2. Functions and inverse functions

Grzegorz Kosiorowski

Krakow University of Economics

Relations and functions

Relations

Let X, Y be any sets. A *relation* (or *binary relation*) is any subset of the Cartesian product $X \times Y$. If $(x, y) \in R \subset X \times Y$, then we denote: xRy and we often say that "x is in relation R with y" or "x is related with y by R".

Functions

A *function* f from a set $X \neq \emptyset$ to a set $Y \neq \emptyset$ (notation: $f : X \to Y$) is a relation in $X \times Y$ such that each element $x \in X$ is related to exactly one $y \in Y$.
X is termed a *domain* of f and denoted by D_f. The elements of X are termed *arguments* of f. Y is called a *codomain* of f.
The set $f(X) = \{y \in Y : \exists x \in X : f(x) = y\}$ is termed the *image* of f. Its elements are called *values* of f.

Sidenotes and interpretations

A definition of a function is equivalent to one that you should know from school. The core of this definition is that a fuction assigns exactly one element of codomain to each element of a domain. You should not forget that to fully describe a function you need not only a "recipe", namely a formula for calculating a value of the function for each argument, but also a domain and codomain.
We can think of a relation as a "mutivalued function", namely an assignement such that multiple (or no) values can be assigned to each argument. Typically, a relation is not a function (however, each function is a relation).

Examples of functions

In this presentation we focus (quite uncharacteristically for our course) on real functions, namely functions which domains and codomains are subsets of $\mathbb{R}$, but there exist other functions:

- The function "mother" defined on the domain of all people assigning to each person their biological mother.
- Number sequences, namely functions defined on $\mathbb{N}$ with values in $\mathbb{R}$ ($a_n = a(n)$).
- A function on the set of countries assigning to each country its biggest trade partner (among other countries).

Examples of non-functions

The examples below are not functions (they are relations):

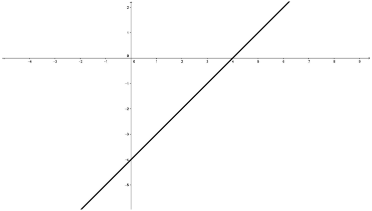
- $f(x) = \frac{1}{x}$, where $X = Y = \mathbb{R}$ (because $0 \in D_f$)
- $f(x) = y \Leftrightarrow x^2 + y^2 = 1$, $X = Y = [-1, 1]$ (because there are two different values assigned to $x = 0$)
- The "sibling relation" on the set of all people which assigns to each person their biological siblings (because some arguments would have no values assigned, and some would have multiple).

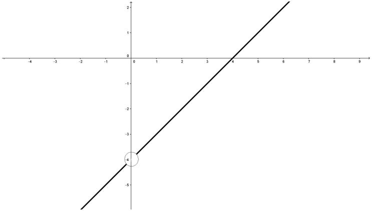
Equal functions

Equal functions

A function f is equal to a function g if $D_f = D_g$ and $\forall_{x \in D_f} f(x) = g(x)$.

Equal function: an example





$f(x) = x - 4$, $D_f = \mathbb{R}$ $\qquad$ $f(x) = \frac{x^2 - 4x}{x}$, $D_f = \mathbb{R} \setminus \{0\}$

The functions above are not equal because they have different domains.

Restriction

Typically, if we do not mention a domain of a function, we assume that it is as large as possible (namely, the largest set for which the formula of the function makes sense). If we need to "artificially" reduce the domain of a function to a certain set, we use the restriction of a function.

Restriction

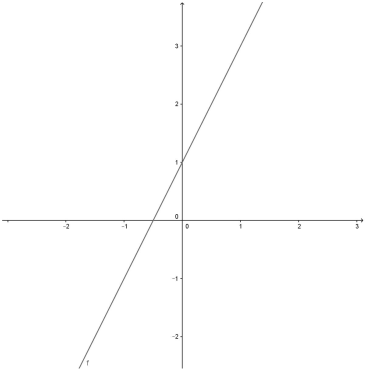
Let $f : X \to Y$ and $A \subset X$. Then $f|_A : A \to Y$ such that $\forall a \in A \; f|_A(a) = f(a)$ is termed the *restriction* of a function f to the set A.

