§. 1 Intro,

ens, logique, raisonnement

→ Méthodologie de preuves / raisonnement.

I. Logique

connecteurs
$\Rightarrow, \wedge, \vee, \exists \dots$

Proposition

Formule construite avec :
- → variables $A, B \dots$
- → connecteurs logiques ...

↳ logique classique : proposition : vraie ou fausse.

Connecteurs

propositions

$\Rightarrow$ implication

$A \Rightarrow B$ vraie si

si A vraie alors B vraie ←

table de vérité de $A \Rightarrow B$

A \ B	V	F
V	V	F
F	V	V

→ Le faux implique n'importe quoi

$A \Rightarrow B \overset{\text{équiv}}{\equiv} \neg A$ ou B ←

$\neg(A \Rightarrow B) \equiv A \wedge \neg B$

ex : $\equiv \forall x \in \emptyset \Rightarrow \dots$ → Vrai

- ET $\wedge$ OU $\vee$ NON $\neg$ → $\neg\neg A \overset{\text{équiv}}{\equiv} A$
- $\Leftrightarrow$ équivalent ($A \Leftrightarrow B$ ssi $A \Rightarrow B$ et $B \Rightarrow A$)

- $\forall$ pour tout
  $\exists$ il existe $\quad \neg$

II. Ensembles

Ensemble : collection d'éléments

→ notation en extension : $\{a, b, 1, e \dots\}$ $\quad \varnothing$ ↓ ens. vide.

↓ énumération

→ notation en intention :

$\{x \in \mathbb{Z} \ ; \ \exists y \in \mathbb{Z} \quad x = 2y\}$ + $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$

|

nombres pairs.

Ensembles :

→ opérations ensemblistes ens → ens

^{C} complémentaire / $\cap$ inter / $\cup$ union / $\triangle$ diff. sym.

→ propositions ensemblistes ens → prop (V/F)

$\subseteq$ inclus $\quad \in$ appartient $\quad =$ égalité ensembliste

Propositions ensemblistes

- $x \in A$ si x est un élément de la collection A.

elt — ensemble

$A_1 = \{1, 2, 3\}$ → ensemble "typé"

$1 \in A_1$, $2 \in A_1$ ...

$A_2 = \{ \{1,2\}, \{1\}, 1, 2 \}$

① ② ③ ④

$\{1\} \in A_2$ $\quad \emptyset \notin A$

ens. non typé → ① ② ens. d'entiers ; ③ ④ entiers.

$B = \{ \emptyset, \{1\}, \{1,2\} \}$

$\emptyset \in B$

- $A \subseteq B$ inclus

ensembles

si $\forall x \in A \quad x \in B$

écriture ~> "propre"

variable "muette"

$\forall x \; (x \in A \Rightarrow x \in B)$

y y y

ex :

$A = \{1,2,3\}$

$\{1,2,3\}$ $\quad \emptyset \quad \{1\} \quad \ldots$ ← sous-ensembles de A

$A_2 = \{ 1, 2, \{1\}, \{1,2\} \}$

$\emptyset \quad \{1\} \quad \{\{1\}\}$ ← $\forall x \in$ $\quad x \in$

toujours vrai

$\forall x \in \emptyset \quad x \in A$ — $\forall x (x \in \emptyset \Rightarrow x \in A)$

F ⇒ ... ✓

$A \Rightarrow B$ vrai si A est fausse

- $A = B$ égalité ensembliste

  ⟺ si $A \subseteq B$ et $B \subseteq A$.

Opérations ensemblistes

$\cup$, $\cap$

- $\complement_A B$ — complémentaire de B ds A

  $=$ $\{x \in A \ ; \ x \notin B\}$ ← tel que

$A, B \ldots \subseteq E$ ← gros ens. E implicite

$\complement_A$, $\complement_B$

Autres notations

$\complement_A B \rightarrow A \setminus B$ ✓

~~$A - B$~~

$\complement A \rightarrow \overline{A}$

ex : entiers — $\mathbb{N}$

$A \subseteq \mathbb{N}$

$\complement_{\mathbb{N}} A$

$\complement_C (\complement_A B)$ ....

