3 Functions

3.1 Functions

Functions are about the most important building blocks in mathematical reasoning. Functions are almost everywhere. Examples are the well known functions $f \in \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$, $f(x) = \sin(x)$, or $f(x) = \frac{1}{x^2+1}$. Actually, such functions are relations on $\mathbb{R}$: we say that $x \in \mathbb{R}$ is related to $y \in \mathbb{R}$ if and only if $f(x) = y$. Thus, every function $f \in \mathbb{R} \to \mathbb{R}$ corresponds to the relation $\{ (x, y) \mid f(x) = y \}$. This is the traditional mathematical way to define functions.

3.1 Definition. A relation R from a set B to a set V is a *function* – also called a *mapping* – if (and only if) it has the following two properties.

(a) For every $b \in B$ there is *at most one* $v \in V$ with $b R v$;

(b) For every $b \in B$ there is *at least one* $v \in V$ with $b R v$;

Requirement (a) is called the requirement of *functionality*. This can be formalized as follows: $b R u \wedge b R v \;\Rightarrow\; u = v$, for all $b \in B$ and $u, v \in V$. In words, if $b \in B$ is in relation to some element of V this element is *unique*.

Requirement (b) is called the requirement of *totality*. It states that *every* $b \in B$ is related to some element of V.

If relation R is functional but not total then R is called a *partial function*, so a (truly) partial function only satisfies (a). To emphasize that a function is not partial, functions satisfying (a) and (b) also are called *total functions*. Notice that requirements (a) and (b) together state that for every $b \in B$ there is *exactly one* $v \in V$ satisfying $b R v$.

□

By default, functions are total, unless stated otherwise. For functions we usually (but not always) use names $f, g, h, \ldots$ or $F, G, H, \ldots$. If f is a (partial or total) function from B to V we write $f(b)$ for the unique element $v \in V$ for which $b f v$, if it exists: so, $f(b) = v \;\Leftrightarrow\; b f v$.

If f is a total function we call B the *domain* of f. Now we have $f(b) \in V$ for *every* $b \in B$. If f is a partial function then f's domain is the *largest* subset of B on which f is defined. That is, subset $A : A \subseteq B$ is f's domain if and only if it satisfies both:

$$(\forall b : b \in A : (\exists v : v \in V : b f v)) \quad \text{, and:}$$
$$(\forall b : b \in B \setminus A : \neg (\exists v : v \in V : b f v)) \quad .$$

So, for partial function f from B to V with domain A we have $f(b) \in V$ for *every* $b \in A$ and $f(b)$ is *undefined* for all b not in A. Notice that every partial function from B to V with domain A is a total function from A to V.

Combining these observations we conclude that every (partial or total) function f from B to V with domain A satisfies $(\forall b : b \in A : f(b) \in V)$, and $A = B$ if and only if f is total.

The set of all functions from B to V is denoted by $B \to V$, also by V^B. If f is a function in this set we also say that "f has type $B \to V$"; also, $f \in B \to V$ and $f : B \to V$ are common ways to denote this.

3.2 Example. We already have encountered numerous examples of functions. Here are some familiar ones.

(a) polynomial functions like $f \in \mathbb{R} \to \mathbb{R}$, with $f(x) = x^3$, for all $x \in \mathbb{R}$.

(b) goniometric functions like cos, sin and tan.

(c) $\sqrt{} \in \mathbb{R}_{\geq 0} \to \mathbb{R}$, mapping the non-negative reals to their square roots.

(d) $\ln \in \mathbb{R}^+ \to \mathbb{R}$, the natural logarithm.

3.2 Equality of functions

If two (total) functions with the same domain have equal values in all points of their common domain then these functions are equal. This is rendered formally as follows:

Principle of Extensionality: Functions f and g in $B \to V$, for some sets B and V, satisfy:

$$(\forall b : b \in B : f(b) = g(b)) \;\Rightarrow\; f = g$$

□

3.3 Monotonicity of function types

If $V \subseteq W$ then every (partial or total) function in $B \to V$ also is a (partial or total) function in $B \to W$. Hence, the set $B \to V$ of functions to V is a subset of the set $B \to W$ of functions to W.