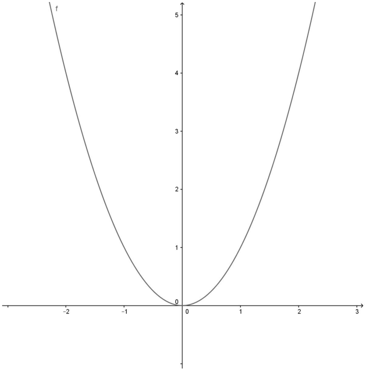
Injection

Injection (injective function)

$f : X \rightarrow Y$ is termed an injection (or an injective function) if it maps distinct elements of its domain to distinct elements of its codomain, namely $\forall_{a,b \in X}(a \neq b \Rightarrow f(a) \neq f(b))$ or (equivalently) $\forall_{a,b \in X}(f(a) = f(b) \Rightarrow a = b)$.

Injection: an example





$f(x) = 2x + 1$ is an injection.

$g(x) = x^2$ is not an injection.

Injection: example

We could easily recognize an injective (or non-injective) function from its graph, but it is always better (and more correct) to back up our intuition with a formal proof.
For a real function given by a formula $f(x) = 2x + 1$ if we assume that $f(a) = f(b)$ for some $a, b \in \mathbb{R}$, then:

$$2a + 1 = 2b + 1 \Rightarrow 2a = 2b \Rightarrow a = b,$$

thus f is an injection.
To prove that a real function $g(x) = x^2$ is not an injection, we construct a counterexample: we know that $g(-1) = 1 = g(1)$, thus g is not injective.

Injection: applications

The fact that a certain function is an injection is critical when we try to solve an equation where such a function appears. For an injection f, if $f(a) = f(b)$, then $a = b$, thus if we have f on both sides of an equation, we may "remove it" from both sides.
For example, we know that $f(x) = \sqrt{x}$ is an injection on $[0, +\infty)$. Therefore, we may transform $\sqrt{x} = 4$ into $\sqrt{x} = \sqrt{16}$ and, by the injectivity of $\sqrt{x}$, "remove" the square root from both sides of the equation and obtain $x = 16$.
This reasoning would not be correct for non-injective functions. For example, let $g(x) = x^2$, $g : \mathbb{R} \to \mathbb{R}$. Then, $x^2 = 4$ can be transformed to $x^2 = 2^2$, but now "removing" the exponent does not lead to an equivalent formula: we obtain only $x = 2$, losing the other root of the equation: $x = -2$.

Basic arithmetic on functions

Arithmetic operations on functions

Let $f : X \to \mathbb{R}$, $g : X \to \mathbb{R}$ and $\alpha \in \mathbb{R}$. Let $\diamond$ denote one of the operations: $+, -, \cdot$. Then we define:

a)$\alpha \cdot f : X \to \mathbb{R}$, $(\alpha \cdot f)(x) = \alpha \cdot f(x)$.

b)$f \diamond g : X \to \mathbb{R}$, $(f \diamond g)(x) = f(x) \diamond g(x)$.

Additionally, if $g(x) = 0 \Leftrightarrow x \in A$, then we define:

c) $\frac{f}{g} : X \setminus A \to \mathbb{R}$, $\frac{f}{g}(x) = \frac{f(x)}{g(x)}$.

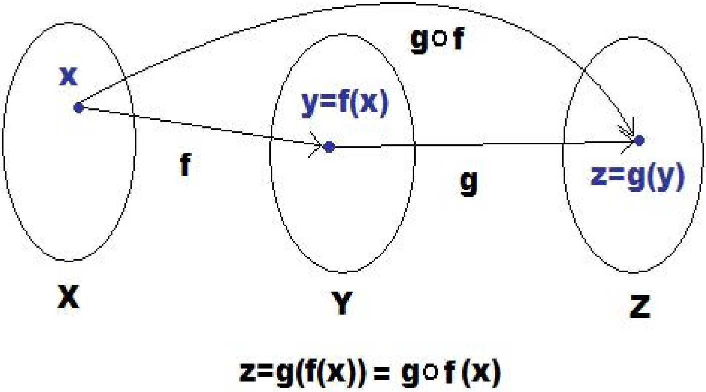
Function composition

There is one additional operation on functions (in comparison to numbers): the composition .

