A) INDENOMBRABILITE (vs. finitude et dénombrabilité)

I) Préliminaires : les preuves

Qu'est-ce qu'une preuve ?

Historiquement, une preuve est une démonstration avec des mots, des formules, des figures… qui donne une compréhension "soudaine" de pourquoi une propriété est forcément vraie. Autrement dit, c'est une argumentation logique et indubitable.

On va s'en remettre à quelques principes logiques. Le but "ultime" serait de pouvoir faire une preuve "automatique". On cherche donc une formalisation extrême par une suite de symboles.

Mais avant de parler d'automatisation de la preuve, on peut débattre de l'automatisation de la vérification d'une preuve, puisqu'on est en effet capable de construire des programmes pour vérifier une preuve donnée.

On peut distinguer cinq techniques/architectures/structures de preuve :

- La preuve directe (pour montrer une implication $P \Rightarrow Q$)
- La preuve par contraposée (pour montrer $P \Rightarrow Q$)
- La preuve par contradiction/par l'absurde (pour montrer une propriété P)
- La preuve par disjonction de cas (pour montrer une propriété P)
- Le principe de récurrence et les ensembles bien ordonnés

Remarque : (rappels sur l'implication)

Schématiquement :

Soient A et B deux propriétés qu'on symbolise ainsi :

A : x x o o o o o o x x

B : x x x x o o o x x x

(où les x correspondent aux éléments qui ne vérifient pas la propriété et les o à ceux qui la vérifient)

Ici, on a $B \Rightarrow A$ car les éléments qui vérifient B vérifient aussi A (et pas l'inverse, ceux qui vérifient A ne vérifient pas nécessairement B)

Table de vérité :

P	Q	$P \iff Q$
F	F	V
F	V	F
V	F	F
V	V	V

1) *La preuve directe*

But : Montrer que P ⇒Q

Approche : Si P alors ..... et donc Q

Exemple : Montrer que : $\forall$ a, b ,c $\in \mathbb{Z}$, si a|b et a|c alors a|b-c (de la forme P ⇒Q)

On a : a|b $\Rightarrow \exists$ p $\in \mathbb{Z}$ tel que $b = ap$

a|c $\Rightarrow \exists$ q $\in \mathbb{Z}$ tel que $c = aq$

Alors $b-c = ap - aq = a(p-q)$

Or $(p-q) \in \mathbb{Z}$ donc par définition, a|b-c

2) *Preuve par contraposée*

But : Montrer que P ⇒Q

Approche : Montrer que si $\overline{Q}$ alors ..... on a $\overline{P}$

Remarque : On fait une preuve directe de $\overline{Q} \Rightarrow \overline{P}$

En effet, en comparant les tables de vérités, il est facile de voir qu'on a équivalence entre ces deux implications.

Exemple : Montrer que $\forall$ n $\in \mathbb{N}$, si n^2 est pair, alors n est pair

Par contraposée : on suppose n $\in \mathbb{N}$ impair (i.e. : $n = 2k + 1$ avec k $\in \mathbb{N}$)

Alors $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

Or $(2k^2 + 2k) \in \mathbb{N}$ donc n^2 est impair

Finalement : on a n^2 pair ⇒n pair

(On aurait aussi pu résoudre ce problème par preuve directe)

3) *La preuve par l'absurde*

But : Montrer une propriété P

Approche : Supposons $\overline{P}$ alors 1) ..... donc R

2) ..... donc $\overline{R}$

Conclusion : on a $\overline{P}$ ⇒R ∪ $\overline{R}$ ce qui est une contradiction donc P est vraie

Exemple : Montrer que $\sqrt{2}$ est irrationnel

Définition : (rationnel)

$$\forall\ a \in \mathbb{R}\ ,\quad a \in \mathbb{Q}\ \text{ si et seulement si }\ \exists\ p \in \mathbb{Z},\ q \in \mathbb{Z}^*\ \text{tels que}\quad a = \frac{p}{q}$$

Théorème : $\forall\ a \in \mathbb{Q},\quad \exists\ p \in \mathbb{Z},\ q \in \mathbb{Z}^*\ \text{ tels que }\ p \wedge q = 1\ \text{ et }\ a = \frac{p}{q}$

(Début preuve):

Supposons que $\sqrt{2}$ est rationnel.