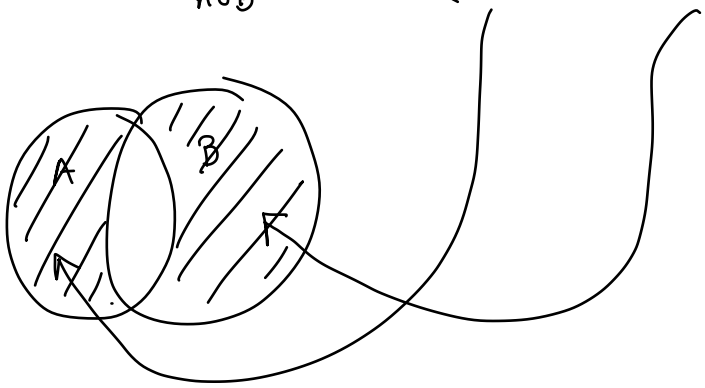
$C - (A - B)$

$\not\equiv$) $\neq$

~~$C - A + B$~~

- $A \Delta B$ — différence symétrique de A et B

$\complement_{A \cup B} A \cap B = (\complement_A B) \cup (\complement_B A)$



Parties d'un ensemble

$\mathcal{P}(E)$ — ensemble des parties de E

↳ ensemble d'ensembles → $|\mathcal{P}(E)| = 2^n$

E : ensemble ← $|E| = n$

sous-ensembles

Cardinal de E

↓

nbre d'elts.

$|E|$ $\#E$

ex : $E = \{1,2,3\}$ ⟶ $\mathcal{P}(E) = \{$ énum par card ↗

$\mathcal{P}(E) = \{A \subseteq E\}$

$|A| \leq |E|$ (3)

$\emptyset$, (0 élts)

$\{1\}, \{2\}, \{3\}$, (1 élt → singletons)

$\{1,2\}, \{1,3\}, \{2,3\}$, (2 élts)

$\{1,2,3\}$ (3 élts)

$|\mathcal{P}(E)| = 8 = 2^3 = 2^{|E|}$

III. Méthodologie du raisonnement

⟶ validation / preuves auto / ↙ preuves formelles

Coq / méthode B / Z / ...

⟶ méthode de démonstration

① Ecrire — garder en tête ne suffit pas ....

② Notations : séparer → hypothèses → encadrées

→ ce que l'on veut montrer → but ?

③ On travaille sur le but — forme → règles en fonction de cette forme : règles de réécriture.

pour montrer ce but → il faut montrer ...

① But : implication $A \Rightarrow B$

pour prouver $A \Rightarrow B$?

→ on suppose A vraie (ajouté aux hyp.)

→ on prouve B

ex : $A \subseteq B \implies A \cap B = A$! ← but

implication ⇝ on suppose ce qui est à gauche

nouveau but : —— droite

On suppose que $A \subseteq B$

$A \cap B = A$!

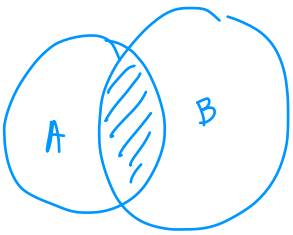
égalité d'ens ⇝ double $\subseteq$ déf

$A \cap B \subseteq A$!

↓

toujours vrai (par déf. de $\cap$)

✓



$A \subseteq A \cap B$!

inclusion ⇝ déf

$\forall x \in$ ens. gauche ... ← hyp.

↓

$x \in$ ens. droite ... ?

(*)

Soit x

On suppose $x \in A$ (*)

$x \in A \cap B$!

