Cours de mathématiques
Partie I – Les fondements
MPSI 4

Alain TROESCH

Version du:

19 octobre 2014

Table des matières

1 Fondements logiques

« La logique est la jeunesse des mathématiques »

(Bertrand Russell)

« La logique est l'hygiène des mathématiques »

(André Weil)

« La logique n'a ni à inspirer l'invention, ni à l'expliquer ; elle se contente de la contrôler et de la vérifier. »

(Louis Couturat)

Ce chapitre a pour but d'introduire les concepts fondamentaux des mathématiques, à savoir les bases-même du raisonnement mathématique : la logique formelle et la notion de démonstration. Évidemment, la logique formelle n'est qu'une mise en forme rigoureuse de la structure de la pensée et du cheminement logique, et ne peut en rien remplacer l'intuition qui seule permet de savoir quel chemin prendre. Pour terminer cette très brève introduction par une dernière citation d'un grand mathématicien du XX^{e} siècle :

*« Car le monde des Idées excède infiniment nos possibilités opératoires, et c'est dans l'intuition que réside l'*ultima ratio *de notre foi en la vérité d'un théorème - un théorème étant, selon une étymologie aujourd'hui bien oubliée, l'objet d'une vision. »*

(René Thom)

I Logique propositionnelle

I.1 Construction formelle d'une formule

La logique propositionnelle est l'étude des formules abstraites qu'on peut écrire à partir d'un certain nombre de variables propositionnelles, représentées par des lettres. Nous nous donnons initialement un ensemble de propositions abstraites (ou *variables propositionnelles*). Les lettres que nous utiliserons (à part celles désignant des formules) désignent ces propositions. Une proposition peut être vraie ou fausse.

Définition 1.1.1 (Formule propositionnelle)

Une *formule propositionnelle* est une succession de caractères, égaux soit à une variable propositionnelle, soit à un symbole $\neg$, $\vee$, $\wedge$, $\Longrightarrow$, $\Longleftrightarrow$, (ou), et pouvant être construites à partir des variables propositionnelles à l'aide des règles suivantes :

- Si P est une variable propositionnelle, alors P est une formule propositionnelle ;

- Si F est une formule propositionnelle, alors $\neg F$ est une formule propositionnelle (*négation* de F)
- Si F et G sont des formules propositionnelles, alors $(F \vee G)$ est une formule propositionnelle (*disjonction* « ou non exclusif »)
- Si F et G sont des formules propositionnelles, alors $(F \wedge G)$ est une formule propositionnelle (*conjonction* « et »)
- Si F et G sont des formules propositionnelles, alors $(F \Longrightarrow G)$ est une formule propositionnelle (*implication*)
- Si F et G sont des formules propositionnelles, alors $(F \Longleftrightarrow G)$ est une formule propositionnelle (*équivalence*)

Toute chaîne de caractère ne pouvant pas être obtenue par applications successives de ces règles en nombre fini n'est pas une formule propositionnelle.

Il s'agit de ce qu'on appelle une « définition inductive », proche d'une définition par récurrence (on donne un ensemble initial, les variables propositionnelles, puis on construit l'ensemble des formules par étape, une étape consistant à appliquer à toutes les formules déjà obtenues chacune des règles ci-dessus). À toute définition inductive correspond une définition par minimalité : ainsi, l'ensemble des formules propositionnelles peut aussi être défini comme le plus petit sous-ensemble de l'ensemble de tous les mots sur l'alphabet constitué des variables propositionnelles, des symboles logiques ci-dessus et des parenthèses, et stable par les constructions ci-dessus.

Remarque 1.1.2

Une formule propositionnelle est ainsi définie de façon purement formelle, comme une succession de caractères, sans pour le moment donner de sens précis à cette succession de caractères.

Exemple 1.1.3 (Formules propositionnelles)

Dans cet exemple, P, Q, R désignent des variables propositionnelles.

1. Ceci est une formule : $((P \Longrightarrow Q) \vee Q) \Longrightarrow ((R \wedge P) \Longleftrightarrow \neg Q)$.
   On n'affirme pas si elle est vraie ou fausse.
2. Ceci n'est pas une formule : $(P \Longrightarrow) \vee R \wedge$
3. Ceci n'est *stricto sensu* par une formule : $P \vee Q$
   En effet il manque les parenthésages. On considérera que lorsqu'il n'y a pas ambiguïté, on peut se dispenser des parenthésages. Par exemple, on peut montrer que $((P \vee Q) \vee R)$ et $(P \vee (Q \vee R))$ sont deux formules « équivalentes » (ce qui s'exprime en disant que $\vee$ est associatif). On s'autorisera à écrire $P \vee Q \vee R$.

I.2 Véracité d'une formule

Chacune des variables apparaissant dans une formule peut prendre la valeur de vérité « vrai » ou « faux ».

Définition 1.1.4 (Distribution de valeurs de vérités)

On appelle distribution de valeurs de vérité sur un ensemble $\mathcal{P}$ de variables propositionnelles une fonction $\delta : \mathcal{P} \longrightarrow \{V, F\}$, où V désigne la valeur de vérité « Vrai » et F désigne la valeur de vérité « Faux ».

Ainsi, une distribution de valeurs de vérité est une façon d'associer à chaque variable une valeur de vérité, Vrai ou Faux.
Étant donnée une formule R construite à partir des variables propositionnelles de $\mathcal{P}$, toute distribution de valeurs de vérité sur $\mathcal{P}$ définit une valeur de vérité pour R.

Exemple 1.1.5 (Valeur de vérité d'une formule)

- Étant donné P et Q deux variables, et R la formule $R = P \wedge Q$, si P prend la valeur V et Q la valeur F (on définit ainsi une distribution de valeurs de vérité), alors $R = P \wedge Q$ prend la valeur F.
- Plus généralement, la formule R ci-dessus ne prend la valeur de vérité V que si P et Q sont vraies toutes les deux.

Définition 1.1.6 (Table de vérité d'une formule)

La table de vérité d'une formule R est un tableau donnant les valeurs de vérité de la formule R en fonction des valeurs de vérité des variables. Ce tableau donne une énumération de toutes les distributions de valeurs de vérités sur l'ensemble des variables propositionnelles utilisées.

L'exemple donné ci-dessus permet d'obtenir sans peine la table de vérité de la conjonction. Remarquez que pour obtenir cette table, on est parti de l'interprétation intuitive qu'on a du « et ». Mais il faut voir les choses dans l'autre sens. La table de vérité définit le comportement du symbole $\wedge$ vis-à-vis des valeurs de vérité. La table est donc à voir comme une définition qui permet de retrouver ensuite l'interprétation intuitive du symbole.
On définit de même les tables des différentes constructions logiques élémentaires, de façon à coller avec leur interprétation intuitive :

Définition 1.1.7 (Définition de l'interprétation sémantique des connecteurs logiques)

Soit P, Q deux variables propositionnelles. Les tables de vérité des formules $\neg P$, $(P \vee Q)$, $(P \wedge Q)$, $(P \Longrightarrow Q)$ et $(P \Longleftrightarrow Q)$ sont définies par :

P	$\neg P$
V	F
F	V

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

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

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

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

Remarque 1.1.8

1. La table de vérité de l'implication peut être un peu troublante à première vue. Si P est faux, alors, quelle que soit la valeur de vérité de Q, $P \Longrightarrow Q$ est vraie. En effet, si l'hypothèse est fausse, la conclusion peut être vraie ou fausse sans que ça contredise l'implication. Cela se comprend mieux en considérant la négation. Dire qu'une implication $P \Longrightarrow Q$, est fausse, c'est dire que malgré le fait que l'hypothèse P soit vraie, la conclusion Q est fausse. cela correspond à $P \wedge \neg Q$, qui n'est vraie que si P est vraie et Q est faux. On retrouve la table de $P \Longrightarrow Q$ en reprenant la négation.
2. Il résulte de cette remarque que dire que $P \Longrightarrow Q$ est vraie ne sous-entend nullement la véracité de P. Ainsi, « $P \Longrightarrow Q$ » n'est pas équivalent à « P donc Q », qui affirme la véracité de P.
   Il convient donc de faire attention à la rédaction : **le symbole « $\Longrightarrow$ » ne peut pas remplacer le mot « donc »**
3. La même remarque vaut pour l'équivalence.
4. Par ailleurs, puisque si P est faux, $P \Longrightarrow Q$ est toujours vrai, pour montrer que $P \Longrightarrow Q$ est vrai, il suffit de se placer dans le cas où P est vrai : on suppose que P est vrai, on montre que Q aussi. Cela correspond à l'interprétation « Si P est vrai, alors Q est vrai ». En revanche, on n'a pas de contrainte lorsque P est faux.
5. Ne pas confondre :
   - P est une condition suffisante à Q : $P \Longrightarrow Q$;

- P est une condition nécessaire à Q : $Q \Longrightarrow P$;
- P est une condition nécessaire et suffisante à Q : $P \Longleftrightarrow Q$.

6. Pour montrer une équivalence $P \Longleftrightarrow Q$, n'oubliez pas de montrer les *deux* implications $P \Longrightarrow Q$ et $Q \Longrightarrow P$. N'oubliez pas la réciproque SVP.

Exemples 1.1.9

1. L'implication suivante est « démontrable » :

   « *Si* $10^n + (-1)^n$ *est divisible par 11, alors* $10^{n+1} + (-1)^{n+1}$ *est divisible par 11.* »

   Pourtant, $10^n + (-1)^n$ n'est divisible par 11 pour aucune valeur de n !
2. Autour de CN et CS (compléter par CN, CS ou CNS) :
   - « n est multiple de 6 » est une ..... pour que n soit paire mais pas une ..... .
   - $x = 1$ est une ..... pour que $x^2 = 1$, mais pas une ..... . En revanche, si x est réel, $x = 1$ est une ..... pour que $x^3 = 1$.
   - Si f est dérivable sur $\mathbb{R}$, $f'(0) = 0$ est une ..... pour que f admette un extremum local en 0, mais ce n'est pas une ..... .

Remarque 1.1.10

On distingue implication formelle et implication sémantique (relation de cause à effet). Par exemple, le grand théorème de Fermat ayant été démontré il y a quelques années, la proposition suivante est vraie :

« *Si le théorème de Fermat est faux, alors les oranges sont bleues* »

En revanche, une telle implication ne traduit aucune relation de cause à effet !

À l'aide des tables de vérité des connecteurs, si on connaît la table de vérité de deux formules F et G, on peut déterminer la table des formules $\neg F$, $F \vee G$, $F \wedge G$, $F \Longrightarrow G$ et $F \Longleftrightarrow G$. Ainsi, connaissant l'expression d'une formule, on peut, en un nombre fini d'étapes, en déterminer la table de vérité.

Exemples 1.1.11

Déterminer les tables de vérité des formules suivantes :

1. $P \vee \neg P$
2. $((P \Longrightarrow Q) \wedge (P \Longrightarrow R)) \Longleftrightarrow ((S \vee P) \vee R)$
3. $(P \vee Q) \vee R$ et $P \vee (Q \vee R)$

I.3 Équivalences entre formules, tautologies

Définition 1.1.12 (formules équivalentes)

On dit que deux formules F et G sont équivalentes et on note $F \equiv G$, ou parfois abusivement $F = G$, si F et G ont même table de vérité.

Par exemple, l'exemple ci-dessus prouve rigoureusement une remarque faite un peu plus haut concernant l'associativité de $\vee$:

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

Propriétés 1.1.13 (quelques équivalences entre formules)

On a les équivalences suivantes (P, Q, R désignent des formules quelconques) :

1. $(P \vee Q) \vee R \equiv P \vee (Q \vee R)$ *(associativité de $\vee$)*
2. $P \vee Q \equiv Q \vee P$ *(commutativité de $\vee$)*
3. $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$ *(associativité de $\wedge$)*
4. $P \wedge Q \equiv Q \wedge P$ *(commutativité de $\wedge$)*
5. $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$ *(distributivité)*
6. $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$ *(distributivité)*
7. $P \vee P \equiv P$
8. $P \wedge P \equiv P$
9. $(P \iff Q) \equiv (P \implies Q) \wedge (Q \implies P)$ *(principe de la double implication)*
10. $(P \implies Q) \equiv (\neg Q \implies \neg P)$ *(principe de la contraposée)*
11. $P \implies (Q \vee R) \equiv (P \wedge \neg Q) \implies R$
12. $(P \vee Q) \implies R \equiv (P \implies R) \wedge (Q \implies R)$ *(disjonction de cas)*
13. $P \implies Q \equiv \neg P \vee Q$.

Les propriétés suivantes permettent d'écrire la négation formelle de toute formule :

Propriétés 1.1.14 (négation d'une formule)

On a les équivalences de formules suivantes (P et Q sont des formules) :

1. $\neg\neg P \equiv P$
2. $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$ *(loi de De Morgan)*
3. $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$ *(loi de De Morgan)*
4. $\neg(P \implies Q) \equiv P \wedge \neg Q$
5. $\neg(P \iff Q) \equiv (P \iff (\neg Q)) \equiv ((\neg P) \iff Q)$.

Il faut savoir nier de façon automatique une proposition formelle. La rapidité et la fiabilité de vos démonstrations par l'absurde ou par la contraposée en dépendent. Entraînez-vous pour gagner les bons automatismes.

Exemples 1.1.15

Niez les propositions suivantes :

1. $((A \implies B) \wedge C) \vee \neg B$
2. $(((A \iff B) \vee C) \implies B) \iff A$

Il existe une classe particulière de formules, celles dont la table de vérité est toujours vraie, quelles que soient les valeurs de vérité des variables propositionnelles. Ce sont les formules qui sont toujours vraies.

Définition 1.1.16 (Tautologie)

Une *tautologie* est une formule F qui prend la valeur de vérité Vrai quelle que soit la distribution de vérité donnée sur les variables intervenant dans F.

Par exemple $P \vee \neg P$ est une tautologie. Ainsi, les tautologies sont exactement toutes les formules équivalentes à $P \vee \neg P$. Ces formules donnent les règles de base du raisonnement formel.

Proposition 1.1.17 (Quelques tautologies)

Les formules suivantes sont des tautologies :

1. $P \vee \neg P$ *(principe du tiers exclus)*
2. $P \Longrightarrow P$
3. $P \Longleftrightarrow P$
4. $P \Longrightarrow P \vee Q$
5. $P \wedge Q \Longrightarrow P$
6. $(P \wedge (P \Longrightarrow Q)) \Longrightarrow Q$ *(modus ponens)*
7. $((P \Longrightarrow Q) \wedge (Q \Longrightarrow R)) \Longrightarrow (P \Longrightarrow R)$ *(transitivité de* $\Longrightarrow$*)*
8. *etc.*

I.4 Démonstration formelle

Pour établir une théorie mathématique, nous ne pouvons pas partir de rien : il faut supposer un certain nombre d'axiomes, qui définiront le contexte dans lequel on travail (comme par exemple le 5^{e} postulat d'Euclide qui définit l'environnement euclidien, mais qui pourrait être remplacé par un autre axiome définissant des géométries dans d'autres contextes). Notons $\mathcal{A}$ cet ensemble d'axiomes (il s'agit donc d'un ensemble de formules).

Définition 1.1.18 (Conséquence sémantique, HP)

Soit F une formule. On dit que F est conséquence sémantique de $\mathcal{A}$ si toute distribution de vérité qui rend vraies toutes les formules de $\mathcal{A}$ rend aussi F vraie : si les axiomes sont vérifiés, alors F aussi.

L'examen des tables de vérité nous donne une façon de vérifier (de façon un peu fastidieuse si une formule est conséquence sémantique de $\mathcal{A}$. Mais il ne s'agit pas d'une démonstration au sens mathématique du terme : on ne donne pas d'explication ou de preuve logique (c'est-à-dire de lien de cause à effet). On peut définir formellement ce qu'est une démonstration mathématique d'une formule à partir d'un ensemble d'axiomes.

Définition 1.1.19 (Démonstration d'une formule, HP)

On dit que F est prouvable à partir de $\mathcal{A}$ s'il existe une suite finie $F_1, \ldots, F_n$ de formules telles que $F_n = F$ et que pour tout $i \in [\![1, n]\!]$, F_i soit obtenue d'une des façons suivante à partir des formules précédentes :

- $F_i \in \mathcal{A}$ (prise d'hypothèse : F_i est un axiome)
- F_i est une tautologie (donc toujours vraie)
- il existe $j < i$ et $k < i$ tels que $F_k = (F_j \Longrightarrow F_i)$ (utilisation du modus ponens)

Ainsi, démontrer une formule F se fait par déductions successives : pour chaque étape, on peut utiliser soit les axiomes, soit les tautologies, soit le modus ponens (déduction logique).

Cette définition d'une démonstration nécessite de connaître les tautologies. On peut se restreindre à un ensemble de tautologies classiques, que l'on utilise souvent sans même s'en rendre compte (transitivité de $\Longrightarrow$, associativité etc). Il existe d'autres façons de définir la notion de démonstration, ne faisant pas appel aux tautologies (on peut d'ailleurs dans ce cas démontrer les tautologies à partir d'un ensemble vide d'axiomes), mais les règles sont un peu plus délicates à exprimer.

Le théorème suivant est juste donné pour votre culture, sans démonstration.

Théorème 1.1.20 (Complétude du calcul propositionnel, HP, admis)
La formule F est conséquence sémantique de l'ensemble d'axiomes $\mathcal{A}$ si et seulement si F est prouvable à partir de $\mathcal{A}$.

Nous terminons ce paragraphe sur la logique propositionnelle par la remarque suivante : cette logique est largement insuffisante pour exprimer la plupart des propriétés mathématiques, notamment celles faisant appel à des variables x. Ainsi, l'énoncé :

« il existe $d \neq 1, n$ tel que d divise n »

ne peut pas être écrit en terme du langage propositionnel ; il ne peut qu'être représenté par une variable propositionnelle, ce qui est très restrictif. C'est plus généralement le cas dès lors qu'une variable donnée intervient dans toute une partie d'une formule : toute cette partie restera « indécomposable » dans le calcul propositionnel, même si elle est constituée d'implications, conjonctions, disjonctions...
Il nous faut donc introduire de nouveau objets formels permettant de gérer cette situation. Il s'agit des quantificateurs. Les formules ainsi obtenues sont appelées prédicats du premier ordre.

II Calcul des prédicats du premier ordre

II.1 Construction formelle d'une formule du calcul des prédicats

Un *prédicat du premier ordre* se définit à peu près de la même façon qu'une formule propositionnelle. Les variables propositionnelles sont remplacées par des « formules atomiques », qui sont des relations ou équations portant sur des « termes » (mathématiques), décrits à l'aide d'un certain nombre d'opérations portant sur des variables ou des constantes. Pour indiquer la dépendance d'une formule atomique F en une variable x, nous écrirons $F(x)$. Nous ne définissons pas de façon rigoureuse la notion de terme et de formule atomique, ce qui nécessiterait trop de technique. Nous renvoyons aux exemples pour une compréhension intuitive de cette notion.

Définition 1.2.1 (Prédicat du premier ordre, quantificateurs)
Les prédicats du premier ordre sont définis à partir des formules atomiques par les mêmes règles qui permettent de définir les formules propositionnelles à partir des variables propositionnelles, mais en ajoutant deux symboles $\forall$ (« quel que soit », ou quantificateur universel) et $\exists$ (« il existe », ou quantificateur existentiel), et les deux règles associées suivantes :
- Si $F(x, y_1, \ldots, y_n)$ est un prédicat (dépendant des variables $x, y_1, \ldots, y_n$), alors $\exists x, F(x, y_1, \ldots, y_n)$ est un prédicat (ne dépendant plus que des variables $y_1, \ldots, y_n$).
- Si $F(x, y_1, \ldots, y_n)$ est un prédicat (dépendant des variables $x, y_1, \ldots, y_n$), alors $\forall x, F(x, y_1, \ldots, y_n)$ est un prédicat (ne dépendant plus que des variables $y_1, \ldots, y_n$).

Exemple 1.2.2

1. $\forall x,\ x \geqslant 2 \Longrightarrow x^2 \geqslant 4$:
   x^2 est un terme, 4 aussi (terme de constante), et la relation $x^2 \geqslant 4$ est une formule atomique. De même x et 2 sont des termes, et $x \geqslant 2$ est une formule atomique ; le reste découle des constructions décrites à partir des formules atomiques.
   Par abus de notation, on abrège souvent la formule ci-dessus en : $\forall x \geqslant 2,\ x^2 \geqslant 4$.
2. Plus généralement, on s'autorisera à écrire $\forall x \in E,\quad F(x)$ au lieu de $\forall x,\quad x \in E \Longrightarrow F(x)$.
3. $\exists x,\quad (x \geqslant 0) \wedge (x^2 = 4)$
   Les formules atomiques sont ici $x \geqslant 0$ et $x^2 = 4$. On s'autorisera à écrire :

$$\exists x \geqslant 0,\quad x^2 = 4.$$

4. Plus généralement, on écrira $\exists x \in E,\ \ F(x)$ plutôt que $\exists x,\ (x \in E) \wedge F(x)$.

Note Historique 1.2.3

- Le symbole $\exists$ (E à l'envers) est introduit par Peano en 1885, puis repris par Russell et Frege.
- Le symbole $\forall$ (A à l'envers, pour « *alles* ») est introduit par Gentzen en 1935.

La construction formelle des prédicats du premier ordre n'est pas à connaître (hors-programme) ; en revanche, il est indispendable de bien savoir manipuler les symboles de quantification.

Dans un prédicat du premier ordre, certaines variables peuvent être quantifiées, d'autres non. Le prédicat ne dépend plus que des variables non quantifiées (ou au moins qui apparaissent dans une portion de la formule sur laquelle ne porte pas la quantification)

Définition 1.2.4 (variables libres, variables liées ou muettes)

- On dit qu'une variable x est *libre* s'il existe au moins une occurrence de x qui ne soit pas dans le champ d'un quantificateur (le cas le plus courant : x n'est pas quantifié)
- On dit qu'une variable x est *liée* (ou *muette*) si toutes ses occurrences sont quantifiées. Dans ce cas, on peut remplacer formellement dans la formule x par toute autre variable y (à condition que y n'intervienne pas dans la formule initiale)

Exemples 1.2.5

1. Soit la formule : $\exists x,\ x + y \leqslant 4$.

   y est une variable libre, x est une variable muette : on peut la remplacer par n'importe quelle autre variable, à l'exclusion de y qui est déjà utilisée. Ainsi, la formule ci-dessus est équivalente à :

   $$\exists z,\ z + y \leqslant 4.$$

2. Déterminer les variables libres et liées dans $(x^2 \geqslant 2) \wedge \forall x, \exists z, yx \leqslant z$

   Peut-on faire des substitutions de variables ? Si oui, lesquelles ?

3. A-t-on : $\exists x, \exists y,\ P(x, y) \equiv \exists y, \exists x,\ P(x, y)$?

   A-t-on : $\forall x, \forall y,\ P(x, y) \equiv \forall y, \forall x,\ P(x, y)$?

   A-t-on : $\forall x, \exists y,\ P(x, y) \equiv \exists y, \forall x,\ P(x, y)$? A-t-on une implication entre les deux expressions ?

Avertissement 1.2.6

- **Attention !** En général, on ne peut pas intervertir $\exists$ et $\forall$!
- Ne jamais utiliser les symboles de quantification dans une phrase : il s'agit d'un symbole mathématique, pas d'une abréviation.

Malgré l'introduction de ces nouveau symboles on peut se rendre compte facilement que les formules décrites encore une fois ne permettent pas d'énoncer toutes les propriétés mathématiques. En effet, les quantifications ne portent que sur des variables élémentaires. On ne peut pas quantifier des objets plus compliqués (comme des ensembles, ou des fonctions). Ainsi, un énoncé du type :

« Pour tout x dans E et y dans F, il existe une fonction $f : E \to F$ telle que $f(x) = y$ »

ne peut pas se traduire sous forme d'un prédicat du premier ordre. On peut définir des prédicats d'ordre 2, puis d'ordre 3 pour pallier au problème. Cette étude ne sera pas faite ici.

II.2 Règles concernant les quantificateurs

Propriétés 1.2.7 (Règles de distributivité)

Soit P, Q des prédicats. On a :

- $\forall x, (P \wedge Q) \equiv (\forall x P) \wedge (\forall x Q)$
- $\exists x, (P \vee Q) \equiv \exists x P \vee \exists x Q$

Remarque 1.2.8

A-t-on :

- $\forall x, (P \vee Q) \equiv \forall x P \vee \forall x Q$?
- $\exists x, (P \wedge Q) \equiv \exists x P \wedge \exists x Q$?

Propriétés 1.2.9

Si Q ne dépend pas de la variable x,

- $\forall x, (P(x) \vee Q) \equiv (\forall x P(x)) \vee Q$
- $\exists x, (P(x) \wedge Q) \equiv (\exists x P(x)) \wedge Q$

Propriétés 1.2.10 (Quantification d'une implication)

1. *Si la propriété P ne dépend pas de x,*
   - *(i)* $\forall x (P \Longrightarrow Q(x)) \equiv P \Longrightarrow (\forall x Q(x))$
   - *(ii)* $\exists x (P \Longrightarrow Q(x)) \equiv P \Longrightarrow (\exists x Q(x))$
2. *Si la propriété Q ne dépend pas de x,*
   - *(i)* $\forall x (P(x) \Longrightarrow Q) \equiv (\exists x P(x)) \Longrightarrow Q$
   - *(ii)* $\exists x (P(x) \Longrightarrow Q) \equiv (\forall x P(x)) \Longrightarrow Q$

Comme pour le calcul propositionnel, il est intéressant d'avoir des règles formelles pour nier facilement une expression du calcul des prédicats. Les règles de négation des connecteurs $\vee$, $\wedge$, $\Longrightarrow$ et $\Longleftrightarrow$ sont les mêmes que pour le calcul des prédicats. Ces règles sont complétées par les deux suivantes :

Propriétés 1.2.11 (Négation des quantificateurs)

(i) $\neg(\forall x P) \equiv \exists x (\neg P)$

(ii) $\neg(\exists x P) \equiv \forall x (\neg P)$.

Exemples 1.2.12

1. Non linéarité d'une fonction de $\mathbb{R}^n$ vers $\mathbb{R}^m$; exemple de $f : x \mapsto x^2$ de $\mathbb{R}$ dans $\mathbb{R}$.
2. Définition de la continuité d'une fonction f en x_0, puis négation. Exemple de la fonction H de Heaviside.

II.3 Valeur de vérité et démonstration

Tout comme pour le calcul propositionnel, on peut associer à chaque prédicat une valeur de vérité (après spécifications de valeurs pour chaque variable libre). On peut également définir une notion de démonstration formelle, en décrivant certaines règles de déduction. Il paraît alors naturel de penser que toute propriété vraie est démontrable, et réciproquement. La réciproque ne pose pas de problème (heureusement, sinon la notion de démonstration n'aurait pas de sens !). En revanche, vers 1930, Gödel a semé

le trouble en montrant qu'il existe des propriétés indécidables (donc ni démontrables ni réfutables). Sa démonstration porte sur une axiomatique de $\mathbb{N}$:

Théorème 1.2.13 (Gödel 1931, premier théorème d'incomplétude, HP, admis)
Étant donné une théorie axiomatique de $\mathbb{N}$ cohérente, il existe des propriétés indécidables par cette théorie.

Autrement dit, une telle propriété n'est pas démontrable, ni sa négation, alors que l'une des deux est vraie !
Le principe de la démonstration est assez simple, et repose sur un argument diagonal, procédé cher aux logiciens depuis Cantor. En revanche, la technique développée dans la preuve est redoutable, car la preuve repose sur la possibilité de numéroter chaque formule (c'est dans cette numérotation que réside l'utilisation de l'axiomatique de $\mathbb{N}$), donc d'établir une bijection entre $\mathbb{N}$ et l'ensemble des formules. Gödel construit cette numérotation de façon totalement explicite.

Note Historique 1.2.14
C'est Gödel qui, en 1931, montre l'existence de propriétés indémontrables. Il parvient à ce résultat, alors qu'il tente de compléter le « programme de Hilbert » datant de 1900, précisé en 1925, qui se voulait une réponse à la « crise des fondements » (dont on reparlera plus loin), et dont le but est de prouver intrinsèquement, par des manipulations algébriques finies, la cohérence des mathématiques. Gödel parviendra à montrer qu'on ne peut pas répondre à cette question, complétant ainsi le 2e des 23 problèmes de Hilbert conernant la cohérence de l'arithmétique. Personne à l'époque n'avait encore envisagé la possibilité que le Vrai et le Démontrable ne soit pas la même chose.
Le logicien allemand Gentzen a tout de même démontré cette cohérence en 1936, mais à l'aide d'une « récurrence transfinie », c'est à dire portant sur les ordinaux et non seulement sur les entiers. Mais c'est une démonstration qui n'est pas intrinsèque à l'arithmétique.

