Chapter 2 : sets and functions

W.DJELLADJ

CYCLE PRÉPARATOIRE

ENP - ALGER

01 Introduction to set theory

Definition of a set

- We use curly brackets to denote sets: {1,2,3} is the set containing 1, 2, and 3.
- “Unordered” sets means that we consider {1,2} and {2,1} the same set, “ignoring repetition” means {1,1}={1}, for example.
- **Elements** or **members** of a set : We write $a \in X$ to mean that a is an element or member of the set X, and $a \notin X$ to mean that a is not an element or member of X.
- **empty set** is written $\emptyset$ or {}.
- **Example.** Let X={1,2,{3}}, Then $1 \in X$, $0 \notin X$, $3 \notin X$, $\{3\} \in X\{3\}$.
- X is a **subset** of Y, written $X \subseteq Y$, if and only if every element of X is also an element of Y.
- X is **equal** to Y, written X=Y, if and only if $X \subseteq Y$ and $Y \subseteq X$.

Subset

The set consisting of all subsets of a set A is called the *power set of* A, written $\mathcal{P}(\mathcal{A})$.

$$\mathcal{P}(\mathcal{A}) = \{B : B \subseteq A\}$$

What are all the possible subsets of $\{a, b, c\}$? They are : $\emptyset$, $\{a\}$, $\{b\}$, $\{c\}$, $\{a, b\}$, $\{a, c\}$, $\{b, c\}$, $\{a, b, c\}$. The set of all these subsets is $\mathcal{P}(\{a, b, c\})$:

$$\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$$

Union, intersection, difference, complement

- Let A,B be sets :
- $A \cup B$, the **union** of A and B, is the set containing the elements of A and also the elements of B.

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$$

- $A \cap B$, the **intersection** of A and B, is the set containing all x such that $x \in A$ and $x \in B$.

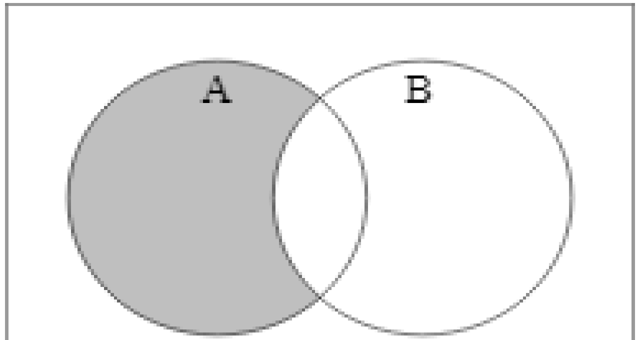
$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

- $A \setminus B$, the **set difference** of A and B, is the set of all elements of A which are not in B.

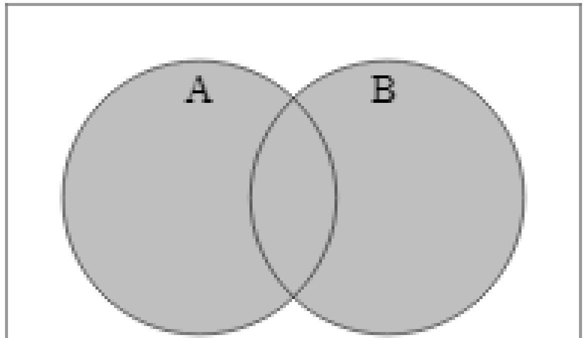
$$A \setminus B = \{x \in A \text{ and } x \notin B\}$$

- If A is a subset of a set Ω then A^c, the **complement** of A in Ω, is the set of all things in Ω which are not in A. Thus $A^c = \Omega \setminus A$

