Mathématiques 2012–2013

Cours d'Algèbre 1 : Structures mathématiques

Simon RAULOT,
Université de Rouen
Laboratoire de Mathématiques Raphaël Salem,
Avenue de l'Université, BP.12,
F76801 Saint-Étienne-du-Rouvray.

Rédigé avec LaTeX
par Hicham AMARIR
le 11 mai 2026

Table des matières

Chapitre 1

Logiques Élémentaires

1.1 Introduction et lexique

1.1.1 But du cours

Le but du cours est double :

① Acquérir le raisonnement mathématique.

② Maîtriser le langage mathématique.

1.1.2 Objet mathématique et définition

Définition 1.1 : (*Objet mathématique*)

On appelle ***objet mathématique*** tous les objets qui interviennent en mathématique.

Ce sont des choses que l'on nomme et que l'on définit par des propriétés qu'ils satisfont.

Exemple :

- $\mathbb{N}$ est l'ensemble des entiers.
- Un cercle est l'ensemble des points du plan qui sont équidistants d'un point donné.

1.1.3 Énoncé mathématique

Elle consiste en la donné d'une propriété concernant des objets mathématiques.

Exemples :

① Théorème de Pythagore.

② Théorème de Fermat :

Si $n \geqslant 3$ avec $n \in \mathbb{N}$, alors :

$$x^n + y^n = z^n$$

ne possède pas de solutions entières x, y, z non toutes nulles.

1.1.4 Théorie Mathématique

Définition 1.2 : (*Axiome*)

Un ***axiome*** est un énoncé mathématique (assertion) que l'on suppose vraie par évidence sans avoir besoin d'être démontré.

Exemple :

Dans la géométrie dans le plan, il y a les Axiomes d'Euclide.

La construction des entiers naturels est l'Axiome de Peano.

Convention 1.3 : (*Axiome du tiers exclu*)

⚠**Principe de non-contradiction :** Une assertion ne peut pas être vraie et fausse à la fois.

$\Longrightarrow$ ⚠**Principe du tiers exclu :** Si une assertion n'est pas vraie, alors elle est forcément fausse et inversement.

Autrement dit : une assertion est soit vraie, soit fausse, il n'y a pas de troisième possibilité (d'où le nom "tiers exclu") :

Schématiquement :

$$\text{Axiome} \xrightarrow{\text{Règle logique}} \text{Nouveau énoncé}$$

Terminologie :

- Assertion importante → Théorème
- Assertion moins importante → Propriété
- Assertion intermédiaire qui permet de démontrer un théorème → Lemme
- Assertion qui découle directement d'un théorème → Corolaire

1.2 Connecteurs logiques

Définition 1.4 : (*Connecteur logique*)

On appelle ***connecteur logique*** un type d'opération agissant sur les assertions pour en construire une nouvelle.

Définition 1.5 : (*Logique mathématique*)

On appelle ***logique mathématique*** la description de la manipulation de ces opérations et ce, quelle que soit la véracité des assertions simples qui la composent.

1.2.1 Table de vérité

Définition 1.6 : (*Table de vérité*)

On appelle ***table de vérité*** un tableau qui donne la valeur de vérité (Vrai ou Faux) d'une assertion composée en fonction des valeurs de vérité des assertions simples qui la composent.

Exemple :

Soient P et Q deux assertions simples.

Une table de vérité de P et de Q avec un connecteur logique entre P et Q est donnée par :

P \ Q	V	F
V	?	?
F	?	?

ou encore donnée par :

P	Q	$P \bigstar Q$
V	V	?
V	F	?
F	V	?
F	F	?

avec « ? » à définir par V ou F selon le connecteur logique $\bigstar$ que l'on souhaite définir.

Définition 1.7 : (*Tautologie*)

Une construction logique qui est ***toujours vraie*** quelque soit la véracité des assertions mises en jeu s'appelle une ***tautologie***.

1.2.2 Énoncés équivalents

Soient P et Q deux énoncés.

Définition 1.8 : (*Équivalence logique*)

On dit que P et Q sont ***équivalents*** s'ils ont la même table de vérité, autrement dit, s'ils sont tous les deux vrais, soit tous les deux faux (on notera alors « $P \iff Q$ »).

Table de vérité :

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

1.2.3 Négation

Définition 1.9 : (*Négation d'une assertion*)

Soit P un assertion.

On appelle ***négation*** de P, notée $\neg P$ (ou « non P », ou enocre « $\overline{P}$ »), l'assertion qui est vraie si P est fausse, et fausse si P est vraie :

P	$\neg P$
V	F
F	V

Exemple :

i) P = « Tous les étudiants présents dans l'amphi auront leur année »

$\neg P$ = « Il existe au moins un étudiant qui n'aura pas son année »

ii) P = « n est un entier pair »

$\neg P$ = « n est un entier impair »

Propriété 1.10 : (*Double négation*)

Soit P une assertion, on a :

$$\neg(\neg P) \iff P$$

Preuve :

P	$\neg P$	$\neg(\neg P)$	$\neg(\neg P) \iff P$
V	F	V	V
F	V	F	V

Définition 1.11 : (*Raisonnement par l'absurde*)

En associant la négation et le principe de non-contradiction, on obtient le ***raisonnement par l'absurde***.

Pour démontrer qu'une assertion P est vraie, on suppose qu'elle est fausse, c'est-à-dire $\neg P$ est vraie, et on essaie d'aboutir à une contradiction.

Exemple :

On veut montrer que l'assertion P : « Il existe une infinité de nombres premiers » est vraie.

Rappel : p est premier si p est un entier naturel strictement supérieur à 1 qui n'admet aucun diviseur autre que 1 et lui-même.

Par exemple, $2, 3, 5, 7, 11, 13, \ldots$ sont des nombres premiers.

Preuve : On suppose que $\neg P$ est vraie, c'est-à-dire $\neg P$ = « Les nombres premiers sont en nombre fini ».

Puisqu'on a un nombre fini de nombres premiers, il existe un plus grand que l'on note p.

On va considérer l'entier $N = p! + 1$ (avec $p! = p \times (p-1) \times (p-2) \times \cdots \times 4 \times 3 \times 2 \times 1$).

On a : $N > p$.

Par hypothèse, N est plus grand que le plus grand des nombres premiers, donc N n'est pas premier.

Or tout entier s'écrit comme un produit de nombres premiers. Donc il existe un nombre premier qui divise N : absurde car N n'admet pas de diviseurs premiers (puisque pour tout nombre premier $q \leqslant p$, on a $q \mid p!$ donc $q \nmid p! + 1 = N$), donc N est premier.

On a donc prouvé que $\neg P$ est fausse, et donc que la proposition P est vraie.

Exemple :

Montrons que $\sqrt{2}$ est un nombre irrationnel.

On rappelle que $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Un nombre irrationnel est un nombre réel qui ne s'écrit pas sous la forme $\frac{p}{q}$ avec p un entier relatif et q un entier relatif non nul. Par exemple, π, e, ...

Preuve : Par l'absurde, on suppose que $\sqrt{2} \in \mathbb{Q}$, c'est-à-dire qu'il existe deux entiers naturels p et q tels que :

$$\sqrt{2} = \frac{p}{q} \quad \text{tel que} \quad \text{PGCD}(p;q) = 1.$$

Ici, le PGCD$(a;b)$ pour a et b des entiers, est le plus grand diviseur commun de a et b.

On a :

$$\sqrt{2} = \frac{p}{q} \quad \text{donc} \quad q\sqrt{2} = p$$

$$2q^2 = p^2$$

D'où 2 divise p^2, alors on peut montrer que 2 divise p. Donc p est pair et il existe k un entier tel que $p = 2k$. On a :

$$2q^2 = (2k)^2 = 4k^2 \quad \text{d'où} \quad q^2 = 2k^2$$

Ainsi 2 divise q^2 et donc q est pair.

Finalement, on a :

$$\text{PGCD}(p,q) \geqslant 2 \quad \begin{cases} 2 \text{ divise } p \\ 2 \text{ divise } q \end{cases}$$

Absurde car par hypothèse le PGCD de p et q vaut 1.

Donc $\sqrt{2}$ n'est pas rationnel, d'où $\sqrt{2}$ est irrationnel.

Autre type de démonstration : On « combine » la négation d'une assertion avec le principe du tiers exclu.

Exemple :

(Raisonnement par disjonction de cas)

On veut montrer que :

$$P : \text{« il existe des nombres irrationnels } a > 0 \text{ et } b > 0 \text{ tels que le nombre } a^b \text{ soit rationnel »}$$

est vraie.

Preuve : Pour démontrer que P est vraie, on va considérer l'assertion suivante :

$$Q : \text{« le nombre } \sqrt{2}^{\sqrt{2}} \text{ est rationnel »}.$$

$\Longrightarrow$ On suppose que Q est vraie :

Alors $\sqrt{2}^{\sqrt{2}}$ est rationnel et donc P est vraie car dans ce cas on peut prendre $a = b = \sqrt{2}$ qui sont bien des irrationnels et puisque Q est vraie, $a^b = \sqrt{2}^{\sqrt{2}}$ est rationnel.

Donc P est vraie.

$\Longrightarrow$ On suppose que Q est fausse, donc non Q est vraie :

Donc $\sqrt{2}^{\sqrt{2}}$ est irrationnel. Si on prend :

— $a = \sqrt{2}^{\sqrt{2}}$ (est irrationnel) > 0

— $b = \sqrt{2} > 0$

Alors :

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$$

Donc a^b est un rationnel.

Donc finalement P est vraie.

Conclusion : Dans les deux cas (qui épuisent toutes les possibilités grâce au tiers exclu), la proposition P est vraie.

1.2.4 Conjonction et disjonctions

Définition 1.12 : (*Conjonction de deux assertions*)

Soient P et Q deux assertions.

On appelle ***conjonction*** de P et Q l'assertion notée $P \wedge Q$ que l'on définit comme vraie si P et Q sont vrais, et $P \wedge Q$ fausse dans tous les autres cas de P et Q.

On lit « $P \wedge Q$ » : P **et** Q.

Table de vérité :

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

Exemple :

Si on désigne un nombre entier n :

- P = « n est un multiple de 2 »
- Q = « n est un multiple de 3 »

Alors $P \wedge Q$ est équivalent à l'assertion « n est un multiple de 6 ».

En effet, n est un multiple de 2 ET de 3 si et seulement si n est un multiple du PPCM de 2 et 3, c'est-à-dire de 6.

Propriété 1.13 : (*Idempotence de la conjonction*)

Soit P une assertion. On a :

$$P \wedge P \iff P.$$

Preuve :

Nous vérifions cette équivalence à l'aide d'une table de vérité.

P	$P \wedge P$	$P \wedge P \iff P$
V	V	V
F	F	V

La colonne finale contient uniquement des Vrai, ce qui prouve que l'équivalence est une tautologie.

Définition 1.14 : (*Disjonction de deux assertions*)

Soient P et Q deux assertions.

On appelle ***disjonction*** de P et Q l'assertion notée $P \vee Q$ que l'on définit comme vraie si au moins l'une des deux assertions P ou Q est vraie, et $P \vee Q$ fausse uniquement si P et Q sont toutes les deux fausses.

On lit « $P \vee Q$ » : P **ou** Q (le mot « ou » est utilisé en français dans le sens inclusif, c'est-à-dire que si une assertion est vraie, alors la disjonction est vraie, même si l'autre affirmation est fausse).

Table de vérité :

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

Exemple :

Pour un entier naturel n on pose :

— $P =$ « n est pair »

— $Q =$ « $n \leqslant 10$ »

Donc $P \vee Q$ est équivalent à :

« n est un entier pair ou n est un nombre impair inférieur ou égal à 10 »

Exemple :

Soit x un nombre réel.

« $x^2+2x-2>0$ » $\iff$ « $x \leqslant -1-\sqrt{3}$ » $\vee$ « $x \geqslant -1+\sqrt{3}$ »

Cela revient à résoudre sur $\mathbb{R}$ l'inéquation :

$$x^2+2x-2>0$$

On cherche les racines de $x^2+2x-2=0$.

On a $\Delta = 4-4\times 1\times(-2) = 12 > 0$.

Donc on a deux racines réelles données par :

$$x_1 = \frac{-2-\sqrt{12}}{2} = -1-\sqrt{3}$$

$$x_2 = \frac{-2+\sqrt{12}}{2} = -1+\sqrt{3}$$

Propriété 1.15 : (*Idempotence de la disjonction*)

Soit P une assertion. On a :

$$P \vee P \iff P.$$

Preuve :

Nous vérifions cette équivalence à l'aide d'une table de vérité.

P	$P \vee P$	$P \vee P \iff P$
V	V	V
F	F	V

La colonne finale contient uniquement des Vrai, ce qui prouve que l'équivalence est une tautologie.

Propriété 1.16 : (*Associativité de la disjonction*)

Soient P, Q et R trois assertions. On a :

$$(P \vee (Q \vee R)) \iff ((P \vee Q) \vee R).$$

Preuve :

(à refaire en exercice)

Nous comparons les tables de vérité des deux membres de l'équivalence.

P	Q	R	$Q \vee R$	$P \vee (Q \vee R)$	$P \vee Q$	$(P \vee Q) \vee R$	$(P \vee (Q \vee R)) \iff ((P \vee Q) \vee R)$
V	V	V	V	V	V	V	V
V	V	F	V	V	V	V	V
V	F	V	V	V	V	V	V
V	F	F	F	V	V	V	V
F	V	V	V	V	V	V	V
F	V	F	V	V	V	V	V
F	F	V	V	V	F	V	V
F	F	F	F	F	F	F	V

Les colonnes correspondant à $P \vee (Q \vee R)$ et $(P \vee Q) \vee R$ sont strictement identiques.

La colonne finale contenant uniquement des Vrai prouve l'équivalence logique.

Propriété 1.17 : (*Associativité de la conjonction*)

Soient P, Q et R trois assertions. On a :

$$(P \wedge (Q \wedge R)) \iff ((P \wedge Q) \wedge R).$$

Preuve :

(à refaire en exercice)

Nous comparons les tables de vérité des deux membres de l'équivalence.

P	Q	R	$Q \wedge R$	$P \wedge (Q \wedge R)$	$P \wedge Q$	$(P \wedge Q) \wedge R$	$(P \wedge (Q \wedge R)) \iff ((P \wedge Q) \wedge R)$
V	V	V	V	V	V	V	V
V	V	F	F	F	V	F	V
V	F	V	F	F	F	F	V
V	F	F	F	F	F	F	V
F	V	V	V	F	F	F	V
F	V	F	F	F	F	F	V
F	F	V	F	F	F	F	V
F	F	F	F	F	F	F	V

Les colonnes de $P \wedge (Q \wedge R)$ et $(P \wedge Q) \wedge R$ coïncident parfaitement.

La colonne finale valide l'équivalence logique.

Propriété 1.18 : (*Distributivité de la conjonction sur la disjonction*)

Soient P, Q et R trois assertions. On a :

$$P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R).$$

Preuve :

(à refaire en exercice)

Nous comparons les tables de vérité des deux membres de l'équivalence.

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$	$(P \wedge (Q \vee R)) \iff ((P \wedge Q) \vee (P \wedge R))$
V	V	V	V	V	V	V	V	V
V	V	F	V	V	V	F	V	V
V	F	V	V	V	F	V	V	V
V	F	F	F	F	F	F	F	V
F	V	V	V	F	F	F	F	V
F	V	F	V	F	F	F	F	V
F	F	V	V	F	F	F	F	V
F	F	F	F	F	F	F	F	V

Les colonnes de $P \wedge (Q \vee R)$ et $(P \wedge Q) \vee (P \wedge R)$ coïncident parfaitement sur les 8 cas possibles.

La colonne finale valide l'équivalence.

Propriété 1.19 : (*Distributivité de la disjonction sur la conjonction*)

Soient P, Q et R trois assertions. On a :

$$P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R).$$

Preuve :

(à refaire en exercice)

Nous comparons les tables de vérité des deux membres de l'équivalence.

P	Q	R	$Q \wedge R$	$P \vee (Q \wedge R)$	$P \vee Q$	$P \vee R$	$(P \vee Q) \wedge (P \vee R)$	$(P \vee (Q \wedge R)) \iff ((P \vee Q) \wedge (P \vee R))$
V	V	V	V	V	V	V	V	V
V	V	F	F	V	V	V	V	V
V	F	V	F	V	V	V	V	V
V	F	F	F	V	V	V	V	V
F	V	V	V	V	V	V	V	V
F	V	F	F	F	V	F	F	V
F	F	V	F	F	F	V	F	V
F	F	F	F	F	F	F	F	V

Les colonnes correspondant à $P \vee (Q \wedge R)$ et $(P \vee Q) \wedge (P \vee R)$ sont strictement identiques.

La dernière colonne, remplie uniquement de Vrai, confirme l'équivalence logique.

