Discrete Mathematics

Supervision 7 – Solutions with Commentary

Marcelo Fiore Ohad Kammar Dima Szamozvancev

9. On bijections

9.1. Basic exercises

1. a) Define a function that has (i) none, (ii) exactly one, and (iii) more than one retraction.

   b) Define a function that has (i) none, (ii) exactly one, and (iii) more than one section.

> ♪ The general pattern (for finite sets) is that the domain of sections is smaller than (or equal to) the codomain so elements can be “selected” from a larger set. Conversely, the domain of a retraction is greater than or equal to the codomain, so a group of elements can be “collapsed” into one. The section-retraction condition states that a section at $a \in A$ selects one of the elements that get mapped to a by the retraction.

2. Let n be an integer.

   a) How many sections are there for the absolute-value map $x \mapsto |x| : [-n..n] \to [0..n]$?

   > The absolute value function maps two integers k and $-k$ to the same natural number $|k|$ (other than 0), so a section for this map can select either of the two integers. The codomain $[0..n]$ has size $n+1$ but 0 can only be mapped to $0 \in [-n..n]$; for the remaining n inputs we have 2 choices each, giving us 2^n possible sections.

   b) How many retractions are there for the exponential map $x \mapsto 2^x : [0..n] \to [0..2^n]$?

   > The retraction only needs to map the powers of two back to their exponents, leaving $2^n - n$ naturals in $[0..2^n]$ that are not in the range of the exponential map and therefore are not constrained by the section-retraction condition. Since each of these can be mapped to any of the $\#[0..n] = n+1$ possible inputs, the exponential map has $(n+1)^{2^n - n}$ retractions.

3. Give an example of two sets A and B and a function $f : A \to B$ such that f has a retraction but no section. Explain how you know that f has these properties.

   > See §9.1.1.

4. Prove that the identity function is a bijection and that the composition of bijections is a bijection.

   > To show that the identity $\mathrm{id}_A : A \to A$ is a bijection , it is sufficient to exhibit a two sided inverse, namely id_A itself. Since it is the unit of composition, we have $\mathrm{id}_A \circ \mathrm{id}_A = \mathrm{id}_A$, which is both the left and right inverse condition.
   >
   > Let $f : A \to B$ and $g : B \to C$ be bijections, with respective inverses f^{-1} and g^{-1}. We need to show that the composite $g \circ f : A \to C$ is a bijection. Consider the function $f^{-1} \circ g^{-1} : C \to A$,

> and calculate using the inverse properties of f and g:
>
> $$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \mathrm{id}_B \circ f = f^{-1} \circ f = \mathrm{id}_A$$
> $$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ \mathrm{id}_B \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_C$$
>
> Thus, $f^{-1} \circ g^{-1}$ is a two-sided inverse of $g \circ f$, making it into a bijection.

5. For $f : A \to B$, prove that if there are $g, h \colon B \to A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ h = \mathrm{id}_B$ then $g = h$. Conclude as a corollary that, whenever it exists, the inverse of a function is unique.

> We show that if a map $f : A \to B$ has two opposite-sided inverses, they must be equal. Assume $g, h \colon B \to A$ satisfy $g \circ f = \mathrm{id}_A$ and $f \circ h = \mathrm{id}_B$. We consider the composite $g \circ f \circ h$ and calculate:
>
> $$g \circ (f \circ h) = g \circ \mathrm{id}_B = g \qquad (g \circ f) \circ h = \mathrm{id}_A \circ h = h$$
>
> and since composition is associative, we have that $g = h$.
>
> Assume a function $f : A \to B$ has two inverses $f_1^{-1}, f_2^{-1} \colon B \to A$. Then, in particular, they satisfy $f_1^{-1} \circ f = \mathrm{id}_A$ and $f \circ f_2^{-1} = \mathrm{id}_B$, so by the first part, we have that $f_1^{-1} = f_2^{-1}$.

9.2. Core exercises

1. We say that two functions $s \colon A \to B$ and $r \colon B \to A$ are a *section-retraction pair* whenever $r \circ s = \mathrm{id}_A$; and that a function $e \colon B \to B$ is an *idempotent* whenever $e \circ e = e$. This question demonstrates that section-retraction pairs and idempotents are closely connected: any section-retraction pair gives rise to an idempotent function, and any idempotent function can be split into a section-retraction pair.

   a) Let $f : C \to D$ and $g : D \to C$ be functions such that $f \circ g \circ f = f$.