✓ $x \in A$ et $x \in B$? ← on ne peut plus "dérouler"

↳ prouvable à partir des hypothèses

$x \in A$ est une hypothèse (*)

et comme $A \subseteq B$

$\implies x \in B$

Donc $x \in A$ et $x \in B$ ✓

◇

(2) But : équivalence $A \iff B$ ← 1 but

pour prouver

|

On montre $A \Rightarrow B$ ← 2 sous. cvls. ex : ....

et $B \Rightarrow A$

③ But : $\forall$ $\forall x\ P(x)$ ← var muette

→ soit x (quelconque) ← variable mauve ← crée une variable "fraîche"

→ on trouve $P(x)$ §

ex : on veut montrer $A \subseteq B \Rightarrow A \cap B = A$

⋮

on suppose $A \subseteq B$ $\quad A \cap B = A$!

$A \cap B \subseteq A$? ✓

$A \subseteq A \cap B$!

$\forall x \ (x \in A \Rightarrow x \in A \cap B)$!

$\forall$

Soit x

$x \in A \Rightarrow x \in A \cap B$!

implication →

on suppose $x \in A$

$x \in A \cap B$!

⋮

④ But : $\exists$ → $\exists x\ P(x)$

→ construire un exemple de x / x particulier tq $P(x)$ vraie

ex : $\forall n \in \mathbb{N} \quad \exists m \in \mathbb{N} \quad$ tq $\quad n \geq 2m$?

$n = 1$
$n = 10$
$n = 2$ marche...
5 ou 0
$10 \geq 2.2$
2.5

$\forall$

Soit $n \in \mathbb{N}$

$\exists m \in \mathbb{N}$ tq $n \geq 2m$?

$\exists$ ss construire un m "qui marche"
↳ on pose $m = \ldots$ ss Rap vraie ...

Preuve 1

si n pair on pose $m = \frac{n}{2}$

on a bien $n \geq 2.m = \cancel{2}.\frac{n}{\cancel{2}}$

si n impair on pose

$m = \frac{n-1}{2}$

$2.m = \cancel{2}.\frac{n-1}{\cancel{2}} \leq n$ ✓

$\exists m$ tq $n \geq 2m$ ✓

Preuve 2

On pose $m = 0$

on a bien $n \geq 2.m = 0$ ✓

car $n \in \mathbb{N}$ (≥ 0)

(5) Raisonnement par l'absurde : pour prouver A

- → on suppose $\neg A$ vraie
- → on en déduit des implications jusqu'à trouver une contradiction

$\Rightarrow \neg A$ fausse $\Rightarrow \neg\neg A$ vraie

$=$

A

ex : $\sqrt{2}$ est irrationnel $(\notin \mathbb{Q})$

$\nexists p, q$ tq $\sqrt{2} = \frac{p}{q}$ $\quad p, q \in \mathbb{Z}$

par l'absurde

on suppose $\exists p, q$ tq $\sqrt{2} = \frac{p}{q}$

on suppose p, q premiers

On a $\sqrt{2} = \frac{p}{q} \overset{\text{12}}{\Longrightarrow} 2 = \frac{p^2}{q^2}$

$\Rightarrow \underbrace{2 \cdot q^2}_{\text{pair}} = p^2$ (1) $\quad \ldots \Rightarrow p$ pair

$\Rightarrow p^2$ pair $\Rightarrow p$ pair

$p^2 = p \times p$

$2 \mid p^2 = p \times p \Rightarrow 2 \mid p$

(2 premier, divise)

Th. Gauss : $p \mid a \times b \Rightarrow p \mid a$ ou $p \mid b$ (p premier)

3×2 : $6 \mid a \times b$ $\not\Rightarrow$ $6 \mid a$ ou $6 \mid b$

Donc $p = 2 \cdot n$

Donc (1) devient $2q^2 = p^2 = (2n)^2 = 4 \cdot n^2$

$\Rightarrow q^2 = 2 \cdot n^2$ (2)

$\Downarrow$ de même

q pair

(1) $2q^2 = p^2$ $\Rightarrow$ p pair

$\rightarrow$ contradiction car on avait supposé p, q premiers ...

