Remark: To prove "$(\forall n \geq n_0)\, P(n)$ is true" by strong induction, we first justify that $P(n_0)$ is true. (This is the "base case"). In "the induction step" we need to justify that the implication "$P(n_0) \wedge P(n_0+1) \wedge \cdots \wedge P(k) \to P(k+1)$ is true" for all natural numbers $k \geq n_0$. So we take an arbitrary natural number $k \geq n_0$, and we assume that each of $P(n_0), P(n_0+1), \ldots, P(k)$ is true. These are the induction hypotheses. Using the induction hypotheses we finally justify that $P(k+1)$ is true.

The format of a proof by strong induction is as follows:

Theorem: $P(n)$ for all natural numbers $n \geq n_0$

Proof: (The proof is by strong induction on n)

Base case: $P(n_0)$ is true

Induction step: Assume $k \in \mathbb{N}$ with $k \geq n_0$. Assume that $P(n_0), P(n_0+1), \ldots, P(k)$ are all true.

induction hypotheses

Then .....

.....

So $P(k+1)$ is true.

Therefore, by the principle of strong mathematical induction $P(n)$ is true for all natural numbers $n \geq n_0$. □

Ex: Prove that every natural number $n \geq 2$ can be written as a product of prime numbers.

Proof: The proof is by strong induction on n. Let "$P(n)$: n can be written as a product of prime numbers".

Base case: For $n=2$, $2=2$ which is a product consisting of one prime which is 2

So $P(2)$ is true.

Induction step: Let $k \geq 2$ be a natural number. Assume that $P(2), P(3), \ldots, P(k)$ are all true. That is, we assume that any natural number m with $2 \leq m \leq k$ can be written as a product of prime numbers. We want to show that $P(k+1)$ is true. That is, we want to show that $k+1$ can be written as a product of prime numbers.

If $k+1$ is a prime number, as in the base case it is the product of one prime number and so $P(k+1)$ is true.

Assume for the rest that $k+1$ is not a prime number. Then $k+1 = ab$ for some natural numbers a, b such that $1 < a, b < k+1$. So $2 \leq a, b \leq k$, and $P(a)$ and $P(b)$ are both true by the induction hypotheses. Thus, both a and b can be written as a product of prime numbers

$$a = p_1 \cdots p_s \quad \text{and} \quad b = q_1 \cdots q_t \qquad \text{where } p_i \text{ and } q_j \text{ are some prime numbers.}$$

Now, $k+1 = ab = p_1 \cdots p_s q_1 \cdots q_t$, a product of prime numbers. So $P(k+1)$ is true.

Hence, it follows from the principle of strong mathematical induction that every natural number $n \geq 2$ can be written as a product of prime numbers. □

We usually don't define an open statement $P(n)$ in our proofs, instead of $P(t)$ we say that the result/formula for $n=t$.

In some proofs by strong inductions we may need to check the truthness of first few $P()$ values (not just the first value $P(1)$). We need this especially in proving results about sequences defined recursively. For instance, we want to prove that $u_n < 3^n$ for all $n \in \mathbb{N}^+$ where u_n is defined recursively as

$$u_{n+2} = 5u_{n+1} - 6u_n \text{ for all } n \in \mathbb{N}^+, \quad u_1 = 1, \; u_2 = 5$$

In the induction step we assume that each of $P(1), P(2), \ldots, P(k)$ is true, and

We want to justify that $P(k+1)$ is true where $k \in \mathbb{N}^+$ is choosen arbitrarily. Using the recursive definition we may write u_{k+1} in terms of u_k and u_{k-1} as

$$u_{k+1} = 5u_k - 6u_{k-1}$$

by putting $n = k-1$, but the last equation is true for $k \geq 2$. So the implication in the induction hypotheses for $k=1$ (i.e., $P(1) \to P(2)$) cannot be justified by using the last equation. We need to check that $P(1)$ and $P(2)$ are both true.

Fact: $(\forall n \in \mathbb{N}^+)\, P(n) \equiv P(1) \wedge P(2) \wedge \cdots \wedge P(m_0) \wedge (\forall k \in \mathbb{N}^+)\left(P(1) \wedge P(2) \wedge \cdots \wedge P(k) \to P(k+1)\right)$

Proof: Exercise. ∎

Ex: Prove that for any natural number n with $n \geq 14$, n can be written as a sum of 3's and 8's. (For instance, $20 = 3+3+3+3+8$ and $25 = 8+8+3+3+3$)

Proof: (Do first some scratch work. We should erase this part after we understand how to prove. We should use (strong) induction. We after checking some base cases are true, we assume that the result is true for all natural numbers $14, 15, \ldots, k$, and then we try to show that the result is true for $k+1$, where $k \geq 14$ is arbitrarily chosen.

Want "$k+1 = \underbrace{3+3+\cdots+3}_{3\text{'s}} + \underbrace{8+\cdots+8}_{8\text{'s}}$"

$k+1-3$ is a sum of 3's & 8's

$\leq k$ induction hypothesis may be applied, if $k+1-3 \geq 14$

$k+1 = 3 + (k-2)$

↑ 3's + 8's by induction hypothesis (if $k-2$ is one $14, 15, \ldots, k$)

$k \geq 16$ ⇑ { So $k+1 \geq 17$. The previous cases $14, 15, 16$ must be checked

So in the base cases we need to check that the result is true for 14, 15, 16.)

The proof is by strong induction on n. Note that

$$14 = 3+3+8, \quad 15 = 3+3+3+3+3, \quad 16 = 8+8.$$

So the result is true for $n = 14, 15, 16$.