Similarly, if $A \subseteq B$ then every function f in $B \to V$ satisfies: $f(b) \in V$ for every $b \in A$. This way, f can be considered as a function of type $A \to V$. Notice, however, that this is not true from a strictly formal point of view. Recalling that a function is a relation, function f, of type $B \to V$, contains a pair (b, v), for every $b \in B$, so, also if $\neg(b \in A)$, whereas the functions in $A \to V$ only contain pairs (b, v) with $b \in A$. By omitting all pairs (b, v) with $\neg(b \in A)$, however, function f can be *restricted* to domain A. Calling the function thus obtained g, it is defined relationally by:

$$g \;=\; \{\, (b, v) \mid b \in A \wedge f(b) = v \,\} \quad .$$

Now function g has type $A \to V$, and it satisfies:

$$(\forall b : b \in A : g(b) = f(b)) \quad .$$

In practical situations, however, we usually will not introduce a separate name for this restricted function g, and we simply state that if $A \subseteq B$ then every function in $B \to V$ also has type $A \to V$.

These properties can be summarized as follows.

3.3 Properties. For sets A, B, V, W:

$$V \subseteq W \;\Rightarrow\; B \to V \subseteq B \to W$$
$$A \subseteq B \;\Rightarrow\; B \to V \subseteq A \to V$$

□

3.4 Example. Every function in $\mathbb{R} \to \mathbb{R}$ also is a function in $\mathbb{N} \to \mathbb{R}$, and every function in $\mathbb{N} \to \mathbb{N}$ also is a function in $\mathbb{N} \to \mathbb{Z}$.

3.4 Function composition

We have seen earlier that if S is a relation from set B to set V and if T is a relation from V to a set Z then their composition, as denoted by $S;T$, is a relation from B to Z. The following lemma states that relational composition of two functions itself is a function again.

3.5 Lemma. If f is a function in $B \to V$ and if g is a function in $V \to Z$ then the relation $f;g$ is a function in $B \to Z$.
□

It is common mathematical practice to write the composition of two functions f and g as $g \circ f$, instead of as $f;g$. Notice, however, that the difference is purely notational, as we now have: $g \circ f = f;g$. So, according to the above lemma, if f has type $B \to V$ and if g has type $V \to Z$ then $g \circ f$ is a function of type $B \to Z$; it is defined by:

$$(g \circ f)(b) \;=\; g(f(b)) \quad \text{, for all } b \in B \quad .$$

3.6 Properties. The following properties (b) and (c) are directly inherited from the corresponding properties of relational composition.

(a) On set B the identity relation I_B is a function from B to B, and $I_B(b) = b$, for every $b \in B$. Not surprisingly, I_B is also called the identity function on B.

(b) I is the identity of function composition: if $f \in B \to V$ then $f \circ I_B = f$ and $I_V \circ f = f$.

(c) Function composition is associative: $h \circ (g \circ f) = (h \circ g) \circ f$, for functions f, g, h of appropriate types.

3.5 Lifting a function

Let B and V be sets and let $f \in B \to V$ be a function from B to V. As stated earlier, set B is called the *domain* of f. Also, set V is called f's *codomain*.

For $b \in B$ element $f(b)$ (in V) is called the *image* of b under f, or the *value of* function f in point b. The subset of V containing all values $f(b)$, for all $b \in B$, is called the *image* of set B under f.

The notion of image can be generalized to arbitrary subsets of B. For any subset $A : A \subseteq B$ the image of A under f is a subset of V, namely:

$$\{ f(b) \mid b \in A \} \quad .$$

This subset depends, in a unique way, on subset A. So, we can define a function F, say, from the set of all subsets of B to the set of all subsets of V, as follows:

$$F(A) \;=\; \{ f(b) \mid b \in A \} \quad \text{, for all } A : A \subseteq B \quad .$$

In common mathematical language the set of all subsets of set B, also called B's *power set*, is denoted by $\mathcal{P}(B)$. Similarly, the power set of V is $\mathcal{P}(V)$. Thus, function F has type $\mathcal{P}(B) \to \mathcal{P}(V)$.

This function F also depends on f, of course. For every function f in $B \to V$ there is corresponding function F in $\mathcal{P}(B) \to \mathcal{P}(V)$, as defined above. We call F the *lifted* version of f. Function F has interesting[5] algebraic properties.