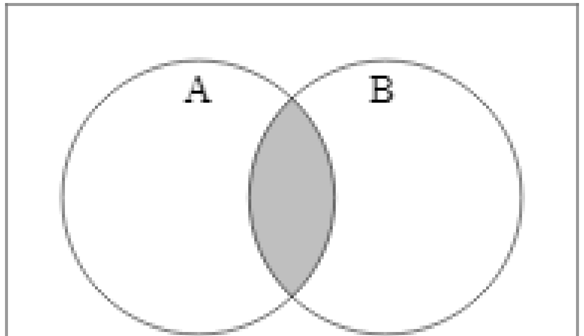
Some mappings



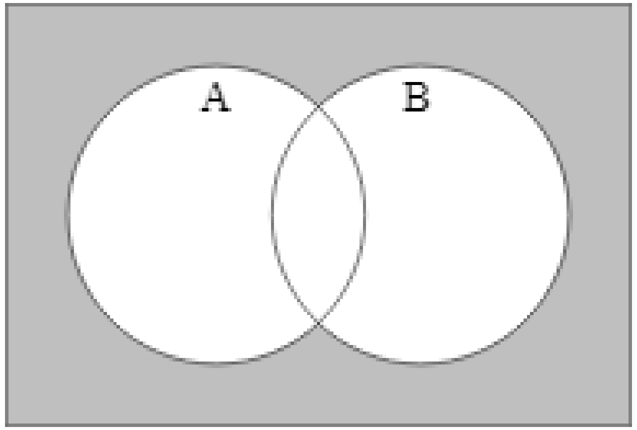
the difference of A and B



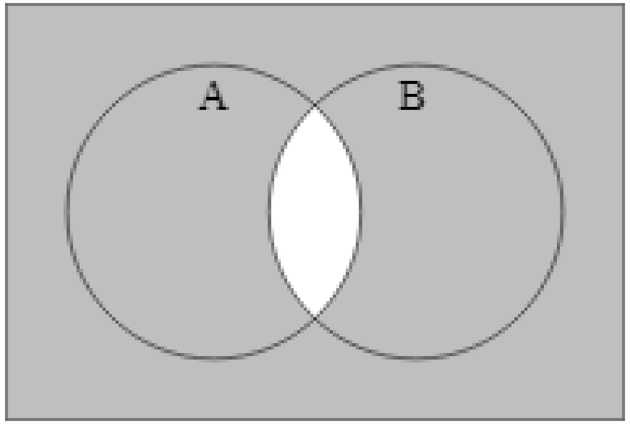
A union B



A intersection B



the complement of (A union B)



the complement of (A intersection B)

Commutativity and associativity

For any subsets A, B, C of a set E, we have:

- $A \cap B = B \cap A$ $A \cup B = B \cup A$ **commutativity**
- $A \cap (B \cap C) = (A \cap B) \cap C$ $A \cup (B \cup C) = (A \cup B) \cup C$ **associativity**
- $A \cup \emptyset = A$, $A \cup A = A$, $A \cap E = A$, $A \cup A^c = E$.
- $(A^c)^c = A$
- $A \subset B \Longleftrightarrow B^c \subset A^c$

The distributive laws

For any sets A, B, C:

- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Proof of $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$: $x \in A \cap (B \cup C) \Longleftrightarrow x \in A$ and $x \in (B \cup C) \Longleftrightarrow x \in A$ and ($x \in B$ or $x \in C$) $\Longleftrightarrow$ ($x \in A$ and $x \in B$) or ($x \in A$ and $x \in C$) $\Longleftrightarrow$ ($x \in A \cap B$) or ($x \in A \cap C$) $\Longleftrightarrow x \in (A \cap B) \cup (A \cap C)$.

$(A \cap B)^c = A^c \cup B^c$.

Proof. Take $x \in (A \cap B)^c$. Then $x \notin A \cap B$. Then $x \notin A$ or $x \notin B$. Then $x \in A^c$ or $x \in B^c$ and so $x \in A^c \cup B^c$. Therefore $(A \cap B)^c \subseteq A^c \cup B^c$.

Now take $x \in A^c \cup B^c$. Then $x \in A^c$ or $x \in B^c$ and so $x \notin A$ or $x \notin B$. Then $x \notin A \cap B$ and so $x \in (A \cap B)^c$. Therefore $A^c \cup B^c \subseteq (A \cap B)^c$ and so $(A \cap B)^c = A^c \cup B^c$.

Theorem

The following statements about sets A and B are equivalent to one another.

I) $A \subseteq B$

II) $A \cap B = A$

III) $A \cup B = B$

Proof :

(I) implies (II). Assume $A \subseteq B$. Since, for all A and B, $A \cap B \subseteq A$, it is sufficient to prove that $A \subseteq A \cap B$. But if $x \in A$, then $x \in B$ and, hence, $x \in A \cap B$. Hence $A \subseteq A \cap B$.
(II) implies (III). Assume $A \cap B = A$. Then
$A \cup B = (A \cap B) \cup B = (A \cup B) \cap (B \cup B) = (A \cup B) \cap B = B$.
(III) implies (I). Assume $A \cup B = B$. Then this and the identity $A \subseteq A \cup B$ imply $A \subseteq B$.

