

BUT Informatique

Année universitaire 2022 / 2023

R1.06 – Mathématiques discrètes


Responsable : A. Ridard


Autres intervenants : R. Fleurquin et T. Godin



Avant-propos

Ce document est spécifiquement rédigé pour des séances de Cours/TD.

Il présente les éléments de cours habituels (définitions et propriétés) enrichis de remarques, indiquées par  , donnant un certain éclairage pour mieux les comprendre, les retenir et les utiliser.

Ce cours est aussi ponctué d'exercices, indiqués par  , qui seront traités en classe ou à la maison pour bien assimiler les différentes notions présentées. Grâce à ces exercices, vous allez fabriquer les exemples du cours ainsi que certaines preuves. C'est effectivement en étant acteur dans ses apprentissages que l'on profite au mieux des enseignements!

Ce document sera complété par des feuilles de TD pour s'entraîner d'avantage.

Bonne lecture, et bon travail...

Table des matières

I.	Rudiments de logique	6
1.	Assertion et premières opérations	6
2.	Règles opératoires	7
3.	Deux autres opérations : l'implication et l'équivalence	8
4.	Quantificateurs	10
5.	Raisonnements et démonstrations	10
II.	Ensemble	15
1.	Définition et inclusion	15
2.	Opérations sur les parties d'un ensemble	17
3.	Règles opératoires	19
4.	Deux autres opérations sur les parties d'un ensemble : la différence et la différence symétrique	20
5.	Produit cartésien	21
III.	Relation binaire de E vers F	22
1.	Définition et représentations	22
2.	Fonction et application	23
3.	Image directe et image réciproque	27
4.	Dénombrement (hors programme)	28
IV.	Relation binaire sur E	32
1.	Définition et propriétés	32
2.	Une relation qui permet de « classifier » : la relation d'équivalence	33
3.	Une relation qui permet de « comparer » : la relation d'ordre	34

I. Rudiments de logique

1. Assertion et premières opérations

Définition (assertion).

Une assertion est une « phrase mathématique syntaxiquement correcte » qui est soit vraie, soit fausse.

Dans ce qui suit, \mathcal{P} , \mathcal{Q} et \mathcal{R} désigneront des assertions.

Définition (négation).

La négation de \mathcal{P} est l'assertion définie comme étant vraie lorsque \mathcal{P} est fausse, et inversement. On la notera « non(\mathcal{P}) » ou encore $\neg\mathcal{P}$.



Autrement dit, la négation de \mathcal{P} a pour table de vérité :

\mathcal{P}	$\neg\mathcal{P}$
V	F
F	V

Définition (conjonction).

La conjonction de \mathcal{P} et \mathcal{Q} est l'assertion définie comme étant vraie si \mathcal{P} et \mathcal{Q} le sont toutes les deux, et fausse sinon. On la notera « \mathcal{P} et \mathcal{Q} » ou encore $\mathcal{P} \wedge \mathcal{Q}$.



Autrement dit, la conjonction de \mathcal{P} et \mathcal{Q} a pour table de vérité :

\mathcal{P}	\mathcal{Q}	$\mathcal{P} \wedge \mathcal{Q}$
V	V	V
V	F	F
F	V	F
F	F	F

Définition (disjonction).

La disjonction de \mathcal{P} et \mathcal{Q} est l'assertion définie comme étant fausse si \mathcal{P} et \mathcal{Q} le sont toutes les deux, et vraie sinon. On la notera « \mathcal{P} ou \mathcal{Q} » ou encore $\mathcal{P} \vee \mathcal{Q}$.



| Le « ou » du langage commun est *exclusif* alors que le « ou » logique est *inclusif*



Autrement dit, la disjonction de \mathcal{P} et \mathcal{Q} a pour table de vérité :

\mathcal{P}	\mathcal{Q}	$\mathcal{P} \vee \mathcal{Q}$
V	V	V
V	F	V
F	V	V
F	F	F

2. Règles opératoires

Définition (équivalence logique).

On dit que \mathcal{P} et \mathcal{Q} sont logiquement équivalentes si elles ont la même table de vérité.
On notera alors $\mathcal{P} \sim \mathcal{Q}$.



- Pour ne pas confondre avec l'équivalence usuelle^a, « $\mathcal{P} \sim \mathcal{Q}$ » pourra se lire « \mathcal{P} a même table de vérité que \mathcal{Q} »
- On utilisera surtout cette notion pour transformer une assertion, en particulier grâce aux règles suivantes

a. L'équivalence usuelle notée \iff sera définie plus tard

Propriété (idempotence).

- $(\mathcal{P} \text{ et } \mathcal{P}) \sim \mathcal{P}$
- $(\mathcal{P} \text{ ou } \mathcal{P}) \sim \mathcal{P}$

Propriété (commutativité).

- $(\mathcal{P} \text{ et } \mathcal{Q}) \sim (\mathcal{Q} \text{ et } \mathcal{P})$
- $(\mathcal{P} \text{ ou } \mathcal{Q}) \sim (\mathcal{Q} \text{ ou } \mathcal{P})$

Propriété (associativité).

- $(\mathcal{P} \text{ et } (\mathcal{Q} \text{ et } \mathcal{R})) \sim ((\mathcal{P} \text{ et } \mathcal{Q}) \text{ et } \mathcal{R})$
- $(\mathcal{P} \text{ ou } (\mathcal{Q} \text{ ou } \mathcal{R})) \sim ((\mathcal{P} \text{ ou } \mathcal{Q}) \text{ ou } \mathcal{R})$



On peut alors supprimer les parenthèses lorsqu'il n'y a que des conjonctions (resp. disjonctions)

Propriété (distributivité).

- $(\mathcal{P} \text{ et } (\mathcal{Q} \text{ ou } \mathcal{R})) \sim ((\mathcal{P} \text{ et } \mathcal{Q}) \text{ ou } (\mathcal{P} \text{ et } \mathcal{R}))$
- $(\mathcal{P} \text{ ou } (\mathcal{Q} \text{ et } \mathcal{R})) \sim ((\mathcal{P} \text{ ou } \mathcal{Q}) \text{ et } (\mathcal{P} \text{ ou } \mathcal{R}))$



Même s'il existe des règles de priorités (d'abord négation, puis conjonction, et enfin disjonction), on évitera de supprimer les parenthèses lorsqu'il y a différentes opérations



Dans ce qui précède, on effectue les transformations suivantes ^a :

Faux	→	0
Vrai	→	1
$\mathcal{P}, \mathcal{Q}, \mathcal{R}$	→	x, y, z
non(.)	→	$\bar{}$
et	→	\times
ou	→	$+$
\sim	→	$=$

1. Compléter les tables de multiplication et d'addition suivantes :

\times	0	1
0		
1		

$+$	0	1
0		
1		

2. Énoncer les deux distributivités.
3. Ces notations \times et $+$ sont-elles dangereuses?

a. On définit ainsi l'algèbre de Boole $\mathbb{B} = (\{0, 1\}, \bar{}, \times, +)$ et ses règles de calcul, particulièrement utile à la conception des circuits logiques en informatique

Propriété (lois de Morgan).

- $(\text{non}(\mathcal{P} \text{ et } \mathcal{Q})) \sim (\text{non}(\mathcal{P}) \text{ ou } \text{non}(\mathcal{Q}))$
- $(\text{non}(\mathcal{P} \text{ ou } \mathcal{Q})) \sim (\text{non}(\mathcal{P}) \text{ et } \text{non}(\mathcal{Q}))$



Démontrer cette propriété (en comparant les tables de vérité)

3. Deux autres opérations : l'implication et l'équivalence

Définition (implication).

L'implication « $\mathcal{P} \Rightarrow \mathcal{Q}$ » est l'assertion définie comme étant fausse si \mathcal{Q} est fausse alors que \mathcal{P} est vraie, et vraie sinon.



Autrement dit, l'implication « $\mathcal{P} \Rightarrow \mathcal{Q}$ » a pour table de vérité :

\mathcal{P}	\mathcal{Q}	$\mathcal{P} \Rightarrow \mathcal{Q}$
V	V	V
V	F	F
F	V	V
F	F	V

Propriété (contraposition).

$$(\mathcal{P} \Rightarrow \mathcal{Q}) \sim (\text{non}(\mathcal{Q}) \Rightarrow \text{non}(\mathcal{P}))$$



On dit que « $\text{non}(\mathcal{Q}) \Rightarrow \text{non}(\mathcal{P})$ » est la *contraposée* de « $\mathcal{P} \Rightarrow \mathcal{Q}$ »



Démontrer cette propriété

Propriété (négation d'une implication).

$$(\text{non}(\mathcal{P} \Rightarrow \mathcal{Q})) \sim (\mathcal{P} \text{ et } \text{non}(\mathcal{Q}))$$



1. Démontrer cette propriété
2. En déduire : $(\mathcal{P} \Rightarrow \mathcal{Q}) \sim (\text{non}(\mathcal{P}) \text{ ou } \mathcal{Q})$. **Ce résultat pourra maintenant être utilisé directement**

Définition (équivalence).

L'équivalence « $\mathcal{P} \Leftrightarrow \mathcal{Q}$ » est l'assertion définie comme étant vraie si \mathcal{P} et \mathcal{Q} ont même valeur de vérité.



Autrement dit, l'équivalence « $\mathcal{P} \Leftrightarrow \mathcal{Q}$ » a pour table de vérité :

\mathcal{P}	\mathcal{Q}	$\mathcal{P} \Leftrightarrow \mathcal{Q}$
V	V	V
V	F	F
F	V	F
F	F	V

Propriété (double implication).

$$(\mathcal{P} \Leftrightarrow \mathcal{Q}) \sim ((\mathcal{P} \Rightarrow \mathcal{Q}) \text{ et } (\mathcal{Q} \Rightarrow \mathcal{P}))$$



Transformer en une assertion logiquement équivalente exprimée uniquement avec des négations et des conjonctions :

1. $\text{non}(\mathcal{P} \text{ ou } \mathcal{Q})$
2. $\mathcal{P} \text{ ou } \mathcal{Q}$
3. $\mathcal{P} \Rightarrow \mathcal{Q}$
4. $\text{non}(\mathcal{P} \Leftrightarrow \mathcal{Q})$

4. Quantificateurs

Lorsque la valeur de vérité de \mathcal{P} dépend d'un paramètre x , cette assertion peut être notée $\mathcal{P}(x)$ afin de souligner cette dépendance.

