

CHAPITRE 1 - RAISONNEMENT ET VOCABULAIRE ENSEMBLISTE



Un peu d'histoire...

La logique mathématique est née à la fin du XIXe siècle de la logique au sens philosophique du terme ; elle est l'une des pistes explorées par les mathématiciens de cette époque afin de résoudre la crise des fondements provoquée par la complexification des mathématiques et l'apparition des paradoxes. Ses débuts sont marqués par la rencontre entre deux idées nouvelles :

- la volonté chez Frege, Russell, Peano et Hilbert de donner une fondation axiomatique aux mathématiques ;
- la découverte par George Boole de l'existence de structures algébriques permettant de définir un « calcul de vérité ».

La logique mathématique se fonde sur les premières tentatives de traitement formel des mathématiques, dues à Leibniz et Lambert (fin XVIIe siècle - début XVIIIe siècle). Leibniz a en particulier introduit une grande partie de la notation mathématique moderne (usage des quantificateurs, symbole d'intégration, etc.). Toutefois on ne peut parler de logique mathématique qu'à partir du milieu du XIXe siècle, avec les travaux de George Boole (et dans une moindre mesure ceux d'Auguste De Morgan) qui introduit un calcul de vérité où les combinaisons logiques comme la conjonction, la disjonction et l'implication, sont des opérations analogues à l'addition ou la multiplication des entiers, mais portant sur les valeurs de vérité faux et vrai (ou 0 et 1) ; ces opérations booléennes se définissent au moyen de tables de vérité.

Le calcul de Boole véhiculait l'idée apparemment paradoxale, mais qui devait s'avérer spectaculairement fructueuse, que le langage mathématique pouvait se définir mathématiquement et devenir un objet d'étude pour les mathématiciens. Toutefois il ne permettait pas encore de résoudre les problèmes de fondements. Dès lors, nombre de mathématiciens ont cherché à l'étendre au cadre général du raisonnement mathématique et on a vu apparaître les systèmes logiques formalisés ; l'un des premiers est dû à Frege au tournant du XXe siècle.

En 1931, Kurt Gödel publie dans son article *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme* (en) (« Sur les propositions formellement indécidables des Principia Mathematica et des systèmes apparentés »). Les théorèmes d'incomplétude de Gödel sont deux théorèmes célèbres de logique mathématique qui ont marqué un tournant dans l'histoire de la logique en apportant une réponse négative à la question de la démonstration de la cohérence des mathématiques posée plus de 20 ans auparavant par le programme de Hilbert.

I. Rudiments de logique

Définition 1

Une **assertion** $\mathcal{P}$ (ou une proposition) est un énoncé mathématique qui est soit vrai, soit faux (principe du tiers exclu).

Exemple 1

- $\mathcal{P}$: « $3 \leq 2$ » est une assertion qui est toujours fausse.
- $\mathcal{P}$: « 18 est divisible par 3 » est une assertion vraie.
- $\mathcal{P}$: « il pleut » est une assertion, soit il pleut, soit il ne pleut pas.
- $\mathcal{P}$: « $x = 3$ » est une assertion, soit $x = 3$, soit $x \neq 3$.

Dans le cours de mathématiques, nous n'écrivons que des propositions vraies.

Remarque 1

- La phrase « cette assertion est fausse » n'est ni vraie, ni fausse. Ce n'est donc pas une assertion logique.
Ce paradoxe est comparable à un individu affirmant « je mens » : il est logiquement impossible de savoir si cet individu dit ou non la vérité. C'est le paradoxe du menteur.
- Mentionnons aussi le paradoxe de Berry : soit E l'ensemble des entiers naturels descriptibles par une phrase (en français) de quinze mots ou moins.
Alors E est un ensemble fini (il n'y a qu'un nombre fini de phrases de quinze mots ou moins).
Soit n_0 le plus petit entier n'appartenant pas à E . Alors n_0 est défini de façon unique par la phrase « Le plus petit entier non descriptible par une phrase de moins de quinze mots ». Or cette phrase comporte 14 mots, donc n_0 appartient à E , ce qui constitue un paradoxe.

Celui-ci ne dévoile aucune incohérence des mathématiques, mais prouve tout simplement que n'importe quelle phrase ne peut être considérée comme une assertion mathématique.

A. Premiers connecteurs logiques

Définition 2

Soient $\mathcal{P}$ et $\mathcal{Q}$ deux propositions. Les connecteurs logiques sont :

1. La conjonction : « et », notée $\wedge$.
 $\mathcal{P} \wedge \mathcal{Q}$ est vraie si $\mathcal{P}$ est vraie et $\mathcal{Q}$ est vraie.
2. La disjonction : « ou », notée $\vee$.
 $\mathcal{P} \vee \mathcal{Q}$ est vraie si au moins l'une des deux propositions $\mathcal{P}$ ou $\mathcal{Q}$ est vraie.
3. La négation : « non », notée $\neg$.
 $\neg \mathcal{P}$ est vraie si $\mathcal{P}$ est fausse.

Remarque 2

Dans le langage courant, « ou » a en général un sens exclusif (fromage « ou » dessert). En mathématiques, le « ou » est toujours inclusif : si $\mathcal{P}$ et $\mathcal{Q}$ sont toutes les deux vraies, alors $\mathcal{P} \vee \mathcal{Q}$ est vraie.

Exemple 2

- L'ensemble des réels vérifiant l'assertion $(x \geq 0) \wedge (x \leq 1)$ est l'ensemble des réels $x \in [0, 1]$.
- Les négations de ces deux assertions sont respectivement $(x < 0)$ et $(x > 1)$.
- À ajouter

Il existe en logique un certain nombre de règles qui établissent un calcul des propositions, semblable au calcul algébrique. Après application de l'une de ces règles sur une assertion, on obtient une assertion équivalente, c'est-à-dire ayant la même valeur de vérité.

Proposition 1 (Lois de Morgan)

Soient $\mathcal{P}$ et $\mathcal{Q}$ deux assertions. Alors

$$\neg(\mathcal{P} \vee \mathcal{Q}) \text{ a même valeur logique que } (\neg\mathcal{P}) \wedge (\neg\mathcal{Q})$$

$$\neg(\mathcal{P} \wedge \mathcal{Q}) \text{ a même valeur logique que } (\neg\mathcal{P}) \vee (\neg\mathcal{Q})$$

En d'autres termes, la négation d'une conjonction est la disjonction des négations, et la négation d'une disjonction est la conjonction des négations.