Lemma

For every pair of sets A and B the following inclusions hold :

$$\emptyset \subseteq A \cap B \subseteq A \subseteq A \cup B.$$

Proof

Take $x \in \emptyset$. Since this is false, we can conclude $x \in A \cap B$ and so $\emptyset \subseteq A \cap B$. Now take $x \in A \cap B$. Then $x \in \{y \mid y \in A \text{ and } y \in B\}$ and so $x \in \{y \mid y \in A\} = A$ and thus $A \cap B \subseteq A$. Now take $x \in A$. Then we must have $x \in \{y \mid y \in A \text{ or } y \in B\} = A \cup B$. Then $A \subseteq A \cup B$.

Definition of a partition of a set

- Two sets A and B are called **disjoint** if $A \cap B = \emptyset$.
- The definition of a partition of X is to say that the union of the parts is X and that any two parts in the partition are disjoint.
- An example of a partition : Every real number is either

strictly positive, strictly negative, or zero.

Cartesian products

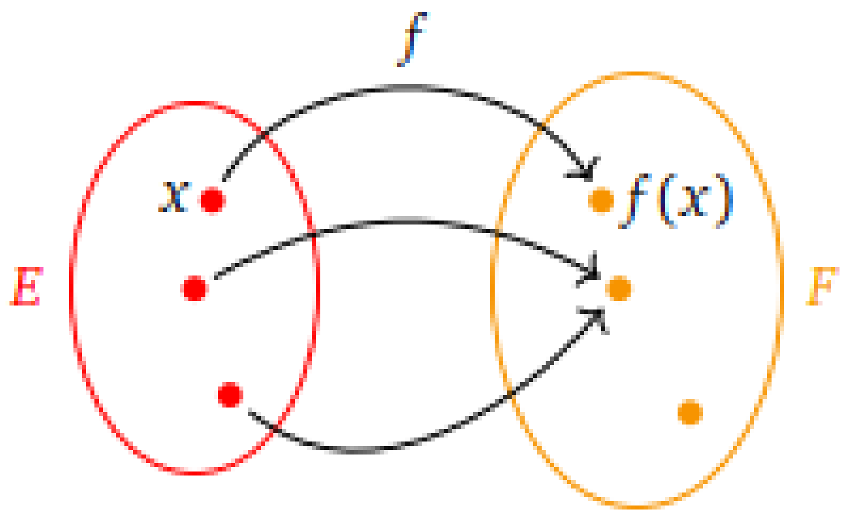
- The Cartesian product of two sets A and B, written $A \times B$, is the set of all ordered pairs in which the first element belongs to A and the second belongs to B.

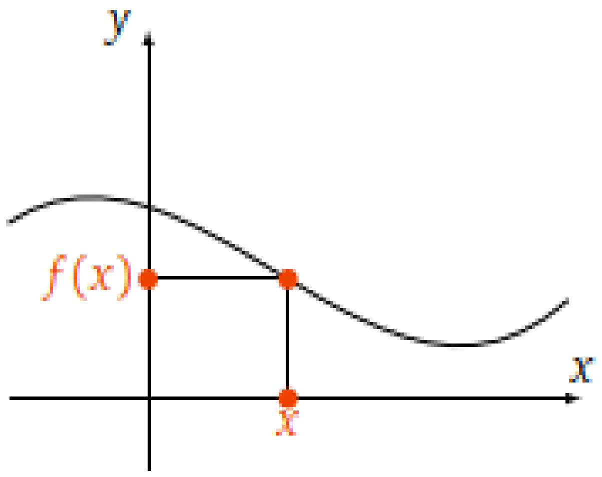
$$A \times B = \{(a,b) : a \in A,\ b \in B\}$$