III Composition d'un texte mathématique

III.1 Description générale

Un texte mathématique est constitué de :

1. **définitions** : des descriptions de certains objets constituant les briques de la théorie. C'est à voir comme un raccourci de langage.
2. **résultats** : des énoncés mettant en jeu les objets définis dans la théorie, et donnant des propriétés vérifiées par ces objets. Un résultat s'énonce sous la forme $A \Longrightarrow B$. On distingue :
   - les *axiomes* : des résultats qui sont des vérités fondamentales de la théorie, et qu'on ne démontre pas (à considérer comme le cahier des charges de la théorie : on impose ces résultats, il n'y a donc pas besoin de les montrer) ;
   - les *théorèmes* : les résultats les plus significatifs, démontrés à partir des axiomes et de résultats démontrés antérieurement ;
   - les *propositions* : des résultats de moindre envergure ;
   - les *lemmes* : des résultats à voir comme des étapes vers des résultats plus consistants (résultats préliminaires, mais pouvant avoir leur intérêt en soi)
   - les *corollaires* : des conséquences assez immédiates d'autres résultats, par exemple des cas particuliers intéressants ;
3. **démonstrations** : des justifications de la véracité des résultats.
4. **exemples et contre-exemples :** pour illuster les notions, ou pour insister sur la nécessité d'une hypothèse (contre-exemple lorsque l'hypothèse est enlevée). Ces exemples ont pour but de développer l'intuition du lecteur

5. **remarques :** il peut s'agir de mises en garde pour ne pas tomber dans certains pièges, ou de préciser des situations typiques d'utilisation de certains résultats, ou encore de donner une digression sur des ouvertures possibles qu'apportent des notions introduites etc.
6. **conjectures** : des énoncés qu'on pense être vrais, mais qu'on n'a pas encore réussi à prouver.

Exemples 1.3.1

1. Le célèbre cinquième axiome d'Euclide, fondant la théorie de la géométrie euclidienne, stipule qu'il existe une seule droite parallèle à une droite donnée, et passant par un point donné. Il existe d'autres types de géométrie, définies en changeant cet axiome :
   - la géométrie de Lobatchevsky (ou géométrie hyperbolique), dans laquelle une droite admet une infinité de parallèles passant par un point donné ;
   - la géométrie sphérique, dans laquelle une droite n'admet pas d'autre parallèle qu'elle même (mais cette géométrie ne respecte pas non plus le premier axiome, stipulant que par deux points donnés passe une et une seule droite.)
2. Un énoncé s'exprime souvent sous la forme $A \Longrightarrow B$.
   La proposition A regroupe les *hypothèses*
   La proposition B regroupe les *conclusions.*
   Ne pas oublier de bien apprendre toutes les hypothèses d'un résultat. Par exemple, considérons le théorème suivant :
   Soit f une fonction dérivable sur un intervalle I. Si f' est positive sur I, alors f est croissante sur I.
   Il y a trois hypothèses dans cet énoncé : bien sûr, $f' \geqslant 0$, que personne n'oublie ; mais aussi f dérivable sur I (sans laquelle l'énoncé n'a pas de sens), et (plus souvent oubliée) le fait que I est un intervalle (sans quoi le résultat est faux !).

Note Historique 1.3.2

Le cinquième axiome (ou postulat) d'Euclide a longtemps été controversé, non pas pour sa véracité (il paraît suffisamment évident), mais plutôt pour la nécessité de le passer en axiome : on a longtemps cru qu'il pouvait se déduire des autres axiomes. Ainsi, de nombreux mathématiciens, parmi les plus célèbres, ont tenté de prouver cet axiome à l'aide des autres, notamment par l'absurde (Saccheri, Lambert, Legendre...). Le mathématicien russe Nicolaï Lobatchevski affirme en 1826 que le cinquième axiome ne découle pas des autres, et s'appuie sur une géométrique abstraite qu'il développe, respectant tous les axiomes d'Euclide sauf le cinquième.

III.2 Comment construire une démonstration

Dans un exercice ou un devoir, c'est au candidat de construire soi-même la démonstration. Il est donc intéressant d'avoir une démarche permettant d'aborder ces démonstrations de façon logique et structurée. Bien entendu, l'application formelle de ces règles n'est pas suffisante, il faut à un moment de la démonstration apporter une ou plusieurs idées personnelles !

La construction rigoureuse d'une preuve repose sur le principe de « déconstruction » formelle des formules logiques (terminologie personnelle). « Déconstruire » une formule logique revient à faire l'inverse du procédé qui a permi de construire la formule à partir de propositions élémentaires et des règles de construction (conjonction, disjonction, implication etc.), en appliquant à chaque étape de cette déconstruction un certain principe de démonstration.

Le point de départ consiste alors dans un premier temps à écrire le résultat à démontrer sous forme d'une formule logique (en y incluant les hypothèses, dans ce cas, on a un énoncé formel du type $A \Longrightarrow B$), puis d'appliquer les principes de démontration suivants (qui deviennent par la même occasion des principes de rédaction) :

Méthode 1.3.3 (Prouver une implication $A \Longrightarrow B$)

On suppose que A est vrai, on démontre B. La rédaction commence par *« Supposons que A est vrai »*.

Dans certaines situations, il peut être plus simple de montrer l'implication contraposée (voir plus loin). Y penser si on bloque !

Méthode 1.3.4 (Prouver une équivalence $A \Longleftrightarrow B$)

On prouve en deux temps $A \Longrightarrow B$ et $B \Longrightarrow A$. Éviter les démonstrations par équivalences, fréquentes sources d'erreurs (sur la validité des réciproques), sauf dans certaines situations bien balisées (résolutions d'équations...)

Méthode 1.3.5 (Prouver une conjonction $A \wedge B$)

On prouve en deux temps : on prouve A, puis on prouve B.

Méthode 1.3.6 (Prouver une disjonction $A \vee B$)

On prouve que $\neg A \Longrightarrow B$, ce qui revient à supposer que A n'est pas vrai, et à en déduire que B est vrai. On peut bien sûr intervertir A et B : un bon choix de la propriété que l'on nie peut parfois simplifier la démonstration.

Méthode 1.3.7 (Prouver $\forall x A$)

La proposition A doit être vraie pour tout choix de x. On pose donc un x **quelconque** (c'est-à-dire sur lequel on n'impose pas de condition), et on montre que pour ce x, A est vérifié. Le fait d'avoir choisi x quelconque montre qu'alors A est vrai pour tout x.
La démonstration débute alors systématiquement par *« Soit x ... »*, puis on démontre $A(x)$.

Méthode 1.3.8 (Prouver $\exists x A$)

Montrer une propriété existentielle est souvent ce qu'il y a de plus délicat. Dans le meilleur des cas, on est capable de définir explicitement une valeur de x qui convient (par exemple, si on montre que A est vrai pour $x = 3$, c'est suffisant). Il n'est pas toujours possible de construire facilement un tel x. Penser alors aux différents théorèmes du cours dont la conclusion s'exprime sous forme d'une existence. Pour trouver une valeur de x qui convient, on peut utiliser la méthode d'analyse-synthèse (voir plus loin)

Avertissement 1.3.9

Attention ! Trop déconstruire une formule peut parfois empêcher de voir la ressemblance avec une propriété du cours, et peut nuire à l'intuition. Ne pas le faire assez nuit très souvent à la rigueur de la rédaction. Il faut donc trouver un juste milieu.

Avertissement 1.3.10

La structure logique, puis les règles de la logique formelle, ne font que structurer la démonstration. Une bonne rédaction passe par une mise en langage de ces règles : on rédige toujours à l'aide de phrases, et non par un enchaînement de formules logiques absconses !

IV Quelques types classiques de démonstration

Nous mettons à part quelques types particuliers de démonstration, les plus fréquemment utilisés. À maîtriser !

IV.1 Le Modus ponens.

Méthode 1.4.1 (Modus ponens)

Pour que B soit vrai, il suffit que A soit vrai et que $A \Longrightarrow B$. Formellement :

$$(A \wedge (A \Longrightarrow B)) \Longrightarrow B$$

On vérifie donc l'hypothèse A, l'implication $A \Longrightarrow B$, et on conclut que la conclusion B est vraie.

Avertissement 1.4.2

Attention, $A \Longrightarrow B$ n'est pas suffisant. Si on veut obtenir B, il faut aussi justifier la véracité de A ! (différence entre « $\Longrightarrow$ » et « donc »)

Le *modus ponens* est donc à voir comme une formalisation du « donc », déduction logique.
La situation typique d'utilisation du *modus ponens* est l'emploi d'un théorème : celui-ci s'écrit $A \Longrightarrow B$, où A est l'hypothèse et B la conclusion. Ainsi, pour montrer B, on vérifie que l'hypothèse A est satisfaite, et on emploie le théorème $A \Longrightarrow B$. Le *modus ponens* nous permet de conclure que la conclusion B est vraie aussi.

Avertissement 1.4.3

Toujours bien préciser A et $A \Longrightarrow B$. En particulier, quand on utilise un théorème, toujours bien préciser le théorème utilisé d'une part (en donnant son nom), et la validité des hypothèses d'autre part.

Cela nécessite un apprentissage rigoureux du cours : la connaissance des hypothèses des théorèmes est aussi importante que la connaissance de leurs conclusions (c'est cette bonne connaissance des hypothèses qui assure aussi qu'on n'utilisera pas le théorème à tort et à travers dans des situations inadaptées).

IV.2 La transitivité de l'implication.

Méthode 1.4.4 (Transitivité de l'implication)

Il ne s'agit de rien de plus que d'enchaîner des modus ponens :

$$A \wedge (A \Longrightarrow A_1) \wedge (A_1 \Longrightarrow A_2) \wedge \cdots \wedge (A_{n-1} \Longrightarrow A_n) \wedge (A_n \Longrightarrow B) \Longrightarrow B.$$

C'est donc un raisonnement déductif en plusieurs étapes. La conclusion d'une étape fournit l'hypothèse de l'étape de modus ponens suivante.

La situation typique est celle d'une démonstration composée de plusieurs étapes (par exemple l'utilisation de plusieurs théorèmes).

Exemple 1.4.5

À l'aide du théorème de Rolle, montrer que si f est une fonction deux fois dérivable sur un intervalle $[a, b]$, et tel que $f(a) = f(b) = f'(a) = 0$, alors f'' s'annule en un point de $[a, b]$.

IV.3 Démonstration par la contraposée.

Il s'agit de l'utilisation de l'équivalence des deux propositions $A \Longrightarrow B$ et $\neg B \Longrightarrow \neg A$.

Méthode 1.4.6 (Démonstration par contraposée)

Pour montrer $A \Longrightarrow B$, on suppose que la conclusion B est fausse, et on montre que dans ce cas, l'hypothèse A ne peut pas être vraie. Cela revient à montrer $\neg G \Longrightarrow \neg A$.

Définition 1.4.7 (Contraposée)

L'expression $\neg B \Longrightarrow \neg A$ s'appelle la *contraposée* de $A \Longrightarrow B$.

Ce type de démonstration apparaît dans de nombreuses situations.

Exemples 1.4.8

1. Soit $n \in \mathbb{N}$. Montrer que si n^2 est pair, alors n est pair.
2. Soit A, B, C trois ensembles. Montrer, sans utiliser les règles opératoires sur les ensembles, que si $A \cap B = \varnothing$ et $A \cap C = \varnothing$, alors $A \cap (B \cup C) = \varnothing$.
3. Montrer que si $x_1 + \cdots + x_n = M$, alors il existe $i \in [\![1, n]\!]$ tel que $x_i \geqslant \frac{M}{n}$.

Avertissement 1.4.9

Ne pas confondre la contraposée $\neg B \Longrightarrow \neg A$ et l'expression $\neg A \Longrightarrow \neg B$, qui n'est pas équivalente à $A \Longrightarrow B$, mais à sa réciproque !

Un cas particulier important de démonstration par la contraposée est le cas de la démonstration par l'absurde. Il s'agit de la situation dans laquelle A est la propriété toujours vraie. Alors $\neg A$ est la propriété toujours fausse (il s'agit d'une contradition).

Méthode 1.4.10 (Cas particulier : démonstration par l'absurde)

Pour démontrer B, il suffit de montrer que le fait de supposer que B est fausse conduit à une contradiction.

Là encore, les démonstrations par l'absurde interviennent dans des situations très diverses. La démonstration par l'absurde la plus connue est certainement la démontration de Pythagore de l'irrationnalité de $\sqrt{2}$:

Exemples 1.4.11

1. Démonstration de l'irrationnalité de $\sqrt{2}$ (Pythagore).
2. Le principe diagonal utilisé dans la preuve du premier théorème d'incomplétude de Gödel repose sur une démonstration par l'absurde. De manière général, les démonstrations reposant sur un argument diagonal sont des démonstrations par l'absurde (Voir théorème de Cantor, un peu plus loin dans le cours).

IV.4 Disjonction des cas.

Ce principe de démonstration repose sur l'équivalence, déjà évoquée plus haut :

$$(A \vee B) \Longrightarrow C \equiv (A \Longrightarrow C) \wedge (B \Longrightarrow C).$$

Méthode 1.4.12 (Disjonction des cas)

Pour montrer $A \vee B \implies C$, on peut séparer en deux cas : voir ce qu'il se passe sous l'hypothèse A, puis sous l'hypothèse B. Ainsi on montre que si on suppose que A est vérifié, alors C aussi, et de même, si B est vérifié, C aussi.

Un cas particulièrement important est le cas où $A \vee B$ est la proposition certaine (A et B regroupe l'ensemble de tous les cas possibles). Dans ce cas, $(A \vee B) \implies C$ équivaut à C. On en déduit :

Méthode 1.4.13 (Démonstration par discussion)

Si $A \vee B$ est l'événement certain, pour montrer une proposition C, il suffit de montrer que A implique C, et que B implique C.

Évidemment, ce principe se généralise dans le cas où la disjonction comporte un plus grand nombre de termes.

Avertissement 1.4.14

Lors d'une démonstration par discussion, prenez garde à bien vérifier C dans tous les cas envisageables (s'assurer que la disjonction initiale est bien la proposition certaine)

Souvent, la discussion n'apparaît pas de façon explicite ; la nécessité de la discussion intervient de façon naturelle au cours de la démonstration. Ces discussions permettent souvent de gérer des cas particuliers dans lesquels la démonstration générale n'est pas valide, ou alors de séparer l'ensemble des possibilités en plusieurs classes sur lesquels la démonstration ne s'effectue pas tout à fait de la même façon.

Exemple 1.4.15

Montrer que pour tout $n \in \mathbb{N}$, $\frac{n(n+1)(2n+1)}{6}$ est entier.

IV.5 Analyse-Synthèse

Ce procédé de démonstration est surtout adapté pour les problèmes existentiels (montrer l'existence d'un objet vérifiant un certain nombre de propriétés). Le principe est le suivant :

Méthode 1.4.16 (Analyse-synthèse)

- Phase d'analyse : On suppose dans un premier temps l'existence d'un objet tel que souhaité, et à l'aide des propriétés qu'il est censé vérifier, on obtient autant d'informations que possible sur la façon de construire un tel objet.
- Phase de synthèse : lorsqu'on a suffisamment d'informations sur une façon de construire l'objet recherché, on construit un objet de la sorte, de façon explicite, et on vérifie qu'il répond au problème.
- Bonus : si la phase d'analyse fournit une expression explicite de l'objet recherché, ne laissant pas le choix pour cet objet, cela fournit même l'unicité.

Remarque 1.4.17

- La phase d'analyse est la recherche de conditions nécessaires.
- La phase de synthèse est la donnée de conditions suffisantes.

Exemple 1.4.18

Soit a un réel et $I = [-a, a]$. Montrer que toute fonction $f : I \longrightarrow \mathbb{R}$ s'écrit comme somme d'une fonction paire et d'une fonction impaire.

Remarque 1.4.19

Cet exemple est un cas particulier d'un exemple générique consistant à prouver qu'un espace vectoriel se décompose en somme (ici somme directe) de deux sous-espaces vectoriels. Se reporter au chapitre idoine pour ces notions.

Remarque 1.4.20

Dans le cadre d'un problème existentiel sans contrainte d'unicité, la phase d'analyse ne sert qu'à deviner une expression répondant au problème. D'un point de vue de la rigueur de rédaction, cette phase n'est pas indispensable, la phase de synthèse est suffisante pour répondre au problème existentiel. Cependant, elle permet au lecteur de mieux comprendre comment on est parvenu à l'expression voulue. Sans cette phase d'analyse, la réponse peut dans certaines situations paraître un peu parachutée.

Savoir si on rédige la phase d'analyse ou non dépend en fait de la complexité de la situation. Dans certaines situations assez simples, on comprend bien l'expression obtenue, on peut parfois même la deviner sans passer par une analyse. Dans ces cas, ne vous cassez pas la tête et faites directement la synthèse.

Avertissement 1.4.21

Soyez très précautionneux dans la rédaction d'une démonstration par analyse-synthèse. Dites bien de façon explicite qu'il s'agit d'un raisonnement de ce type. En effet, comme la phase d'analyse consiste en une recherche de conditions nécessaires, elle consiste souvent à supposer la conclusion vraie pour essayer d'obtenir le maximum d'informations sur l'expression recherchée. Un lecteur pressé (et les correcteurs au concours sont à classer dans cette catégorie) risque de prendre votre démonstration pour une pétition de principe (montrer un résultat en le supposant vrai au départ !)

IV.6 Raisonnement par récurrence

Le principe de récurrence est un axiome de la construction de $\mathbb{N}$. Il s'énonce ainsi :

$$[\mathcal{P}(0) \wedge (\forall n \in \mathbb{N},\ (\mathcal{P}(n) \Longrightarrow \mathcal{P}(n+1))] \Longrightarrow (\forall n \in \mathbb{N},\ \mathcal{P}(n))$$

« $\mathcal{P}(0)$ » est l'initialisation, « $\forall n \in \mathbb{N},\ (\mathcal{P}(n) \Longrightarrow \mathcal{P}(n+1))$ » est l'hérédité (ou le caractère héréditaire ou transmissible).

Méthode 1.4.22 (Démonstration par récurrence simple)

Pour montrer une propriété $\mathcal{P}(n)$ dépendant d'un entier $n \in \mathbb{N}$, on procède suivant le schéma suivant :

- Initialisation : montrer que $\mathcal{P}(0)$ est vraie.
- Hérédité : montrer que pour tout $n \in \mathbb{N}$, $\mathcal{P}(n) \Longrightarrow \mathcal{P}(n+1)$, ce qui se fait, d'après les principes développés précédemment en posant n quelonque (« Soit $n \in \mathbb{N}$ »), en supposant que pour ce n, $\mathcal{P}(n)$ est vrai, et en montrant qu'alors $\mathcal{P}(n+1)$ l'est aussi.
- Conclure, en faisant référence au principe de récurrence.

Ce principe peut s'adapter à des situations légèrement différentes :

- Le rang initial peut être un autre entier (éventuellement négatif). Cela modifie aussi alors le rang initial pour le caractère héréditaire.

- On peut faire des récurrences descendantes pour une propriété $\mathcal{P}(n)$, à démontrer sur un intervalle du type $]\!]-\infty, n_0]\!]$. On initialise alors avec $\mathcal{P}(n_0)$ et on montre que pour tout $n \leqslant n_0$, $\mathcal{P}(n) \Longrightarrow \mathcal{P}(n-1)$.
- On peut faire des récurrences bornées, pour montrer une propriété $\mathcal{P}(n)$ sur un intervalle borné, par exemple $[\![0, n_0]\!]$. On initialise alors avec $\mathcal{P}(0)$ et on montre que $\mathcal{P}(n)$ implique $\mathcal{P}(n+1)$ pour tout $n \in [\![0, n_0 - 1]\!]$. D'un point de vue purement logique, il ne s'agit pas de l'utilisation du principe de récurrence, mais d'une itération (utilisation répétée, en nombre fini, du modus ponens, par transitivité de l'implication).
- Ces récurrences bornées s'adaptent aussi au cas de récurrences descendantes.
- Nous verrons un peu plus loin deux variantes du principe de récurrence : la récurrence d'ordre k, et la récurrence forte.

Exemples 1.4.23

1. Montrer (par récurrence) que pour tout $n \in \mathbb{N}^*$, $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.
2. Formule du binôme de Newton : pour tout $a, b \in \mathbb{C}^2$ et tout $n \in \mathbb{N}$:

$$(a+b)^n = \sum_{k=0}^{n} \binom{a}{k} a^k b^{n-k} = \binom{n}{0} a^0 b^{n-0} + \binom{n}{1} a^1 b^{n-1} + \cdots + \binom{n}{n} a^{n-0} b^0$$

(voir le chapitre sur les sommes pour la définition des coefficients binomiaux).

Avertissement 1.4.24

N'oubliez pas l'initialisation ! Prouver l'hérédité à tout rang ne suffit pas !

Exemple 1.4.25

$10^n + (-1)^n$ est-il divisible par 11 pour tout $n \in \mathbb{N}$?

Voici enfin un dernier exemple développé :

Exemple 1.4.26 (Le problème des crayons de couleur)

Nous montrons dans cet exemple que tout ensemble de crayons de couleur est monochrome. Nous notons pour tout $n \in \mathbb{N}^*$, $\mathcal{P}(n)$ la propriété affirmant que tout ensemble de n crayons de couleurs est constitué de crayons ayant tous la même couleur.

- La propriété $\mathcal{P}(1)$ est trivialement vraie, ce qui initialise la récurrence
- Soit $n \in \mathbb{N}^*$. Supposons que $\mathcal{P}(n)$ est vrai. Soit alors un ensemble de $n+1$ crayons de couleur, qu'on peut supposer numérotés de 1 à $n+1$. En appliquant l'hypothèse de récurrence aux n premiers crayons et aux n derniers crayons, le crayon 1 a la même couleur que les crayons 2 à n qui on ont aussi même couleur que le crayons $n+1$, ce qui prouve $\mathcal{P}(n+1)$ (figure 1.1)
- D'après le principe de récurrence, on peut donc conclure qu'il n'existe au monde que des crayons d'une même couleur.

Où est l'erreur ?

Méthode 1.4.27 (Récurrence d'ordre k)

Il s'agit d'une variante du principe de récurrence, s'exprimant ainsi :

$$((\mathcal{P}(0) \wedge \cdots \wedge \mathcal{P}(k-1)) \wedge (\forall n \in \mathbb{N},\ \mathcal{P}(n) \wedge \cdots \wedge \mathcal{P}(n+k-1) \Longrightarrow \mathcal{P}(n+k))) \Longrightarrow \forall n \in \mathbb{N},\ \mathcal{P}(n).$$

- Principe : on utilise la propriété aux k rangs précédents pour montrer l'hérédité.

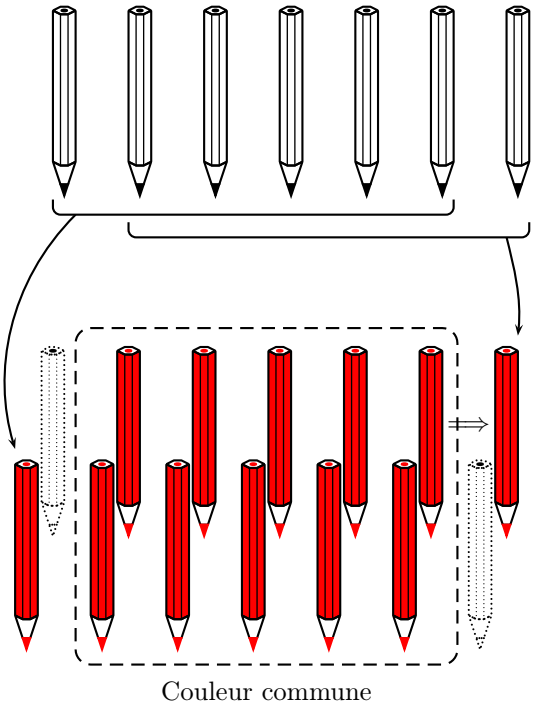


FIGURE 1.1 – Caractère héréditaire pour le problème des crayons de couleur

- Schéma de rédaction :
  - Initialisation : montrer $\mathcal{P}(0), \dots, \mathcal{P}(k-1)$.
  - Hérédité : poser $n \geqslant 0$, supposer $\mathcal{P}(n), \dots, \mathcal{P}(n+k-1)$, en déduire $\mathcal{P}(n+k)$.
  - Conclure en faisant appel au principe de récurrence.

Avertissement 1.4.28

Ne pas oublier d'initialiser pour les k premières valeurs ! (sinon la première implication de l'hérédité n'est pas valable)

On peut bien sûr adapter le principe dans le cas où le rang initial n'est pas 0.

Exemples 1.4.29

1. Soit $(F_n)_{n\in\mathbb{N}}$ définie par $F_0 = 0$, $F_1 = 1$ et pour tout $n \geqslant 0$, $F_{n+2} = F_{n+1} + F_n$ (suite de Fibonacci).
   Avec une mauvaise initialisation on peut « montrer » que F_n est divisible par 3, ce qui est évidemment faux !
2. Soit $n \in \mathbb{N}$. Montrer que F_n est paire si et seulement si n est multiple de 3.

Pour votre culture, ce dernier exemple est une situation particulière du résultat plus général suivant :

$$\forall (m,n) \in (\mathbb{N}^*)^2,\ F_{m\wedge n} = F_m \wedge F_n,$$

avec $m = 3$.
Voici une dernière variante du principe de récurrence :

Méthode 1.4.30 (Récurrence forte)

La récurrence forte est basée sur la propriété formelle suivante :

$$(\mathcal{P}(0) \wedge (\forall n \geqslant 1,\ \mathcal{P}(0) \wedge \cdots \wedge \mathcal{P}(n-1) \Longrightarrow \mathcal{P}(n))) \Longrightarrow \forall n \in \mathbb{N},\ \mathcal{P}(n).$$

- Principe : on suppose la propriété vraie à tous les rangs précédents pour la montrer à un rang donné.
- Schéma de rédaction :
  - Initialisation pour $\mathcal{P}(0)$ (une seule valeur suffit ici)
  - Poser $n > 0$, supposer $\mathcal{P}(k)$ vrai pour tout $k < n$, et montrer qu'alors $\mathcal{P}(n)$ est vrai.
  - Conclure en faisant référence au principe de récurrence.

Exemple 1.4.31

1. Tout nombre entier $n \geqslant 0$ admet une décomposition en nombres de Fibonacci distincts non consécutifs (théorème de Zeckendorf)
2. Tout nombre entier $n \geqslant 1$ admet une décomposition en produit de nombres premiers.

Remarque 1.4.32

On retiendra du dernier exemple que le principe de récurrence forte est en particulier très utile dans de nombreuses questions liées à des propriétés de divisibilité.

Enfin, on peut faire des récurrences simultanément sur plusieurs variables, ce qui revient la plupart du temps à imbriquer les récurrences les unes dans les autres. Attention à bien initialiser (à tous les « bords » du domaine, en général).

IV.7 Principe de la descente infinie

Nous terminons sur une dernière méthode classique, plus anecdotique pour une grande part des mathématiques, mais d'une telle efficacité pour certains problèmes d'arithmétique qu'on ne peut pas ne pas la mentionner.

Méthode 1.4.33 (Descente infinie)

Le principe de la descente infinie est un mélange de démonstration par l'absurde et de démonstration par récurrence. Soit $(\mathcal{P}(n))_{n\in\mathbb{N}}$ une propriété dont on veut démontrer qu'elle est fausse pour tout $n \in \mathbb{N}$: il suffit de montrer que si elle est supposée vraie à un certain rang n, il existe alors un rang $m < n$ tel qu'elle soit encore vraie.

En effet en itérant alors ce procédé, on pourrait construire une chaîne infinie d'entiers strictement décroissants telle que $\mathcal{P}(n)$ soit vraie, ce qui est impossible d'après la propriété fondamentale de $\mathbb{N}$, ce qui amène la contradiction recherchée.