(p, q pairs $\Rightarrow$ 2 facteur commun ...)

Donc $\nexists\, p, q$ tq $\sqrt{2} = \frac{p}{q}$ ◇

(6) Raisonnement par récurrence

Pour prouver des propriétés $P(n)$ $\forall n \in \mathbb{N}$ $n \geq n_0$

Récurrence stricte ~généralement

→ Au rang n_0
on prouve $P(n_0)$

→ Au rang n
on suppose $P(n)$ vraie

→ Au rang $n+1$
on montre $P(n+1)$?

→ Ccl : $\forall n \geq n_0$ $P(n)$ vraie

ex : $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$ (*)

$\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

$\sum_{i=0}^{n} i^3 = (*)^2 = \frac{n^2(n+1)^2}{4}$

Récurrence forte

→ Au rang n_0
on prouve $P(n_0)$

→ Au rang n
on suppose $P(k)$ vraie $\forall k \leq n$ → la prop. vraie jusqu'à n

→ Au rang $n+1$
on montre $P(n+1)$?

→ Ccl : $\forall n \geq n_0$ $P(n)$ vraie

ex : Tout entier est factorisable en prod. de facts premiers

$\forall n \in \mathbb{N}^*$ $n = p_1^{k_1} \times \dots \times p_m^{k_m}$

premiers.

Preuve par réc. sur n

→ Au rang $n=1$ 1 est premier ~> $1 = 1$ ... ✓

→ Au rang n on suppose que k factorisable ... $\forall k \leq n$

→ Au rang $n+1$ ~> factorisons $n+1$ ...

~> si $n+1$ premier $n+1 = n+1$ ... ✓

~> Sinon il se décompose

→ $\exists a, b$ tq $n+1 = a \times b$ (>1) ≥ 2

$20 = 4 \times 5$

$\Downarrow$

$a, b \leq \frac{n+1}{2} \leq n$ → on peut appliquer l'HR à a, b

HR : a ~> factorisable

b ~> "

$\Rightarrow$ $a \times b$ factorisable

IV. Applications — notion ensembliste

fonctions → plus facilement définie par tout E

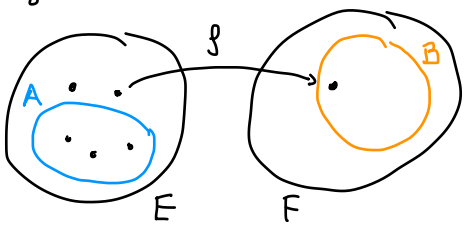
≠

analyse

* déf: E, F ensembles

Une application de E ds F $(f: E \to F)$ associe à tout élt de E un (unique) élt. de F

$x \in E \longmapsto f(x) \in F$



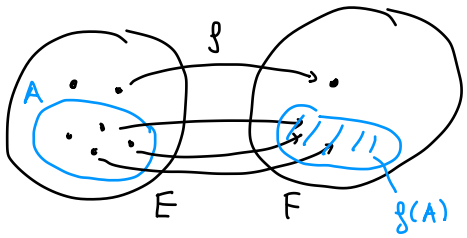
① Image directe et réciproque

* déf: $f: E \to F$ une application

$A \subseteq E$

L'image directe de A par f (notée $f(A)$) est

$$f(A) = \{ f(x) \,;\, x \in A \} \subseteq F$$

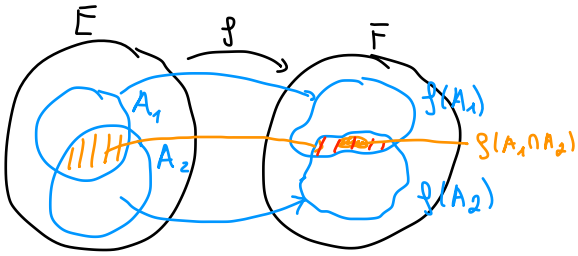


Prop. si $A_1, A_2 \subseteq E$

i) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$

ii) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$

iii) si $A_1 \subseteq A_2$ $\quad f(A_1) \subseteq f(A_2)$



dém. de iii)

$f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$?

inclusion ⇝ soit $x \in \ldots$ $\quad x \in \ldots$?