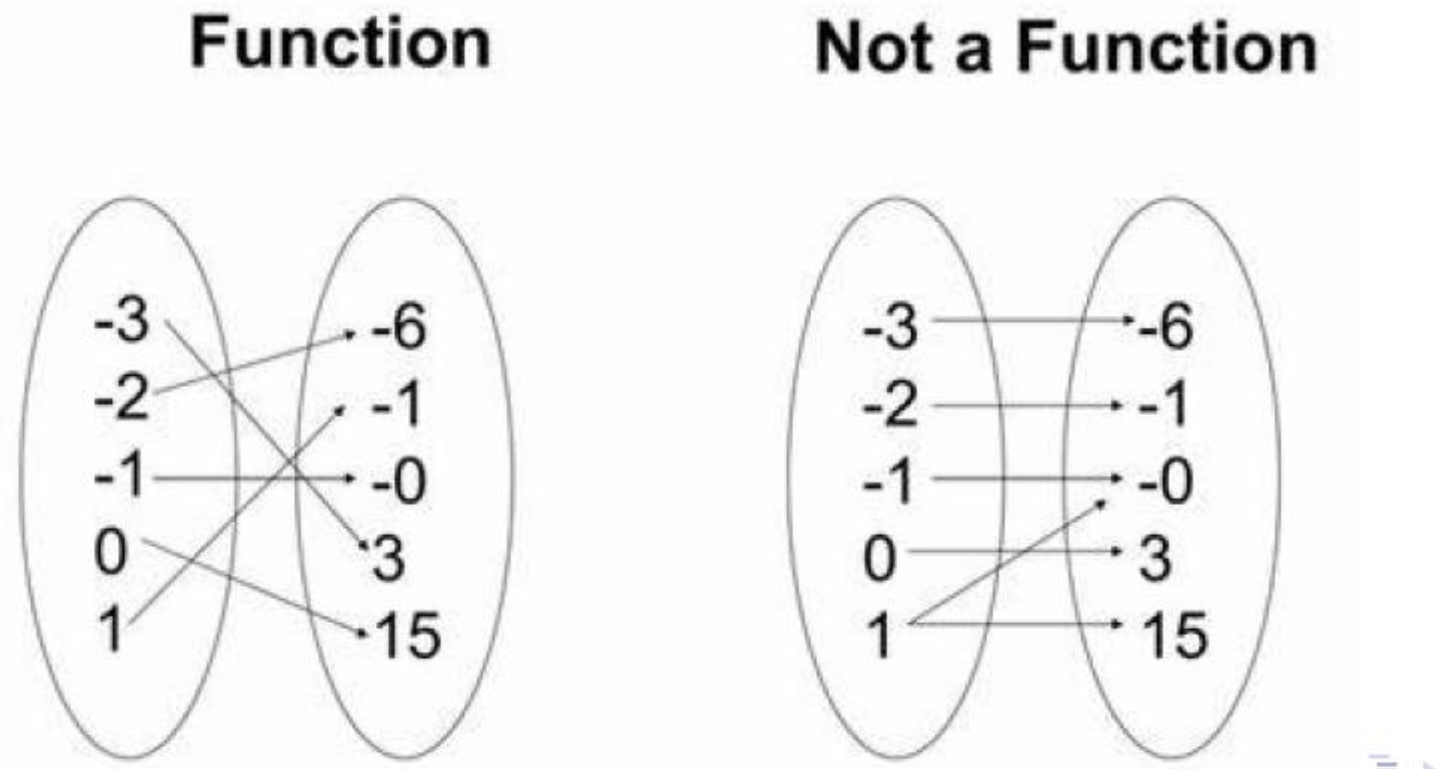
- Notice that the size of $A \times B$ is the size of A times the size of B, that is, $|A \times B| = |A||B|$.
- Example. $\{1,2\} \times \{2,3\} = \{(1,2),(1,3),(2,2),(2,3)\}$.
- Of course we produce ordered triples (a,b,c) as well, and ordered quadruples, and so on.

02 Introduction to functions

- f:X→Y to mean that f is a function from X to Y. X is called the **domain** of f and Y is called the **codomain** of f.
- x in domain is an input and y is the output.
- For any set X, the **identity function** id:X→X is defined by id(x)=x.






Function
-3
-2
-1
0
1
-6
-1
-0
3
15
Not a Function
-3
-2
-1
0
1
-6
-1
-0
3
15

Equal functions

Two functions f and g are equal if and only if

- they have the same domain, say X, the same codomain, and
- $f(x)=g(x)$ for every $x \in X$.

<u>*Example:*</u> f, g : $\{0,1\} \rightarrow \{0,1\}$. $f(x)=x^2$ and $g(x)=x$.

Are they equal?

the answer is yes : they have the same domain, same codomain, and the same output for every input from the domain).

Function composition

- $f:X \to Y$ and $g:Y \to Z$. The **composition** of g and f, written $g \circ f$, is the function $g \circ f:X \to Z$ with the rule $(g \circ f)(x)=g(f(x))$.

Lemma: let $f:X \to Y$, $g:Y \to Z$, $h:Z \to W$. Then $h \circ (g \circ f)=(h \circ g) \circ f$.