Alors $\exists\ p \in \mathbb{Z},\ q \in \mathbb{Z}^*\ \text{ tels que }\ p \wedge q = 1\ \text{ et }\ \sqrt{2} = \frac{p}{q}$

D'où : $2 = \frac{p^2}{q^2} \Rightarrow 2q^2 = p^2 \Rightarrow p$ est pair (cf. preuve précédente)

Autrement dit : $\exists\ k \in \mathbb{Z}$ tel que $p = 2k$

D'où : $2q^2 = (2k)^2 = 4k^2 \Rightarrow q^2 = 2k^2$ donc q^2 est pair

Par le théorème précédent, on a donc q pair.

Or 2 est facteur commun à p et q mais on a aussi $p \wedge q = 1$: contradiction !

Finalement, $\sqrt{2}$ est irrationnel

4) *Preuve par disjonction de cas*

<u>But :</u> Montrer une propriété P

<u>Approche :</u> On sait que A ∪ B. On montre que A ⇒P et B ⇒P

Conclusion : on a P

Exemple : Montrer que $\exists\ x, y \in \mathbb{R}/\mathbb{Q}$ tels que $x^y \in \mathbb{Q}$

Cas A : $\sqrt{2}^{\sqrt{2}}$ est rationnel ⇒CQFD (on pose $x = \sqrt{2}$ et $y = \sqrt{2}$)

Cas B : $\sqrt{2}^{\sqrt{2}}$ est irrationnel ⇒on a $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = (\sqrt{2})^2 = 2 \in \mathbb{Q}$

(on pose $x = \sqrt{2}^{\sqrt{2}}$ et $y = \sqrt{2}$)

Dans les deux cas, on a montré la propriété.

Remarque : avec cette méthode on ne peut pas donner de x et y, on ne sait pas dans quel cas on est)

5) *Preuves par récurrence et principe des ensembles bien ordonnés*

- La preuve par récurrence simple :

But : Montrer que $\forall\ n \in \mathbb{N}$, on a P(n)

Approche : On montre P(0) *(initialisation)*

On montre $\forall\ i \in \mathbb{N}$: $P(i) \Rightarrow P(i+1)$ *(hérédité)*

Alors : $\forall\ n \in \mathbb{N}$, on a P(n)

- La preuve par récurrence forte :

But : Montrer que $\forall\ n \in \mathbb{N}$, on a P(n)

Approche : On montre P(0)

On montre $\forall\ i \in \mathbb{N}$: Si ($\forall\ k \in \mathbb{N}$, $k \leq i \Rightarrow P(k)$) alors $P(i+1)$

Alors : $\forall\ n \in \mathbb{N}$, on a P(n)

L'idée est que dans l'hérédité, on considère que la propriété est vraie au rang i et pour tous les $k \leq i$. On peut s'en servir si besoin.

- Le principe des ensembles bien ordonnés :

Définition : (ensemble bien ordonné)

On le note $(X, \leq)$ tel que l'ensemble X est muni d'une relation d'ordre totale $\leq$.

$(X, \leq)$ est bien ordonné si et seulement si :

$\forall\ X' \subseteq X$, $X' \neq \emptyset$, X' possède un plus petit élément.

Définition : (relation)

Soit R une relation sur l'ensemble X. On a $R \subseteq \{ (x, y) \mid x \in X \text{ et } y \in X\}$

Définition : (relation d'ordre)

Il s'agit d'une relation qui est :

- Transitive : $\forall\ x, y, z \in X$, xRy et $yRz \Rightarrow xRz$
- Antisymétrique : $\forall\ x, y \in X$, si xRy et yRx alors $x = y$
- Réflexive : $\forall\ x \in X$, xRx

On parle de relation d'ordre totale si : $\forall\ x, y \in X$, on a xRy ou yRx

Exemple : L'ensemble $(\mathbb{N}, \leq)$ est bien ordonné

L'ensemble $(\mathbb{R}, \leq)$ ne l'est pas ($X' = \{ x \in \mathbb{R} \mid x \geq 1 \} \subseteq \mathbb{R}$ n'admet pas de plus petit élément)

