2, 2 before 3, 3 before 1. Each decision alone is harmless, but together they break transitivity, and adding the pairs that transitivity demands puts 1 before 3 and 3 before 1, against (PO2). Lemma 6.2.3 adds one comparison and then passes the consequences along; the next comparison is made in the new order, where the earlier ones are already visible. The template is what turns this one-step move into a total order when the pairs cannot be listed.

Sometimes no Zorn is needed, because a formula gives the extension.

Example. A total order containing divisibility

On $\mathbb{N}$, let $x \sqsubseteq y$ mean: $y = 0$, or $x \neq 0$ and $x \leq y$. Show that $\sqsubseteq$ is a total order on $\mathbb{N}$ containing $|$, and that $\leq$ does not contain $|$.

Solution. In words, $\sqsubseteq$ is the usual order on the positive integers with 0 moved to the top.

(PO1): if $x = 0$, then $x \sqsubseteq x$ by the first alternative; otherwise $x \leq x$.

Total: let $x, y \in \mathbb{N}$. If $y = 0$, then $x \sqsubseteq y$; if $x = 0$, then $y \sqsubseteq x$; if both are non-zero, $x \leq y$ or $y \leq x$, by totality of $\leq$.

(PO2): let $x \sqsubseteq y$ and $y \sqsubseteq x$. If $y = 0$, then $y \sqsubseteq x$ cannot hold by the second alternative, which needs $y \neq 0$; so $x = 0 = y$. The case $x = 0$ is the same with the roles exchanged. If both are non-zero, $x \leq y \leq x$, so $x = y$.

(PO3): let $x \sqsubseteq y$ and $y \sqsubseteq z$. If $z = 0$, then $x \sqsubseteq z$. Otherwise the second alternative holds for (y, z): $y \neq 0$ and $y \leq z$. Then $x \sqsubseteq y$ with $y \neq 0$ also holds by the second alternative: $x \neq 0$ and $x \leq y$. So $x \leq z$, and $x \sqsubseteq z$.

Contains $|$*:* let $a, b \in \mathbb{N}$ with $a \mid b$, say $b = ka$ with $k \in \mathbb{Z}$ (Definition 1.1.2). If $b = 0$, then $a \sqsubseteq b$. If $b \neq 0$, then $a \neq 0$, since $0 \mid b$ would mean $b = k \cdot 0 = 0$. With $a, b > 0$, $k > 0$, so $k \geq 1$ and $b = ka \geq a$: $a \sqsubseteq b$.

$\leq$ *does not contain* $|$*:* $2 \mid 0$, since $0 = 0 \cdot 2$, but $2 \leq 0$ fails.

Where a formula exists, it is the better proof. Theorem 6.2.4 matters for orders such as $\subseteq$ on $\mathcal{P}(\mathbb{R})$, for which no formula for a total extension is known.

Quick check. Put $0, 1, 4, 6, 12$ in $\sqsubseteq$-order. Which two of them are comparable under $\sqsubseteq$ but not under $|$?

Solution. $1 \sqsubseteq 4 \sqsubseteq 6 \sqsubseteq 12 \sqsubseteq 0$. Every pair is comparable under $\sqsubseteq$, which is total. Under $|$: 1 divides all of them, all of them divide 0, $4 \mid 12$ and $6 \mid 12$. The remaining pair is 4, 6: $4 \sqsubseteq 6$, but neither divides the other. So 4 and 6 are the only such pair.

The four uses of the template on the main line of this chapter, side by side:

Object	Partial objects	Why unions of chains stay partial objects	Why a maximal one is complete
choice function (Theorem 6.1.3)	graphs defined on part of I	(C1), (C2) mention at most two pairs	a missed index can be added
representatives (Example (A set of representatives))	sets meeting each class at most once	the condition mentions two elements	a missed class can be added
injection (Theorem 6.2.1)	partial matchings	(M1), (M2) mention two pairs	if both sides have an unpaired element, they can be paired
total order (Theorem 6.2.4)	partial orders containing $\preceq$	(PO2), (PO3) mention two pairs	an incomparable pair can be compared (Lemma 6.2.3)

6.2.3 Optional: every vector space has a basis

Nothing later in the book depends on this subsection. For a reader who has met vector spaces, it sketches, without proving here, how *Linear Algebra*, Section 1.8 uses the same template.