Let $k \geq 14$ be an arbitrary natural number. Assume that the result is true for $n = 14, 15, 16, \ldots, k$. That is, we assume that any natural number m such that $14 \leq m \leq k$ can be written as a sum of 3's and 8's. We want to show that the result is true for $n = k+1$. That is, we want to show that $k+1$ can be written as a sum of 3's and 8's. As we have already checked that 14, 15, 16 can be written as a sum 3's and 8's, we may assume that $k+1 > 16$. Now

$$k+1 = 3 + (k-2)$$

As $k+1 > 16$, $14 \leq k-2 \leq k$. Thus the induction hypotheses can be applied to $(k-2)$ and gives that $(k-2)$ is a sum of 3's and 8's. Hence,

$$k+1 = 3 + (\text{a sum of 3's and 8's}) = \text{a sum of 3's and 8's}.$$

□

Ex: Prove that for any $n \in \mathbb{N}^+$ there are distinct positive integers x and y such that $x^2 + y^2 = 5^n$

Proof: (Erase this part from your final solution. Let us try to understand how we can prove. Note that $1^2 + 2^2 = 5^1$, $10^2 + 5^2 = 5^3$, ... Consider the induction step. Assume that the result is true for $n = k$. So $x_0^2 + y_0^2 = 5^k$ for some distinct positive integers x_0 and y_0. We want to find distinct positive integers x and y such that $x^2 + y^2 = 5^{k+1} = 5 \cdot 5^k \overset{\text{induction hypothesis}}{=} 5(x_0^2 + y_0^2) = 5x_0^2 + 5y_0^2$

It is not clear how to find x and y (in terms of x_0 and y_0) such that $x^2+y^2 = 5x_0^2 + 5y_0^2$. One obvious choice is $x = \sqrt{5}\,x_0$ and $y = \sqrt{5}\,y_0$, but then x and y are not integers. However, it is clear now that $5x_0$ and $5y_0$ are distinct positive integers such that $(5x_0)^2 + (5y_0)^2 = 5^2(x_0^2+y_0^2) = 5^2 5^k = 5^{k+2}$. So the result is true for $n = k+2$. To sum up, letting $P(n)$ the desired result for n, we have managed to show that the implication $P(k) \to P(k+2)$ is true. So the truthness of $P(m+1)$ can be obtained from the truthness of $P(m-1)$ (not of $P(m)$). So we need to apply "strong induction" As $m-1 = 0$ for $m+2 = 2$, thruthess of $P(2)$ cannot be obtained because $P(0)$ is not allowed. So we need to check $P(2)$ also in base cases).

The proof will be by strong induction on n. Let $P(n)$ be the open statement "there are distinct positive integers x and y such that $x^2+y^2 = 5^n$".

Base cases: As $1^2+2^2 = 5^1$ and $3^2+4^2 = 5^2$, $P(1)$ and $P(2)$ are both true.

Induction step: Let $k \in \mathbb{N}^+$. Assume that all of $P(1), P(2), \dots, P(k)$ are true. (That is we assume that for any $t \in \mathbb{N}^+$ with $1 \le t \le k$ there are positive distinct integers x and y such $x^2+y^2 = 5^t$). We want to prove that $P(k+1)$ is true. As we have already checked that $P(1)$ and $P(2)$ are both true, we may assume that $k+1 > 2$. So $k-1 \ge 1$ (and we may use the induction hypothesis that "$P(k-1)$ is true"). By the induction hypotheses, $P(k-1)$ is true. So there are distinct positive integers x_0 and y_0 such that $x_0^2 + y_0^2 = 5^{k-1}$. Multiplying both sides by 5^2 we get $(5x_0)^2 + (5y_0)^2 = 5^{k+1}$. As $(5x_0)$ & $(5y_0)$ are distinct positive integers, $P(k+1)$ is true, as desired.

Consequently, the result follows by strong induction. □

Ex: Prove that $5^n - 3^n - 2^n$ is divisible by 30 for any odd natural number n.

Sol: As any odd natural number is of the form $2m+1$ with $m \in \mathbb{N}$, the given

result is equivalent to "$5^{2m+1} - 3^{2m+1} - 2^{2m+1}$ is divisible by 30 for any $m \in \mathbb{N}$"
We will prove this equivalent version. Let $P(m)$ denotes the open statement "$5(25)^m - 3(9)^m - 2(4)^m$ is divisible by m". We are required to prove that $(\forall m \in \mathbb{N})\ P(m)$ is true.

The proof will be by induction on m.

Base case: For $m=0$, $5(25)^m - 3(9)^m - 2(4)^m = 0$ and it is divisible by 30.

So $P(0)$ is true.

Induction step: Let $k \in \mathbb{N}$. Assume that $P(k)$ is true. That is, assume that $5(25)^k - 3(9)^k - 2(4)^k$ is divisible by 30. We want to show that $P(k+1)$ is true. That is, we want to show that $5(25)^{k+1} - 3(9)^{k+1} - 2(4)^{k+1}$ is divisible by 30. (Erase this part from your proof. Think for a while how to show. To make use of the induction hypothesis it is reasonable to write the last formula as $125(25)^k - 27(9)^k - 8(4)^k$. Denote it by N. We may try to find multiples of the induction hypothesis in N.

$$N = 25\underbrace{\left(5(25)^k - 3(9)^k - 2(4)^k\right)}_{\text{divisible by 30}} + \underbrace{48(9)^k + 42(4)^k}_{\text{not know whether 30 divides}}$$

(We further try to find multiples of 30)

$$= 25\underbrace{(\cdots\cdots)}_{\text{divisible by 30}} + \underbrace{30(9)^k + 30(4)^k}_{\text{divisible by 30}} + \underbrace{18(9^k) + 12(4)^k}_{\text{not know}}$$

(It may be useful to write it as $\cdots (9^k - 4^k)$)

$$= 25\underbrace{(\cdots\cdots)}_{} + 30(9)^k + 30(4)^k + \underbrace{18(9)^k - 18(4^k)}_{18(9^k - 4^k)} + \underbrace{18(4)^k + 12(4)^k}_{= 30(4)^k \text{ divisible by 30}}$$

