

## 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  $[0], [1], \dots, [11]$ . 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  $g: \mathbb{Z} \rightarrow Y$  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  $f: X \rightarrow Y$  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  $f: X \rightarrow Y$  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  $f: X \rightarrow Y$  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  $f(X) \rightarrow X/\sim_f$ . 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  $\Phi: f(X) \rightarrow X/\sim_f$  (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  $\Phi$  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  $f: \mathcal{P}(\{1, 2, 3\}) \rightarrow \{0, 1, 2, 3\}$  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  $f: \{1, \dots, 6\} \rightarrow \{0, 1, 2\}$ , 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  $q: X \rightarrow X/\sim_f$ ,  $q(x) = [x]$  (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**  $\iota: f(X) \rightarrow Y$ ,  $\iota(y) = y$  (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  $f$ .

$$\begin{array}{ccccccc} X & \xrightarrow{q} & X/\sim_f & \xrightarrow{\bar{f}} & f(X) & \xrightarrow{\iota} & Y \\ & & & & \searrow & & \\ & & & & f & & \end{array}$$

#### Theorem 5.2.2. Canonical Factorization

Let  $f: X \rightarrow Y$  be a function, let  $q: X \rightarrow X/\sim_f$  be the quotient map, and let  $\iota: f(X) \rightarrow Y$  be the inclusion map. There is **exactly one** function  $\bar{f}: X/\sim_f \rightarrow f(X)$  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  $\iota$  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)),<br>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),<br>well defined               |
| $f(x) = f(x')$                                                                            | $[x] = [x']$ : injective, the same equivalence<br>read right to left        |

$y \in f(X)$ , so  $y = f(a)$  with  $a \in X$   $y = \bar{f}([a])$ : 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  $\bar{f}([x]) := f(x)$  defines a function  $\bar{f}: X/\sim_f \rightarrow f(X)$  (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  $\bar{f}': X/\sim_f \rightarrow f(X)$  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  $\iota$  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** ( $\iota$ , 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  $\iota$ . 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  $\iota = \text{id}_Y$ .

*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  $f: \mathbb{Z} \times \mathbb{Z}_{>0} \rightarrow \mathbb{Q}$ ,  $f(a, b) := a/b$ . 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  $(1, 2), (2, 4), (3, 6), \dots$ , 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  $\iota = \text{id}_{\mathbb{Q}}$ . 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  $p(a, b) := a$ . 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  $q, \bar{f}, \iota$  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](#).  $\iota$  is injective, as every inclusion is; here it is  $\text{id}_{\mathbb{Q}}$ , 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  $q: X \rightarrow X/\sim$  be its quotient map, and let  $g: X \rightarrow Z$  be a function.

- (a) There is a function  $\bar{g}: X/\sim \rightarrow Z$  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  $\bar{g}([x]) := g(x)$  defines a function  $\bar{g}: X/\sim \rightarrow Z$  (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  $h: X/\sim \rightarrow Z$  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  $X \rightarrow f(X)$ ,  $x \mapsto f(x)$ . 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  $r: \mathbb{Z} \rightarrow \{0, 1\}$  send each integer to its remainder on division by 2. Show that “ $[a]_{12} \mapsto r(a)$ ” is a function  $\mathbb{Z}/12 \rightarrow \{0, 1\}$ , 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  $t: \mathbb{Z}/12 \rightarrow \mathbb{Z}/12$ .

*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),  $\bar{r}([a]_{12}) := r(a)$  is a function  $\mathbb{Z}/12 \rightarrow \{0, 1\}$ : “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  $\mathbb{Z}/2 \rightarrow \{0, 1\}$  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  $g(a) := [a + 1]_{12}$ , a function  $\mathbb{Z} \rightarrow \mathbb{Z}/12$ . 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  $t([a]_{12}) := [a + 1]_{12}$  is a function  $\mathbb{Z}/12 \rightarrow \mathbb{Z}/12$ , the **tick** of the clock. *A bijection.* In the same way,  $(a - 1) - (a' - 1) = a - a'$ , so  $s([a]_{12}) := [a - 1]_{12}$  is a function  $\mathbb{Z}/12 \rightarrow \mathbb{Z}/12$ . 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  $f: X \rightarrow Y$  is onto, then  $\iota = \text{id}_Y$ , and Theorem 5.2.2 reads  $f = \bar{f} \circ q$  with  $\bar{f}: X/\sim_f \rightarrow Y$  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  $c: X/\sim \rightarrow X$  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  $\mathbb{Z}/10 \rightarrow \mathbb{Z}/5$ ? Is it injective? Is it surjective?

*Solution.* Take  $g: \mathbb{Z} \rightarrow \mathbb{Z}/5$ ,  $g(a) = [a]_5$ . *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

- For  $f: \mathbb{R} \rightarrow \mathbb{R}$ ,  $f(x) = x^2 - 1$ , find the fibers over 3, over  $-1$  and over  $-2$ . Which of them are classes of  $\sim_f$ ?
- Let  $f: \{a, b, c, d\} \rightarrow \{1, 2, 3\}$  send  $a$  and  $c$  to 1, and  $b$  and  $d$  to 3. Write down  $X/\sim_f$ ,  $f(X)$ ,  $\bar{f}$  and  $\iota$  of Theorem 5.2.2.
- 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  $f(\{a, c\}) = 1$ ,  $f(\{b, d\}) = 3$ , and  $\iota: \{1, 3\} \rightarrow \{1, 2, 3\}$  sends  $1 \mapsto 1$  and  $3 \mapsto 3$ . The value 2 is in the codomain but outside the image, which is why  $\iota$  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  $f: \mathbb{R} \rightarrow \mathbb{R}$ ,  $f(x) = |x|$ . 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  $\mathbb{R}/\sim_f \rightarrow \mathbb{R}$ .