Il est bon de s'en convaincre sur les exemples. Pour démontrer cette proposition, il suffit d'envisager tous les cas possibles selon que $\mathcal{P}$ et $\mathcal{Q}$ sont vraies ou fausses. Pour cela on peut par exemple établir la **table de vérité** des assertions considérées. Par exemple les tables de vérité de « $\neg(\mathcal{P} \vee \mathcal{Q})$ » et « $(\neg\mathcal{P}) \wedge (\neg\mathcal{Q})$ » coïncident et sont données par :

$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P} \vee \mathcal{Q}$	$\neg(\mathcal{P} \vee \mathcal{Q})$
0	0	0	1
0	1	1	0
1	0	1	0
1	1	1	0

$\mathcal{P}$	$\mathcal{Q}$	$\neg\mathcal{P}$	$\neg\mathcal{Q}$	$(\neg\mathcal{P}) \wedge (\neg\mathcal{Q})$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	0	0	0

Exercice 1.

Écrire les tables de vérité de $\neg(\mathcal{P} \wedge \mathcal{Q})$ et $(\neg\mathcal{P}) \vee (\neg\mathcal{Q})$ afin de démontrer la deuxième proposition.

Exemple 3**B. Implication, équivalence, réciproque, contraposée**

On considère l'assertion

« S'il pleut, (alors) il prend son parapluie »

Elle est formée à partir des assertions « il pleut » et « il prend son parapluie ». Même si on sait que l'assertion ci-dessus est vraie, on ne peut pas dire s'il pleut ou non. On ne peut pas dire non plus s'il a pris ou non son parapluie. Par contre si on sait aussi qu'il pleut, alors on peut déduire qu'il a pris son parapluie. Finalement, la seule situation qui est exclue par ci-dessus est celle où il pleut mais où il ne prend pas son parapluie. Mais il se peut qu'il n'ait pas pris son parapluie, il se peut également qu'il ne pleuve pas mais qu'il prenne quand même son parapluie (on n'est jamais trop prudent).

Prenons l'exemple suivant :

$$\text{« Si } x \geq 2 \text{ alors } x^2 \geq 4 \text{ »}$$

Cette assertion est vraie, quelle que soit la valeur de x . Pourtant la conséquence $x^2 \geq 4$ peut être fausse (par exemple pour $x = 1$).

D'autre part on peut avoir $x^2 \geq 4$ même si l'assertion $x \geq 2$ n'est pas vraie (par exemple pour $x = -3$).

Tout ce que dit cette assertion est qu'il est impossible d'avoir à la fois $x \geq 2$ et $x^2 < 4$.

Définition 3

Étant données deux assertions $\mathcal{P}$ et $\mathcal{Q}$, l'assertion « Si $\mathcal{P}$ alors $\mathcal{Q}$ », ou « $\mathcal{P}$ implique $\mathcal{Q}$ » a même valeur logique que

$$\neg(\mathcal{P} \wedge \neg\mathcal{Q})$$

Cette assertion est notée

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

Remarque 3

— $\mathcal{P} \Rightarrow \mathcal{Q}$ et $\neg(\mathcal{P} \wedge \neg \mathcal{Q})$ ont même valeur logique.

Leur la table de vérité commune est :

$\mathcal{P}$	$\mathcal{Q}$	$\neg \mathcal{Q}$	$\mathcal{P} \wedge \neg \mathcal{Q}$	$\neg(\mathcal{P} \wedge \neg \mathcal{Q})$
0	0	1	0	1
0	1	0	0	1
1	0	1	1	0
1	1	0	0	1

— D'après les lois de Morgan, $\neg(\mathcal{P} \wedge \neg \mathcal{Q})$ a même valeur logique que $(\neg \mathcal{P}) \vee (\mathcal{Q})$. Donc $\mathcal{P} \Rightarrow \mathcal{Q}$ est vraie si $\mathcal{P}$ est faux ou $\mathcal{Q}$ est vraie.

En mathématiques, un résultat vrai n'implique jamais un résultat faux.

— Donc, si $\mathcal{P}$ est fausse, alors $\mathcal{P} \Rightarrow \mathcal{Q}$ est toujours vraie, quelle que soit la valeur de vérité de $\mathcal{Q}$. Et on a $(\mathcal{P} \Rightarrow \mathcal{Q}) \Leftrightarrow ((\neg \mathcal{P}) \vee \mathcal{Q})$.

— Contrairement à la conjonction ou la disjonction, l'implication dépend de l'ordre des deux propositions. Les propositions $\mathcal{P} \Rightarrow \mathcal{Q}$ et $\mathcal{Q} \Rightarrow \mathcal{P}$ sont différentes, comme le précise la prochaine définition.

Exemple 4

1. « $1 = 2 \Rightarrow 2 = \pi$ » est vraie.

2. $\neg(\text{« il pleut »} \Rightarrow \text{« je prends un parapluie »}) \Leftrightarrow (\text{« il pleut »} \wedge \text{« je ne prends pas de parapluie »})$. À MODIFIER.

Définition 1.

Étant données deux assertions $\mathcal{P}$ et $\mathcal{Q}$, on appelle **réci-proque** de l'implication $\mathcal{P} \Rightarrow \mathcal{Q}$ l'assertion $\mathcal{Q} \Rightarrow \mathcal{P}$. Attention, ce n'est pas parce qu'une implication est vraie que sa réciproque est vraie ou fausse ...

Définition 4

On dit que deux assertions $\mathcal{P}$ et $\mathcal{Q}$ sont **équivalentes** si $\mathcal{P} \Rightarrow \mathcal{Q}$ et $\mathcal{Q} \Rightarrow \mathcal{P}$ (sont vraies).

L'assertion « $\mathcal{P}$ et $\mathcal{Q}$ sont équivalentes » est notée

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

La table de vérité de l'assertion $\mathcal{P} \Leftrightarrow \mathcal{Q}$ est :

$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P} \Rightarrow \mathcal{Q}$	$\mathcal{Q} \Rightarrow \mathcal{P}$	$\mathcal{P} \Leftrightarrow \mathcal{Q}$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	1	1	1

Exemple 5

1. $\neg(x = 3) \Leftrightarrow (x \neq 3)$.

2. $((x > -2) \wedge (x \leq 5)) \Leftrightarrow (x \in]-2; 5])$.

Définition 5

Soient $\mathcal{P}$ et $\mathcal{Q}$ deux assertions. On appelle **contraposée** de l'implication $\mathcal{P} \Rightarrow \mathcal{Q}$ l'assertion $(\neg \mathcal{Q}) \Rightarrow (\neg \mathcal{P})$

Propriété 1.

Une implication et sa contraposée sont équivalentes. En symboles,

$$(\mathcal{P} \Rightarrow \mathcal{Q}) \Leftrightarrow (\neg \mathcal{Q} \Rightarrow \neg \mathcal{P})$$

Exemple 6 La contraposée de l'assertion

« S'il pleut, alors il prend son parapluie »

est l'assertion

« S'il ne prend pas son parapluie alors il ne pleut pas »

Attention à ne pas confondre l'implication avec un lien de causalité. On n'est pas en train de dire que c'est l'absence de parapluie qui provoque l'absence de pluie, on dit simplement que si on sait qu'il n'a pas pris de parapluie, alors on sait qu'il ne pleut pas.