$18(9^k - 4^k)$
$= 18(9-4)(9^{k-1} + \cdots + 4^{k-1})$ if $k>0$
$= 18(0)$ if $k=0$
In any case it is divisible by 30

Now,

$$5(25)^{k+1} - 3(9)^{k+1} - 2(4)^{k+1} = 25\underbrace{\left(5(25)^k - 3(9)^k - 2(4)^k\right)}_{\text{divisible by 30 by induction hypothesis}} + \underbrace{30(9)^k + 60(4)^k + 18(9^k - 4^k)}_{\text{divisible by 30}}$$

So the number on the LHS of the above equation is divisible by 30, because $18(9^k - 4^k) = 18(9-4)(9^{k-1} + 9^{k-2}4 + \cdots + 9\,4^{k-2} + 4^{k-1})$ is divisible by 30.

So $P(k+1)$ is true, as desired. □

Exercise: Prove that $(3+\sqrt{5})^n + (3-\sqrt{5})^n$ is an even integer for all $n \in \mathbb{N}$

"Assume that P(k-1) is true, and show that P(k) is true" This is what textbook does in the induction steps

"Assume that P(k) is true and show that P(k+1) is true" This is what I did in the induction steps

EXERCISE 16.19. Explain what is wrong with the following "proof" that all horses have the same colour.

Attempt at a proof by induction. Define

$P(n)$: In every set of n horses, all of the horses have the same colour.

(i) *Base case.* For $n = 1$, let H be any set of n horses. Since $n = 1$, there is only one horse in H, so it is obvious that all of the horses in H have the same colour.

(ii) *Induction step.* Assume $n > 1$, and let H be any set of n horses. Remove one horse h_1 from H to form a set H_1 of $n-1$ horses. By the induction hypothesis, we know that

(16.20) all of the horses in H_1 have the same colour.

$H_1 = H - \{h_1\}$

P(n-1) is true by the induction hypothesis

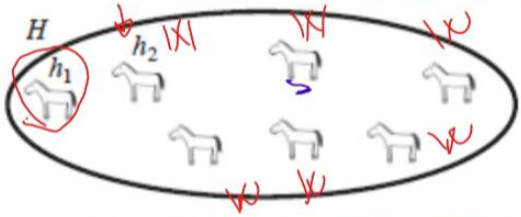
Now, remove some other horse h_2 from H to form a different set H_2 of $n-1$ horses. By applying the induction hypothesis again, we know that

(16.21) all of the horses in H_2 have the same colour.

$H_2 = H - \{h_2\}$

Now, since H_1 and H_2 each contain all but one of the elements of H, they have an intersection. (Namely, all of the horses other than h_1 and h_2 are in both H_1 and H_2.)

No



n=2

H

h_1 h_2

Therefore, we may choose some horse h that is in both H_1 and H_2. Then, from (16.21) and (16.21), we see that all of the horses in H_1 have the same colour as h, and so do all of the horses in H_2. So all of the horses in $H_1 \cup H_2$ have the same colour (namely, the colour of horse h). Since it is clear that $H = H_1 \cup H_2$ (because H_1 contains every horse except h_1, which is in H_2), we conclude that all of the horses in H have the same colour.

By the Principle of Mathematical Induction, we conclude that, in every (finite) set of horses, all of the horses have the same colour. □

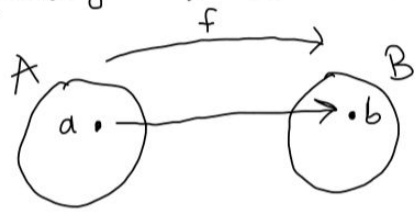
The case for n=2 is Not correct. !

for n=2, $H_1 \cap H_2 = \emptyset$

Functions

Definition: Let A and B be sets.

(1) A function f from A to B denoted by $f: A \to B$, is a rule assigning every element a of A to a unique (exactly one) element b of B. We write $f(a) = b$ to denote this.



$f: A \to B$, $f(a) = b$

$a \overset{f}{\mapsto} b$

(The property "assigning every element a of A to a unique element b of B" is called being the well-defined. We will see this in our future lectures. Functions must be well-defined. If $f(a) = b$, we may say that "a maps to b" or "a goes to b" under f)

(Identifying a function with its graph we may define a function as a set which is sometimes more useful, and which allows us to get rid of the ambigious word "rule" in the definition (1). So the definition (2) below is the formal definition of a function)

(2) A function f from A to B, denoted by $f: A \to B$, is any subset f of $A \times B$ such that for any $a \in A$ there is exactly one pair (a, b) in f whose first coordinate is a (that is, for any $a \in A$ there is a unique $b \in B$ such that $(a, b) \in f$)

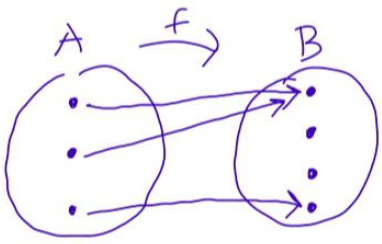
(3) The passages between the definitions (1) and (2) are obvious. If $f(x) = y$ is the rule defining a function $f: A \to B$, then $f = \{(x, f(x)) \mid x \in A\} \subseteq A \times B$. Conversely, if a subset f of $A \times B$ is a function $f: A \to B$, then f is defined by the rule $f(x) = y$ for any $(x, y) \in f$.

(4) If $f: A \to B$ is a function, then A is called the domain of A and B is called the codomain of B.

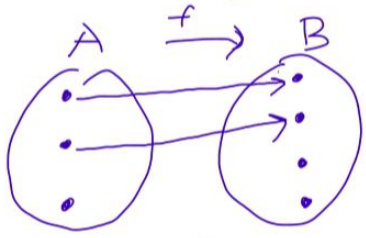
(5) Any subset of $A \times B$ is called a relation from A to B. So any function is a relation but not conversely. We will study relations later.