      (i) Can you conclude that $f \circ g$ is idempotent? What about $g \circ f$? Justify your answers.

      > Both are idempotent, since by associativity of $\circ$ and the assumption we have:
      >
      > $$(f \circ g) \circ (f \circ g) = (f \circ g \circ f) \circ g = f \circ g$$
      > $$(g \circ f) \circ (g \circ f) = g \circ (f \circ g \circ f) = g \circ f$$

      (ii) Define a map g' using f and g that satisfies both

      $$f \circ g' \circ f = f \qquad \text{and} \qquad g' \circ f \circ g' = g'$$

      > Let $g' = g \circ f \circ g$. Then:
      >
      > $$f \circ g' \circ f = f \circ g \circ (f \circ g \circ f) = f \circ g \circ f = f$$
      > $$g' \circ f \circ g' = g \circ (f \circ g \circ f) \circ g \circ f \circ g = g \circ (f \circ g \circ f) \circ g = g \circ f \circ g = g'$$

> ♪ Straightforward questions intended to get you used to “the algebra of functions”: calculating with compositions of functions, rather than their values at arguments.

b) Show that if $s\colon A \to B$ and $r\colon B \to A$ are a section-retraction pair then the composite $s \circ r\colon B \to B$ is idempotent.

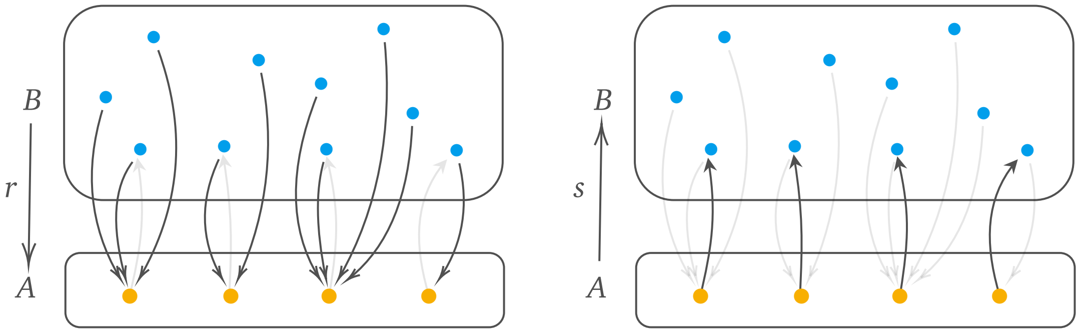
> Let $s\colon A \to B$ and $r\colon B \to A$ be a section-retraction pair with $r \circ s = \mathrm{id}_A$. We show that $s \circ r\colon B \to B$ is idempotent as follows:
>
> $$(s \circ r) \circ (s \circ r) \;=\; s \circ (r \circ s) \circ r \;=\; s \circ \mathrm{id}_A \circ r \;=\; s \circ r$$
>
> where we use assumption along with the associativity of composition and neutrality of the identity function.

c) Show that for every idempotent $e\colon B \to B$ there exists a set A (called a *retract* of B) and a section-rectraction pair $s\colon A \to B$ and $r\colon B \to A$ such that $s \circ r = e$.