Propriété 1.20 : (*Commutativité de la conjonction*)

Soient P et Q deux assertions.

On a l'équivalence :

$$P \wedge Q \iff Q \wedge P$$

Preuve :

Nous vérifions cette équivalence à l'aide d'une table de vérité.

P	Q	$P \wedge Q$	$Q \wedge P$	$(P \wedge Q) \iff (Q \wedge P)$
V	V	V	V	V
V	F	F	F	V
F	V	F	F	V
F	F	F	F	V

Les colonnes de $P \wedge Q$ et $Q \wedge P$ sont strictement identiques. La dernière colonne, remplie uniquement de Vrai, confirme l'équivalence logique.

Propriété 1.21 : (*Commutativité de la disjonction*)

Soient P et Q deux assertions.

On a l'équivalence :

$$P \vee Q \iff Q \vee P$$

Preuve :

Nous vérifions cette équivalence à l'aide d'une table de vérité.

P	Q	$P \vee Q$	$Q \vee P$	$(P \vee Q) \iff (Q \vee P)$
V	V	V	V	V
V	F	V	V	V
F	V	V	V	V
F	F	F	F	V

Les colonnes de $P \vee Q$ et $Q \vee P$ coïncident parfaitement. La colonne finale valide ainsi l'équivalence logique.

Propriété 1.22 : (*Lois de De Morgan*)

Soient P et Q deux assertions, alors :

i) $\neg(P \vee Q) \iff (\neg P) \wedge (\neg Q)$

ii) $\neg(P \wedge Q) \iff (\neg P) \vee (\neg Q)$

Preuve :

Preuve du i)

P	Q	$\neg P$	$\neg Q$	$P \vee Q$	$\neg(P \vee Q)$	$(\neg P) \wedge (\neg Q)$	$\neg(P \vee Q) \iff (\neg P) \wedge (\neg Q)$
V	V	F	F	V	F	F	V
V	F	F	V	V	F	F	V
F	V	V	F	V	F	F	V
F	F	V	V	F	V	V	V

Donc finalement :

$$\neg(P \vee Q) \iff (\neg P) \wedge (\neg Q)$$

Preuve du ii)

P	Q	$\neg P$	$\neg Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$(\neg P) \vee (\neg Q)$	$\neg(P \wedge Q) \iff (\neg P) \vee (\neg Q)$
V	V	F	F	V	F	F	V
V	F	F	V	F	V	V	V
F	V	V	F	F	V	V	V
F	F	V	V	F	V	V	V

Donc finalement :

$$\neg(P \wedge Q) \iff (\neg P) \vee (\neg Q)$$

1.2.5 Implication

L'***implication*** est un connecteur logique essentiel car à la base du raisonnement déductif.

Ce connecteur est la traduction de « Si ... , alors ... ».

Définition 1.23 : (*Implication ($\Longrightarrow$)*)

Soient P et Q deux assertions.

On dit que « P ***implique*** Q » et on note « $P \Longrightarrow Q$ » si :

P	Q	$P \Longrightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

Propriété 1.24 : (*Fausseté d'une implication*)

Pour montrer qu'une implication $P \Longrightarrow Q$ est fausse, il suffit de démontrer que l'assertion de départ P est vraie et que l'assertion d'arrivée Q est fausse.

Preuve :

D'après la table de vérité de la définition 1.23, l'assertion $P \Longrightarrow Q$ n'est fausse que dans un seul cas : lorsque P est vraie et Q est fausse (deuxième ligne du tableau). Ainsi, pour établir la fausseté d'une implication, il suffit de vérifier cette unique configuration.

Propriété 1.25 : (*Caractérisation de l'équivalence logique*)

Soient P et Q deux assertions.

On a l'équivalence fondamentale :

$$(P \Longleftrightarrow Q) \Longleftrightarrow \big((P \Longrightarrow Q) \wedge (Q \Longrightarrow P)\big)$$

Autrement dit, démontrer une équivalence revient à démontrer une double implication : l'implication directe et sa réciproque.

Preuve :

Nous allons vérifier cette équivalence à l'aide d'une table de vérité.

P	Q	$P \Longrightarrow Q$	$Q \Longrightarrow P$	$(P \Longrightarrow Q) \wedge (Q \Longrightarrow P)$	$P \Longleftrightarrow Q$	$(P \Longleftrightarrow Q) \Longleftrightarrow ((P \Longrightarrow Q) \wedge (Q \Longrightarrow P))$
V	V	V	V	V	V	V
V	F	F	V	F	F	V
F	V	V	F	F	F	V
F	F	V	V	V	V	V

Les colonnes correspondant à $P \Longleftrightarrow Q$ et $(P \Longrightarrow Q) \wedge (Q \Longrightarrow P)$ sont strictement identiques. La dernière colonne, remplie uniquement de Vrai, confirme l'équivalence logique.

Propriété 1.26 : (*Simplification de la conjonction*)

Soient P et Q deux assertions.

Si P et Q sont vraies simultanément, alors P est nécessairement vraie :

$$(P \wedge Q) \implies P$$

Preuve :

Nous vérifions cette implication à l'aide d'une table de vérité.

P	Q	$P \wedge Q$	$(P \wedge Q) \implies P$
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	V

La colonne finale contient uniquement des Vrai, ce qui prouve que l'implication est une tautologie.

Propriété 1.27 : (*Affaiblissement par disjonction*)

Soient P et Q deux assertions.

Si P est vraie, alors l'assertion "P ou Q" est également vraie :

$$P \implies (P \vee Q)$$

Preuve :

Nous vérifions cette implication à l'aide d'une table de vérité.

P	Q	$P \vee Q$	$P \implies (P \vee Q)$
V	V	V	V
V	F	V	V
F	V	V	V
F	F	F	V

La colonne finale contient uniquement des Vrai, ce qui prouve que l'implication est une tautologie.

Propriété 1.28 : (*Loi de l'implication matérielle*)

Soient P et Q deux assertions.

L'implication peut se reformuler à l'aide de la négation et de la disjonction :

$$(P \implies Q) \iff (\neg P \vee Q)$$

Autrement dit, démontrer une implication revient à montrer que soit l'hypothèse P est fausse, soit la conclusion Q est vraie.

En pratique, cela signifie qu'il est impossible d'avoir P vraie et Q fausse simultanément.

Preuve :

Pour établir cette loi, nous comparons les tables de vérité des deux membres.

P	Q	$\neg P$	$\neg P \vee Q$	$P \Longrightarrow Q$	$(\neg P \vee Q) \Longleftrightarrow (P \Longrightarrow Q)$
V	V	F	V	V	V
V	F	F	F	F	V
F	V	V	V	V	V
F	F	V	V	V	V

Les colonnes correspondant à $\neg P \vee Q$ et $P \Longrightarrow Q$ sont strictement identiques sur les quatre cas possibles. La dernière colonne valide ainsi l'équivalence logique.

Propriété 1.29 : (*Raisonnement par inférence (Modus Ponens)*)

Soient P et Q deux assertions, alors :

$$P \wedge (P \Longrightarrow Q) \Longrightarrow Q$$

est une tautologie.

Autrement dit, si l'on sait que P est vraie et que l'implication $P \Longrightarrow Q$ a été démontrée, alors on peut en déduire avec certitude que Q est vraie. Ce mécanisme est le fondement du raisonnement déductif : il permet de passer d'une hypothèse vérifiée à une conclusion nécessaire, et structure l'enchaînement de la plupart des théorèmes.

Preuve :

Nous allons vérifier que l'assertion est une tautologie en dressant sa table de vérité complète.

P	Q	$P \Longrightarrow Q$	$P \wedge (P \Longrightarrow Q)$	$(P \wedge (P \Longrightarrow Q)) \Longrightarrow Q$
V	V	V	V	V
V	F	F	F	V
F	V	V	F	V
F	F	V	F	V

1. La 3e colonne calcule l'implication $P \Longrightarrow Q$.
2. La 4e colonne calcule la conjonction de P avec cette implication (c'est l'hypothèse du raisonnement).
3. La dernière colonne évalue l'implication finale.

Puisque la dernière colonne ne contient que des **Vrai** (V), l'assertion est toujours vraie, quelle que soit la valeur de vérité de P et Q. C'est donc bien une tautologie.

Propriété 1.30 : (*Transitivité*)

Soient P, Q et R trois assertions, alors :

$$((P \Longrightarrow Q) \wedge (Q \Longrightarrow R)) \Longrightarrow (P \Longrightarrow R)$$

Cela illustre le découpage d'une démonstration en étapes :

si P implique Q et que Q implique R, alors on peut conclure que P implique R.

C'est un principe fondamental du raisonnement logique, qui permet de construire des chaînes d'implications pour établir des résultats plus complexes à partir de résultats plus simples.

Preuve :

Nous allons démontrer que cette assertion est une tautologie à l'aide d'une table de vérité.

P	Q	R	$P \Longrightarrow Q$	$Q \Longrightarrow R$	$(P \Longrightarrow Q) \wedge (Q \Longrightarrow R)$	$P \Longrightarrow R$	**Transitivité**
V	V	V	V	V	V	V	V
V	V	F	V	F	F	F	V
V	F	V	F	V	F	V	V
V	F	F	F	V	F	F	V
F	V	V	V	V	V	V	V
F	V	F	V	F	F	V	V
F	F	V	V	V	V	V	V
F	F	F	V	V	V	V	V

1. Les colonnes 4 et 5 calculent les implications intermédiaires.
2. La colonne 6 représente l'hypothèse (les deux implications doivent être vraies).
3. La colonne 7 représente la conclusion.
4. La dernière colonne vérifie : Hypothèse $\Longrightarrow$ Conclusion.

Puisque la colonne finale ne contient que des **Vrai**, l'assertion est une tautologie.

Propriété 1.31 : (*Négation d'une implication*)

Soient P et Q deux assertions, alors :

$$\neg(P \Longrightarrow Q) \Longleftrightarrow (P \wedge \neg Q)$$

Preuve :

Il n'est pas toujours nécessaire de faire une table de vérité complète pour prouver une équivalence logique.

Nous pouvons utiliser les propriétés déjà établies pour transformer l'expression de la négation de l'implication et montrer qu'elle est équivalente à $P \wedge \neg Q$.

En effet, en utilisant la propriété 1.28, on a :

$$(P \Longrightarrow Q) \Longleftrightarrow (\neg P \vee Q)$$

d'où en appliquant la négation à chaque membre on a :

$$\begin{aligned} \neg(P \Longrightarrow Q) &\Longleftrightarrow \neg(\neg P \vee Q) && \text{(Loi de l'implication matérielle 1.28)} \\ &\Longleftrightarrow (\neg(\neg P)) \wedge (\neg Q) && \text{(Lois de De Morgan 1.22)} \\ &\Longleftrightarrow P \wedge (\neg Q) && \text{(Double négation 1.10)} \end{aligned}$$

Propriété 1.32 : (*Contraposition*)

Soient P et Q deux assertions.

L'implication « $P \Longrightarrow Q$ » est logiquement équivalente à sa ***contraposée*** $\neg Q \Longrightarrow \neg P$:

$$(P \Longrightarrow Q) \Longleftrightarrow (\neg Q \Longrightarrow \neg P).$$

Autrement dit, pour démontrer que P implique Q, il est tout aussi valide de démontrer que si Q est fausse, alors P est forcément fausse.

Preuve :

Nous allons prouver cette équivalence en transformant le membre de droite (la contraposée) pour retrouver le membre de gauche, à l'aide des propriétés précédentes.

$$\begin{aligned}
\neg Q \implies \neg P &\iff \neg(\neg Q) \vee \neg P && \text{(Loi de l'implication matérielle 1.28)}\\
&\iff Q \vee \neg P && \text{(Double négation 1.10)}\\
&\iff \neg P \vee Q && \text{(Commutativité de la disjonction 1.21)}\\
&\iff P \implies Q && \text{(Loi de l'implication matérielle 1.28)}
\end{aligned}$$

L'implication et sa contraposée ont donc exactement la même valeur de vérité.

Exemple :

(Démonstration par contraposition)

Soient :

— P : « n^2 est un entier pair »

— Q : « n est un entier pair »

On veut démontrer que $(P \implies Q)$ est vraie.

On va le montrer par contraposée, c'est-à-dire : $(\neg Q \implies \neg P)$.

On suppose que $\neg Q$ est vraie, c'est-à-dire :

$$\neg Q : \text{« } n \text{ est un entier impair »}$$

Et on veut montrer que $\neg P$ est vraie, c'est-à-dire que n^2 est un entier impair.

On suppose que n est impair donc il existe k un entier tel que $n = 2k+1$, alors :

$$\begin{aligned}
n^2 &= (2k+1)^2\\
n^2 &= 4k^2 + 4k + 1\\
n^2 &= 2(2k^2 + 2k + 1) + 1
\end{aligned}$$

d'où n^2 est impair.

$(\neg Q \implies \neg P)$ est vraie donc par contraposée $(P \implies Q)$ est vraie.

1.3 Quantificateurs

Les quantificateurs sont des symboles logiques qui permettent de préciser sur quels éléments d'un ensemble porte une assertion. Ils sont indispensables pour formaliser rigoureusement les assertions mathématiques. Certaines assertions sont fondés au travers d'une variable ou indéterminé, c'est-à-dire un objet mathématique qui peut prendre plusieurs valeurs.

Exemple :

« L'entier $n(n+1)$ est pair ».

Soit E un ensemble. Si une assertion P dépend de la variable $x \in E$, on la notera $P\{x\}$ ou $P(x)$.

S'il y a plusieurs variables, on notera $P\{x, y\}$ ou $P(x, y)$.

1.3.1 Quantificateur universel ($\forall$)

Définition 1.33 : (*Quantificateur universel*)

On appelle ***quantificateur universel*** le symbole $\forall$, qui signifie « pour tout » , « pour chaque » , « quel que soit » , « peu importe » ou « n'importe quel ».

Ce quantificateur est utilisé pour décrire une propriété qui est vraie pour tous les éléments d'un ensemble donné.

Soit E un ensemble et $P(x)$ une assertion dépendant de $x \in E$.

L'assertion :

$$\forall x \in E, P(x)$$

est **vraie** si et seulement si $P(x)$ est vraie pour tous les éléments x de E.

Elle est fausse dès qu'il existe au moins un élément de E pour lequel $P(x)$ est fausse. Dans ce cas, on dit que $P(x)$ est ***contredite*** par cet élément, qui est alors appelé un ***contre-exemple***.

Exemple :

- $\forall x \in \mathbb{R}, x^2 \geqslant 0$ est vraie.
- $\forall n \in \mathbb{N}, n^2 \geqslant n$ est vraie.
- $\forall x \in \mathbb{R}, x > 0$ est fausse (contre-exemple : $x = -1$).

1.3.2 Quantificateur existentiel ($\exists$)

Définition 1.34 : (*Quantificateur existentiel*)

On appelle ***quantificateur existentiel*** le symbole $\exists$, qui signifie « il existe » ou « il existe au moins un ».

Soit E un ensemble et $P(x)$ une assertion dépendant de $x \in E$.

L'assertion :

$$\exists x \in E,\ P(x)$$

est **vraie** s'il existe au moins un élément $x \in E$ tel que $P(x)$ soit vraie.

Elle est fausse si $P(x)$ est fausse pour tous les éléments de E.

Dans le cas où il existe un unique élément $x \in E$ tel que $P(x)$ soit vraie, on peut renforcer l'assertion en écrivant :

$$\exists! x \in E,\ P(x)$$

qui se lit « il existe un unique x dans E tel que $P(x)$ soit vraie ».

Un élément $x \in E$ vérifiant $P(x)$ est appelé un ***témoin*** de l'assertion existentielle.

Exemple :

— $\exists x \in \mathbb{R},\ x^2 = 4$ est vraie (témoins : $x = 2$ ou $x = -2$).

— $\exists! x \in \mathbb{R},\ x^2 = 4$ est fausse (car il existe deux témoins : $x = 2$ et $x = -2$).

— $\exists x \in \mathbb{R},\ x^2 = -1$ est fausse.

— $\exists! x \in \mathbb{R},\ x + 1 = 3$ est vraie (l'unique témoin est $x = 2$).

1.3.3 Propriétés de $\forall$ et $\exists$

Propriété 1.35 : (*Négation des quantificateurs*)

Soit E un ensemble et $P\{x\}$ une assertion qui dépend de $x \in E$. Alors :

i) $\neg(\forall x \in E, P\{x\}) \iff \exists x \in E, \neg P\{x\}$

ii) $\neg(\exists x \in E, P\{x\}) \iff \forall x \in E, \neg P\{x\}$

Preuve :

Preuve du i) : Montrons la double implication par analyse sémantique.

$\boxed{\Rightarrow}$ Supposons que $\neg(\forall x \in E,\ P\{x\})$ est vraie.

Alors l'assertion $\forall x \in E,\ P\{x\}$ est fausse.