3.7 Properties.

(a) $F(\emptyset) = \emptyset$

(b) $F(\{b\}) \;=\; \{ f(b) \}$, for all $b \in B$

(c) F *distributes over* arbitrary unions; that is, for any collection Ω of subsets of B –so, $\Omega \subseteq \mathcal{P}(B)$–, we have:

$$F((\bigcup_{A : A \in \Omega} A)) \;=\; (\bigcup_{A : A \in \Omega} F(A))$$

(d) F is *monotonic*; that is, for all subsets $A0, A1$ of B:

$$A0 \subseteq A1 \;\Rightarrow\; F(A0) \subseteq F(A1)$$

(e) If F is lifted f and if G is lifted g, then $G \circ F$ is lifted $g \circ f$.

(f) For every subset $A \subseteq B$ and subset $U \subseteq V$:

$$F(A) \subseteq U \;\Leftrightarrow\; (\forall b : b \in A : f(b) \in U) \quad .$$

□

[5] In the chapter on partial orders we will see why.

Notice that Property (b) shows that, in turn, function F uniquely determines function f from which F was obtained. In a (not too strict) way, F is a *generalization* of f, of which f can be considered an instance.

A function f, of type $B \to V$, and its lifted version, of type $\mathcal{P}(B) \to \mathcal{P}(V)$ and called F above, are entirely different functions. Nevertheless, it is common mathematical practice to *denote both* by the same name f; so, instead of $f(b)$ and $F(A)$ we write $f(b)$ and $f(A)$. This, so-called, *overloading* of the name f is rather harmless, but the interpretation of an expression like $f(x)$ now depends on the type of x: if $x \in B$ the expression just means $f(x)$, but if $x \subseteq B$, that is: $x \in \mathcal{P}(B)$, then the expression means $F(x)$.

We have called the set of function values $f(b)$, for all $b \in B$, the *image* or *range* of f. In terms of lifted f the image of f just is $f(B)$.

3.8 Properties. Functions $f \in B \to V$ and $g \in V \to Z$ satisfy:

(a) $(g \circ f)(B) = g(f(B))$.

(b) $(g \circ f)(B) \subseteq g(V)$.

□

* * *

An element $b \in B$ satisfying $f(b) = v$, for some $v \in V$, is called an *original* of v under function f. As we know, because f is a function every $b \in B$ is related to a unique value, written as $f(b)$, in V. Conversely, it is not necessarily true that every $v \in V$ has a unique original in B: for any $v \in V$ set B may contain $0, 1$, or many elements b satisfying $f(b) = v$. The *whole set* of such elements b, however, is unique. That is, by lifting again, we can define a function G, say, of type $\mathcal{P}(V) \to \mathcal{P}(B)$, by:

$$G(U) \;=\; \{\, b \mid b \in B \wedge f(b) \in U \,\} \quad \text{, for all } U : U \subseteq V \quad .$$

Set $G(U)$ is called the *pre-image* under f of set U. In particular, for any value $v \in V$, the set of all elements $b \in B$ satisfying $f(b) = v$ now is $G(\{\, v \,\})$; so, the pre-image of $\{\, v \,\}$ is the set of all originals of v.

In common mathematical notation $G(U)$ is written as $f^{-1}(U)$. As we will see later, some functions f have the property that, for every $v \in V$ there is a unique $b \in B$ with $f(b) = v$. Then, a function exists, of type $V \to B$, mapping every v to this unique b. This function is called f's *inverse* and it is denoted by f^{-1}. Function G, as defined here on sets, then is the lifted version of f^{-1}, which is why it is also written as f^{-1}. So, generally we have:

$$f^{-1}(U) \;=\; \{\, b \mid b \in B \wedge f(b) \in U \,\} \quad \text{, for all } U : U \subseteq V \quad ,$$

and if function f has an inverse we have, for all $b \in B$ and $v \in V$:

$$b = f^{-1}(v) \;\Leftrightarrow\; f(b) = v \quad \text{, and:}$$

$$\{ f^{-1}(v) \} \;=\; f^{-1}(\{ v \}) \;\;,$$

3.9 Example.

(a) Let $f \in \mathbb{R} \to \mathbb{R}$ with $f(x) = x^2$ for all $x \in \mathbb{R}$. Then $f^{-1}([\,0\,,\,4\,]) \;=\; [\,-2\,,\,2\,]$.