Ex: Determine whether each of the following is a function or not:

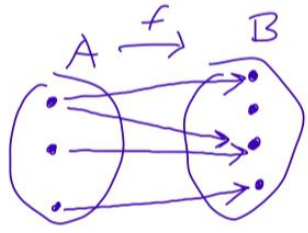
(1)



a function



not a function



not a function

(2) $A=\{a,b,c\}$ $B=\{1,2,3,4\}$

$f=\{(a,1),(b,1),(c,1)\}$, $f=\{(a,1),(b,2)\}$, $f=\{(a,1),(b,2),(c,3),(a,4)\}$

a function not a function not a function.

(3) let $f(x)=\frac{1}{x+1}$. Then f is a function, $f: \mathbb{R}-\{-1\}\to\mathbb{R}$.

Note that the domain of f cannot contain -1.

let $g(x)=x^2$. Then g is a function, $g:\mathbb{R}\to\{x\in\mathbb{R}\mid x\geq 0\}$. Note that any subset of $\mathbb{R}$ containing $\{x\in\mathbb{R}\mid x\geq 0\}$ can be taken as a codomain.

(4) If $f:\mathbb{R}\to\mathbb{R}$ is a function defined by $f(x)=x^2$ for all $x\in\mathbb{R}$, then as a subset of $\mathbb{R}\times\mathbb{R}$ we have $f=\{(x,x^2)\mid x\in\mathbb{R}\}$

If $f=\{(a,1),(b,2),(c,2)\}$ is a function from $A=\{a,b,c\}$ to $B=\{1,2,3,4\}$, then f is defined by the rule $f(a)=1$, $f(b)=2$ and $f(c)=2$.

Ex: let A be a nonempty set. Find the number functions $A\to\phi$ and $\phi\to A$ where ϕ is the empty set.

Sol: As $A\neq\phi$, there is an $a\in A$. For any function $f:A\to\phi$, by the

definition of a function there must be a unique $b \in \phi$ such that $f(a) = b$.
As ϕ has no elements, "there is a (unique) $b \in \phi$" cannot be true.
Hence, there is no function $A \to \phi$.

Any function $g: \phi \to A$ is a subset g of $\phi \times A$ satisfying the condition: "for any $x \in \phi$ there is a unique y such that $(x,y) \in g$".

$\Vert\Vert$

"for any x, if $x \in \phi$ then there is a unique y such that $(x,y) \in g$"

False

True

So the condition is vacously true. Hence any subset of $\phi \times A$ is a function.
As $\phi \times A = \phi$, there is only one function $\phi \to A$ ——— ∘ ———

Definition (Equality of functions)
Two functions $f: A \to B$ and $g: C \to D$ are called equal if $A = C$, $B = D$ and $f(a) = g(a)$ for all $a \in A$ (that is, they have the same domain, codomain and rule)

Image, Preimage, Range

Definition: Let $f: A \to B$ be a function where A and B are sets.

(1) For any subset P of A we define the image of P under f to be the set

$$f(P) = \{ f(x) \mid x \in P \} = \{ y \in B \mid y = f(x) \text{ for some } x \in P \},$$ which is a subset of B.

(2) For any subset Q of B we define the preimage of Q under f to be the set

$$f^{-1}(Q) = \{ a \in A \mid f(a) \in Q \},$$ which is a subset of A.

(Here $f^{-1}(Q)$ is just a notation, that is f^{-1} is not a function)

(3) The image of A under f is called the range of f. So the range of f is

$$f(A) = \{f(a) \mid a \in A\}$$ which is a subset of the codomain B of f.

(4) When we consider the images/preimages of singletons (i.e., sets with one element) we omit the set braces. That is, for any $a \in A$ and for any $b \in B$, we write

$f(a)$ instead of $f(\{a\})$ and $f^{-1}(b)$ instead of $f^{-1}(\{b\})$.

Ex: (1) $f: \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$

$$f([-2,1)) = \{f(x) \mid x \in [-2,1)\} = \{x^2 \mid x \in [-2,1)\} = [0,4]$$

$$f^{-1}([0,4]) = \{x \in \mathbb{R} \mid f(x) \in [0,4]\} = \{x \in \mathbb{R} \mid x^2 \in [0,4]\} = [-2,2]$$

$$f^{-1}([-100,4)) = \{x \in \mathbb{R} \mid f(x) \in [-100,4)\} = \{x \in \mathbb{R} \mid x^2 \in [-100,4)\} = (-2,2)$$

(2) P = the set of all people, W = the set of all women, $f: P \to W$ is the function defined by the rule: $f(x)$ is the mother of x for any $x \in P$.

Let x_0 denote you. Then

x_0 = you

$f(x_0)$ = your mother

$$f^{-1}(f(x_0)) = f^{-1}(\{f(x_0)\}) = \{x \in P \mid f(x) \in \{f(x_0)\}\} = \{x \in P \mid f(x) = f(x_0)\}$$

$$= \{x \in P \mid \text{the mother of } x = \text{your mother}\} = \text{the set of your siblings including you.}$$

(3) $f: \mathbb{N} \to \mathbb{N}$ be the function given by $f(x)$ = the sum of all the digits of x for any $x \in \mathbb{N}$. For instance $f(203) = 2+0+3 = 5$.