Cela signifie qu'il n'est pas vrai que $P\{x\}$ soit satisfaite pour tous les éléments de E.

Il existe donc au moins un élément $x_0 \in E$ tel que $P\{x_0\}$ est fausse, c'est-à-dire $\neg P\{x_0\}$ est vraie.

Par définition du quantificateur existentiel, $\exists x \in E,\ \neg P\{x\}$ est vraie.

$\boxed{\Leftarrow}$ Supposons que $\exists x \in E,\ \neg P\{x\}$ est vraie.

Il existe alors un élément $x_0 \in E$ tel que $\neg P\{x_0\}$ est vraie, donc $P\{x_0\}$ est fausse.

Puisqu'il existe au moins un contre-exemple dans E, l'affirmation « $P\{x\}$ est vraie pour tout $x \in E$ » est nécessairement fausse.

Ainsi, $\neg(\forall x \in E,\ P\{x\})$ est vraie.

Les deux assertions s'impliquant mutuellement, donc d'après 1.25, elles sont logiquement équivalentes.

Preuve du ii) : On procède de manière analogue.

$\boxed{\Rightarrow}$ Supposons $\neg(\exists x \in E, P\{x\})$ vraie.

Alors $\exists x \in E, P\{x\}$ est fausse, ce qui signifie qu'aucun élément de E ne vérifie P.

Autrement dit, pour **tout** $x \in E$, $P\{x\}$ est fausse, donc $\neg P\{x\}$ est vraie.

D'où $\forall x \in E, \neg P\{x\}$.

$\boxed{\Leftarrow}$ Supposons $\forall x \in E, \neg P\{x\}$ vraie.

Alors pour tout $x \in E$, $P\{x\}$ est fausse.

Il est donc impossible de trouver un $x \in E$ tel que $P\{x\}$ soit vraie.

L'assertion $\exists x \in E, P\{x\}$ est donc fausse,

ce qui équivaut à dire que $\neg(\exists x \in E, P\{x\})$ est vraie.

D'après 1.25, l'équivalence est ainsi établie par double implication.

Propriété 1.36 : (*Distributivité des quantificateurs*)

Soit E un ensemble et soient $P\{x\}$ et $Q\{x\}$ deux assertions qui dépendent de $x \in E$.

Les quantificateurs se distribuent sur les connecteurs logiques de la manière suivante :

i) Le quantificateur universel se distribue sur la conjonction (le « et ») :

$$\forall x \in E, (P\{x\} \wedge Q\{x\}) \iff (\forall x \in E, P\{x\}) \wedge (\forall x \in E, Q\{x\}).$$

ii) Le quantificateur existentiel se distribue sur la disjonction (le « ou ») :

$$\exists x \in E, (P\{x\} \vee Q\{x\}) \iff (\exists x \in E, P\{x\}) \vee (\exists x \in E, Q\{x\}).$$

Propriété 1.37 : (*Implications simples (Pièges fréquents)*)

Soit E un ensemble et soient $P\{x\}$ et $Q\{x\}$ deux assertions qui dépendent de $x \in E$.

Il est important de noter que la distributivité ne fonctionne pas toujours dans les deux sens. On a seulement des implications simples dans ce sens (la réciproque est fausse en général) :

i) L'existence d'un élément vérifiant P et Q implique qu'il existe un élément vérifiant P et un (autre potentiellement) vérifiant Q :

$$\exists x \in E, (P\{x\} \wedge Q\{x\}) \implies (\exists x \in E, P\{x\}) \wedge (\exists x \in E, Q\{x\}).$$

ii) Le fait que P soit vraie pour tout $x \in E$ ou que Q soit vraie pour tout $x \in E$ implique que pour tout $x \in E$, P ou Q est vraie :

$$(\forall x \in E, P\{x\}) \vee (\forall x \in E, Q\{x\}) \implies \forall x \in E, (P\{x\} \vee Q\{x\}).$$

Exemple :

(Contre-exemple pour la réciproque du ii))

Soient les assertions :

$$P(n) : \text{« } n \text{ est un entier pair »} \quad \text{et} \quad Q(n) : \text{« } n \text{ est un entier impair ».}$$

On a :

— $\exists n \in \mathbb{N}$, $P(n)$ est vraie (pour $n = 2$).

— $\exists n \in \mathbb{N}$, $Q(n)$ est vraie (pour $n = 3$).

— Mais $\exists n \in \mathbb{N}$, $(P(n) \wedge Q(n))$ est fausse car un nombre ne peut être pair et impair simultanément.

Cette situation illustre que même si P est vérifiée pour au moins un élément de E et que Q est vérifiée pour au moins un élément de E, il n'est pas nécessairement vrai qu'il existe un élément de E qui vérifie à la fois P et Q. C'est pourquoi la réciproque de l'implication du ii) est fausse en général.

Propriété 1.38 : (*Permutation des quantificateurs*)

Soient E et F deux ensembles et $P\{x;y\}$ une assertion qui dépend de deux variables $x \in E$ et $y \in F$.

i) Si **deux quantificateurs successifs sont de même nature**, on peut intervertir leur ordre sans changer la valeur de vérité de l'assertion :

$$\forall x \in E, \forall y \in F, P\{x;y\} \iff \forall y \in F, \forall x \in E, P\{x;y\}$$

et

$$\exists x \in E, \exists y \in F, P\{x;y\} \iff \exists y \in F, \exists x \in E, P\{x;y\}.$$

ii) Si **deux quantificateurs successifs sont de nature différente**, l'ordre est essentiel et ne peut pas être interverti (la réciproque est fausse en général) :

$$\exists x \in E, \forall y \in F, P\{x;y\} \implies \forall y \in F, \exists x \in E, P\{x;y\}.$$

Explication : La réciproque est fausse. L'assertion « Il existe un $x \in E$ qui marche pour tous les $y \in F$ » est beaucoup plus forte que « Pour chaque $y \in F$, il existe un $x \in E$ (qui peut dépendre de y) ».

Propriété 1.39 : (*Négation des quantificateurs imbriqués*)

La négation d'une assertion avec plusieurs quantificateurs s'obtient en :

- Niant l'assertion principale
- Remplaçant chaque $\forall$ par $\exists$ et chaque $\exists$ par $\forall$

Exemples :

— $\neg(\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y \leq x) \iff \exists x \in \mathbb{R}, \forall y \in \mathbb{R}, y > x$

— $\neg(\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, y \leq x) \iff \forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y > x$

Exemple :

L'assertion $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, y \leq x$ est fausse car il n'existe aucun nombre réel plus grand que tous les autres.

Sa négation $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y > x$ est vraie : pour tout réel x, on peut prendre $y = x+1$, alors $y > x$.

1.4 Démonstration par récurrence

Propriété 1.40 : (*Principe de récurrence*)

Soit n_0 un entier naturel et soit $P(n)$ une assertion qui dépend d'un entier $n \geq n_0$.

Pour démontrer que $P(n)$ est vraie pour tout $n \geq n_0$, on procède en deux étapes :

1. **Initialisation :** On vérifie que $P(n_0)$ est vraie.
2. **Hérédité :** On suppose que $P(n)$ est vraie pour un entier $n \geq n_0$ fixé (hypothèse de récurrence), et on démontre que $P(n+1)$ est vraie.

Si ces deux étapes sont vérifiées, alors $P(n)$ est vraie pour tout entier $n \geq n_0$.

Exemple :

(Somme des n premiers entiers)

Montrons par récurrence que pour tout entier $n \geq 1$:

$$\sum_{k=1}^{n} k = 1+2+3+\cdots+n = \frac{n(n+1)}{2}.$$

Soit $P(n)$ l'assertion : $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Initialisation ($n=1$) :

$$\sum_{k=1}^{1} k = 1 \quad \text{et} \quad \frac{1(1+1)}{2} = \frac{2}{2} = 1.$$

Donc $P(1)$ est vraie.

Hérédité : Supposons que $P(n)$ soit vraie pour un entier $n \geq 1$ fixé, c'est-à-dire :

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}. \quad \text{(hypothèse de récurrence)}$$

Montrons que $P(n+1)$ est vraie, c'est-à-dire :

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

On a :

$$\begin{aligned}
\sum_{k=1}^{n+1} k &= \sum_{k=1}^{n} k + (n+1) \\
&= \frac{n(n+1)}{2} + (n+1) && \text{(d'après l'hypothèse de récurrence)} \\
&= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\
&= \frac{n(n+1)+2(n+1)}{2} \\
&= \frac{(n+1)(n+2)}{2}.
\end{aligned}$$

Donc $P(n+1)$ est vraie.

Conclusion : Par le principe de récurrence, $P(n)$ est vraie pour tout entier $n \geq 1$.

Exercice 1. *Formule du binôme de Newton*

Démontrer par récurrence que pour tous réels a, b et tout entier $n \in \mathbb{N}$:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

où $\displaystyle\binom{n}{k} = \frac{n!}{k!(n-k)!}$ sont les coefficients binomiaux.

Indication : Utiliser la relation de Pascal $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Preuve :

Soient $a, b \in \mathbb{R}$.

On note $P(n)$ la propriété :

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Initialisation ($n = 0$) :

$$(a+b)^0 = 1 \quad \text{et} \quad \sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k} = \binom{0}{0} a^0 b^0 = 1.$$

Donc $P(0)$ est vraie.

Hérédité : Supposons que $P(n)$ soit vraie pour un entier $n \geq 0$ fixé. Montrons que $P(n+1)$ est vraie.

On a :

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b) \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} && \text{(par hypothèse de récurrence)} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1}.
\end{aligned}$$

Dans la première somme, on effectue le changement d'indice $j = k+1$ (donc $k = j-1$) :

$$\sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} = \sum_{j=1}^{n+1} \binom{n}{j-1} a^j b^{n+1-j}.$$

Dans la deuxième somme, on pose $j = k$:

$$\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} = \sum_{j=0}^{n} \binom{n}{j} a^j b^{n+1-j}.$$

Donc :

$$\begin{aligned}
(a+b)^{n+1} &= \sum_{j=1}^{n+1} \binom{n}{j-1} a^j b^{n+1-j} + \sum_{j=0}^{n} \binom{n}{j} a^j b^{n+1-j} \\
&= \binom{n}{n} a^{n+1} b^0 + \sum_{j=1}^{n} \binom{n}{j-1} a^j b^{n+1-j} + \binom{n}{0} a^0 b^{n+1} + \sum_{j=1}^{n} \binom{n}{j} a^j b^{n+1-j} \\
&= a^{n+1} + b^{n+1} + \sum_{j=1}^{n} \left(\binom{n}{j-1} + \binom{n}{j} \right) a^j b^{n+1-j}.
\end{aligned}$$

D'après la relation de Pascal, $\binom{n}{j-1} + \binom{n}{j} = \binom{n+1}{j}$. Donc :

$$\begin{aligned}
(a+b)^{n+1} &= a^{n+1} + b^{n+1} + \sum_{j=1}^{n} \binom{n+1}{j} a^j b^{n+1-j} \\
&= \binom{n+1}{n+1} a^{n+1} b^0 + \binom{n+1}{0} a^0 b^{n+1} + \sum_{j=1}^{n} \binom{n+1}{j} a^j b^{n+1-j} \\
&= \sum_{j=0}^{n+1} \binom{n+1}{j} a^j b^{n+1-j}.
\end{aligned}$$

Ainsi, $P(n+1)$ est vraie.

Conclusion : Par récurrence, $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

Chapitre 2

Les ensembles

Exemple :

Pour aller plus loin sur les fondements logiques, on pourra consulter sur internet la théorie axiomatique des ensembles de Zermelo-Fraenkel (en particulier l'axiome du choix).

2.1 Notion d'ensemble

Convention 2.1 : (*Ensemble, élément et appartenance*)

On appelle ***ensemble***, intuitivement, une collection d'objets bien définis, appelés les ***éléments*** de l'ensemble.

Si un objet nommé x est un élément de l'ensemble X, on note :

$$x \in X \quad \text{(on lit « } x \textbf{ ***appartient*** à } X \text{ »).}$$

Dans le cas contraire, on note :

$$\neg(x \in X) \iff x \notin X \quad \text{(on lit « } x \textbf{ ***n'appartient pas*** à } X \text{ »).}$$

Exemple :

— $\mathbb{N}$ désigne l'ensemble des entiers naturels. On a $3 \in \mathbb{N}$ mais $\sqrt{2} \notin \mathbb{N}$.

— L'ensemble des lettres du mot « algèbre » peut se noter $L = \{\text{a, l, g, è, b, r, e}\}$.

Définition 2.2 : (*Cardinal, ensemble fini et ensemble vide*)

Un ensemble X est dit ***fini*** s'il contient un nombre entier naturel n d'éléments, et on appelle ce nombre le ***cardinal*** de X, noté $\text{card}(X)$ ou $|X|$.

— Si $\text{card}(X) = |X| = n$, on peut énumérer ses éléments (notation ***en extension***) : $X = \{x_1, x_2, \ldots, x_n\}$.

— Si $\text{card}(X) = |X| = 1$, on dit que X est un ***singleton***.

On le note alors $X = \{a\}$ pour un certain élément a, et on a bien $a \in X$ c'est-à-dire que $a \in \{a\}$. Mais l'écriture $a \subset \{a\}$ est incorrecte, car a n'est pas un ensemble et ne peut donc pas être inclus dans un autre ensemble. Il est important de ne pas confondre a et $\{a\}$: a est un élément, tandis que $\{a\}$ est un ensemble qui contient cet élément.

Exemple :

— L'ensemble des solutions réelles de $x^2 - 2x + 1 = 0$ est $\mathscr{S} = \{1\}$. C'est un singleton.

— On peut généraliser cette écriture à des ensembles infinis :

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ est un ensemble infini.

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ est un autre ensemble infini.

$\mathbb{R}$ est problématique pour être écrit en extension.

— L'ensemble des entiers $n \in \mathbb{N}$ vérifiant $n^2 < 0$ n'a aucun élément, donc il s'agit d'un ensemble sans élément.

Convention 2.3 : (*Axiome de l'ensemble vide*)

Il existe un unique ensemble de cardinal nul, appelé ***ensemble vide***, noté $\emptyset$.

Par convention,

$$\text{card}(\emptyset) = 0 \quad \text{et} \quad \forall x,\, x \notin \emptyset.$$

Définition 2.4 : (*Notation en compréhension*)

Lorsqu'un ensemble est défini par une propriété vérifiée par ses éléments, on utilise la notation ***en compréhension*** :

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

où E est un ensemble de référence et $P(x)$ est une assertion dépendant de x.

Cette notation désigne l'ensemble de tous les éléments x de E qui vérifient la propriété $P(x)$.

La barre verticale « | » se lit « tel que » ou « vérifiant ».

Exemple :

— Par exemple, $A = \left\{x \in \mathbb{R} \;\middle|\; x^2 = 4\right\}$ désigne l'ensemble des nombres réels x tels que $x^2 = 4$, c'est-à-dire $\{-2;2\}$.

$A = \left\{x \in \mathbb{R} \;\middle|\; x^2 = 4\right\} = \{-2;2\}$.

— $B = \left\{n \in \mathbb{N} \;\middle|\; n \text{ est pair}\right\} = \{0;2;4;\ldots\}$.

— $\mathbb{Q} = \left\{\frac{p}{q} \;\middle|\; p \in \mathbb{Z}, q \in \mathbb{N}^*\right\}$ est l'ensemble des nombres rationnels.

— $X = \left\{x \in \mathbb{R} \;\middle|\; x^2 - 2x + 1 = 0\right\} = \{1\}$.

2.2 Partie d'un ensemble

Convention 2.5 : (*Axiome d'extensionnalité*)

Deux ensembles sont égaux si et seulement s'ils ont les mêmes éléments :

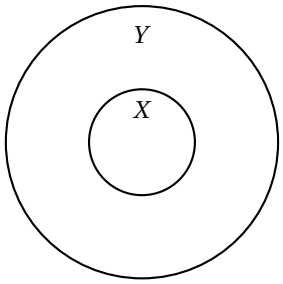
$$X = Y \iff (\forall x,\, x \in X \iff x \in Y).$$

Définition 2.6 : (*Sous-ensemble (partie)*)

Soient X et Y deux ensembles.

On dit que X est une ***partie*** (ou ***sous-ensemble***) de Y, et on note $X \subset Y$, si tout élément de X est aussi élément de Y :

$$X \subset Y \iff \forall x \in X,\, x \in Y.$$



Propriété 2.7 : (*Propriétés élémentaires de l'inclusion*)

Soit X un ensemble. On a :

i) $\emptyset \subset X$ (l'ensemble vide est inclus dans tout ensemble).

ii) $X \subset X$ (tout ensemble est inclus dans lui-même, c'est la **réflexivité**).

Preuve :

Preuve du i) : Montrons que $\emptyset \subset X$.

Par définition, il faut vérifier que pour tout élément x, si $x \in \emptyset$, alors $x \in X$.