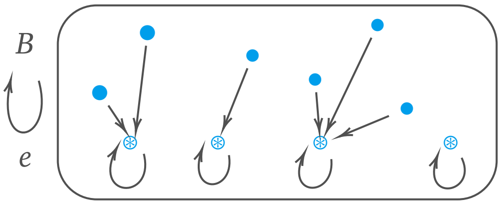
> Let $e\colon B \to B$ be an idempotent function. We need to show that there exists a set A such that e can be split into the composition $e = s \circ r$ where $s\colon A \to B$ and $r\colon B \to A$ form a section-retraction pair.
>
> Take A to be the subset $\{\, e(x) \mid x \in B \,\} \subseteq B$, i.e. the direct image of B under e. Let $s\colon A \to B$ be the subset injection $A \rightarrowtail B$, and $r\colon B \to A$ be e with its codomain restricted to its range. That is:
>
> $$s(x) = x \qquad r(y) = e(y)$$
>
> Now, the composite $s \circ r$ maps $x \in B$ to $e(x) \in A$ which is then injected to B unchanged, so $s \circ r = e$. The reverse composite $r \circ s$ maps an element $y : A$ to $e(y)$, but by definition of A there must be an $x \in B$ such that $y = e(x)$, and by the idempotence of e we have that $e(y) = e(e(x)) = e(x) = y$; thus, $r \circ s = \mathrm{id}_A$ and the two maps form a section-retraction pair.
>
> ♪ This is a rather abstract exercise which establishes a connection between idempotent maps and section-retraction pairs, namely: every sr-pair gives rise to an idempotent map, and every idempotent map can be split into a sr-pair.
>
> Idempotent maps are functions which do not need to be applied more than once: $f(f(x)) = f(x)$, so in general $f^n(x) = f(x)$ for any natural number n. Examples are the absolute value function $|{-}|\colon \mathbb{Z} \to \mathbb{Z}$, sorting algorithms and other “normalisation” procedures (once something is brought into a standardised, normal form, it should not change if normalised again), mapping a set X to its closure under some property $\mathrm{Cl}_P(X)$ (e.g. for an arbitrary relation R, taking the transitive closure of $\mathrm{Cl}_t(R)$ should be a no-op), pressing the elevator or road crossing indicator button, etc.
>
> Section-retraction pairs normally capture the idea of sorting a set of elements B into disjoint groupings labelled by A: the retraction $r\colon B \to A$ maps an element $b \in B$ to

its group label in A, while the section $s\colon A \to B$ selects a particular element $s(a) \in B$ labelled by $a \in A$. Clearly the group that a particular element of the group belongs to will be the starting group, giving rise to the required one-sided inverse condition. Examples are cities grouped by countries, students grouped by subject/college, products grouped by brands, employees grouped by department, and so on (you can probably find even more examples in the Databases course).

A common characteristic of all of these is that the set of entities is larger than the set of groups, and each group has at least one element (since the section has to select something). This is usually visualised as a vertical internal diagram, where the retraction r maps several entities in B to a single element in A, and the section s maps an element in A to one of the elements that is mapped to it by r. As this representation demonstrates, elements in B get clustered by which group they belong to, which equips B with an implicit partitioning (see §10.2.3). The section then selects a "representative element" of each partition. The section-retraction condition $r \circ s = \mathrm{id}_A$ simply states that the representative elements are in the clusters they represent – certainly desirable! For the example of cities grouped by countries, the representative element of each city cluster may be the capital city (and let's assume every country has exactly one capital), which of course has to be in the country it is a capital of.



Section-retraction parts only have a one-directional inverse property $r \circ s = \mathrm{id}_A$; nevertheless, the reverse composite $s \circ r$ – not required to be the identity – cannot be completely arbitrary either. As shown in the exercise, it has to be an idempotent map: once we do one round trip between B and A, we are "stuck" no matter how many new round trips we do. Mathematically, we have found the *fixed point* of an endofunction, i.e. the value x such that $f(x) = x$. It is easy to see that every idempotent map $e\colon B \to B$ has a fixed point $e(x)$ for all $x \in B$, since the idempotence condition $e(e(x)) = e(x)$ is precisely a fixed point equation. Graphically, we can see that following any 2-step path from $x \in B$ will lead us to the representative element, from which any round trip is merely the identity map. The composite $s \circ r$ can therefore be seen as a function on B, representing the mapping of any element in a cluster to its representative; for example, any city to the capital of its country, any student to their college student union president, any employee to their department manager.

> Now, we consider a different problem: we *start* with a set B and an endomap $e : B \to B$ satisfying $e \circ e = e$. As before, idempotence clusters elements in B since one application of e maps them to a unique representative and any new applications will simply loop on the representatives.
>
> 
>
>
> The question is: can we recover the set A and the section-retraction pair that induces e just from B and e? While we can't expect to be able to do this exactly – we'd need to figure out the names of colleges only based on the students – we can do the next best thing: find a decomposition which will be *isomorphic* to the original grouping. Looking at the diagram, it should be quite clear which elements act as representatives of the clusters and can therefore be abstractly characterised: all the outputs of the idempotent map e, i.e. the set of fixed points of e. Thus, we take the retract A to be nothing more than the subset $A \triangleq \{f(x) \mid x \in B\}$. Intuitively, we exploit the (simplified) fact that the set of capitals/presidents/managers is isomorphic to the set of countries/colleges/departments. Now, we need to find $s : A \to B$ and $r : B \to A$ satisfying $r \circ s = \mathrm{id}_A$ and $s \circ r = e$. Since A is a subset of B, there is a canonical section $s : A \to B$ that embeds A into its superset: $s(x \in A) = x \in B$. Conversely, the retraction that maps B to A is the idempotent function e itself, with its codomain restricted to its range: $r(y \in B) = e(y)$. The composite $s \circ r$ is an application of e followed by an "identity" map, so we clearly have $s \circ r = e$. To prove the section-retraction condition, take an $x \in A$ and consider $r(s(x)) = r(x) = e(x)$, which is not exactly what we need; however, we know that $x \in A$ so it must be of the form $x = e(y)$ for some $y \in B$. Thus, $r(s(x)) = r(s(e(y))) = e(e(y)) = e(y) = x$, as required.