Soit $y \in f(A_1 \cap A_2)$

$y \in f(A_1) \cap f(A_2)$?

$\Leftrightarrow$

$y \in f(A_1)$ et $y \in f(A_2)$?

$\exists x_1 \in A_1$ tq $y = f(x_1)$? (*)

$\exists \ldots$

$\exists x_2 \in A_2$ tq $y = f(x_2)$? (**)

$\exists \ldots$

⇝ trouver $x_1, x_2 \ldots$

↳ hyp. ...

⚠ NOMS DE VARIABLES !

$f: E \to F$

$x \quad x'$

$x_1 \quad x_2$

$y \quad y'$

$y_1 \quad y_2$

On a $y \in f(A_1 \cap A_2)$

$\Rightarrow \exists x \in A_1 \cap A_2$ tq $y = f(x)$

$x \in A_1$ et $x \in A_2$

prendre $x_1 = x$ convient pour prouver (*)

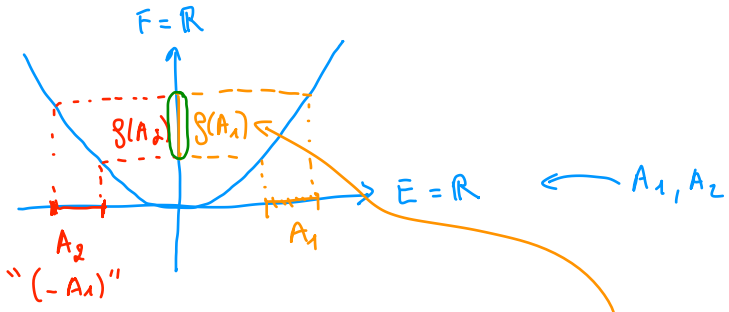
$x_2 = x$ ——— (**)

$f(A_1) \cap f(A_2) \supseteq f(A_1 \cap A_2)$ ($f(A_1 \cap A_2) = \emptyset$)

$f(A_1) \cap f(A_2) \not\subseteq f(A_1 \cap A_2)$

$f : \mathbb{R} \longrightarrow \mathbb{R}$

$x \longmapsto x^2$



$f(A_1) \cap f(A_2) = f(A_1) = f(A_2)$!

$f(A_1 \cap A_2) = \emptyset$

$\emptyset$

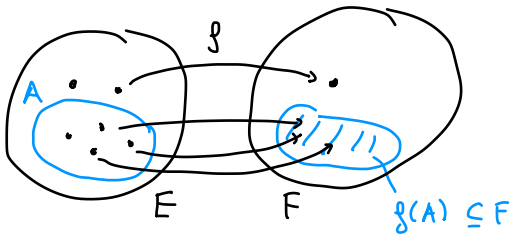
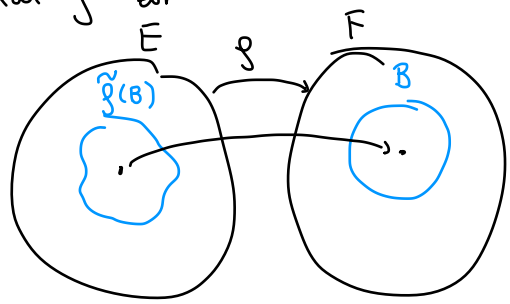