L'assertion "$x \in \emptyset$" est toujours fausse car l'ensemble vide ne contient aucun élément.

Donc il n'est pas possible de trouver un élément $x \in \emptyset$ tel que $x \notin X$.

Donc, $\emptyset \subset X$.

Preuve du ii) : Montrons que $X \subset X$.

Par définition, il faut vérifier que pour tout $x \in X$, on a $x \in X$.

C'est une évidence (réflexivité de l'égalité). Donc l'inclusion est vraie.

Propriété 2.8 : (*Caractérisation de l'égalité ensembliste*)

Soient X et Y deux ensembles. On a :

$$(X = Y) \iff (X \subset Y \text{ et } Y \subset X).$$

Preuve :

C'est la définition même de l'égalité ensembliste (principe d'extensionnalité 2.5).

Deux ensembles sont égaux si et seulement s'ils contiennent exactement les mêmes éléments, ce qui revient à dire que chacun est inclus dans l'autre.

Propriété 2.9 : (*Transitivité de l'inclusion*)

Soient X, Y et Z trois ensembles. On a :

$$(X \subset Y \text{ et } Y \subset Z) \implies (X \subset Z).$$

Preuve :

Supposons que $X \subset Y$ et $Y \subset Z$.

Soit $x \in X$.

— Comme $X \subset Y$, on a $x \in Y$.

— Comme $Y \subset Z$, on a $x \in Z$.

Ainsi, tout élément de X appartient à Z, donc $X \subset Z$.

Exemple :

$(\mathbb{N} \subset \mathbb{Q} \text{ et } \mathbb{Q} \subset \mathbb{R}) \implies (\mathbb{N} \subset \mathbb{R})$.

Définition 2.10 : (*Ensemble des parties*)

Soit X un ensemble.

Il existe un unique ensemble que l'on note $\mathscr{P}(X)$ constitué de tous les sous-ensembles de X.

On appelle $\mathscr{P}(X)$ l'***ensemble des parties de*** X, autrement dit :

$$\mathscr{P}(X) = \{Y \mid Y \subset X\}.$$

⚠⚠⚠ Un **élément** de $\mathscr{P}(X)$ est un **sous-ensemble** de X. ⚠⚠⚠

Pour dire que $Y \subset X$ on peut écrire : $Y \in \mathscr{P}(X)$.

Par contre, si on écrit $Q \subset \mathscr{P}(X)$, on veut dire que Q est un ensemble constitué de parties de X.

Exemple :

$\emptyset \in \mathscr{P}(X)$ et $X \in \mathscr{P}(X)$ (car $X \subset X$).

$\{\emptyset; X\} \subset \mathscr{P}(X)$.

2.3 Opérations ensemblistes

Définition 2.11 : (*Intersection de deux ensembles*)

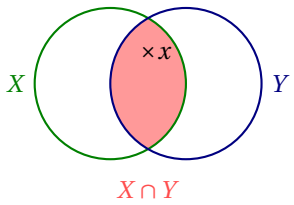
Soient X et Y deux ensembles.

On appelle ***intersection de*** X ***et*** Y l'ensemble noté $X \cap Y$ (« X inter Y ») constitué des éléments qui appartiennent à la fois à X et à Y.

Autrement dit :

$$x \in X \cap Y \iff x \in X \wedge x \in Y$$

Shématiquement, $X \cap Y$ correspond à la partie commune aux deux ensembles X et Y :

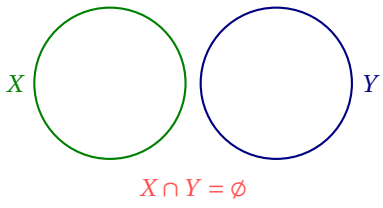


Définition 2.12 : (*Ensembles disjoints*)

Deux ensembles X et Y sont dits ***disjoints*** si leur intersection est vide, c'est-à-dire si :

$$X \cap Y = \emptyset.$$

Cela signifie qu'ils n'ont aucun élément en commun.



Propriété 2.13 : (*Inclusions triviales de l'intersection*)

Soient X et Y deux ensembles.

L'intersection de deux ensembles est toujours incluse dans chacun d'eux :

$$X \cap Y \subset X \quad \text{et} \quad X \cap Y \subset Y.$$

Preuve :

Soit $x \in X \cap Y$.

$$\begin{aligned} x \in X \cap Y &\implies x \in X \wedge x \in Y && \text{(car 2.11)} \\ &\implies x \in X && \text{(car 1.26)} \end{aligned}$$

Ce qui prouve que $X \cap Y \subset X$.

Soit $x \in X \cap Y$.

$$\begin{aligned} x \in X \cap Y &\implies x \in X \wedge x \in Y && \text{(car 2.11)} \\ &\implies x \in Y && \text{(car 1.26)} \end{aligned}$$

Ce qui prouve que $X \cap Y \subset Y$.

Propriété 2.14 : (*Idempotence de l'intersection*)

Soit X un ensemble.

L'intersection d'un ensemble avec lui-même est l'ensemble lui-même :

$$X \cap X = X.$$

Preuve :

Montrons $X \cap X = X$ par double inclusion.

$\boxed{\subset}$ Soit $x \in X \cap X$,

$$\begin{aligned} x \in X \cap X &\implies x \in X \wedge x \in X && \text{(car 2.11)} \\ &\implies x \in X && \text{(car 1.26)} \end{aligned}$$

Ainsi $X \cap X \subset X$.

$\boxed{\supset}$ Soit $x \in X$,

$$\begin{aligned} x \in X &\implies x \in X \wedge x \in X && \text{(car 2.11)} \\ &\implies x \in X \cap X && \text{(car 1.26)} \end{aligned}$$

Ainsi $X \subset X \cap X$.

On conclut en faisant la synthèse des deux résultats : $X \subset X \cap X \subset X$.

D'où l'égalité $X = X \cap X$.

Propriété 2.15 : (*Commutativité de l'intersection*)

Soient X et Y deux ensembles. Alors :

$$X \cap Y = Y \cap X.$$

Preuve :

Montrons $X \cap Y = Y \cap X$ par double inclusion.

$\boxed{\subset}$ Soit $x \in X \cap Y$,

$$\begin{aligned} x \in X \cap Y &\implies x \in X \wedge x \in Y && \text{(car 2.11)} \\ &\implies x \in Y \wedge x \in X && \text{(car 1.20)} \\ &\implies x \in Y \cap X && \text{(car 2.11)} \end{aligned}$$

Donc $X \cap Y \subset Y \cap X$.

$\boxed{\supset}$ Soit $x \in Y \cap X$,

$$\begin{aligned} x \in Y \cap X &\implies x \in Y \wedge x \in X && \text{(car 2.11)} \\ &\implies x \in X \wedge x \in Y && \text{(car 1.20)} \\ &\implies x \in X \cap Y && \text{(car 2.11)} \end{aligned}$$

Donc $Y \cap X \subset X \cap Y$.

Donc $X \cap Y \subset Y \cap X \subset X \cap Y$.

D'où l'égalité $X \cap Y = Y \cap X$.

Propriété 2.16 : (*Associativité de l'intersection*)

Soient X, Y et Z trois ensembles. Alors :

$$(X \cap Y) \cap Z = X \cap (Y \cap Z).$$

Preuve :

Soit $x \in (X \cap Y) \cap Z$.

Par définition, cela signifie $x \in X \cap Y$ et $x \in Z$,

soit $(x \in X \wedge x \in Y) \wedge x \in Z$.

Par associativité du connecteur logique $\wedge$, on a $(x \in X \wedge x \in Y) \wedge x \in Z \iff x \in X \wedge (x \in Y \wedge x \in Z)$.

Ceci équivaut à $x \in X \cap (Y \cap Z)$. Les deux ensembles contiennent donc exactement les mêmes éléments, d'où l'égalité.

La preuve peut être écrite de manière plus formelle de la manière suivante :

$$\begin{aligned}
x \in (X \cap Y) \cap Z &\iff x \in X \cap Y \wedge x \in Z && \text{(car 2.11)} \\
&\iff (x \in X \wedge x \in Y) \wedge x \in Z && \text{(car 2.11)} \\
&\iff x \in X \wedge (x \in Y \wedge x \in Z) && \text{(car 1.17)} \\
&\iff x \in X \wedge (x \in Y \cap Z) && \text{(car 2.11)} \\
&\iff x \in X \cap (Y \cap Z) && \text{(car 2.11)}
\end{aligned}$$

En conclusion, $(X \cap Y) \cap Z = X \cap (Y \cap Z)$.

Propriété 2.17 : (*Élément absorbant pour l'intersection*)

Soit X un ensemble.

L'ensemble vide est ***absorbant*** pour l'intersection :

$$X \cap \emptyset = \emptyset.$$

Preuve :

- $\subset$ D'après la propriété « inclusions triviales de l'intersection » 2.13, $X \cap \emptyset \subset \emptyset$.
- $\supset$ D'après les « propriétés élémentaires de l'inclusion » 2.7, l'ensemble vide est inclus dans tout ensemble, donc $\emptyset \subset X \cap \emptyset$.

Conclusion : $X \cap \emptyset \subset \emptyset \subset X \cap \emptyset$

Par double inclusion, on a donc $X \cap \emptyset = \emptyset$.

Définition 2.18 : (*Union de deux ensembles*)

Soient X et Y deux ensembles.

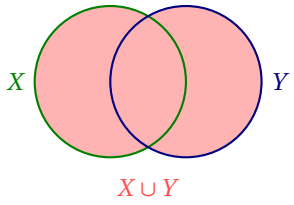
On appelle ***union de X et Y*** l'ensemble noté $X \cup Y$ (« X union Y ») constitué des éléments de X et de Y :

$$X \cup Y = \{x \mid x \in X \vee x \in Y\}$$

Autrement dit :

$$x \in X \cup Y \iff x \in X \vee x \in Y.$$

Schématiquement, $X \cup Y$ correspond à la réunion des deux ensembles X et Y :



Propriété 2.19 : (*Inclusions triviales de l'union*)

Soient X et Y deux ensembles.

Chaque ensemble est inclus dans leur union :

$$X \subset X \cup Y \quad \text{et} \quad Y \subset X \cup Y$$

Preuve :

Soit $x \in X$.

$$\begin{aligned} x \in X &\implies x \in X \vee x \in Y && \text{(car 1.27)} \\ &\implies x \in X \cup Y && \text{(car 2.18)} \end{aligned}$$

Ce qui prouve que $X \subset X \cup Y$.

Soit $x \in Y$.

$$\begin{aligned} x \in Y &\implies x \in X \vee x \in Y && \text{(car 1.27)} \\ &\implies x \in X \cup Y && \text{(car 2.18)} \end{aligned}$$

Ce qui prouve que $Y \subset X \cup Y$.

Propriété 2.20 : (*Idempotence de l'union*)

Soit X un ensemble.

L'union d'un ensemble avec lui-même est l'ensemble lui-même :

$$X \cup X = X$$

Preuve :

Montrons $X \cup X = X$ par double inclusion.

$\boxed{\subset}$ Soit $x \in X \cup X$,

$$\begin{aligned} x \in X \cup X &\implies x \in X \vee x \in X && \text{(car 2.18)} \\ &\implies x \in X && \text{(car 1.15)} \end{aligned}$$

Ainsi $X \cup X \subset X$.

$\boxed{\supset}$ Soit $x \in X$,

$$\begin{aligned} x \in X &\implies x \in X \vee x \in X && \text{(car 1.27 ou car 1.15)} \\ &\implies x \in X \cup X && \text{(car 2.18)} \end{aligned}$$

Ainsi $X \subset X \cup X$.

On conclut en faisant la synthèse des deux résultats : $X \subset X \cup X \subset X$.

D'où l'égalité $X = X \cup X$.

Propriété 2.21 : (*Commutativité de l'union*)

Soient X et Y deux ensembles. Alors :

$$X \cup Y = Y \cup X.$$

Preuve :

Montrons $X \cup Y = Y \cup X$ par double inclusion.

$\boxed{\subset}$ Soit $x \in X \cup Y$,

$$\begin{aligned} x \in X \cup Y &\implies x \in X \vee x \in Y && \text{(car 2.18)} \\ &\implies x \in Y \vee x \in X && \text{(car 1.21)} \\ &\implies x \in Y \cup X && \text{(car 2.18)} \end{aligned}$$

Donc $X \cup Y \subset Y \cup X$.

$\boxed{\supset}$ Soit $x \in Y \cup X$,

$$\begin{aligned} x \in Y \cup X &\implies x \in Y \vee x \in X && \text{(car 2.18)} \\ &\implies x \in X \vee x \in Y && \text{(car 1.21)} \\ &\implies x \in X \cup Y && \text{(car 2.18)} \end{aligned}$$

Donc $Y \cup X \subset X \cup Y$.

Donc $X \cup Y \subset Y \cup X \subset X \cup Y$.

D'où l'égalité $X \cup Y = Y \cup X$.

Propriété 2.22 : (*Associativité de l'union*)

Soient X, Y et Z trois ensembles. Alors :

$$(X \cup Y) \cup Z = X \cup (Y \cup Z)$$

Preuve :

Soit $x \in (X \cup Y) \cup Z$.

Par définition, cela signifie $x \in X \cup Y$ ou $x \in Z$,

soit $(x \in X \vee x \in Y) \vee x \in Z$.

Par associativité du connecteur logique $\vee$, on a $(x \in X \vee x \in Y) \vee x \in Z \iff x \in X \vee (x \in Y \vee x \in Z)$.

Ceci équivaut à $x \in X \cup (Y \cup Z)$. Les deux ensembles contiennent donc exactement les mêmes éléments, d'où l'égalité.

La preuve peut être écrite de manière plus formelle de la manière suivante :

$$\begin{aligned} x \in (X \cup Y) \cup Z &\iff x \in X \cup Y \vee x \in Z && \text{(car 2.18)} \\ &\iff (x \in X \vee x \in Y) \vee x \in Z && \text{(car 2.18)} \\ &\iff x \in X \vee (x \in Y \vee x \in Z) && \text{(car 1.16)} \\ &\iff x \in X \vee x \in Y \cup Z && \text{(car 2.18)} \\ &\iff x \in X \cup (Y \cup Z) && \text{(car 2.18)} \end{aligned}$$

En conclusion, $(X \cup Y) \cup Z = X \cup (Y \cup Z)$.

Propriété 2.23 : (*Élément neutre pour l'union*)

Soit X un ensemble.

L'ensemble vide est ***neutre*** pour l'union :

$$X \cup \emptyset = X.$$

Preuve :

Montrons $X \cup \emptyset = X$ par double inclusion.

$\boxed{\subset}$ Soit $x \in X \cup \emptyset$.

$$\begin{aligned} x \in X \cup \emptyset &\implies x \in X \vee x \in \emptyset && \text{(car 2.18)} \\ &\implies x \in X && \text{(car 2.3 : } x \in \emptyset \text{ est toujours fausse)} \end{aligned}$$

Ainsi $X \cup \emptyset \subset X$.

$\supset$ Soit $x \in X$.

$$x \in X \implies x \in X \vee x \in \emptyset \qquad \text{(car 1.27)}$$
$$\implies x \in X \cup \emptyset \qquad \text{(car 2.18)}$$

Ainsi $X \subset X \cup \emptyset$.

On conclut en faisant la synthèse des deux résultats : $X \cup \emptyset \subset X \subset X \cup \emptyset$.

D'où l'égalité $X \cup \emptyset = X$.

Propriété 2.24 : (*Caractérisation de l'inclusion par l'union*)

Soient X et Y deux ensembles. On a l'équivalence :

$$X \subset Y \iff X \cup Y = Y.$$

Preuve :

Preuve du sens direct ($\Rightarrow$) : Supposons $X \subset Y$. Montrons $X \cup Y = Y$ par double inclusion.

$\subset$ Soit $x \in X \cup Y$.

Alors $x \in X$ ou $x \in Y$.

Si $x \in X$, alors $x \in Y$ (car c'est l'hypothèse de départ : $X \subset Y$).

Donc dans les deux cas de la disjonction, $x \in Y$.

Ainsi $X \cup Y \subset Y$.

$\supset$ D'après les « inclusions triviales de l'union » 2.19, on a toujours $Y \subset X \cup Y$.

On conclut que $X \cup Y \subset Y \subset X \cup Y$, d'où l'égalité $X \cup Y = Y$.

Preuve de la réciproque ($\Leftarrow$) : Supposons $X \cup Y = Y$. Montrons $X \subset Y$.

$\subset$ D'après les « inclusions triviales de l'union » 2.19, on a toujours $X \subset X \cup Y$.

Comme $X \cup Y = Y$ par hypothèse, on en déduit par substitution que $X \subset Y$.

Ainsi $X \subset Y$.

Les deux implications étant établies, l'équivalence est démontrée.