A basis of a vector space V is a linearly independent set of vectors that spans V. The theorem there is that every linearly independent set $S \subseteq V$ lies in a basis. In the language of Example (Method: the maximality template), the partial objects are the linearly independent sets containing S, ordered by $\subseteq$; S itself is one. Independence is a condition on finitely many vectors at a time: a set is independent when no finite non-trivial combination of its vectors is 0. So a dependence among vectors of the union of a chain involves finitely many vectors, which lie in one member of the chain (Lemma 6.1.1 (b)), and that member is independent: the union is a partial object. Zorn's lemma gives a maximal independent set M. It spans V, since a vector outside its span could be added to M without creating a dependence, giving a strictly larger partial object. With $S = \emptyset$, every vector space has a basis, including $\mathbb{R}$ as a vector space over $\mathbb{Q}$, where no basis can be written down.

6.2.4 Exercises

6.2.4.1 A. Check your understanding

Exercise. A1

These questions are about the proof of Theorem 6.2.1.

(a) Where does the proof use (M1), and where (M2)?

(b) Why can "some $a \in A$ is unpaired" and "some $b \in B$ is unpaired" not both hold for a maximal M?

(c) If $A = \emptyset$, what is M, and which case occurs?

(d) In two sentences, give the proof's idea.

Solution.

(a) The chain step uses both, to show that the union of a chain lies in P. The step "M uses up a side" uses both for M, to see that $M \cup \{(a_0, b_0)\}$ still satisfies them. Case 1 uses (M1) to get a function $A \to B$ and (M2) for its injectivity; Case 2 uses (M2) to get a function $B \to A$ and (M1) for its injectivity.

(b) Then the pair (a, b) can be added: $M \cup \{(a, b)\}$ satisfies (M1) and (M2) and is strictly larger, so M is not maximal.

(c) $A \times B = \emptyset$, so $P = \{\emptyset\}$ and $M = \emptyset$. Case 1 occurs: every element of $\emptyset$ occurs in M, vacuously, and M is the graph of the empty function $\emptyset \to B$, which is injective. If also $B = \emptyset$, Case 2 holds as well.

(d) A maximal partial matching between A and B cannot be extended, so it uses up A or B. Read in the right direction, it is an injection.

6.2.4.2 B. Practice

Exercise. B1: Name the move, then complete it

Let R be a relation from A to B whose domain is A (Definition 1.4.3). Prove that there is a function $f\colon A \to B$ whose graph is contained in R.

Below, the proof is started; the second half is blank. *Name the move, then complete it.*

> Let P be the set of $G \subseteq R$ such that each $a \in A$ occurs in at most one pair of G, ordered by $\subseteq$. Then $\emptyset \in P$. _____ Hence the graph of f is contained in R.

Solution. The move is the maximality template, Example (Method: the maximality template); steps (2) to (4) remain.

Completion. Let $\mathcal{C} \subseteq P$ be a non-empty chain. Its union lies in R, and two pairs of the union lie in one member of $\mathcal{C}$ (Lemma 6.1.1 (b)), so an element of A occurs in at most one pair of the union. The union is in P and is an upper bound of $\mathcal{C}$. By Theorem 6.1.2, P has a maximal element M. Suppose some $a_0 \in A$ occurs in no pair of M. Since a_0 is in the domain of R, there is b_0 with $(a_0, b_0) \in R$ (one use of $\exists$E). Then $M \cup \{(a_0, b_0)\} \subseteq R$, a_0 occurs in it once, and it is strictly larger than M: a contradiction with maximality. So each $a \in A$ occurs in exactly one pair of M, and M is the graph of a function $f\colon A \to B$ (Definition 1.5.1), with $M \subseteq R$.

Exercise. B2: A total order on the subsets of a three-element set

(a) Write the eight subsets of $\{1, 2, 3\}$ in a list such that $A \subsetneq B$ always puts A before B, and prove that it does.

(b) How many total orders on $\mathcal{P}(\{1, 2\})$ contain $\subseteq$?

Solution.

(a) $\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}$. The list is arranged by the number of elements. If $A \subsetneq B$, then A has fewer elements than B (Proposition 2.5.6), so A comes in an earlier block of the list.

(b) Two. The empty set must come first, since $\emptyset \subseteq Y$ for every Y, and $\{1, 2\}$ last, since every $Y \subseteq \{1, 2\}$. The sets $\{1\}$ and $\{2\}$ are incomparable under $\subseteq$, so they may come in either order, and both orders work.