Exemple : Montrer que $\forall\ n \in \mathbb{N}\backslash\{0,1\}$, n est premier ou n est produit de nombres premiers

Initialisation : si $n = 2$, n est premier

si $n = 4 = 2*2$, n est produit de nombres premiers

Hérédité : On suppose que la propriété est vraie au rang $n \in \mathbb{N}$ et pour tout $k \leq n$ *(on utilise ici une récurrence forte)*. Montrons qu'elle est vraie au rang n+1 :

Si (n+1) est premier : il vérifie la propriété.

Sinon : $\exists\ a, b \in \mathbb{N}$ tels que $a \leq n$ et $b \leq n$ tels que $n + 1 = ab$

Or, puisque a et b sont inférieurs (ou égaux) à n, ils vérifient la propriété. Autrement dit, ils sont soit premiers, soit produit de nombres premiers.

Dans les deux cas, on a que (n+1) vérifie la propriété.

Conclusion : Par le principe de récurrence forte, on en conclut que la propriété est vraie pour tout entier naturel $n \geq 2$.

Schéma de la preuve en utilisant le principe des ensembles bien ordonnés :

But : Montrer que pour tout $n \in \mathbb{N}$, on a $P(n)$ (où P une propriété)

Approche :

Par l'absurde, supposons $\exists\ m \in \mathbb{N}$ tel que $\overline{P}(m)$ et on a alors que $A = \{ m \in \mathbb{N} \mid \overline{P}(m) \}$ non vide.

Donc par principe des ensembles bien ordonnés, on pose $a \in A$ le plus petit élément de A.

Alors ..... soit $a \notin A$ $\Rightarrow$ contradiction

soit $\exists\ b \in A$ tel que $b < a$ $\Rightarrow$ contradiction

Conclusion : $A \neq \varnothing \Rightarrow$ contradiction

Donc on doit avoir $A = \varnothing$ ce qui entraîne que $(\forall\ n \in \mathbb{N})$ on a $P(n)$

Remarque : $\forall\ x, y \in \mathbb{R}$, $x < y \Leftrightarrow x \leq y$ et $x \neq y$

Remarque : Il existe une notion d'ensembles quasiment bien ordonnés (résultat utile et puissant en recherche de nos jours)

II) Indénombrabilité

Il est pertinent de s'interroger sur la taille des ensembles (en particulier sur la taille de $\mathbb{N}$ et $\mathbb{R}$) afin notamment de les comparer. Or, on a grandement avancé sur ces questions –avec, par exemple, le travail de Cantor- et on peut maintenant affirmer que $\mathbb{N}$ et $\mathbb{R}$ sont tous deux des ensembles infinis. En allant encore plus loin, on constate qu'on a l'inclusion $\mathbb{N} \subseteq \mathbb{R}$, ce qui implique que $\mathbb{R}$ est plus grand que $\mathbb{N}$ (pourtant tous deux de taille infinie…).

Le but ici, va être de donner une définition formelle de ce qu'on appelle "ensemble infini" et d'expliciter un moyen de comparer les tailles d'ensembles infinis (autre que les inclusions qui ne sont pas toujours suffisantes ou pertinentes), à savoir la notion de bijection.

Définition :