$$f(\{n \in \mathbb{N} \mid 10 \le n \le 100\}) = \{f(n) \mid n \in \mathbb{N} \text{ and } 10 \le n \le 100\} = \{\text{The sum of all digits of } n \mid n \in \mathbb{N} \text{ and } 10 \le n \le 100\}$$

if $n \neq 100$, ab → a: $1,2,3,\ldots,9$ ← b: $0,1,2,\ldots,9$

$= \{1,2,3,\dots,18\} = \{n \in \mathbb{N} \mid 1 \le n \le 18\}$

$f^{-1}(1) = \{n \in \mathbb{N} \mid f(n) = 1\} = \{n \in \mathbb{N} \mid$ the sum of digits of n is $1\} = \{10^n \mid n \in \mathbb{N}\}$

$10\underbrace{\dots 0}_{\text{all zero}}$

$f^{-1}(\{1,2\}) = ?$ (exercise)

(4) Let $A = \{1,2,3,4\}$ and $B = \{x,y,z,t,u,v\}$ and f be the function

$f = \{(1,x), (2,x), (3,u), (4,x)\}$ So $f(1)=x$, $f(2)=x$, $f(3)=u$, $f(4)=x$

$f(\{1,4\}) = \{f(1), f(4)\} = \{x\}$, The range of f is $\{x,u\}$

$f^{-1}(\{t,u\}) = \{a \in A \mid f(a) \in \{t,u\}\} = \{a \in A \mid f(a)=t \text{ or } f(a)=u\} = \{3\}$

$f^{-1}(x) = \{1,2,4\}$, $f^{-1}(\{z,t,v\}) = \phi$

Ex: Let f be a function from A to B. Suppose that f is given as a subset of $A \times B$. For any subset P of A and for any subset Q of B, write $f(P)$ and $f^{-1}(Q)$ in terms of the elements of $A \times B$ and its subset f.

Sol: Recall that "$f(x)=y$ iff $(x,y) \in f$". So

$f(P) = \{f(x) \mid x \in P\} = \{y \in B \mid y = f(x) \text{ for some } x \in P\} = \{y \in B \mid (x,y) \in f \ \exists x \in P\}$

$f^{-1}(Q) = \{a \in A \mid f(a) \in Q\} = \{a \in A \mid f(a) = b \text{ for some } b \in Q\} = \{a \in A \mid (a,b) \in f \ \exists b \in Q\}$

Terminology: Some books may prefer to say "map" or "transformation" instead of function.

We write "$\forall a,b \,/\, \exists\, \forall a,b \in A$" instead of "$\forall a, \forall b \,/\, \exists\, \forall a \in A, \exists\, \forall b \in B$". Thus, for instance,

"for all a and b in A" means "for all $a \in A$ and for all $b \in B$".

Injective, Surjective, Bijective (One to one, Onto, One to one & onto)

Definition/Remark: Let $f: A \to B$ be a function.

(1) f is called injective (or one to one) if $f(a_1) \neq f(a_2)$ for all a_1 and a_2 in A such that $a_1 \neq a_2$ $\left((\forall a_1, a_2 \in A)(a_1 \neq a_2 \longrightarrow f(a_1) \neq f(a_2)\right)$. (Contrapositive of this implication is more useful, and injective functions may also be defined as follows)

(2) f is called injective if, for all a_1 and a_2 in A, $f(a_1) = f(a_2)$ implies $a_1 = a_2$

$\left((\forall a_1, a_2 \in A)(f(a_1) = f(a_2) \longrightarrow a_1 = a_2)\right)$

(3) f is not injective iff there are some a_1 and a_2 in A such that $f(a_1) = f(a_2)$ and $a_1 \neq a_2$

(4) f is called surjective (or onto) if for any $b \in B$ there is some $a \in A$ such that $f(a) = b$.

(5) f is surjective iff $f(A) = B$ iff the range of f is B.

(6) f is not surjective iff there is a $b \in B$ such that for any $a \in A$, $f(a) \neq b$.

(7) f is called bijective if f is injective and surjective.

(8) f is bijective iff for any $b \in B$ there is a unique $a \in A$ such that $f(a) = b$

Exercise: Take (1), (4) and (7) of the above as the definitions of injective, surjective and bijective function, and prove the other parts

Remark: Let $f: A \to B$ be a function.

(1) To show that f is one to one, we take arbitrary elements a_1 and a_2 in A, and we assume that $f(a_1) = f(a_2)$, and then we try to show that $a_1 = a_2$. (we may take arbitrary elements a_1 and a_2 such that $f(a_1) = f(a_2)$, and then try to show that $a_1 = a_2$)

(2) To show that f is not one to one, we find specific elements a_1 and a_2 of A such that $f(a_1) = f(a_2)$ but $a_1 \neq a_2$

(3) To show that f is onto, we first take an arbitrary element b of B, and then try to find a specific element a of A (usually a depends on b) such that $f(a) = b$

(4) To show that f is not onto, we find a specific element b of B such that $f(a) \neq b$ for all $a \in A$

(5) To show that f is bijective, we show that f is both injective and surjective

(6) To show that f is not bijective, we should show that either f is not injective or f is not surjective.

Ex (1) $f: \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$

f is not injective because for instance $f(-1) = f(1)$ but $-1 \neq 1$

f is not surjective because for instance there is no $x \in \mathbb{R}$ such that $f(x) = -1$

(i.e., $f(x) \neq -1 \ \forall x \in \mathbb{R}$)

(2) P = the set of all people, M = the set of all men, $f: P \to M$ is for any $x \in P$ by

$f(x)$ = the father of x.