10. On equivalence relations

10.1. Basic exercises

1. Prove that the isomorphism relation $\cong$ between sets is an equivalence relation.

> **Reflexive**. The identity $\mathrm{id}_A : A \to A$ is a bijection (§9.1.4), so we have the isomorphism $A \cong A$ for all sets A.
>
> **Symmetric**. Assume $A \cong B$; that is, there is a bijection $f : A \to B$. Its inverse $f^{-1} : B \to A$ is a bijection too, so we have the isomorphism $B \cong A$, as required.
>
> **Transitive**. Assume $A \cong B$ and $B \cong C$ with respective bijections f and g. Then the composite $g \circ f : A \to C$ is a bijection too (§9.1.4) and exhibits the isomorphism $A \cong C$.

2. Prove that the identity relation id_A on a set A is an equivalence relation, and that $A/\mathrm{id}_A \cong A$.

> The identity relation $\mathrm{id}_A : A \nrightarrow A$ is equal to the equality relation $\{ (x, y) \in A \times A \mid x = y \}$ which is an equivalence relation.
>
> The quotient set A/id_A is the set of equivalence classes of A under the equality relation: $A/\mathrm{id}_A = \{ [a]_= \subseteq A \mid a \in A \}$. The equivalence class $[a]_=$ contains all elements that are equal to a, which of course is a itself since sets have no repeated elements. Hence every equivalence class is the singleton set, and we can construct a bijection $f : A \to A/\mathrm{id}_A$ by mapping $x \in A$ to $\{ x \} \in A/\mathrm{id}_A$, and the inverse f^{-1} mapping $\{ y \}$ to y.

3. Show that, for a positive integer m, the relation $\equiv_m$ on $\mathbb{Z}$ given by

$$x \equiv_m y \iff x \equiv y \pmod{m}$$

is an equivalence relation. What are the equivalence classes of this relation?

> We have already proved that congruence is reflexive, transitive and symmetric in §2.1.1, so it is indeed an equivalence relation. The equivalence classes of congruence modulo m are the congruence classes $k_m = \{ n \in \mathbb{Z} \mid (m \mid k - n) \}$, and the quotient $\mathbb{Z}/\equiv_m$ is isomorphic to the set $\mathbb{Z}_m$ of integers modulo m.

4. Show that the relation $\equiv$ on $\mathbb{Z} \times \mathbb{Z}^+$ given by

$$(a, b) \equiv (x, y) \iff a \cdot y = x \cdot b$$

is an equivalence relation. What are the equivalence classes of this relation?

> **Reflexive**. We have to show that $(a, b) \equiv (a, b)$ for $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$; by definition, this is $a \cdot b = a \cdot b$, which is true by reflexivity of equality.
>
> **Symmetric**. Assume $(a, b) \equiv (x, y)$; that is, $ay = xb$. By symmetry of equality we have $x \cdot b = a \cdot y$ which implies $(x, y) \equiv (a, b)$, as required.
>
> **Transitive**. Assume $(a, b) \equiv (x, y)$ and $(x, y) \equiv (m, n)$; then, ① $a \cdot y = x \cdot b$ and ② $x \cdot n = m \cdot y$. We have to show that ③ $a \cdot n = m \cdot b$. Multiplying both sides of ① by n, then rearranging and applying ②, we have the following:
>
> $$a \cdot y \cdot n = x \cdot b \cdot n = x \cdot n \cdot b = m \cdot y \cdot b$$
>
> Since $y \in \mathbb{Z}^+$, it is nonzero and we can divide both sides of $a \cdot y \cdot n = m \cdot b \cdot y$ to get ③, as required.
>
> An equivalence class of this relation for a pair (a, b) contains all pairs (x, y) such that $a \cdot y = x \cdot b$; in other words, $\frac{a}{b} = \frac{x}{y}$. Thus, the relation expresses the equality of fractions, with an equivalence class corresponding to different “representations” of the same fraction, and a representative element for every class being the fraction in lowest terms. The quotient set $\mathbb{Z} \times \mathbb{Z}^+ / \equiv$ has elements corresponding to rational numbers (represented by an infinite number of distinct, but equivalent fractions of integers) so it is isomorphic to $\mathbb{Q}$.