(b) Consider the function $\mathsf{mod}\, 8$ in $\mathbb{Z} \to \mathbb{Z}$. The originals of 3 then are the elements of the set $\{\, \ldots, -13, -5, 3, 11, 19, \ldots \}$.

3.10 Theorem. Every function $f \in B \to V$ satisfies:

(a) $A \subseteq f^{-1}(f(A))$, for all $A : A \subseteq B$;

(b) $f(f^{-1}(U)) \subseteq U$, for all $U : U \subseteq V$.

□

3.11 Example. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$, for all $x \in \mathbb{R}$. Then the range $f^{-1}(f([\,0\,,\,1\,]))$ equals $[\,-1\,,\,1\,]$, which properly contains $[\,0\,,\,1\,]$. Moreover, we have $f^{-1}(f([\,-4\,,\,4\,])) \;=\; [\,0\,,\,4\,]$, which is properly contained in $[\,-4\,,\,4\,]$. This shows that we can have strict inclusions in the above theorem.

3.6 Surjective, injective, and bijective functions

Some functions have additional and useful properties. Here we define some of them.

3.12 Definition. A function $f : B \to V$ is *surjective* if every element in V is the value of f for *at least* one value in B, that is, if:

$$(\exists b : b \in B : f(b) = v) \;\;, \text{ for all } v \in V \;\;.$$

A function f in $B \to V$ is *injective* if every element in V is the value of f for *at most* one value in B, that is, if:

$$f(a) = f(b) \;\Rightarrow\; a = b \;\;, \text{ for all } a, b \in B \;\;.$$

A function f in $B \to V$ is *bijective* if it is both surjective and injective. Hence, a function is bijective if every element in V is the value of f for *exactly one* value in B.

□

3.13 Lemma. A function f in $B \to V$ is surjective if and only if $f(B) = V$.

Proof. Always holds $f(B) \subseteq V$, so it remains to prove that surjectivity is equivalent to $V \subseteq f(B)$:

f is surjective

$\Leftrightarrow$ { Definition }

$(\exists b : b \in B : f(b) = v)$ for all $v \in V$

$\Leftrightarrow$ { Definition }

$v \in f(B)$ for all $v \in V$

$\Leftrightarrow$ { Definition }

$V \subseteq f(B)$.

□

3.14 Lemma. Let $f : B \to V$ and $g : V \to Z$. Then

(a) if $g \circ f$ is injective, then f is injective;

(b) if $g \circ f$ is surjective, then g is surjective;

(c) if f and g are injective, then $g \circ f$ is injective;

(d) if f and g are surjective, then $g \circ f$ is surjective.

(e) if f and g are bijective, then $g \circ f$ is bijective.

Proof.

(a) Let $g \circ f$ is injective, we have to prove that f is injective. Let $x, x' \in B$ satisfy $f(x) = f(x')$. Then $g \circ f(x) = g(f(x)) = g(f(x')) = (g \circ f)(x')$. Since $g \circ f$ is injective we conclude $x = x'$. This proves that f is injective.

(b) Let $g \circ f$ is surjective, we have to prove that g is surjective. Let $z \in Z$, we have to find $y \in V$ such that $g(y) = z$. Since $g \circ f$ is surjective there exists $x \in B$ such that $z = (g \circ f)(x) = g(f(x)$, so choosing $y = f(x)$ does the job.

(c) Assume that f and g are injective, we have to prove that $g \circ f$ is injective. So let $x, x' \in B$ such that $(g \circ f)(x) = (g \circ f)(x')$. Since g is injective and $g(f(x)) = (g \circ f)(x) = (g \circ f)(x') = g(f(x'))$ we conclude $f(x) = f(x')$. Since f is injective we conclude that $x = x'$, proving that $g \circ f$ is injective.

(d) Assume that f and g are surjective, we have to prove that $g \circ f$ is surjective. Let $z \in Z$. Since g is surjective there exists $y \in V$ such that $g(y) = z$. Since f is surjective there exists $x \in B$ such that $f(x) = y$. Now $(g \circ f)(x) = g(f(x)) = g(y) = z$, so $g \circ f$ is surjective.

(e) Combine (c) and (d).

□

3.15 Example. This example illustrates that the "same" function is or is not surjective or injective, depending on which domain one considers.