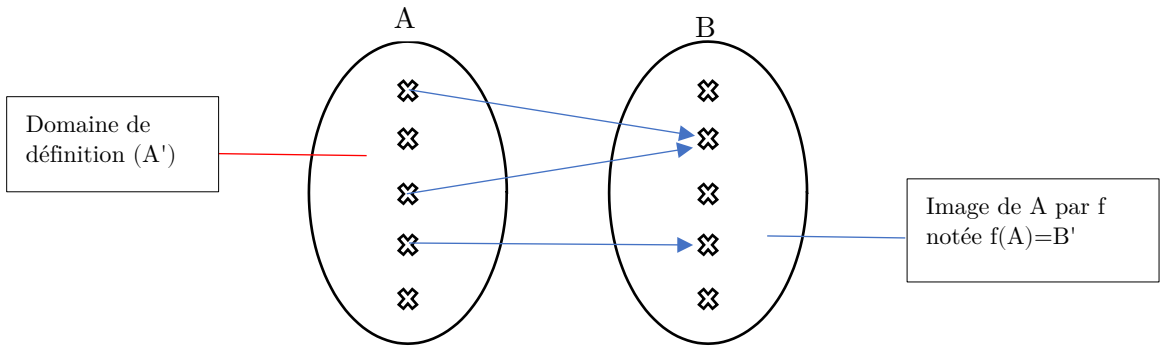
Soit Γ l'ensemble des relations sur deux ensembles A et B (on a $\Gamma \subseteq AxB$).
Alors on a que $(a, b) \in \Gamma$ si et seulement si il existe une relation R telle que aRb (i.e. $a \in A$ est en relation avec $b \in B$)

Définition : (fonction)

Soient A et B deux ensembles. Une fonction f de A dans B associe à tout élément de $a \in A$ au plus une image dans B, notée f(a). En terme de relation, on écrit :

$$\forall\ a \in A,\ \text{si}\ \exists\ b \in B\ \text{tel que}\ aR_f b\ \text{alors}\ \exists!\ b \in B\ \text{tel que}\ aR_f b$$

Schéma :



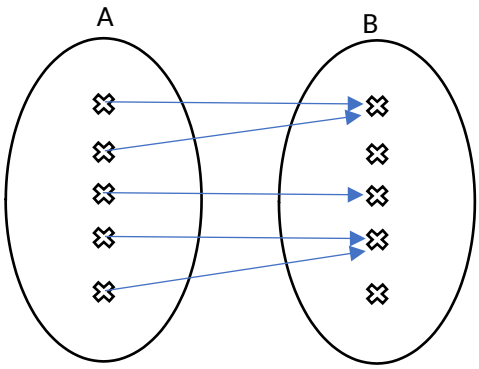
Définition : (application de A dans B)

Il s'agit d'une fonction de A vers B telle que tous les éléments de A ont une image:

$$\forall\ a \in A,\ \exists\ b \in B\ \text{tel que}\ b = f(a)$$

En reprenant les notations du schéma précédent, on peut dire qu'une application irait de A' vers B

Schéma :



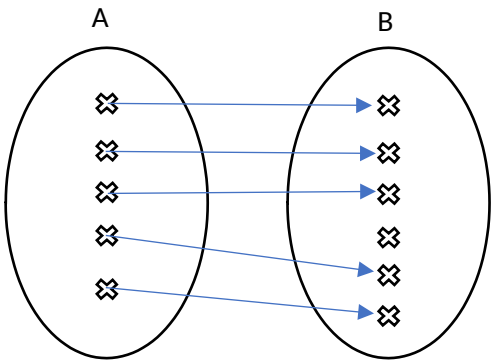
Définition : (Application injective)

Une application f de A vers B est dite injective si deux éléments distincts de A ont toujours deux images distinctes dans B.

$$\forall\ x, y\ \in A,\ \ x \neq y \quad \Rightarrow f(x) \neq f(y)$$

(on peut aussi écrire la contraposée : $\forall\ x, y\ \in A,\ \ f(x) = f(y) \quad \Rightarrow x = y$)

Schéma :

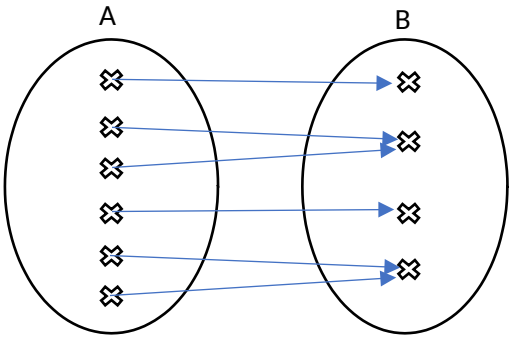


Définition : (Application surjective)