Exemple 1.4.34

- Variante de la démonstration de l'irrationnalité de $\sqrt{2}$
- Démonstration du théorème de Fermat dans le cas où $n = 4$: il n'existe pas d'entiers non nuls x, y et z tels que $x^4 + y^4 = z^4$ (exemple non développé)

Note Historique 1.4.35

- La démonstration par l'absurde est déjà connue du temps de Pythagore (preuve de l'irrationnalité de $\sqrt{2}$)

- On trouve des prémices du raisonnement par récurrence dans les *Éléments* d'Euclide, mais cela reste très vague. La vraie naissance du raisonnement par récurrence date de 1654, lorsque Blaise Pascal écrit son *Traité du triangle arithmétique*.
- Pierre de Fermat met en place, à peu près à la même époque, le principe de la descente infinie, mélange entre le principe de récurrence et la démonstration par l'absurde. Ce type de raisonnement aussi apparaît déjà plus ou moins dans les *Éléments* d'Euclide, mais gagne vraiment sa notoriété grâce à Fermat. Il est par exemple utilisé pour montrer le grand théorème de Fermat pour l'exposant 4.

2 Ensembles

« Nul n'a le droit de nous exclure du Paradis que Cantor a créé pour nous »

(David Hilbert)

La notion d'ensemble semble à première vue une notion intuitive évidente, ne nécessitant pas de précautions particulières. Cette notion intuitive est à la base de toutes les mathématiques, depuis leur origine, que ce soit l'arithmétique élémentaire (ensemble d'entiers, puis de divers autres types de nombres, utilisés depuis qu'on sait compter), la géométrie d'Euclide à nos jours (une figure est un sous-ensemble du plan), l'analyse (on étudie des fonctions définies sur des ensembles), ou l'algèbre moderne (étude des structures algébriques, définies comme des ensembles munis d'un certain nombre de lois supplémentaires).

Longtemps, les mathématiciens se sont contentés de ce point de vue intuitif, sans chercher à formaliser cette notion. Ce n'est qu'à l'aube du XX^{e} siècle qu'on s'est penché sur cette formalisation, qui a bien failli faire vasciller l'édifice mathématique sur ses fondations. En effet, Cantor, puis Russell au travers de son célèbre paradoxe, ont montré qu'on ne pouvait pas se contenter de cette approche intuitive, et que celle-ci amenait même des contradictions si on admettait que toute collection pouvait être une ensemble : ainsi, le paradoxe de Russell montre qu'il ne peut pas exister d'ensemble des ensembles. Les mathématiciens pensèrent même un moment qu'il n'était pas possible de donner une formalisation correcte de la notion d'ensemble ; cela aurait signifié ni plus ni moins que la faillite des mathématiques. Heureusement, au prix d'une axiomatique assez lourde, les mathématiciens logiciens de l'époque ont réussi à mettre en place cette formalisation. On peut dire que cette « crise des fondements » a marqué la naissance des mathématiques et de la logique moderne, par une formalisation systématique de toutes les notions utilisées. Depuis, l'édifice mathématique a des fondements solides et ne s'assoit plus sur des sables mouvants. Même la notion d'indécidabilité, dans un premier temps assez choquante, a fini par trouver sa place dans cet édifice solide, par une latitude qu'autorisent ces résultats indécidables dans le choix de l'axiomatique initiale. Ainsi, par exemple, l'axiome du choix dont on parlera dans la suite de ce chapitre étant indécidable (pour l'axiomatique de Zermelo-Frankel), on pourra construire deux théories mathématiques, l'une incluant l'axiome du choix, l'autre, beaucoup plus pauvre, ne l'incluant pas. Ainsi, dans certaines théories, l'axiome du choix permet d'aller un peu, ou beaucoup plus loin, en permettant notamment de construire certains objets infinis.

En ce qui nous concerne, nous nous contenterons du point de vue intuitif. Nous souleverons tout de même les problèmes que peut engendrer ce point de vue, et nous évoquerons de façon très superficielle le problème de l'axiomatisation de la théorie des ensembles.

I Théorie intuitive des ensembles

I.1 Définition intuitive

Pour définir rigoureusement la notion d'*ensemble*, il faut une axiomatique très complexe, c'est pourquoi nous admettons cette notion. Nous nous contentons de :

Définition 2.1.1 (Ensemble, point de vue intuitif)

- Un *ensemble* E est une collection d'objets.
- Les objets dont est constituée la collection définissant E sont appelés *éléments de* E.
- On dit que x *appartient à* E si x est élément de E, et on note $x \in E$.

Remarque 2.1.2

La définition donnée est insuffisante : on ne peut pas prendre pour E n'importe quelle collection d'objets, sinon la théorie devient contradictoire (paradoxe de Russell). Pour éviter cela, on peut imposer que E ne se contienne pas lui-même.

Note Historique 2.1.3

La notation $\in$ est introduite par l'italien Peano en 1890. Il s'agit d'un epsilon, pour désigner la lettre E de « esti » (« il est » en italien)

Il existe plusieurs façons de décrire un ensemble

Définition 2.1.4 (Définitions d'ensembles)

- Une définition *par énumération* d'un ensemble E est la donnée explicite de tous les éléments de l'ensemble.
- Une définition *par compréhension* d'un ensemble E est la donnée d'une propriété P caractérisant les éléments de E (parmi les éléments d'un ensemble plus gros F)
- Une définition *par induction structurelle* de E est la donnée d'un certain nombre d'éléments de E, et d'une façon de construire, étape par étape les autres éléments de E à partir de ceux donnés.
- Une définition *par constructions* (unions, intersections) est une façon de construire un ensemble à partir d'autres ensembles (ce sera étudié dans le paragraphe suivant)

Notation 2.1.5

- L'ensemble E défini par énumération est noté en mettant entre des accolades { et } la liste complète des éléments de E.
- L'ensemble E défini par compréhension est noté en mettant entre accolades l'appartenance de l'élément générique x au sur-ensemble F suivi de la propriété P caractérisant les éléments de E.

Remarques 2.1.6

1. Il n'y a pas de notion d'ordre des éléments d'un ensemble E : on peut énumérer les éléments de E dans l'ordre qu'on veut.
2. Il n'y a pas de notion de multiplicité d'un élément : un élément appartient ou n'appartient pas à un ensemble, mais il ne peut pas « appartenir plusieurs fois ». S'il apparaît plusieurs fois dans une énumération des éléments de E, attention au fait qu'il s'agit bien du même élément !
3. L'énumération des éléments d'un ensemble est généralement donnée entre accolades {...} pour désigner l'ensemble.

Exemples 2.1.7

1. Énumération : $\{1,3,7,9\} = \{3,9,7,1\} = \{1,1,3,3,3,7,9,9\}$.
2. Compréhension : $\{x \in \mathbb{R} \mid \exists y \in \mathbb{N},\ x^2 = y.\}$, ou $\{x \in \mathbb{R} \mid x^2 - 4x + 1 \geqslant 0\}$
3. Induction structurelle :
   (i) L'ensemble E tel que $2, 3 \in E$ et si p et q sont dans E, pq est dans E.
   (ii) L'ensemble $\mathcal{A}$ des arbres binaires, contenant l'arbre vide $\varnothing$, et, étant donnés deux arbres A_1, A_2 de $\mathcal{A}$, l'arbre $A = (A_1, A_2)$, constitué d'une racine à laquelle sont attachés (par leur racine) le fils gauche A_1 et le fils droit A_2 (figure 2.1)
   (iii) L'ensemble des formules propositionnelles, défini comme sous-ensemble de toutes les chaînes de caractère, qui contient les variables propositionnelles, et stable par certaines contructions du type $A \vee B$...

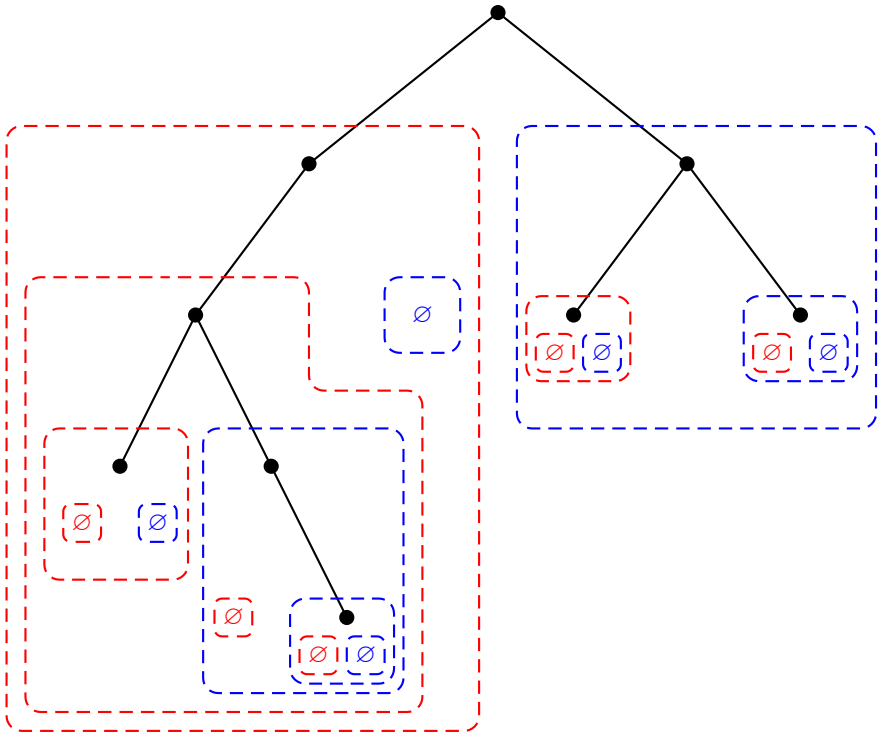


Figure 2.1 – Un arbre binaire A et sa décomposition récursive

Remarque 2.1.8

Une définition de E par induction structurelle est la donnée de certains éléments $A_1, \ldots, A_n$ de E et de certaines propriétés de stabilité $P_1, \ldots, P_k$, dépendant respectivement de $n_1, \ldots, n_k$ variables, s'exprimant de la manière suivante :

$$\forall j \in [\![1,k]\!], \forall (B_1, \ldots, B_{n_j}) \in E^{n_j},\quad P_j(B_1, \ldots, B_{n_j}) \in E.$$

Ainsi, un ensemble E défini par induction structurelle peut être appréhendé de deux façons :

- par le bas :
  On part des éléments initiaux, et on construit étape par étape des nouveaux éléments en appliquant, à chaque étape, les règles de construction aux éléments déjà obtenus.

- par le haut (possible si on connaît un ensemble F contenant E, c'est le cas du premier et du dernier exemple) :
  E est « le plus petit ensemble » contenant $A_1, \cdots, A_n$, et stable par les constuctions $P_1, \ldots, P_k$. Cela se traduit souvent par une intersection de tous les ensembles possédant cette propriété de stabilité.

Quelques définitions supplémentaires :

Définition 2.1.9 (Sous-ensemble)
Soit E un ensemble. Un sous-ensemble de E est un ensemble F tel que tout élément de F est aussi élément de E. On note $F \subset E$.

Ainsi, E est un sous-ensemble de F si et seulement si : $\forall x, \quad x \in E \Longrightarrow x \in F$.
On a clairement :

Proposition 2.1.10 (Principe de double-inclusion)
$E = F$ si et seulement si $E \subset F$ et $F \subset E$

Notation 2.1.11 (Ensemble vide)
L'ensemble vide est l'unique ensemble ne contenant aucun élément. Il est noté $\varnothing$.

Proposition 2.1.12
L'ensemble vide est sous-ensemble de tout ensemble E.

En effet :

$$\forall x, \quad x \in \varnothing \Longrightarrow x \in E$$

(la source de l'implication étant toujours fausse, l'implication est vraie)
Le seul sous-ensemble de $\varnothing$ est $\varnothing$ lui même.

Terminologie 2.1.13 (singleton)
On appelle *singleton* un ensemble constitué d'un unique élément, donc de la forme $\{a\}$.

La notion de singleton nous donne un lien entre appartenance et inclusion :

Proposition 2.1.14 (Appartenance et inclusion)
Soit E un ensemble et a un objet. Alors : $a \in E \Longleftrightarrow \{a\} \subset E$

Définition 2.1.15 (Cardinal, notion intuitive)
Intuitivement, le cardinal d'un ensemble correspond à sa taille. Pour un ensemble fini, il s'agit du nombre de ses éléments. On note dans ce cas $\mathrm{Card}(E)$ ou $|E|$ le cardinal de E.

Exemple 2.1.16
- $\mathrm{Card}(\varnothing) = 0$.
- $\mathrm{Card}(\{\varnothing\}) = 1$.

On peut définir, comme on le verra plus tard, une notion de cardinal pour des ensembles infinis, mais l'intuition en est moins évidente. Par exemple, $\mathbb{N}$ et $\mathbb{Q}$ ont même cardinal !

I.2 Opérations sur les ensembles

Nous étudions dans ce paragraphe les constructions classiques permettant de définir des ensembles à partir d'autres.

Définition 2.1.17 (Intersection, figure 2.4)

Soit E et F deux ensembles. L'intersection de E et F, notée $E \cap F$, est l'ensemble des éléments contenus à la fois dans E et dans F :

$$x \in E \cap F \iff (x \in E) \wedge (x \in F).$$

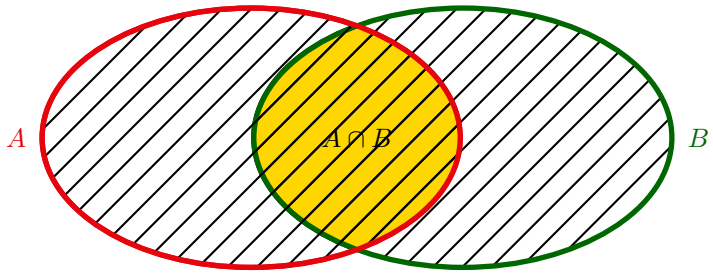


Figure 2.2 – Intersection de deux ensembles

Proposition 2.1.18 (Propriétés de l'intersection)

Soit E, F, G des ensembles. Alors :

1. $E \cap F = F \cap E$ *(commutativité)*
2. $(E \cap F) \cap G = E \cap (F \cap G)$ *(associativité, figure 2.3)*
3. $E \cap F \subset E$ *et* $E \cap F \subset F$ *et* $E \cap F$ *est maximal pour cette propriété ;*
4. $E \cap \varnothing = \varnothing$
5. *Si* $E \subset F$, *alors* $E \cap F = E$.

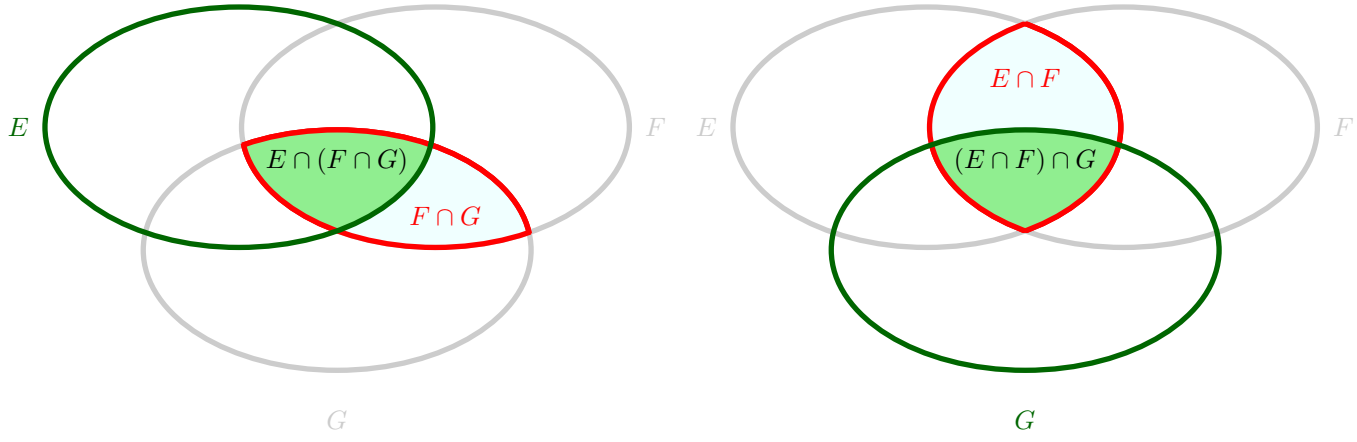


Figure 2.3 – Associativité de l'intersection

Définition 2.1.19 (Union)

Soit E et F deux ensembles. L'union de E et F, notée $E \cup F$, est l'ensemble des éléments contenus soit dans E soit dans F :

$$x \in E \cup F \iff (x \in E) \vee (x \in F).$$

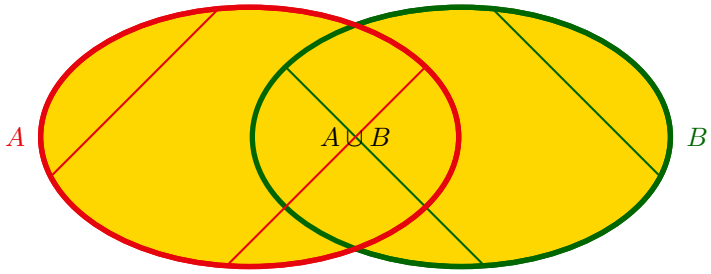


FIGURE 2.4 – Union de deux ensembles

Proposition 2.1.20 (propriétés de l'union)

Soit E, F, G des ensembles. Alors :

1. $E \cup F = F \cup E$ *(commutativité)*
2. $(E \cup F) \cup G = E \cup (F \cup G)$ *(associativité)*
3. $E \subset E \cup F$ *et* $F \subset E \cup F$ *et* $E \cup F$ *est minimal pour cette propriété ;*
4. $E \cup \varnothing = E$
5. *Si* $E \subset F$*, alors* $E \cup F = F$*.*
6. $(E \cup F) \cap G = (E \cap G) \cup (F \cap G)$ *(distributivité de* $\cap$ *sur* $\cup$*, figure 2.5)*
7. $(E \cap F) \cup G = (E \cup G) \cap (F \cup G)$ *(distributivité de* $\cup$ *sur* $\cap$*, figure 2.6)*

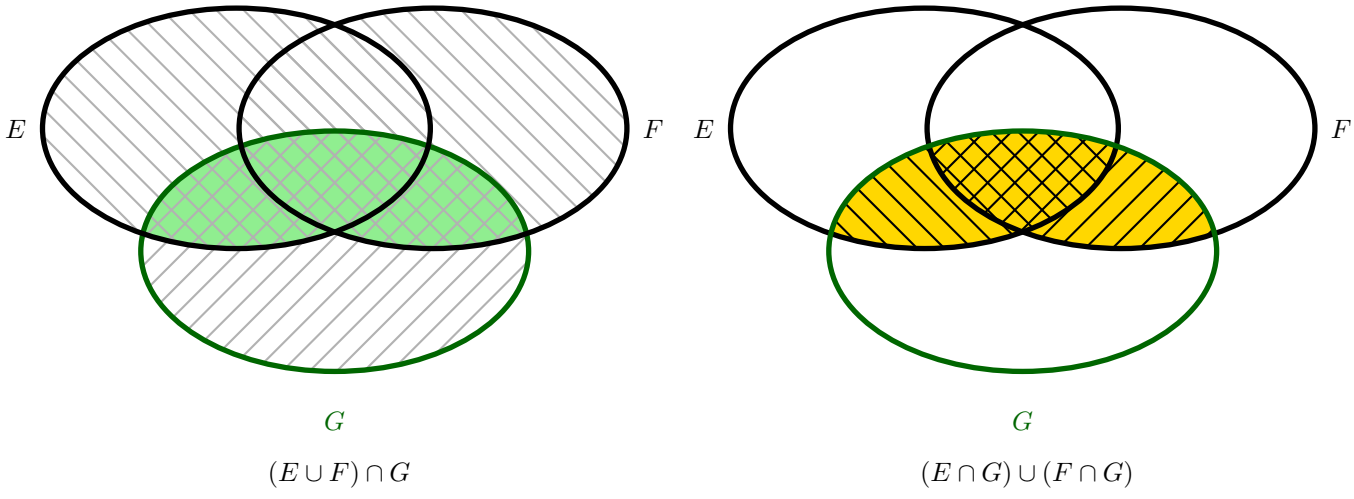


FIGURE 2.5 – Distributivité de l'intersection sur l'union

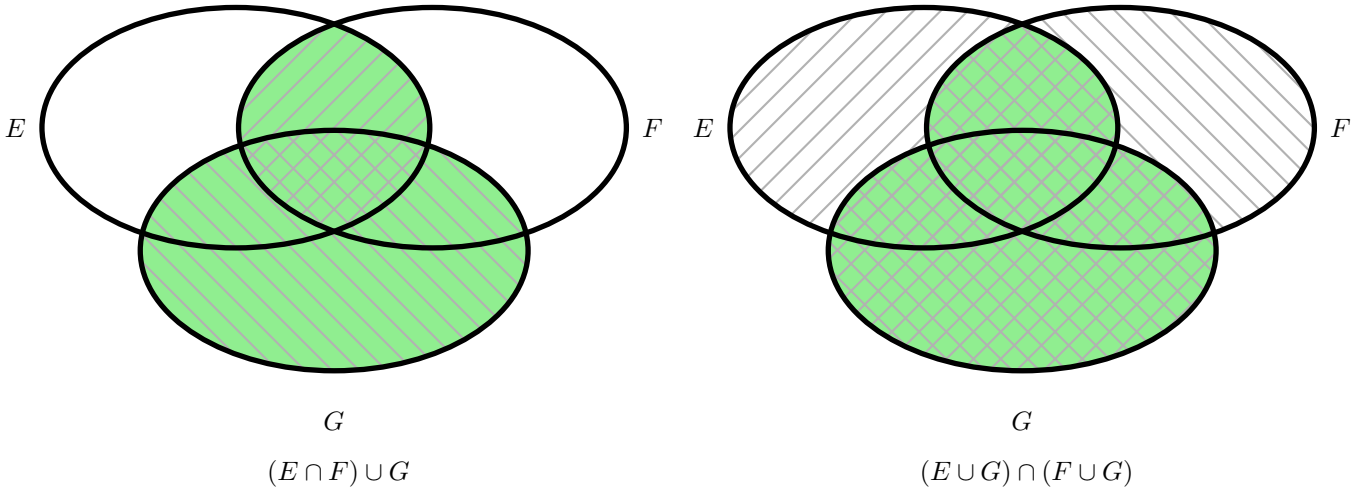


Figure 2.6 – Distributivité de l'union sur l'intersection

Définition 2.1.21 (Ensembles disjoints)
Deux ensembles E et F sont disjoints si $E \cap F = \varnothing$.

Avertissement 2.1.22
Attention à ne pas confondre *disjoint* et *distinct* !

Notation 2.1.23 (union disjointe)
Si A et B sont disjoints, l'union $A \cup B$ peut être notée $A \sqcup B$. Cette notation *affirme* que A et B sont disjoints.

Définition 2.1.24 (Complémentation)
Soit $F \subset E$. Le *complémentaire* de F dans E, noté $\complement_E F$ ou $E \setminus F$, est l'ensemble des éléments de E qui ne sont pas dans F :

$$x \in \complement_E F \iff (x \in E) \wedge (x \notin F).$$

En particulier, $\complement_E F \cup F = E$ et $\complement_E F \cap F = \varnothing$

Proposition 2.1.25 (Lois de De Morgan, figure 2.7)
Soit E un ensemble et F et G deux sous-ensembles de E. On a :

1. $\complement_E(F \cup G) = \complement_E F \cap \complement_E G$
2. $\complement_E(F \cap G) = \complement_E F \cup \complement_E G$

Il s'agit bien entendu de la version ensembliste des lois de De Morgan données pour la logique.
Une autre construction importante est la différence symétrique :

Définition 2.1.26 (Différence symétrique, figure 2.8)
Soit E et F deux ensembles. La différence symétrique $E \triangle F$ est l'ensemble des éléments x appartenant

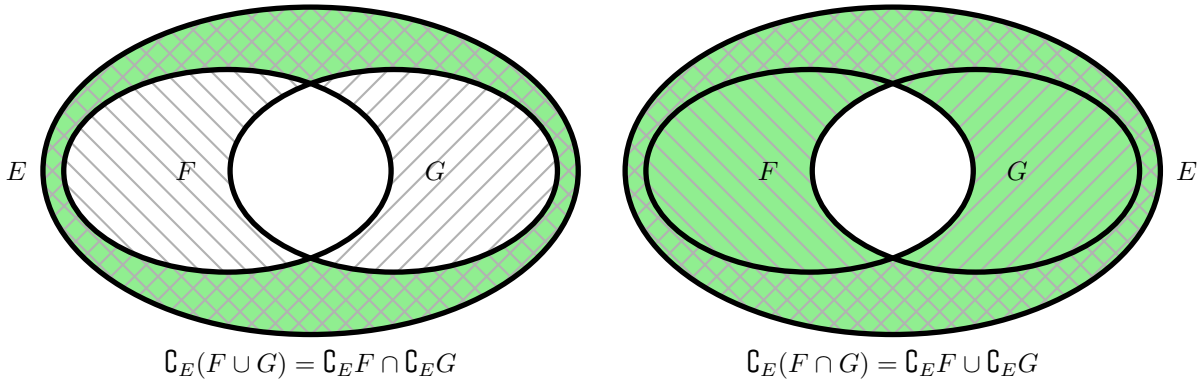


FIGURE 2.7 – Lois de De Morgan

à l'un des deux ensembles E ou F, mais pas à l'autre :

$$E \triangle F = \{x \mid x \in E \setminus F \text{ ou } x \in F \setminus E\}.$$

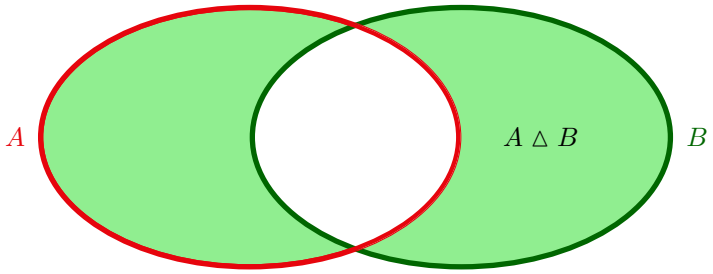


FIGURE 2.8 – Différence symétrique

Il faut bien garder en tête la correspondance entre opérations ensemblistes et connecteurs logiques :

$\cup \equiv \vee$	$x \in A \cup B \iff (x \in A) \vee (x \in B)$
$\cap \equiv \wedge$	$x \in A \cap B \iff (x \in A) \wedge (x \in B)$
$\complement \equiv \neg$	si $x \in A$, $\big(x \in \complement_A B \iff \neg(x \in B)\big)$
$\subset \equiv \implies$	$A \subset B \iff (\forall x,\ x \in A \implies x \in B)$,
$\triangle \equiv$ ou exclusif	$x \in A \triangle B \iff x \in A$ ou (exclusif) $x \in B$
$= \equiv \iff$	$A = B \iff (\forall x,\ x \in A \iff x \in B)$.

Définition 2.1.27 (Produit cartésien, figure 2.9)
Soit E et F deux ensembles. Le produit cartésien de E et F, noté $E \times F$, est l'ensemble des couples (a, b), tels que $a \in E$ et $b \in F$.

Ainsi, pour chaque élément a de E, on dispose d'une copie complète de B, identifiée au produit $\{a\} \times B$, c'est-à-dire à l'ensemble des couples (a, b), pour b parcourant B. On peut bien entendu aussi le voir en inversant le rôle de A et B. Il faut relier cette notion à celle de **rectangle plein**, qui n'est autre que le produit cartésien de deux intervalles de $\mathbb{R}$

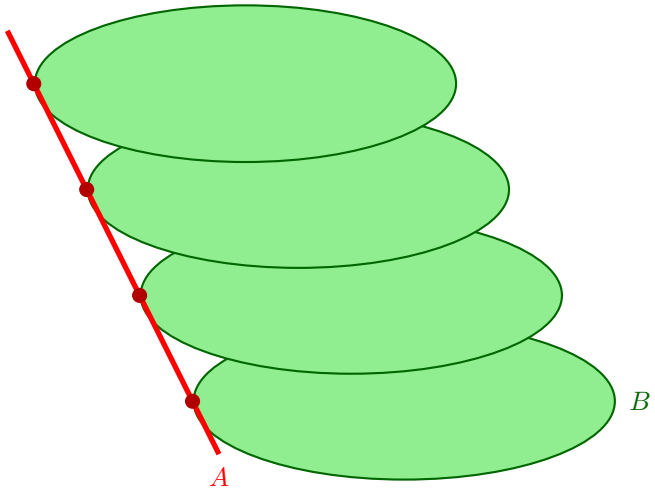


Figure 2.9 – Produit cartésien de deux ensembles

Notation 2.1.28

On note $E^2 = E \times E$, et plus généralement E^n pour un produit catésien à n termes.