Proof: Both $h \circ (g \circ f)$ and $(h \circ g) \circ f$ have the same domain X, same codomain W, and same rule $x \mapsto h(g(f(x)))$.

- *Composition with the identity function*

if $f:X \to Y$ then $f=f \circ id_X=id_Y \circ f$

since for example $(f \circ id_X)(x)=f(id_X(x))=f(x)$, for any $x \in X$.

Injection, surjection, bijection

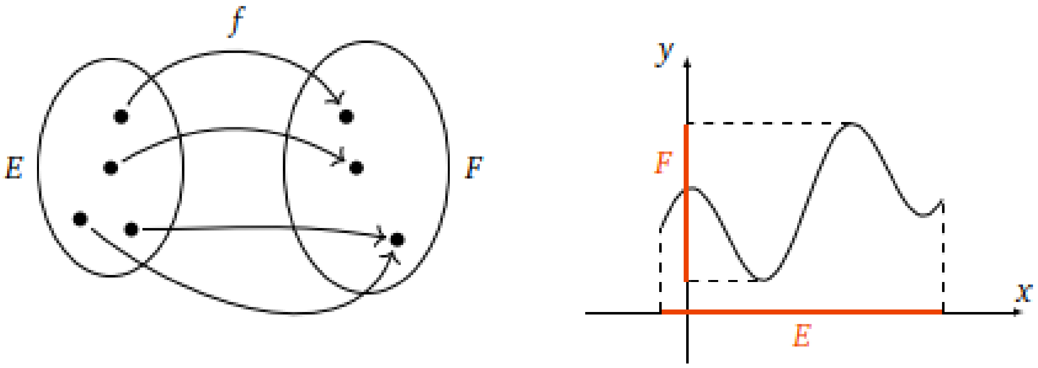
- Let $f:X\rightarrow Y$. Then the **image** of f is $im(f)=\{f(x):x\in X\}$.
- f is **injective** or **one-to-one** if and only if for all $a,b\in X$, if $f(a)=f(b)$ then $a=b$

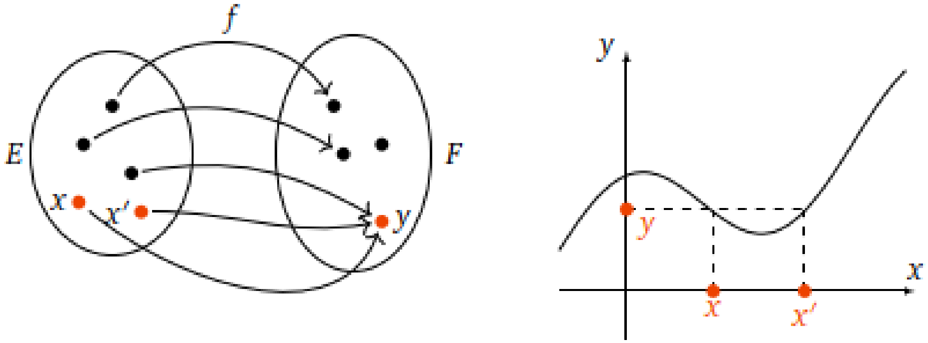
  So $y \in Y$ has at most one $x \in X$.
- F is **surjective** or **onto** if and only if for all $y\in Y$ there is at least one $x\in X$ such that $f(x)=y$.
- f is a **bijection** if and only if it is injective and surjective. It implies the uniqness of x.

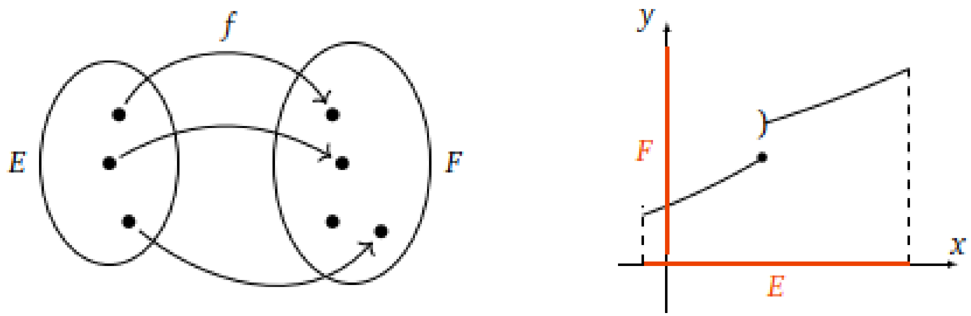
Remarque: Another way to write the definition of surjective would be that a function is surjective if and only if its image equals its codomain.