Définition (quantification universelle).

La quantification universelle « $\forall x \in E, \mathcal{P}(x)$ » est l'assertion définie comme étant vraie si $\mathcal{P}(x)$ est vraie pour tout élément x de l'ensemble^a E .

^a. On reviendra sur la notion d'ensemble plus tard

Définition (quantification existentielle).

La quantification existentielle « $\exists x \in E, \mathcal{P}(x)$ » est l'assertion définie comme étant vraie si $\mathcal{P}(x)$ est vraie pour au moins un élément x de l'ensemble E .



- Les symboles \forall et \exists se lisent « quelque soit » et « il existe »
- La variable x est dite muette (on peut la remplacer par une autre, y par exemple, sans changer la valeur de vérité)



Quand l'assertion suivante est-elle vraie?

$$\left((\exists x \in E, \mathcal{P}(x)) \text{ et } (\forall x \in E, \forall x' \in E, (\mathcal{P}(x) \text{ et } \mathcal{P}(x')) \implies (x = x')) \right)$$

On la notera plus simplement :

$$\exists ! x \in E, \mathcal{P}(x)$$


Axiome (négation d'une phrase quantifiée).

- $\text{non}(\forall x \in E, \mathcal{P}(x)) \sim \exists x \in E, \text{non}(\mathcal{P}(x))$
- $\text{non}(\exists x \in E, \mathcal{P}(x)) \sim \forall x \in E, \text{non}(\mathcal{P}(x))$



Dans une théorie formelle, mathématique ou non, un axiome est une assertion considérée comme étant vraie sans justification, servant ainsi de point de départ. Une théorie est alors un empilement ordonné d'axiomes, de démonstrations et de propriétés appelées aussi théorèmes, incluant également des définitions pour créer des classes d'objets.

5. Raisonnements et démonstrations

Dans cette partie, nous présentons les raisonnements de base utilisés en Mathématiques, accompagnés de leur rédaction  . Nous nous limitons ici aux cas les plus fréquents, mais un exposé exhaustif est disponible en annexe.

Présentons d'abord deux techniques générales de démonstration.

Pour démontrer une assertion \mathcal{P} c'est à dire montrer que \mathcal{P} est vraie

Propriété (par déduction).

On détermine une assertion vraie \mathcal{Q} telle que « $\mathcal{Q} \implies \mathcal{P}$ » soit vraie.



Lorsque l'implication « $\mathcal{Q} \implies \mathcal{P}$ » est vraie, on dit que :

- \mathcal{Q} est une condition suffisante pour avoir \mathcal{P}
- ou encore, il suffit d'avoir \mathcal{Q} pour avoir \mathcal{P}

Mais, on dit aussi que :

- \mathcal{P} est une condition nécessaire pour avoir \mathcal{Q}
- ou encore, il faut avoir \mathcal{P} pour avoir \mathcal{Q}

L'implication vraie « $\mathcal{Q} \implies \mathcal{P}$ » peut représenter une propriété du cours exprimée sous la forme « Si \mathcal{Q} , alors \mathcal{P} ».

En montrant que l'hypothèse \mathcal{Q} est vraie, on est bien certain que la conclusion \mathcal{P} le soit aussi (savez-vous pourquoi?)

On pourra évidemment utiliser un « enchaînement d'implications ».



Ne surtout pas utiliser le connecteur logique « \implies » à la place du mot « donc » dans une démonstration par déduction.

En général, on évitera de mélanger dans une même phrase le langage mathématique et le langage commun.



\mathcal{Q} est vraie

Or $\mathcal{Q} \implies \mathcal{P}$ est vraie

Donc \mathcal{P} est vraie

Plus simplement ^a, on écrira :

\mathcal{Q}

Or $\mathcal{Q} \implies \mathcal{P}$

Donc \mathcal{P}

^a. En logique, on doit toujours préciser la valeur de vérité d'une assertion (elle peut être soit vraie, soit fausse). En Mathématiques, lorsque l'on écrit une assertion sans préciser sa valeur de vérité, c'est qu'elle est vraie! Par exemple, on n'écrit pas « $\forall x \in \mathbb{R}, e^x > 0$ est vraie », mais simplement « $\forall x \in \mathbb{R}, e^x > 0$ ». **Dès à présent, sauf dans les explications des raisonnements logiques qui suivent (pour un maximum de clarté), on préférera ce langage simplifié.**



1. Démontrer « $\ln(\pi) > 0$ » en utilisant ^a « $\pi > 1 \implies \ln(\pi) > 0$ ».

2. L'implication « $\pi < 1 \implies \ln(\pi) > 0$ » est-elle vraie? Permet-elle de démontrer « $\ln(\pi) > 0$ »?

^a. Il est entendu que cette implication est vraie

Propriété (par équivalence).

On détermine une assertion vraie \mathcal{Q} telle que « $\mathcal{P} \iff \mathcal{Q}$ » soit vraie.



Lorsque l'équivalence « $\mathcal{P} \iff \mathcal{Q}$ » est vraie, on dit que :

- \mathcal{Q} est une condition nécessaire et suffisante pour avoir \mathcal{P}
- ou encore, il faut et il suffit d'avoir \mathcal{Q} pour avoir \mathcal{P}

L'équivalence vraie « $\mathcal{P} \iff \mathcal{Q}$ » peut représenter une propriété du cours appelée *caractérisation*.

En montrant que \mathcal{Q} est vraie, on est bien certain que \mathcal{P} le soit aussi (savez-vous pourquoi?)

Cette technique est à privilégier lorsque la démonstration de \mathcal{P} n'est pas « évidente ». Elle permet en fait de transformer l'assertion à démontrer \mathcal{P} en une assertion ayant même valeur de vérité \mathcal{Q} mais plus simple à démontrer!



$\mathcal{P} \iff \mathcal{Q}$
Or \mathcal{Q}
Donc \mathcal{P}

Pour rappel, cela signifie :

$\mathcal{P} \iff \mathcal{Q}$ est vraie
Or \mathcal{Q} est vraie
Donc \mathcal{P} est vraie



Démontrer « La fonction carrée est décroissante sur $] -\infty, 0]$ » en utilisant ^a la caractérisation :

$$(x \mapsto x^2 \text{ est décroissante sur }] -\infty, 0]) \iff (\forall x \in] -\infty, 0], 2x \leq 0)$$

a. Là encore, il est entendu que cette équivalence est vraie, c'était le dernier rappel.;

Pour exploiter ces deux techniques, il faut savoir démontrer une implication et une équivalence.

Pour démontrer une implication « $\mathcal{P} \implies \mathcal{Q}$ »

Propriété (directement).

On suppose \mathcal{P} vraie, et on montre que \mathcal{Q} l'est aussi.



Supposons \mathcal{P}
Montrons \mathcal{Q}
: } Preuve de \mathcal{Q}



Étant donné un réel $x \in [0, 1]$, démontrer « $x - x^2 \in \mathbb{N} \implies x = 0$ ou $x = 1$ »

Propriété (par contraposition).

On démontre « $\text{non}(\mathcal{Q}) \implies \text{non}(\mathcal{P})$ ».



Cette technique est à privilégier lorsque $\text{non}(\mathcal{P})$ est plus facile à démontrer que \mathcal{Q}



Raisonnons par contraposition, et supposons $\text{non}(\mathcal{Q})$
Montrons $\text{non}(\mathcal{P})$
: } Preuve de $\text{non}(\mathcal{P})$



Étant donné n un entier naturel, démontrer « n^2 pair $\implies n$ pair ».

Pour démontrer une équivalence « $\mathcal{P} \iff \mathcal{Q}$ »

Propriété (directement).

On utilise une « suite d'équivalences » en modifiant peu à peu \mathcal{P} en \mathcal{Q} .



Se méfier des fausses équivalences



$\mathcal{P} \iff \dots$
 $\iff \dots$
 $\iff \mathcal{Q}$



Étant donné un réel x strictement positif, démontrer « $(x^2 - 4x + 3)(1 - \ln x) = 0 \iff x = 1$ ou $x = 3$ ou $x = e$ »

Propriété (par double implication).

On démontre « $\mathcal{P} \implies \mathcal{Q}$ » et « $\mathcal{Q} \implies \mathcal{P}$ »



Cette technique est à privilégier lorsque la méthode *directe* ne convient pas (c'est très souvent le cas)



Montrons $\mathcal{P} \implies \mathcal{Q}$:

Supposons \mathcal{P}

Montrons \mathcal{Q}

\vdots } Preuve de \mathcal{Q}

Montrons $\mathcal{Q} \implies \mathcal{P}$:

Supposons \mathcal{Q}

Montrons \mathcal{P}

\vdots } Preuve de \mathcal{P}



Étant donnés deux réels x et y , démontrer « $x^2 + y^2 = 0 \iff x = 0$ et $y = 0$ ».

Expliquons enfin comment démontrer une assertion qui commence par un quantificateur.

Pour démontrer une quantification universelle « $\forall x \in E, \mathcal{P}(x)$ »

Propriété (en introduisant une variable).

On considère un x quelconque de E que l'on fixe le temps de la preuve, et on montre que $\mathcal{P}(x)$ est vraie.



Soit $x \in E$
Montrons $\mathcal{P}(x)$
: } Preuve de $\mathcal{P}(x)$



Démontrer « $\forall x \in \mathbb{R}, \frac{x}{x^2 + 1} \leq \frac{1}{2}$ »

Pour démontrer une quantification existentielle « $\exists x \in E, \mathcal{P}(x)$ »

Propriété (de manière constructive).

On détermine (concrètement) un x qui convient.



Cette méthode permet, en particulier, de montrer qu'une quantification universelle est fausse. Le x qui convient est alors un contre-exemple!



Posons^a $x = \dots$
Vérifions $\mathcal{P}(x)$
: } Vérification de $\mathcal{P}(x)$

a. Trouver un x qui convient n'est pas toujours évident, ni même faisable



1. A-t-on « $\forall x \in \mathbb{R}, x^2 \geq x$ »?
2. Démontrer « $\forall x, y \in \mathbb{R}, \exists z \in \mathbb{R}, z > x + y$ »^a.
3. A-t-on « $\exists z \in \mathbb{R}, \forall x, y \in \mathbb{R}, z > x + y$ »?

a. Par abus, on regroupe x et y derrière le même quantificateur \forall au lieu de :

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \exists z \in \mathbb{R}, z > x + y$$

II. Ensemble

1. Définition et inclusion

Définition (ensemble).