Propriété 2.25 : (*Distributivité de l'union sur l'intersection*)

Soient X, Y et Z trois ensembles. On a :

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z).$$

Preuve :

Montrons l'égalité par équivalence logique.

$$x \in X \cup (Y \cap Z) \iff x \in X \vee x \in Y \cap Z \qquad \text{(car 2.18)}$$
$$\iff x \in X \vee (x \in Y \wedge x \in Z) \qquad \text{(car 2.11)}$$
$$\iff (x \in X \vee x \in Y) \wedge (x \in X \vee x \in Z) \qquad \text{(car 1.19)}$$
$$\iff x \in X \cup Y \wedge x \in X \cup Z \qquad \text{(car 2.18)}$$
$$\iff x \in (X \cup Y) \cap (X \cup Z). \qquad \text{(car 2.11)}$$

Les deux ensembles contiennent exactement les mêmes éléments, d'où l'égalité.

Propriété 2.26 : (*Distributivité de l'intersection sur l'union*)

Soient X, Y et Z trois ensembles. On a :

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z).$$

Preuve :

Montrons l'égalité par équivalence logique.

$$\begin{aligned}
x \in X \cap (Y \cup Z) &\iff x \in X \wedge x \in Y \cup Z && \text{(car 2.11)} \\
&\iff x \in X \wedge (x \in Y \vee x \in Z) && \text{(car 2.18)} \\
&\iff (x \in X \wedge x \in Y) \vee (x \in X \wedge x \in Z) && \text{(car 1.18)} \\
&\iff x \in X \cap Y \vee x \in X \cap Z && \text{(car 2.11)} \\
&\iff x \in (X \cap Y) \cup (X \cap Z). && \text{(car 2.18)}
\end{aligned}$$

Les deux ensembles contiennent exactement les mêmes éléments, d'où l'égalité.

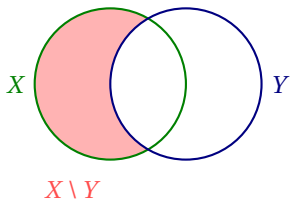
2.3.1 Différences ensemblistes

Définition 2.27 : (*Différence entre deux ensembles*)

Soient X et Y deux ensembles.

On appelle ***différence de*** X ***par*** Y l'ensemble noté $X \setminus Y$ (« X privé de Y ») constitué des éléments qui sont dans X et qui ne sont pas dans Y :

$$X \setminus Y = \{x \in X \mid x \notin Y\}.$$



Propriété 2.28 : (*Propriétés de la différence*)

Soient X, Y et Z des ensembles :

(1) $X \setminus \emptyset = X$

(2) $X \setminus X = \emptyset$

(3) $(X \cup Y) \setminus Z = (X \setminus Z) \cup (Y \setminus Z)$

(4) $(X \cap Y) \setminus Z = (X \setminus Z) \cap (Y \setminus Z)$

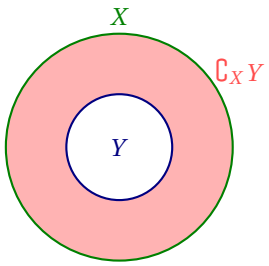
(5) $X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z)$

Supposons maintenant que Y est une partie de X (i.e. $Y \in \mathscr{P}(X)$) $\iff Y \subset X$.

Définition 2.29 : (*Complémentaire d'un ensemble dans un autre*)

Pour $Y \subset X$, on définit le ***complémentaire de*** Y ***dans*** X comme étant l'ensemble noté $\complement_X Y$ et défini par :

$$\complement_X Y = \{x \in X \mid x \notin Y\} = X \setminus Y.$$



Propriété 2.30 : (*Propriétés du complémentaire (Lois de De Morgan)*)

(1) $\complement_X \emptyset = X$

(2) $\complement_X X = \emptyset$

(3) $\complement_X (\complement_X Y) = Y$

(4) $\complement_X Y \cap Y = \emptyset$

(5) $Y \cup \complement_X Y = X$

(6) $\complement_X (Y \cap Z) = (\complement_X Y) \cup (\complement_X Z)$

(7) $\complement_X (Y \cup Z) = (\complement_X Y) \cap (\complement_X Z)$

2.3.2 Partition d'un ensemble

Définition 2.31 : (*Partition d'un ensemble*)

Soit X un ensemble (non vide) et $Q \subset \mathscr{P}(X)$ un ensemble de parties non vides de X.

On dit que Q est une ***partition*** de X si :

i) Si $A, B \in Q$ sont deux éléments distincts de Q, alors elles sont disjointes, i.e. $A \cap B = \emptyset$, c'est-à-dire :

$$\forall A, B \in Q \text{ tels que } A \neq B \implies A \cap B = \emptyset.$$

ii) $\forall x \in X, \exists A \in Q$ tel que $x \in A$, autrement dit « Q recouvre X » complètement.

Une manière équivalente de dire que Q est une partition de X :

$$\forall x \in X, \exists! A \in Q \text{ tel que } x \in A.$$

Exemple :

1. $\mathbb{N} = A \cup B$, $\{A, B\} \subset \mathscr{P}(\mathbb{N})$ avec $A = \{\text{nombres pairs}\}$, $B = \{\text{nombres impairs}\}$.

   (i) est vérifiée car $A \cap B = \emptyset$. (ii) est vérifiée car $\forall n \in \mathbb{N}$, $n \in A$ ou $n \in B$.

2. Soit X un ensemble $\neq \emptyset$ et soit $A \subset X$, alors $\{A, C_X A\}$ est une partition de X.

   (i) est vérifiée car $A \cap C_X A = \emptyset$. (ii) est vérifiée car $\forall x \in X$, $x \in A$ ou $x \notin A$, i.e. $x \in A$ ou $x \in C_X A$.

2.4 Produits cartésiens

Soient X, Y deux ensembles.

Définition 2.32 : (*Produit cartésien*)

Le ***produit cartésien*** de X et Y est l'ensemble, noté $X \times Y$, défini par :

$$X \times Y = \{(x; y) \mid x \in X,\ y \in Y\}.$$

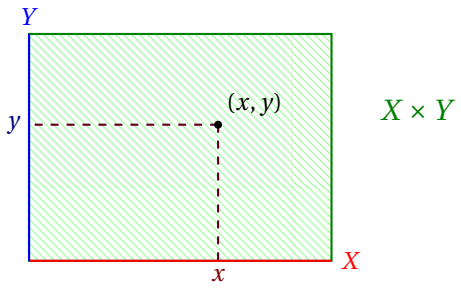
On dit que $(x; y)$ est le **couple** constitué des éléments x et y.

Exemple :

$(y; x) \notin X \times Y$ avec $y \in Y$ et $x \in X$. Ici $(y; x) \in Y \times X$.

Exemple : $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$.

Schématiquement : Le produit cartésien $X \times Y$ se représente comme un rectangle dans le plan, dont les côtés sont X (axe horizontal) et Y (axe vertical). $(x; y)$ est un élément de $X \times Y$.



Notation : on note $X \times X = X^2$. $\mathbb{N}^2 \neq \{a^2 \mid a \in \mathbb{N}\}$, $\mathbb{N}^2 = \{(m; m) \mid m, m \in \mathbb{N}\}$.

Propriété 2.33 : (*Propriétés du produit cartésien*)

Soient X, Y, Z, T quatre ensembles :

i) $X \times (Y \cup Z) = (X \times Y) \cup (X \times Z)$

ii) $(X \cup Y) \times Z = (X \times Z) \cup (Y \times Z)$

iii) $(X \cap Y) \times (Z \cap T) = (X \times Z) \cap (Y \times T)$

Preuve :

En exercice.

On peut généraliser cette construction dans le cas de n ensembles, i.e. si $X_1, \ldots, X_n$ des ensembles non vides, alors :

$$X_1 \times \cdots \times X_n = \{(x_1; \ldots; x_n) \mid x_1 \in X_1, \ldots, x_n \in X_n\}$$

Exemple :

Si $X_1 = X_2 = \cdots = X_n$, on note :

$$\underbrace{X \times X \times X \times \cdots \times X}_{n \text{ fois}} = X^n.$$

Chapitre 3

Relations

Introduction : En mathématiques, on rencontre deux grands types de relations sur un ensemble X :

→ Relation d'équivalence (exemple : $\mathbb{Z} = \{\text{pairs}\} \cup \{\text{impairs}\}$, qui donne $\mathbb{Z}/2\mathbb{Z} = \{0;1\}$).

→ Relation d'ordre (exemple : dans $\mathbb{R}$, on sait ordonner les réels : $-1 \leqslant 0 \leqslant \frac{1}{2} \leqslant \sqrt{2} \leqslant \pi \leqslant 7{,}8$).

3.1 Relation

3.1.1 Définition

Définition 3.1 : (*Relation*)

On appelle ***relation*** ou ***correspondance*** $\mathscr{R}$ tout triplet $(X, \Gamma, Y) = \mathscr{R}$ où X, Y sont deux ensembles et Γ est un sous-ensemble de $X \times Y$ (i.e. $\Gamma \subset X \times Y$).

On dit que X est l'***ensemble de départ***.

On dit que Y est l'***ensemble d'arrivée***.

On dit que Γ le ***graphe*** de la relation.

On dira que $\mathscr{R}$ est une relation de X dans Y si $(x;y)$ est un couple de $X \times Y$ qui vérifie $(x;y) \in \Gamma$.

Exemple :

Soient $X = \{a;b;c;d\}$, $Y = \{1;2;3\}$ et $\Gamma = \{(a;3);(b;1);(c;2);(d;3)\}$.

$\Gamma \subset X \times Y$.

Pour $\mathscr{R} = (X, \Gamma, Y)$:

i) a est en relation avec 3 car $(a;3) \in \Gamma$; ici on note $a \mathscr{R} 3$.

ii) a n'est pas en relation avec 2 car $(a;2) \notin \Gamma$.

3.1.2 Relation binaire

Définition 3.2 : (*Relation binaire*)

Une relation d'un ensemble **dans lui-même** s'appelle une ***relation binaire***.

Si X est un ensemble, une relation binaire est la donnée d'un sous-ensemble :

$$\Gamma \subset X \times X.$$

Dans ce cas, on note $(X, \mathscr{R})$ avec $\mathscr{R} = (X, \Gamma, X)$.

Exemple :

i) Si X est un ensemble non vide, alors « être un sous-ensemble de » est une relation binaire :

$$\forall A, B \in \mathscr{P}(X), \quad A \mathscr{R} B \iff (A \subset B \text{ ou } B \subset A).$$

ii) Sur $\mathbb{Z}$, on dit que $x \mathscr{R} y \iff x - y$ est divisible par 3 : c'est une relation binaire sur $\mathbb{Z}$.

iii) Soit P le plan $\mathbb{R}^2$ et soit D l'ensemble des droites de ce plan. Sur D, on peut définir pour $\Delta_1, \Delta_2 \in D$:

— $\Delta_1 \parallel \Delta_2 \iff \Delta_1$ est parallèle à Δ_2

— $\Delta_1 \perp \Delta_2 \iff \Delta_1$ est orthogonale à Δ_2

Dans toute la suite, on considère un ensemble X muni d'une relation binaire $\mathscr{R}$.

Définition 3.3 : (*Relation réflexive*)

La relation $\mathscr{R}$ est ***réflexive*** si :

$$\forall x \in X, \quad x \mathscr{R} x.$$

Exemple :

i) On considère $(\mathscr{P}(X), \subset)$: alors $A \mathscr{R} A$ car $A \subset A$. Donc l'inclusion est une relation réflexive.

ii) Sur $\mathbb{Z}$ avec $x \mathscr{R} y \iff 3$ divise $(x; y)$: Est-ce que $x \mathscr{R} x$, $\forall x \in \mathbb{Z}$?

On a $x \mathscr{R} x \iff 3$ divise $x - x = 0$, vrai car $0 = 3 \times 0$.

iii) Pour $D_1 \perp D_2$, la relation est fausse car une droite n'est pas orthogonale à elle-même.

Pour $D_1 \parallel D_2$, la relation est vraie car toute droite est parallèle à elle-même.

Définition 3.4 : (*Relation symétrique*)

On dit que $\mathscr{R}$ est une ***relation symétrique*** si :

$$\forall x, y \in X, \quad x \mathscr{R} y \implies y \mathscr{R} x.$$

Exemple :

i) Sur $\mathscr{P}(X)$: $A \mathscr{R} B \iff (A \subset B)$. Si $(A \mathscr{R} B \implies B \mathscr{R} A) \iff (A \subset B \implies B \subset A)$. $\implies$ Relation **non symétrique**.

ii) Sur $\mathbb{Z}$: $x \mathscr{R} y \iff 3$ divise $(x - y)$. Alors $x \mathscr{R} y \implies y \mathscr{R} x$?

$$(3 \text{ divise } (x - y)) \overset{?}{\implies} 3 \text{ divise } (y - x)$$

$\iff \exists k \in \mathbb{Z}$ t.q. $x - y = 3k \iff y - x = 3(-k)$, d'où $y - x$ est divisible par $3 \implies y \mathscr{R} x$.

iii) $\Delta_1 \perp \Delta_2 \implies \Delta_2 \perp \Delta_1$: vrai. $\Delta_1 \parallel \Delta_2 \implies \Delta_2 \parallel \Delta_1$: vrai.

iv) Sur $\mathbb{R}$, on pose : $x \mathscr{R} y \iff x \leqslant y$. Cette relation n'est pas symétrique car $1 \mathscr{R} 2$ $(1 \leqslant 2)$ mais $2 \not\mathscr{R} 1$ car $2 \leqslant 1$ est faux.

Définition 3.5 : (*Relation anti-symétrique*)

On dit que $\mathscr{R}$ est ***anti-symétrique*** si :

$$\forall (x; y) \in X^2, \quad x \mathscr{R} y \text{ et } y \mathscr{R} x \implies x = y.$$

Exemple :

i) Sur $\mathscr{P}(X)$, $A \mathscr{R} B \iff A \subset B$:

$$\left.\begin{array}{l} A \mathscr{R} B \implies A \subset B, \\ B \mathscr{R} A \implies B \subset A \end{array}\right\} A \subset B \subset A \implies A = B.$$

Elle est donc anti-symétrique.

ii) Sur $\mathbb{Z}$: $x \mathscr{R} y \iff x - y$ est divisible par 3.

$$x \mathscr{R} y \implies x - y = 3k \quad \text{et} \quad y \mathscr{R} x \implies -(y - x) = 3k'$$

$$x - y = 3k \quad \text{et} \quad x - y = 3(-k') \implies 3(k + k') = 0 \implies k' = -k.$$

Trouver des éléments de $\mathbb{Z}$ t.q. $x \mathscr{R} y$ et $y \mathscr{R} x$ et $x \neq y$:

— $5 \mathscr{R} 2$ car $5-2=3$ donc $3 \mid 5-2$.

— $2 \mathscr{R} 5$ car $2-5=-3$ donc $3 \mid 2-5$.

— Et pourtant $2 \neq 5$.

Donc $\mathscr{R}$ n'est **pas** anti-symétrique.

Définition 3.6 : (*Relation transitive*)

On dit que $\mathscr{R}$ est ***transitive*** si :

$$\forall (x;y;z) \in X^3, \quad x \mathscr{R} y \text{ et } y \mathscr{R} z \Longrightarrow x \mathscr{R} z$$

Exemple :

i) Sur $(\mathscr{P}(X), \subset)$: Soient $A, B, C \in \mathscr{P}(X)$ t.q. $A \mathscr{R} B$ et $B \mathscr{R} C$, $\iff A \subset B$ et $B \subset C$, $\Longrightarrow A \subset C$, $\Longrightarrow A \mathscr{R} C$. D'où $\mathscr{R}$ transitive.

ii) Sur $\mathbb{Z}$, $x \mathscr{R} y \iff x-y$ est divisible par 3 :

$$\begin{cases} x \mathscr{R} y \iff \exists k_1 \in \mathbb{Z},\ x-y=3k_1 \\ y \mathscr{R} z \iff \exists k_2 \in \mathbb{Z},\ y-z=3k_2 \end{cases}$$

$\Longrightarrow x-y+y-z=3(k_1+k_2) \iff x-z=3(k_1+k_2) \iff x \mathscr{R} z. \Longrightarrow \mathscr{R}$ est transitive.

iii) P est le plan $\mathbb{R}^2$, $D = \{$ensembles des droites de $P\}$, $\forall D_1, D_2 \in D$:

$$D_1 \parallel D_2 \iff D_1 \text{ et } D_2 \text{ sont parallèles}, \quad D_1 \perp D_2 \iff D_1 \text{ et } D_2 \text{ sont orthogonales.}$$

Si $D_1 \parallel D_2$ et $D_2 \parallel D_3 \Longrightarrow D_1 \parallel D_3$: vrai.

Si $D_1 \perp D_2$ et $D_2 \perp D_3 \overset{?}{\Longrightarrow} D_1 \perp D_3$: **Faux**, donc $\perp$ n'est pas transitive.