Proposition 2.1.29 (propriétés du produit cartésien)

Soit E, E' et F des ensembles. Alors :

1. $E \times F = \varnothing \iff (E = \varnothing) \vee (F = \varnothing)$;
2. $(E \cup E') \times F = (E \times F) \cup (E' \times F)$;
3. $(E \cap E') \times F = (E \times F) \cap (E' \times F)$;

Une partie d'un ensemble est un autre nom donné à un sous-ensemble.

Notation 2.1.30 (Ensemble des parties d'un ensemble)

On note $\mathcal{P}(E)$ l'ensemble des parties de E, c'est-à-dire l'ensemble dont les éléments sont les sous-ensembles de E : $F \in \mathcal{P}(E) \iff F \subset E$.

Remarque 2.1.31

Ainsi que nous l'avons évoqué en début de section, toute collection d'éléments ne peut pas nécessairement être considérée comme un ensemble. Par exemple, on ne peut pas parler de l'ensemble des ensembles. Il n'est donc *a priori* pas évident que $\mathcal{P}(E)$ soit toujours un ensemble. En fait, cela fait partie des axiomes que l'on pose pour définir la théorie des ensembles.

Proposition 2.1.32

Pour tout ensemble E, $\varnothing \in \mathcal{P}(E)$ et $E \in \mathcal{P}(E)$. Ainsi, $\mathcal{P}(E)$ n'est jamais vide. Il contient toujours $\varnothing$ et E.

Exemples 2.1.33

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

1. $E = \varnothing$
2. $E = \{1\}$
3. $E = \{1, 2, 3\}$
4. $E = \{\varnothing, \{\varnothing\}\}$

Définition 2.1.34 (partition d'un ensemble)

Une partition de E est un sous-ensemble de $\mathcal{P}(E)$ dont les éléments sont des sous-ensembles non vides de E, deux à deux disjoints et d'union égale à E.
Par exemple, une partition finie, est un ensemble $\{A_1, \dots, A_n\}$ de sous-ensembles de E tels que :

1. $\forall i \in [\![1, n]\!],\ E_i \neq \varnothing$,
2. $\forall (i, j) \in [\![1, n]\!]^2,\ i \neq j \implies E_i \cap E_j = \varnothing$,
3. $E_1 \cup \cdots \cup E_n = E$.

Les sous-ensembles A_i sont appelés *parts* de la partition, et n est appelé *longueur* de la partition.

Puisque les parts d'une partition ne peuvent pas être vides, il n'existe qu'un nombre fini de partitions d'un ensemble donné. Ce nombre est égal, par définition, au nombre de Bell B_n.

I.3 Unions et intersections sur une famille

Définition 2.1.35 (unions et intersections sur une famille)

Soit $(A_i)_{i \in I}$ une famille (finie ou infinie) d'ensembles. On définit alors l'union et l'intersection de cette famille par :

- $\bigcup_{i \in I} A_i = \{x \mid \exists i \in I,\ x \in A_i\}$
- $\bigcap_{i \in I} A_i = \{x \mid \forall i \in I,\ x \in A_i\}$

On pourrait également définir des produits cartésiens infinis, mais cela nécessite un peu plus de technique, et c'est hors-programme.

Notation 2.1.36 (Union disjointe)

Si les A_i sont deux à deux disjoints, on peut noter l'union $\bigsqcup_{i \in I} A_i$.

Proposition 2.1.37 (propriétés liées aux unions et intersections infinies)

Un certain nombre de propriétés vues dans le paragraphe précédent se généralisent aux unions et intersections infinies. Étant donné $(A_i)_{i \in I}$ une famille d'ensembles, et B un ensemble, tous inclus dans un ensemble E :

1. $B \cap \left(\bigcup_{i \in I} A_i \right) = \bigcup_{i \in I} (B \cap A_i)$ *(distributivité)*
2. $B \cup \left(\bigcap_{i \in I} A_i \right) = \bigcap_{i \in I} (B \cup A_i)$ *(l'autre distributivité)*
3. $\complement_E \left(\bigcup_{i \in I} A_i \right) = \bigcap_{i \in I} \left(\complement_E A_i \right)$ *(loi de De Morgan)*

4. $\complement_E\left(\bigcap_{i\in I} A_i\right) = \bigcup_{i\in I}(\complement_E A_i)$ *(loi de De Morgan)*

I.4 Fonction caractéristique

En admettant momentanément la notion intuitive de fonction, on peut associer, à tout sous-ensemble de E, une fonction de E dans $\{0,1\}$.

Définition 2.1.38 (Fonction caractéristique d'un ensemble)

Soit E un ensemble et A un sous-ensemble de E. La fonction caractéristique de A, notée $\mathbb{1}_A$, est la fonction de E dans $\{0,1\}$ définie par :

$$\begin{array}{rccl} \mathbb{1}_A : & E & \longrightarrow & \{0,1\} \\ & x & \mapsto & \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A. \end{cases} \end{array}$$

On trouve parfois la notation χ_A au lieu de $\mathbb{1}_A$.
Un certain nombre de propriétés élémentaires se traduisent sur les fonctions caractéristiques. Les constructions élémentaires se transcrivent également très bien au niveau des fonctions caractéristiques.

Proposition 2.1.39 (propriétés des fonctions caractéristiques)

Soit E un ensemble, et A, B des sous-ensembles de E. On a alors :

1. $A = \{x \in E \mid \mathbb{1}_A(x) = 1\}$.
2. $\mathbb{1}_{A\cap B} = \mathbb{1}_A\mathbb{1}_B$
3. $\mathbb{1}_{\complement_E A} = 1 - \mathbb{1}_A$
4. *Si A et B sont disjoints,* $\mathbb{1}_{A\sqcup B} = \mathbb{1}_A + \mathbb{1}_B$
5. *Dans le cas général,* $\mathbb{1}_{A\cup B} = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_{A\cap B} = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_A\mathbb{1}_B$

Certaines propriétés se traduisent sur les fonctions caractéristiques. Par exemple, A et B sont disjoints si et seulement si $\mathbb{1}_A\mathbb{1}_B = 0$, ou bien $\{A_1, \ldots, A_n\}$ est une partition de E si et seulement si les A_i sont non vides et $\mathbb{1}_{A_1} + \cdots + \mathbb{1}_{A_n} = 1$.

II Axiomatisation de la théorie des ensembles

II.1 La crise des fondements

Note Historique 2.2.1

- En 1896, alors qu'il essaye de donner une construction de $\mathbb{N}$ et des ordinaux plus généraux (nombres transfinis), Georg Cantor se rend compte d'une contradiction dans sa théorie des ensembles (il définit un ensemble comme une collection quelconque d'objets). En effet, il prouve que pour tout ensemble E, $\mathrm{Card}(\mathcal{P}(E)) > \mathrm{Card}(E)$ (dans le sens qu'il donne à la notion de cardinal, défini à l'aide des ordinaux). Cette contradiction empêche de parler de l'ensemble des ensembles, ou encore, dans le contexte qui l'intéresse, de l'ensemble des ordinaux. Ainsi, on ne peut pas définir un ensemble comme n'importe quelle collection d'objets !
  Il n'en parle à personne car sa théorie est menacée, à part à David Hilbert, qui fait autorité à l'époque, et à qui il envoie une lettre.
- En 1897, Cesare Burali-Forti parvient à la même conclusion et publie son résultat, sans vraiment être persuadé que cela remet tout en cause.

- En 1901, le logicien et philosophe anglais Bertrand Russell exprime le premier paradoxe simple prouvant que toute collection ne peut pas être un ensemble. En effet, en définissant

$$E = \{\text{ensembles F qui ne se contiennent pas eux-mêmes}\},$$

si E était un ensemble :
∗ si $E \notin E$, alors par définition de E, E est élément de E, d'où une contradiction ;
∗ si $E \in E$, alors, par définition de E, E n'est pas élément de E, d'où une contradiction.
Cet argument très simple montre que E ne peut pas être un ensemble.
Ce paradoxe est connu sous le nom de « paradoxe de Russell » ou parfois « paradoxe du barbier ». En effet, la situation s'apparente à celle d'un barbier qui rase tout homme qui ne se rase pas lui-même. Ce barbier peut-il être un homme ?
- Ce paradoxe a en fait été envoyé par Russell au logicien et philosophe allemand Gottlob Frege, suite à la parution du premier volume de son ouvrage *Les fondements de l'arithmétique*, pour lui prouver que son ouvrage reposait sur une contradiction. Frege publie tout de même le second volume, en lui adjoignant un appendice dans lequel il fait l'aveu et le constat sans doute les plus désarmants de toute l'histoire des mathématiques :

> « Pour un écrivain scientifique, il est peu d'infortunes pires que de voir l'une des fondations de son travail s'effondrer alors que celui-ci s'achève. C'est dans cette situation inconfortable que m'a mis une lettre de M. Bertrand Russell, alors que le présent volume allait paraître »

Par la suite, Frege cessa presque entièrement ses travaux mathématiques.
- D'autres paradoxes, recherchant des formes amusantes, virent alors le jour, comme le paradoxe de Jules Richard (1905), dont un enoncé simplifié est le paradoxe de Berry (formulé par Russell en 1906, il l'attribue à un bibliothécaire londonien du nom de Berry) :
Soit E l'« ensemble » des entiers qui ne peuvent pas se définir en moins de 16 mots. Cet ensemble est non vide car son complémentaire est fini (car il y a un nombre fini de mots dans la langue française)
Par les propriétés des sous-ensembles de $\mathbb{N}$, cet « ensemble » admet un plus petit élément, qui peut être défini par : « le plus petit entier qui ne peut pas se définir en moins de seize mots », définition qui n'utilise que 15 mots !

II.2 Tentatives d'axiomatisation

Note Historique 2.2.2

- De nombreuses tentatives d'axiomatisation de la théorie des ensembles à la suite de cette crise des fondements, toutes n'ont pas été fructueuses
- Le choix qui s'est imposé est finalement l'axomatique de Zermelo-Fraenkel à laquelle on ajoute ou non l'axiome du choix.

La théorie des ensembles de Zermelo-Fraenkel définit les ensembles comme étant des objets satisfaisant à un certain nombre d'axiomes. Dans cette théorie, les éléments eux-même sont tous des ensembles. Les nombres (les entiers relatifs dans un premier temps) sont alors définis comme étant des ensembles en particulier, par exemple à la façon des ordinaux de Cantor.

Axiome 2.2.3 (les axiomes de la théorie de Zermelo-Fraenkel, HP)

Voici les noms des différents axiomes, et leur interprétation intuitive :

- *Axiome d'extentionnalité : c'est lui qui dit que deux ensembles sont égaux si et seulement si ils ont mêmes éléments. Cet axiome est notamment à la base du principe de double-inclusion.*
- *Axiome de la paire : il affirme l'existence des paires $\{a, b\}$, lorsque a et b sont deux ensembles. En particulier, l'axiome de la paire affirme aussi l'existence des singletons $\{a\}$, pour un ensemble a (prendre $a = b$!)*
- *Axiome de la réunion : il donne la possibilité de construire des unions des éléments d'un ensemble (ces éléments étant eux-même des ensembles)*
- *Axiome des parties : il affirme que si a est un ensemble, alors $\mathcal{P}(a)$ aussi.*

- *Schéma d'axiome (*i.e. *série d'axiomes) de compréhension : il permet en particulier de définir un ensemble par compréhension (comme sous-ensemble d'un ensemble donné, constitué des éléments vérifiant une certaine propriété)*
- *Axiome de l'infini : il donne l'existence de l'infini, et notamment des ensembles infinis.*
- *Axiome de fondation : il dit en particulier qu'un ensemble ne peut pas s'appartenir (on ne peut pas avoir $x \in x$).*

À ces différents axiomes, on ajoute ou non (suivant la théorie) l'axiome du choix. Cet axiome du choix est indécidable à partir des axiomes de Zermelo-Fraenkel, et il est actuellement couramment admis qu'il doit être considéré comme vrai.

Axiome 2.2.4 (Axiome du choix, HP)
Soit I un ensemble, et pour tout $i \in I$, E_i un ensemble. Alors il existe une fonction $f : I \longrightarrow \bigcup_{i \in I} E_i$ telle que pour tout $i \in I$, $f(i) \in E_i$.

Autrement dit, étant donné une famille d'ensembles, on peut choisir un élément dans chaque ensemble, d'où le nom de cet axiome. Évidemment, si I est fini, ce n'est pas très étonnant, et cela résulte de l'axiome de récurrence (car par définition-même de l'interprétation du symbole $\exists$, on peut toujours choisir **un** élément d'un ensemble non vide). N'invoquez donc l'axiome du choix que pour un choix infini, c'est dans cette situation qu'il est pertinent.

Remarque 2.2.5

1. L'axiome de la paire, couplée à l'axiome de l'union, permet de considérer $A \cup B$ pour tous ensembles A et B
2. En itérant cet argument, on peut considérer l'union de n ensembles.
3. L'intersection d'une famille quelconque (non réduite à l'ensemble vide) d'ensembles s'obtient par compréhension (axiome de compréhension, en se plaçant globalement dans un des ensembles donnés)
4. l'union d'une famille quelconque pose davantaage de problème ; il faut déjà préciser ce qu'on entend par famille $(a_i)_{i \in I}$: il s'agit d'une application d'un *ensemble* I dans un autre *ensemble* E qui à $i \in I$ associe a_i. Ainsi, les a_i doivent eux-même être des éléments d'un ensemble. C'est le cas en particulier si les a_i sont tous des sous-ensembles d'un même ensemble B (dans ce cas, les a_i sont tous éléments de $\mathcal{P}(B)$, qui est un ensemble, d'après l'axiome des parties). Dans ce cas, l'image $\{a_i, i \in I\}$ de cette famille est un ensemble (on peut la définir par compréhension), donc on peut considérer l'union de ses éléments (axiome de l'union).
5. L'existence (et l'unicité) de l'ensemble vide provient de l'axiome de compréhension, à partir d'un ensemble A quelconque (on sait qu'il existe au moins un ensemble, d'après l'axiome de l'infini ; de toute façon, si ce n'était pas le cas, la théorie serait bien pauvre). L'ensemble vide peut alors se définir par compréhension de la façon suivante :
$$\varnothing = \{x \in A \mid x \neq x\}.$$
6. Le produit cartésien se définit à l'aide de couples, un couple (a, b) de $A \times B$ étant défini comme la paire $\{a, \{a, b\}\}$.

III L'ensemble $\mathbb{N}$ des entiers naturels

III.1 Axiomatique de $\mathbb{N}$ (hors-programme)

Nous avons vu les difficultés amenées par la conception de la notion d'ensemble. Définir les ensembles sans prendre de précaution peut amener à des théories contradictoires. La formalisation de la théorie des ensembles impose alors de devoir aussi redéfinir axiomatiquement les ensembles classiques, notamment les nombres entiers, et leurs propriétés arithmétiques (donc la définition de la somme et du produit).
L'ensemble $\mathbb{N}$ est alors défini comme un ensemble contenant un élément nul 0, et tel que tout élément n ait un successeur, noté $n+1$, et tout élément n, à l'exclusion de 0, ait un prédecesseur m (tel que $m+1=n$). À cela, on ajoute un certain nombre d'axiomes techniques (les axiomes de Peano) servant à définir rigoureusement les opérations dans $\mathbb{N}$.

Remarque 2.3.1

Cette définition est insuffisante pour caractériser $\mathbb{N}$: si on se limite à la description par l'existence de successeurs et prédécesseurs, on pourrait imaginer un ensemble constitué des éléments de $\mathbb{N}$ (la version intuitive), suivi d'une copie de $\mathbb{Z}$, suivi d'une autre copie de $\mathbb{Z}$ (la construction d'un tel ensemble qui vérifie cette définition avec les axiomes de Peano est un peu plus compliquée que cela, car il faut aussi imposer la stabilité par les opérations, mais un tel ensemble existe, et est à la base de la logique non-standard, puis de l'analyse non-standard, ou l'on remplace $\mathbb{N}$ par un tel ensemble). Il faut rajouter une hypothèse de minimalité pour obtenir l'ensemble $\mathbb{N}$ que nous connaissons bien.

On peut se demander, après avoir formalisé l'arithmétique de $\mathbb{N}$ à l'aide de ces axiomes, si la formalisation construite est bonne, en particulier si l'ensemble des axiomes donnés est cohérent (c'est-à-dire non contradictoire). Gödel apporte en 1931 une réponse assez surprenante à cette question :

Théorème 2.3.2 (Théorème de Gödel, 1931, HP)

La non contradiction de toute axiomatique de l'arithmétique de $\mathbb{N}$ est indécidable intrinsèquement.

Plus surprenant encore : si on parvient à donner une preuve de la non-contradiction de l'axiomatique de $\mathbb{N}$, cela signifie que cette axiomatique est contradictoire !

III.2 Propriétés de $\mathbb{N}$

Parmi les axiomes de Peano, il en est un dont on se sert fréquemment, c'est l'axiome de récurrence, que nous avons déjà étudié, et que nous rappelons ici.

Axiome 2.3.3 (principe de récurrence)

Soit $\mathcal{P}$ une propriété dépendant d'un entier $n \in \mathbb{N}$. On note $\mathcal{P}(n)$ la propriété au rang n. Alors :

$$\big(\mathcal{P}(0) \wedge (\forall n \in \mathbb{N},\ (\mathcal{P}(n) \Longrightarrow \mathcal{P}(n+1)))\big) \Longrightarrow \big(\forall n \in \mathbb{N}, \mathcal{P}(n)\big).$$

En d'autres termes, pour montrer une propriété $\mathcal{P}$ dépendant de $n \in \mathbb{N}$, il suffit :
- de montrer $\mathcal{P}(0)$ (initialisation)
- pour tout $n \in \mathbb{N}$, de montrer $\mathcal{P}(n) \Longrightarrow \mathcal{P}(n+1)$ (hérédité), ce qui revient à fixer n quelconque, supposer $\mathcal{P}(n)$ et démontrer $\mathcal{P}(n+1)$.

On en déduit :

Théorème 2.3.4 (propriété fondamentale de $\mathbb{N}$)

Tout sous-ensemble non vide et majoré de $\mathbb{N}$ admet un plus grand élément.

Corollaire 2.3.5

Tout sous-ensemble non vide de $\mathbb{N}$ admet un plus petit élément.

En fait, la terminologie « propriété fondamentale » n'est pas anodine. On aurait pu construire une axiomatique de $\mathbb{N}$ basée sur ce théorème (qui fonderait donc l'ensemble $\mathbb{N}$) plutôt que sur l'axiome de récurrence. C'est ce que montre le théorème suivant :

Théorème 2.3.6

La propriété fondamentale de $\mathbb{N}$ est équivalente à l'axiome de récurrence.

3 Applications, relations

« Les mathématiciens n'étudient pas des objets mais les relations entre ces objets. »

(Henri Poincaré)

« Ce n'est pas un lemme, et il n'est pas de moi »

(Max Zorn, à propos du « lemme de Zorn »)

Une civilisation constituée de groupes de personnes n'interagissant pas entre eux serait assez pauvre. Ce sont les relations entre groupes d'individus qui permettent de comparer, d'apprendre, de progresser, de transmettre, que ce soient des relations internes à un groupe donné, ou des relations d'un groupe à un autre. Une civilisation sans relation est vouée à la stérilité et à l'immobilisme, et donc à l'extinction.

Il en est de même pour les ensembles mathématiques. La théorie axiomatique des ensembles est certes très belle en soi, mais si on n'y rajoute pas une couche, elle est d'un intérêt assez limité pour le mathématicien recherchant le débouché concret (on a tendance à oublier que ce débouché concret a longtemps été la motivation-même des scientifiques, y compris mathématiciens). Comme dans le cas d'une civilisation, il faut faire interagir les ensembles, il faut créer des relations permettant de comparer les éléments d'un ensemble d'une façon une d'une autre. Ce n'est qu'ainsi qu'on peut donner vie aux ensembles.

I Applications

I.1 Définitions élémentaires

Définition 3.1.1 (Application, définition intuitive)

Soit E et F deux ensembles. Une application f est un objet qui à tout élément x de E associe un élément $f(x)$ de F.

Définition 3.1.2 (Application, définition formelle rigoureuse ; Graphe)

Soit E et F deux ensembles.

- Une application f est la donnée d'un sous-ensemble $G \subset E \times F$ tel que pour tout x dans E, il existe un et un seul élément y de F tel que $(x, y) \in G$.
- L'ensemble G est appelé *graphe* de f.
- Étant donné x, l'unique élément y de F tel que $(x, y) \in G$ est noté $f(x)$, et appelé *image de x par f*.

Définir une fonction nécessite donc la donnée de E, de F et du graphe G, ce qui revient à définir, d'une façon ou d'une autre, un élément $f(x)$ pour tout $x \in E$. L'ensemble de ces données est souvent synthétisé

par la notation suivante :

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

en remplaçant $f(x)$ par son expression, par exemple $\cos(x)$.
Attention, une expression $f(x)$ ne désigne pas une fonction, mais seulement la valeur d'une fonction en un point. Parler de « la fonction $x\cos(x)$ » n'a pas de sens. Tout au plus est-il acceptable de parler de la fonction $x \mapsto x\cos(x)$, même si les ensembles E et F sont omis dans cette notation.

Note Historique 3.1.3

- La notion est ancienne, mais reste longtemps vague et mal définie, sans réelle notation.
- En 1694, Leibniz est le premier à parler de « fonction d'un point M », puis Newton parle de « fluente du temps t ».
- Leibniz est le premier à proposer une notation, notamment dans le cas où on utilise plusieurs fonctions : il propose $\overline{x} \mid \underline{1}$ et $\overline{x} \mid \underline{2}$ pour ce qu'on noterait actuellement $f_1(x)$ et $f_2(x)$.
- Euler introduit en 1734 la notation fx, encore en vigueur actuellement (au parenthésage près).

Lorsque f est une fonction d'un sous-ensemble de $\mathbb{R}$ dans $\mathbb{R}$, le graphe de f est un sous-ensemble de $\mathbb{R}^2$. On visualise une fonction f en représentant son graphe dans le plan muni d'un repère (figure 3.1)

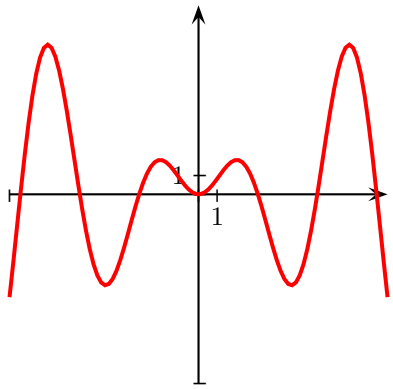


FIGURE 3.1 – Graphe de $x \mapsto x\sin x$

De même, pour des fonctions de deux variables à valeurs dans $\mathbb{R}$, le graphe est un sous-ensemble de $\mathbb{R}^3$, et on peut représenter une projection sur le plan de cet espace, aidant à la compréhension de la fonction (figure 3.2)
Lorsque E et F sont des ensembles finis, on peut représenter l'application f sous forme d'un *diagramme sagittal* : on représente les éléments de E d'un côté, ceux de F d'un autre côté, l'application f est alors représentée par une série de flèches reliant les éléments x de E à leur image $f(x)$ dans F.
Par exemple, l'application de $[\![1,6]\!]$ dans $[\![1,4]\!]$ définie par $f(1)=3$, $f(2)=1$, $f(3)=1$, $f(4)=4$, $f(5)=3$ et $f(6)=2$ sera représentée par le diagramme sagittal de la figure 3.3

Remarque 3.1.4 (Application ou fonction ?)

La distinction entre les deux n'est pas claire dans la littérature, et peut varier suivant le contexte :

- Usuellement, une fonction $f : E \to F$ n'a besoin d'être définie que sur un sous-ensemble E' de E, contrairement à une application qui doit être définie sur E.
- Parfois, le terme « fonction » permet aussi de distinguer parmi toutes les applications d'un certain type celles qui sont à valeurs dans $\mathbb{R}$ ou $\mathbb{C}$.

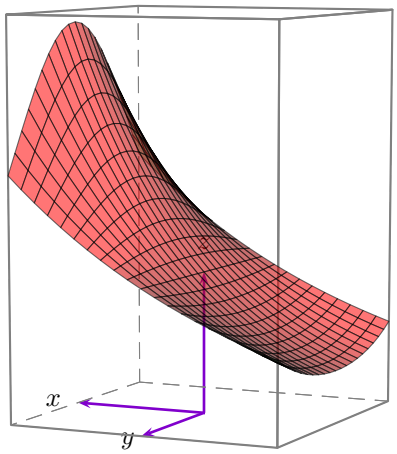


Figure 3.2 – Graphe de $f : (x, y) \mapsto \mathrm{e}^{x \cos y}$

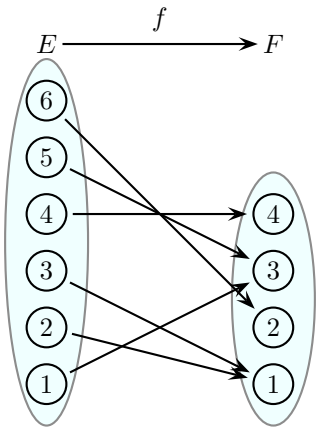


Figure 3.3 – Diagramme sagittal

Exemples 3.1.5

1. Application identique (identité)
2. Soit $E \subset F$. L'injection canonique $i : E \to F$.
3. Soit $E \subset F$. La fonction caractéristique de E dans F, $\mathbb{1}_E : F \to \{0, 1\}$.
4. La projection canonique $p_E : E \times F \to E$.

Notation 3.1.6

On note $\mathcal{F}(E, F)$, ou encore F^E l'ensemble des applications de E dans F.

Notons deux types de fonctions que nous rencontrerons assez rapidement :

Définition 3.1.7 (Familles et suites)

- Une *famille* $(x_i)_{i \in I}$ d'éléments d'un ensemble E, indexée par un ensemble I, est une application $x : I \longrightarrow E$. Dans cette situation, on utilise plutôt une notation indicielle x_i à la place de $x(i)$. L'ensemble I est appelé l'ensemble des indices de la famille $(x_i)_{i \in I}$
- Une suite d'éléments d'un ensemble E est une famille indexée par $\mathbb{N}$, ou éventuellement par un

ensemble $\{n \in \mathbb{N} \mid n \geqslant n_0\}$. Nous étudierons notamment les suites réelles ($E = \mathbb{R}$) et les suites complexes ($E = \mathbb{C}$)

Voici quelques moyens de définir une fonction (la liste n'est pas exhaustive) :

- **Définition par une formule explicite :**

$$\forall x \in \mathbb{R}, \quad f(x) = \frac{\sin x}{1+x^2}$$

- **Définition par disjonction de cas (fonction définie par morceaux) :**

$$\forall x \in \mathbb{R}, \quad f(x) = \begin{cases} \mathrm{e}^x & \text{si } x < 0 \\ 0 & \text{si } x = 0 \\ \frac{1}{x} & \text{si } x > 0. \end{cases}$$

- **Définition par récurrence ou induction structurelle :**

$$u_0 = 2 \qquad \text{et} \qquad \forall n \in \mathbb{N}, \quad u_{n+1} = 3u_n^2 - 2,$$

ou bien la fonction f définie sur l'ensemble des arbres binaires par :

$$f(\varnothing) = 0 \qquad \text{et} \qquad f(A) = f(G) + f(D) + 1,$$

où A est l'arbre dont les fils gauche et droit de la racine sont G et D. Que représente la fonction f ?

- **Définition implicite :**
La fonction f est définie comme étant, pour une valeur de x donnée, l'unique solution d'une certaine équation. Par exemple :

$$\forall x \in \mathbb{R}_+, \quad \int_0^{f(x)} \frac{\mathrm{e}^{xt^2}}{\mathrm{d}t} = x$$

- **Définition par une équation fonctionnelle ou différentielle :**
Exemple : il existe une unique fonction f telle que $f(0) = 1$ et pour tout $(x, y) \in \mathbb{R}^2$, $f(x+y) = f(x)f(y)$ (laquelle ?)
Exemple : il existe une unique fonction f dérivable sur $\mathbb{R}$, telle que $f(0) = 1$ et $f' = f$ (laquelle ?)

Définition 3.1.8 (composition de fonction, figure 3.4)

Soit $f : E \longrightarrow F$ et $g : F \longrightarrow G$. Alors, la fonction composée de f et de g est la fonction, notée $g \circ f$, définie par :

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

Définition 3.1.9 (Restriction, corestriction)

Soit E et F deux ensembles, et soit $E' \subset E$ et $F' \subset F$.