Un ensemble est une collection d'objets appelés éléments de cet ensemble.



- Pour signifier l'appartenance (resp. la non appartenance) d'un élément x à un ensemble E , on écrit :

$$x \in E \quad (\text{resp. } x \notin E)$$

- L'ensemble ne contenant aucun élément est appelé l'ensemble vide, et est noté \emptyset
- Un ensemble ^a peut être défini :
 - en extension ^b : $E = \{1, 2, 3\}$
 - en pseudo-extension ^c : $E = \{1, 3, 5, 7, 9, \dots\}$
- Dans un ensemble :
 - il n'y a pas de doublon (deux fois le même élément)
 - l'ordre d'écriture des éléments n'a pas d'importance : $\{1, 2, 3\} = \{1, 3, 2\}$
- Même si les éléments d'un ensemble peuvent être a priori de natures différentes ^d, ça n'arrive pas en Mathématiques ^e

a. Toujours noté avec des accolades

b. Ses éléments sont explicitement décrits

c. Certains éléments sont sous-entendus et remplacés par ...

d. Ce n'est pas rare en Informatique théorique où le formalisme mathématique est d'ailleurs très présent!

e. On verra pourquoi plus tard avec la notion de structure algébrique.

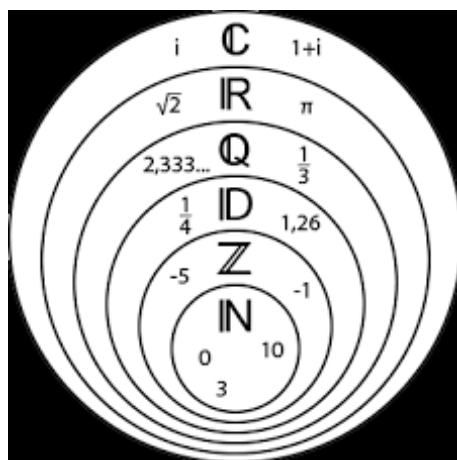
Définition (inclusion - partie).

Un ensemble F est inclus dans un ensemble E si tous les éléments de F appartiennent à E .

On notera alors $F \subset E$, et on dira que F est une partie ou un sous-ensemble de E .



Nous manipulerons des ensembles de nombres



Mais aussi des ensembles de couples, de fonctions, de suites, de matrices, ...



Point de vue logique

L'inclusion ensembliste correspond à l'implication logique :

$$(F \subset E) \iff (\forall x \in F, x \in E) \iff (x \in F \implies x \in E)$$



Pour démontrer $F \subset E$

Soit $x \in F$

Montrons $x \in E$

\vdots } Preuve de $x \in E$



Cette notion fournit une autre manière de définir un ensemble lorsqu'il s'agit d'une partie :

$$F = \{x \in E \mid \mathcal{P}(x)\}$$

Autrement dit,

$$\forall x \in E, (x \in F \iff \mathcal{P}(x))$$

Cette définition de l'ensemble F est dite en compréhension^a

a. Ses éléments ne sont pas explicitement décrits, mais sont déterminés par une condition (nécessaire et suffisante) d'appartenance



Démontrer $\{x \in \mathbb{R} \mid \exists y \in \mathbb{R}_+, x \geq y\} \subset \mathbb{R}_+$.

Définition (égalité).

Deux ensembles sont égaux s'ils possèdent exactement les mêmes éléments.



Point de vue logique

L'égalité ensembliste correspond à l'équivalence logique :

$$(E = F) \iff (x \in E \iff x \in F)$$

Propriété (double inclusion).

$$(E = F) \iff (E \subset F \text{ et } F \subset E)$$



Cette *caractérisation* fournit une méthode pour démontrer l'égalité entre deux ensembles



Démontrer $\{x \in \mathbb{R} \mid \forall y \in \mathbb{R}_+, x \leq y\} = \mathbb{R}_-$.



Raisonnement par analyse-synthèse

Résoudre dans \mathbb{R} l'équation $x = \sqrt{4x+5}$, autrement dit déterminer l'ensemble des solutions :

$$\mathcal{S} = \{x \in \mathbb{R} \mid x = \sqrt{4x+5}\}$$

D'abord (analyse), on recherche tous les candidats possibles de sorte que $\mathcal{S} \subset \{\text{candidats possibles}\}$.

Ensuite (synthèse), on ne garde que les candidats qui conviennent de sorte que $\mathcal{S} = \{\text{candidats qui conviennent}\}$.

Pour un modèle de rédaction, on pourra se reporter à la démonstration de l'unicité puis de l'existence.

2. Opérations sur les parties d'un ensemble

On considère A , B et C trois parties d'un ensemble E .

Définition (ensemble des parties).

L'ensemble des parties de E , noté $\mathcal{P}(E)$, est constitué^a de toutes les parties de E .

^a. Comme son nom l'indique!



- Comme $A \subset E$, il est évident que $A \in \mathcal{P}(E)$
- Nous allons donc définir ci-dessous des opérations agissant sur les éléments de $\mathcal{P}(E)$



Déterminer $\mathcal{P}(E)$ dans chacun des cas suivants :

1. $E = \{1, 2\}$
2. $E = \{1, 2, 3\}$
3. $E = \{1\}$
4. $E = \emptyset$
5. $E = \mathcal{P}(\{1\})$

Définition (complémentaire).

Le complémentaire de A (dans E) est l'ensemble défini par :

$$\bar{A} = \{x \in E \mid x \notin A\}$$



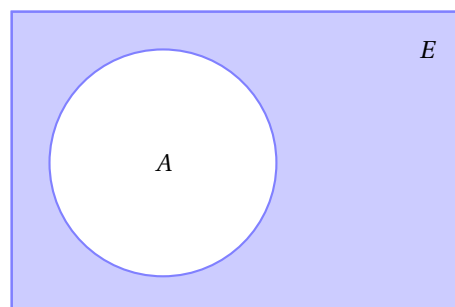
Point de vue logique

La complémentarité ensembliste correspond à la négation logique :

$$\forall x \in E, (x \in \bar{A} \iff x \notin A \iff \text{non}(x \in A))$$



Diagramme de Venn



Définition (intersection).

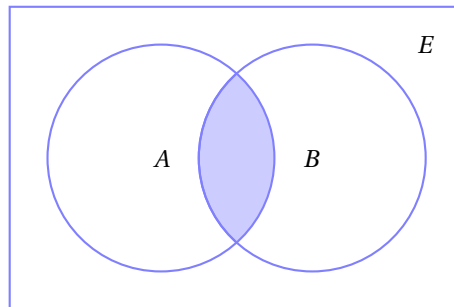
L'intersection de A et B est l'ensemble défini par :

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

Point de vue logique

L'intersection ensembliste correspond à la conjonction logique :

$$\forall x \in E, (x \in A \cap B \iff x \in A \text{ et } x \in B)$$

Diagramme de Venn

Si $A \cap B = \emptyset$, on dit que A et B sont disjoints

Définition (union).

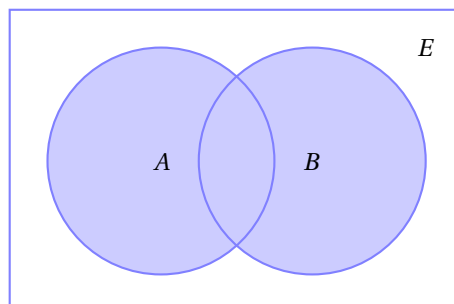
L'union de A et B est l'ensemble défini par :

$$A \cup B = \{x \in E \mid x \in A \text{ ou } x \in B\}$$

Point de vue logique

L'union ensembliste correspond à la disjonction logique :

$$\forall x \in E, (x \in A \cup B \iff x \in A \text{ ou } x \in B)$$

Diagramme de Venn

3. Règles opératoires

On considère encore A , B et C trois parties d'un ensemble E .

Par négation, conjonction et disjonction, on vérifie les propriétés suivantes :

Propriété (idempotence).

- $A \cap A = A$
- $A \cup A = A$

Propriété (commutativité).

- $A \cap B = B \cap A$
- $A \cup B = B \cup A$

Propriété (associativité).

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



On peut alors supprimer les parenthèses lorsqu'il n'y a que des intersections (resp. unions)

Propriété (distributivité).

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



Même s'il existe des règles de priorités (d'abord complémentarité, puis intersection, et enfin union), on évitera de supprimer les parenthèses lorsqu'il y a différentes opérations

Propriété (lois de Morgan).

- $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Propriété (neutralité).

- $A \cap E = A$
- $A \cup \emptyset = A$

4. Deux autres opérations sur les parties d'un ensemble : la différence et la différence symétrique

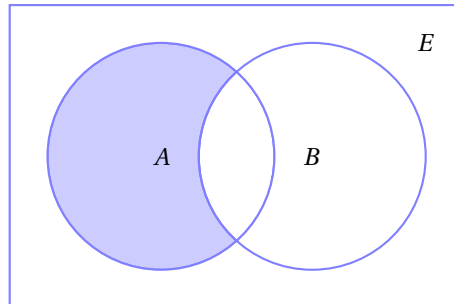
On considère A et B deux parties d'un ensemble E .

Définition (différence).

La différence de A et B est l'ensemble défini par :

$$A \setminus B = A \cap \bar{B}$$

Diagramme de Venn

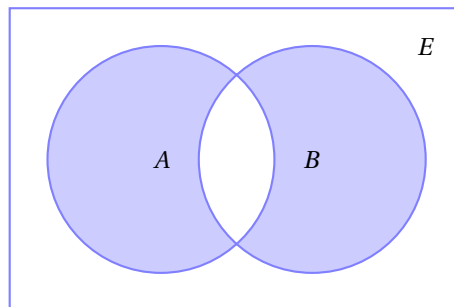


Définition (différence symétrique).

La différence symétrique de A et B est l'ensemble défini par :

$$A \Delta B = (A \cup B) \setminus (A \cap B)$$

Diagramme de Venn



1. Montrer $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
2. Montrer $A \setminus B = C \implies A \cup B = B \cup C$

5. Produit cartésien

Définition (produit cartésien).

