S. 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

$\Rightarrow$ implication

propositions

$A \Rightarrow B$ vraie si

si A vrai alors B vraie ←

table de vérité de $A \Rightarrow B$

$A \backslash B$	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 : $\forall x \in \emptyset \Rightarrow \dots$ → vrai

- ET OU NON

  $\wedge \quad \vee \quad \neg$ → $\neg\neg A \overset{\text{équiv}}{\equiv} A$

- $\Leftrightarrow$ équivalent

  $(A \Leftrightarrow B$ ssi $A \Rightarrow B$ et $B \Rightarrow A$

• $\forall$ pour tout

$\exists$ il existe

$\neg$

II. Ensembles

Ensemble : collection d'éléments

→ notation en extension : $\{a, b, 1, e \dots\}$ — énumération

$\emptyset$ — ens. vide.

→ notation en intention : $\{x \in \mathbb{Z} \,;\, \exists y \in \mathbb{Z} \quad x = 2y\}$ — nombres pairs.

+ $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$

Ensembles :

→ opérations ensemblistes — ens → ens

$\complement$ complémentaire, $\cap$ inter, $\cup$ union, Δ diff. sym.

→ propositions ensemblistes — ens → prop (V/F)

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

Propositions ensemblistes

• $x \in A$ (elt, ensemble) si x est un élément de la collection A.

$A_1 = \{1, 2, 3\}$ → ensemble "typé"

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

$A_2 = \{\underbrace{\{1,2\}}_{①}, \underbrace{\{1\}}_{②}, \underbrace{1}_{③}, \underbrace{2}_{④}\}$ $\quad \{1\} \in A_2 \quad \emptyset \notin A$

ens. non typé

① ②) ens. d'entiers

③ ④) entiers.

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

$\emptyset \in B$

- $\underbrace{A \subseteq B}_{\text{ensembles}}$ inclus

si $\forall x \in A \quad x \in B$ écriture $\rightsquigarrow$ "propre" $\forall \cancel{x}_y \, (\cancel{x}_y \in A \Rightarrow \cancel{x}_y \in B)$

variable "muette"

ex :

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

$\rotatebox{45}{$\subseteq$} \quad \cup\!\!\mid \quad \supseteq$

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

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

$\rotatebox{45}{$\subseteq$} \qquad \cup\!\!\mid$ (*) $\qquad \cup\!\!\mid$

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

↓

toujours vrai

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

F $\Rightarrow$ ... ✓

$A \Rightarrow B$ 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

Autres notations

⚠ $\complement_A B \to A \setminus B$ ✓

$\cancel{A - B}$

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

$\complement A$, $\complement B$

$\complement A \to \overline{A}$

ex : entiers — $\mathbb{N}$

$A \subseteq \mathbb{N}$

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

⚠

$\complement_C (\complement_A B) \ldots$

$\neq$

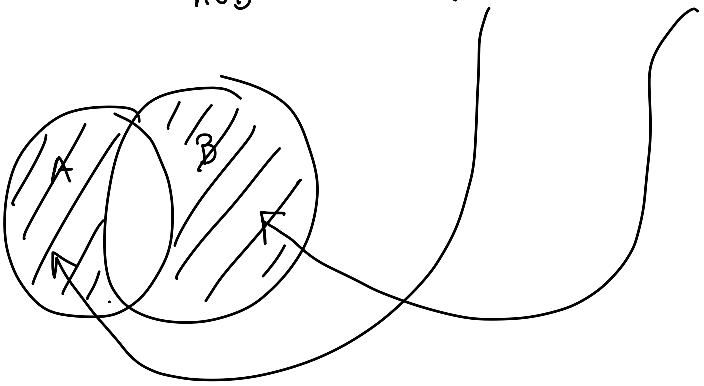
$C - (A - B)$

$\neq$

$\cancel{C - A + B}$) $\neq$

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

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



Parties d'un ensemble

E : ensemble — $|E| = n$

$\mathcal{P}(E)$ — ensemble des sous-ensembles / parties de E

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

Cardinal de E

↓

nbre d'élts.

$|E|$ $\#E$

ex :

$E = \{1,2,3\} \longrightarrow \mathcal{P}(E) = \{ \underbrace{\emptyset}_{0 \text{ élts}}, \underbrace{\{1\},\{2\},\{3\}}_{1 \text{ élt} \to \text{singletons}}, \underbrace{\{1,2\},\{1,3\},\{2,3\}}_{2 \text{ élts}}, \underbrace{\{1,2,3\}}_{3 \text{ élts}} \}$

énum par card ↗

$\mathcal{P}(E) = \{ A \subseteq E \}$ | $|A| \leq \underbrace{|E|}_{3}$

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

III. Méthodologie du raisonnement

→ validation / preuves auto / preuves formelles

Coq / méthode B | ...