f is not one to one, f is not onto

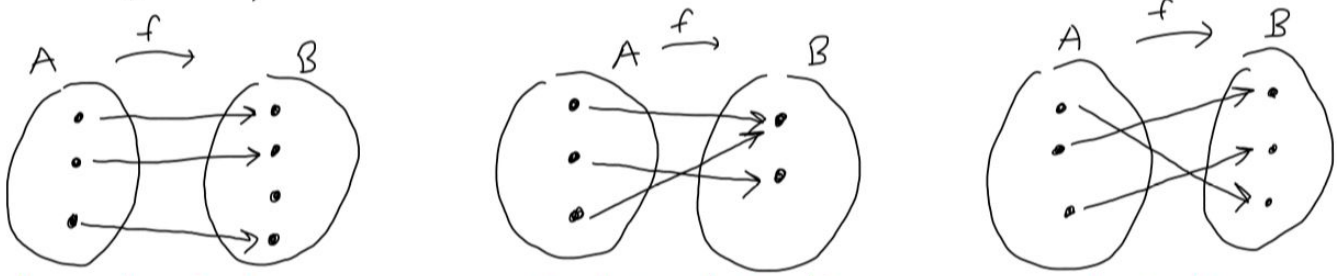
(3) $f: \mathbb{N} \to \mathbb{N}$ defined by $f(x)$ = the sum of digits of x

f is surjective, because $f(0)=0$ and given any $n \in \mathbb{N}-\{0\}$, $\underbrace{11\cdots1}_{n \text{ times}} \in \mathbb{N}$

and $f(11\cdots1)=n$.

f is not injective, because for instance $f(101)=f(11)$ and $101 \neq 11$

(4)



injective, not surjective

surjective, not injective

bijective

(5) $A=\{a,b,c,d\}$, $B=\{1,2,3,4\}$. Consider the following function

$f=\{(a,1),(b,2),(c,1),(d,4)\}$, which is a function from A to B

f is not injective because $f(a)=1=f(c)$ and $a \neq c$

f is not surjective because there is no $x \in A$ such that $f(x)=3$

Remark: Let $f: A \to B$ be a function.

(1) f is onto iff $f^{-1}(b) \neq \emptyset$ for all $b \in B$

(2) f is one to one iff $|f^{-1}(b)| \leq 1$ for all $b \in B$

(3) f is bijective iff $|f^{-1}(b)|=1$ for all $b \in B$

Proof Exercise □

Ex: Let $f: A \to B$ be a function defined as a subset of $A \times B$. Write conditions on the subset f equivalent to f being injective / surjective

Sol: f is injective iff $(\forall a_1, a_2 \in A)\ (f(a_1) = f(a_2) \to a_1 = a_2)$, $(y = f(x)$ iff $(x,y) \in f)$

iff $(\forall (a_1, b_1), (a_2, b_2) \in f\ )(\ b_1 = b_2 \to a_1 = a_2)$

f is surjective iff $\forall b \in B, \exists a \in A,\ f(a) = b$

iff $\forall b \in B, \exists a \in A,\ (a, b) \in f$

Terminology: f is injective $\equiv$ f is (an) injection

surjective $\equiv$ surjection

bijective $\equiv$ bijection

↑ adjective ↑ noun

Proposition / Exercise: Let $P_1 \subseteq A$, $P_2 \subseteq A$ and $Q_1 \subseteq B$, $Q_2 \subseteq B$ be sets, and let $f: A \to B$ be a function. Then:

(1) $f(\phi) = \phi$ and $f^{-1}(\phi) = \phi$ and $f^{-1}(B) = A$

(2) $P_1 \subseteq P_2 \implies f(P_1) \subseteq f(P_2)$

(3) $Q_1 \subseteq Q_2 \implies f^{-1}(Q_1) \subseteq f^{-1}(Q_2)$

(4) $f(P_1 \cup P_2) = f(P_1) \cup f(P_2)$

$f(P_1 \cap P_2) \subseteq f(P_1) \cap f(P_2)$

If f is injective then $f(P_1 \cap P_2) = f(P_1) \cap f(P_2)$

(5) $f^{-1}(Q_1 \cup Q_2) = f^{-1}(Q_1) \cup f^{-1}(Q_2)$

$f^{-1}(Q_1 \cap Q_2) = f^{-1}(Q_1) \cap f^{-1}(Q_2)$

(6) $P_1 \subseteq f^{-1}(f(P_1))$; If f is one to one then $P_1 = f^{-1}(f(P_2))$

(7) $f(f^{-1}(Q_1)) \subseteq Q_1$; If f is onto then $f(f^{-1}(Q_1)) = Q_1$

Proof: Exercise. We prove only (4) and (7) for illustration.

(4) Recall first the definition of the image: $f(U) = \{f(x) \mid x \in U\} = \{y \in B \mid y = f(x) \text{ for some } x \in U\}$ where $U \subseteq A$

$y \in f(P_1 \cup P_2)$ iff $y = f(x)$ for some $x \in P_1 \cup P_2$

iff $y = f(x)$ for some $x \in P_1$ or $x \in P_2$

iff $y = f(x)$ for some $x \in P_1$ or $y = f(x)$ for some $x \in P_2$

iff $y \in f(P_1)$ or $y \in f(P_2)$

iff $y \in f(P_1) \cup f(P_2)$

Therefore, it follows that $f(P_1 \cup P_2) = f(P_1) \cup f(P_2)$

Alternatively, $f(P_1 \cup P_2) = \{f(x) \mid x \in P_1 \cup P_2\} = \{f(x) \mid x \in P_1 \text{ or } x \in P_2\}$

$= \{f(x) \mid x \in P_1\} \cup \{f(x) \mid x \in P_2\}$

$= f(P_1) \cup f(P_2)$

We now want to show that $f(P_1 \cap P_2) \subseteq f(P_1) \cap f(P_2)$: Let $b \in f(P_1 \cap P_2)$. Then by the definition of the image of a subset we see that $b = f(a)$ for some $a \in P_1 \cap P_2$. As $a \in P_1 \cap P_2$, $a \in P_1$ and $a \in P_2$. Again the definition of the image gives that $f(a) \in f(P_1)$ and $f(a) \in f(P_2)$. Since $f(a)$ is in both of the sets $f(P_1)$ and $f(P_2)$, $b = f(a) \in f(P_1) \cap f(P_2)$, as desired.