Le produit cartésien de deux ensembles E et F est l'ensemble défini par :

$$E \times F = \{(x, y) \mid x \in E \text{ et } y \in F\}$$

Un élément (x, y) d'un tel ensemble est appelé couple et vérifie :

$$(x, y) = (x', y') \iff x = x' \text{ et } y = y'$$



- Si $E = F$, on note plus légèrement E^2 au lieu de $E \times E$
- Le produit cartésien de trois ensembles E, F et G est défini par :

$$E \times F \times G = (E \times F) \times G$$

Ses éléments se nomment des triplets et se visualisent sous la forme (x, y, z) avec x dans E , y dans F et z dans G

- Plus généralement, on définit par récurrence le produit cartésien de $n \geq 3$ ensembles E_1, E_2, \dots, E_n :

$$E_1 \times \dots \times E_{n-1} \times E_n = (E_1 \times \dots \times E_{n-1}) \times E_n$$

Ses éléments se nomment des n -uplets et se visualisent sous la forme (x_1, x_2, \dots, x_n) avec x_i dans E_i



Au niveau des BDD

On considère le contenu d'une table de colonnes C_1, C_2, \dots, C_n à un instant donné.

Une ligne peut être modélisée par un n -uplet (x_1, x_2, \dots, x_n) .

L'ensemble des lignes apparaît alors comme une partie du produit cartésien $E_1 \times E_2 \times \dots \times E_n$ où E_i désigne le domaine de C_i c'est à dire l'ensemble des valeurs possibles, a priori, pour un élément x_i de C_i .

III. Relation binaire de E vers F

On considère E, F et G des ensembles.

1. Définition et représentations

Définition (relation binaire de E vers F).

Une relation binaire de E vers F est un triplet $\mathcal{R} = (E, F, U)$ où U désigne une partie de $E \times F$.



- E est appelé l'ensemble de départ et F celui d'arrivée
- Par abus ^a, on dit qu'une relation binaire de E vers F est (tout simplement) une partie de $E \times F$ (le U de la définition)
- Pour définir une telle relation, on note :

$$\forall x \in E, \forall y \in F, x \mathcal{R} y \iff (x, y) \in U$$

$x \mathcal{R} y$ se lit « x est en relation avec y »

- Lorsque x n'est pas en relation avec y , on note : $x \not\mathcal{R} y$

a. lorsqu'il n'y a pas d'ambiguïté sur E et F



Diagramme sagittal

On considère la relation binaire $\mathcal{R} = (E, F, U)$ avec $E = \{a, b, c, d\}$, $F = \{1, 2, 3, 4\}$ et $U = \{(a, 1), (a, 2), (b, 3), (c, 2)\}$.

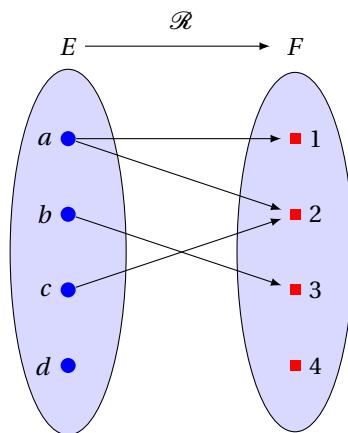
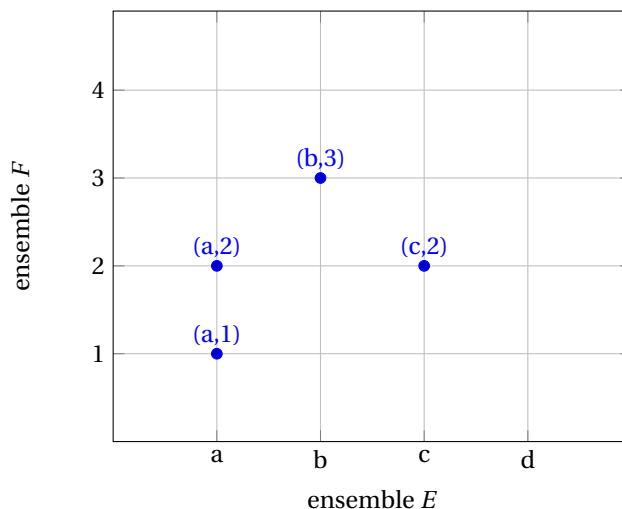


Diagramme cartésien

On considère encore la relation binaire $\mathcal{R} = (E, F, U)$ avec $E = \{a, b, c, d\}$, $F = \{1, 2, 3, 4\}$ et $U = \{(a, 1), (a, 2), (b, 3), (c, 2)\}$.

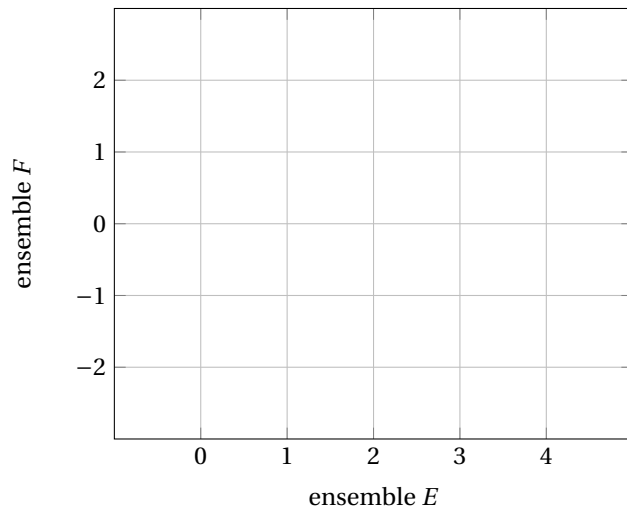
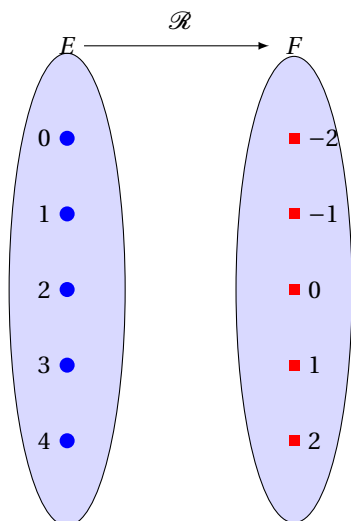




On considère $E = \{0, 1, 2, 3, 4\}$, $F = \{-2, -1, 0, 1, 2\}$ et \mathcal{R} la relation binaire de E vers F définie par :

$$\forall x \in E, \forall y \in F, x \mathcal{R} y \iff x = y^2$$

Compléter les diagrammes ci-dessous :



2. Fonction et application

Définition (fonction).

Une fonction est une relation binaire où tout élément au départ est en relation avec au plus un élément à l'arrivée.



On considère encore $E = \{0, 1, 2, 3, 4\}$, $F = \{-2, -1, 0, 1, 2\}$ et \mathcal{R} la relation binaire de E vers F définie par :

$$\forall x \in E, \forall y \in F, x \mathcal{R} y \iff x = y^2$$

1. \mathcal{R} est-elle une fonction de E vers F ?
2. A partir de \mathcal{R} , on peut définir une nouvelle relation de F vers E appelée « relation réciproque de \mathcal{R} », et notée \mathcal{R}^{-1} :

$$\forall y \in F, \forall x \in E, y \mathcal{R}^{-1} x \iff x \mathcal{R} y$$

- (a) Représenter le diagramme sagittal de \mathcal{R}^{-1} .
- (b) \mathcal{R}^{-1} est-elle une fonction de F vers E ?
- (c) A quelle condition une relation réciproque est-elle une fonction?



- Une fonction se note en général f plutôt que \mathcal{R} , et on écrit $y = f(x)$ plutôt que $x \mathcal{R} y$
- Lorsque $y = f(x)$, on dit que :
 - y est l'image de x par f ou encore y est la valeur de f en x
 - x est un antécédent de y par f
- En fait, une fonction f de E vers F se note :

$$\begin{aligned} f: E &\longrightarrow F \\ x &\longmapsto f(x) \end{aligned}$$

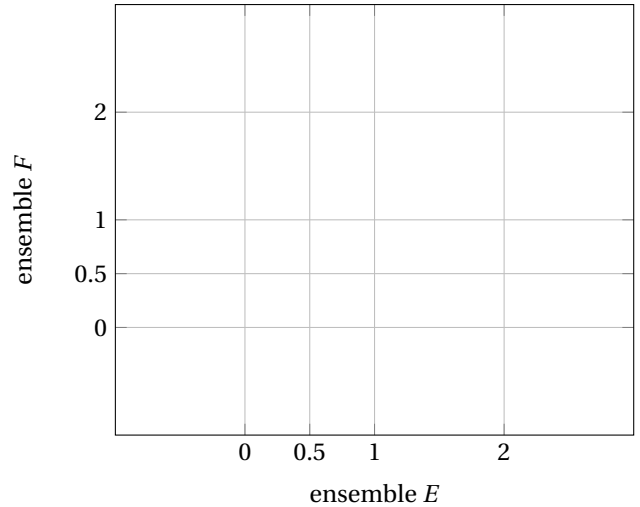
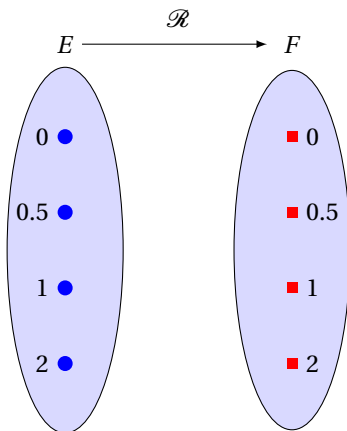
- En Mathématiques, il est commun de définir une fonction f en donnant l'expression permettant de « calculer » $f(x)$



On considère $E = F = \{0, 0.5, 1, 2\}$ et f la fonction définie par :

$$\begin{aligned} f: E &\longrightarrow F \\ x &\longmapsto \frac{1}{x} \end{aligned}$$

1. Est-il toujours possible de « calculer » $f(x)$?
2. Compléter les diagrammes suivants.



Définition (ensemble de définition).