Cette équivalence entre une implication et sa contraposée est la base du raisonnement « par contraposée ». Cela consiste à montrer l'implication $(\neg \mathcal{P}) \Rightarrow (\neg \mathcal{Q})$ plutôt que $\mathcal{P} \Rightarrow \mathcal{Q}$ lorsque la première implication s'avère plus facile à prouver.

Exercice 2.

Montrer par contraposition, que quelque soit l'entier naturel n , $2^n - 1$ premier $\Rightarrow n$ premier .

Remarque 4

Par la suite, on ne parlera plus en général de proposition « vraie » ou « fausse ».

On parlera d'une proposition en supposant implicitement qu'elle est vraie, sauf mention explicite du contraire.

Par exemple on écrira simplement $\mathcal{P} : x \geq 2$, qui s'écrirait en toute rigueur « $x \geq 2$ est vraie ».

Résumé des tables de vérité à connaîtreTable de vérité de $\mathcal{P} \wedge \mathcal{Q}$

$\mathcal{Q} \backslash \mathcal{P}$	1	0
1	1	0
0	0	0

Table de vérité de $\mathcal{P} \vee \mathcal{Q}$

$\mathcal{Q} \backslash \mathcal{P}$	1	0
1	1	1
0	1	0

Table de vérité de $\mathcal{P} \Rightarrow \mathcal{Q}$

$\mathcal{Q} \backslash \mathcal{P}$	1	0
1	1	1
0	0	1

Table de vérité de $\mathcal{P} \Leftrightarrow \mathcal{Q}$

$\mathcal{Q} \backslash \mathcal{P}$	1	0
1	1	0
0	0	1

C. Quantificateurs

Il y a deux quantificateurs logiques :

Définition 6

- Le **quantificateur universel** $\forall$ signifie « pour tout » (ou « quel que soit »). Par exemple, l'assertion

$$\forall x \in \mathbb{R}, f(x) > 0$$

signifie « pour tout nombre réel x , $f(x)$ est strictement positif » que l'on traduirait plutôt « f est une fonction strictement positive sur $\mathbb{R}$ ».

- Le **quantificateur existentiel** $\exists$ signifie « il existe ». Par exemple l'assertion

$$\exists x \in \mathbb{R} | f(x) > 0$$

signifie « il existe un nombre réel x tel que $f(x)$ soit strictement positif ».

- Pour exprimer l'unicité en plus de l'existence, le symbole utilisé est $\exists!$ (le quantificateur existentiel suivi d'un point d'exclamation) ; $\exists!$ signifie donc « il existe un unique ». Par exemple, l'assertion

$$\exists! x \in \mathbb{R} | f(x) > 0$$

signifie « il existe un unique nombre réel x tel que $f(x)$ soit strictement positif ».

Remarque 5

Il convient de faire un usage modéré de ces quantificateurs. Il ne s'agit pas de signes sténographiques (i.e. il ne s'agit pas d'abréviations) et il n'est pas le bienvenu d'écrire « $\exists$ un nombre réel » ou encore « $\forall x \in \mathbb{R}$, on a $f(x) > 0$ ».

Exemple 7

- $\forall x \in \mathbb{R}, x^2 \geq 0$: « pour tout réel x , x au carré est positif » (ce qui est vrai).
- $\forall x \in \mathbb{C}, x^2 \in \mathbb{R}$: « pour tout x complexe, le carré de x est réel » (ce qui est faux).
- $\forall n \in \mathbb{N}, (2|n^2) \Rightarrow (2|n)$: « pour tout entier naturel n , si 2 divise n au carré, alors 2 divise n . (ce qui est vrai) ».
- $\exists x \in \mathbb{R}, x^2 = 5$: « il existe un réel x dont le carré vaut 5 » (ce qui est vrai).
- $\exists x \in \mathbb{R}, x^2 = -1$: « il existe un réel x dont le carré vaut -1 » (ce qui est faux).
- $\exists n \in \mathbb{N}, 10n \geq 100$: « il existe un entier naturel n tel que $10n$ est plus grand que 100 » (ce qui est vrai).
- $\exists! x \in \mathbb{R}^+, x^2 = 2$: « il existe un unique réel positif x dont le carré vaut 2 » (ce qui est vrai).

D. Négation et quantificateurs/Méthode pour nier une assertion

Attention à la négation des assertions contenant des quantificateurs.

Le contraire de « Tous les chemins mènent à Rome » n'est pas « Aucun chemin ne mène à Rome », car ces deux assertions peuvent être simultanément fausses.

La négation est plutôt :

« Il existe un chemin qui ne mène pas à Rome ».

Comment se comporte alors une proposition précédée d'un quantificateur lorsque l'on en prend la négation ?

Proposition 2 La négation de la proposition :

- « $\forall x \in E, \mathcal{P}(x)$ » est la proposition « $\exists x \in E, (\neg \mathcal{P}(x))$ » ;
- « $\exists x \in E, \mathcal{P}(x)$ » est la proposition « $\forall x \in E, (\neg \mathcal{P}(x))$ »

Exemple 8

- $\neg(\forall x \in \mathbb{R}, x^2 \geq 0) \Leftrightarrow (\exists x \in \mathbb{R}, x^2 < 0)$
- $\neg(\exists n \in \mathbb{N}, n^2 \geq 3) \Leftrightarrow (\forall n \in \mathbb{N}, n^2 \neq 3)$
- $\neg(\forall z \in i\mathbb{R}, z^2 \in \mathbb{R}^-) \Leftrightarrow (\exists z \in \mathbb{C}, z^2 \notin \mathbb{R}^-)$

E. Plusieurs quantificateurs

Dans certaines propositions, on utilise plusieurs quantificateurs (on ne considère pas ici le quantificateur particulier $\exists!$), par exemple :

$$\forall n \in \mathbb{N}, \exists m \in \mathbb{N}, m \geq n,$$

qui se lit « pour tout entier naturel n , il existe un entier naturel m tel que m est plus grand que n » (ce qui est vrai, il suffit de prendre $m = n + 1$).

Question : Si on permute l'ordre des quantificateurs, la proposition reste-t-elle la même ? Il semble que non puisque si l'on permute dans l'exemple précédent on obtient :

$$\exists n \in \mathbb{N}, \forall m \in \mathbb{N}, m \geq n,$$

qui se lit « il existe un entier m tel que pour tout entier n , m est plus grand que n » (ce qui est faux : aucun entier n'est plus grand que tous les autres entiers)

Proposition 3 Lorsqu'on a plusieurs quantificateurs au début d'une proposition :

- on peut permuter les quantificateurs sans changer la proposition si les quantificateurs sont de même nature.
- on ne peut pas permuter les quantificateurs s'ils sont de nature différente, sans changer le sens de la proposition.
- s'il y a les deux types de quantificateurs dans une proposition, on peut permuter des quantificateurs de même nature s'ils sont à la suite dans la proposition, sans changer le sens de la proposition.