We finally want to show that if f is injective, then $f(P_1 \cap P_2) = f(P_1) \cap f(P_2)$: Assume that f is injective. We want to show that $f(P_1 \cap P_2) = f(P_1) \cap f(P_2)$. Since we have already shown in the above paragraph that $f(P_1 \cap P_2) \subseteq f(P_1) \cap f(P_2)$ it suffices to prove the converse containment. Let $b \in f(P_1) \cap f(P_2)$.

Then $b \in f(P_1)$ and $b \in f(P_2)$. So there is an $a_1 \in P_1$ such that $f(a_1)=b$ and there is an $a_2 \in A$ such that $f(a_2)=b$. Thus $f(a_1)=f(a_2)$. As f is injective, $a_1=a_2$. Denote these equal elements a_1 and a_2 by c. Then $c \in P_1$ (because $c=a_1$) and $c \in P_2$ (because $c=a_2$), and hence $c \in P_1 \cap P_2$.

From $c \in P_1 \cap P_2$, we conclude that $f(c) \in f(P_1 \cap P_2)$. As $c=a_1=a_2$, $f(c)=f(a_1)=b$. Therefore, $b \in f(P_1 \cap P_2)$. Having justified that an arbitrary element b in $f(P_1) \cap f(P_2)$ is in $f(P_1 \cap P_2)$, it follows that $f(P_1) \cap f(P_2) \subseteq f(P_1 \cap P_2)$

(7) We only prove the part "If f is onto then $Q_1 \subseteq f(f^{-1}(Q_1))$" Recall first the definitions of the image and preimage: For any $U \subseteq A$ and $V \subseteq B$,

$$f(U)=\{f(x) \mid x \in U\}=\{y \in B \mid y=f(x) \ \exists x \in U\}, \quad f^{-1}(V)=\{a \in A \mid f(a) \in V\}$$

Let $b \in Q_1$. There is an $a \in A$ such that $f(a)=b$ because $f: A \to B$ is onto and $b \in B$. As $f(a)=b \in Q_1$, $a \in f^{-1}(Q_1)$. From $a \in f^{-1}(Q_1)$, it follows that $b=f(a) \in f(f^{-1}(Q_1))$. Hence, $Q_1 \subseteq f(f^{-1}(Q_1))$ □

Some frequently used functions

Definition: Let A and B be nonempty sets

(1) The function $A \to A$ which maps any element $a \in A$ to itself is called the identity function on A, and it is denoted by 1_A. So the identity function $1_A: A \to A$ is defined as $1_A(a)=a \ \forall a \in A$.

(2) A function $f: A \to B$ is called a constant function if $|f(A)|=1$ (that is, there is exactly one element in the range of f). Thus, f is constant iff there is a $b_0 \in B$ such that $f(a)=b_0$ for all $a \in A$. For instance, $f: \mathbb{R} \to \mathbb{R}$ given by $f(x)=3$ for all $x \in \mathbb{R}$ is a constant function. Note that constant functions from A to B are the subsets of $A \times B$ of the form $A \times \{b_0\}$ where $b_0 \in B$.

(3) If $C \subseteq A$, then the function $\iota: C \to A$ defined by $\iota(c)=c$ for all $c \in C$ is called the inclusion function

(4) The functions $\pi_A: A \times B \to A$, $\pi_A((a,b))=a$ and $\pi_B: A \times B \to B$, $\pi_B((a,b))=b$ are called projection maps For instance, the maps $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$ given by $(x,y) \mapsto x$ and $(x,y) \mapsto y$ are projection maps.

EXERCISES 9.15.

2) Suppose

- f is a function whose domain is $\{0, 2, 4, 6\}$, and
- $f(x) = 4x - 5$, for every x in the domain.

Describe the function in each of the following ways:

(a) Make a table.

(b) Use ordered pairs.

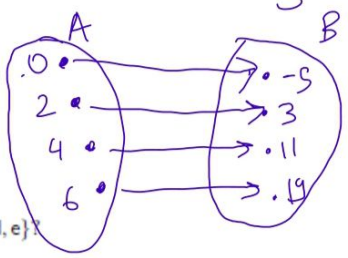
(c) Draw an arrow diagram involving two sets.

(a)

x	f(x)
0	-5
2	3
4	11
6	19

(b) $\{(0,-5), (2,3), (4,11), (6,19)\}$

(c)



3) Which of the following sets of ordered pairs are functions from $\{x, y, z\}$ to $\{a, b, c, d, e\}$?

- If it is such a function, then what is its range?
- If it is not such a function, then explain why not.

(a) $\{(y, a), (x, b), (y, c)\}$ No because y is mapped to distinct elements

(b) $\{(y, a), (x, b), (z, c)\}$ Yes

(c) $\{(y, a), (x, c), (z, a)\}$ Yes

5) For the given sets A and B:

(i) Find all of the functions from A to B.
(Write each function as a set of ordered pairs.)
[*Hint:* You may assume, without proof, that if A has exactly m elements, and B has exactly n elements, then the number of functions from A to B is n^m. (Do you see why?)]

$A = \{a_1, \ldots, a_m\}$

$B = \{b_1, \ldots, b_n\}$

$A \to B$

$a_i \to$ can be any element of B

(ii) Find the range of each function.

(a) $A = \{a, b, c\}$, $B = \{d\}$ $1^3 = 1$ $f(a) = f(b) = f(c) = d$

(b) $A = \{a, b\}$, $B = \{c, d\}$ $2^2 = 4$

(c) $A = \{a\}$, $B = \{b, c, d\}$

(d) $A = \{a, b\}$, $B = \{c, d, e\}$

Exercise.

EXERCISES 10.9.