*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  $\geq 0$ , 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  $f: X \rightarrow Y$  and  $g: X \rightarrow Z$  be functions. Prove that  $\sim_f = \sim_g$  if and only if there is a bijection  $h: f(X) \rightarrow g(X)$  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  $\bar{f}: X/\sim \rightarrow f(X)$  and  $\bar{g}: X/\sim \rightarrow g(X)$  with  $\bar{f}([x]) = f(x)$  and  $\bar{g}([x]) = g(x)$ . The inverse  $\bar{f}^{-1}: f(X) \rightarrow X/\sim$  is a bijection (Definition 1.6.2, Theorem 1.6.4), so  $h := \bar{g} \circ \bar{f}^{-1}: f(X) \rightarrow g(X)$  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  $X/\sim \rightarrow X/\approx$ . Give the instance  $\mathbb{Z}/12 \rightarrow \mathbb{Z}/4$ .

*Solution.* Apply [Theorem 5.2.3](#) to the relation  $\sim$  and to  $g := q_\approx: X \rightarrow X/\approx$ , 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  $\mathbb{Z}/12 \rightarrow \mathbb{Z}/4$ , 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  $g: X \rightarrow Z$  is constant on the classes of an equivalence relation  $\sim$  on  $X$  and  $g$  is surjective, then  $\bar{g}: X/\sim \rightarrow Z$  is a bijection.
- (b) For every function  $f: X \rightarrow Y$ ,  $|f(X)| = |X/\sim_f|$ .
- (c) If  $f: X \rightarrow Y$  is injective, then the quotient map  $X \rightarrow X/\sim_f$  is a bijection.
- (d) The rule  $[a]_4 \mapsto [3a]_{12}$  is a bijection  $\mathbb{Z}/4 \rightarrow \mathbb{Z}/12$ .
- (e) If  $f, g: X \rightarrow Y$  satisfy  $\sim_f = \sim_g$ , then  $f = g$ .

*Solution.*

- (a) **False.** Let  $X = \{1, 2\}$ , let  $\sim$  be equality, and let  $g: X \rightarrow \{0\}$  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  $X = Y = \mathbb{R}$ ,  $f = \text{id}_{\mathbb{R}}$  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  $f: X \rightarrow \{1, \dots, k\}$  be a function such that the fiber  $f^{-1}(\{i\})$  has exactly  $m$  elements for every  $i \in \{1, \dots, k\}$ . 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  $f: X \rightarrow \{1, \dots, k\}$  all of whose fibers over  $1, \dots, k$  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  $\{1, \dots, 0\} = \emptyset$ , so  $f$  is a function  $X \rightarrow \emptyset$ , and  $X = \emptyset$  by Proposition 1.5.2 (b). Then  $n = 0$ : for  $n \geq 1$ , a bijection  $\{1, \dots, n\} \rightarrow \emptyset$  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  $f: X \rightarrow \{1, \dots, k+1\}$  have every fiber of  $m$  elements. Put  $X' := f^{-1}(\{1, \dots, k\})$  and  $F := f^{-1}(\{k+1\})$ . 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  $f': X' \rightarrow \{1, \dots, k\}$ ,  $f'(x) := f(x)$ ; this is a function, because  $f(x) \in \{1, \dots, k\}$  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  $\bar{g}: X/\sim \rightarrow Z$  and  $h: X/\sim \rightarrow Z$  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  $\iota: \{0\} \rightarrow \{0, 1\}$  is injective; let  $u = \text{id}_{\{0,1\}}$  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  $f: X \rightarrow Y$  and  $g: X \rightarrow Z$  be functions such that, for all  $x, x' \in X$ ,  $f(x) = f(x')$  implies  $g(x) = g(x')$ .

- Prove that there is exactly one function  $h: f(X) \rightarrow Z$  with  $g(x) = h(f(x))$  for every  $x \in X$ .
- For  $f: \mathbb{R} \rightarrow \mathbb{R}$ ,  $f(x) = x^2$ , decide whether  $g(x) = x^4$  and whether  $g(x) = x^3$  are of the form  $h \circ f$  for some function  $h: f(\mathbb{R}) \rightarrow \mathbb{R}$ .

*Solution.*

- Existence.* The hypothesis says that  $g$  is constant on the classes of  $\sim_f$ . By [Theorem 5.2.3](#) (a), there is a function  $\bar{g}: X/\sim_f \rightarrow Z$  with  $\bar{g}([x]) = g(x)$ . By [Theorem 5.2.2](#),  $\bar{f}: X/\sim_f \rightarrow f(X)$ ,  $\bar{f}([x]) = f(x)$ , is a bijection, so it has an inverse  $\bar{f}^{-1}: f(X) \rightarrow X/\sim_f$

(Theorem 1.6.4), and  $\bar{f}^{-1}(f(x)) = [x]$  for every  $x \in X$ . Put  $h := \bar{g} \circ \bar{f}^{-1}$ . Then, for every  $x \in X$ ,

$$h(f(x)) = \bar{g}(\bar{f}^{-1}(f(x))) = \bar{g}([x]) = g(x).$$

*Uniqueness.* Let  $h, h': f(X) \rightarrow Z$  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  $h(t) := t^2$  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  $h(f(x)) := g(x)$  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  $h(y) := g(x)$  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.