Composition of functions

Let $f : X \rightarrow Y$ and $g : Y \rightarrow Z$. Then $h : X \rightarrow Z$ defined by a formula $h(x) = g(f(x))$ is termed the *composition* of functions f and g. We denote it by $h = g \circ f$. f is called the *inner* function, and g - the *outer* function of this composition.

Composition: an illustration



Composition: an example

Let $f(x) = 1 - x$ and $g(x) = x^2$, $f, g : \mathbb{R} \to \mathbb{R}$. Then,
$g(f(x)) = g(1 - x) = (1 - x)^2$. Thus, $g \circ f(x) = (1 - x)^2$.
We can compose these functions in a reverse order:
$f(g(x)) = f(x^2) = 1 - x^2$. Thus, $f \circ g(x) = 1 - x^2$.
The example above shows that the composition of functions IS NOT commutative.
In particular, $g \circ f(-1) = 2^2 = 4$, and $f \circ g(-1) = 1 - 1 = 0$.

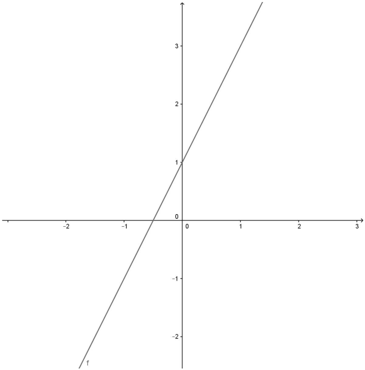
Surjection

Surjection

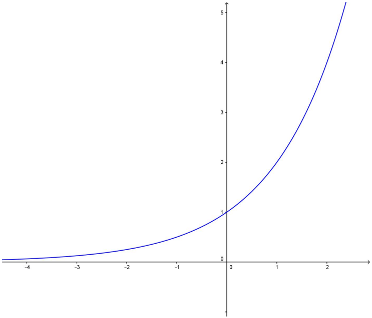
A function $f : X \to Y$ is termed a *surjection* if its codomain is equal to its image, namely $\forall_{y \in Y} \exists_{x \in X} : f(x) = y$.

For example, polynomials of odd degrees are surjections on $\mathbb{R}$. Any function can be easily transformed into a surjection: we need nothing more than reducing its codomain.

Surjection: an example



$f(x) = 2x + 1$ is a surjection as $f : \mathbb{R} \to \mathbb{R}$



$g(x) = 2^x$ is not a surjection as a function $g : \mathbb{R} \to \mathbb{R}$, but it is a surjection if $g : \mathbb{R} \to \mathbb{R}_+$

Bijection

Bijection

A function $f : X \rightarrow Y$ is termed a *one-to-one correspondence* or a *bijection* if it is an injection and a surjection.

Any monotonic function is a bijection on its domain and image (e.g. exponential functions) If $X = Y$ is a finite set, then any bijection $f : X \rightarrow X$ is termed a permutation. A permutation is often interpreted as changing the ordering of a set.

Inverse function

Inverse function

For a bijection $f : X \to Y$ we define its *inverse function* (or simply: its *inverse*) $f^{-1} : Y \to X$ as follows: $f^{-1}(y) = x$, where x is such that $f(x) = y$. This is the only function satisfying $f \circ f^{-1} = id_Y$, $f^{-1} \circ f = id_X$. A function that admits an inverse is termed *invertible*.

If f were not an injection, f^{-1} would not be uniquely defined for some elements of Y. If f were not a surjection, f^{-1} would not be defined for some elements of Y. Thus, f has to be a bijection to be invertible. We may say that the inverse function undoes the operation of an original function.