Une application f de A vers B est dite surjective si tout élément de b admet au moins un antécédent dans A.

$$\forall\ b \in B,\ \ \exists\ \ a \in A\ \ \text{tel que}\ \ f(a) = b$$

Schéma :

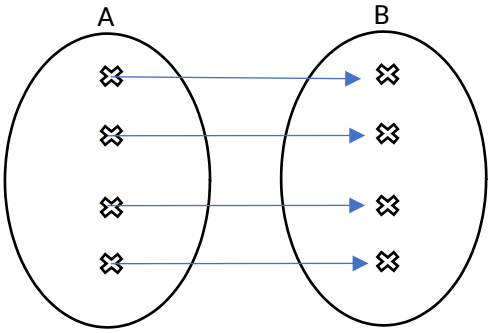


Définition : (Application bijective)

Une application f de A vers B est dite bijective si elle est à la fois injective et surjective.

$$\forall\ a \in A,\ \ \exists!\ \ b \in B\ \ \text{tel que}\ f(a) = b$$

Schéma :



On a une correspondance, un à un, entre les éléments de A et les éléments de B

En ce qui concerne la taille des ensembles maintenant, il nous faut introduire la notion d'ensemble infini.

Définition : (ensemble infini)

Soit X un ensemble. On dit que X est infini s'il existe une bijection de X vers un sous-ensemble de X qui n'est pas lui-même.

Exemple : On peut montrer que $\mathbb{N}$ est infini.

En effet, si on pose f une fonction de $\mathbb{N}^*$ dans $\mathbb{N}$ qui à $n \in \mathbb{N}^*$ associe $(n+1)$, on a bien f une bijection. En effet :

- Il s'agit d'une application de par la définition de $\mathbb{N}$ selon laquelle tout entier a un suivant
- Elle est injective : Soient $p, q \in \mathbb{N}$ tels que $p+1 = q+1$. Alors on a $p = q$.
- Elle est surjective : tout entier non nul a un précédent (dont il est le suivant)

$\forall p \in \mathbb{N}^*, \quad f(p-1) = p$

Définition : (ensembles de même taille)

Deux ensembles A et B (possiblement infinis) sont de même taille si et seulement si il existe une bijection de l'un dans l'autre.

Définition : (ensemble dénombrable)

Un ensemble infini X est dénombrable si et seulement si X est en bijection avec $\mathbb{N}$.

Corollaire :

Soient Y et X deux ensembles tels que $Y \subseteq X$. Si Y infini, alors X est infini.

Remarque : "Dénombrable" équivaut à "énumérable" dans le sens où dire qu'un ensemble est dénombrable revient à dire qu'on peut indexer chacun de ses éléments.

Remarque : on a que $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$

Il existe d'autres ensembles bien connus notamment celui des nombres algébriques (et de leur complémentaire, l'ensemble des nombres transcendants). Un nombre réel x est dit algébrique s'il existe un polynôme non nul P à coefficients rationnels tel que P(x)=0.

Exemple : Montrer que $\mathbb{Z}$ est dénombrable.

- Méthode 1 : On veut établir une bijection entre $\mathbb{Z}$ et $\mathbb{N}$.

Soit f la fonction qui va de $\mathbb{Z}$ dans $\mathbb{N}$ et qui à x ($x \in \mathbb{Z}$) associe :

- 2^*x si $x \geq 0$
- $2^*|x| - 1$ sinon

On a bien que f est une bijection puisque :

(i) f est une application par définition de $\mathbb{Z}$

(ii) f est surjective : Soit $n \in \mathbb{N}$.