L'ensemble de définition d'une fonction f de E vers F est constitué des éléments au départ possédant une image :

$$\mathcal{D}_f = \{x \in E \mid f(x) \text{ existe}\}$$

Définition (application).

Une application est une fonction où tout élément au départ possède une image.



- Une application désigne en fait une fonction où l'ensemble de définition est l'ensemble de départ tout entier
- En Mathématiques, on ne s'intéresse qu'aux applications^a
- En Informatique, on parle de « fonction totale » plutôt que d'application, et de « fonction partielle » plutôt que de fonction. Cette dernière notion y est d'ailleurs très présente : un programme définit en général une « fonction partielle » car on ne peut pas limiter le domaine du paramètre en entrée (excepté son type éventuellement), ce qui ne doit pas l'empêcher de respecter la spécification qui peut, quant à elle, limiter le domaine du paramètre en entrée.
- En BDD, une clé étrangère traduit une relation fonctionnelle de la table contenant la clé vers la table référencée par la clé. Avec une contrainte d'existence sur la clé (valeur NULL non autorisée), cette fonction devient une application.

a. Dans l'étude d'une fonction, on commence toujours par déterminer son ensemble de définition pour s'y restreindre!

Définition (injection).

Une application de E vers F est injective si tout élément à l'arrivée admet au plus un antécédent, autrement dit si deux éléments différents au départ ont des images différentes :

$$\forall x, x' \in E, x \neq x' \implies f(x) \neq f(x')$$



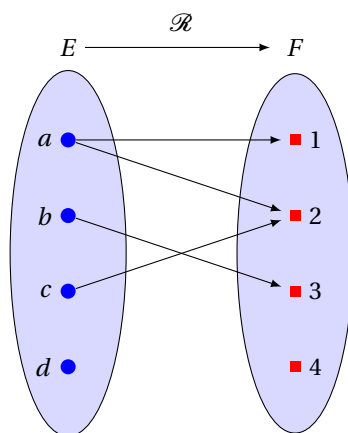
- Pour démontrer l'injectivité d'une application, on préfère la contraposée :

$$\forall x, x' \in E, f(x) = f(x') \implies x = x'$$

- Une application est injective si elle ne prend jamais deux fois la même valeur



Revenons sur notre première relation :



1. \mathcal{R} est-elle une fonction?
2. **On retire de \mathcal{R} le couple $(a, 1)$.**
 - (a) Obtient-on une fonction?
 - (b) Obtient-on une application?
 - (c) **On retire de E l'élément d .**
 - i. Obtient-on une application?
 - ii. Est-elle injective?
 - iii. La relation réciproque est-elle une fonction?
3. **On retire^a de \mathcal{R} le couple $(a, 2)$.**
 - (a) Obtient-on une fonction?
 - (b) Obtient-on une application?
 - (c) **On retire de E l'élément d .**
 - i. Obtient-on une application?
 - ii. Est-elle injective?
 - iii. La relation réciproque est-elle une fonction?
 - iv. La relation réciproque est-elle une application?
 - v. A quelle condition la relation réciproque serait-elle une application?

^a. Les modifications réalisées dans la question 2. ne sont évidemment plus valables

Définition (surjection).

Une application de E vers F est surjective si tout élément à l'arrivée possède au moins un antécédent :

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



Une application est surjective si elle prend toutes les valeurs à l'arrivée

Définition (bijection).

Une application de E vers F est bijective si tout élément à l'arrivée possède exactement un antécédent :

$$\forall y \in F, \exists ! x \in E, y = f(x)$$



| Une application est bijective si elle prend toutes les valeurs à l'arrivée une fois et une seule

Définition (application réciproque d'une bijection).

Lorsqu'une application f de E vers F est bijective, on peut définir son application réciproque par :

$$\begin{aligned} f^{-1}: F &\longrightarrow E \\ y &\longmapsto x \text{ tel que } y = f(x) \end{aligned}$$



- L'image de y par f^{-1} est son unique antécédent par f
- Cette application f^{-1} est également bijective et $(f^{-1})^{-1} = f$
- Cette définition coïncide avec celle de relation réciproque



| Contrairement à \mathcal{R}^{-1} qui est toujours bien définie, f^{-1} n'existe pas si f n'est pas une application bijective



On considère l'application f définie par :

$$\begin{aligned} f: \mathbb{N} &\longrightarrow \mathbb{N}^* \\ n &\longmapsto n+1 \end{aligned}$$

Montrer que f est bijective et préciser f^{-1} .

Propriété (caractérisation d'une bijection).

Une application de E vers F est bijective si et seulement si elle est injective et surjective.

Définition (composition).

Étant données deux applications $f: E \rightarrow F$ et $g: F \rightarrow G$, la composée de g par f est l'application définie par :

$$\begin{aligned} g \circ f: E &\longrightarrow G \\ x &\longmapsto g(f(x)) \end{aligned}$$



| La composition est associative, mais pas commutative

Propriété (autre caractérisation d'une bijection).

Une application $f : E \rightarrow F$ est bijective si et seulement s'il existe une application $g : F \rightarrow E$ telle que :

$$g \circ f = Id_E \quad \text{et} \quad f \circ g = Id_F$$

Dans ce cas, g est l'application réciproque de f .



Id_E est l'application « identité sur E » définie par :

$$Id_E : E \longrightarrow E \\ x \longmapsto x$$



Les deux égalités sont nécessaires (cf. exercice suivant)



On considère f et g les applications définies par :

$$f : \mathbb{N} \longrightarrow \mathbb{N} \quad \text{et} \quad g : \mathbb{N} \longrightarrow \mathbb{N} \\ k \longmapsto 2k \qquad \qquad \qquad k \longmapsto \begin{cases} k/2 & \text{si } k \text{ est pair} \\ (k-1)/2 & \text{si } k \text{ est impair} \end{cases}$$

1. Montrer que f est injective mais pas surjective.
2. Montrer que g est surjective mais pas injective.
3. Montrer que $g \circ f = Id_{\mathbb{N}}$ mais $f \circ g \neq Id_{\mathbb{N}}$

3. Image directe et image réciproque

On considère une application $f : E \rightarrow F$.

Définition (image directe).

L'image directe de $A \subset E$ par f est la partie de F définie par :

$$f(A) = \{y \in F \mid \exists x \in A, y = f(x)\} = \{f(x) \mid x \in A\}$$



- $f(A)$ est l'ensemble des images des éléments de A
- En particulier, $f(E)$ qui désigne l'ensemble des valeurs prises par f est appelée « l'image de f » et notée $Im(f)$
- L'application $f : E \rightarrow F$ est surjective si et seulement si $Im(f) = F$
- En restreignant l'ensemble d'arrivée d'une application à son image, on peut toujours la rendre surjective

Définition (image réciproque).

L'image réciproque de $B \subset F$ par f est la partie de E définie par :

$$f^{-1}(B) = \{x \in E \mid f(x) \in B\}$$



- $f^{-1}(B)$ est l'ensemble des antécédents des éléments de B
- Cette notation ne présume pas de l'existence de f^{-1} autrement dit $f^{-1}(B)$ existe même si f n'est pas bijective
- Heureusement, si f est bijective, l'image réciproque de B par f coïncide avec l'image directe de B par f^{-1}



On considère l'application f définie par :

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

$$x \longmapsto x^2$$

1. Déterminer $Im(f)$, $f([-1, 2])$ et $f^{-1}([1, 4])$
2. f est-elle surjective? f est-elle injective?
3. Montrer la bijectivité de l'application \tilde{f} , induite^a par f , définie par :

$$\tilde{f}: \mathbb{R}_+ \longrightarrow \mathbb{R}_+$$

$$x \longmapsto x^2$$

Préciser l'application réciproque de \tilde{f} .

4. Déterminer $(\tilde{f})^{-1}([4, 9])$

a. La « formule » ne change pas, seuls les ensembles de départ et d'arrivée sont modifiés

4. Dénombrement (hors programme)

La notion de cardinal

Définition (ensemble fini - cardinal).

L'ensemble E est fini s'il est en bijection avec l'ensemble^a $\{1, \dots, n\}$ pour une certaine valeur de $n \in \mathbb{N}$.
Ce naturel n est alors unique, il s'appelle le cardinal de E et se note $Card(E)$.

a. Par convention, on considère que $\{1, \dots, 0\} = \emptyset$



- L'ensemble $\{1, \dots, n\}$ est aussi désigné par $[[1, n]]$
- En notant $\varphi: [[1, n]] \rightarrow E$ une telle bijection, et en posant $x_i = \varphi(i)$, on obtient une « description » de E :

$$E = \{x_1, \dots, x_n\}$$

- Lorsque E n'est pas fini, on dit qu'il est infini^a, et on note $Card(E) = +\infty$

a. Parmi les ensembles infinis, ceux qui sont en bijection avec \mathbb{N} sont appelés les ensembles dénombrables.
Une telle bijection fournit alors une « description » de la forme :

$$E = \{x_0, x_1, x_2, \dots\}$$

Propriété (cardinal d'une union).

Soit A, B deux parties de E .

Si A et B sont finies, alors $A \cup B$ et $A \cap B$ le sont aussi, et on a :

$$Card(A \cup B) = Card(A) + Card(B) - Card(A \cap B)$$



- Sans déterminer $A \cap B$, on peut toujours affirmer :

$$\text{Card}(A \cup B) \leq \text{Card}(A) + \text{Card}(B)$$

- Si A et B sont disjointes, on a évidemment :

$$\text{Card}(A \cup B) = \text{Card}(A) + \text{Card}(B)$$

- En particulier, avec $B = \overline{A}$, il vient :

$$\text{Card}(E) = \text{Card}(A) + \text{Card}(\overline{A})$$

Propriété (cardinal d'une partie).

Soit A une partie de E .

Si E est fini, alors A l'est aussi et $\text{Card}(A) \leq \text{Card}(E)$.

De plus, $A = E$ si et seulement si $\text{Card}(A) = \text{Card}(E)$.

Propriété (condition nécessaire de bijectivité).

Soit $f : E \rightarrow F$ une application.