Exemple 9 Lorsqu'on a plusieurs quantificateurs au début d'une proposition :

- $(\forall x \in \mathbb{R}, \forall y \in \mathbb{C}, x + y^2 \in \mathbb{R}) \Leftrightarrow (\forall y \in \mathbb{C}, \forall x \in \mathbb{R}, x + y^2 \in \mathbb{R})$
- L'exemple plus haut montre qu'on ne peut pas permuter les quantificateurs s'ils sont de nature différente, sans changer le sens de la proposition.
- $\forall x \in E, \forall y \in F, \exists z \in G$ a le même sens que $\forall y \in F, \forall x \in E, \exists z \in G$, mais un sens différent de $\forall x \in E, \exists z \in G, \forall y \in F$.

F. Méthodes de raisonnement

DÉMONSTRATION DIRECTE

C'est la méthode qu'on pourrait qualifier de « classique » ou de « directe » pour prouver une assertion du type $\mathcal{P}$ (resp. $\mathcal{P} \Rightarrow \mathcal{Q}$). On prouve directement la proposition $\mathcal{P}$ (resp. on part des hypothèses $\mathcal{P}$ et on montre directement la proposition $\mathcal{Q}$).

Exemple 10 Montrons que : $\forall n \in \mathbb{N}, 2|n \Rightarrow 2|n^2$.

Si $2|n$ alors il existe $m \in \mathbb{N}$ tel que $n = 2m$.

On a alors $n^2 = (2m)^2 = 4m^2 = 2(2m^2)$ qui est donc divisible par 2. CQFD.

Remarque 6

On peut être amené à prouver une équivalence plutôt qu'une implication : $\mathcal{P} \Leftrightarrow \mathcal{Q}$.

En général dans ce cas on prouve séparément $\mathcal{P} \Rightarrow \mathcal{Q}$ et $\mathcal{Q} \Rightarrow \mathcal{P}$.

DÉMONSTRATION D'UNE IMPLICATION PAR CONTRAPOSITION

C'est la méthode qui utilise la propriété de logique qui dit qu'une implication et sa contraposée sont les mêmes. Donc pour montrer une assertion du type $\mathcal{P} \Rightarrow \mathcal{Q}$, on va utiliser la méthode précédente (démonstration directe) mais pour prouver $\neg \mathcal{Q} \Rightarrow \neg \mathcal{P}$.

Exemple 11 Montrons par exemple par contraposée que $\forall n \in \mathbb{N}, 2^n - 1$ premier $\Rightarrow n$ premier.

On montre donc la proposition contraposée qui est :

$$n \text{ non premier} \Rightarrow 2^n - 1 \text{ non premier.}$$

n non premier signifie $\exists (a, b) \in \mathbb{N}^2 \mid 2 \leq a \leq n$ et $2 \leq b \leq n$ et $n = ab$.

On a alors

$$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1) \left(1 + 2^a + (2^a)^2 + (2^a)^3 + \dots + (2^a)^{b-1} \right)$$

De plus, $2^a - 1 \geq 3$ car $a \geq 2$, et $(1 + 2^a + (2^a)^2 + (2^a)^3 + \dots + (2^a)^{b-1}) \geq 1 + 2^a \geq 5$ car $b - 1 \geq 1$.

Et donc $2^n - 1$ n'est pas premier car il se décompose en produit de deux facteurs supérieurs ou égaux à 2. CQFD.

DÉMONSTRATION PAR L'ABSURDE

La démonstration par l'absurde est la méthode qui consiste à prouver une proposition $\mathcal{P}$ (resp. une implication du type $\mathcal{P} \Rightarrow \mathcal{Q}$) en supposant la négation de cette proposition, à savoir $\neg \mathcal{P}$ (resp. $\mathcal{P} \wedge \neg \mathcal{Q}$) et d'aboutir à une contradiction, ce qui prouve que la négation de la proposition est fausse, et donc que la proposition est vraie.

Exemple 12 Montrons par exemple par l'absurde que $\sqrt{2}$ est un nombre irrationnel.

On suppose donc que c'est faux, c'est-à-dire que $\sqrt{2}$ est un nombre rationnel.

Il existe donc $(p, q) \in \mathbb{N}^2$ tels que $\sqrt{2} = \frac{p}{q}$ avec p et q premiers entre eux, c'est-à-dire que si un nombre $n \in \mathbb{N}$ divise à la fois p et q alors $n = 1$. En particulier au moins un des nombres parmi p et q est impair.

On a alors $p^2 = 2q^2$, donc p^2 est pair, donc p est pair (puisque le carré d'un nombre impair est impair). Il existe donc $m \in \mathbb{N}$ tel que $p = 2m$, et donc $p^2 = 4m^2 = 2q^2$ et donc $q^2 = 2m^2$, ce qui prouve que q^2 est pair et donc q est pair, ce qui contredit le fait que au moins un des nombres parmi p et q est impair. CQFD.

DÉMONSTRATION PAR ANALYSE-SYNTÈSE

Le raisonnement par analyse-synthèse est utilisé pour déterminer l'ensemble des solutions d'un problème, tout cela en deux étapes :

- Première phase : **analyse**. Dans cette phase on considère une solution du problème (sans savoir encore s'il en existe) et on cherche des propriétés que cette solution doit vérifier. On raisonne dans cette phase par condition nécessaire.
- Deuxième phase : **synthèse**. Dans cette phase, on considère l'ensemble des objets vérifiant les propriétés trouvées pendant l'analyse et on cherche, parmi ceux-ci, lesquels sont effectivement solution du problème de départ.

Remarque 7

- Il peut arriver que l'ensemble des objets trouvés en phase d'analyse soient exactement les solutions du problème de départ, surtout s'il n'y en a qu'un seul (auquel cas on obtient l'unicité en plus de l'existence).
- Il peut aussi arriver qu'aucun des objets trouvés en phase d'analyse ne soit solution du problème de départ. Le problème n'a alors aucune solution.

Exemple 13

- Prouver que toute fonction $f : \mathbb{R} \rightarrow \mathbb{R}$ se décompose de manière unique comme somme d'une fonction paire et d'une fonction impaire.
- Trouver toutes les applications $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$ vérifiant

$$\forall (n, m) \in \mathbb{Z}^2, \phi(n + m) = \phi(n) + \phi(m)$$

DÉMONSTRATION PAR RÉCURRENCE

Récurrence simple :

La démonstration par récurrence consiste à prouver une propriété $\mathcal{P}(n)$ qui dépend d'un indice entier n .

Le principe de cette démonstration est de prouver la propriété à un certain rang n_0 , ce qu'on appelle l'**initialisation**, puis de prouver que, si la propriété est vraie à un rang $n \geq n_0$, alors elle sera vraie au rang suivant $n + 1$, ce que l'on appelle l'**hérédité**.

La propriété est alors vraie pour tous les entiers $n \geq n_0$.