(a) The function $\sin : \mathbb{R} \to \mathbb{R}$ is neither surjective nor injective.

(b) The function $\sin : [\,-\pi/2\,,\,\pi/2\,] \to \mathbb{R}$ is injective and not surjective.

(c) The function $\sin : \mathbb{R} \to [\,-1\,,\,1\,]$ is surjective and not injective.

(d) The function $\sin : [\,-\pi/2\,,\,\pi/2\,] \to [\,-1\,,\,1\,]$ is bijective.

□

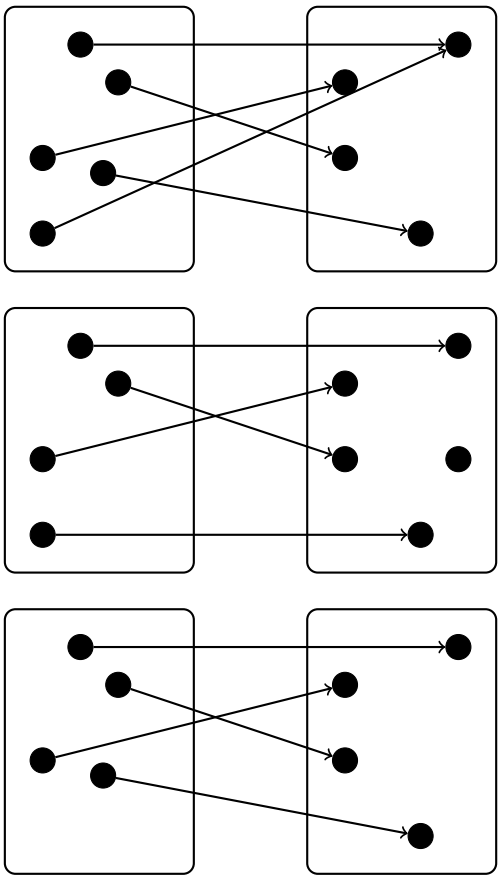

Figure 22: Surjective, injective and bijective functions

3.7 Inverse functions

In the definition of "function", in the beginning of this chapter, we have stated the requirements of "totality" and "functionality". The notion of "surjectivity" is equivalent to the notion of "totality", but with sets B and V interchanged. Similarly, the

notion of "injectivity" is equivalent to the notion of "functionality", but with B and V interchanged. Recall that for every relation R from B to V its transposition R^{T} is the relation from V to B defined by:

$$v\, R^{\mathrm{T}}\, b \;\Leftrightarrow\; b\, R\, v \quad \text{, for all } b, v \quad .$$

Function f being surjective now means that relation f^{T} is total, and f being injective means that relation f^{T} is functional. From this we conclude immediately that if f is bijective relation then f^{T} is a function from V to B. This function happens to be f's *inverse*, and it is denoted by f^{-1}.

3.16 Definition. Function g in $V \to B$ is an *inverse* of function f in $B \to V$ if:

$$g \circ f \;=\; I_B \;\wedge\; f \circ g \;=\; I_V \quad .$$

3.17 Lemma. A function has *at most one* inverse, that is, if g and h both are inverses of f, then $g = h$.

Proof. Assume that g and h both are inverses of f. Then

$$g = g \circ I_V = g \circ (f \circ h) = (g \circ f) \circ h = I_B \circ h = h.$$

□

Lemma 3.17 justifies to speak about 'the' inverse of a function rather than 'an' inverse, and to fix the notation f^{-1} for it.

3.18 Lemma. Function g is the *inverse* of function f if and only if f is the inverse of g.

Proof. Directly by definition. □

3.19 Lemma. A function f has an inverse if and only if f is bijective.

Proof. First assume that $f : B \to V$ has an inverse $g : V \to B$. Let $y \in V$, then $f(g(y)) = (f \circ g)(y) = I_V(y) = y$, proving that f is surjective.

Assume that $x, x' \in B$ satisfy $f(x) = f(x')$. Then

$$x = I_B(x) = (g \circ f)(x) = g(f(x)) = g(f(x')) = (g \circ f)(x') = I_B(x') = x',$$

proving that f is injective. So f is bijective.