Résumé :

Soit X un ensemble et $\mathscr{R}$ une relation binaire sur X.

i) $\mathscr{R}$ est ***réflexive*** $\iff \forall x \in X,\ x \mathscr{R} x$.

ii) $\mathscr{R}$ est ***symétrique*** $\iff \forall (x;y) \in X^2,\ x \mathscr{R} y \Longrightarrow y \mathscr{R} x$.

iii) $\mathscr{R}$ est ***anti-symétrique*** $\iff \forall (x;y) \in X^2,\ x \mathscr{R} y$ et $y \mathscr{R} x \Longrightarrow x = y$.

iv) $\mathscr{R}$ est ***transitive*** $\iff \forall (x;y;z) \in X^3,\ x \mathscr{R} y$ et $y \mathscr{R} z \Longrightarrow x \mathscr{R} z$.

Exemple :

Si $\mathscr{R}$ est symétrique et anti-symétrique :

$$\forall (x,y) \in X^2,\ x \mathscr{R} y \Longrightarrow y \mathscr{R} x \Longrightarrow x = y \quad \Longrightarrow \quad \mathscr{R} \text{ “} \iff \text{”} =$$

3.2 Relation d'équivalence

Définition 3.7 : (*Relation d'équivalence*)

Soit X un ensemble et soit $\mathscr{R}$ une relation binaire sur X.

On dit que $\mathscr{R}$ est une ***relation d'équivalence*** si :

i) $\mathscr{R}$ est ***réflexive*** : $\forall x \in X,\ x \mathscr{R} x$.

ii) $\mathscr{R}$ est ***symétrique*** : $\forall (x;y) \in X^2,\ x \mathscr{R} y \implies y \mathscr{R} x$.

iii) $\mathscr{R}$ est ***transitive*** : $\forall (x;y;z) \in X^3,\ x \mathscr{R} y$ et $y \mathscr{R} z \implies x \mathscr{R} z$.

Exemple :

i) Sur P, la relation $D_1 \parallel D_2$ est une relation d'équivalence.

ii) Sur $\mathbb{Z}$, la relation sur $\mathbb{Z}$ de congruence modulo 3 est une relation d'équivalence.

iii) La relation (sur $\mathscr{P}(X)$) d'inclusion n'est pas une relation d'équivalence car elle n'est pas symétrique.

3.2.1 Classe d'équivalence

Soit $\mathscr{R}$ une relation d'équivalence.

Définition 3.8 : (*Classe d'équivalence*)

Soit $x \in X$, on appelle la ***classe d'équivalence*** de x le sous-ensemble de X, notée $[x]$ ou $\dot{x}$ ou $\overline{x}$ ou encore $\mathrm{Cl}_{\mathscr{R}}(x)$, et défini par :

$$\mathrm{Cl}_{\mathscr{R}}(x) = \dot{x} = \overline{x} = [x] = \left\{ y \in X \;\middle|\; x \mathscr{R} y \right\}$$

Exemple :

— $[x] \subset X$.

— On a $[x] \neq \emptyset$ car $x \mathscr{R} x$ (par réflexivité de $\mathscr{R}$), $\implies x \in [x]$.

Définition 3.9 : (*Ensemble quotient*)

L'ensemble des classes d'équivalence est appelé ***ensemble quotient*** de X par la relation d'équivalence $\mathscr{R}$. On le note $X/_{\mathscr{R}}$:

$$X/_{\mathscr{R}} = \{[x] \mid x \in X\}$$

Exemple :

1. $X/_{\mathscr{R}} \subset \mathscr{P}(X)$.
2. L'ensemble quotient $X/_{\mathscr{R}}$ est un ensemble d'ensembles, c'est-à-dire un ensemble dont les éléments sont des ensembles.
3. La réunion de toutes les classes d'équivalence est égale à X.

   Les classes d'équivalence forment donc une partition de X.

3.2.2 Relation de congruence

Définition 3.10 : (*Congruence modulo n*)

Soit $n \in \mathbb{N}^*$ et $(x;y) \in \mathbb{Z}^2$. On dit que x est ***congru*** à y modulo n si $y-x$ est divisible par n. On notera $x \equiv y\,[n]$.

$$x \equiv y\,[n] \iff \exists k \in \mathbb{Z}, \quad y-x = kn.$$

Propriété 3.11 : (*La congruence modulo n est une relation d'équivalence*)

Pour $n \in \mathbb{N}^*$, la relation $\mathscr{R}$ notée aussi $\equiv_n$ qui est la relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

Preuve :

→ Réflexivité : $x \mathscr{R} x \iff x \equiv x\,[n]$. En effet, $x-x = 0 = 0 \times n$.

→ Symétrie : On suppose que $x \mathscr{R} y \iff x \equiv y\,[n] \implies \exists k \in \mathbb{Z}, y-x = kn \iff \exists k \in \mathbb{Z}, x-y = -kn$, avec $-k \in \mathbb{Z} \implies y \equiv x\,[n] \iff y \mathscr{R} x$.

→ Transitivité :

$$\begin{cases} x \mathscr{R} y \iff x \equiv y\,[n] \\ y \mathscr{R} z \iff y \equiv z\,[n] \end{cases} \iff \begin{cases} y-x = k_1 n \quad (\text{avec } k_1 \in \mathbb{Z}) \\ z-y = k_2 n \quad (\text{avec } k_2 \in \mathbb{Z}) \end{cases}$$

$\implies z-x = k_1 n + k_2 n = n(k_1+k_2) \iff z-x = nk_3$ (avec $k_3 \in \mathbb{Z}$) $\iff x \equiv z\,[n] \iff x \mathscr{R} z$.

→ Détermination de la classe de $x \in \mathbb{Z}$:

$$[x] = \{y \in \mathbb{Z} \mid x \equiv y\,[n]\}.$$

Or $x \equiv y\,[n] \iff \exists k \in \mathbb{Z}, y-x = kn \implies y = x+kn \implies [x] = \{x+kn \mid k \in \mathbb{Z}\}$

Finalement, on note l'ensemble quotient $\mathbb{Z}/_{\equiv\cdot\,[n]}$ par $\mathbb{Z}/n\mathbb{Z}$ ($\mathbb{Z}$ sur $n\mathbb{Z}$).

Définition 3.12 : ($\mathbb{Z}/n\mathbb{Z}$)

On appelle $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n.

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/_{\equiv\cdot\,[n]} = \mathbb{Z}/_{\equiv_n} = \{\text{classes d'équivalence de } \mathbb{Z} \text{ par la relation } \equiv_n\}$$

Il est important de comprendre que $\mathbb{Z}/n\mathbb{Z}$ est une **notation** pour l'ensemble quotient de $\mathbb{Z}$ par la relation d'équivalence de congruence modulo n.

En effet, $n\mathbb{Z}$ n'est pas une relation mais un ensemble.

On utilise la notation $\mathbb{Z}/n\mathbb{Z}$ pour aléger la notation $\mathbb{Z}/_{\equiv_n}$ qui est plus lourde à écrire.

De manière générale :

$$\boxed{\mathbb{Z}/n\mathbb{Z} = \{[0]; [1]; \ldots; [n-2]; [n-1]\}}$$

Exemple :

Pour $n = 2 \implies \mathbb{Z}/2\mathbb{Z} = \{[x] \mid x \in \mathbb{Z}\}$. On a $[x] = \{x+2k \mid k \in \mathbb{Z}\}$.

$$[0] = \{2k \mid k \in \mathbb{Z}\} = \{\text{entiers pairs}\}$$

$$[1] = \{1+2k \mid k \in \mathbb{Z}\} = \{\text{entiers impairs}\}$$

$$[2] = \{2+2k \mid k \in \mathbb{Z}\} = [0]$$

$$[3] = \{3+2k \mid k \in \mathbb{Z}\} = \{1+2(k+1) \mid k \in \mathbb{Z}\} = [1].$$

Donc $\mathbb{Z}/2\mathbb{Z} = \{[0]; [1]\}$.

Pour $n=3 \implies \mathbb{Z}/3\mathbb{Z} = \{[x] \mid x \in \mathbb{Z}\}$. On a $[x] = \{x+3k \mid k \in \mathbb{Z}\}$.

$$[0] = \{3k \mid k \in \mathbb{Z}\} = \{\text{multiples de 3}\}$$

$$[1] = \{1+3k \mid k \in \mathbb{Z}\} = \{\text{entiers dont le reste de la division par 3 est 1}\}$$

$$[2] = \{2+3k \mid k \in \mathbb{Z}\} = \{\text{entiers dont le reste de la division par 3 est 2}\}$$

$$[3] = [0]; \quad [4] = [1]; \quad [27] = [0].$$

Donc $\mathbb{Z}/3\mathbb{Z} = \{[0]; [1]; [2]\}$.

3.2.3 Caractérisation des relations d'équivalence

Propriété 3.13 : (*$X/_{\mathscr{R}}$ est une partition de X*)

Soit X un ensemble et soit $\mathscr{R}$ une relation d'équivalence sur X : l'ensemble $X/_{\mathscr{R}}$ est une partition de X.

Rappel : On dit que $Q \subset \mathscr{P}(X)$ est une partition si :

i) $\forall A, B \in Q,\ A \neq B \implies A \cap B = \emptyset$.

ii) $\forall x \in X, \exists A \in Q,\ x \in A$.

Preuve :

Il faut montrer que $X/_{\mathscr{R}} = \{[x] \mid x \in X\} \subset \mathscr{P}(X)$ est une partition.

i) Soient $[x], [y] \in X/_{\mathscr{R}}$ tels que $[x] \neq [y]$. Est-ce que $[x] \neq [y] \implies [x] \cap [y] = \emptyset$? On va montrer que la contraposée est vraie : $[x] \cap [y] \neq \emptyset \overset{?}{\implies} [x] = [y]$.

$$[x] \cap [y] \neq \emptyset \iff \exists z \in [x] \cap [y]$$

$$\iff \exists z \in [x] \text{ et } z \in [y]$$

$$\begin{cases} z \in [x] \iff x \mathscr{R} z \\ z \in [y] \iff y \mathscr{R} z \overset{\text{Sym.}}{\implies} z \mathscr{R} y \end{cases}$$

$\mathscr{R}$ étant une relation d'équivalence $\implies$ par transitivité $x \mathscr{R} z$ et $z \mathscr{R} y \implies x \mathscr{R} y$.

$\rightarrow$ Soit $x_1 \in [x] \iff \begin{cases} x_1 \mathscr{R} x \overset{\text{trans.}}{\implies} x_1 \mathscr{R} y \\ x \mathscr{R} y \end{cases}$

$\iff x_1 \in [y]$, d'où $[x] \subset [y]$ et par symétrie $[y] \subset [x]$.

$\implies [x] = [y]$, donc la contraposée est vraie.

ii) $\forall x \in X, \exists A \in X/_{\mathscr{R}}$ tel que $x \in A = [x]$.

On a $x \in [x]$ par réflexivité.

$\implies X/_{\mathscr{R}}$ est une partition de X (i.e. $X/_{\mathscr{R}} \in \mathscr{P}(X)$).

Propriété 3.14 : (*Toute partition définit une relation d'équivalence*)

Soit X un ensemble et $Q \subset \mathscr{P}(X)$ (une partition de X).

La relation binaire :

$$x \mathscr{R}_Q y \iff \exists A \in Q \text{ t.q. } \{x; y\} \subset A, \quad x, y \in X,$$

est une relation d'équivalence dont la partition associée est Q.

Preuve :

→ Relation d'équivalence :

① $\mathscr{R}_Q$ est réflexive : En effet, Q est une partition donc $\forall x \in X, \exists A \in Q,\ x \in A$, or $x \in A \iff \{x\} \subset A \iff \{x;x\} \subset A \iff x \mathscr{R}_Q x$.

② $\mathscr{R}_Q$ est symétrique : En effet, $x \mathscr{R}_Q y \iff \exists A \in Q$ t.q. $\{x;y\} \subset A \iff \exists A \in Q$ t.q. $\{y;x\} \subset A \iff y \mathscr{R}_Q x$.

③ $\mathscr{R}_Q$ est transitive : En effet, $x \mathscr{R}_Q y$ et $y \mathscr{R}_Q z$

$$\iff \begin{cases} \exists A \in Q \text{ t.q. } \{x;y\} \subset A \\ \exists B \in Q \text{ t.q. } \{y;z\} \subset B \end{cases}$$

Or $A, B \in Q$ et $y \in A \cap B \implies A \cap B \neq \emptyset \implies A = B$ (car Q est une partition, i.e. $Q \in \mathscr{P}(X)$).

$$\implies \{x;y;z\} \subset A \implies \{x;z\} \subset A \implies x \mathscr{R}_Q z.$$

→ La partition associée à $\mathscr{R}_Q$ est Q :

i.e. $X/_{\mathscr{R}_Q} = Q$.

Soit $[x] \in X/_{\mathscr{R}_Q}$. Puisque $x \in X$ et $Q \in \mathscr{P}(X) : \exists! A \in Q$ t.q. $x \in A$.

Soit $y \in [x] \implies x \mathscr{R}_Q y \implies \exists B \in Q$ t.q. $\{x;y\} \subset B$.

Or $x \in A$ et $x \in B \implies A \cap B \neq \emptyset \implies A = B \implies y \in A$.

Donc $[x] \subset A$. Réciproquement : soit $y \in A \implies \{x;y\} \subset A \implies x \mathscr{R}_Q y \implies y \in [x]$.

Donc $A \subset [x]$, d'où $[x] = A$. Ainsi $X/_{\mathscr{R}_Q} = Q$.

3.3 Relation d'ordre

Définition 3.15 : (*Relation d'ordre*)

Soit X un ensemble et soit $\mathscr{R}$ une relation binaire sur X.

On dit que $\mathscr{R}$ est une ***relation d'ordre*** si :

i) $\mathscr{R}$ est ***réflexive*** : $\forall x \in X,\ x \mathscr{R} x$.

ii) $\mathscr{R}$ est ***anti-symétrique*** : $\forall (x;y) \in X^2,\ x \mathscr{R} y$ et $y \mathscr{R} x \implies x = y$.

iii) $\mathscr{R}$ est ***transitive*** : $\forall (x;y;z) \in X^3,\ x \mathscr{R} y$ et $y \mathscr{R} z \implies x \mathscr{R} z$.

On note généralement une relation d'ordre en remplaçant $\mathscr{R}$ par $\leqslant$ (même si ce n'est pas toujours l'ordre usuel) ou encore pour bien inssister qu'il ne s'agit pas de la relation d'ordre uselle par $\preccurlyeq$.

Exemple :

i) Sur $\mathbb{R}$, la relation $\leqslant$ est une relation d'ordre (appelée **ordre usuel**).

ii) Sur $\mathscr{P}(X)$, la relation $\subset$ (inclusion) est une relation d'ordre.

iii) Sur $\mathbb{N}^*$, la relation de divisibilité $|$ est une relation d'ordre :

$$a \mid b \iff \exists k \in \mathbb{N},\ b = k \cdot a.$$

iv) La relation $\leqslant$ sur $\mathbb{R}$ n'est pas une relation d'équivalence car elle n'est pas symétrique.

3.3.1 Ordre total et ordre partiel

Définition 3.16 : (*Ordre total et ordre partiel*)

Soit $(X, \preccurlyeq)$ un ensemble muni d'une relation d'ordre.

— On dit que l'ordre est ***total*** si deux éléments quelconques de X sont toujours comparables :

$$\forall (x;y) \in X^2, \quad x \preccurlyeq y \text{ ou } y \preccurlyeq x.$$

— On dit que l'ordre est ***partiel*** si elle n'est pas total, c'est-à-dire s'il existe au moins deux éléments non comparables :

$$\exists (x;y) \in X^2, \quad x \not\preccurlyeq y \text{ et } y \not\preccurlyeq x.$$

Exemple :

i) $(\mathbb{R}, \leqslant)$ est un ensemble **totalement ordonné** : deux réels sont toujours comparables.

ii) $(\mathscr{P}(X), \subset)$ est un ensemble **partiellement ordonné** (si $\text{card}(X) \geqslant 2$) :

$$\text{Si } A = \{1\} \text{ et } B = \{2\}, \text{ alors } A \not\subset B \text{ et } B \not\subset A.$$

iii) $(\mathbb{N}^*, |\,)$ (où $|$ est la relation « divise ») est un ensemble **partiellement ordonné** :

$$2 \nmid 3 \text{ et } 3 \nmid 2 \text{ donc } 3 \text{ et } 2 \text{ ne sont pas comparable.}$$

3.3.2 Éléments remarquables d'un ensemble ordonné

Définition 3.17 : (*Majorant, minorant, maximum, minimum*)

Soit $(X, \leqslant)$ un ensemble ordonné et soit $A \subset X$.