La propriété $\mathcal{P}(n)$ est appelée **hypothèse de récurrence**.

Exemple 14 Montrons par exemple que la somme des n premiers entiers consécutifs ($n \geq 1$) est égale à

$$\sum_{k=1}^n k = \frac{n(n+1)}{2}$$

La propriété $\mathcal{P}(n)$ que l'on veut montrer est donc : $\mathcal{P}(n) : \sum_{k=1}^n k = \frac{n(n+1)}{2}$.

Initialisation : pour $n = 1$, on a $1 + \dots + n = 1$, et $\frac{1(1+1)}{2} = 1$, donc $\mathcal{P}(1)$ est vraie.

Hérédité : supposons que $\mathcal{P}(n)$ soit vraie, montrons que $\mathcal{P}(n+1)$ l'est alors aussi.

On suppose $\sum_{k=1}^n k = 1 + 2 + \dots + n = \frac{n(n+1)}{2}$, et on sait que :

$$\sum_{k=1}^{n+1} k = 1 + 2 + \dots + n + (n+1) = \left(\sum_{k=1}^n k \right) + (n+1)$$

Donc d'après l'hypothèse de récurrence :

$$\begin{aligned} \sum_{k=1}^{n+1} k &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2} \\ &= \frac{(n+1)(n+1+1)}{2} \end{aligned}$$

et donc $\mathcal{P}(n+1)$ est vraie.

La propriété $\mathcal{P}(n)$ est donc vraie pour tout $n \geq 1$. CQFD.

Récurrence d'ordre p :

la récurrence d'ordre p suit le même principe que la récurrence simple, sauf qu'il faut initialiser la proposition à p rangs consécutifs : $n_0, n_0 + 1, \dots, n_0 + p - 1$, et l'hérédité consiste à supposer que pour un certain $n \geq n_0$, la proposition est vraie aux rangs $n, n+1, \dots, n+p-1$, et de montrer qu'elle est vraie au rang $n+p$. La proposition est alors vraie pour tous les rangs $n \geq n_0$.

Exemple 15 Récurrence d'ordre 2 : Montrer que la suite de Fibonacci définie par

$$\begin{cases} u_0 &= 1 \\ u_1 &= 1 \\ u_{n+2} &= u_{n+1} + u_n \end{cases}$$

s'exprime de manière explicite par

$$\forall n \geq 0, u_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^{n+1}$$

Récurrence forte :

La récurrence forte suit le principe de la récurrence simple : On initialise à un certain rang n_0 , par contre pour l'hérédité, on suppose que la propriété est vraie à **tous les rangs précédents**.

Exemple 16 Montrer en utilisant la récurrence forte que tout nombre entier supérieur ou égal à 2 est divisible par un nombre premier.

DÉMONSTRATION PAR DISJONCTION DE CAS

Soient E un ensemble, et $\mathcal{P}$ un prédicat sur E . On veut démontrer que $\forall x \in E, \mathcal{P}(x)$ est vraie. Une démonstration par disjonction des cas consiste à trouver des sous-ensembles $E_1, \dots, E_n$ de E tels que :

- (1) $E = E_1 \cup \dots \cup E_n$
- (2) pour tout $i \in \{1, \dots, n\}$, l'assertion $\forall x \in E_i, \mathcal{P}(x)$ est vraie.

Alors l'assertion $\forall x \in E, \mathcal{P}(x)$ est vraie.

Dans la pratique, cette méthode consiste à montrer que $\mathcal{P}(x)$ est vraie quand x vérifie certaines hypothèses supplémentaires, puis que chaque élément de E vérifie l'une au moins de ces hypothèses.

Exemple 17 Montrons par disjonction de cas que

pour tout entier naturel n , $n^3 - n$ est pair.

On peut toujours écrire : $n^3 - n = n(n^2 - 1) = n(n - 1)(n + 1)$.

- Si n est pair, alors le produit est pair (car n est facteur).
- Si n est impair, alors $n + 1$ est pair, et donc le produit est pair.

Comme n est forcément pair ou impair et que la propriété est démontrée dans les deux cas, alors elle est montrée pour tout n .

II. Notions ensemblistes

L'objectif des mathématiques est d'explorer l'intuition que nous avons d'un certain nombre d'objets abstraits (comme les nombres ou les fonctions continues), ce qui nous permet d'en déduire de nouvelles propriétés de ces objets.

Il existe bien sûr une grande variété d'objets mathématiques, dont certains sont de nature ensembliste, et d'autres non. Cependant, il est agréable de constater que la théorie des ensembles fournit un cadre universel d'étude pour tous ces objets. C'est ainsi qu'on peut représenter les nombres entiers, rationnels, ou réels, par des ensembles.

A. Vocabulaire

Notation : Appartenance

Soit E un ensemble, on note :

- $x \in E$ pour « x appartient à E ».
- $x \notin E$ pour « x n'appartient à E ».

Exemple 18

- $2 \in \mathbb{R}$
- $i \in \mathbb{C}$
- $\sqrt{2} \notin \mathbb{Q}$

Définition 7

- L'**ensemble vide** est l'ensemble qui ne contient aucun élément. On le note $\emptyset$.
- On appelle **singleton** un ensemble E à un élément. On le note $\{a\}$, où a est l'unique élément de E .

Exemple 19

- De manière générale, quand on décrit un ensemble à partir de ses éléments, on note l'ensemble avec des accolades qui contiennent les éléments, séparés par des virgules.

$$\{1, 3, 7, 8\} \quad \{i, e\} \quad \{\pi\}.$$

L'ordre dans lequel on a énuméré les éléments ne joue aucun rôle, ainsi on a $\{1, 3, 7, 8\} = \{3, 7, 8, 1\}$.

- On peut s'autoriser des raccourcis : $\{1, 2, \dots, 48\}$.

L'ensemble des entiers naturels se note $\mathbb{N} = \{0, 1, 2, \dots\}$.

- À partir d'ensembles connus il y a plusieurs façons de définir de nouveaux ensembles plus subtils. Par exemple on peut définir l'ensemble des entiers pairs par $\{2n, n \in \mathbb{Z}\}$ ou par $\{n \in \mathbb{Z} \mid 2 \text{ divise } n\}$.

Définition 8

A est **une partie** de E si

$$\forall x \in A, x \in E.$$

On note $A \subset E$, ou encore $E \supset A$.

Exemple 20

- Remarquons tout d'abord que $E \subset E$ et $\emptyset \subset E$.
- $\mathbb{R} \subset \mathbb{C}$
- $\mathbb{N} \subset \mathbb{Q}$
- $\{0\} \subset \mathbb{R}$

B. Opérations ensemblistes

Définition 9

On note $\mathfrak{P}$ l'ensemble des parties de E . Les éléments de $\mathfrak{P}$ sont donc des ensembles.
Si $E = \emptyset$, par convention on a $\mathfrak{P} = \{\emptyset\}$.