Typical inverse real functions

Below, I leave defining domains and codomains as an exercise to the readers:

- Addition and subtraction of the same number: $f(x) = x + a$ and $g(x) = x - a$ are inverse functions of each other for $a \in \mathbb{R}$ because $(x + a) - a = (x - a) + a = x$.
- Exponentiation and taking roots of the same exponent: $f(x) = x^a$ and $g(x) = \sqrt[a]{x}$ are inverse functions of each other for $a > 0$ and appropriate domains because $\sqrt[a]{x^a} = (\sqrt[a]{x})^a = x$.
- Exponential and logarithmic functions of the same base: $f(x) = a^x$ and $g(x) = \log_a x$ are inverse functions of each other for $a > 0$ and appropriate domains because $a^{\log_a x} = \log_a(a^x) = x$.

Inverting functions: a procedure

Assume that we have the formula for a real function $f(x) = \ldots$. How to find the inverse to f?

- In the initial formula we swap places of x and $f(x)$, and then substitute $f^{-1}(x)$ in place of $f(x)$ (we can also use y instead of $f^{-1}(x)$ to simplify calculations).
- We solve the obtained equation with respect to $y = f^{-1}(x)$.
- We obtain the formula for $f^{-1}(x)$

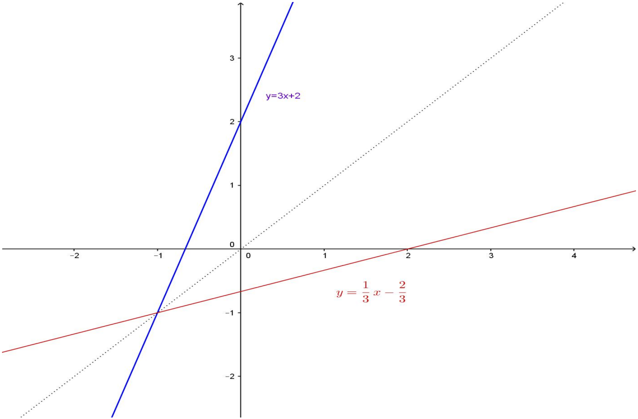
Inverting a function: an example

For example, let $f(x) = 3x + 2$, $f : \mathbb{R} \to \mathbb{R}$.
We change the original formula into $x = 3f^{-1}(x) + 2$ and, for simplicity, substitute $y = f^{-1}(x)$. We obtain $x = 3y + 2$.
We solve this equation with respect to y:

$$x = 3y + 2 \Rightarrow x - 2 = 3y \Rightarrow y = \frac{1}{3}x - \frac{2}{3}.$$

Thus, $f^{-1}(x) = \frac{1}{3}x - \frac{2}{3}$.

Graphs of inverse functions



Graphs of inverse functions

The graphs of real functions inverse to each other are symmetrical with respect to the line $y = x$.

Extra theorems

The socks-shoes property

If $f : X \to Y$ and $g : Y \to Z$ are invertible, then $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Inverse and monotonicity

If $f : X \to Y$ is increasing (resp. decreasing) and invertible, then $f^{-1} : Y \to X$ is also increasing (resp. decreasing).

Inverse for discrete sets

We are going to use inverse functions defined on discrete sets, particularly for cryptology. For example:

$$A = \{a, b, c\};\ B = \{\alpha, \beta, \gamma\}.$$

Let $f : A \to B$ be defined as follows: $f(a) = \alpha$, $f(b) = \gamma$, $f(c) = \beta$. f is a bijection so we may construct an inverse: $f^{-1} : B \to A$ as follows: $f^{-1}(\alpha) = a$, $f^{-1}(\beta) = c$ and $f^{-1}(\gamma) = b$.

Inverse for discrete sets

Example:

$$A = \{a, b, c\};\ B = \{\alpha, \beta, \gamma\}.$$

Let $g : A \rightarrow B$ be defined as follows: $g(a) = \alpha$, $g(b) = \gamma$, $g(c) = \gamma$. g is not bijective, thus not invertible: we cannot construct a value of $g^{-1}(\beta)$ (for that, surjectivity would be necessary) nor a value of $g^{-1}(\gamma)$ (for that, we would need injectivity).

Inverse for discrete sets

A bijection can only exist between sets of the same number of elements:

$$A = \{a, b, c\};\ \ C = \{1, 2, 3, 4\}.$$

Here, there exist no bijections from A to C, nor from C to A. More precisely, there are no surjections from A to C and no injections from C to A.