Exercise. B3: A total order on the plane

On $\mathbb{R}^2$, let $(x_1, x_2) \leq_p (y_1, y_2)$ mean $x_1 \leq y_1$ and $x_2 \leq y_2$; and let $(x_1, x_2) \leq_l (y_1, y_2)$ mean $x_1 < y_1$, or $x_1 = y_1$ and $x_2 \leq y_2$.

(a) Show that $\leq_p$ is a partial order and not total.

(b) Show that $\leq_l$ is a total order containing $\leq_p$.

Solution.

(a) (PO1), (PO2) and (PO3) for $\leq_p$ hold coordinate by coordinate, from the same proper-

ties of $\leq$ on $\mathbb{R}$; for (PO2), $x_1 = y_1$ and $x_2 = y_2$ give equal pairs. The points $(0, 1)$ and $(1, 0)$ are incomparable: $0 \leq 1$ but $1 \not\leq 0$ in the second coordinate, and the reverse in the first.

(b) That $\leq_l$ is a total order is the argument of Section 4.3, Exercises A1 (d) and C1 (a), with $\mathbb{R}$ in place of $\mathbb{N}$: it uses only trichotomy and transitivity of $\leq$. Containment: if $x_1 \leq y_1$ and $x_2 \leq y_2$, then either $x_1 < y_1$, or $x_1 = y_1$ and $x_2 \leq y_2$; in both cases $(x_1, x_2) \leq_l (y_1, y_2)$.

6.2.4.3 C. Going deeper

Exercise. C1: Exit check: an order is the intersection of its total extensions

Let $\preceq$ be a partial order on a set X, and let $\mathcal{T}$ be the set of total orders on X that contain $\preceq$. Prove that $\preceq = \bigcap \mathcal{T}$.

Solution (Hint 1). For a pair (a, b) not in $\preceq$, you need one $T \in \mathcal{T}$ without it. If a and b are incomparable, find a partial order containing $\preceq$ and the pair (b, a).

Solution. By Theorem 6.2.4, $\mathcal{T} \neq \emptyset$, so the intersection is defined, and $\preceq \subseteq \bigcap \mathcal{T}$ since every $T \in \mathcal{T}$ contains $\preceq$.

Let $(a, b) \in X \times X$ with $(a, b) \notin \preceq$. Then $a \neq b$ by (PO1). Since $a \preceq b$ fails, either $b \preceq a$ or a and b are incomparable.

Case $b \preceq a$. Every $T \in \mathcal{T}$ contains (b, a). If it also contained (a, b), then $a = b$ by (PO2) for T. So no $T \in \mathcal{T}$ contains (a, b), and since $\mathcal{T} \neq \emptyset$, $(a, b) \notin \bigcap \mathcal{T}$.

Case a, b incomparable. Lemma 6.2.3, with b, a in place of a, b, gives a partial order $R \supseteq \preceq$ with $(b, a) \in R$. Theorem 6.2.4 applied to R gives a total order $T \supseteq R$. Then $T \in \mathcal{T}$ and $(b, a) \in T$, so $(a, b) \notin T$ by (PO2), as $a \neq b$. Hence $(a, b) \notin \bigcap \mathcal{T}$.

In both cases $(a, b) \notin \bigcap \mathcal{T}$, so $\bigcap \mathcal{T} \subseteq \preceq$.

Marking scheme. (10 points) - 1: $\mathcal{T} \neq \emptyset$, cited from Theorem 6.2.4. - 1: $\preceq \subseteq \bigcap \mathcal{T}$. - 2: the two cases are exhaustive, because $a \preceq b$ fails. - 2: the case $b \preceq a$, with (PO2) and $a \neq b$. - 2: a partial order containing $\preceq$ and (b, a) (for example, the lemma with a and b exchanged). - 2: the extension of R to a total order and the conclusion. Fatal error (0 for the case concerned): applying the lemma to (a, b) unexchanged, which puts (a, b) into the extension instead of keeping it out.

Exercise. C2: Find the error

Claim: any two sets are comparable. "Proof": If A or B is empty, the empty function is an injection. Otherwise choose $a_0 \in A$ and $b_0 \in B$ and pair them. Choose $a_1 \in A \setminus \{a_0\}$ and $b_1 \in B \setminus \{b_0\}$, and so on. When one set runs out, the pairs so far are an injection from it into the other.

Is the conclusion true? Does the argument prove it?