Exemple 21 Si $E = \{0, 1, 2\}$ alors

$$\mathfrak{P}(E) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}$$

Proposition 4 (Opérations dans $\mathfrak{P}(E)$)

Si $(A, B) \in (E)^2$, on peut effectuer les opérations suivantes :

- Union : $A \cup B = \{x \in E \mid x \in A \text{ ou } x \in B\}$.
- Intersection : $A \cap B = \{x \in E \mid x \in A \text{ et } x \in B\}$.
- Complémentaire : $A^C = \{x \in E \mid x \notin A\}$.
- Privation : $A \setminus B = \{x \in E \mid x \in A \text{ et } x \notin B\} = A \cap B^C$.
- Différence symétrique $A \Delta B = (A \cup B) \setminus (A \cap B) = (A \cap B^C) \cup (B \cap A^C)$.

Proposition 5 Soient A, B et C trois parties de E , c'est à dire des éléments de $\mathfrak{P}(E)$.

— Les opérations $\cap$ et $\cup$ sont commutatives :

$$A \cap B = B \cap A \text{ et } A \cup B = B \cup A$$

et associatives :

$$A \cap (B \cap C) = (A \cap B) \cap C = A \cap B \cap C \text{ et } A \cup (B \cup C) = (A \cup B) \cup C = A \cup B \cup C$$

— L'opération $\cap$ est distributive par rapport à $\cup$:

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

— L'opération $\cup$ est distributive par rapport à $\cap$:

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

C. Propriétés

Proposition 6 (Lois de Morgan)

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

Exemple 22

D. Produit cartésien d'ensembles**Définition 10**

Soient E et F deux ensembles. On appelle produit cartésien de E par F , que l'on note $E \times F$ l'ensemble suivant :

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

Si $E = F$, on note $E \times E = E^2$.

Soient n ensembles quelconques $E_1, E_2, \dots, E_n$, alors :

$$E_1 \times E_2 \times \dots \times E_n = \{(x_1, x_2, \dots, x_n) \mid x_1 \in E_1, x_2 \in E_2, \dots, x_n \in E_n\}.$$

Notation

Si $E_1, E_2, \dots, E_n$ sont n ensembles, on note :

$$E_1 \times E_2 \times \dots \times E_n = \prod_{i=1}^n E_i.$$

Si $E_1 = E_2 = \dots = E_n$, on écrit

$$\underbrace{E \times E \times \dots \times E}_{n \text{ fois}} = E^n.$$

Exemple 23

III. Application

A. Premières définitions

Définition 11

On appelle application f d'un ensemble E dans un ensemble F l'objet mathématique

$$\begin{aligned} f : E &\rightarrow F \\ x &\mapsto y = f(x) \end{aligned}$$

- E est l'ensemble de définition de f (ensemble de départ).
- F est l'ensemble d'arrivée.
- Pour tout $x \in E$, $f(x)$ est défini de manière unique et s'appelle l'**image** de x par f .

Définition 12

On appelle graphe de f l'ensemble suivant :

$$\Gamma(f) = \{(x, y) \in E \times F \mid y = f(x)\} \subset E \times F.$$

B. Un exemple : la fonction caractéristique d'une partie d'un ensemble

Définition 13

Soit E un ensemble et $A \in \mathfrak{P}(E)$, on définit la fonction caractéristique de A comme l'application $\mathbf{1}_A$ (parfois aussi notée χ_A) définie par :

$$\begin{aligned} \mathbf{1}_A : E &\rightarrow \{0, 1\} \\ x \in A &\mapsto 1 \\ x \notin A &\mapsto 0 \end{aligned}$$

Proposition 7

- $\mathbf{1}_{A^c} = \mathbf{1}_E - \mathbf{1}_A$
- $\mathbf{1}_{A \cup B} = \mathbf{1}_A + \mathbf{1}_B - \mathbf{1}_A \times \mathbf{1}_B$
- $\mathbf{1}_{A \cap B} = \mathbf{1}_A \times \mathbf{1}_B$
- $\mathbf{1}_{A \Delta B} = (\mathbf{1}_A - \mathbf{1}_B)^2$

Définition 14

On note F^E l'ensemble des applications de $E \rightarrow F$. L'application

$$\begin{aligned} \mathfrak{P}(E) &\rightarrow \{0, 1\}^E \\ A &\mapsto \mathbf{1}_A \end{aligned}$$

On peut utiliser cette bijection pour prouver le résultat suivant :

Proposition 8 Soit E un ensemble.

$(\mathfrak{P}(E), \Delta)$ est un groupe.

C. Application injective, surjective, bijective

Définition 15

$f : E \longrightarrow F$ est une application injective si

$$\forall (x, y) \in E^2, f(x) = f(y) \Rightarrow x = y.$$

f est non injective s'écrit donc

$$\exists (x, y) \in E^2, x \neq y \text{ et } f(x) = f(y).$$

Une application injective s'appelle aussi une injection.

Exemple 24 L'application

$$\begin{aligned} f : \mathbb{R}^+ &\rightarrow \mathbb{R} \\ x &\mapsto x^2 \end{aligned}$$

est injective mais l'application

$$\begin{aligned} g : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto x^2 \end{aligned}$$

n'est pas injective.

Définition 16

$f : E \longrightarrow F$ est une application surjective si

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

x est appelé **antécédent** de y par f . Une application surjective s'appelle aussi une surjection.

Exemple 25 L'application

$$\begin{aligned} f : \mathbb{R} &\rightarrow \mathbb{R}^+ \\ x &\mapsto x^2 \end{aligned}$$

est surjective mais l'application

$$\begin{aligned} g : \mathbb{R}^+ &\rightarrow \mathbb{R} \\ x &\mapsto x^2 \end{aligned}$$

n'est pas surjective.

Définition 17

Une application $f : E \longrightarrow F$ est bijective si elle est à la fois injective et surjective :

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

On définit ainsi lorsque f est bijective une nouvelle application :

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

f^{-1} s'appelle l'**application réciproque** de f .

f^{-1} est aussi une bijection et

$$(f^{-1})^{-1} = f.$$

D. Composition d'application**Définition 18**

Soient E, F et G trois ensembles, et

$$\begin{aligned} f : E &\longrightarrow F \\ g : F &\longrightarrow G \end{aligned}$$

On définit l'application $g \circ f$ par

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

$$E \xrightarrow{f} F \xrightarrow{g} G \underbrace{\qquad}_{g \circ f}$$

Proposition 9 $\circ$ est une loi de composition interne **associative**, c'est à dire que si

$$f : E \longrightarrow F, \quad g : F \longrightarrow G, \quad h : G \longrightarrow H$$

alors $(h \circ g) \circ f = h \circ (g \circ f)$. On peut donc omettre les parenthèses et écrire $h \circ g \circ f$.

$$E \xrightarrow{f} F \xrightarrow{g} G \xrightarrow{h} H \underbrace{\qquad}_{h \circ g \circ f}$$

Proposition 10

- La composition de deux injections est une injection.
- La composition de deux surjections est une surjection.
- La composition de deux bijections est une bijection.