Conversely, assume that $f : B \to V$ is bijective. Define $g : V \to B$ by defining $g(y)$ to be the unique element $x \in B$ such that $f(x) = y$, for every $y \in V$. Then $g(f(x)) = x$ and $f(g(y)) = y$ for all $x \in B$ and all $y \in V$, proving

$$g \circ f \;=\; I_B \;\wedge\; f \circ g \;=\; I_V,$$

hence g is the inverse of f. □

3.20 Lemma. If functions f in $B \to V$ and g in $V \to Z$ both are bijective then

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1} \quad .$$

□

Proof. We have to prove that $f^{-1} \circ g^{-1}$ is the inverse of $g \circ f$. This follows from

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ I_V \circ f = f^{-1} \circ f = I_B$$

and

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ I_V \circ g^{-1} = g \circ g^{-1} = I_Z.$$

□

3.8 Finite sets and counting

The elements of finite sets can be counted. That is, we can define a function $\#$, say, that maps every finite set to its *number of elements*. So, for finite set V its number of elements $\#V$ is a natural number. This function can be defined recursively, as follows. After all, every finite set either is $\emptyset$ or is $U \cup \{v\}$, for some smaller finite set U and some value v not in U.

3.21 Definition. For every finite set U and value v with $v \notin U$:

$$\begin{aligned} \#\emptyset &= 0 \\ \#(U \cup \{v\}) &= \#U + 1 \end{aligned}$$

□

Without proof we state that $\#$ has the following properties, which can be proved by induction on the structure of the finite sets, if so desired.

3.22 Properties. For all finite sets U, V and value v:

(0) $\#U = 0 \;\Leftrightarrow\; U = \emptyset$

(1) $\#\{v\} = 1$

(2) $0 \leq \#U$

(3) $\#(U \cup V) = \#U + \#V - \#(U \cap V)$

(4) $\#(U \cup V) \leq \#U + \#V$

(5) $\#(U \cup V) = \#U + \#V$, if $U \cap V = \emptyset$

(6) $\#V = \#U + \#(V \setminus U)$, if $U \subseteq V$

(7) $\#U \leq \#V$, if $U \subseteq V$

(8) $\#U = \#V \;\Leftrightarrow\; U = V$, if $U \subseteq V$

□

Notice that these properties are mutually dependent. For example, property (4) follows directly from (3) and (2), property (5) is an instance of (3), and (6) is an instance of (5), whereas (7) follows from (6) and (2).

* * *

Functions on finite sets yield finite images. In what follows function f has type $B \to V$, where B and V are finite sets.

3.23 Lemma. $\#(f(B)) \leq \#B$

Proof. By induction on the structure of B. If $B = \emptyset$ then $f(B) = \emptyset$ too, hence, in this case we even have $\#(f(B)) = \#B$. If $B = A \cup \{b\}$, for some b not in A we have:

$$
\begin{array}{ll}
 & \#(f(A \cup \{b\})) \\
= & \quad \{\ f \text{ over } \cup\ \} \\
 & \#(f(A) \cup f(\{b\})) \\
\leq & \quad \{\ \text{property } 3.22\,(4)\ \} \\
 & \#(f(A)) + \#(f(\{b\})) \\
= & \quad \{\ \text{definition of } f(\{b\})\ \} \\
 & \#(f(A)) + \#(\{f(b)\}) \\
= & \quad \{\ \text{property } 3.22\,(1) \text{ (twice)}\ \} \\
 & \#(f(A)) + \#(\{b\}) \\
\leq & \quad \{\ \text{Induction Hypothesis}\ \} \\
 & \#A + \#(\{b\}) \\
= & \quad \{\ \text{property } 3.22\,(5), \text{ using } \neg(b \in A)\ \} \\
 & \#(A \cup \{b\})
\end{array}
$$

□

3.24 Lemma. "f is injective" $\;\Leftrightarrow\;$ $\#(f(B)) = \#B$

Proof. By mutual implication.

"$\Rightarrow$": Very similar to the proof of Lemma 3.23, using that $\#(f(A) \cup f(\{b\}))$ now is *equal* to $\#(f(A)) + \#(f(\{b\}))$, because for injective f we have $\neg(f(b) \in f(A))$

if $\neg(b \in A)$.