10.2. Core exercises

1. Let E_1 and E_2 be two equivalence relations on a set A. Either prove or disprove the following statements.

   a) $E_1 \cup E_2$ is an equivalence relation on A.

   > The statement is false. Let $A = \{a, b, c\}$ and consider the equivalence relations $E_1 = \{(a,a),(a,b),(b,a),(b,b),(c,c)\}$ and $E_2 = \{(a,a),(b,b),(b,c),(c,b),(c,c)\}$. Then, the union $E_1 \cup E_2$ contains the pairs (a,b) and (b,c) but not the pair (a,c), so the union – while still being reflexive and symmetric – is not transitive.

   b) $E_1 \cap E_2$ is an equivalence relation on A.

   > Let E_1 and E_2 be two equivalence relations on A. We show that $E_1 \cap E_2$ is an equivalence relation as well, using the sufficient conditions of §6.1.3.
   >
   > **Reflexive**. We show that $\mathrm{id}_A \subseteq E_1 \cap E_2$ or equivalently, $\mathrm{id}_A \subseteq E_1$ and $\mathrm{id}_A \subseteq E_2$, which hold since E_1 and E_2 are reflexive.
   >
   > **Symmetric**. By §6.1.3(b), $(E_1 \cap E_2)^{\mathrm{op}} = {E_1}^{\mathrm{op}} \cap {E_2}^{\mathrm{op}} = E_1 \cap E_2$, since both relations are symmetric.
   >
   > **Transitive**. It is sufficient to show that $(E_1 \cap E_2) \circ (E_1 \cap E_2) \subseteq E_1 \cap E_2$, or equivalently, $(E_1 \cap E_2) \circ (E_1 \cap E_2) \subseteq E_1$ and $(E_1 \cap E_2) \circ (E_1 \cap E_2) \subseteq E_2$. Since $E_1 \cap E_2 \subseteq E_1$, by §6.2.1 we have $(E_1 \cap E_2) \circ (E_1 \cap E_2) \subseteq E_1 \circ E_1$, and by transitivity of E_1, $E_1 \circ E_1 \subseteq E_1$. The case for E_2 is similar.
   >
   > ♪ Could we have done this quite easily with element-wise reasoning? Yes. Is this approach far more satisfying? Also yes.

2. For an equivalence relation E on a set A, show that $[a_1]_E = [a_2]_E$ iff $a_1 \, E \, a_2$, where

$$[a]_E = \{ x \in A \mid x \, E \, a \}.$$

> Let E be an equivalence relation on A, and take two elements $a_1, a_2 \in A$.
>
> ($\Rightarrow$) Assume $[a_1]_E = [a_2]_E$; we need to prove that $a_1 \, E \, a_2$. By definition of equivalence classes and set equality, all elements $x \in A$ are related to a_1 if and only if they are related to a_2: $x \, E \, a_1 \iff x \, E \, a_2$. In particular, for $x = a_1$, we have $a_1 \, E \, a_1 \iff a_1 \, E \, a_2$; but E is reflexive, so $a_1 \, E \, a_1$ and from this $a_1 \, E \, a_2$ follows.
>
> ($\Leftarrow$) Assume $a_1 \, E \, a_2$ and prove that for all $x \in A$, $x \, E \, a_1$ if and only if $x \, E \, a_2$. If $x \, E \, a_1$, then by assumption and the transitivity of E, $x \, E \, a_2$. Conversely, if $x \, E \, a_2$, we can chain this with the opposite assumption $a_2 \, E \, a_1$ to get $x \, E \, a_1$, as required.

3. For a function $f : A \to B$ define a relation $\equiv_f$ on A by the rule: for all $a, a' \in A$,

$$a \equiv_f a' \iff f(a) = f(a')$$

   a) Show that for every function $f : A \to B$, the relation $\equiv_f$ is an equivalence relation on A.