Proposition 11 Soit $f : E \longrightarrow F$ et $g : F \longrightarrow G$.

- Si $g \circ f$ est injective, alors f est injective.
- Si $g \circ f$ est surjective, alors g est surjective.

Définition 19

Soit E un ensemble, on définit l'application « identité de E », notée Id_E par

$$\begin{aligned}\text{Id}_E : E &\longrightarrow E \\ x &\longmapsto x\end{aligned}$$

Proposition 12 Pour qu'une application $f : E \longrightarrow F$ soit bijective, il faut et il suffit qu'il existe une application $g : F \longrightarrow E$ telle que

$$f \circ g = \text{Id}_F \quad \text{et} \quad g \circ f = \text{Id}_E.$$

Dans ce cas, g est unique et $g = f^{-1}$.

Proposition 13 Soit $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux bijections, alors

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

« La bijection réciproque de la composée est la composée des bijections réciproques, mais dans l'autre sens. »

E. Image directe, image réciproque

Dans toute cette partie, on considère une application $f : E \longrightarrow F$.

Définition 20

- Soit $A \subset E$, on appelle image directe de A par f la partie de F définie par

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

- Soit $B \subset F$, on appelle image réciproque de B par f la partie de E définie par

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

Exemple 26

- $\sin\left(\left[-\frac{\pi}{2}; \frac{\pi}{2}\right]\right) = [-1, 1].$
- $\sin^{-1}\left(\left\{\frac{1}{2}\right\}\right) = \left\{\frac{\pi}{6} + 2k\pi, k \in \mathbb{Z}\right\} \cup \left\{\frac{5\pi}{6} + 2k\pi, k \in \mathbb{Z}\right\}.$
- $\sin^{-1}(\{2\}) = \emptyset.$

Remarque 8**ATTENTION :**

La notation $f^{-1}(B)$ ne signifie pas que f est bijective ! L'image réciproque d'un sous-ensemble de l'espace d'arrivée est toujours définie indépendamment du fait que f^{-1} soit définie.

Proposition 14 Soit $f : E \longrightarrow F$, alors

$$f \text{ surjective} \implies f(E) = F.$$

Proposition 15 (Propriétés des images directes et réciproques)

Soit $f : E \longrightarrow F$, $(A, B) \in \mathfrak{P}(E)^2$ et $(A', B') \in \mathfrak{P}(F)^2$:

Images réciproques	Images directes
$A' \subset B' \Rightarrow f^{-1}(A') \subset f^{-1}(B')$	$A \subset B \Rightarrow f(A) \subset f(B)$
$f^{-1}(A' \cup B') = f^{-1}(A') \cup f^{-1}(B')$	$f(A \cup B) = f(A) \cup f(B)$
$f^{-1}(A' \cap B') = f^{-1}(A') \cap f^{-1}(B')$	$f(A \cap B) \subset f(A) \cap f(B)$
$f^{-1}(A'^C) = f^{-1}(A')^C$	$f(A^C)$ aucune relation $f(A)^C$

F. Restriction et prolongement**Définition 21**

- Soit $f : E \longrightarrow F$ une application et A une partie de E .
On appelle **restriction** de f à A l'application notée $f|_A$ définie par

$$\begin{aligned} f|_A : A &\longrightarrow F \\ x &\longmapsto f(x). \end{aligned}$$

- Soit $G \supset E$, on appelle **prolongement** de f à G toute application

$$g : G \longrightarrow F$$

telle que $g|_E = f$.

- Soit $f : E \longrightarrow E$ et $A \subset E$ stable par f , c'est à dire telle que $f(A) \subset A$.
On appelle **application induite** par f sur A l'application définie par

$$\begin{aligned} f_{//A} : A &\longrightarrow A \\ x &\longmapsto f(x). \end{aligned}$$

Remarque 9

- La restriction de f à A est unique.
- Un prolongement de f à G n'est, en général, pas unique.
- Une application induite $f_{//A}$ ne peut être définie que si A est stable par f .

Exemple 27

- Soit :

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto x^2 \end{aligned}$$

alors la restriction de f à $\mathbb{R}^+$ est l'application

$$\begin{aligned} f : \mathbb{R}^+ &\longrightarrow \mathbb{R} \\ x &\longmapsto x^2 \end{aligned}$$

- Les applications

$$\begin{aligned} g_1 : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto x^3 \end{aligned}$$

et

$$\begin{aligned} g_2 : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto |x|^3 \end{aligned}$$

sont deux prolongements de l'application

$$\begin{aligned} f : \mathbb{R}^+ &\longrightarrow \mathbb{R} \\ x &\longmapsto x^3 \end{aligned}$$

- Soit $n \in \mathbb{N}$, on considère l'application

$$\begin{aligned} f_n : \mathbb{R}^+ &\longrightarrow \mathbb{R} \\ x &\longmapsto x^n \end{aligned}$$

L'ensemble $[0, 1]$ est stable par f_n , on peut donc définir l'application induite $f_{n//[0,1]}$:

$$\begin{aligned} f_{n//[0,1]} : [0, 1] &\longrightarrow \mathbb{R} \\ x &\longmapsto x^n \end{aligned}$$

G. Famille

Soit E un ensemble quelconque et I un ensemble. On appelle famille d'éléments de E indexée par I toute application

$$\begin{aligned} I &\longrightarrow E \\ i &\longmapsto x_i \end{aligned}$$

On note cette famille $(x_i)_{i \in I}$.

Exemple 28 $I = \mathbb{N}$ et $E = \mathbb{R}$, on a

$$\begin{aligned} \mathbb{N} &\longrightarrow \mathbb{R} \\ n &\longmapsto x_n \end{aligned}$$

$(x_n)_{n \in \mathbb{N}}$ est une suite réelle de terme général x_n .

Remarque 10**Attention :**

Ne pas confondre $(x_i)_{i \in I}$ qui est une application de I dans E , et $\{x_i, i \in I\}$ qui est un ensemble.

Définition 22

Soit $(A_i)_{i \in I}$ une famille de parties de E , on définit :

- $\bigcup_{i \in I} A_i = \{x \in E, \exists i \in I, x \in A_i\}$.
- $\bigcap_{i \in I} A_i = \{x \in E, \forall i \in I, x \in A_i\}$.
- On note E^I l'ensemble des suites d'éléments de E indexées par I qui est donc aussi l'ensemble des applications de $I \longrightarrow E$.
Par exemple $\mathbb{R}^{\mathbb{N}}$ est l'ensemble des suites réelles.

Définition 23

Soit E un ensemble, et $(A_i)_{i \in I}$ une famille de parties de E .