Image directe

* déf : soit $f : E \to F$

Soit $B \subseteq F$, l'image réciproque de B par f est

$\tilde{f}(B) = \{ x \in E \ ; \ f(x) \in B \}$



rem : $f : \mathbb{R} \longrightarrow \mathbb{R}$

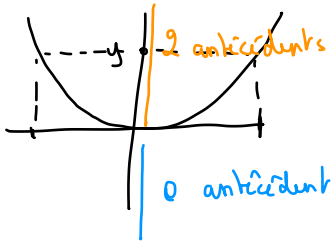
$x \longmapsto x^2$

~~f^{-1}~~

$x^2 = 1$

$f(x) = 1$

~~f^{-1}~~



$\tilde{f}(\{1\}) = \{ x \in \mathbb{R} \text{ tq } f(x) \in \{1\} \}$

$= \{1, -1\}$

~~$f^{-1}(1) = 1, -1$~~

$\tilde{f}(\{-2\}) = \emptyset$

~~$f^{-1}(-2) = ?$~~

~~f^{-1}~~

$\tilde{f}$

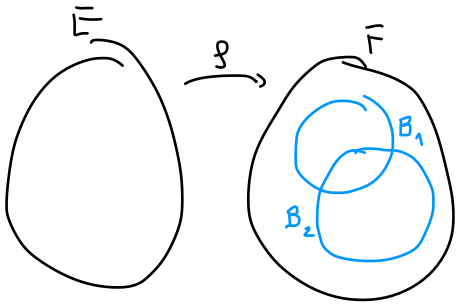
$\tilde{f}([1,2]) = [1, \sqrt{2}] \cup [-\sqrt{2}, -1]$

Prop

i) $\tilde{f}(B_1 \cap B_2) = \tilde{f}(B_1) \cap \tilde{f}(B_2)$

ii) $\tilde{f}(B_1 \cup B_2) = \tilde{f}(B_1) \cup \tilde{f}(B_2)$

iii) $B_1 \subseteq B_2 \implies \tilde{f}(B_1) \subseteq \tilde{f}(B_2)$



Prop. ← pt. injectivité

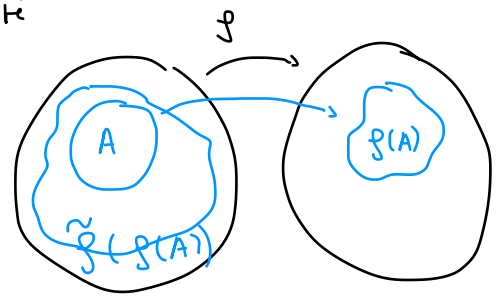
i) $A \subseteq \tilde{f}(f(A))$ $\quad A \subseteq E$ ←

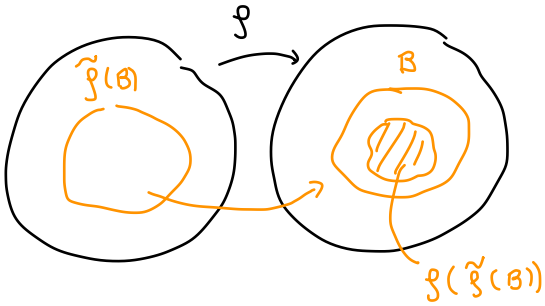
ii) $f(\tilde{f}(B)) \subseteq B$ $\quad B \subseteq F$