1. Soit $f : E \longrightarrow F$ et $g : E' \longrightarrow F$. Si pour tout $x \in E'$, $f(x) = g(x)$ (*i.e.* f et g coincident sur E'), on dit que g est la restriction de f à E' (une telle restriction est unique), et on la note $g = f\,|_{E'}$. On dit que f est un prolongement de g (non unique !)
2. Soit $f : E \longrightarrow F$ et $g : E \longrightarrow F'$. Si pour tout $x \in E$, $f(x) = g(x)$, alors on dit que g est la corestriction de f à F'. Si elle existe, la corestriction est unique. Elle existe si et seulement si $\mathrm{Im}(f) \subset F'$.

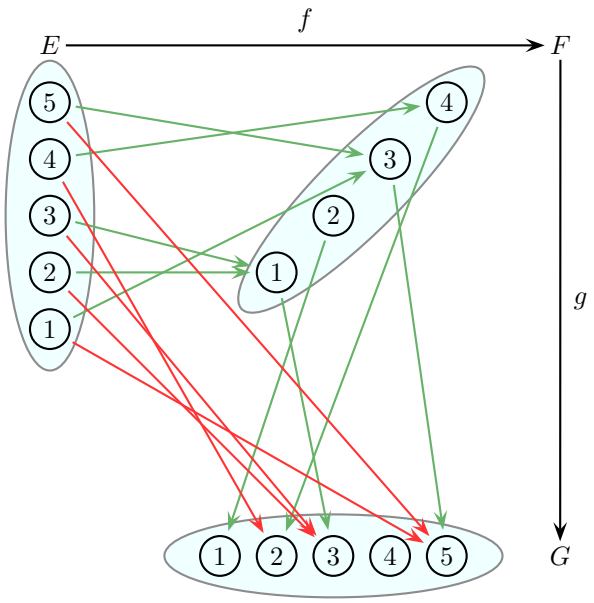


Figure 3.4 – Diagramme sagittal associé à une composition

I.2 Image directe, image réciproque

Soit E et F deux ensembles, et $f : E \longrightarrow F$ une application de E vers F.

Définition 3.1.10 (Image d'une application)
L'image de f est l'ensemble $\mathrm{Im}(f) = \{y \in F \mid \exists x \in E,\ f(x) = y\}$. C'est l'ensemble des points de F qui sont images d'un certain point x.

Définition 3.1.11 (Image directe)

1. Soit $E' \subset E$ un sous-ensemble de E. L'image directe de E' par f est l'ensemble :
$$f(E') = \{y \in F \ \mid \ \exists x \in E',\ f(x) = y.\}.$$
C'est l'ensemble des valeurs qui sont images d'un x de E'.
2. L'application « image directe », notée généralement $\hat{f}$ est l'application définie par :
$$\begin{array}{rccc} \hat{f} : & \mathcal{P}(E) & \longrightarrow & \mathcal{P}(F) \\ & E' & \longmapsto & f(E') \end{array}$$

Définition 3.1.12 (antécédent d'un élément)
Soit $y \in F$. Un antécédent par f de y est un élément x de E tel que $f(x) = y$

Remarque 3.1.13
Un élément de F peut ne pas avoir d'antécédent par F, ou peut en avoir plusieurs.

Définition 3.1.14 (Image réciproque)

1. Soit $F' \subset F$ un sous-ensemble de F. L'image réciproque de F' est l'ensemble : $\widehat{f^{-1}}(F') = \{x \in E \mid f(x) \in F'\}$ (souvent noté plus simplement $f^{-1}(F')$, ce qui n'entre pas en conflit avec l'image directe de la fonction réciproque, comme on le verra plus tard).

   C'est l'ensemble des éléments dont l'image est dans F', ou, autrement dit, l'ensemble des antécédents d'éléments de F'.
2. L'application « image réciproque », notée $\widehat{f^{-1}}$ est l'application définie par :

$$\begin{array}{rccc} \widehat{f^{-1}} : & \mathcal{P}(F) & \longrightarrow & \mathcal{P}(E) \\ & F' & \longmapsto & f^{-1}(F') \end{array}$$

Ainsi, un élément x de E est dans $f^{-1}(F')$ si et seulement si $f(x) \in F'$.

Remarque 3.1.15

Les applications $\hat{f}$ et $\widehat{f^{-1}}$ prennent en argument des ensembles, et renvoient des ensembles. Pour alléger les notations, on s'autorise à écrire $f^{-1}(y)$ pour $f^{-1}(\{y\})$. Il faut être conscient de l'abus de notation que l'on fait en écrivant cela. Il ne faut pas confondre $\widehat{f^{-1}}$ avec la fonction réciproque f^{-1}, qui n'existe que si f est bijective (cf plus bas), et qui est définie de F dans E, et non sur des ensembles.

Par exemple, l'ensemble des antécédents d'un élément y de F est $f^{-1}(\{y\})$, parfois noté simplement $f^{-1}(y)$, mais cette notation est ambiguë lorsque f est bijective (donc admet une réciproque f^{-1} : dans ce cas, $f^{-1}(y)$ désigne l'image directe par f^{-1} de y, et est un élément de E, alors $f^{-1}(\{y\})$ est un sous-ensemble de E. Dans cette situation, on a :

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

Propriétés 3.1.16 (Images directes et réciproques d'unions ou intersections)

Soit E et F deux ensembles, $f : E \longrightarrow F$ une application, et E', E'' deux sous-ensembles de E, F' et F'' deux sous-ensembles de F. Alors :

1. $f(E' \cup E'') = f(E') \cup f(E'')$
2. $f(E' \cap E'') \subset f(E') \cap f(E'')$
3. $f^{-1}(F' \cup F'') = f^{-1}(F') \cup f^{-1}(F'')$
4. $f^{-1}(F' \cap F'') = f^{-1}(F') \cap f^{-1}(F'')$

Exemple 3.1.17

On peut avoir une inclusion stricte $f(E' \cap E'') \subset f(E') \cap f(E'')$. Pour un exemple, voir figure 3.5

I.3 Injectivité, surjectivité, bijectivité

Proposition/Définition 3.1.18 (Injectivité)

Une application $f : E \longrightarrow F$ est dite *injective* si une des propositions équivalentes suivantes est vérifiée :

(i) tout élément de F admet au plus un antécédent par f ;

(ii) $\forall y \in F,\ \mathrm{Card}(f^{-1}(y)) \leqslant 1$,

(iii) $\forall (x, y) \in E^2,\ x \neq y \Longrightarrow f(x) \neq f(y)$,

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

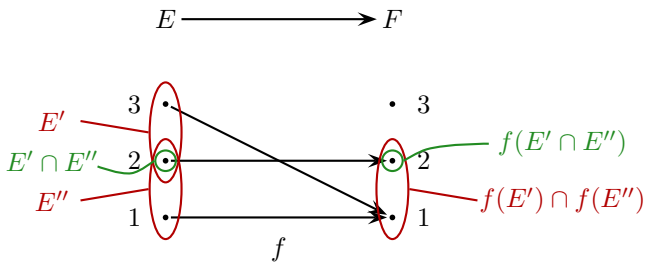


Figure 3.5 – Exemple dans lequel $f(E' \cap E'') \neq F(E') \cap f(E'')$

Proposition/Définition 3.1.19 (Surjectivité)

Une application $f : E \longrightarrow F$ est dite *surjective* si une des propositions équivalentes suivantes est vérifiée :

(i) tout élément de F admet au moins un antécédent par f ;

(ii) $\forall y \in F,\ \mathrm{Card}(f^{-1}(y)) \geqslant 1$;

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

(iv) $\mathrm{Im}(f) = F$.

Définition 3.1.20 (Bijectivité)

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

Dans le cas d'ensembles finis, on peut illustrer ces notions sur des diagrammes sagittaux (figure 3.6).

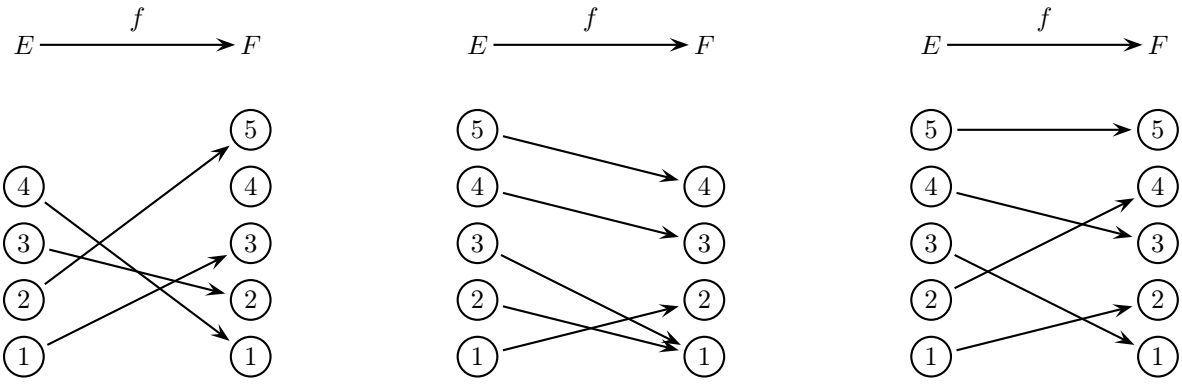


Figure 3.6 – Diagramme sagittal d'une fonction f injective, surjective ou bijective

Terminologie 3.1.21 (permutation, groupe symétrique)

Une bijection de E dans lui-même est appelée *permutation* de E. On note $\mathfrak{S}(E)$ l'ensemble des permutations de E. Si $E = \{1, \ldots, n\}$, on note $\mathfrak{S}_n$ au lieu de $\mathfrak{S}(E)$. L'ensemble $\mathfrak{S}_n$ est appelé *n-ième groupe symétrique*.

La notation $\mathfrak{S}$ est l'écriture gothique de la lettre S. On trouve parfois aussi plus simplement la notation

S_n au lieu de $\mathfrak{S}_n$ pour désigner le groupe symétrique (et $S(E)$ au lieu de $\mathfrak{S}(E)$, notation du programme officiel). On trouve également parfois Σ_n et $\Sigma(E)$

Exemples 3.1.22

1. Soit $E \subset F$. L'injection $i : E \to F$ est ..... .
2. Soit E et F deux ensembles, $F \neq \varnothing$. La projection $p_E : E \times F \to E$ est ..... .
3. La fonction identité $E \to E$ est ..... .
4. À quelle condition la fonction caractéristique $\mathbb{1}_E$ est-elle surjective ? injective ?
5. La fonction $x \mapsto x^2$ est :
   - ..... si elle est vue comme fonction de $\mathbb{R}$ dans $\mathbb{R}_+$;
   - ..... si elle est vue comme fonction de $\mathbb{R}_+$ dans $\mathbb{R}$
   - ..... si elle est vue comme fonction de $\mathbb{R}_+$ dans $\mathbb{R}_+$
   - ..... si elle est vue comme fonction de $\mathbb{R}$ dans $\mathbb{R}$.

   Il est donc important de porter une attention particulière aux domaines de départ et d'arrivée dans l'étude des propriétés d'injectivité et de surjectivité. D'autre part, constatez sur cet exemple qu'une fonction peut n'être ni injective ni surjective.

Remarque 3.1.23

Intuitivement, si $f : E \to F$ est une injection, il y a plus d'éléments dans F que dans E. C'est l'inverse si f est une surjection, et c'est E et F ont même cardinal si f est une bijection. C'est vrai si E et F sont finis. Attention, aux cas où E et F sont infinis : la situation peut parfois être contraire à l'intuition.

Exemples 3.1.24

1. Principe de l'hôtel de Hilbert : soit $x \notin \mathbb{N}$. Alors $\mathbb{N}$ et $\mathbb{N} \cup \{x\}$ peuvent être mis en bijection (on dit qu'ils ont même cardinal).
2. La numérotation en diagonales de $\mathbb{N} \times \mathbb{N}$ est une bijection de $\mathbb{N}$ sur $\mathbb{N}^2$.
3. Une bijection utilisée dans la numérotation de Gödel des formules. Soit $\mathcal{S}$ l'ensemble des suites finies (éventuellement vides) d'entiers positifs (il s'agit en fait de l'ensemble des polynômes à coefficients entiers positifs). Soit Ω la fonction

$$\begin{array}{rccc} \Omega : & \mathcal{S} & \longrightarrow & \mathbb{N}^* \\ & (x_1, \ldots, x_n) & \longmapsto & p_1^{x_1} \cdots p_n^{x_n} \end{array}$$

   où p_i désigne le i-ième nombre premier (par exemple $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ etc.).

   La fonction Ω est une bijection.
4. $\tan :]-\frac{\pi}{2}, \frac{\pi}{2}[\longrightarrow \mathbb{R}$ est une bijection (rappel : pour tout x pour lequel $\cos(x) \neq 0$, $\tan(x) = \frac{\sin(x)}{\cos(x)}$). Pourtout, il y a « plus » d'éléments dans $\mathbb{R}$ que dans $]-\frac{\pi}{2}, \frac{\pi}{2}[$.
5. Soit $f : [0,1[^2 \longrightarrow [0,1[$ définie de la façon suivante : étant donné x et y dans $[0,1[$, on note x_i le i-ième chiffre de x après la virgule dans son écriture décimale, et de même pour y_i. On rappelle que si x est décimal, x admet deux écritures décimales, l'une qui termine par une infinité de 0, l'autre qui termine par une infinité de 9 (car $0.9999999... = 1$). On choisit dans ce cas, afin que les x_i et les y_i soient définis de façon unique, la représentation terminant par des 0. On définit alors f sur le couple (x, y) par :

$$f(x, y) = 0.x_1 y_1 x_2 y_2 x_3 y_3 ....$$

   Il s'agit donc du réel de $[0,1[$ obtenu en alternant les chiffres de x et ceux de y.

   La fonction f est injective. Est-elle surjective ?

6. On peut de même contruire une fonction $g : [0,1[\longrightarrow [0,1[^2$ par :

$$g(x) = (0.x_1x_3x_4....; 0.x_2x_4x_6....),$$

les x_i représentant encore les chiffres de x dans l'écriture décimale, avec les mêmes conventions pour les réels décimaux.

La fonction f est surjective. Est-elle injective ?

Les exemples précédents permettent d'établir (avec la notion de cardinal définie plus loin) que $\mathbb{N}$ est de même cardinal que $\mathbb{N}^2$, que $]-\frac{\pi}{2}, \frac{\pi}{2}[$ est de même cardinal de $\mathbb{R}$ (en fait, tout intervalle non vide et non restreint à un singleton est de même cardinal que $\mathbb{R}$), et, plus surprenant encore, que $[0,1[^2$ est de même cardinal que $[0,1[$ (de quoi il ressort que $\mathbb{R}^2$ est de même cardinal que $\mathbb{R}$!)

Lemme 3.1.25 (partition associée à une fonction)

- *Soit f une fonction de E dans F. Alors les ensembles $f^{-1}(\{y\}), y \in F$ sont deux à deux disjoints, et $\bigcup_{y\in F} f^{-1}(\{y\}) = E$.*
- *Si f est surjective, $\{f^{-1}(\{y\}), y \in F\}$ est une partition de E.*
- *Sinon, $\{f^{-1}(\{y\}), y \in F\} \setminus \{\varnothing\}$ est une partition de E.*

Proposition 3.1.26 (Composée d'injections, surjections, bijections)

Soit $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications. Alors :

1. *si f et g sont injective, alors $g \circ f$ aussi ;*
2. *si f et g sont surjectives, alors $g \circ f$ aussi ;*
3. *si f et g sont bijectives, alors $g \circ f$ aussi ;*

Cette proposition admet une réciproque partielle (démonstration à savoir refaire sur demande)

Proposition 3.1.27 (« Dé-composée » d'injections, surjections, bijections, HP)

Soit $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications. Alors :

1. *si $g \circ f$ est injective, alors f est .....*
2. *si $g \circ f$ est surjective, alors g est .....*

Cette proposition est le premier pas vers la caractérisation suivante :

Théorème 3.1.28 (Caractérisation de l'injectivité et de la surjectivité)

Soit $f : E \longrightarrow F$ une fonction.

1. *f est surjective si et seulement s'il existe une fonction $g : F \to E$ telle que $f \circ g = \mathrm{id}_F$*
2. *f est injective si et seulement s'il existe une fonction $g : F \to E$ telle que $g \circ f = \mathrm{id}_E$.*

Ainsi, f est surjective si et seulement f est inversible à droite, et injective si et seulement si f est inversible à gauche.

Avertissement 3.1.29

La fonction g du théorème précédent n'est en général pas unique !

Si la fonction f est à la fois injective et surjective, on obtient l'unicité de g, et l'égalité de g dans les deux points :

Théorème 3.1.30 (Caractérisation de la bijectivité)

Soit $f : E \longrightarrow F$ une application. Les deux propriétés suivantes sont équivalentes :

(i) f est bijective

(ii) il existe une fonction $g : F \longrightarrow E$ telle que $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$.

De plus, dans ce cas, la fonction g est unique.

Avertissement 3.1.31

Attention, il ne suffit pas que $g \circ f = \mathrm{id}_E$ ou $f \circ g = \mathrm{id}_F$ pour obtenir la bijectivité : il faut avoir les deux égalités.

Définition 3.1.32 (Application réciproque)

Dans la situation du théorème précédent, l'application g telle que $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$ est appelée *application réciproque* de f, et est notée f^{-1}.

On vérifie facilement qu'étant donné $F' \subset F$ l'image directe $f^{-1}(F')$ par f^{-1} coïncide avec l'image réciproque $\widehat{f^{-1}}(F')$ par f. Cela nous permet d'omettre le chapeau dans la notation, l'ambiguïté entre la fonction image réciproque et l'application réciproque n'étant pas gênante.

II Cardinaux

On ne peut pas définir directement de cardinal d'un ensemble quelconque, sans introduire de nouveaux objets. En revanche, on peut définir sans difficulté des classes de cardinaux (donc définir une condition pour que deux ensembles aient même cardinal, ce qui permet ensuite de grouper les ensembles en classes d'ensembles de même cardinal). On peut ensuite comparer les cardinaux entre eux. Si on admet l'axiome du choix, deux cardinaux pevent toujours être comparés (l'un d'eux sera plus petit que l'autre).

Définition 3.2.1 (Définition de la cardinalité selon Frege)

On dit que deux ensembles E et F ont *même cardinal* s'il existe une bijection de E à F. On note $\mathrm{Card}(E) = \mathrm{Card}(F)$.

II.1 Cardinal d'un ensemble fini

Définition 3.2.2 (Ensemble de cardinal n)

On dit qu'un ensemble E est *de cardinal n* s'il est de même cardinal que $[\![1, n]\!]$, c'est-à-dire s'il existe une bijection de $[\![1, n]\!]$ vers E. On note $\mathrm{Card}(E) = n$, ou $|E| = n$.

En particulier :

- $|E| = 0$ si et seulement si $E = \varnothing$,
- $|[\![1, n]\!]| = n$.

Voyons maintenant les différentes règles de calcul des cardinaux relatives aux différentes constructions possibles sur les ensembles.

Proposition 3.2.3 (Cardinal d'une union disjointe)
Soit A, B, $A_1, \dots, A_n$ des ensembles finis.

1. *Si $A \cap B = \varnothing$, alors $|A \sqcup B| = |A| + |B|$.*
2. *Plus généralement, si pour tout $(i,j) \in [\![1,n]\!]^2$ tel que $i \neq j$, $A_i \cap A_j = \varnothing$, alors*

$$|A_1 \sqcup \cdots \sqcup A_n| = |A_1| + \cdots + |A_n|.$$

Proposition 3.2.4 (Cardinal d'un complémentaire)
Si $A \subset B$, alors $\left|\complement_B A\right| = |B| - |A|$.

Corollaire 3.2.5 (Cardinal d'un sous-ensemble)
Si $A \subset B$, alors $|A| \leqslant |B|$, avec égalité si et seulement si $A = B$.

On obtient alors le résultat, intuitivement évident, suivant :

Proposition 3.2.6 (Injectivité, surjectivité, bijectivité et cardinal)
Soit E et F deux ensembles finis, et soit $f : E \longrightarrow F$ une application. Alors :

1. *Si f est injective,* Card(E)....Card(F)
2. *Si f est surjective,* Card(E)....Card(F)
3. *Si f est bijective,* Card(E)....Card(F).

On en déduit notamment une caractérisation des applications bijectives entre ensembles de même cardinal :

Corollaire 3.2.7 (Caractérisation des bijections)
Soit A et B deux ensembles finis de même cardinal, et $f : A \to B$. Alors les 3 propriétés suivantes sont équivalentes :

(i) f est bijective
(ii) f est injective
(iii) f est surjective

Si l'union n'est pas disjointe, la somme $|A| + |B|$ compte deux fois les éléments de $A \cap B$. On obtient donc :

Proposition 3.2.8 (Cardinal d'une union quelconque)
Soit A et B des ensembles finis. On a :

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Plus généralement, on a :

Théorème 3.2.9 (Formule du crible de Poincaré, ou formule d'inclusion-exclusion, HP)
Soit $A_1, \dots, A_n$ des ensembles finis. Alors :

$$|A_1 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} |A_{i_1} \cap \cdots \cap A_{i_k}| = \sum_{\substack{I \subset [\![1,n]\!] \\ I \neq \varnothing}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right|.$$

On en verra la démonstration (par récurrence sur n) plus tard. Elle est assez technique, et nécessite une bonne maîtrise des signes $\sum$.

Proposition 3.2.10 (Cardinal d'un produit cartésien)

1. *Soit A et B deux ensembles finis. Alors $|A \times B| = |A| \times |B|$.*
2. *Plus généralement, soit $A_1, \dots, A_n$ des ensembles finis. Alors*

$$|A_1 \times \cdots \times A_n| = \prod_{i=1}^{n} |A_i|.$$

Enfin, le résultat suivant justifie la notation F^E pour désigner l'ensemble des applications de E dans F :

Proposition 3.2.11 (Cardinal d'un ensemble d'applications)
Soit E et F deux ensembles finis. On a alors : $|F^E| = |F|^{|E|}$.

II.2 Dénombrabilité

Notation 3.2.12 (cardinal de $\mathbb{N}$, HP)
On note $\aleph_0$ le cardinal de $\mathbb{N}$.

Définition 3.2.13 (Dénombrabilité, Spé)
Un ensemble E est *dénombrable* s'il peut être mis en bijection avec $\mathbb{N}$, donc s'il est de cardinal $\aleph_0$.
Un ensemble E est *au plus dénombrable* s'il est fini ou dénombrable.

Remarque 3.2.14
Un ensemble fini n'est pas dénombrable, seulement « au plus » dénombrable.

Lemme 3.2.15 (Caractérisation des ensembles au plus dénombrables, Spé)
Soit E un ensemble non vide. Les trois propriétés suivantes sont équivalentes :

(i) E est au plus dénombrable

(ii) il existe une fonction injective $f : E \longrightarrow \mathbb{N}$.

(iii) il existe une fonction surjective $f : \mathbb{N} \longrightarrow E$.

(iv) il existe un sous-ensemble F de $\mathbb{N}$ et une bijection $f : F \longrightarrow E$

Proposition 3.2.16 (Construction d'ensembles dénombrables, Spé)

1. *Un sous-ensemble infini d'un ensemble dénombrable est dénombrable.*
2. *Une union d'un nombre fini ou dénombrable d'ensembles au plus dénombrables est au plus dénombrable, et dénombrable si au moins un des ensembles l'est (ce n'est pas une équivalence dans le cas d'une union ayant une infinité de termes).*
3. *Si E et F sont au plus dénombrables, $E \times F$ aussi.*
4. *Si E est dénombrable et F est au plus dénombrable non vide, alors $E \times F$ est dénombrable.*
5. *Plus généralement, un produit d'un nombre fini d'ensembles au plus dénombrables est au plus dénombrable ; il est dénombrable si au moins un l'est et si les autres sont non vides.*

Corollaire 3.2.17 (Spé)

1. *L'ensemble $\mathbb{Z}$ est dénombrable.*
2. *L'ensemble $\mathbb{N}^2$ et plus généralement $\mathbb{N}^p$ est dénombrable.*
3. *L'ensemble $\mathbb{Q}$ des rationnels est dénombrable.*
4. *L'ensemble $\mathbb{Z}[x]$ des fonctions polynomiales à coefficients entiers est dénombrable.*

Théorème 3.2.18 (Spé)

L'ensemble des réels $\mathbb{R}$ est non dénombrable.

Définition 3.2.19 (Nombres algébriques, transcendants sur $\mathbb{Q}$, HP)

Soit $x \in \mathbb{R}$.
- On dit que x est algébrique sur $\mathbb{Q}$ s'il existe un polynôme P à coefficients dans $\mathbb{Q}$ tel que $P(x) = 0$.
- On dit que x est transcendant sur $\mathbb{Q}$ s'il n'est pas algébrique.

En admettant provisoirement que tout polynôme a un nombre fini de racines, on obtient le joli résultat suivant

Proposition 3.2.20 (cardinal de l'ensemble des nombres algébriques, HP)

L'ensemble des nombres algébriques est dénombrable.

Corollaire 3.2.21 (existence de nombres transcendants, HP)

Il existe des nombres transcendants.

Note Historique 3.2.22 (nombres transcendants, HP)

Il a fallu attendre Liouville vers la fin du 19-ième siècle pour trouver explicitement un nombre transcendant (la constante de Liouville $\sum_{i \geqslant 1} 10^{-i!}$). Ce n'est qu'après que Hermitte montrent la transcendance de e, et Lindemann la transcendance de π (dans les années 1880)

Définition 3.2.23

On dit que $\mathrm{Card}(E) \leqslant \mathrm{Card}(F)$ si et seulement s'il existe une injection de E dans F, et $\mathrm{Card}(E) < \mathrm{Card}(F)$ si et seulement si $\mathrm{Card}(E) \leqslant \mathrm{Card}(F)$ et $\mathrm{Card}(E) \neq \mathrm{Card}(F)$.

Théorème 3.2.24 (Cantor, 1891, HP)
Pour tout ensemble X, on a $\mathrm{Card}(X) < \mathrm{Card}(\mathcal{P}(X))$.

Comme on l'a signalé plus haut, ce résultat entre en contradiction avec l'existence de l'ensemble des ensembles.

Théorème 3.2.25 (cardinal de $\mathbb{R}$, HP)
Les ensembles $\mathbb{R}$ et $\mathcal{P}(\mathbb{N})$ ont même cardinal.

Terminologie 3.2.26 (puissance du continu, HP)
Le cardinal de $\mathbb{R}$ est appelé *puissance du continu*, et noté $\mathcal{C}$.

Y a-t-il des ensembles de cardinal intermédiaire entre $\mathbb{N}$ et $\mathbb{R}$? Cette question est indécidable. On admet généralement que non : il s'agit de *l'hypothèse du continu* :

Axiome 3.2.27 (hypothèse du continu, HP)
Il n'existe pas d'ensemble X tel que $\aleph_0 < \mathrm{Card}(X) < \mathcal{C}$.

On note $\aleph_1$ le plus petit cardinal strictement supérieur à $\aleph_0$. L'hypothèse du continu s'exprime alors de la manière suivante : $\mathcal{C} = \aleph_1$.

III Relations

III.1 Généralités

Définition 3.3.1 (relation n-aire)
Soit $n \in \mathbb{N}^*$. Une *relation n-aire* entre n ensembles $E_1, E_2, \ldots, E_n$ est un sous-ensemble G de $\prod_{i=1}^{n} E_i$.
L'entier n est appelé *arité* de la relation.

Le cas le plus important, et le seul que nous considérerons, est le cas des *relations binaires*, d'arité 2.

Notation 3.3.2
Étant donné une relation binaire entre E et F, c'est-à-dire un sous-ensemble G de $E \times F$, on note souvent $x\mathcal{R}y$ pour dire que $(x, y) \in G$, et on dit que x est en relation avec y. On parle alors de la relation $\mathcal{R}$.
Certains types de relation sont aussi notés $x \equiv y$, ou $x \sim y$, ou $x \leqslant y$...

Exemples 3.3.3

1. appartenance à une droite
2. appartenance à un parti politique : les deux éléments en relation ne sont pas nécessairement de même nature, et certains éléments peuvent n'être en relation avec rien.
3. L'inclusion entre ensemble. L'appartenance entre ensembles.
4. L'égalité des cardinaux.
5. Les congruences d'entiers.

Comme pour les fonctions, on peut représenter une relation par un diagramme sagittal. Par exemple, la relation représentée par la figure 3.7 est la relation entre $[\![1,5]\!]$ et $[\![1,4]\!]$ définie par le sous-ensemble $G = \{(1,2),(1,3),(2,3),(2,4),(4,1),(5,1),(5,2),(5,4)\}$, donc la relation définie par $1\mathcal{R}2$, $1\mathcal{R}3$, $2\mathcal{R}3$, $2\mathcal{R}4$, $4\mathcal{R}1$, $5\mathcal{R}1$, $5\mathcal{R}2$, $5\mathcal{R}4$, les autres paires n'étant pas en relation.