- Si f est injective et F fini, alors E l'est aussi et $\text{Card}(E) \leq \text{Card}(F)$
- Si f est surjective et E fini, alors F l'est aussi et $\text{Card}(E) \geq \text{Card}(F)$
- Si f est bijective et l'un des ensembles (E ou F) fini, alors l'autre l'est aussi et $\text{Card}(E) = \text{Card}(F)$



Pour qu'une application entre deux ensembles finis soit bijective, il faut qu'ils aient le même cardinal. Cette condition n'est pas suffisante^a, mais lorsqu'elle est remplie, on dispose d'une caractérisation « efficace » de la bijectivité.

a. Savez-vous le prouver?

Propriété (caractérisation « efficace » d'une bijection).

Soit $f : E \rightarrow F$ une application avec $\text{Card}(E) = \text{Card}(F) < +\infty$. Alors, on a :

$$f \text{ bijective} \iff f \text{ injective} \iff f \text{ surjective}$$

Cardinaux usuels

Propriété (cardinal du produit cartésien).

Si E et F sont finis, alors $E \times F$ l'est aussi et $\text{Card}(E \times F) = \text{Card}(E) \times \text{Card}(F)$.

Propriété (cardinal de l'ensemble des parties).

Si E est fini, alors l'ensemble $\mathcal{P}(E)$ de ses parties l'est aussi et $\text{Card}(\mathcal{P}(E)) = 2^{\text{Card}(E)}$



Démontrer cette propriété en identifiant une partie de E à un mot binaire de longueur $\text{Card}(E)$.

On considère un ensemble E de cardinal n et un entier p inférieur (ou égal) à n .

Définition (p -liste).

Une p -liste formée d'éléments de E est un choix ordonné de p éléments de E avec répétition possible :

$$(x_1, \dots, x_p) \quad \text{avec } x_i \in E$$



Une telle p -liste s'identifie à une application de $\llbracket 1, p \rrbracket$ vers E , x_i désignant l'image de l'entier i .
Compter le nombre d'applications de $\llbracket 1, p \rrbracket$ vers E revient donc à compter le nombre de p -listes.

Propriété (nombre de p -listes).

Le nombre de p -listes formées d'éléments de E est n^p .

Définition (p -arrangement).

Un p -arrangement formé d'éléments de E est un choix ordonné de p éléments de E sans répétition possible :

$$(x_1, \dots, x_p) \quad \text{avec } x_i \in E \quad \text{et} \quad i \neq j \Rightarrow x_i \neq x_j$$



Un tel p -arrangement s'identifie à une injection de $\llbracket 1, p \rrbracket$ vers E , x_i désignant l'image de l'entier i .
Compter le nombre d'injections de $\llbracket 1, p \rrbracket$ vers E revient donc à compter le nombre de p -arrangements.

Propriété (nombre de p -arrangements).

Le nombre de p -arrangements formés d'éléments de E est $n \times (n-1) \times \dots \times (n-p+1)$.

Définition (permutation).

Une permutation de E est un n -arrangement formé d'éléments de E .



Une telle permutation s'identifie à une bijection de $\llbracket 1, n \rrbracket$ vers E , x_i désignant l'image de l'entier i .
Compter le nombre de bijections de $\llbracket 1, n \rrbracket$ vers E revient donc à compter le nombre de permutations.

Propriété (nombre de permutations).

Le nombre de permutations de E est $n \times (n-1) \times \dots \times 2 \times 1 = n!$

Définition (p -combinaison).

Une p -combinaison formée d'éléments de E est un choix non ordonné de p éléments de E sans répétition possible :

$$\{x_1, \dots, x_p\} \quad \text{avec } x_i \in E \quad \text{et} \quad i \neq j \Rightarrow x_i \neq x_j$$



Une telle p -combinaison s'identifie à une partie de E à p éléments.
Compter le nombre de parties de E à p éléments revient donc à compter le nombre de p -combinaisons.

Propriété (nombre de p -combinaisons).

Le nombre de p -combinaisons formées d'éléments de E est :

$$\frac{n \times (n-1) \times \cdots \times (n-p+1)}{p!} = \frac{n!}{p!(n-p)!} = \binom{n}{p}$$



On considère l'alphabet $\Sigma = \{a, b, c, d\}$.

1. Combien de mots de longueur 3 est-il possible de construire?
2. Combien de mots de longueur 3, avec des lettres toutes distinctes, est-il possible de construire?
3. Combien de mots de longueur 3, avec des lettres toutes distinctes et sans d , est-il possible de construire?
4. Combien de mots de longueur 3, avec des lettres toutes distinctes, est-il possible de construire, à une permutation près des lettres?

IV. Relation binaire sur E

On considère E un ensemble.

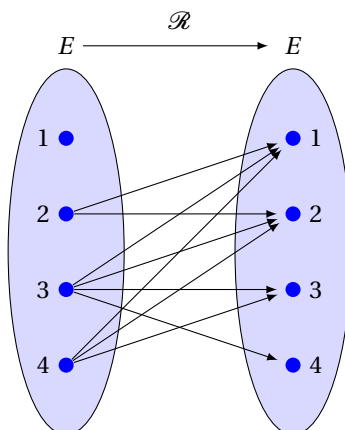
1. Définition et propriétés

Définition (relation binaire sur E).

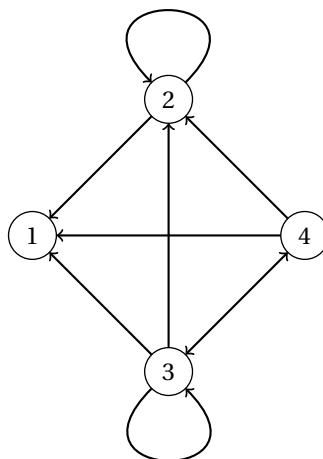
Une relation binaire sur E est une relation binaire de E vers E .

Diagramme sagittal

On considère la relation binaire sur $E = \{1, 2, 3, 4\}$ définie par $U = \{(2, 1), (2, 2), (3, 1), (3, 2), (3, 3), (3, 4), (4, 1), (4, 2), (4, 3)\}$.



Lorsque les ensembles au départ et à l'arrivée coïncident, on préfère la représentation sous forme de « graphe ^a » :



^a. On y reviendra dans un prochain module, mais on peut déjà parler de sommets pour les éléments de E et d'arcs pour les couples de U

Dans la suite de cette section 1, \mathcal{R} désigne une relation binaire sur E .

Définition (réflexivité, symétrie, antisymétrie et transitivité).

- \mathcal{R} est réflexive lorsque : $\forall x \in E, x \mathcal{R} x$
- \mathcal{R} est symétrique lorsque : $\forall x, y \in E, x \mathcal{R} y \implies y \mathcal{R} x$
- \mathcal{R} est antisymétrique lorsque : $\forall x, y \in E, (x \mathcal{R} y \text{ et } y \mathcal{R} x) \implies x = y$
- \mathcal{R} est transitive lorsque : $\forall x, y, z \in E, (x \mathcal{R} y \text{ et } y \mathcal{R} z) \implies x \mathcal{R} z$



Seule l'égalité vérifie ces quatre propriétés

Propriété (caractérisation par le « graphe »).

- \mathcal{R} est réflexive si et seulement si chaque sommet possède une boucle
- \mathcal{R} est symétrique si et seulement si chaque arc est à double sens
- \mathcal{R} est antisymétrique si et seulement si aucun arc n'est à double sens (excepté les boucles éventuelles)
- \mathcal{R} est transitive si et seulement si pour chaque couple d'arcs adjacents, le « raccourci » est un arc du graphe



L'antisymétrie n'est pas la négation de la symétrie.

- Donner un exemple de relation symétrique et antisymétrique
- Donner un exemple de relation ni symétrique, ni antisymétrique



Modifier (le moins possible) la relation \mathcal{R} du début pour qu'elle soit (chaque cas est indépendant) :

- réflexive
- symétrique
- antisymétrique
- transitive

2. Une relation qui permet de « classifier » : la relation d'équivalence

Définition (relation d'équivalence).

Une relation d'équivalence est une relation binaire réflexive, symétrique et transitive.



- Si \mathcal{R} est une relation d'équivalence, on note souvent $x \sim y$ plutôt que $x \mathcal{R} y$
- Si $x \sim y$, on dit que x et y sont « équivalents »
- Une relation d'équivalence se comprend souvent comme une égalité « modulo » certains critères. En réunissant entre eux les éléments équivalents, on définit le concept suivant.

Dans la suite de cette section 2, \sim désigne une relation d'équivalence sur E .

Définition (classe d'équivalence).

La classe d'équivalence d'un élément $x \in E$ est l'ensemble des éléments de E équivalents à x :

$$Cl(x) = \{y \in E \mid y \sim x\}$$



L'élément « privilégié » x qui permet de désigner sa classe d'équivalence est appelé un représentant de cette classe.

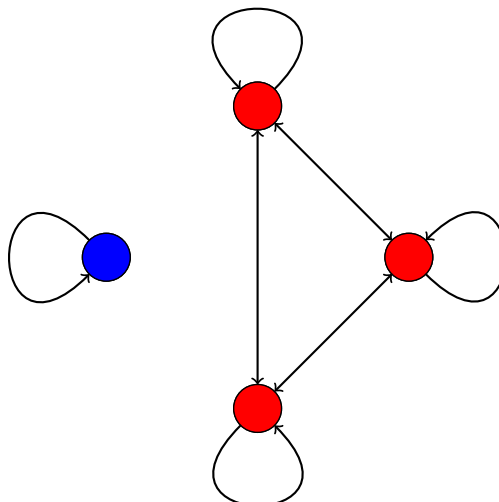
Propriété (partition).

Les classes d'équivalence forment une partition^a de E .

^a. Elles sont non vides, disjointes deux à deux et leur union est égale à E



Voici une relation d'équivalence et sa partition :



On considère la relation binaire sur \mathbb{Z} définie par :

$$\forall m, n \in \mathbb{Z}, m \mathcal{R} n \iff \exists k \in \mathbb{Z}, m - n = 3k$$

Montrer que \mathcal{R} est une relation d'équivalence ^a.

On note $\mathbb{Z}/3\mathbb{Z}$ l'ensemble des classes d'équivalence ^b :

$$\mathbb{Z}/3\mathbb{Z} = \{Cl(0), Cl(1), Cl(2)\} = \{\bar{0}, \bar{1}, \bar{2}\}$$

^a. Il s'agit de la congruence modulo 3 que l'on note souvent : $m \equiv n \pmod{3}$

^b. On choisit souvent le reste dans la division euclidienne par 3 comme représentant

3. Une relation qui permet de « comparer » : la relation d'ordre

Définition (relation d'ordre).