↳ pt … 1 pt de F a plusieurs antécédents

↳ pt … pts de F sans antécédents

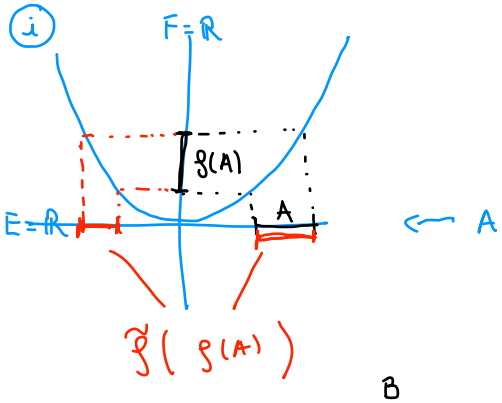
↑ pt. surjectivité



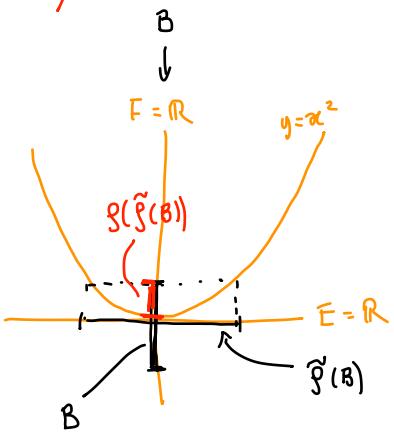


ex : $f : x \longmapsto x^2$

i)



ii)



(2) Injective, surjective, bijective

Bijective → 2 pts qui peuvent l'empêcher …

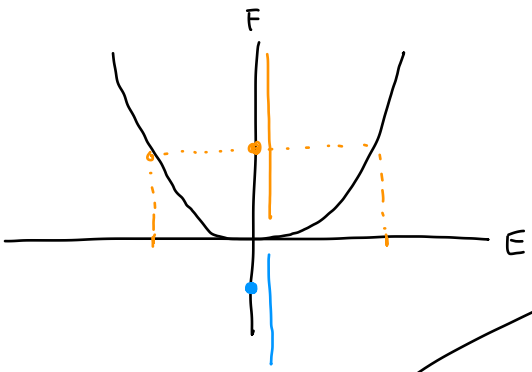
↓

$f : E \to F$

"un pour un"

$f : \mathbb{R} \longrightarrow \mathbb{R}$

$x \longmapsto x^2$



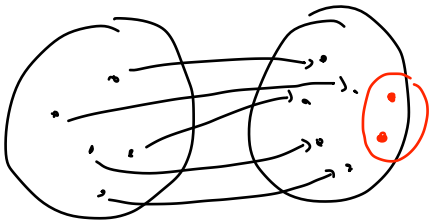
pas bijective ...

car :

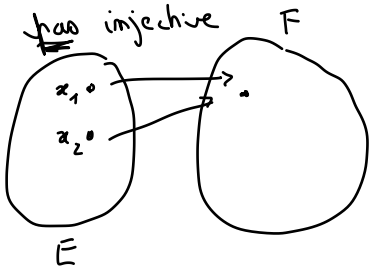
1) $\forall y \in F < 0$ pas d'antécédent

2) $\forall y \in F > 0$ 2 antécédents

pas surjective



pas injective



* déf : $f : E \longrightarrow F$ est injective

$\forall x_1, x_2 \in E \quad f(x_1) = f(x_2) \Longrightarrow x_1 = x_2$

→ intuition : $\forall y \in F$ pas $\exists x$ tq $y = f(x)$ alors $\nexists x'$ tq $f(x) = f(x') = y$

"par l'absurde" .....

il existe au plus ...

* déf : $f : E \longrightarrow F$ est surjective

$\forall y \in F \quad \exists x \in E$ tq $y = f(x)$

Bijective = injective + surjective

Prop. Si f bijective alors $\exists\, g : F \longrightarrow E$ tq

$f \circ g = Id_F$ et $g \circ f = Id_E$

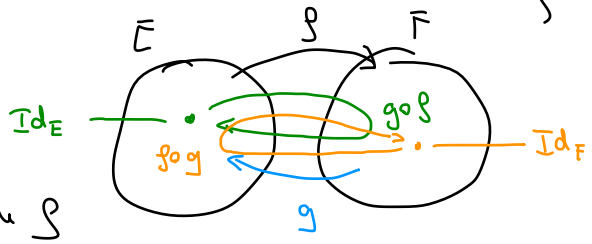
$Id_E : E \longrightarrow E$

$x \longmapsto x$

Cette appli est unique

→ notée f^{-1}

→ application réciproque de f



⚠ si f non bijective $\not\exists f^{-1}$

ex:

$$f : \mathbb{R}^2 \longrightarrow \mathbb{R}$$

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto x \times y$$