Z

⇝ méthode de démonstration

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

② Notations : séparer → hypothèses → $\boxed{\text{encadrées}}$

→ ce que l'on veut montrer → but ?

③ On travaille sur le but $\xrightarrow{\text{forme}}$ 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 : $A \subseteq B \Longrightarrow A \cap B = A$? ← but

implication ⇝ on suppose ce qui est à gauche

nouveau but : ——— droite

On suppose que $\boxed{A \subseteq B}$

$A \cap B = A$?

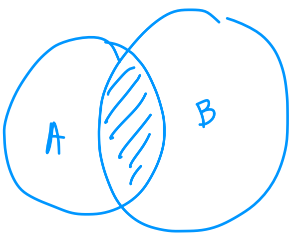
égalité d'ens ⇝ déf double $\subseteq$

$A \cap B \subseteq A$?

↓

toujours vrai (par déf. de $\cap$)

✓



$A \subseteq A \cap B$?

inclusion ⇝ déf $\forall x \in$ ens. gauche ... ← hyp.

↓

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

(*)

Soit $\boxed{x}$

On suppose $\boxed{x \in A}$ (*)

$x \in A \cap B$?

$\Updownarrow$

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

↳ prouvable à partir des hypothèses

$x \in A$ est une hypothèse (*)

et comme $A \subseteq B$

$\Longrightarrow x \in B$

Donc $x \in A$ et $x \in B$ ✓

◇

② But : équivalence $A \Longleftrightarrow B$ ← 1 but

pour prouver

On montre $A \Rightarrow B$ ← 2 sous-buts.   ex : .....
et $B \Rightarrow A$

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

→ $\boxed{\text{soit } x}$ ← variable neuve (quelconque)   ⇐ crée une variable "fraîche"

→ on prouve $P(x)$

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

⋮

on suppose $\boxed{A \subseteq B}$ $A \cap B = A$!

$A \cap B \subseteq A$? $A \subseteq A \cap B$?

✓   ⇕

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

∀

Soit $\boxed{\cancel{x}}$

$\cancel{x} \in A \Longrightarrow \cancel{x} \in A \cap B$!

implication ⤳

on suppose $\boxed{x \in A}$

$x \in A \cap B$?

⋮

(4) But : ∃ → $\exists x \; P(x)$

→ construire un exemple de x / x particulier tq $P(x)$ vraie ex : $\forall n \in \mathbb{N} \quad \exists m \in \mathbb{N}$ tq $n \geq 2m$?

$n = 1$

$n = 10$

$\forall$

Soit $\boxed{n \in \mathbb{N}}$

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

$m = 2$ marche...

5 ~

0

$10 \geq 2.2$

2.5

$\exists$ ~> construire un m "qui marche"

↳ on pose $m = \ldots$ ~> Prop 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 $n \geq 2.m$ ✓

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

$\Longrightarrow \neg A$ fausse $\Longrightarrow \neg\neg A$ vraie

$\neg\neg A = A$

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

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

par l'absurde

on suppose

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

on suppose p, q premiers

On a $\sqrt{2} = \dfrac{p}{q} \overset{\wedge 2}{\Longrightarrow} 2 = \dfrac{p^2}{q^2}$

$\Longrightarrow \underbrace{2 \cdot q^2}_{\text{pair}} = p^2 \quad (1) \qquad \cdots \Longrightarrow p \text{ pair}$

$\Longrightarrow \underset{\substack{\shortparallel \\ p \times p}}{p^2} \text{ pair} \Longrightarrow p \text{ pair}$

$\left. \begin{array}{l} 2 \mid p^2 = p \times p \\ 2 \text{ premier} \end{array} \right) \Longrightarrow 2 \mid p$

divise

th. Gauss $\left| \begin{array}{l} p \mid a \times b \\ p \text{ premier} \end{array} \right. \Longrightarrow p \mid a$ ou $p \mid b$

$\underset{3 \times 2}{6} \mid a \times b \;\not\Longrightarrow\; 6 \mid a$ ou $6 \mid b$

Donc $p = 2 \cdot n$

Donc (1) devient $\cancel{2} q^2 = p^2 = (2n)^2 = \cancel{4}^{\,2} \cdot n^2$

$\Longrightarrow q^2 = 2 \cdot n^2 \quad (2)$

$\Downarrow$ de même

q pair

(1) $2q^2 = p^2$

$\Downarrow$

p pair

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

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

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

$\diamond$

6) Raisonnement par récurrence

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

Récurrence stricte ~ généralement

→ Au rang n_0

on prouve $P(n_0)$

→ Au rang n

on suppose $\boxed{P(n)}$ vraie

→ Au rang $n+1$

on montre $P(n+1)$?