On dit que la famille $(A_i)_{i \in I}$ définit une **partition de E** si

1. $\forall i \in I, A_i \neq \emptyset$;
2. $\forall i \neq j, A_i \cap A_j = \emptyset$;
3. $\bigcup_{i \in I} A_i = E$.

Exemple 29

- La famille à deux éléments formée par les nombres pairs et les nombres impairs forme une partition de $\mathbb{Z}$.
- Les pièces d'un puzzle forment une partition du puzzle entier.
- Si E est un ensemble, la famille $(\{x\})_{x \in E}$ forme une partition de E , ainsi que la famille réduite au seul ensemble E .

IV. Relation d'équivalence

Dans toute cette partie, E désigne un ensemble.

A. Notion de relation

Définition 24

Une **relation binaire** sur l'ensemble E est un prédicat sur $E \times E$.

Autrement dit, une relation est une assertion qui dépend de deux variables prises dans E .

Intuitivement, une relation sur E est un procédé qui permet de comparer deux éléments de l'ensemble E . Pour exprimer que deux éléments x et y de E satisfont la relation $\mathcal{R}$, on notera $x\mathcal{R}y$ au lieu de $\mathcal{R}(x, y)$.

Exemple 30

- a) Sur tout ensemble E , l'égalité est une relation binaire.
- b) Sur $\mathbb{R}$, « $x < y$ » est une relation binaire.
- c) Sur $\mathbb{N}$, « p divise q » est une relation binaire.

B. Relation d'équivalence

Définition 25

Soit $\mathcal{R}$ une relation binaire sur E .

On dit que $\mathcal{R}$ est une **relation d'équivalence** si les propositions suivantes sont vérifiées :

- (1) $\mathcal{R}$ est **réflexive** : $\forall x \in E, x\mathcal{R}x$
- (2) $\mathcal{R}$ est **symétrique** : $\forall (x, y) \in E^2, x\mathcal{R}y \Rightarrow y\mathcal{R}x$
- (3) $\mathcal{R}$ est **transitive** : $\forall (x, y, z) \in E^3, (x\mathcal{R}y \wedge y\mathcal{R}z) \Rightarrow x\mathcal{R}z$

Une relation d'équivalence a des propriétés semblables à la relation d'égalité. On peut voir une telle relation comme étant un « critère de ressemblance » entre deux objets.

Exemple 31

- a) Sur tout ensemble E , l'égalité est une relation d'équivalence.
- b) Si E est un ensemble et $(A_i)_{i \in I}$ est une partition de E , alors la relation binaire $\mathcal{R}$ définie par :

$$x\mathcal{R}y \Leftrightarrow \exists i \in I, x \in A_i \text{ et } y \in A_i$$

est une relation d'équivalence.

- c) La congruence modulo $\alpha \neq 0$ est une relation d'équivalence.
- d) Sur l'ensemble des mots de la langue française, la relation « x et y commencent par la même lettre » est une relation d'équivalence.
- e) Sur l'ensemble des êtres humains, la relation « x et y ont le même âge » est une relation d'équivalence.
- f) Voici un dernier exemple, dont nous reparlerons plus tard dans l'année.

Soit $\mathcal{D}$ une partie de $\mathbb{R}$, et soit $x_0 \in \overline{\mathcal{D}}$. Sur l'ensemble des fonctions $\mathcal{D} \rightarrow \mathbb{R}$, la relation « $f \underset{x_0}{\sim} g$ » est une relation d'équivalence.

C. Exemple fondamental : congruence dans $\mathbb{Z}$

Si une relation d'équivalence constitue un critère de ressemblance, alors il est naturel de regrouper en paquets les éléments qui se ressemblent.

Définition 26

Soit $\mathcal{R}$ une relation d'équivalence sur E , et soit $x \in E$.

On appelle **classe d'équivalence** de x pour $\mathcal{R}$, et on note $Cl_{\mathcal{R}}(x)$, l'ensemble $\{y \in E | x\mathcal{R}y\}$. Quand il n'y aura pas de confusion possible, on notera $Cl(x)$ au lieu de $Cl_{\mathcal{R}}(x)$.

Théorème 1

Soit $\mathcal{R}$ une relation d'équivalence sur E . Alors l'ensemble des classes d'équivalence d'éléments de E pour $\mathcal{R}$ forme une partition de E .

Exemple 32 La partition de l'ensemble des mots en classes d'équivalence pour la relation « x et y commencent par la même lettre » coïncide avec le découpage des dictionnaires.

Définition 27

Soit $n > 0$ un entier naturel. Si a et b sont deux entiers relatifs, on dit que a est congru à b modulo n , et on note

$$a \equiv b [n]$$

si $a - b$ est divisible par n .

Proposition 16 Soit $n > 0$ un entier naturel fixé. Alors la relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

Exemple 33 On prend $E = \mathbb{Z}$ et comme relation d'équivalence la congruence modulo 5. On a alors 5 classes d'équivalence :

$$\begin{aligned} Cl(0) &= \{5p, p \in \mathbb{Z}\} = 5\mathbb{Z} \\ Cl(1) &= \{5p + 1, p \in \mathbb{Z}\} = 1 + 5\mathbb{Z} \\ Cl(2) &= \{5p + 2, p \in \mathbb{Z}\} = 2 + 5\mathbb{Z} \\ Cl(3) &= \{5p + 3, p \in \mathbb{Z}\} = 3 + 5\mathbb{Z} \\ Cl(4) &= \{5p + 4, p \in \mathbb{Z}\} = 4 + 5\mathbb{Z} \end{aligned}$$

C'est une façon de partitionner l'ensemble $\mathbb{Z}$ des entiers relatifs.

Remarque 11

On vérifie facilement que la congruence modulo n est compatible avec l'addition et la multiplication de $\mathbb{Z}$. On peut donc additionner, soustraire et multiplier les classes d'équivalence modulo n . En mathématiques, on dit que l'on peut ainsi munir l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ d'une structure d'anneau.

Table des matières

I.	Rudiments de logique	2
A.	Premiers connecteurs logiques	2
B.	Implication, équivalence, réciproque, contraposée	3
C.	Quantificateurs	5
D.	Négation et quantificateurs/Méthode pour nier une assertion	6
E.	Plusieurs quantificateurs	6
F.	Méthodes de raisonnement	7
II.	Notions ensemblistes	11
A.	Vocabulaire	11
B.	Opérations ensemblistes	12
C.	Propriétés	12
D.	Produit cartésien d'ensembles	13
III.	Application	14
A.	Premières définitions	14
B.	Un exemple : la fonction caractéristique d'une partie d'un ensemble	14
C.	Application injective, surjective, bijective	15
D.	Composition d'application	16
E.	Image directe, image réciproque	17
F.	Restriction et prolongement	18
G.	Famille	19
IV.	Relation d'équivalence	21
A.	Notion de relation	21
B.	Relation d'équivalence	21
C.	Exemple fondamental : congruence dans $\mathbb{Z}$	21