Une relation d'ordre est une relation binaire réflexive, antisymétrique et transitive.



- La relation \leq d'infériorité (au sens large) sur un ensemble de nombres est une relation d'ordre
- Si \mathcal{R} est une relation d'ordre, on note souvent $x \leq y$ plutôt que $x \mathcal{R} y$
- Si $x \leq y$, on dit que x est « plus petit que » y ou que y est « plus grand que » x

Définition (diagramme de Hasse).

Un diagramme de Hasse est un « graphe allégé » spécifique aux relations d'ordre :

- les sommets sont positionnés du plus petit au plus grand ^a
- les boucles sont omises (sous-entendues par réflexivité)
- les raccourcis sont omis (sous-entendus par transitivité)

^a. de la gauche vers la droite ou de bas en haut



On considère $E = \{a, b, c\}$ et \mathcal{R} la relation binaire sur $\mathcal{P}(E)$ définie par :

$$\forall A, B \in \mathcal{P}(E), A \mathcal{R} B \iff A \subset B$$

1. Montrer que \mathcal{R} est une relation d'ordre.
2. Représenter son diagramme de Hasse (de bas en haut).

Dans la suite de cette section 3, \leq désigne une relation d'ordre sur E ^[1].

Définition (ordre total/partiel).

L'ordre est total si tous les éléments de E sont « comparables » deux à deux :

$$\forall x, y \in E, x \leq y \text{ ou } y \leq x$$

Sinon, l'ordre n'est que partiel.



- La relation \leq d'infériorité (au sens large) sur un ensemble de nombres est un ordre total
- La relation \subset d'inclusion (au sens large) sur $\mathcal{P}(E)$ n'est qu'un ordre partiel

On considère enfin une partie A de E .

Définition (maximum).

S'il existe, le maximum de A est l'élément de A plus grand que tous les autres :

$$\max(A) \in A \text{ et } \forall x \in A, x \leq \max(A)$$



- On parle aussi du plus grand élément de A
- On définit de manière analogue, s'il existe, le minimum (ou le plus petit élément) de A que l'on note $\min(A)$
- un extremum est un maximum ou un minimum



I Démontrer l'unicité du maximum de A .

Définition (majorant).

Un élément $M \in E$ est un majorant de A s'il est plus grand que tous les éléments de A :

$$\forall x \in A, x \leq M$$



- On définit de manière analogue un minorant de A
- S'il existe, le maximum de A est un majorant de A

[1]. On dit alors que E est ordonné

Définition (borne supérieure).

Si elle existe^a, la borne supérieure de A est le plus petit des majorants de A :

$$\sup(A) = \min \left(\{M \in E \mid \forall x \in A, x \leq M\} \right)$$

a. Elle est définie comme le minimum d'une partie



- On définit de manière analogue, si elle existe, la borne inférieure de A que l'on note $\inf(A)$
- Si le maximum de A existe, la borne supérieure de A aussi et les deux coïncident
- Si la borne supérieure de A existe et si elle est dans A , le maximum de A existe aussi et les deux coïncident

Définition (élément maximal).

Un élément $M' \in A$ est maximal dans A s'il n'existe pas d'élément dans A plus grand que lui :

$$\forall x \in A, M' \leq x \implies x = M'$$



- On définit de manière analogue un élément minimal dans A
- S'il existe, le maximum de A est maximal dans A
- Lorsque l'ordre est total, un élément maximal dans A est le maximum de A



On reprend la relation d'inclusion sur $\mathcal{P}(E)$ avec $E = \{a, b, c\}$.

1. L'ensemble $\mathcal{P}(E)$ admet-il un maximum (resp. minimum)?
2. On considère $A = \mathcal{P}(E) \setminus \{E\}$.
 - (a) La partie A admet-elle un minimum?
 - (b) La partie A admet-elle un maximum?
 - (c) La partie A admet-elle une borne supérieure?
 - (d) La partie A admet-elle des éléments maximaux?
3. On considère $B = \{\emptyset, \{a\}, \{b\}\}$.
 - (a) La partie B admet-elle un minimum?
 - (b) La partie B admet-elle un maximum?
 - (c) La partie B admet-elle une borne supérieure?
 - (d) La partie B admet-elle des éléments maximaux?

Annexe - Raisonnements et démonstrations

Pour démontrer une assertion \mathcal{P} c'est à dire montrer que \mathcal{P} est vraie

Propriété (par déduction).

On détermine une assertion vraie \mathcal{Q} telle que « $\mathcal{Q} \implies \mathcal{P}$ » soit vraie.



Lorsque l'implication « $\mathcal{Q} \implies \mathcal{P}$ » est vraie, on dit que :

- \mathcal{Q} est une condition suffisante pour avoir \mathcal{P}
- ou encore, il suffit d'avoir \mathcal{Q} pour avoir \mathcal{P}

Mais, on dit aussi que :

- \mathcal{P} est une condition nécessaire pour avoir \mathcal{Q}
- ou encore, il faut avoir \mathcal{P} pour avoir \mathcal{Q}

L'implication vraie « $\mathcal{Q} \implies \mathcal{P}$ » peut représenter une propriété du cours exprimée sous la forme « Si \mathcal{Q} , alors \mathcal{P} ».

En montrant que l'*hypothèse* \mathcal{Q} est vraie, on est bien certain que la *conclusion* \mathcal{P} le soit aussi (savez-vous pourquoi?)

On pourra évidemment utiliser un « enchaînement d'implications ».



Ne surtout pas utiliser le connecteur logique « \implies » à la place du mot « donc » dans une démonstration par déduction. En général, on évitera de mélanger dans une même phrase le langage mathématique et le langage commun.



\mathcal{Q} est vraie
Or $\mathcal{Q} \implies \mathcal{P}$ est vraie
Donc \mathcal{P} est vraie

Plus simplement ^a, on écrira :

\mathcal{Q}
Or $\mathcal{Q} \implies \mathcal{P}$
Donc \mathcal{P}

^a. En logique, on doit toujours préciser la valeur de vérité d'une assertion (elle peut être soit vraie, soit fausse). En Mathématiques, lorsque l'on écrit une assertion sans préciser sa valeur de vérité, c'est qu'elle est vraie! Par exemple, on n'écrit pas « $\forall x \in \mathbb{R}, e^x > 0$ est vraie », mais simplement « $\forall x \in \mathbb{R}, e^x > 0$ ». **Dès à présent, sauf dans les explications des raisonnements logiques qui suivent (pour un maximum de clarté), on préférera ce langage simplifié.**



1. Démontrer « $\ln(\pi) > 0$ » en utilisant ^a « $\pi > 1 \implies \ln(\pi) > 0$ ».
2. L'implication « $\pi < 1 \implies \ln(\pi) > 0$ » est-elle vraie? Permet-elle de démontrer « $\ln(\pi) > 0$ »?

^a. Il est entendu que cette implication est vraie

Propriété (par équivalence).

On détermine une assertion vraie \mathcal{Q} telle que « $\mathcal{P} \iff \mathcal{Q}$ » soit vraie.

[2]. Cette présentation est inspirée de l'excellent document, rédigé par Christophe Bertault, disponible [ici](#)

[3]. Vous profiterez également de la lecture du [Petit manuel de bonne rédaction](#), écrit par le même auteur



Lorsque l'équivalence « $\mathcal{P} \iff \mathcal{Q}$ » est vraie, on dit que :

- \mathcal{Q} est une condition nécessaire et suffisante pour avoir \mathcal{P}
- ou encore, il faut et il suffit d'avoir \mathcal{Q} pour avoir \mathcal{P}

L'équivalence vraie « $\mathcal{P} \iff \mathcal{Q}$ » peut représenter une propriété du cours appelée *caractérisation*.

En montrant que \mathcal{Q} est vraie, on est bien certain que \mathcal{P} le soit aussi (savez-vous pourquoi?)

Cette technique est à privilégier lorsque la démonstration de \mathcal{P} n'est pas « évidente ». Elle permet en fait de transformer l'assertion à démontrer \mathcal{P} en une assertion ayant même valeur de vérité \mathcal{Q} mais plus simple à démontrer!



$\mathcal{P} \iff \mathcal{Q}$

Or \mathcal{Q}

Donc \mathcal{P}

Pour rappel, cela signifie :

$\mathcal{P} \iff \mathcal{Q}$ est vraie

Or \mathcal{Q} est vraie

Donc \mathcal{P} est vraie



Démontrer « La fonction carrée est décroissante sur $] -\infty, 0]$ » en utilisant ^a la caractérisation :

$$(x \mapsto x^2 \text{ est décroissante sur }] -\infty, 0]) \iff (\forall x \in] -\infty, 0], 2x \leq 0)$$

^a. Là encore, il est entendu que cette équivalence est vraie, c'était le dernier rappel.)

Propriété (par disjonction de cas).

On détermine une assertion \mathcal{Q} telle que « $\mathcal{Q} \implies \mathcal{P}$ » et « $\text{non}(\mathcal{Q}) \implies \mathcal{P}$ » soient toutes les deux vraies.



Cette technique est à privilégier lorsque l'on a besoin « d'augmenter les hypothèses » sans pour autant perdre en généralité. Souvent, la difficulté réside dans le fait de trouver le « bon \mathcal{Q} » permettant de démontrer les deux implications ^a.

^a. On pourra revenir sur la rédaction suivante lorsque l'on aura vu comment démontrer une implication



1^{er} cas : supposons \mathcal{Q}

Montrons \mathcal{P}

\vdots } Preuve de \mathcal{P}

2^e cas : supposons $\text{non}(\mathcal{Q})$

Montrons \mathcal{P}

\vdots } Preuve de \mathcal{P}



On peut aussi généraliser à plus de deux cas, pas obligatoirement disjoints mais couvrant toutes les possibilités



Démontrer « La somme d'un entier naturel et de son carré est un nombre pair ».

