

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 pigeon-hole 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.-1.1 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 $X \rightarrow \{0, 1\}$; 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.-1.2 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 de-

fined)), 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.-1.3 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.-1.4 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.-1.5 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 $X \times X \rightarrow X$; 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 : $A \rightarrow Y$ 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 $f: X \rightarrow Y$ over y : the set $\{x \in X : f(x) = y\}$ (Example (The fibers of a function), Proposition 5.2.1).
 - **fixed point** of $f: X \rightarrow X$: 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** $\iota_A: A \rightarrow X$, $a \mapsto a$ (Definition 5.1.1).
 - **indicator function** $\mathbf{1}_A: X \rightarrow \{0, 1\}$ 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 $X \rightarrow X$; 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).