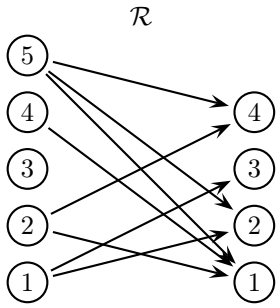


Figure 3.7 – Diagramme sagittal d'une relation

On peut également représenter cette relation sous forme d'un tableau à double-entrée, en décidant de représenter par deux signes distinctifs le fait que $x\mathcal{R}y$ soient en relation ou non (par exemple par une croix ou par rien) Ainsi, la relation précédente est représentée par le tableau de la figure 3.8

E \ F	1	2	3	4
1		×	×	
2	×			×
3				
4	×			
5	×	×		×

Figure 3.8 – Représentation tabulaire (ou matricielle) d'une relation

Remarque 3.3.4

Les fonctions sont des cas particuliers de relation binaire. Une relation binaire définissant une fonction est appelée relation fonctionnelle.

Plus précisément :

Définition 3.3.5 (relation fonctionnelle)

Une relation $\mathcal{R}$ entre E et F est *fonctionnelle* si pour tout x de E il existe un et un seul y de F tel que $x\mathcal{R}y$.

Lorsque $\mathcal{R}$ est une relation entre E et lui-même, on dit que $\mathcal{R}$ est une relation sur E. Dans ce cas, on dispose d'une troisième représentation possible, correspondant à la représentation sagittale dans laquelle on a identifié les éléments des deux ensembles de départ et d'arrivée. On obtient de la sorte un graphe orienté dont les sommets sont les éléments de E. Par exemple, la relation définie sur $[\![1,4]\!]$ par $1\mathcal{R}1$, $1\mathcal{R}3$, $2\mathcal{R}3$, $3\mathcal{R}2$, $3\mathcal{R}4$, $4\mathcal{R}1$ et $4\mathcal{R}4$ est représentée par le graphe de la figure 3.9

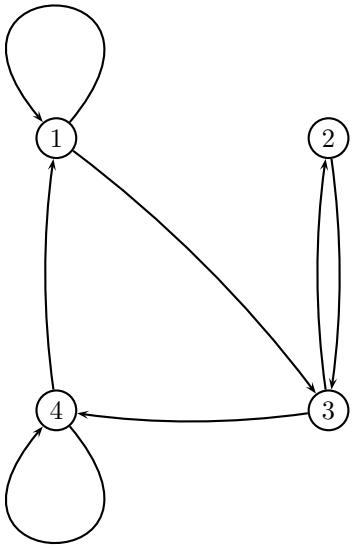


FIGURE 3.9 – Graphe d'une relation sur E

III.2 Opérations sur les relations

La composition des fonctions se généralise aux relations :

Définition 3.3.6 (Composée de deux relations)
Soit $\mathcal{R}$ une relation de E à F et $\mathcal{S}$ une relation de F à G. Alors la relation $\mathcal{S} \circ \mathcal{R}$ est la relation de E à G définie par :

$$\forall (x, z) \in E \times G, \quad x(\mathcal{S} \circ \mathcal{R})z \iff \exists y \in F, \quad (x\mathcal{R}y) \wedge (y\mathcal{S}z).$$

Sur les diagrammes sagittaux, la composition se traduit par la composition des flèches de toutes les manières possibles. Pour un exemple, voir la figure 3.10.

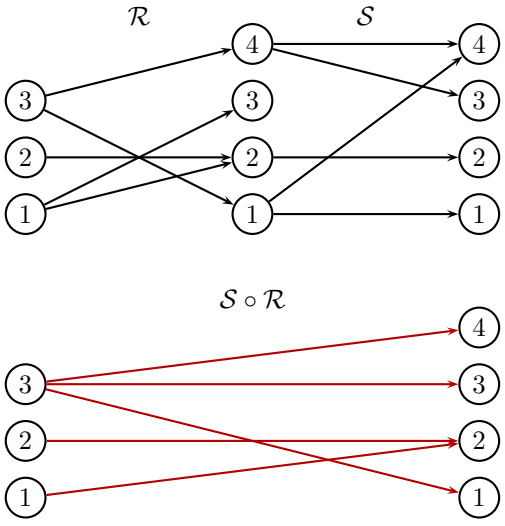


FIGURE 3.10 – Composée de deux relations

Si les relations sont fonctionnelles, la composition des relations coïncide avec la composition des fonctions.

Définition 3.3.7 (Réciproque d'une relation, HP)
Étant donné une relation $\mathcal{R}$ de E à F, la réciproque de $\mathcal{R}$, notée $\mathcal{R}^{-1}$, est la relation de F à E définie par :

$$\forall (x,y) \in F \times E, \quad x\mathcal{R}^{-1}y \iff y\mathcal{R}x.$$

Lorsque E et F sont finis, cela consiste simplement à inverser l'ordre des flèches dans le diagramme sagittal (ou dans le graphe, lorsque $E = F$). On illustre cela dans la figure 3.11

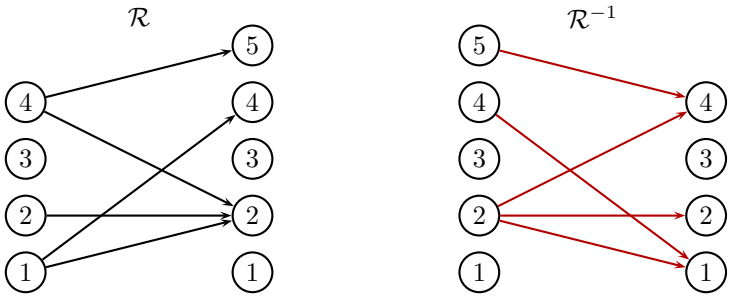


Figure 3.11 – Réciproque d'une relation

Ainsi, toute relation admet une réciproque. En particulier, toute fonction f (vue comme relation fonctionnelle) admet une réciproque au sens des relations, mais cette réciproque n'est une relation fonctionnelle que si f est bijective. Dans ce cas, les notions de réciproque d'une relation et de réciproque d'une fonction coïncident.

III.3 Définition de quelques propriétés sur les relations

On définit maintenant un certain nombre de propriétés susceptibles d'être satisfaites par une relation d'un ensemble E dans lui-même.

Définition 3.3.8 (reflexivité, symétrie, antisymétrie, transitivité)
Soit $\mathcal{R}$ une relation sur E. On dit que :
- $\mathcal{R}$ est reflexive si pour tout $x \in E$, $x\mathcal{R}x$;
- $\mathcal{R}$ est symétrique si pour tout $(x,y) \in E^2$, $x\mathcal{R}y \implies y\mathcal{R}x$;
- $\mathcal{R}$ est antisymétrique si pour tout $(x,y) \in E^2$, $(x\mathcal{R}y) \wedge (y\mathcal{R}x) \implies (x = y)$;
- $\mathcal{R}$ est transitive si pour tout $(x,y,z) \in E^3$, $(x\mathcal{R}y) \wedge (y\mathcal{R}z) \implies (x\mathcal{R}z)$.

Ainsi :
- $\mathcal{R}$ est reflexive ssi $\mathrm{id}_E \subset \mathcal{R}$ (au sens des sous-ensembles de $E \times E$, id_E étant la diagonale de cet ensemble)
- $\mathcal{R}$ est symétrique ssi $\mathcal{R} = \mathcal{R}^{-1}$
- $\mathcal{R}$ est antisymétrique ssi $\mathcal{R} \cap \mathcal{R}^{-1} \subset \mathrm{id}_E$
- $\mathcal{R}$ est transitive ssi $\mathcal{R} \circ \mathcal{R} \subset \mathcal{R}$.

Nous allons maintenant définir deux types de relations que l'on rencontre fréquemment.

III.4 Relations d'équivalence

Définition 3.3.9 (relation d'équivalence)
Une relation d'équivalence sur E est une relation reflexive, symétrique et transitive. On note souvent $x \equiv y$ ou $x \sim y$ pour indiquer que x et y sont en relation.

Exemples 3.3.10

1. Égalité.
2. Congruences modulo n dans $\mathbb{N}$ (notation $\equiv_{[n]}$ ou $\equiv ...[n]$).
3. Congruences dans $\mathbb{R}$.
4. Appartenance à la même part d'une partition.
5. La relation définissant $\mathbb{Q}$ sur $\mathbb{Z} \times \mathbb{N}^*$: $(p, q) \equiv_{\mathbb{Q}} (p', q')$ si et seulement $pq' = p'q$ (ces deux couples vont définir le même rationnel).
6. Égalité des cardinaux.
7. Conjugaison dans $\mathfrak{S}_n$.
8. Multiplication par un scalaire non nul dans $\mathbb{R}^n$ ou $\mathbb{C}^n$.
9. Multiplication par un scalaire $\lambda > 0$ dans $\mathbb{R}^n$.

Une relation d'équivalence sur un ensemble fini peut être représenté par son graphe orienté (figure 3.12). Ce graphe possède un certain nombre de caractéristiques :

- Le graphe se décompose en un certain nombre de blocs non reliés les uns les autres, les points au sein d'un même bloc étant reliés (on parle de composantes connexes du graphe)
- Chaque point appartient à un bloc (il y est éventuellement seul). Ainsi, les blocs forment une partition de E.
- À l'intérieur de chaque bloc, toutes les flèches possibles sont présentes (y compris celles reliant un point et lui-même.

Les différents blocs sont appelés *classes d'équivalence*.

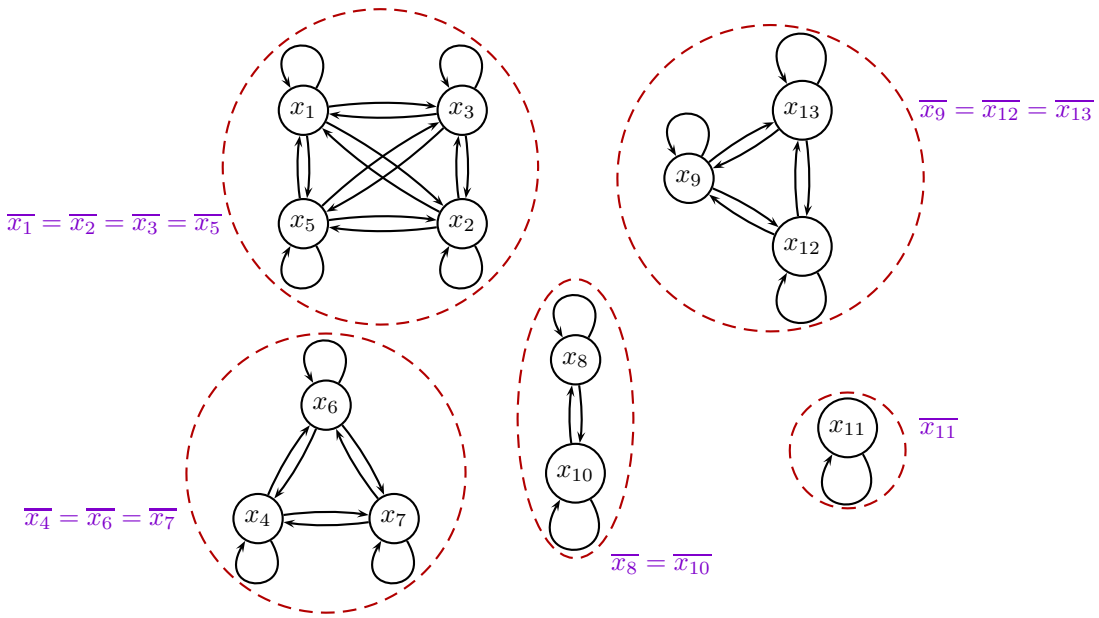


FIGURE 3.12 – Graphe d'une relation d'équivalence sur $E = \{x_1, x_2, \ldots, x_{13}\}$.

Cette situation se généralise :

Définition 3.3.11 (classes d'équivalence)

Soit $\mathcal{R}$ une relation d'équivalence sur E, et $x \in E$. La *classe d'équivalence de x sous la relation $\mathcal{R}$* est le sous-ensemble C_x de E constitué des éléments en relation avec x :

$$C_x = \{y \in E \mid x\mathcal{R}y\}.$$

Théorème 3.3.12 (Partition formée par les classes d'équivalence)

Soit E un ensemble, et $\mathcal{R}$ une relation d'équivalence sur E. L'ensemble des classes d'équivalence sous $\mathcal{R}$ forme une partition de E.

En particulier, si $y \in C_x$, alors $C_x = C_y$.
Pour les propriétés « stables » par la relation d'équivalence, les points d'une même classe d'équivalence jouent des rôles similaires, et n'ont pas lieu d'être distingués. On formalise cela en introduisant un ensemble dont les éléments sont les classes d'équivalences (ainsi, tous les points d'une même classe représentent la même classe, et sont considérés comme égaux dans ce nouvel ensemble) :

Définition 3.3.13 (Ensemble quotient, HP)

L'ensemble des classes sous la relation $\mathcal{R}$ s'appelle *l'ensemble quotient de E par $\mathcal{R}$*, et est noté $E/\mathcal{R}$. C'est un sous-ensemble de $\mathcal{P}(E)$.

Ainsi, en notant $\overline{x}$ la classe d'équivalence d'un élément x de E, l'ensemble $E/\mathcal{R}$ est l'ensemble formé des éléments $\overline{x}$, où l'on impose $\overline{x} = \overline{y}$ dès que $x\mathcal{R}y$.

Exemples 3.3.14

1. On définit $\mathbb{Q}$ comme étant le quotient $(\mathbb{Z} \times \mathbb{N}^*)/\equiv_{\mathbb{Q}}$.
2. On définit $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\equiv_{[n]}$. C'est un ensemble à n éléments.
3. Espace projectif réel ou complexe.

Dans l'exemple 2 ci-dessus, l'ensemble $\mathbb{Z}$ étant muni d'une loi d'addition et d'une loi de multiplication, on aimerait savoir si ces lois « passent au quotient » autrement dit, si elles permettent de définir une somme et un produit sur $\mathbb{Z}/n\mathbb{Z}$. La notion de congruence est adaptée à cette situation.

Définition 3.3.15 (Congruence)

Soit E un ensemble, muni d'un certain nombre d'opérations $\times_1, \times_2, \ldots, \times_n$. On dit qu'une relation d'équivalence $\mathcal{R}$ est une congruence sur $(E, \times_1, \ldots, \times_n)$ si

$$\forall (x, y, x', y') \in E^4,\ \forall i \in [\![1, n]\!],\quad (x\mathcal{R}x') \wedge (y\mathcal{R}y') \Longrightarrow (x \times_i y)\mathcal{R}(x' \times_i y').$$

Proposition 3.3.16 (Congruence des entiers)

La relation de congruence des entiers $\equiv_{[n]}$ est une congruence sur $(\mathbb{Z}, +, \times)$.

Proposition 3.3.17 (Passage au quotient des opérations, HP)

Soit $(E, \times_1, \ldots, \times_n)$ un ensemble muni de n lois d'opérations, et $\mathcal{R}$ une congruence sur $(E, \times_1, \ldots, \times_n)$. Alors on peut définir sur $E/\mathcal{R}$ des lois $\dot{\times}_1, \ldots, \dot{\times}_n$ telles que pour tout $i \in [\![1, n]\!]$, et tout $(x, y) \in E^2$:

$$\overline{x}\dot{\times}_i\overline{y} = \overline{x \times_i y}.$$

Corollaire 3.3.18 (Addition et multiplication de $\mathbb{Z}/n\mathbb{Z}$, HP)

On peut munir $\mathbb{Z}/n\mathbb{Z}$ d'une addition $\dot{+}$ et d'une multiplication $\dot{\times}$, notées plus simplement $+$ et $\times$ (la multiplication est parfois aussi simplement notée par un point $\cdot$, ou même simplement omise), telles que :

$$\forall (x,y) \in \mathbb{Z}^2, \quad \overline{x} + \overline{y} = \overline{x+y} \text{ et } \overline{x} \times \overline{y} = \overline{x \times y}$$

Exemple 3.3.19

Table des lois de $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$.

III.5 Relations d'ordre

Une autre famille de relation est celle qui permet de définir des inégalités.

Définition 3.3.20 (relation d'ordre large)

Une relation d'ordre sur E est une relation reflexive, antisymétrique et transitive. On note souvent $x \leqslant y$ pour indiquer que y est en relation avec x. Les écritures $x \leqslant y$ et $y \geqslant x$ sont équivalentes.

La relation d'ordre stricte $<$ associée à la relation d'ordre large $\leqslant$ est définie par :

$$\forall (x,y) \in E^2, \quad x < y \iff (x \leqslant y) \wedge (x \neq y).$$

Exemples 3.3.21

1. L'inégalité usuelle $\leqslant$ sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$ définit une relation d'ordre sur ces ensembles.
2. L'inégalité opposée $\geqslant$ définit une autre relation d'ordre ; il s'agit de la relation réciproque de $\leqslant$.
3. De façon générale, étant donné une relation d'ordre $\mathcal{R}$ sur un ensemble, $\mathcal{R}^{-1}$ est encore une relation d'ordre.
4. La relation de divisibilité $a \mid b$ est une relation d'ordre sur $\mathbb{N}^*$ mais pas sur $\mathbb{Z}$.
5. L'inclusion dans $\mathcal{P}(E)$.
6. Le raffinement des partitions d'un ensemble.
7. L'ordre produit sur $\mathbb{N}^n$
8. L'ordre lexicographique sur $\mathbb{N} \times \mathbb{N}$, et plus généralement sur $\mathbb{N}^n$.
9. Étant donné un alphabet A muni d'une relation d'ordre $\leqslant$, l'ordre lexicographique sur l'ensemble des mots définis par A.
10. L'égalité.

La figure 3.13 donne le graphe orienté associé à une relation d'ordre sur un ensemble fini. Certaines flèches sont nécesairement présentes (les flèches d'un élément vers lui-même, par reflexivité), ou déduites des autres (par transitivité). On se limite alors souvent au digramme constitué par les flèches élémentaires (engendrant les autres), c'est-à-dire les flèches entre deux éléments consécutifs. Pour l'exemple donné dans la figure 3.13, on obtient alors le diagramme de la question 3.14. Par convention, dans ce diagramme, les flèches vont en montant : plus un élément est placé haut, plus il est « grand » pour le relation d'ordre (à condition de pouvoir être comparé).
Dans $\mathbb{R}$ muni de l'ordre usuel, on peut comparer deux à deux tous les éléments, mais ce n'est pas toujours le cas (cas de la divisibilité par exemple). Cette remarque motive la définition suivante :

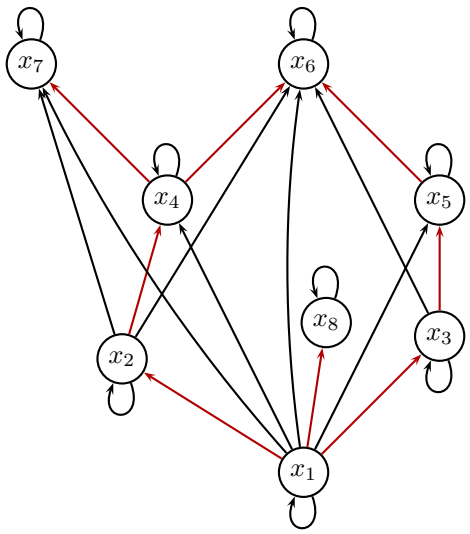


Figure 3.13 – Graphe d'une relation d'ordre sur $E = \{x_1, x_2, \ldots, x_8\}$.

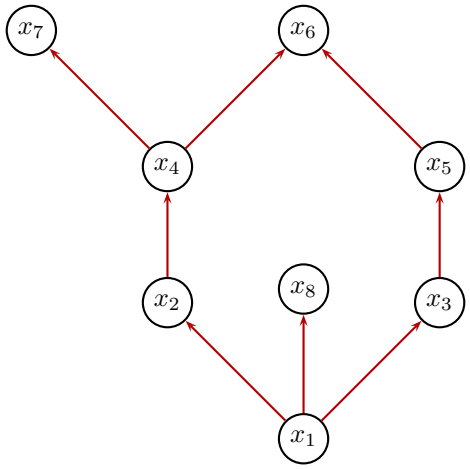


Figure 3.14 – Diagramme associé à la relation de la figure 3.13

Définition 3.3.22 (ordre total, ordre partiel)

- Soit $\mathcal{R}$ une relation d'ordre sur un ensemble E. On dit que $\mathcal{R}$ est une relation d'ordre total si pour tout $(x, y) \in E$, soit $x \leqslant y$ soit $y \leqslant x$.
- Dans le cas contraire, on dit que $\mathcal{R}$ est une relation d'ordre partiel.

Exemples 3.3.23

1. L'ordre défini par le diagramme de la figure 3.14 n'est pas total : par exemple x_8 et x_7 ne sont pas comparables. En fait, le diagramme associé à une relation d'ordre total est linéaire.
2. L'ordre usuel sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$, ainsi que l'ordre lexicographique sur $\mathbb{N}^n$, ou sur l'ensemble des mots définis à partir d'un alphabet sont des ordres totaux.
3. L'ordre produit sur $\mathbb{N}^n$ (pour $n \geqslant 2$), la relation de divisibilité dans $\mathbb{N}^*$, la relation d'inclusion dans $\mathcal{P}(E)$ (lorsque E possède au moins 2 éléments), le raffinement des partitions de E (lorsque E possède au moins 3 éléments) sont des ordres partiels.

4. Si $\leqslant$ est un ordre total, alors $\geqslant$ est un ordre total.

Proposition/Définition 3.3.24 (restriction d'une relation d'ordre)

Soit E un ensemble muni d'une relation d'ordre $\mathcal{R}$, et A un sous-ensemble de E. Alors $\mathcal{R}$ définit sur A une relation d'ordre $\mathcal{R}'$ par :

$$\forall (x,y) \in A^2, \quad x\mathcal{R}'y \iff x\mathcal{R}y.$$

Il s'agit de la restriction à A de la relation $\mathcal{R}$, ou de la relation induite par $\mathcal{R}$ sur A. Elle est généralement notée $\mathcal{R}$ également.

Définition 3.3.25 (minimum, maximum)

Soit $(E, \leqslant)$ un ensemble muni d'une relation d'ordre.

1. Un élément m de E est appelé *plus petit élément de* E (ou *élément minimum*) si : $\forall m' \in E,\ m \leqslant m'$.
2. Un élément M de E est appelé *plus grand élément de* E (ou *élément maximum*) si : $\forall m' \in E,\ M \geqslant m'$.
3. Étant donné un sous-ensemble A de E, un élément minimum (*resp.* maximum) de A est un élément minimum (*resp.* maximum) pour la relation d'ordre $\mathcal{R}'$ induite par $\mathcal{R}$ sur A.

Proposition 3.3.26 (unicité du minimum)

S'il existe, le plus petit élément de E (resp. *de* $A \subset E$) *est unique. De même pour le plus grand élément.*

Un ensemble n'a pas nécessairement de minimum ou de maximum ($\mathbb{Z}$ par exemple, ou $\mathcal{P}(E) \setminus \{E, \varnothing\}$, pour la relation d'inclusion).

Exemple 3.3.27

Dans l'exemple de la figure 3.14, E n'admet par de maximum, mais admet un minimum.

Définition 3.3.28 (élément minimal, maximal ; HP)

Soit $(E, \leqslant)$ un ensemble muni d'une relation d'ordre.

1. Un élément m de E est appelé *élément minimal* de E s'il n'existe pas d'élément x de E tel que $x < m$..
2. Un élément M de E est appelé *élément maximal*) s'il n'existe pas d'élément x de E tel que $x > M$.

Remarque 3.3.29 (distinction élément minimum/élément maximal)

Si l'ordre défini sur E est total, la notion d'élément minimal coïncide avec la notion d'élément minimum. Mais ce n'est plus vrai si la relation n'est que partielle, car $x < m$ n'est dans ce cas pas la négation de $x \geqslant m$.

Exemples 3.3.30

1. Dans l'exemple de la figure 3.14, x_6, x_7 et x_8 sont des éléments maximaux, mais pas maximums. Le seul élément minimal est x_1, qui est aussi le minimum.

   Dans un diagramme de ce type, un élément maximal est un élément duquel ne part aucune flèche.

2. Soit E ayant au moins deux éléments. Dans $\mathcal{P}(E) \setminus \{E, \varnothing\}$, étant donné $x \in E$, $\{x\}$ est minimal mais pas minimum. De même $E \setminus \{x\}$ est maximal mais pas maximum.
   Étant donné $y \in E$, $y \neq x$, $\{y\}$ est un autre élément minimal, et $E \setminus \{y\}$ est un autre élément maximal. Ainsi, contrairement à ce qu'il se passe pour le maximum et le minimum, on n'a pas unicité de l'élément maximal ou minimal.
3. Dans $\mathbb{N} \setminus \{0, 1\}$, les nombres premiers sont minimaux pour la relation de divisibilité, mais il n'y a pas d'élément minimum.

Définition 3.3.31 (minorant, majorant)

Soit $(E, \leqslant)$ un ensemble muni d'une relation d'ordre. Soit $A \subset E$.

1. Un minorant m de A est un élément $m \in E$ tel que : $\forall a \in A,\ a \geqslant m$
2. Un majorant M de A est un élément $M \in E$ tel que : $\forall a \in A,\ a \leqslant M$

Définition 3.3.32 (borne supérieure, borne inférieure)

Soit $(E, \leqslant)$, et soit $A \subset E$.

1. La borne inférieure de A dans E, notée $\inf\limits_{x \in A}{}_E\ x$ ou $\inf\limits_{x \in A} x$ ou $\inf A$ est le plus grand des minorants de A, **s'il existe**.
2. La borne supérieure de A dans E, notée $\sup\limits_{x \in A}{}_E\ x$ ou $\sup\limits_{x \in A} x$ ou $\sup A$ est le plus petit des majorants de A, **s'il existe**.
3. Étant donnés $x_1, \ldots, x_n$ dans E, la borne inférieure (*resp.* la borne supérieure) des éléments $x_1, \ldots, x_n$, notée $\inf(x_1, \ldots, x_n)$ (*resp.* $\sup(x_1, \ldots, x_n)$) est la borne inférieure (*resp.* supérieure) de l'ensemble $\{x_1, \ldots, x_n\}$.

Exemple 3.3.33 (Propriété fondamentale de $\mathbb{R}$)

Tout sous-ensemble non vide majoré de $\mathbb{R}$ admet une borne supérieure. Cette propriété soit doit être prise comme axiome pour la construction de $\mathbb{R}$, soit découle immédiatement d'axiomes équivalents (il y a plusieurs façons équivalentes de construire $\mathbb{R}$, en imposant dans le cahier des charges des propriétés différentes)

Avertissement 3.3.34

Attention à l'ensemble dans lequel on considère la borne supérieure. Tout sous-ensemble borné de $\mathbb{Q}$ admet une borne supérieure dans $\mathbb{R}$, mais pas nécessairement dans $\mathbb{Q}$.

Théorème 3.3.35 (Caractérisation de la borne supérieure pour un ordre total)

Soit E un ensemble totalement ordonné et A un sous-ensemble de E. Pour que $b \in E$ soit la borne supérieure de A dans E, il faut et il suffit que :

1. $\forall a \in A,\ a \leqslant b$ *(i.e. b est un majorant de A) ;*
2. $\forall c \in E,\ c < b \Longrightarrow (\exists a \in A,\ a > c)$ *(i.e. b est le plus petit des majorants)*

Énoncé similaire pour la borne inférieure.

Dans $\mathbb{R}$, on exprime souvent la deuxième condition sous la forme suivante :

$$\forall \varepsilon > 0,\ \exists x \in A,\ b - \varepsilon < x \leqslant b.$$

Exemples 3.3.36 (bornes inférieures, supérieures)

1. Dans $\mathbb{N}^*$ muni de la divisibilité, $\inf(a,b) = \text{pgcd}(a,b)$, et $\sup(a,b) = \text{ppcm}(a,b)$.
2. Dans $\mathcal{P}(E)$, muni de l'inclusion, $\inf(A,B) = A \cap B$, $\sup(A,B) = A \cup B$
3. Dans $\mathbb{N}^2$ muni de l'ordre produit, $\inf((x_1,y_1),(x_2,y_2)) = (\min(x_1,x_2), \min(y_1,y_2))$

Proposition 3.3.37

Soit $(E, \leqslant)$, et $A \subset E$. A admet un maximum M (plus grand élément) si et seulement si A admet une borne supérieure b et si $b \in A$. Dans ce cas $M = b$. Énoncé similaire pour le minimum.