Étant donné n un entier naturel ^a, on peut considérer les deux cas « \mathcal{Q} » et « $\text{non}(\mathcal{Q})$ » où \mathcal{Q} désigne l'assertion « n est pair » c'est à dire « $\exists k \in \mathbb{N}, n = 2k$ » ou encore « n est de la forme $2k$ avec k un entier naturel ».

a. On y reviendra lorsque l'on aura vu comment démontrer une quantification universelle. En effet, l'assertion se formalise de la manière suivante :

$$\forall n \in \mathbb{N}, \underbrace{\exists k \in \mathbb{N}, n + n^2 = 2k}_{n+n^2 \text{ est pair}}$$

On peut déjà remarquer que dans l'expression « un entier naturel », l'article « un » est indéfini autrement dit l'entier naturel est bien quelconque.

Propriété (par l'absurde).

On détermine une assertion fausse \mathcal{Q} telle que « $\text{non}(\mathcal{P}) \implies \mathcal{Q}$ » soit vraie.



Justifier ce raisonnement à l'aide de la table de vérité de l'implication « $\text{non}(\mathcal{P}) \implies \mathcal{Q}$ ».



Cette technique est à privilégier lorsque l'on a l'intuition que \mathcal{P} ne peut pas être fausse. La difficulté est évidemment de mettre la main sur une contradiction, il faut accepter de chercher un peu.



Raisonnons par l'absurde, et supposons $\text{non}(\mathcal{P})$.

∴ } Recherche d'une contradiction

On en déduit \mathcal{Q}

Or $\text{non}(\mathcal{Q})$

Donc \mathcal{P}



Démontrer « Un entier naturel ne peut pas être à la fois pair et impair ».

Étant donné n un entier naturel, on va supposer qu'il est à la fois pair et impair, puis chercher une contradiction.

Pour démontrer une implication « $\mathcal{P} \implies \mathcal{Q}$ »

Propriété (directement).

On suppose \mathcal{P} vraie, et on montre que \mathcal{Q} l'est aussi.



Supposons \mathcal{P}

Montrons \mathcal{Q}

∴ } Preuve de \mathcal{Q}



Étant donné un réel $x \in [0, 1]$, démontrer « $x - x^2 \in \mathbb{N} \implies x = 0$ ou $x = 1$ »

Propriété (par contraposition).

On démontre « $\text{non}(\mathcal{Q}) \implies \text{non}(\mathcal{P})$ ».



| Cette technique est à privilégier lorsque $\text{non}(\mathcal{P})$ est plus facile à démontrer que \mathcal{Q}



Raisonnons par contraposition, et supposons $\text{non}(\mathcal{Q})$

Montrons $\text{non}(\mathcal{P})$

: } Preuve de $\text{non}(\mathcal{P})$



| Étant donné n un entier naturel, démontrer « n^2 pair $\implies n$ pair ».

Pour démontrer une équivalence « $\mathcal{P} \iff \mathcal{Q}$ »

Propriété (directement).

On utilise une « suite d'équivalences » en modifiant peu à peu \mathcal{P} en \mathcal{Q} .



| Se méfier des fausses équivalences



$\mathcal{P} \iff \dots$
 $\iff \dots$
 $\iff \mathcal{Q}$



| Étant donné un réel x strictement positif, démontrer « $(x^2 - 4x + 3)(1 - \ln x) = 0 \iff x = 1$ ou $x = 3$ ou $x = e$ »

Propriété (par double implication).

On démontre « $\mathcal{P} \implies \mathcal{Q}$ » et « $\mathcal{Q} \implies \mathcal{P}$ »



| Cette technique est à privilégier lorsque la méthode *directe* ne convient pas (c'est très souvent le cas)



Montrons $\mathcal{P} \Rightarrow \mathcal{Q}$:

Supposons \mathcal{P}

Montrons \mathcal{Q}

\vdots } Preuve de \mathcal{Q}

Montrons $\mathcal{Q} \Rightarrow \mathcal{P}$:

Supposons \mathcal{Q}

Montrons \mathcal{P}

\vdots } Preuve de \mathcal{P}



Étant donnés deux réels x et y , démontrer « $x^2 + y^2 = 0 \iff x = 0$ et $y = 0$ ».

Pour démontrer une disjonction « \mathcal{P} ou \mathcal{Q} »

Propriété (en niant l'une des deux).

On démontre l'assertion logiquement équivalente « $\text{non}(\mathcal{P}) \Rightarrow \mathcal{Q}$ ».



Supposons $\text{non}(\mathcal{P})$

Montrons \mathcal{Q}

\vdots } Preuve de \mathcal{Q}



Étant donné un réel x , démontrer « $x^2 \geq 1$ ou $(x-2)^2 \geq 1$ »

Pour démontrer une quantification universelle « $\forall x \in E, \mathcal{P}(x)$ »

Propriété (en introduisant une variable).

On considère un x quelconque de E que l'on fixe le temps de la preuve, et on montre que $\mathcal{P}(x)$ est vraie.



Le langage commun « masque » parfois la quantification universelle.

Par exemple, l'exercice précédent consiste en fait à démontrer :

$$\forall x \in \mathbb{R}, (x^2 \geq 1 \text{ ou } (x-2)^2 \geq 1)$$

On peut aussi revenir sur l'exercice qui s'intéresse à la parité de la somme d'un entier naturel avec son carré.



Soit $x \in E$

Montrons $\mathcal{P}(x)$

\vdots } Preuve de $\mathcal{P}(x)$



Démontrer « $\forall x \in \mathbb{R}, \frac{x}{x^2+1} \leq \frac{1}{2}$ »

Pour démontrer une quantification existentielle « $\exists x \in E, \mathcal{P}(x)$ »

Propriété (de manière constructive).

On détermine (concrètement) un x qui convient.



Cette méthode permet, en particulier, de montrer qu'une quantification universelle est fausse.
Le x qui convient est alors un contre-exemple!



Posons ^a $x = \dots$

Vérifions $\mathcal{P}(x)$

\vdots } Vérification de $\mathcal{P}(x)$

a. Trouver un x qui convient n'est pas toujours évident, ni même faisable



1. A-t-on « $\forall x \in \mathbb{R}, x^2 \geq x$ »?
2. Démontrer « $\forall x, y \in \mathbb{R}, \exists z \in \mathbb{R}, z > x + y$ »^a.
3. A-t-on « $\exists z \in \mathbb{R}, \forall x, y \in \mathbb{R}, z > x + y$ »?

a. Par abus, on regroupe x et y derrière le même quantificateur \forall au lieu de :

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \exists z \in \mathbb{R}, z > x + y$$

Propriété (de manière théorique).

On montre qu'il est possible de trouver un x qui convient, sans pour autant être capable de le déterminer.



On pourra penser, par exemple, à la propriété de Cauchy^a qui fournit un tel x . Cet élément n'est pas connu de manière exacte, mais il peut être approché par des méthodes d'analyse numérique présentées dans le module d'analyse au semestre 2.

a. Soit f une fonction réelle continue sur un intervalle I , et $a < b$ deux réels dans I .

$$\text{Si } f(a)f(b) < 0, \text{ alors } \exists c \in]a, b[, f(c) = 0$$

Autrement dit, une fonction continue qui change de signe s'annule en un point (au moins)

Propriété (séparément).

On montre l'existence (il en existe au moins un) et l'unicité (il en existe au plus un) dans l'ordre qui nous arrange ^a.

^a. Lorsque l'on ne parvient pas à déterminer un x qui convient, on peut commencer par l'unicité qui permet en fait de déterminer le seul candidat possible! Montrer l'existence consiste alors à vérifier que ce candidat convient. Cette technique qui consiste à rechercher d'abord tous les candidats possibles, pour ensuite ne garder que ceux qui conviennent est appelée le raisonnement par analyse-synthèse. On y reviendra plus tard.



• **Si on commence par l'existence**

Existence :

Posons $x = \dots$

Vérifions $\mathcal{P}(x)$

\vdots } Vérification de $\mathcal{P}(x)$

Unicité ^a :

Soit $x, x' \in E$

Supposons $\mathcal{P}(x)$ et $\mathcal{P}(x')$

Montrons $x = x'$

\vdots } Preuve de $x = x'$

• **Si on commence par l'unicité**

Unicité :

Soit $x \in E$

Supposons $\mathcal{P}(x)$

\vdots } On cherche des conditions nécessaires sur x pour avoir $\mathcal{P}(x)$

Donc $x = \dots$

Existence :

Posons ^b $x = \dots$

Vérifions $\mathcal{P}(x)$

\vdots } Vérification de $\mathcal{P}(x)$

^a. En fait, l'unicité se formalise de la manière suivante :

$$\forall x, x' \in E, (\mathcal{P}(x) \text{ et } \mathcal{P}(x') \implies x = x')$$

^b. On reprend évidemment le seul candidat possible issu de l'unicité



Démontrer « $\exists ! x \in \mathbb{R}_+, x^2 = 1$ » en commençant par l'existence.

Pour démontrer une quantification universelle sur les entiers naturels « $\forall n \in \mathbb{N}, \mathcal{P}(n)$ »

Propriété (par récurrence).

On utilise l'implication suivante ^a :

$$\left(\underbrace{\mathcal{P}(0)}_{\text{Initialisation}} \text{ et } \underbrace{(\forall n \in \mathbb{N}, \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1))}_{\text{Hérédité}} \right) \Rightarrow (\forall n \in \mathbb{N}, \mathcal{P}(n))$$

a. Il s'agit du principe de récurrence



- Cette technique est à privilégier lorsque la démonstration *directe* ^a n'aboutit pas
- On peut généraliser :
 - en initialisant à un entier $n_0 > 0$
 - en considérant une récurrence « forte » voire multiple ^b

a. Considérer un n quelconque de \mathbb{N} et montrer $\mathcal{P}(n)$

b. Cela sort du cadre de ce cours



Initialisation :

Vérifions $\mathcal{P}(0)$

\vdots } Vérification de $\mathcal{P}(0)$

Hérédité :

Soit $n \in \mathbb{N}$

Supposons ^a $\mathcal{P}(n)$

Montrons $\mathcal{P}(n+1)$

\vdots } Preuve de $\mathcal{P}(n+1)$

a. Il s'agit de l'Hypothèse de Récurrence (HR)



On considère la suite $(u_n)_{n \in \mathbb{N}}$ définie par : $u_0 = 1$ et $\forall n \in \mathbb{N}, u_{n+1} = 2u_n$.
Démontrer « $\forall n \in \mathbb{N}, u_n = 2^n$ ».