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

Récurrence (forte / large)

→ Au rang n_0

on prouve $P(n_0)$

→ Au rang n → la prop. vraie jusqu'à n

(on suppose $\boxed{P(\cancel{n} k)}$ vraie $\forall k \leq n$

→ Au rang $n+1$

on montre $P(n+1)$?

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

ex :

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

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

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

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

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

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 $n+1$ ⇝ factoriser $n+1$ ...

⇝ si $n+1$ premier $n+1 = n+1$ ... ✓

⇝ sinon il se décompose

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

$20 = 4 \times 5$

$\Downarrow$

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

HR HR

a ⇝ factorisable

b ⇝ "

$a \times b$ factorisable

IV. Applications — notion ensembliste

fonctions ⟶ pas forcément définie sur tout E

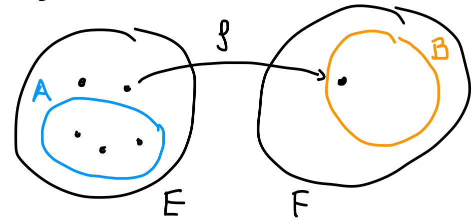
✗

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

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



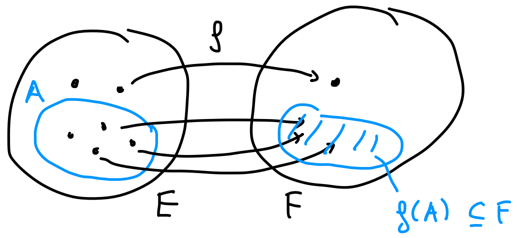
① Image directe et réciproque

* **déf**: $f : E \to F$ une application

$A \subseteq E$

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

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

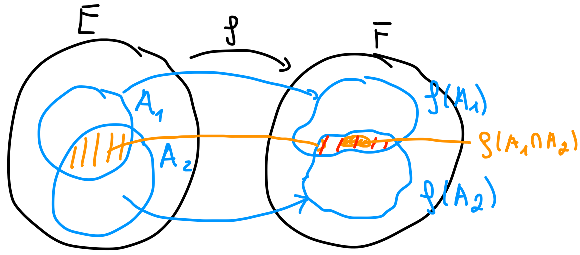


Prop. si $A_1, A_2 \subseteq E$

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

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

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



dém. de ii)

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

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

Soit $\boxed{y \in f(A_1 \cap A_2)}$ $\qquad y \in f(A_1) \cap f(A_2)$?

$\Longleftarrow$

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

$\Updownarrow \qquad \Updownarrow$

$\exists x_1 \in A_1$ tq $y = f(x_1)$? $\quad (*)$ $\qquad \exists x_2 \in A_2$ tq $y = f(x_2)$? $\quad (**)$

$\exists \ldots \qquad \exists \ldots$

⇝ trouver $x_1, x_2 \ldots$

↳ Rep. ...

⚠ NOMS DE VARIABLES !

$f : E \longrightarrow F$

$x \quad x'$ $\qquad y \quad y'$

$x_1 \quad x_2$ $\qquad y_1 \quad y_2$

$\vdots \qquad \vdots$

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

$\Longrightarrow \underbrace{\exists x \in A_1 \cap A_2}_{\Downarrow}$ tq $y = f(x)$

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

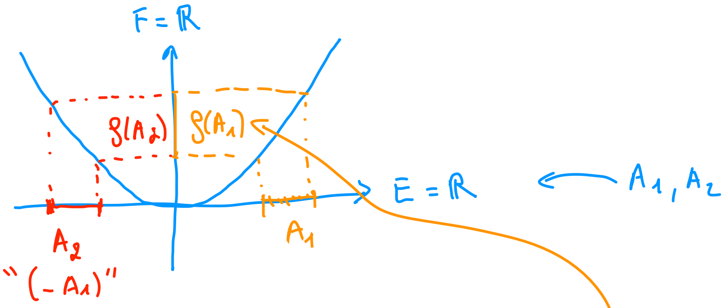
prendre $x_1 = x$ convient pour prouver (*)

$x_2 = x$ ______ (**)

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

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

$x \longmapsto x^2$



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

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

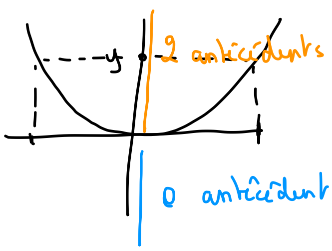
Rem : $f : \mathbb{R} \longrightarrow \mathbb{R}$

$x \longmapsto x^2$

$\cancel{f^{-1}}$

$x^2 = 1$

$f(x) = 1$



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

$= \{1, -1\}$

$\cancel{f^{-1}(1)}$ 1, -1

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

$\cancel{f^{-1}(-2)}$?

$\cancel{f^{-1}}$

$\tilde{f}$

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