Si n est pair, il existe $x \in \mathbb{Z}_+$ tel que $f(x) = n$

Si n est impair, il existe $x \in \mathbb{Z}_-^*$ tel que $f(x) = n$

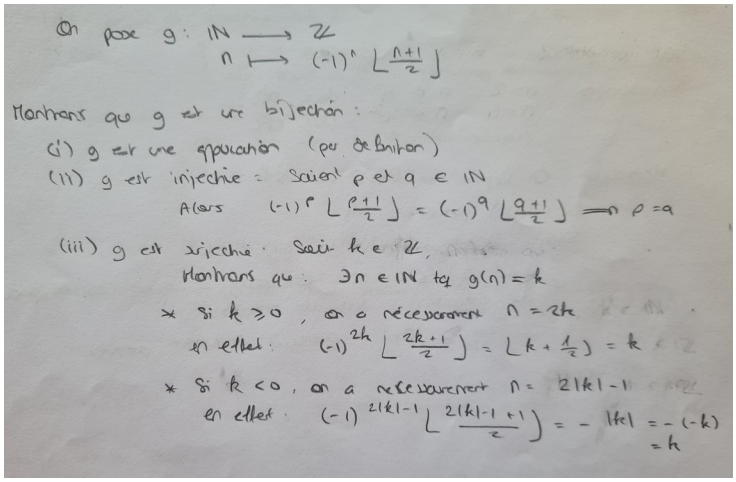
(iii) f est injective : Soient $x, y \in \mathbb{Z}$ tels que $x \neq y$.

Si $x < 0$ et $y > 0$ on a nécessairement $2|x| - 1 \neq 2y$

Si $x, y > 0$, on a aussi que $2x \neq 2y$

Si $x, y < 0$, on a aussi que $2|x| - 1 \neq 2|y| - 1$

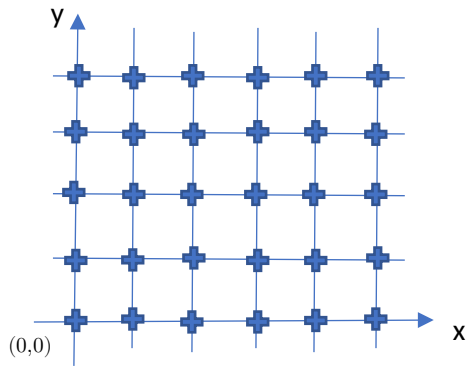
- Méthode 2 : On veut établir une bijection entre $\mathbb{Z}$ et $\mathbb{N}$



Exemple : Montrer que $\mathbb{N}^2$ est dénombrable

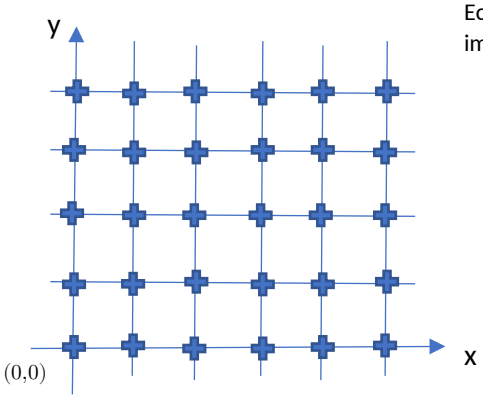
On rappelle que $\mathbb{N}^2 = \{ (a, b) \mid a \in \mathbb{N} \text{ et } b \in \mathbb{N}\}$.

Schématiquement, on peut représenter $\mathbb{N}^2$ ainsi :



On voit qu'on peut passer par tous les points en effectuant ce parcours.
Autrement dit, on est capable d'indexer tous les points

Afin de vérifier qu'on passe effectivement par tous les points, on peut écrire un programme (dont on sera sûr qu'il se termine en un nombre fini d'itérations) qui modélise ce chemin. Pour plus de faciliter et de cohérence, on garde la même idée en changeant légèrement ledit parcours. Ainsi, en posant (a,b) le couple à trouver on a :



Ecrivons un programme pour implémenter ce parcours :

```
k <-- max(a,b)
tant que vrai :
    pour i allant de 0 à k :
        afficher (i,k)
    pour i allant de 1 à k :
        afficher (k, k-i)
    k <-- k + 1
```

ou autre prossibilité :

```
i <-- 0
j <-- 0
tant que vrai :
    tant que vrai :
        afficher (i,j)
        j <-- j + 1
    fin tant que
    i <-- i + 1
fin tant que
```

Une autre possibilité consiste en le parcours (et le programme) suivant :

```
k <-- a + b
tant que vrai :
    pour i allant de 0 à k :
        affiher (i, k-i)
```