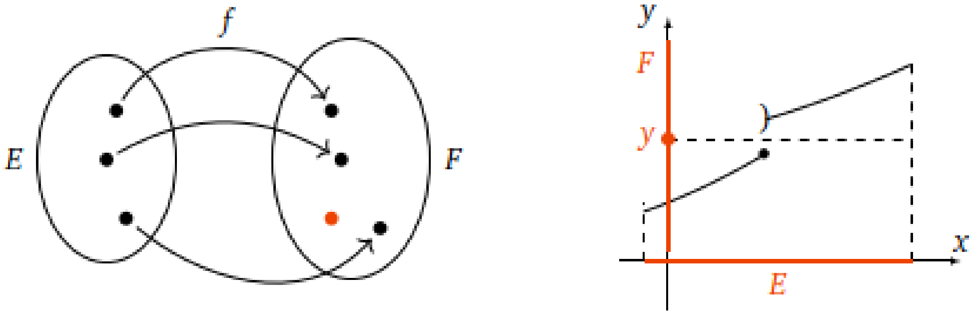
f est injective si et seulement si tout élément y de F a au plus un antécédent (et éventuellement aucun).

f est surjective si et seulement si tout élément y de F a au moins un antécédent.


f
E
F
y
x
F
E


f
E
F
x
x′
y
y
x
y
x
x′


f
E
F
y
x
F
E


f
E
F
y
F
y
x
E

Examples:

- $f:\boldsymbol{R}\to\boldsymbol{R}$, $f(x)=x^2$. It isn't injective as $f(-1)=f(1)$ and it isn't surjective as -1 is in the codomain, but there's no element x in the domain such that $f(x)=-1$.
- $g:\boldsymbol{R}\to[0,\infty)$, $g(x)=x^2$. This is not injective for the same reason as before, but this time it is surjective: for each $y\geq 0$ we can find an element of the domain which g sends to y: for example. $g(\sqrt{y})=y$.
- $h:[0,\infty)\to\boldsymbol{R}$, $h(x)=x^2$. Not surjective, forthe same reason, f isn't surjective (the codomain contains negative numbers, but the image doesn't contain any negative numbers, so the image doesn't equal the codomain). But h is injective: if x and y are in the domain of h and $h(x)=h(y)$ then $x^2=y^2$, so $x=\pm y$. Since elements of the domain of h are nonnegative, it must be that $x=y$.

03 Invertibility

- a **left-inverse** to f is a function $g:Y \rightarrow X$ such that $g \circ f = id_X$
- a **right-inverse** to f is a function $h:Y \rightarrow X$ such that $f \circ h = id_y$
- an **inverse** (or a **two-sided inverse**) to f is a function $k:Y \rightarrow X$ which is a left and a right inverse to f.

Remarque: if the function $f : E \rightarrow F$

- $f \circ g = id_Y$ means $\forall y \in F$, $f(g(y)) = y$.
- $g \circ f = id_X$ means $\forall x \in E$, $g(f(x)) = x$.

When is a function invertible?

Theorem 1: Let $f:X\to Y$ and assume $X\neq\emptyset$. Then

1. f has a left-inverse if and only if it is injective
2. f has a right-inverse if and only if it is surjective
3. f is invertible if and only if it is bijective

Proof:

1. Let g be left-inverse to f, so $g\circ f=id_X$. Suppose $f(a)=f(b)$. Then applying g to both sides, $g(f(a))=g(f(b))$, so $a=b$.

2. IF. Suppose f has a right inverse g, so $f\circ g=id_Y$. If $y\in Y$ then $f(g(y))=id_Y(y)=y$, so $y\in im(f)$. Every element of Y is therefore in the image of f, so f is onto.
   - ONLY IF. Suppose f is surjective. Let $y\in Y$. Then y is in the image of f, so we can choose an element $g(y)\in X$ (because $g:Y\to X$) such that $f(g(y))=y$ (because f surjective). This defines a function $g:Y\to X$ which is evidently a right-inverse to f.