Solution. The conclusion is true: it is Theorem 6.2.1. The argument does not prove it. It fails at "and so on ... when one set runs out", the gap that (N13) of Logic and Proof, Example (What is not allowed) flags: an "and so on" needs its step, and here the process has no last step in general. Indexed by $\mathbb{N}$, it uses a countable set of elements of each side (Proposition 3.1.4), and for $A = B = \mathbb{R}$ neither side runs out, since $\mathbb{R}$ is uncountable (Theorem 3.3.4). That is a counterexample to the step "the process ends". The argument also makes infinitely many choices with no rule (Section 3.2). The repair is the proof by the template, in which "cannot be continued" replaces "runs out".

Marking scheme. (10 points) - 2: the conclusion is true, with a citation. - 3: the failing line ("and so on ... runs out") identified, with the reason that it has no step. - 3: a counterexample to the step "the process ends" (for example $A = B = \mathbb{R}$), with the countability reason. - 2: the repair by the maximality template.

6.2.4.4 R. Review

Exercise. R1: Surjections one way or the other

Let A and B be non-empty sets. Prove that there is a surjection $A \to B$ or a surjection $B \to A$.

Solution. By Theorem 6.2.1, $|A| \leq |B|$ or $|B| \leq |A|$. In the first case, since $A \neq \emptyset$, Proposition 3.4.2 gives a surjection $B \to A$. In the second, since $B \neq \emptyset$, the same proposition with the roles exchanged gives a surjection $A \to B$.

Marking scheme. (10 points) - 3: comparability cited, with the two cases. - 4: in the first case, a surjection $B \to A$ from Proposition 3.4.2, with $A \neq \emptyset$ used and the direction correct. - 3: the second case, with the roles exchanged and $B \neq \emptyset$ used.

Exercise. R2: Maximal chains give Zorn's lemma

(a) Let C be a maximal chain of a partially ordered set $(X, \preceq)$: a chain contained properly in no chain. Let u be an upper bound of C in X. Show that $u \in C$, that u is the greatest element of C, and that u is a maximal element of X.

(b) Deduce Theorem 6.1.2 from the statement that every chain lies in a maximal chain.

Solution.

(a) Every element of C is below u, so $C \cup \{u\}$ is a chain containing C; by maximality it is not larger, so $u \in C$. Then $u \in C$ is above every element of C: it is the greatest element of C. Suppose $u \prec x$ for some $x \in X$. For every $c \in C$, $c \preceq u \preceq x$, so $C \cup \{x\}$ is a chain, and maximality gives $x \in C$. Then $x \preceq u$, and with $u \preceq x$, (PO2) gives $x = u$, contradicting $u \prec x$. So u is maximal in X.

(b) Let P be a non-empty partially ordered set in which every non-empty chain has an upper bound. The empty set is a chain, so by Section 6.1, Exercise B1 (Exercise (B1: Maximal chains)) with $C_0 = \emptyset$, P has a maximal chain C. It is not empty: for $p \in P$, $\{p\}$ is a chain properly containing $\emptyset$. So C has an upper bound u, and u is a

maximal element of P by (a). Since Exercise B1 was proved from Zorn's lemma, the two statements are equivalent.

Marking scheme. (10 points) - 1: $u \in C$ in (a). - 1: u is the greatest element of C. - 3: u is maximal in X, using (PO2). - 2: a maximal chain C from Exercise B1 with $C_0 = \emptyset$. - 1: $C \neq \emptyset$. - 2: an upper bound of C, and the conclusion.

Exercise. R3: The basis theorem, read as a template

This item is optional and goes with the optional subsection. A set of vectors is linearly independent when no finite non-trivial combination of its vectors is 0.

(a) Which of the template's four steps uses that independence is tested on finitely many vectors at a time?

(b) Why would the template fail for the property "S is a finite independent set"?

(c) A maximal element of a partial order need not be greatest. What does this say about bases?

Solution.

(a) Step (2), the chains: a dependence among vectors of the union of a chain involves finitely many vectors, all in one member (Lemma 6.1.1 (b)), and that member is independent.

(b) The union of a chain of finite sets need not be finite (the second warning of Section 6.1), so step (2) fails: the union need not be a partial object.

(c) This is the point of Example (Maximal elements that are not greatest). Maximal independent sets need not contain one another, so a vector space can have many bases, none of them greatest. In $\mathbb{R}^2$, $\{(1,0),(1,1)\}$ and $\{(2,0),(0,3)\}$ are both bases, and neither contains the other.