"$\Leftarrow$": By contraposition, that is, if f is not injective then $\#(f(B)) \neq \#B$. If f is not injective then B contains elements a, b , say, with $a \neq b$ and $f(a) = f(b)$. Now:

$$
\begin{array}{ll}
 & \#(f(B)) \\
= & \quad \{\ a \neq b \text{ and } f(a) = f(b), \text{ so } f(B \backslash \{a\}) = f(B)\ \} \\
 & \#(f(B \backslash \{a\})) \\
\leq & \quad \{\ \text{Lemma 3.23}\ \} \\
 & \#(B \backslash \{a\}) \\
= & \quad \{\ a \in B\ \} \\
 & \#B - 1 \quad ,
\end{array}
$$

from which we conclude that $\#(f(B)) < \#B$, hence, also $\#(f(B)) \neq \#B$.

□

3.25 Lemma. "f is injective" $\Rightarrow$ $\#B \leq \#V$

Proof.

$$
\begin{array}{ll}
 & \#B \\
= & \quad \{\ f \text{ is injective: Lemma 3.24}\ \} \\
 & \#(f(B)) \\
\leq & \quad \{\ f(B) \subseteq V\text{: property 3.22 (7)}\ \} \\
 & \#V
\end{array}
$$

□

3.26 Lemma. "f is surjective" $\Rightarrow$ $\#V \leq \#B$

Proof.

$$
\begin{array}{ll}
 & \#V \\
= & \quad \{\ f \text{ is surjective: } f(B) = V\ \} \\
 & \#(f(B)) \\
\leq & \quad \{\ \text{Lemma 3.23}\ \} \\
 & \#B
\end{array}
$$

□

Corollary: "f is bijective" $\Rightarrow$ $\#V = \#B$

□

Aside: Without further proofs we observe that the converses to the two latter lemmas hold as well.

Properties.

(0) $\#B \leq \#V \;\Rightarrow\; (\exists f : f \in B \to V : \text{“}f \text{ is injective”})$

(1) $\#V \leq \#B \;\Rightarrow\; (\exists f : f \in B \to V : \text{“}f \text{ is surjective”})$

□

Now we are ready for the main theorem of this subsection.

3.27 Theorem. For f a function of type $B \to V$, for finite sets B, V, and if $\#B = \#V$, we have:

$$\text{“}f \text{ is injective”} \;\Leftrightarrow\; \text{“}f \text{ is surjective”}$$

Proof.

“f is injective”

$\Leftrightarrow$ { Lemma 3.24 }

$\#(f(B)) = \#B$

$\Leftrightarrow$ { $\#B = \#V$ }

$\#(f(B)) = \#V$

$\Leftrightarrow$ { $f(B) \subseteq V$: property 3.22 (8) }

$f(B) = V$

$\Leftrightarrow$ { Lemma 3.13 }

“f is surjective”

□

As a consequence of Theorem 3.27 we conclude that for functions from a finite set to itself, the properties injectivity and surjectivity coincide. Here finiteness is essential. For instance, the function $s : \mathbb{N} \to \mathbb{N}$ defined by $s(x) = x + 1$ for all $x \in \mathbb{N}$ is injective, but not surjective since no element maps to 0. Conversely, the function $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x - 1$ for all $x > 0$, and $f(0) = 0$ is surjective, but not injective since $f(0) = 0 = f(1)$.

3.28 Example. Suppose p and q are two different prime numbers. We consider the function φ in $[0\,..\,p) \to [0\,..\,p)$, defined by $\varphi(x) = (x * q) \bmod p$, for all $x \in [0\,..\,p)$.

We prove that φ is a bijection. By Theorem 3.27 it suffices to show that φ is injective. To this end we derive, for $x, y \in [0\,..\,p)$:

$\varphi(x) = \varphi(y)$

$\Leftrightarrow$ { definition of φ }

$$
\begin{array}{ll}
 & (x*q) \bmod p \;=\; (y*q) \bmod p \\
\Leftrightarrow & \quad \{ \text{ property of } \mathsf{mod} \ \} \\
 & ((x-y)*q) \bmod p \;=\; 0 \\
\Leftrightarrow & \quad \{ \text{ property of } \mathsf{mod} \text{ and } | \ \} \\
 & p \mid ((x-y)*q) \\
\Leftrightarrow & \quad \{ \text{ “}p \text{ is prime”: } (p\,|\,) \text{ distributes over } * \ \} \\
 & p \mid (x-y) \;\; \vee \;\; p \mid q \\
\Leftrightarrow & \quad \{ \text{ “}p \text{ and } q \text{ are prime” and } p \neq q \text{, hence: } \neg(p \mid q) \ \} \\
 & p \mid (x-y) \\
\Leftrightarrow & \quad \{ \ x, y \in [\,0\,..\,p\,) \text{, hence } -p < x-y < p \ \} \\
 & x \;=\; y \quad .
\end{array}
$$