3. If f is a bijection it has a left inverse $g:Y\to X$ and a right inverse $h:Y\to X$. But "invertible" required a single function which was both a left *and* a right inverse. We must show $g=h$:

$$
\begin{aligned}
g &= g\circ id_Y \\
&= g\circ(f\circ h) && \text{as } f\circ h = id_Y \\
&= (g\circ f)\circ h && \text{associativity} \\
&= id_X\circ h && \text{as } g\circ f = id_X \\
&= h
\end{aligned}
$$

so $g=h$ is an inverse of f

Notation: if f is invertible, we write f^{-1} for the inverse of f.

To conclude:

Proposition

P_1 : If $f\colon A \to B$ is injective, then there is a *left inverse* $g\colon B \to A$ of f so that $g(f(x)) = x$ for all $x \in A$.

P_2 : If $f\colon A \to B$ is surjective, then there is a *right inverse* $h\colon B \to A$ of f so that $f(h(y)) = y$ for all $y \in B$.

P_3 : If $f\colon A \to B$ is bijective, there is a function $f^{-1}\colon B \to A$ so that for all $x \in A$, $f^{-1}(f(x)) = x$ and for all $y \in B$, $f(f^{-1}(y)) = y$.

P_4 : If $f\colon A \to B$ has a left inverse g and a right inverse h, then $h = g$.

P_5 : Every function f has at most one inverse.

Inversion examples

- $f\colon \mathbb{R} \to [0,+\infty[\colon x \mapsto exp(x)$ is injective, then there is a *left inverse* $g\colon [0,+\infty[\to \mathbb{R}$ of f so that $g(f(x)) = x$ for all $x \in \mathbb{R}$.

$\leadsto$ $ln(exp(x)) = x$

- $f\colon \mathbb{R} \to [0,+\infty[\colon x \mapsto exp(x)$ is surjective, then there is a *right inverse* $h\colon [0,+\infty[\to \mathbb{R}$ of f so that $f(h(y)) = y$ for all $y \in [0,+\infty[$.

$\leadsto$ $exp(ln(x)) = x$

$\leadsto$ $f(x) = exp(x)$ and $f^{-1}(x) = ln(x)$, $g(x) = h(x) = ln(x)$.

Inverse of a composition

Theorem 2: If $f{:}E \to F$ and $g{:}F \to G$ are invertible then so is $g \circ f$, and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof: From the precedent property, it exists $u : F \to E$ such that $u \circ f = id_E$ et $f \circ u = id_F$. It exists also

$v : G \to F$ such that $v \circ g = id_F$ et $g \circ v = id_G$. So

$(g \circ f) \circ (u \circ v) = g \circ (f \circ u) \circ v = g \circ id_F \circ v = g \circ v = id_G$.

and $(u \circ v) \circ (g \circ f) = u \circ (v \circ g) \circ f = u \circ id_F \circ f = u \circ f = id_E$. Thus $g \circ f$ is bijective and its inverse is $u \circ v$.

u is the inverse of f et v the inverse of g then : $u \circ v = f^{-1} \circ g^{-1}$.

04 Binary Relations

- Informally, a **relation** on a set X is a property of an ordered pair of elements of X that could be true or false.

For example :

- ≤ is a relation on ***R*** . For any ordered pair (x,y) of real numbers, x≤y is either true or false.
- ≠ is a relation on ***Z***. For any ordered pair (x,y) of integers, x≠y is either true or false.

Exemple 2: La correspondance $\mathcal{R}_2$ qui lie les chiffres aux voyelles utilisées pour écrire le chiffre en toutes lettres, est une relation de l'ensemble $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ vers l'ensemble $\{a, e, i, o, u, y\}$
On a dans ce cas $0\mathcal{R}_2 e$, $0\mathcal{R}_2 o$, $0\not\mathcal{R} a$, $9\not\mathcal{R} y$, $6\mathcal{R}_2 i$ et $1\mathcal{R}_2 u$

Congruence modulo n

- For each integer $n \neq 0$, there is a relation on $\mathbb{Z}$ called **congruence modulo** n. Two integers x and y are congruent modulo n if and only if $x-y$ is divisible by n so $x-y=nk$ with k in $\mathbb{Z}$.
- We write $x \equiv y$ modn $\equiv y$ [n].

Examples :

- $85 \equiv 5$ [10]   ie $85-5=80$ divisible by 10.
- 3 and -7 are congruent modulo 2, as $3-(-7)=10$ is divisible by 2.
- But 3 and 8 are not congruent modulo 2 because $3-8=-5$ isn't a multiple of 2.