— Un élément $M \in X$ est un ***majorant*** de A si :

$$\forall a \in A, \quad a \leqslant M.$$

— Un élément $m \in X$ est un ***minorant*** de A si :

$$\forall a \in A, \quad m \leqslant a.$$

— Un élément $M \in A$ est le ***maximum*** de A (noté $\max A$) si :

$$M \in A \quad \text{et} \quad \forall a \in A, \quad a \leqslant M.$$

— Un élément $m \in A$ est le ***minimum*** de A (noté $\min A$) si :

$$m \in A \quad \text{et} \quad \forall a \in A, \quad m \leqslant a.$$

Exemple :

— Un majorant (ou minorant) n'appartient pas nécessairement à A.

— Le maximum et le minimum, s'ils existent, sont **uniques** (par anti-symétrie).

— $\max A$ existe $\Longrightarrow$ A est majorée, mais la réciproque est fausse en général.

Exemple :

i) Dans $(\mathbb{R}, \leqslant)$, pour $A = [0;1[$:

- Majorants : tous les réels $\geqslant 1$
- Minorants : tous les réels $\leqslant 0$
- $\min A = 0$ (existe et appartient à A)
- $\max A$ n'existe pas ($1 \notin A$)

ii) Dans $(\mathscr{P}(\{1;2\}), \subset)$, pour $A = \{\emptyset, \{1\}\}$:

- Majorants : $\{1\}, \{1;2\}$
- Minorant : $\emptyset$
- $\max A = \{1\}$
- $\min A = \emptyset$

3.3.3 Borne supérieure et borne inférieure

Définition 3.18 : (*Borne supérieure et borne inférieure*)

Soit $(X, \leqslant)$ un ensemble ordonné et soit $A \subset X$.

- La ***borne supérieure*** de A (notée $\sup A$) est le **plus petit des majorants** de A :

$$\sup A = \min \{M \in X \mid \forall a \in A,\ a \leqslant M\}.$$

- La ***borne inférieure*** de A (notée $\inf A$) est le **plus grand des minorants** de A :

$$\inf A = \max \{m \in X \mid \forall a \in A,\ m \leqslant a\}.$$

Propriété 3.19 : (*Lien entre extrema et bornes*)

Soit $A \subset X$ dans un ensemble ordonné $(X, \leqslant)$.

- Si $\max A$ existe, alors $\sup A$ existe et $\sup A = \max A$.
- Si $\min A$ existe, alors $\inf A$ existe et $\inf A = \min A$.

Exemple :

Dans $(\mathbb{R}, \leqslant)$:

A	$\sup A$	$\inf A$	$\max A$	$\min A$
$[0;1]$	1	0	1	0
$[0;1[$	1	0	n'existe pas	0
$]0;1[$	1	0	n'existe pas	n'existe pas
$\mathbb{N}$	$+\infty$	0	n'existe pas	0

3.3.4 Propriété de la borne supérieure dans $\mathbb{R}$

Théorème 3.20 : (*Propriété de la borne supérieure (Axiome de complétude de $\mathbb{R}$)*)

Toute partie non vide et majorée de $\mathbb{R}$ admet une borne supérieure dans $\mathbb{R}$.

Autrement dit :

$$\forall A \subset \mathbb{R}, \quad A \neq \emptyset \text{ et } A \text{ majorée} \implies \sup A \in \mathbb{R}.$$

Exemple :

— Cette propriété **caractérise** $\mathbb{R}$: elle est fausse dans $\mathbb{Q}$.

— Exemple dans $\mathbb{Q}$: $A = \{x \in \mathbb{Q} \mid x^2 < 2\}$ est majorée dans $\mathbb{Q}$ mais $\sup A = \sqrt{2} \notin \mathbb{Q}$.

— Par symétrie, toute partie non vide et minorée de $\mathbb{R}$ admet une borne inférieure dans $\mathbb{R}$.

3.3.5 Récapitulatif des types de relations

Exemple :

Tableau récapitulatif des propriétés des relations binaires :

Type de relation	**Réflexive**	**Symétrique**	**Transitive**
Relation d'équivalence	Oui	Oui	Oui
Relation d'ordre	Oui	Non (anti-symétrique)	Oui

Différence clé :

— Une relation d'**équivalence partitionne** l'ensemble en classes disjointes.

— Une relation d'**ordre structure** l'ensemble en permettant de comparer les éléments.

Chapitre 4

Applications

4.1 Généralités sur les applications

Définition 4.1 : (*Application*)

Soient X et Y deux ensembles non vides. Une ***application*** f de X dans Y est une correspondance qui à tout élément $x \in X$ associe un **unique** élément $y \in Y$, appelé **image** de x par f et noté $f(x)$.

On note :

$$f : \begin{cases} X \longrightarrow Y \\ x \longmapsto f(x) \end{cases} \quad \text{ou} \quad \begin{array}{rccc} f : & X & \longrightarrow & Y \\ & x & \longmapsto & f(x) \end{array}$$

X est l'***ensemble de départ*** (ou domaine de définition) et Y est l'***ensemble d'arrivée*** (ou codomaine).

Exemple :

Changer X, Y, ou la relation $x \mapsto f(x)$ change l'application.

Définition 4.2 : (*Graphe d'une application*)

Le ***graphe*** de $f : X \to Y$ est l'ensemble :

$$\Gamma_f = \{(x, f(x)) \mid x \in X\} \subset X \times Y.$$

4.2 Image directe et image réciproque

Définition 4.3 : (*Image directe*)

Soit $f : X \to Y$ et $A \subset X$. L'***image directe*** de A par f est :

$$f(A) = \{f(x) \mid x \in A\} = \{y \in Y \mid \exists x \in A,\ y = f(x)\} \subset Y.$$

En particulier, $f(X)$ est appelé ***image*** de f.

Propriété 4.4 : (*Propriétés de l'image directe*)

Soient $f : X \to Y$, $A_0 \subset A_1 \subset X$ et $B_0, B_1 \subset X$. Alors :

(a) Si $A_0 \subset A_1$, alors $f(A_0) \subset f(A_1)$.

(b) $f(A_0 \cup A_1) = f(A_0) \cup f(A_1)$.

(c) $f(A_0 \cap A_1) \subset f(A_0) \cap f(A_1)$ (l'inclusion peut être stricte).

Preuve :

(b) : Soit $y \in f(A_0 \cup A_1) \iff \exists x \in A_0 \cup A_1,\ y = f(x) \iff \exists x \in A_0$ ou $x \in A_1,\ y = f(x) \iff y \in f(A_0) \vee y \in f(A_1) \iff y \in f(A_0) \cup f(A_1)$.

(c) : Soit $y \in f(A_0 \cap A_1) \implies \exists x \in A_0 \cap A_1,\ y = f(x) \implies x \in A_0$ et $x \in A_1 \implies y \in f(A_0)$ et $y \in f(A_1) \implies y \in f(A_0) \cap f(A_1)$.

L'inclusion peut être stricte : exemple $f : \{a, b\} \to \mathbb{R}$, $f(a) = f(b) = 1$, $A_0 = \{a\}$, $A_1 = \{b\}$, $A_0 \cap A_1 = \emptyset$, $f(\emptyset) = \emptyset$ mais $f(A_0) \cap f(A_1) = \{1\}$.

Définition 4.5 : (*Image réciproque*)

Soit $f : X \to Y$ et $B \subset Y$. L'***image réciproque*** de B par f est :

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

⚠Ne pas confondre $f^{-1}(B)$ (image réciproque d'un ensemble, toujours définie) et f^{-1} (application réciproque, définie seulement si f est bijective). ⚠

Propriété 4.6 : (*Propriétés de l'image réciproque*)

Soient $f : X \to Y$ et $B_0, B_1 \subset Y$. Alors :

(a) Si $B_0 \subset B_1$, alors $f^{-1}(B_0) \subset f^{-1}(B_1)$.

(b) $f^{-1}(B_0 \cup B_1) = f^{-1}(B_0) \cup f^{-1}(B_1)$.

(c) $f^{-1}(B_0 \cap B_1) = f^{-1}(B_0) \cap f^{-1}(B_1)$.

(d) $f^{-1}(B_0 \setminus B_1) = f^{-1}(B_0) \setminus f^{-1}(B_1)$.

(e) $f^{-1}(C_Y B) = C_X f^{-1}(B)$.

Propriété 4.7 : (*Relations entre image directe et image réciproque*)

Soient $f : X \to Y$, $A \subset X$ et $B \subset Y$. Alors :

(a) $A \subset f^{-1}(f(A))$ (avec égalité si f est injective).

(b) $f(f^{-1}(B)) \subset B$ (avec égalité si f est surjective).

4.3 Injections, surjections, bijections

Définition 4.8 : (*Application injective*)

L'application $f : X \to Y$ est dite ***injective*** si tout élément de Y possède **au plus** un antécédent par f :

$$\forall x_1, x_2 \in X, \quad f(x_1) = f(x_2) \implies x_1 = x_2.$$

(De manière équivalente par contraposée : $x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$.)

Définition 4.9 : (*Application surjective*)

L'application $f : X \to Y$ est dite ***surjective*** si tout élément de Y possède **au moins** un antécédent :

$$\forall y \in Y, \exists x \in X, \quad f(x) = y.$$

Autrement dit : $f(X) = Y$.

Définition 4.10 : (*Application bijective*)

L'application $f : X \to Y$ est dite ***bijective*** si elle est à la fois injective et surjective, c'est-à-dire si tout élément de Y possède un **unique** antécédent :

$$\forall y \in Y, \exists! x \in X, \quad f(x) = y.$$

Exemple :

1. $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto 2x - 3$ est bijective.
2. $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ n'est ni injective ($f(1) = f(-1)$) ni surjective ($-1 \notin f(\mathbb{R})$).
3. $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto \cos x$ est ni injective ni surjective.
4. $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^3$ est bijective.
5. $f : \mathbb{R} \to \mathbb{R}_+^*$, $x \mapsto e^x$ est bijective.

Propriété 4.11 : (*Critère d'injectivité via les images réciproques*)

$f : X \to Y$ est injective si et seulement si pour tout $y \in Y$, $f^{-1}(\{y\})$ est soit vide soit un singleton.

Propriété 4.12 : (*Caractérisation de l'injectivité*)

Soit $f : X \to Y$. Les assertions suivantes sont équivalentes :

(1) f est injective.

(2) Pour tous $A, B \in \mathscr{P}(X)$, $f(A \cap B) = f(A) \cap f(B)$.

(3) Pour tout $A \subset X$, $f^{-1}(f(A)) = A$.

4.4 Composition des applications

Définition 4.13 : (*Application composée*)

Soient $f : X \to Y$ et $g : Y \to Z$ deux applications (telles que l'ensemble d'arrivée de f est l'ensemble de départ de g). On définit l'***application composée*** $g \circ f$ par :

$$\begin{array}{rccc} g \circ f : & X & \longrightarrow & Z \\ & x & \longmapsto & (g \circ f)(x) = g(f(x)) \end{array}$$

On lit « g rond f ».

Exemple :

En général, $f \circ g \neq g \circ f$.

Propriété 4.14 : (*Composition et injectivité/surjectivité*)

Soient $f : A \to B$ et $g : B \to C$ deux applications. Alors :

(1) $g \circ f$ injective $\implies$ f injective.

(2) $g \circ f$ surjective $\implies$ g surjective.

(3) Si f et g sont injectives (resp. surjectives, bijectives), alors $g \circ f$ est injective (resp. surjective, bijective).

Preuve :

(1) : Supposons $g \circ f$ injective. Soient $x_1, x_2 \in A$ tels que $f(x_1) = f(x_2)$. Alors $g(f(x_1)) = g(f(x_2))$, i.e. $(g \circ f)(x_1) = (g \circ f)(x_2)$. Par injectivité de $g \circ f$, $x_1 = x_2$. Donc f est injective.

(2) : Supposons $g \circ f$ surjective. Soit $z \in C$. $\exists x \in A$ tel que $(g \circ f)(x) = z$, i.e. $g(f(x)) = z$. Posons $y = f(x) \in B$, alors $g(y) = z$. Donc g est surjective.

4.5 Application réciproque

Définition 4.15 : (*Application réciproque*)

Soit $f : X \to Y$ une bijection. L'***application réciproque*** de f, notée f^{-1}, est l'application :

$$\begin{array}{rccc} f^{-1}: & Y & \longrightarrow & X \\ & y & \longmapsto & \text{l'unique } x \in X \text{ tel que } f(x) = y \end{array}$$

Propriété 4.16 : (*Caractérisation de la bijectivité*)

$f : X \to Y$ est bijective si et seulement s'il existe $g : Y \to X$ telle que :

$$g \circ f = \mathrm{Id}_X \quad \text{et} \quad f \circ g = \mathrm{Id}_Y.$$

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

Propriété 4.17 : (*Propriétés de la réciproque*)

Si $f : X \to Y$ est bijective :

(1) $f^{-1} \circ f = \mathrm{Id}_X$ et $f \circ f^{-1} = \mathrm{Id}_Y$.

(2) f^{-1} est bijective et $(f^{-1})^{-1} = f$.

(3) Si $g : Y \to Z$ est aussi bijective, alors $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Exemple :

1. $\exp : \mathbb{R} \to \mathbb{R}_+^*$, $x \mapsto e^x$ est bijective, de réciproque $\ln : \mathbb{R}_+^* \to \mathbb{R}$.
2. $f : \mathbb{R}^3 \to \mathbb{R}^3$, $f(x,y,z) = (x-y+2z, -x+y-z, 2x-y+z)$: étudier l'injectivité, la surjectivité, la bijectivité et déterminer f^{-1} si elle existe (voir Examen 08/01/2013).

4.6 Fonction indicatrice

Définition 4.18 : (*Fonction indicatrice*)

Soit E un ensemble et $A \subset E$. La ***fonction indicatrice*** (ou caractéristique) de A est l'application $\mathbb{1}_A : E \to \{0,1\}$ définie par :

$$\mathbb{1}_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases}$$

Propriété 4.19 : (*Propriétés des fonctions indicatrices*)

Soient $A, B \subset E$. Alors :

(a) $\mathbb{1}_{A \cap B} = \mathbb{1}_A \cdot \mathbb{1}_B$.

(b) $\mathbb{1}_{\complement_E A} = 1 - \mathbb{1}_A$.

(c) $\mathbb{1}_{A \cup B} = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_A \cdot \mathbb{1}_B$.

(d) $\mathbb{1}_{A \setminus B} = \mathbb{1}_A(1 - \mathbb{1}_B) = \mathbb{1}_A - \mathbb{1}_A \cdot \mathbb{1}_B$.

(e) $\mathbb{1}_{A \Delta B} = \mathbb{1}_A + \mathbb{1}_B - 2\mathbb{1}_A\mathbb{1}_B$ (différence symétrique $A \Delta B = (A \setminus B) \cup (B \setminus A)$).

(f) $A = B \iff \mathbb{1}_A = \mathbb{1}_B$.

4.7 Cardinal d'un ensemble fini

Définition 4.20 : (*Ensemble fini, cardinal*)

Un ensemble E est dit ***fini*** s'il existe $n \in \mathbb{N}$ et une bijection de $\{1, \dots, n\}$ sur E.

L'entier n est unique et s'appelle le ***cardinal*** de E, noté $\text{card}(E)$ ou $|E|$.

Par convention, $\text{card}(\emptyset) = 0$.

Propriété 4.21 : (*Dénombrement des applications*)

Soient E et F deux ensembles finis avec $\text{card}(E) = n$ et $\text{card}(F) = p$.

(1) Le nombre d'applications de E dans F est p^n.

(2) Le nombre d'injections de E dans F (avec $p \geqslant n$) est $p(p-1)\cdots(p-n+1) = \dfrac{p!}{(p-n)!}$.

(3) Le nombre de bijections de E dans F (si $p = n$) est $n!$.

Propriété 4.22 : (*Cardinal de $\mathscr{P}(A)$*)

Si A est un ensemble fini à n éléments, alors $\text{card}(\mathscr{P}(A)) = 2^n$.

Preuve :

On construit une bijection entre $\mathscr{P}(A)$ et les applications de A dans $\{0,1\}$ via les fonctions indicatrices : à $B \subset A$ on associe $\mathbb{1}_B$. Le nombre de telles applications est 2^n. D'après la Prop précédente avec $p = 2$, on a bien $\text{card}(\mathscr{P}(A)) = 2^n$.

Exemple :

On peut montrer qu'il n'existe pas de bijection entre $\mathscr{P}(X)$ et X (même si X est infini), par l'argument diagonal de Cantor.

Chapitre 5

Groupes

5.1 Loi de composition interne

Définition 5.1 : (*Loi de composition interne (LCI)*)

Soit E un ensemble.

Une ***loi de composition interne*** sur E est une application T définie par :

$$\begin{array}{rccc} T: & E\times E & \longrightarrow & E \\ & (x,y) & \longmapsto & x\,T\,y = T(x,y) \end{array}$$

Autrement dit, c'est une application qui à tout couple (x,y) d'éléments de E associe un élément de E (stabilité).