□

3.9 Exercises

1. Set A is given by $A = \{1, 2, 3, 4\}$. Which of the following relations are functions from A to A?

   (a) $\{(1,3),(2,4),(3,1),(4,2)\}$;
   (b) $\{(1,3),(2,4)\}$;
   (c) $\{(1,1),(2,2),(3,3),(4,4),(1,3),(2,4),(3,1),(4,2)\}$;
   (d) $\{(1,1),(2,2),(3,3),(4,4)\}$.

2. Suppose f and g are functions from $\mathbb{R}$ to $\mathbb{R}$ defined by $f(x) = x^2$ and $g(x) = x+1$ for all $x \in R$. What is $g \circ f$ and what is $f \circ g$?

3. Which of the following functions from $\{1,2,3,4\}$ to $\{a,b,c,d\}$ is injective, surjective and/or bijective?

   (a) $\{(1,a),(2,d),(3,c),(4,b)\}$.
   (b) $\{(1,b),(2,d),(3,c),(4,b)\}$.
   (c) $\{(1,d),(2,b),(3,a),(4,c)\}$.
   (d) $\{(1,c),(2,d),(3,c),(4,b)\}$.

   For the bijective functions determine their inverses.

4. Which of the following functions is injective, surjective and/or bijective?

   (a) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ for all $x \in \mathbb{R}$.
   (b) $f : \mathbb{R} \to \mathbb{R}_{\geq 0}$, $f(x) = x^2$ for all $x \in \mathbb{R}$.
   (c) $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, $f(x) = x^2$ for all $x \in \mathbb{R}$.

5. Suppose R and S are relations on a set V with $R\,;S = I$ and $S\,;R = I$. Prove that both R and S are bijective functions.

6. Let R be a finite relation with adjacency matrix A. Prove the following statements:

   (a) If every row of A contains exactly one non-zero entry, then R is a function.

   (b) If, in addition, every column of A contains at most one entry, then function R is injective.

   (c) If every row and column of A contain exactly one 1, then R is a bijection. What is the adjacency matrix of the inverse function?

7. Let B and V be sets and let R be a relation from B to V. Then, for every $v \in V$, we have defined[6] the *pre-image* of v as the set ${}_R[v]$, thus:

$$ {}_R[v] = \{\, b \in B \mid bRv \,\} \quad , $$

   which, obviously, is a subset of B.

   (a) Prove that the relation $\{\, (v\,,\, {}_R[v]) \mid v \in V \,\}$ is a function from V to $\mathcal{P}(B)$ (the set of all subsets of B).

   (b) Prove that, if F is a function in $V \to \mathcal{P}(B)$, then the set R_F defined by $R_F = \{\, (b, v) \mid b \in F(v) \wedge v \in V \,\}$ is a relation from B to V, with ${}_{R_F}[v] = F(v)$, for all $v \in V$.

8. Given are two bijective functions f, of type $U \to V$, and g, of type $V \to W$. Prove that: $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

9. We consider functions f, g, h, of type $U \to U$, such that both $g \circ f$ and $h \circ g$ are bijective. Prove that $h \circ g \circ f$ is bijective as well.

10. Prove that an injective function f in $B \to V$ has a *partial inverse*, that is, a partial function g from V to B such that $g \circ f = I_B$. What is the domain of g?

11. (a) Give an example of a set A and a surjective function $f : A \to A$ for which $f(a) = f(b)$ for some $a, b \in A$, $a \neq b$.

    (b) Prove that this is not possible if A is finite.

12. Let $f, g : A \to A$ for a finite set A for which $f \circ g$ is injective. Prove that both f and g are surjective.

13. (a) Give an example of two sets $A \subseteq B$ and an injective function $f : B \to A$ such that $A \neq B$.

    (b) Prove that, if $A \subseteq B$ are finite sets and $f : B \to A$ is injective, then $A = B$.

---

[6] See the chapter on relations.