Relation properties

- Let $\sim$ be a binary relation on a set X.
- $\sim$ is **reflexive** (R) if and only if $\forall x \in X : x \sim x$.
- $\sim$ is **symmetric** (S) if and only if $\forall x,y \in X$: $x \sim y \Longrightarrow y \sim x$.
- $\sim$ is **transitive** (T) if and only if $\forall x,y,z \in X$: $x \sim y$ and $y \sim z$ implies $x \sim z$.
- $\sim$ is anti**symmetric** (AS) if and only if $\forall x,y \in X$: $x \sim y$ and $y \sim x \Longrightarrow x = y$.

$\sim$ is an **equivalence relation** if and only if it has all three properties (R), (S), and (T).

relation and set	Reflexive	Symetric	Transitive	Equivalence
$\leq$, $\boldsymbol{R}$	Y	no, $1\leq2$ but $2\nleq1$	y	No
$<$, $\boldsymbol{R}$	n	n	y	No
a~b if a-b even, $\boldsymbol{Z}$	y	y	y	Yes
$\neq$, $\boldsymbol{N}$	n	y	n	No

Order relation

- Many of our comparisons involve describing some objects as being "less than", "equal to", or "greater than" other objects, in a certain respect. These involve *order* relations.
- But there are different kinds of order relations. For instance, some require that any two objects be comparable, others don't. Some include identity (like $\leqslant$) and some exclude it (like $<$).

Partial or total Order ?

- *R* is a partial **ordered relation** if and only if it has all three properties (R), (AS), and (T).

Example : The less-than-or-equal-to relation on the set of integers ***N*** is a partial order.

Definition(total order): A binary relation R on a set *A* is a total order if and only if it is
(1) a partial order, and
(2) for any pair of elements *a* and *b* of *A*, a R *b* or b *R* *a*.

Example 1: The less-than-or-equal-to relation on the set of integers ***N*** is a total order

Exemple 2: The inclusion relation ⊆ on P(N) is a partial ordered relation

- (X ⊆ X ; (X ⊆ Y et Y ⊆ X) implies X = Y ; (X ⊆ Y et Y ⊆ Z) implies X ⊆ Z
- The subsets {1,2} and {1,3} are not comparable.

Definition of equivalence class

- Let R be an equivalence relation on X and $x \in X$. The **equivalence class** of a is

$$[x] = \{a \in X : a\ R\ x\}.$$

- The equivalence classes for the congruence modulo 2 relation on Z: Recall that x and y are congruent modulo 2 if and only if $x-y$ is divisible by 2 (that is, $x-y$ is even).

$$[0] = \{a \in Z : aR0 \quad \text{ie } a \equiv 0\ [2]\} = \{\ldots,-4,-2,0,2,4,\ldots\}$$

So it's the set of all even integers.

We easily check that $[4]=\{\ldots,-4,-2,0,2,4,\ldots,\}=[0]$

The equivalence class [1]: An integer y is congruent to 1 modulo 2 if and only if $y-1$ is even. That's true if and only if y is odd, so [1] is the set of all odd numbers:

$$[1]=\{\ldots,-3,-1,1,3,\ldots\}$$

We check that $[-3]=\{\ldots,-3,-1,1,3,\ldots\}=[1]$.

There are exactly two different equivalence classes : set of odd and set of even.

Theorem and définition: The relation R_n defined on Z by: x R_n y iff n divides y- x
Is an equivalence relation.
The relation R_n called congruence relation modulo
The set of equivalence classes $\bar{x}$ of this relation is noted Z/nZ

$$\mathbb{Z}_{/\mathcal{R}_n} = \{n\mathbb{Z} + a \ / \ \bar{a} \in \mathbb{Z}\}$$

It is the quetient set on *Z.*

Remark: Poset=order relation

Minimum and maximum element

minimal/maximal element

Let $(A, \preceq)$ be a poset, where $\preceq$ represents an arbitrary partial order. Then an element $b \in A$ is a minimal element of A if there is no element $a \in A$ that satisfies $a \preceq b$. Similarly an element $b \preceq A$ is a maximal element of A if there is no element $a \in A$ that satisfies $b \preceq a$.

least/greatest element

Let $(A, \preceq)$ be a poset. Then an element $b \in A$ is the least element of A if for every element $a \in A, b \preceq a$.

- Note that the least element of a poset is unique if one exists because of the antisymmetry of $\preceq$.
- The poset of the set of natural numbers with the less-than-or-equal-to relation has the least element 0.
- The poset of the powerset of $\{1, 2\}$ with $\subseteq$ has the least element $\emptyset$.