Exemple :

1. L'addition $+$ et la multiplication $\times$ sont des LCI sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.
2. La soustraction n'est pas une LCI sur $\mathbb{N}$ (car $1-2\notin\mathbb{N}$), mais l'est sur $\mathbb{Z}$.
3. La composition $\circ$ est une LCI sur l'ensemble des applications de E dans E.
4. Sur $\mathbb{R}\setminus\{1\}$, la loi $x*y=x+y-xy$ est une LCI (à vérifier : $x*y=1-(1-x)(1-y)\neq 1$ si $x\neq 1$ et $y\neq 1$).

Définition 5.2 : (*Propriétés d'une LCI*)

Soit T une LCI sur E.

- T est ***associative*** si : $\forall x,y,z\in E,\ (x\,T\,y)\,T\,z = x\,T\,(y\,T\,z)$.
- T est ***commutative*** si : $\forall x,y\in E,\ x\,T\,y = y\,T\,x$.
- $e\in E$ est un ***élément neutre*** pour T si : $\forall x\in E,\ e\,T\,x = x\,T\,e = x$.
- Soit e l'élément neutre. $x'\in E$ est un ***symétrique*** (ou inverse) de x pour T si : $x\,T\,x' = x'\,T\,x = e$.

Propriété 5.3 : (*Unicité de l'élément neutre et du symétrique*)

(1) S'il existe, l'élément neutre est unique.

(2) Si T est associative et si x admet un symétrique, celui-ci est unique.

Preuve :

(1) : Supposons e et e' deux éléments neutres. Alors $e = e\,T\,e' = e'$ (en utilisant que e' est neutre puis que e est neutre).

(2) : Supposons x' et x'' deux symétriques de x. Alors : $x' = x'\,T\,e = x'\,T\,(x\,T\,x'') = (x'\,T\,x)\,T\,x'' = e\,T\,x'' = x''$.

5.2 Notion de groupe

Définition 5.4 : (*Groupe*)

On dit que $(G,*)$ est un ***groupe*** si $*$ est une LCI sur G vérifiant :

G1. Associativité : $\forall x,y,z\in G,\ (x*y)*z=x*(y*z)$.

G2. Élément neutre : $\exists e\in G,\ \forall x\in G,\ e*x=x*e=x$.

G3. Symétrique : $\forall x\in G,\ \exists x^{-1}\in G,\ x*x^{-1}=x^{-1}*x=e$.

Si de plus $*$ est commutative, on dit que $(G,*)$ est un ***groupe abélien*** (ou commutatif).

Exemple :

1. $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ sont des groupes abéliens.
2. $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$ sont des groupes abéliens.
3. $(\mathbb{N},+)$ n'est pas un groupe (pas de symétrique pour $n\geqslant 1$).
4. $(\mathbb{Z},\times)$ n'est pas un groupe (pas de symétrique pour $|n|\geqslant 2$).
5. $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe abélien.
6. $(\mathscr{P}(X),\Delta)$ est un groupe abélien (élément neutre $\emptyset$, tout élément est son propre symétrique).
7. $(U_1,\times)$ où $U_1=\{z\in\mathbb{C}\mid |z|=1\}$ est un groupe abélien.

Propriété 5.5 : (*Propriétés dans un groupe*)

Soit $(G,*)$ un groupe d'élément neutre e. Pour tous $x,y\in G$:

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

(2) $(x*y)^{-1}=y^{-1}*x^{-1}$.

(3) **Lois de simplification :** $x*y=x*z\implies y=z$ (simplification à gauche) et $y*x=z*x\implies y=z$ (simplification à droite).

(4) L'équation $a*x=b$ (resp. $x*a=b$) a une unique solution $x=a^{-1}*b$ (resp. $x=b*a^{-1}$).

5.3 Sous-groupes

Définition 5.6 : (*Sous-groupe*)

Soit $(G,*)$ un groupe. Un sous-ensemble $H \subset G$ est un ***sous-groupe*** de G si $(H,*)$ est lui-même un groupe, c'est-à-dire :

SG1. $H \neq \emptyset$ (ou de manière équivalente $e \in H$).

SG2. $\forall x, y \in H,\ x * y \in H$ (stabilité).

SG3. $\forall x \in H,\ x^{-1} \in H$ (stabilité par passage au symétrique).

Exemple :

Les conditions 2 et 3 peuvent se remplacer par une seule : $\forall x, y \in H,\ x * y^{-1} \in H$.

Propriété 5.7 : (*Intersection de sous-groupes*)

Si G_1 et G_2 sont deux sous-groupes de G, alors $G_1 \cap G_2$ est un sous-groupe de G.

Propriété 5.8 : (*Réunion de sous-groupes*)

$G_1 \cup G_2$ est un sous-groupe de G si et seulement si $G_1 \subset G_2$ ou $G_2 \subset G_1$.

Propriété 5.9 : (*Sous-groupes de $\mathbb{Z}$*)

Les sous-groupes de $(\mathbb{Z},+)$ sont exactement les ensembles de la forme :

$$k\mathbb{Z} = \{kn \mid n \in \mathbb{Z}\}, \quad k \in \mathbb{N}.$$

Preuve :

$k\mathbb{Z}$ **est un sous-groupe :** $0 = k \cdot 0 \in k\mathbb{Z}$, si $x = km$ et $y = kn$ alors $x + y = k(m+n) \in k\mathbb{Z}$, $-x = k(-m) \in k\mathbb{Z}$.

Tout sous-groupe est de cette forme : Soit G un sous-groupe de $\mathbb{Z}$. Si $G = \{0\}$, alors $G = 0\mathbb{Z}$. Sinon, G contient un élément non nul ℓ, donc aussi $-\ell$, donc G contient un entier strictement positif. Posons $k = \min\{\ell \in \mathbb{N}^*, \ell \in G\}$. Montrons $G = k\mathbb{Z}$:

- Si $\ell \in G$, alors $\ell\mathbb{Z} \subset G$ (par stabilité).
- Soit $g \in G$. Par division euclidienne, $g = kq + r$ avec $0 \leqslant r < k$. Or $r = g - kq \in G$ (stabilité). Par minimalité de k, $r = 0$. Donc $g = kq \in k\mathbb{Z}$.

Exemple :

Les sous-groupes de $(\mathbb{Z},+)$ sont $\{0\} = 0\mathbb{Z}$, $\mathbb{Z} = 1\mathbb{Z}$, $2\mathbb{Z}$ (entiers pairs), $3\mathbb{Z}$, etc.

5.4 Morphismes de groupes

Définition 5.10 : (*Morphisme de groupes*)

Soient $(G,*)$ et $(H,\cdot)$ deux groupes. Une application $f : G \to H$ est un ***morphisme de groupes*** (ou homomorphisme) si :

$$\forall x, y \in G, \quad f(x * y) = f(x) \cdot f(y).$$

Propriété 5.11 : (*Propriétés des morphismes*)

Soit $f : G \to H$ un morphisme de groupes, e_G (resp. e_H) l'élément neutre de G (resp. H). Alors :

(1) $f(e_G) = e_H$.

(2) $\forall x \in G$, $f(x^{-1}) = (f(x))^{-1}$.

(3) $f(G)$ (l'image de f) est un sous-groupe de H.

(4) $\mathrm{Ker}(f) = f^{-1}(\{e_H\}) = \{x \in G \mid f(x) = e_H\}$ est un sous-groupe de G, appelé ***noyau*** de f.

Propriété 5.12 : (*Injectivité et noyau*)

Un morphisme $f : G \to H$ est injectif si et seulement si $\mathrm{Ker}(f) = \{e_G\}$.

Preuve :

($\Longrightarrow$) : Si f est injective et $x \in \mathrm{Ker}(f)$, alors $f(x) = e_H = f(e_G)$, donc $x = e_G$.

($\Longleftarrow$) : Si $\mathrm{Ker}(f) = \{e_G\}$ et $f(x) = f(y)$, alors $f(x \cdot y^{-1}) = f(x) \cdot f(y)^{-1} = e_H$, donc $x * y^{-1} \in \mathrm{Ker}(f) = \{e_G\}$, d'où $x * y^{-1} = e_G$, soit $x = y$.

Définition 5.13 : (*Isomorphisme, automorphisme*)

— Un ***isomorphisme*** est un morphisme bijectif.

— Un ***automorphisme*** est un isomorphisme de G dans lui-même.

— On dit que G et H sont ***isomorphes*** ($G \simeq H$) s'il existe un isomorphisme de G dans H.

Exemple :

1. $f : (\mathbb{R},+) \to (\mathbb{R}_+^*,\times)$, $x \mapsto e^x$ est un isomorphisme (réciproque : ln).
2. $f : (\mathbb{Z},+) \to (k\mathbb{Z},+)$, $n \mapsto kn$ est un isomorphisme pour tout $k \neq 0$.
3. $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $k \mapsto \bar{k}$ est un morphisme surjectif de noyau $n\mathbb{Z}$.
4. Les racines n-ièmes de l'unité $R_n = \{e^{2i\pi k/n} \mid k = 0,\dots,n-1\}$ forment un sous-groupe de $(U_1,\times)$ isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$.

Propriété 5.14 : (*Morphismes de* $(\mathbb{Z},+)$)

Tout morphisme de $(\mathbb{Z},+)$ dans $(\mathbb{Z},+)$ est de la forme $n \mapsto kn$ pour un certain $k \in \mathbb{Z}$.

— Il est injectif ssi $k \neq 0$.

— Il est surjectif ssi $k = \pm 1$.

Propriété 5.15 : ($(\mathbb{Z}/n\mathbb{Z},+)$ *est un groupe abélien*)

La loi $\bar{x}+\bar{y}=\overline{x+y}$ est bien définie sur $\mathbb{Z}/n\mathbb{Z}$ et munit cet ensemble d'une structure de groupe abélien, d'élément neutre $\bar{0}$, et où le symétrique de $\bar{x}$ est $\overline{-x}$.

Propriété 5.16 : (*Critère d'abélianité*)

Soit $(G,*)$ un groupe. Alors G est abélien si et seulement si l'application $x \mapsto x^{-1}$ est un morphisme de G.

Chapitre 6

Constitution des réels

6.1 Corps des réels

Définition 6.1 : (*Corps*)

Un ***corps*** est un ensemble $\mathbb{K}$ muni de deux LCI $+$ et $\times$ telles que :

C1. $(\mathbb{K}, +)$ est un groupe abélien, d'élément neutre 0.

C2. $(\mathbb{K}^*, \times)$ est un groupe abélien, d'élément neutre 1.

C3. Distributivité : $\forall x, y, z \in \mathbb{K},\ x \times (y+z) = x \times y + x \times z$.

Exemple :

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps. $\mathbb{Z}$ n'est pas un corps (les entiers $\geqslant 2$ n'ont pas d'inverse pour $\times$).

Définition 6.2 : (*Corps ordonné*)

Un corps $(\mathbb{K}, +, \times)$ est dit ***ordonné*** si l'on dispose d'une relation d'ordre $\leqslant$ compatible avec les opérations, c'est-à-dire :

(1) $\forall x, y, z \in \mathbb{K},\ x \leqslant y \implies x+z \leqslant y+z$.

(2) $\forall x, y, z \in \mathbb{K},\ x \leqslant y$ et $0 \leqslant z \implies xz \leqslant yz$.

6.2 Propriété de la borne supérieure

Définition 6.3 : (*Majorant, minorant, borne supérieure, borne inférieure*)

Soit $A \subset \mathbb{R}$, $A \neq \emptyset$.

— $M \in \mathbb{R}$ est un ***majorant*** de A si $\forall a \in A,\ a \leqslant M$.

— $m \in \mathbb{R}$ est un ***minorant*** de A si $\forall a \in A,\ a \geqslant m$.

— A est ***majorée*** (resp. ***minorée***) si elle admet un majorant (resp. minorant).

— A est ***bornée*** si elle est à la fois majorée et minorée.

— S'il existe, le plus petit des majorants de A s'appelle la ***borne supérieure*** de A, notée $\sup A$.

— S'il existe, le plus grand des minorants de A s'appelle la ***borne inférieure*** de A, notée $\inf A$.

Théorème 6.4 : (*Théorème de la borne supérieure (propriété fondamentale de $\mathbb{R}$)*)

Toute partie non vide et majorée de $\mathbb{R}$ admet une borne supérieure.

Toute partie non vide et minorée de $\mathbb{R}$ admet une borne inférieure.

Exemple :

Ce théorème caractérise la **complétude** de $\mathbb{R}$. Il est faux dans $\mathbb{Q}$: par exemple $A = \{x \in \mathbb{Q} \mid x^2 < 2\}$ est majorée dans $\mathbb{Q}$ mais $\sup A = \sqrt{2} \notin \mathbb{Q}$.

Propriété 6.5 : (*Caractérisation de* $\sup A$)

Soit $A \subset \mathbb{R}$ non vide et majorée, et $M \in \mathbb{R}$. Alors :

$$M = \sup A \iff \begin{cases} \forall a \in A,\ a \leqslant M & (M \text{ est majorant}) \\ \forall \varepsilon > 0,\ \exists a_\varepsilon \in A,\ a_\varepsilon > M - \varepsilon & (M \text{ est le plus petit}) \end{cases}$$

6.3 Propriété d'Archimède

Propriété 6.6 : (*Propriété d'Archimède*)

$\mathbb{R}$ est ***archimédien*** : pour tout $\varepsilon > 0$ et tout $x \in \mathbb{R}$, il existe $n \in \mathbb{N}$ tel que $n\varepsilon > x$.

En particulier :

$$\forall \varepsilon > 0,\ \exists n \in \mathbb{N}^*,\ \frac{1}{n} < \varepsilon.$$

Définition 6.7 : (*Partie entière*)

Pour tout $x \in \mathbb{R}$, il existe un unique entier $n \in \mathbb{Z}$ tel que $n \leqslant x < n+1$. Cet entier n est appelé ***partie entière*** de x et noté $\lfloor x \rfloor$ ou $\mathrm{E}(x)$.

6.4 Densité de $\mathbb{Q}$ dans $\mathbb{R}$

Propriété 6.8 : (*Densité de* $\mathbb{Q}$ *dans* $\mathbb{R}$)

Entre deux réels quelconques $x < y$, il existe un rationnel $r \in \mathbb{Q}$ tel que $x < r < y$.

Autrement dit, tout intervalle ouvert non vide de $\mathbb{R}$ contient un rationnel.

Propriété 6.9 : (*Densité des irrationnels dans* $\mathbb{R}$)

Entre deux réels quelconques $x < y$, il existe un irrationnel $z \in \mathbb{R} \setminus \mathbb{Q}$ tel que $x < z < y$.

6.5 Construction de $\mathbb{R}$

L'ensemble $\mathbb{R}$ peut être construit de plusieurs façons équivalentes à partir de $\mathbb{Q}$:

- **Coupures de Dedekind :** $\mathbb{R}$ est l'ensemble des coupures de Dedekind dans $\mathbb{Q}$, i.e. les partitions $(\mathbb{Q}_1, \mathbb{Q}_2)$ de $\mathbb{Q}$ avec $\mathbb{Q}_1 < \mathbb{Q}_2$ élément par élément et $\mathbb{Q}_1$ sans maximum.
- **Suites de Cauchy :** $\mathbb{R}$ est le complété de $\mathbb{Q}$ pour la distance usuelle, obtenu comme ensemble des classes d'équivalence de suites de Cauchy de rationnels.

Théorème 6.10 : (*Caractérisation de* $\mathbb{R}$)

$\mathbb{R}$ est l'unique corps totalement ordonné et complet (au sens de la propriété de la borne supérieure).

Plus précisément, si $\mathbb{K}$ est un corps totalement ordonné et vérifiant la propriété de la borne supérieure, alors $\mathbb{K}$ est isomorphe à $\mathbb{R}$ (en tant que corps ordonné).

Exemple :

La propriété de la borne supérieure est ce qui distingue $\mathbb{R}$ de $\mathbb{Q}$: $\mathbb{Q}$ est un corps totalement ordonné, archimédien, mais pas complet.

Définition 6.11 : (*Nombres réels et représentation décimale*)

Tout réel $x \in [0,1[$ admet une ***développement décimal*** :

$$x = \sum_{n=1}^{+\infty} \frac{a_n}{10^n} = ,a_1 a_2 a_3 \dots$$

où $a_n \in \{0,1,\dots,9\}$. Ce développement est unique si l'on impose que la suite (a_n) ne soit pas ultimement constante égale à 9.

Un réel est rationnel si et seulement si son développement décimal est **ultimement périodique**.

Exemple :

$\pi = 3{,}14159265\dots$ est irrationnel (et même transcendant). $\sqrt{2} = 1{,}41421356\dots$ est irrationnel.

$\frac{1}{3} = ,333\dots = 0,\overline{3}$ est rationnel avec développement périodique.