> **Reflexive**. We need to show that for all $a \in A$, $a \equiv_f a$, or equivalently, $f(a) = f(a)$ – but the latter holds by reflexivity.
>
> **Symmetric**. Assume $a \equiv_f b$, that is, $f(a) = f(b)$. Then $f(b) = f(a)$, so $b \equiv_f a$, proving that $\equiv_f$ is symmetric.
>
> **Transitive**. Assume $a \equiv_f b$ and $b \equiv_f c$, that is, $f(a) = f(b)$ and $f(b) = f(c)$. By transitivity of equality, $f(a) = f(c)$, so $a \equiv_f c$, as required.

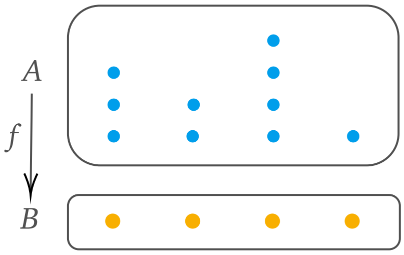
b) Prove that every equivalence relation E in a set A is equal to $\equiv_q$, where $q : A \twoheadrightarrow A/E$ is the quotient function $q(a) = [a]_E$.

> Let E be an equivalence relation on A. We need to show that for all $a, b \in A$, $a \mathrel{E} b$ if and only if $a \equiv_q b$, or, by definition, $[a]_E = [b]_E$. But this follows directly from §10.2.2.

c) Prove that for every surjection $f : A \twoheadrightarrow B$,

$$B \cong \big(A/\equiv_f\big)$$

> Let $f : A \twoheadrightarrow B$ be a surjection. We prove the isomorphism by exhibiting a bijection $g : B \to \big(A/\equiv_f\big)$ with a two-sided inverse $g^{-1} : \big(A/\equiv_f\big) \to B$.
>
> Let g map a $b \in B$ to the set $\{ a \in A \mid f(a) = b \}$; this is a non-empty set since f is a surjection, and it is an equivalence class of elements under $\equiv_f$ because any a_1, a_2 in the set gets mapped to b by f and therefore $f(a_1) = b = f(a_2)$ implies $a_1 \equiv_f a_2$.
>
> Let g^{-1} be a mapping from an equivalence class $[a]_{\equiv_f}$ of an $a \in A$ to $f(a) \in B$.
>
> We show that for all $b \in B$, $g^{-1}(g(b)) = b$. By definition of g, $g(b) = \{ a \in A \mid f(a) = b \}$ which is nonempty by the surjectivity of f; let a be one of its representative elements so that $g(b) = [a]_{\equiv_f}$. Then, $g^{-1}([a]_{\equiv_f}) = f(a)$, but by assumption, $f(a) = b$, so we indeed have $g^{-1} \circ g = \mathrm{id}_B$.
>
> Conversely, let $[a]_{\equiv_f} \in \big(A/\equiv_f\big)$ be the equivalence class of an element $a \in A$. We then have $g(g^{-1}([a]_{\equiv_f})) = g(f(a)) = \{ a' \in A \mid f(a') = f(a) \}$. But this set is precisely $\{ a' \in A \mid a' \equiv_f a \}$, the equivalence class $[a]_{\equiv_f}$ of a. Thus, $g \circ g^{-1} = \mathrm{id}_{A/\equiv_f}$, and the bijection g exhibits the isomorphism $B \cong \big(A/\equiv_f\big)$, as required.
>
> ♪ As before, the best way to get an intuition for this question is to draw a diagram. A useful visualisation of functions – similar to the clustering representation in §9.2.1 – is as elements of the domain stacked over the elements of the codomain that they are mapped to, with the individual mapping arrows left implicit (and functionality captured by the fact that a dot in A can only be over exactly one dot in B).



If the function is an injection, each column can at most one element; if it is a surjection (like f here), each column must have at least one element. The equivalence relation $\equiv_f$ in this question relates two elements in A precisely when they are in the same column, and since f is a surjection, the elements of A are all partitioned into disjoint, non-empty columns. Since each column is above an element in B, there is a bijection between the set of partitions (i.e. the set A quotiented by $\equiv_f$) and B, exhibited by a mapping between $b \in B$ and the stack of A elements that get mapped to b (sometimes called the *fiber* over b).