Étant donné deux ensembles munis d'une relation d'ordre, il est possible de définir une notion de fonction croissante (ou décroissante)

Définition 3.3.38 (Fonction croissante ou isotone)

Soit E et F deux ensembles, munis chacun d'une relation d'ordre $\leqslant_E$ et $\leqslant_F$ respectivement. Une fonction $f : E \to F$ est dite *croissante* ou *isotone* si

$$\forall (x,y) \in E^2, \quad x \leqslant_E y \Longrightarrow f(x) \leqslant_F f(y).$$

Une fonction décroissante est aussi appelée fonction antitone.

Avertissement 3.3.39

Prenez garde au fait que les propriétés usuelles des fonctions réelles croissantes ne sont pas toutes vraies dans une situation plus générale. Par exemple, étant donné E un ensemble fini, l'application de $\mathcal{P}(E)$ dans $\mathbb{N}$ définie par $X \mapsto \text{Card}(X)$ est strictement croissante mais non injective !

Pour terminer ce chapitre, nous donnons un résultat équivalent à l'axiome du choix (donc tout aussi indécidable), qui est la version sous laquelle l'axiome du choix est le plus fréquemment utilisé. Pour cela, nous commençons par donner une définition :

Définition 3.3.40 (ensemble inductif, HP)

Soit $(E, \leqslant)$ un ensemble ordonné. On dit que E est un ensemble inductif si pour tout sous-ensemble $F \subset E$ *totalement ordonné*, F admet un majorant.

Exemples 3.3.41

- Tout ensemble ordonné fini est inductif.
- L'ensemble $(\mathbb{Z}, \leqslant)$ n'est pas inductif.
- $(\mathcal{P}(E), \subset)$ est inductif.

Théorème 3.3.42 (lemme de Zorn, ou de Kuratowski-Zorn, HP)

Tout ensemble inductif admet un élément maximal.

Le lemme de Zorn est équivalent à l'axiome du choix.

4 Sommes

« La totalité est plus que la somme des parties »

(Aristote)

« $1+2+3+4+\cdots=-\dfrac{1}{12}$ »

(Leonhard Euler)

Introduction

Le but de ce chapitre introductif est de systématiser l'usage du signe $\sum$ pour désigner une somme d'éléments. Dans la mesure du possible, l'utilisation de cette notation est préférable à celle utilisant des petits points, bien moins rigoureuse.
Nous supposons connues les notions et notations suivantes :

- la compréhension intuitive des ensembles de nombres usuels, et les notations standard :
  - $\mathbb{N}$: ensemble des entiers naturels (*i.e.* positifs ou nuls) ;
  - $\mathbb{Z}$: ensemble des entiers relatifs (*i.e.* de signe quelconque) ;
  - $\mathbb{Q}$: ensemble des nombres rationnels (*i.e.* pouvant s'écrire sous forme d'une fraction) ;
  - $\mathbb{D}$: ensemble des nombres décimaux (*i.e.* admettant une écriture finie en base décimale) ;
  - $\mathbb{R}$: ensemble de tous les nombres réels ;
  - $\mathbb{C}$: ensemble de tous les nombres complexes ;
- les sous-ensembles particuliers suivants de $\mathbb{R}$ et $\mathbb{C}$:
  - $\mathbb{R}_+$: ensemble des réels positifs ou nuls ;
  - $\mathbb{R}_-$: ensemble des réels négatifs ou nuls ;
  - $\mathbb{R}^*$: ensemble des réels non nuls ;
  - $\mathbb{R}_+^*$: ensemble des réels positifs non nuls ;
  - $\mathbb{R}_-^*$: ensemble des réels négatifs non nuls ;
  - $\mathbb{C}^*$: ensemble des nombres complexes non nuls ;
  - $\mathbb{N}^*$: ensemble des entiers naturels non nuls ;
  - $\mathbb{Z}_-$: ensemble des entiers négatifs ou nuls ;
  - $\mathbb{Z}^*$: ensemble des entiers non nuls ;
  - de même que pour $\mathbb{R}$, on peut définir $\mathbb{Q}_+$, $\mathbb{Q}_-$, $\mathbb{Q}^*$, $\mathbb{Q}_+^*$, $\mathbb{Q}_-^*$, $\mathbb{D}_+$, $\mathbb{D}_-$, $\mathbb{D}^*$, $\mathbb{D}_+^*$ ou $\mathbb{D}_-^*$; on rencontre aussi parfois $\mathbb{Z}_+$ pour désigner $\mathbb{N}$, et $\mathbb{Z}_-^*$;
- les intervalles de réels :
  - pour $a \leqslant b$, la notation $[a,b]$ désigne l'intervalle fermé délimité par les réels a et b, c'est-à-dire l'ensemble des réels x tels que $a \leqslant x \leqslant b$;
  - pour $a < b$, la notation $]a,b]$ désigne l'ensemble des réels x tels que $a < x \leqslant b$. On définit de manière similaire $[a,b[$ et $]a,b[$;

  - $+\infty$ désigne l'infini positif, $-\infty$ désigne l'infini négatif ;
  - les intervalles de $\mathbb{R}$ peuvent être délimités par un infini, à condition d'avoir une borne ouverte : $[a, +\infty[$ par exemple désigne l'intervalle des réels x tels que $a \leqslant x$;
- les intervalles d'entiers : si a et b sont deux entiers tels que $a \leqslant b$, $[\![a, b]\!]$ désigne l'intervalle d'entiers délimité par a et b, c'est-à-dire :

$$[\![a, b]\!] = \{a, a+1, \ldots, b-1, b\} = \{n \in \mathbb{Z} \,|, a \leqslant n \leqslant b\};$$

  On trouve parfois $[\![a, +\infty[\![$, lorsque l'intervalle n'est pas majoré ;
- la notion de fonction bijective d'un ensemble fini dans un autre ;

Note Historique 4.0.43

Si on comprend assez bien les notations $\mathbb{N}$, $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{D}$, il n'en est pas de même de $\mathbb{Z}$ et $\mathbb{Q}$. Voici un bref apreçu historique de ces notations :

- $\mathbb{N}$: notation introduite par Peano (fin 19^{e}, de l'italien *Naturale*)
- $\mathbb{Z}$: notation introduite par Dedekind (fin 19^{e} siècle, de l'allemand *Zahlen*)
- $\mathbb{D}$: notation introduite par les programmes pédagogiques français (1970)
- $\mathbb{Q}$: notation introduite par Peano (de l'italien *Quotiente*)
- $\mathbb{R}$: notation introduite par Dedekind (de l'allemand *Real*)
- $\mathbb{C}$: notation introduite par Gauss en 1831.

I Manipulation des signes $\sum$ et $\prod$

Nous rappelons qu'une famille d'éléments de E indexée sur un ensemble I est une fonction $x : I \longrightarrow E$, généralement donnée en notation indicielle (on note x_i au lieu de $x(i)$). L'objet « famille » dans sa globalité est noté $(x_i)_{i\in I}$, ou parfois (x_i) lorsque le contexte est clair, en opposition à x_i, désignant uniquement le terme d'indice i.
Dans cette section, nous considérerons uniquement le cas de familles finies, c'est-à-dire de familles indexées sur un ensemble I fini.

I.1 Définition des notations

Notation 4.1.1 (signes $\sum$ et $\prod$: définition générale)

Soit I un ensemble fini et $(a_i)_{i\in I}$ une famille de nombres réels ou complexes.

- L'expression $\displaystyle\sum_{i\in I} a_i$ désigne la somme de tous les éléments a_i, pour tout $i \in I$.
- L'expression $\displaystyle\prod_{i\in I} a_i$ désigne le produit de tous les éléments a_i, pour tout $i \in I$.

Remarques 4.1.2

1. La lettre i utilisée pour énumérer les éléments de I résulte évidemment d'un choix arbitraire : on peut remplacer cette lettre par toute autre lettre n'ayant pas de signification externe à la somme. On dit que i est une *variable muette*. Ainsi :

$$\sum_{i\in I} a_i = \sum_{j\in I} a_j = \sum_{\beta\in I} a_\beta$$

   En revanche, $\displaystyle\sum_{n\in[\![1,n]\!]} a_n$ n'a pas de sens.
2. Pour une définition rigoureuse et universelle, il faut se donner un ordre de sommation. Dans $\mathbb{R}$ ou $\mathbb{C}$, ou les autres ensembles que l'on recontrera, l'addition sera toujours commutative, et l'ordre de sommation importe peu. C'est moins vrai pour les produits (voir le produit des matrices par exemple)

3. La donnée d'un ordre de sommation est la donnée d'une numérotation des éléments de I, possible parce que I est fini. Ainsi, si I est de cardinal n, on peut trouver une numérotation

$$I = \{i_1, \dots, i_n\}.$$

Une telle numérotation est équivalente à la donnée d'une bijection $\varphi : [\![1, n]\!] \longrightarrow I$: il suffit de poser $i_k = \varphi(k)$. Il est important de bien conserver à l'esprit que toute bijection φ de $[\![1, n]\!] \longrightarrow I$ définit la même somme.

Notation 4.1.3 (signes $\sum$ et $\prod$ sur des ensembles d'entiers consécutifs)

Dans le cas particulier où $I = [\![n, p]\!]$, donc où I est un ensemble d'entiers consécutifs, on écrit généralement :

- $\sum_{i=n}^{p} a_i$ au lieu de $\sum_{i \in [\![n,p]\!]} a_i$; ainsi, $\sum_{i=n}^{p} a_i = a_n + a_{n+1} + \cdots + a_p$.
- $\prod_{i=n}^{p} a_i$ au lieu de $\prod_{i \in [\![n,p]\!]} a_i$; ainsi, $\prod_{i=n}^{p} a_i = a_n \times a_{n+1} \times \cdots \times a_p$.

On lit respectivement « somme pour i allant de n à p des a_i » et « produit pour i allant de n à p des a_i ».

Lorsque $m = n$, la somme (ou le produit) est réduite à un seul terme :

$$\sum_{i=n}^{n} a_i = a_n.$$

Convention 4.1.4 (somme vide, produit vide)

Lorsque $I = \varnothing$, on pose par convention :

$$\sum_{i \in \varnothing} a_i = 0 \qquad \text{et} \qquad \prod_{i \in \varnothing} a_i = 1.$$

Ainsi, si $p < n$, $[\![n, p]\!]$ est vide, donc $\sum_{i=n}^{p} a_i = 0$. Par exemple, $\sum_{i=2}^{1} i^2 = 0$.

Remarque 4.1.5

On notera qu'en général, une somme n'est pas forcément prise sur un ensemble d'entiers successifs, ni même sur un ensemble d'entiers. La seule condition est que **l'ensemble des indices soit fini** (on étudiera le cas où l'ensemble des indices est $\mathbb{N}$ dans le chapitre sur les séries).

Note Historique 4.1.6

Le signe $\sum$ a été introduit par le mathématicien suisse Leonhard Euler en 1755, le symbole $\prod$ date de Gauss, mais on en trouve trace chez Descartes. Mais leur usage ne s'est pas répandu immédiatement, et de nombreux mathématiciens ont continué à utiliser des points de suspension (par exemple Abel au début du 19^{e} siècle)

Exemples 4.1.7

1. $\sum_{k=1}^{4} k(k-1) = 1(1-1) + 2(2-1) + 3(3-1) + 4(4-1) = 2 + 6 + 12 = 20.$
2. $\sum_{i \in \{2,3,5\}} i^2 = 2^2 + 3^2 + 5^2 = 4 + 9 + 25 = 38.$

3. si $E = \{(i,j) \in \mathbb{N}^2 \mid i+j=5\} = \{(0,5),(1,4),\dots,(5,0)\}$, alors
$$\sum_{(i,j)\in E} \frac{i}{j+1} = \frac{0}{6}+\frac{1}{5}+\frac{2}{4}+\frac{3}{3}+\frac{4}{2}+\frac{5}{1} = \frac{87}{10}.$$
4. $\displaystyle\sum_{i\in E} 1 = 1+\cdots+1 = |E|$ (autant de termes 1 que d'éléments dans E).
5. Soit $E = \{(i,j,k) \in (\mathbb{N}^*)^3 \mid i+j+k=5\}$. Calculer $\displaystyle\sum_{(i,j,k)\in E} \frac{i+k}{j+k}$.

Remarque 4.1.8

À part dans le cas trivial où un des termes du produit est nul, un produit peut toujours se ramener à une somme en appliquant le logarithme à sa valeur absolue (et en comptant les signes). Ainsi, si k est le nombre de termes négatifs dans le produit,
$$\prod_{i\in I} a_i = (-1)^k \exp\left(\sum_{i\in I} \ln(|a_i|)\right).$$
De cette manière, la plupart des règles données pour les sommes peuvent facilement être transcrites au cas des produits.

L'ensemble des indices E peut dépendre d'un paramètre, le plus souvent d'un entier n (parfois d'un couple d'entiers, ou d'un p-uplet). Dans ce cas, le résultat est une expression dépendant de ce paramètre. Par exemple si E dépend de n, le résultat de la somme dépend aussi de n.

Exemples 4.1.9

1. $E = \{1,\cdots,n\}$, $\displaystyle\sum_{i=1}^{n} 1 = |E| = n$.
2. $E = \{n, n+1, \dots, 2n\}$, $\displaystyle\sum_{i=n}^{2n} f(i) = f(n)+\cdots+f(2n)$.
3. $E = \{(i,j) \in \mathbb{N}^2 \mid i+j=n\}$. Que vaut $\displaystyle\sum_{(i,j)\in E} 1$? $\displaystyle\sum_{(i,j)\in E} i$? $\displaystyle\sum_{(i,j)\in E} j-i$?
4. Par définition de la factorielle, pour $n \in \mathbb{N}$, $n! = \displaystyle\prod_{k=1}^{n} k$.
   Avec la convention 4.1.4, il vient : $0! = 1$.

I.2 Règles de manipulation des signes $\sum$ et $\prod$

Nous donnons maintenant un certain nombre de règles élémentaires sur les sommes.

Proposition 4.1.10 (Somme indexée dans une union disjointe)

On suppose que $I = I_1 \sqcup I_2$ est une union disjointe, et I fini. Alors :
$$\sum_{i\in I} a_i = \sum_{i\in I_1} a_i + \sum_{i\in I_2} a_i.$$

Exemples 4.1.11

1. Soit $E = \{1, \dots, n\}$ et $k \in \{1, \dots, n\}$. Alors
$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{k} a_i + \sum_{i=k+1}^{n} a_i$$
Si $k = n$ la deuxième somme est vide, donc nulle.
2. Soit $E = \{0, \dots, 2n-1\}$. En écrivant E sous la forme de l'union de ses éléments pairs et de ses éléments impairs, calculer $\sum_{i=0}^{2n-1} \left\lfloor \frac{i}{2} \right\rfloor$, où $\lfloor x \rfloor$ désigne la partie entière de x.

Remarque 4.1.12

Attention à prendre une union *disjointe*, sinon on somme deux fois chaque élément indexé par un indice de l'intersection. Dans le cas d'une union non disjointe $I = I_1 \cup I_2$, on peut écrire :
$$\sum_{i \in I} a_i = \sum_{i \in I_1} a_i + \sum_{i \in I_2} a_i - \sum_{i \in I_1 \cap I_2} a_i.$$

Plus généralement, on obtient le résultat suivant :

Proposition 4.1.13 (Sommation par groupement de termes)

Soit I un ensemble fini et $(I_1, \dots, I_n)$ une partition de I. Soit $(a_i)_{i \in I}$ une famille. Alors
$$\sum_{i \in I} a_i = \sum_{i \in I_1} a_i + \sum_{i \in I_2} a_i + \cdots + \sum_{i \in I_n} a_i = \sum_{j=1}^{n} \sum_{i \in I_j} a_j.$$

Proposition 4.1.14 (Linéarité du symbole $\sum$)

Soit I un ensemble fini et $(a_i)_{i \in I}$ et $(b_i)_{i \in I}$ deux familles (réelles ou complexes), et λ, μ deux nombres réels ou complexes. Alors :

- $\sum_{i \in I} a_i + \sum_{i \in I} b_i = \sum_{i \in I} (a_i + b_i)$.
- $\lambda \sum_{i \in I} a_i = \sum_{i \in I} \lambda a_i$.
- *En combinant les deux égalités :* $\lambda \sum_{i \in I} a_i + \mu \sum_{i \in I} b_i = \sum_{i \in I} (\lambda a_i + \mu b_i)$.

Cette proposition énonce le fait que $\sum$ est une « forme linéaire sur l'espace vectoriel des familles indexées par un ensemble fini donné I. » (voir chapitre *Espaces vectoriel et Applications linéaires*)

Corollaire 4.1.15 (somme de termes constants)

Soit E un ensemble fini et a un nombre réel ou complexe. Alors :
$$\sum_{i \in E} a = a \cdot \sum_{i \in E} 1 = a \cdot |E|.$$

Exemples 4.1.16

1. $\displaystyle\sum_{k=0}^{n} k(k+1) = \sum_{k=0}^{n} k^2 + \sum_{k=0}^{n} k = \frac{n(n+1)(2n+1)}{6} + \frac{n(n+1)}{2}$.
2. Soit $E = \{(i,j) \mid i+j=n\}$. Calculer $\displaystyle\sum_{(i,j)\in E} j-i$, en séparant la somme en deux.

Remarque 4.1.17

Attention à prendre des sommes indexées sur le *même* ensemble ! Si ce n'est pas le cas, on ne peut regrouper les sommes que sur l'intersection des indices, en laissant chacun dans leur somme les éléments indexés hors de cette intersection :

$$\sum_{i\in I_1} a_i + \sum_{i\in I_2} b_i = \sum_{i\in I_1\cap I_2} (a_i+b_i) + \sum_{i\in I_1\setminus(I_1\cap I_2)} a_i + \sum_{i\in I_1\setminus(I_1\cap I_2)} b_i.$$

Exemple 4.1.18

Soit $E = \{0,\dots,n\}$ et $E' = \{1,\dots,n+1\}$. Alors

$$\sum_{i=0}^{n} a_i + \sum_{i=1}^{n+1} b_i = a_0 + \sum_{i=1}^{n}(a_i+b_i) + b_{n+1}.$$

Les règles similaires pour le produit sont :

Proposition 4.1.19 (règles pour les produits)

Avec des notations cohérentes, on obtient les règles suivantes :

- *Si* $I_1 \cap I_2 = \varnothing$, $\displaystyle\prod_{i\in I_1} a_i \prod_{i\in I_2} a_i = \prod_{i\in I_1\cup I_2} a_i$.
- $\displaystyle\left(\prod_{i\in I} a_i\right)^{\lambda}\left(\prod_{i\in I} b_i\right)^{\mu} = \prod_{i\in I}(a_i^{\lambda} b_i^{\mu})$.
- $\displaystyle\prod_{i\in I} a = a^{|I|}$.

I.3 Changements d'indice

Nous en venons maintenant à une technique importante, qui est celle du changement d'indice. La technique énoncée est la même pour la somme et le produit. Nous nous contentons de la donner dans le cas de la somme.

Théorème 4.1.20 (Changements d'indice)

Soit I et J deux ensembles, et $f : I \to J$ une bijection *de I sur J. Alors, pour toute famille $(b_j)_{j\in J}$,*

$$\sum_{j\in J} b_j = \sum_{i\in I} b_{f(j)}$$

En appliquant ce résultat à la bijection réciproque f^{-1}, on a alors aussi, pour toute famille $(a_i)_{i\in I}$:

$$\sum_{i\in I} a_i = \sum_{j\in J} a_{f^{-1}(i)}$$

Exemple 4.1.21

Soit $I = \{2, 4, 5\}$, $J = \{1, 2, 3\}$ et f définie par $f(2) = 1$, $f(4) = 3$, $f(5) = 2$. Alors

$$\sum_{j\in J} a_{f^{-1}(j)} = a_{f^{-1}(1)} + a_{f^{-1}(2)} + a_{f^{-1}(3)} = a_2 + a_5 + a_4 = \sum_{i\in I} a_i.$$

De même,

$$\sum_{i\in I} b_{f(i)} = b_{f(2)} + b_{f(4)} + b_{f(5)} = b_1 + b_3 + b_2 = \sum_{j\in J} b_j.$$

Le cas le plus fréquent est celui où la bijection est donnée par une translation sur des ensembles d'entiers conscutifs :

Corollaire 4.1.22 (changements d'indices par translation)

Soit n, p et ℓ trois entiers tels que $n \leqslant p$. Soit $(a_i)_{i\in[\![n,m]\!]}$ une famille. Alors :

$$\sum_{i=n}^{p} a_i = \sum_{i=n-\ell}^{m-\ell} a_{i+\ell}.$$

Exemple 4.1.23

Montrer que $\displaystyle\sum_{k=0}^{n} a_k + \sum_{k=0}^{n} b_k = a_0 + \sum_{k=1}^{n}(a_k + b_{k-1}) + b_n$

Voici quelques exemples de changements d'indice moins triviaux :

Exemples 4.1.24

1. Soit $E_{p,n} = \{(i_1, \dots, i_p) \in \mathbb{N}^p \mid i_1 + \cdots + i_p = n\}$ et $E'_{p,n} = \{(i_1, \dots, i_p) \in (\mathbb{N}^*)^p \mid i_1 + \cdots + i_p = n\}$. Montrer que
$$\sum_{(i_1,\dots,i_p)\in E_{p,n}} a_{i_1,\dots,i_p} = \sum_{(j_1,\dots,j_p)\in E'_{p,n+p}} a_{j_1-1,\dots,j_p-1}.$$
2. Démonstration de la formule du multinôme (supposant connue la formule du binôme)

I.4 Sommes télescopiques

Définition 4.1.25 (somme télescopique)

On dit qu'une somme $\displaystyle\sum_{k=0}^{n} a_k$ est téléscopique si pour tout $k \in \{0, \dots, n\}$, on peut écrire de façon simple a_k sous la forme $a_k = b_{k+1} - b_k$.

Les sommes téléscopiques se calculent facilement. La technique utilisée (séparer la somme en deux et faire un changement d'indice sur une des deux sommes) est à retenir : elle s'adapte à des situations plus générales.

Proposition 4.1.26 (calcul des sommes téléscopiques)

Soit $\sum(b_{k+1} - b_k)$ une somme téléscopique. Alors :

$$\sum_{k=0}^{n}(b_{k+1} - b_k) = b_{n+1} - b_0.$$

Exemples 4.1.27

1. Calculer $\sum_{k=0}^{n} k \cdot k!$.
2. Calculer $\sum_{k=1}^{n} \frac{1}{k(k+1)}$.
3. Trouver un polynôme P de degré 2 tel que pour tout $x \in \mathbb{R}$, $P(x+1) - P(x) = x$. En déduire $\sum_{k=n}^{m} k$.
4. Trouver des réels (a, b, c) tels que pour tout $k \in \mathbb{N}^*$,

$$\frac{1}{k(k+1)(k+2)} = \frac{a}{k} + \frac{b}{k+1} + \frac{c}{k+2}$$

En déduire l'expression de $\sum_{k=1}^{n} \frac{1}{k(k+1)(k+2)}$. Le retrouver par un télescopage simple.

On peut adapter ces résultats au cas des produits :

Définition 4.1.28 (produit télescopique)
On dit qu'un produit $\prod_{k=0}^{n} a_k$ est téléscopique si pour tout $k \in \{0, \dots, n\}$, on peut écrire de façon simple a_k sous la forme $a_k = \frac{b_{k+1}}{b_k}$.

Proposition 4.1.29 (calcul des produits téléscopiques)
Soit $\prod \frac{b_{k+1}}{b_k}$ un produit téléscopique. Alors :

$$\prod_{k=0}^{n} \frac{b_{k+1}}{b_k} = \frac{b_{n+1}}{b_0}.$$

I.5 Sommes multiples

Nous étudions maintenant les sommes multiples. Certaines familles peuvent être indexées sur un produit cartésien (ou au moins un sous-ensemble). Soit K un sous-ensemble de $I \times J$, et $(a_{i,j})_{(i,j)\in K}$ une famille doublement indexée (*i.e.* indexée sur un produit cartésien). Le but est d'étudier la somme $\sum_{(i,j)\in K} a_{i,j}$ en se ramenant à des sommes portant sur un seul des deux indices. Pour cela, on introduit la notion de « coupe » de l'ensemble K.

Définition 4.1.30 (coupes d'un sous-ensemble de $I \times J$, voir figure 4.1)
Soit $K \subset I \times J$.

- Soit $i \in I$; la coupe de K suivant i est le sous-ensemble $K_{i,\bullet}$ (éventuellement vide) de J défini par :

$$K_{i,\bullet} = \{j \in J \mid (i,j) \in K\}$$

- Soit $j \in J$; la coupe de K suivant j est le sous-ensemble $K_{\bullet,j}$ (éventuellement vide) de I défini par :

$$K_{\bullet,j} = \{i \in I \mid (i,j) \in K\}$$

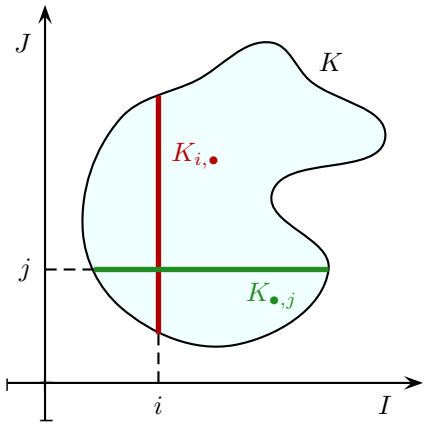


Figure 4.1 – Coupes d'un ensemble

Théorème 4.1.31 (Interversion de signes somme)

Soit $K \subset I \times J$, et $(a_{i,j})_{(i,j)\in K}$ une famille indexée sur K. Alors :

$$\sum_{(i,j)\in K} a_{i,j} = \sum_{i\in I} \sum_{j\in K_{i,\bullet}} a_{i,j} = \sum_{j\in J} \sum_{i\in K_{\bullet,j}} a_{i,j}.$$

Dans la pratique ce résultat est très fréquemment utilisé pour intervertir des signes somme (passer du deuxième terme au troisième terme de cette égalité) lorsque les bornes de l'indice de la somme interne dépendent de l'indice de la somme externe (dans ce cas, on essaie de voir la somme interne comme la somme sur une certaine coupe).

Corollaire 4.1.32 (somme sur un pavé)

Soit $(a_{i,j})_{(i,j)\in[\![1,n]\!]\times[\![1,m]\!]}$. Alors

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_{i,j} = \sum_{j=1}^{m}\sum_{i=1}^{n} a_{i,j}.$$

Ce résultat se généralise à un nombre plus important de sommes, ou à d'autres bornes pour les indices, à condition que ces bornes soient indépendantes des indices des autres sommes.

Corollaire 4.1.33 (produit de deux sommes)

Soit $(a_i)_{i\in I}$ et $(b_j)_{j\in J}$. Alors

$$\sum_{i\in I}\sum_{j\in J} a_i b_j = \sum_{j\in J}\sum_{i\in I} a_i b_j = \left(\sum_{i\in I} a_i\right)\left(\sum_{j\in J} b_j\right).$$

Remarque 4.1.34

Attention, si on effectue le produit de deux sommes indexées sur le même ensemble, et pour lesquels le même indice est utilisé, pensez à d'abord rendre les indices indépendants (les indices étant muets, changez l'un des deux afin d'avoir deux indices différents) :

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{i=1}^{n} b_i\right) = \left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{(i,j)\in[\![1,n]\!]^2} a_i b_j.$$

Avertissement 4.1.35

Attention, en revanche,

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{i=1}^{n} b_i\right) \neq \sum_{i=1}^{n} a_i b_i,$$

Le terme de gauche est la somme sur un carré alors que la somme de droite n'est la somme que sur la diagonale de ce carré !

Avertissement 4.1.36

Attention, en général, il ne suffit pas d'intervertir purement et simplement les signes sommes. Dans la plupart des cas, une telle interversion amène d'ailleurs à une expression qui n'a pas de sens.

Exemple 4.1.37 (somme sur un triangle, à savoir faire !)

Montrer que $\sum_{i=0}^{n}\sum_{j=0}^{i} a_{i,j} = \sum_{j=0}^{n}\sum_{i=j}^{n} a_{i,j}$.

I.6 Rapide introduction à la notion de série

Nous terminons l'étude générale des sommes en donnant une piste, qui sera développée ultérieurement, pour une généralisation au cas d'un nombre infini de termes (indexés par $\mathbb{N}$).