2) Give a proof to justify the following theorem: Suppose

(1) • $f: A \to B$,

(2) • f is one-to-one,

(3) • $g: B \to C$,

(4) • g is one-to-one,

(5) • $a_1, a_2 \in A$,

(6) • $b_1, b_2 \in B$,

(7) • $f(a_1) = b_1$,

(8) • $f(a_2) = b_2$, and

(9) • $g(b_1) = g(b_2)$.

Then $a_1 = a_2$.

From (4) and (9) we get $b_1 = b_2$

Then (7) and (8) give that $f(a_1) = f(a_2)$

Since f is one to one by (2), $a_1 = a_2$.

—o—

EXERCISES 11.9.

2) Each of the following sets of ordered pairs is a function from $\{1, 2, 3, 4, 5\}$ to $\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$. Which of the functions are onto? *Briefly justify your answers.*

(a) $a = \{(1, \clubsuit), (2, \diamondsuit), (3, \heartsuit), (4, \spadesuit), (5, \clubsuit)\}$ ONTO

(b) $b = \{(1, \clubsuit), (2, \heartsuit), (3, \clubsuit), (4, \heartsuit), (5, \clubsuit)\}$ NOT ONTO

(c) $c = \{(1, \heartsuit), (2, \heartsuit), (3, \heartsuit), (4, \heartsuit), (5, \heartsuit)\}$

(d) $d = \{(1, \diamondsuit), (2, \spadesuit), (3, \heartsuit), (4, \spadesuit), (5, \clubsuit)\}$ Exercise

(e) $e = \{(1, \clubsuit), (2, \spadesuit), (3, \heartsuit), (4, \spadesuit), (5, \clubsuit)\}$

EXERCISE 11.10. Define functions f and g from $\mathbb{R}$ to $\mathbb{R}$ by:

$$f(x) = \begin{cases} 1/x & \text{if } x > 0 \\ x+1 & \text{if } x \leq 0 \end{cases}$$

and

$$g(x) = \begin{cases} 1/x & \text{if } x > 0 \\ x-1 & \text{if } x \leq 0. \end{cases}$$

Show:

1) f is onto;
2) g is not onto;
3) f is not one-to-one; and
4) g is one-to-one.

① Take any $r \in \mathbb{R}$. Case I: Assume $r > 0$. Then $1/r > 0$ and $f(1/r) = r$

Case II: Assume $r \leq 0$. Then $r - 1 < 0$ and $f(r-1) = r$

Hence f is onto

② 0 has no preimage. That is, there is no $x \in \mathbb{R}$ such that $g(x) = 0$

(or for any $x \in \mathbb{R}$, $g(x) \neq 0$)

If $x > 0$ then $g(x) = \frac{1}{x} \neq 0$

If $x \leq 0$ then $g(x) = 1 - x \neq 0$ (because $1 - x = 0$ implies $x = 1$ and so the condition "$x \leq 0$" is not satisfied)

③ As $0 \neq 1$ but $f(0) = 1 = f(1)$, f is not one to one

④ Let $a, b \in \mathbb{R}$ such that $g(a) = g(b)$. We have 4 cases:

$a > 0, b > 0$; $a > 0, b \leq 0$; $a \leq 0, b > 0$; $a \leq 0, b \leq 0$

$g(a) = 1/a$, $g(b) = b - 1$ From $1/a = b - 1$, $b = \underbrace{\left(1 + \frac{1}{a}\right)}_{\leq 0} > 1$, impossible, i.e., a contradiction

So the second case cannot happen.

⋮ Exercise

EXERCISES 11.14. Suppose that $f: A \to B$, that $A_1 \subset A$, and that $B_1 \subset B$.

4) Show that if f is one-to-one, then $A_1 = f^{-1}(f(A_1))$.
5) Show $f\left(f^{-1}(f(A_1))\right) = f(A_1)$.

Exercise !

EXERCISE 12.8. Each formula defines a function from $\mathbb{R}$ to $\mathbb{R}$. Which of the functions are bijections? *Show that your answers are correct.*

1) $a(x) = 1$. ✗ Not one to one Not onto
2) $b(x) = x$. yes
3) $c(x) = x^2$. Not one to one not onto
4) $d(x) = 3x + 2$.
5) $e(x) = 1/(|x| + 1)$.
6) $f(x) = 4x - 6$.
7) $g(x) = \sqrt[3]{x} - 5$. Yes →
8) $h(x) = \sqrt{x^2 + 1}$

$g\left((b+5)^3\right) = b$ So g is onto

$\sqrt[3]{a_1} - 5 = \sqrt[3]{a_2} - 5 \Rightarrow \sqrt[3]{a_1} = \sqrt[3]{a_2} \Rightarrow a_1 = a_2$

So g is one to one

EXERCISES 12.13. 1) Define $f: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $f(m, n) = m^2 + n$.

(a) Show that f is onto. $f(0, b) = b$ So f is onto

(b) Show that f is *not* one-to-one. $f(-1, 0) = 1 = f(1, 0)$ So f is not one to one

2) Define $g: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ by $g(m, n) = (m + n, m - n)$.

(a) Show that g is *not* onto.

(b) Show that g is one-to-one. Exercise

$\mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}\times\mathbb{Z}$

$(m,n) \longmapsto (x, y)$

$x = m + n$

$+\ y = m - n$

$x + y = 2m$

For instance, $(1,0)$ has no preimage.

Indeed, if $g(m,n) = (1,0)$ for some $(m,n) \in \mathbb{Z}\times\mathbb{Z}$,

then $(m+n, m-n) = (1,0)$, implying that $m+n=1$ and $m-n=0$

$\Downarrow$

$m = n$

$\swarrow$

$m = n = \frac{1}{2} \notin \mathbb{Z}$

$(m,n) \notin \mathbb{Z}\times\mathbb{Z}$, a contradiction.

So $(1,0)$ has no preimage, implying that g is not onto.