Définition 4.1.38 (série, définition intuitive)

Étant donné une suite $(a_n)_{n\in\mathbb{N}}$, la série de terme général a_n (désignée par la notation synthétique $\sum a_n$) est la suite $(S_n)_{n\in\mathbb{N}}$, où

$$\forall n \in \mathbb{N}, \quad S_n = \sum_{i=0}^{n} a_i.$$

Le terme S_n est appelé n-ième somme partielle de la série de terme général a_n.

Il ne s'agit de rien d'autre qu'un point de vue particulier sur une suite, ou l'on voit une suite $(S_n)_{n\in\mathbb{N}}$ comme somme de ses différences successives (a_n). Assez logiquement, on définit :

Définition 4.1.39 (convergence)

On dit que la série $\sum a_n$ converge si la suite $(S_n)_{n\in\mathbb{N}}$ de ses sommes partielles admet une limite finie S. Dans ce cas, on définit la somme de cette série comme étant égale à S et on écrit :

$$\sum_{n=0}^{+\infty} a_n = S.$$

Une série peut ne pas converger, dans ce cas, on dit qu'elle diverge. On ne peut alors pas donner de sens à la somme $\sum_{n=0}^{+\infty} a_n$.

Le théorème le plus important pour justifier la convergence d'une série est le suivant :

Théorème 4.1.40 (Théorème de comparaison des séries à termes positifs)

Soit $\sum u_n$ et $\sum v_n$ deux séries à termes positifs telles que pour tout $n \in \mathbb{N}$, $u_n \leqslant v_n$ (ou au moins à partir d'un certain rang). Alors :

- *Si* $\sum v_n$ *converge,* $\sum u_n$ *aussi*
- *Si* $\sum u_n$ *diverge,* $\sum v_n$ *aussi.*

Afin de pouvoir nous servir de toute la puissance de ce résultat dès maintenant, nous admettons provisoirement le résultat suivant :

Théorème 4.1.41 (Nature des séries de Riemann)
La série de Riemann $\sum_{n\geqslant 1} \frac{1}{n^\alpha}$ *est convergente si et seulement si* $\alpha > 1$.

Nous verrons par ailleurs dans la suite de ce chapitre que les séries géométriques $\sum a^n$ sont convergentes si et seulement si $|a| < 1$.

On étudiera plus précisément les propriétés de convergence des séries dans un chapitre ultérieur. On verra que l'étude de la convergence d'une série est souvent plus simple que l'étude de la convergence d'une suite, essentiellement du fait de l'existence de résultats de comparaison tels que ci-dessus. En revanche, même connaissant la convergence d'une série, le calcul explicite de sa somme S est souvent beaucoup plus dur, voire impossible.

II Sommes classiques à connaître

De nombreuses sommes se calculent en se ramenant à des sommes connues. Pour cette raison, il est important d'avoir un catalogue de sommes (finies) qu'on sait calculer. Ces sommes sont celles de ce paragraphe, auxquelles s'ajoutent les sommes télescopiques, et certaines sommes obtenues par des techniques d'analyse (dérivation des sommes géométriques par exemple).

II.1 Somme des puissances d'entiers

Proposition 4.2.1 (somme des puissances d'entiers, petits exposants)
Pour tout $n \in \mathbb{N}$,

- $\sum_{k=1}^{n} k^0 = \sum_{k=1}^{n} 1 = n$
- $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.
- $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.
- $\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$.

On donne une interprétation géométrique des cas des exposants 1 et 3 dans la figure 4.2
Notons, de façon générale, pour tout $(n,p) \in (\mathbb{N}^*)^2$,

$$S_n(p) = \sum_{k=1}^{n} k^p.$$

On peut calculer $S_n(p)$ de proche en proche à l'aide de la formule du binôme (rappelée un peu plus loin).

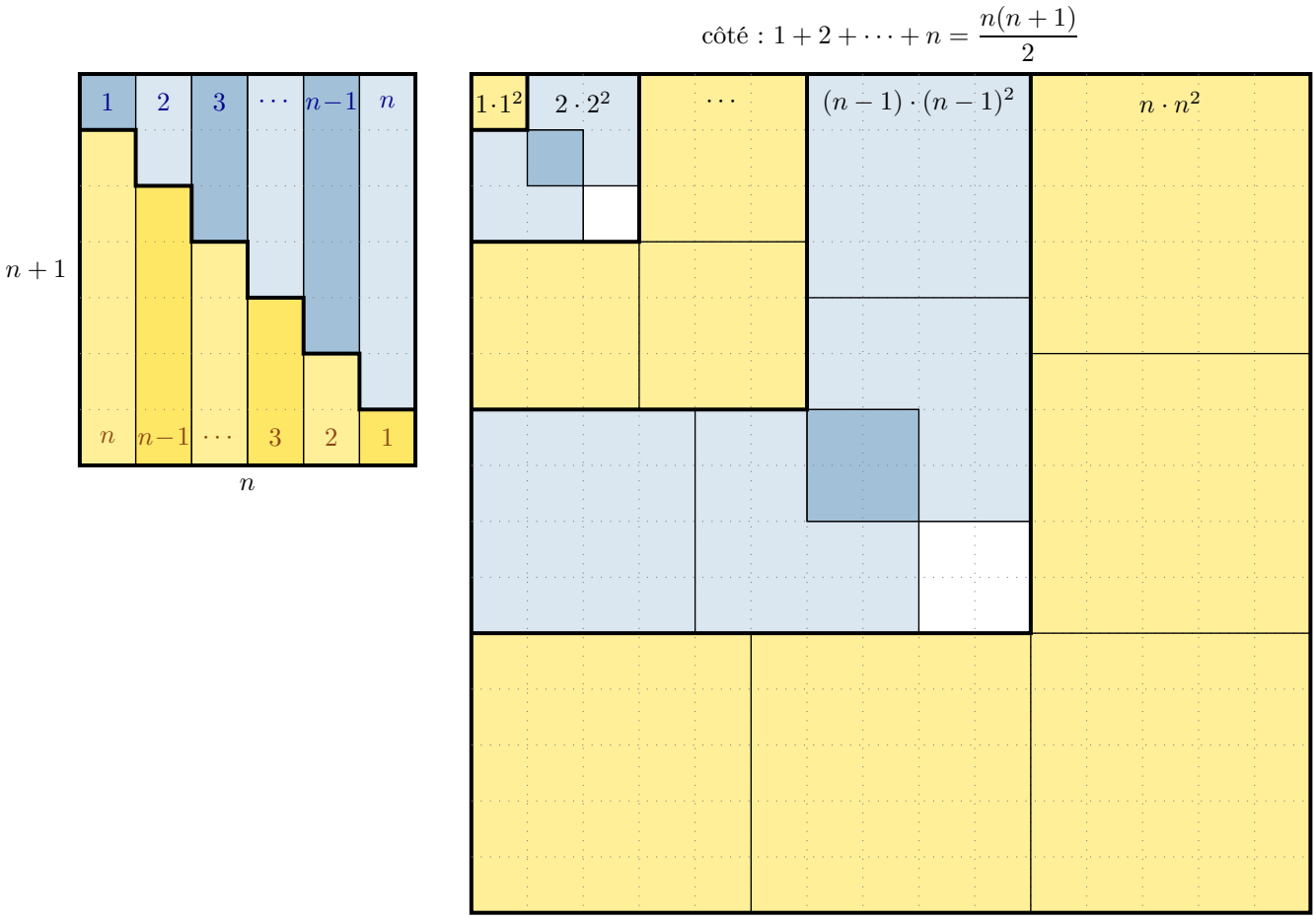


FIGURE 4.2 – Interprétation géométrique de $\sum_{k=1}^{n} k$ et $\sum_{k=1}^{n} k^3$.

Méthode 4.2.2 (Calcul de proche en proche des $S_n(p)$)

Pour calculer $S_n(p)$ en fonction des sommes précédentes, considérer la somme :

$$S=\sum_{k=1}^{n}((1+k)^{p+1}-k^{p+1}).$$

La somme S peut être calculée d'une part comme somme télescopique, d'autre part à l'aide du développement du binôme (ce qui fait partir les termes d'exposant $p+1$). Isoler ensuite les termes d'exposant p.

Remarque 4.2.3

En utilisant les formules précédentes, on obtient sans peine la somme des nombres impairs consécutifs :

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

Cette formule a une interprétation géométrique toute simple, déjà connue des Grecs antiques (Euclide) : elle est donnée en figure 4.3.

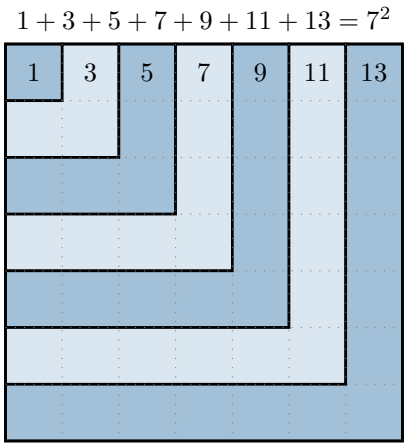


Figure 4.3 – Interprétation géométrique de la somme des entiers impairs

Exemples 4.2.4

1. Calculer $\sum_{k=1}^{n}(k+1)(k+2)$.
2. Calculer $\sum_{k=m}^{n} k^2$ $(m < n)$.

II.2 Sommes géométriques

La deuxième grande famille de sommes à bien connaître est la famille des sommes géométriques.

Proposition 4.2.5 (Sommes géométriques)

Soit $z \in \mathbb{C}$ et $n \in \mathbb{N}$. Alors :

- *si $z = 1$,* $\sum_{k=0}^{n} z^k = n + 1$;
- *si $z \neq 1$,* $\sum_{k=0}^{n} z^k = \dfrac{1 - z^{n+1}}{1 - z}$.

Exemples 4.2.6

1. Calculer $\sum_{k=0}^{4n}(2\,\mathrm{i})^k$.
2. Calculer $\sum_{k=0}^{n} p^{2k}$ en fonction de $p \in \mathbb{R}$ et $n \in \mathbb{N}$.
3. Calculer, pour $n \geqslant 4$, $\sum_{k=6}^{n+2} \mathrm{e}^{-3k}$.

Proposition 4.2.7 (Factorisations de $a^n - b^n$ et $a^n + b^n$)

Soit a et b des nombres complexes et n un entier. Alors :

- $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1}) = (a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k$;

- *En particulier, pour $b = 1$, on obtient :*

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1) = (a-1)\sum_{k=0}^{n-1} a^k;$$

- *si n est impair, alors :*

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 + \cdots - ab^{n-2} + b^{n-1}) = (a+b)\sum_{k=0}^{n-1}(-1)^k a^{n-1-k}b^k;$$

Exemple 4.2.8

1. Que retrouve-t-on pour $n = 2$?
2. Quelles sont les racines dans $\mathbb{C}$ du polynôme $1 + X + X^2$? du polynôme $1 + X + X^2 + X^3$?
3. Donner une factorisation dans $\mathbb{C}$ de $a^{4k+2} + b^{4k+2}$ ($k \in \mathbb{N}$). En donner une factorisation dans $\mathbb{R}$ (par $(a^2 + b^2)$)

Méthode 4.2.9 (Dérivées de sommes géométriques réelles)

1. Pour calculer $\sum_{k=0}^{n}(k+1)x^k$, dériver l'expression donnant $\sum_{k=0}^{n} x^{k+1}$ (pour x réel)
2. En théorie, cela permet de calculer toutes les sommes $\sum_{k=0}^{n}(k+1)(k+2)\cdots(k+\ell)x^k$, par dérivations successives de sommes géométriques. En pratique, les calculs deviennent vite assez pénibles lorsque ℓ grandit.
3. En admettant que tout polynôme de degré d peut s'écrire comme combinaison linéaire des polynômes 1, $X+1$, $(X+1)(X+2), \ldots, (X+1)(X+2)\ldots(X+d)$, cela fournit une méthode théorique de calcul de toutes les sommes $\sum_{k=0}^{n} P(k)x^k$, pour un réel x quelconque, et un polynôme P (le cas $x = 1$ résulte du paragraphe précédent, puisqu'on a dans ce cas des sommes de puissances d'entiers).

Exemple 4.2.10

1. Calculer $\sum_{k=0}^{n} \frac{k}{3^k}$.
2. Calculer $\sum_{k=0}^{n} k^2 x^k$, pour tout $x \in \mathbb{R}$.

III Coefficients binomiaux, formule du binôme

Définition 4.3.1 (Coefficient binomial)
Soit n et p deux entiers naturels. Le coefficient binomial $\binom{n}{p}$ est défini comme étant le nombre de sous-ensembles de cardinal p de $[\![1, n]\!]$.

Convention 4.3.2 (Valeurs du coefficient binomial)

- Si n ou p est strictement négatif, on pose par convention $\binom{n}{p} = 0$.
- De la définition il résulte également que si $p > n$, $\binom{n}{p} = 0$ et que $\binom{0}{0} = 1$.

Proposition 4.3.3 (diverses interprétations du coefficient binomial)

Le coefficient binomial $\binom{n}{p}$ *est :*

(i) le nombre de sous-ensembles de cardinal p de n'importe quel ensemble de cardinal n ;

(ii) le nombre de choix de p éléments non ordonnés parmi n éléments deux à deux discernables ;

(iii) le nombre de mots de longueur n formés avec les lettres a et b, et possédant exactement p lettres a ;

(iv) le nombre de chemins à pas unitaires vers la droite ou vers le haut, rejoignant le point $(0,0)$ et le point $(p, n-p)$;

(v) le nombre de chemins ayant exactement p succès de l'arbre d'un schéma de Bernoulli d'ordre n.

Proposition 4.3.4 (Valeurs particulières à retenir)

Pour tout $n > 0$:

$$\binom{n}{0} = 1, \qquad \binom{n}{1} = n, \qquad \binom{n}{n-1} = n, \qquad \binom{n}{n} = 1.$$

Des principes élémentaires de combinatoire amènent facilement :

Théorème 4.3.5 (Formule du coefficient binomial)

Pour tout $(n,p) \in \mathbb{N}^2$ tel que $p \leqslant n$,

$$\binom{n}{p} = \frac{n!}{p!(n-p)!}$$

Voici deux propriétés utiles qui découlent de façon immédiate de la formule du coefficient binomial, mais qui peuvent être démontrée aussi par la combinatoire, en revenant à la définition par les sous-ensembles :

Proposition 4.3.6 (propriétés du coefficient binomial)

Soit $(n,k) \in \mathbb{Z}^2$. On a :

- $\binom{n}{k} = \binom{n}{n-k}$ *(symétrie du coefficient binomial)*
- $k\binom{n}{k} = n\binom{n-1}{k-1}$

La formule suivante, source de la construction du fameux triangle de Pascal, se démontre aisément avec l'expression factorielle des coefficients binomiaux, mais peut elle aussi être démontrée par un argument combinatoire.

Proposition 4.3.7 (Formule de Pascal)

Pour tout $(n,p) \in \mathbb{Z}^2 \setminus \{(-1,-1)\}$, $\binom{n}{p} + \binom{n}{p+1} = \binom{n+1}{p+1}$.

Grâce à cette formule, on peut contruire les coefficients binomiaux par ligne (une ligne représentant une valeur de n donnée), de proche en proche. Cette construction est particulièrement utile lorsqu'on recherche des coefficients binomiaux pour une valeur raisonnablement petite de n (disons $n \leqslant 10$), par exemple en vue d'utiliser la formule du binôme de Newton (présentée un peu plus loin). La construction de ce triangle est expliquée dans la figure 4.4.

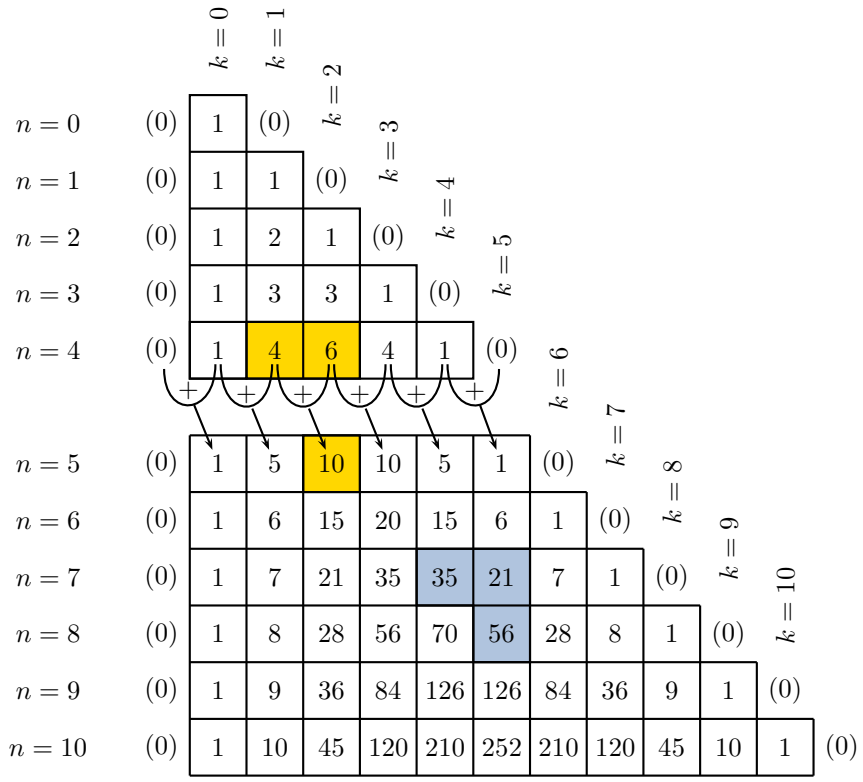


FIGURE 4.4 – Triangle de Pascal pour le calcul de $\binom{n}{p}$

Note Historique 4.3.8

Le triangle des coefficients binomiaux, que nous appelons communément « triangle de Pascal » était en fait connu depuis bien longtemps déjà lorsque Blaise Pascal s'y intéressa : on y trouve mention déjà chez Halayudha, mathématicien indien du 10e siècle, ainsi qu'en Chine au 13e siècle. La contribution de Pascal a essentiellement été de démontrer en 1654 un grand nombre de propriétés de ce triangle, jusque-là admises. C'est d'ailleurs à cette occasion qu'il a mis au point le principe de la démonstration par récurrence !

Théorème 4.3.9 (Formule du binôme de Newton)

Soit a et b deux nombres complexes, et $n \in \mathbb{N}$. Alors

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

Cette formule reste vraie dans un anneau quelconque, (par exemple pour des matrices), mais à condition que a et b commutent c'est-à-dire $ab = ba$.

Note Historique 4.3.10

La formule du binôme était elle aussi déjà connue depuis longtemps, notamment en Inde et en Chine, en relation

avec le triangle de Pascal. L'apport de Newton est bien réel et important, mais ne concerne pas les exposants entiers naturels. Isaac Newton a en fait généralisé cette formule pour tout exposant réel, sous forme d'une somme infinie. Pour les entiers négatifs, c'est ce qu'on appelle la « formule du binôme négatif ».

La formule du binôme est fondamentale, car elle est à la base d'une propriété importante des suites géométriques, constamment utilisée en analyse :

Corollaire 4.3.11 (limite des suites géométriques)

Soit a un nombre réel.

(i) Si $a > 1$, alors $\lim_{n\to+\infty} a^n = +\infty$;

(ii) si $a \in]-1, 1[$, alors $\lim_{n\to+\infty} a^n = 0$;

(iii) si $a < -1$, alors $(a^n)_{n\in\mathbb{N}^*}$ n'admet pas de limite.

Corollaire 4.3.12 (Convergence des séries géométriques)

La série géométrique $\sum z^n$ $(z \in \mathbb{C})$ converge si et seulement si $|z| < 1$. Dans ce cas, on a :

$$\sum_{n=0}^{+\infty} z^n = \frac{1}{1-z}.$$

5 Les corps $\mathbb{Q}$ et $\mathbb{R}$

Pour moi, les mathématiques, c'est la conquête du continu par le discret.

(René Thom)

Introduction

Nous étudions dans ce chapitre les ensembles de nombres que nous utilisons usuellement : l'ensemble des nombres rationnels, puis l'ensemble des nombres réels. Nous étudierons dans le chapitre suivant l'ensemble des nombres complexes.
Ces ensembles possèdent une structure particulière, que nous appelons *structure de corps*, et que nous aurons l'occasion d'étudier plus généralement dans un chapitre ultérieur. Nous nous contentons pour l'instant d'en donner une définition approximative :

Définition 5.0.1 (corps, version approximative)
Un corps est un ensemble muni de deux types d'opérations (appelées *lois*), généralement notées $+$ et $\times$, tel que :
- $+$ et $\times$ vérifient un certain nombre de propriétés d'associativité, de commutativité et de distributivité,
- il existe un élément 0, neutre pour $+$ (*i.e.* $0 + x = x$ pour tout x),
- il existe un élément 1, neutre pour $\times$ (*i.e.* $1 \times x = x$ pour tout x),
- tout élément x admet un opposé y pour $+$, tel que $x + y = 0$,
- tout élément $x \neq 0$ admet un inverse pour $\times$.

Ce dernier point a pour conséquence que $\mathbb{Z}$ (par exemple) n'est pas un corps (on parle dans ce cas d'anneau)

I De $\mathbb{Q}$ à $\mathbb{R}$

I.1 Construction de $\mathbb{Q}$

Nous avons déjà vu dans un chapitre antérieur une façon de construire $\mathbb{Q}$ comme ensemble des quotients $\frac{a}{b}$ de deux entiers relatifs. Plus précisément, pour définir correctement les cas d'égalités entre fraction, il convient de définir $\mathbb{Q}$ comme l'ensemble des classes d'équivalence de $\mathbb{Z} \times \mathbb{Z}^*$ muni de la relation $\equiv_{\mathbb{Q}}$ définie par :

$$(a, b) \equiv (c, d) \qquad \Longleftrightarrow \qquad ad - bc = 0.$$

En d'autres termes, $\mathbb{Q}$ est l'espace quotient de $\mathbb{Z} \times \mathbb{Z}^*$ par la relation $\equiv_{\mathbb{Q}}$.

Quotienter par cette relation d'équivalence donne les conditions d'égalités de deux fractions $\frac{a}{b}$ et $\frac{c}{d}$. C'est ce quotient qui permet de gérer de façon rigoureuse la non unicité de l'écriture d'un rationnel sous forme d'un couple (numérateur, dénominateur).

I.2 De l'existence de nombres non rationnels

Note Historique 5.1.1

Les premiers à avoir compris l'existence de nombres non rationnels étaient sans doute les Pythagoriciens, par l'étude de la diagonale du carré de coté 1 (voir ci-dessous). Les nombres étant défini comme des rapports, ils parlent de longueurs *incommensurables* (elles ne peuvent pas se mesurer à l'aide d'une unité commune)

Définition 5.1.2 (Nombres incommensurables)

Soit $(x, y) \in (\mathbb{R}^*)^2$. On dit que x et y sont incommensurables si $\frac{x}{y}$ est irrationnel.

Exemple 5.1.3 (existence de nombres irrationnels)

Le réel $\sqrt{2}$ est irrationnel. En d'autres termes, le côté et la diagonale d'un carré sont incommensurables.

On pourrait montrer plus généralement que $\sqrt{n}$ est irrationnel dès que l'entier n n'est pas un carré parfait.

I.3 L'ensemble $\mathbb{R}$

L'ensemble $\mathbb{R}$ est alors obtenu en « bouchant les trous » laissés par les éléments de $\mathbb{Q}$, un peu comme on coulerait du mortier pour celler un ensemble de petites pierres, ou comme le bitume autour des gravillons. La façon de percevoir les trous de $\mathbb{Q}$ est d'étudier l'exemple suivant :

Exemple 5.1.4 (un sous-ensemble borné de $\mathbb{Q}$ n'admettant pas de borne supérieure)

Soit $E = \{x \in \mathbb{Q}_+ \mid x^2 \leqslant 2.\}$. Alors E est borné, et n'admet pas dans $\mathbb{Q}$ de borne supérieure.

Si on se rapproche de plus en plus du bord de cet intervalle, on tombe dans un trou... il n'y a rien au bord !
C'est ce vide que l'on comble en construisant $\mathbb{R}$ comme l'ensemble $\mathbb{Q}$, complété des bornes supérieures de tous les sous-ensembles non vides bornés. Là encore, on a besoin de le faire sous forme d'un quotient pour une certaine relation d'équivalence, donnant une condition pour que deux bornes supérieures soit égales. Cette construction, qui n'est pas au programme, se résume par la propriété fondamentale de $\mathbb{R}$, *fondamentale* dans le sens où elle est intrinsèque à la définition de $\mathbb{R}$. Cette propriété ne pouvant être justifiée que par la manière rigoureuse de construire $\mathbb{R}$, nous l'admettrons.

Théorème 5.1.5 (propriété fondamentale de $\mathbb{R}$)

Soit E un sous-ensemble non vide et majoré de $\mathbb{R}$. Alors E admet une borne supérieure dans $\mathbb{R}$.

Évidemment, on en a une version équivalente pour la borne inférieure :

Théorème 5.1.6 (propriété fondamentale de $\mathbb{R}$, exprimée avec la borne inférieure)

Soit E un sous-ensemble non vide et minorée de $\mathbb{R}$. Alors E admet une borne inférieure dans $\mathbb{R}$.

Note Historique 5.1.7

La propriété de la borne supérieure a été énoncée (et démontrée, mais avec une erreur due à une absence de définition correcte de $\mathbb{R}$) en 1817 par le mathématicien tchèque d'origine italienne Bernhard Bolzano, en vue de donner une démonstration rigoureuse du théorème des valeurs intermédiaires (aussi appelé théorème de Bolzano), jusque-là démontré par un dessin (Cauchy, auteur de ce théorème se contente d'un dessin comme preuve)

I.4 Division euclidienne dans $\mathbb{R}$

Le principe de la division euclidienne dans $\mathbb{R}$ repose sur le résultat suivant, bien utile par ailleurs, notamment pour prouver des propriétés de densité :

Proposition 5.1.8 (Propriété d'Archimède)

Soit x et y deux réels strictement positifs. Il existe un entier $n \in \mathbb{N}$ tel que $x < ny$.

Corollaire 5.1.9

Dans les mêmes hypothèses, il existe un unique entier $n \in \mathbb{N}$ tel que $(n-1)y \leqslant x < ny$.

Théorème 5.1.10 (division euclidienne, Euclide)

Soit x et y deux réels strictement positifs. Il existe un unique entier n et un unique réel $r \in [0, y[$ tels que $x = ny + r$.

C'est un résultat très concret : si un menuisier doit couper des planches de longueur donnée y dans une grande planche de longueur x, n est le nombre de planches de la bonne longueur qu'il peut obtenir, et r est la longueur du bout inutile qu'il lui reste à la fin.
On peut ensuite étendre sans problème ce résultat à des réels de signe quelconque, en autorisant $n \in \mathbb{Z}$ et en imposant $r \in [0, |y|[$. On procède par disjonction de cas, en étudiant les différentes possibilités de signe.

Note Historique 5.1.11

Archimède est légèrement postérieur à Euclide (3^{e} siècle avant J.-C.). La propriété d'Archimède figure en fait déjà dans les *Éléments* d'Euclide. Archimède utilise largement cette propriété, sans pour autant prétendre à sa paternité.

I.5 Caractérisation de l'incommensurabilité par la division euclidienne

Note Historique 5.1.12

Quelques siècles après Pythagore, Euclide a énoncé un critère, lié à la division euclidienne, caractérisant l'incommensurabilité de deux grandeurs. Cette caractérisation donne par exemple une démonstration géométrique quasi-évidente de l'incommensurabilité du côté et de la diagonale d'un pentagone.

Proposition 5.1.13 (caractérisation de l'incommensurabilité, Euclide, HP)

« Deux grandeurs inégales étant proposées, et si la plus petite étant toujours retranchée de la plus grande, le reste ne mesure jamais le reste précédent, ces grandeurs seront incommensurables. »

Ainsi, en répétant des divisions euclidiennes (en divisant à chaque nouvelle étape l'ancien diviseur par le reste obtenu), le processus ne s'arrête jamais, dans le sens où on n'obtiendra jamais de reste nul, contrairement à ce qu'il se passe lorsqu'on applique ce procédé à deux entiers (vous aurez peut-être reconnu l'algorithme d'Euclide pour le calcul du pgcd).
La démonstration est facile par la contraposée, en utilisant le principe de la descente infinie de Fermat.
Nous donnons la figure 5.1 prouvant géométriquement l'incommensurabilité du côté et de la diagonale d'un pentagone, en utilisant cette propriété. Dans cette figure, le côté du pentagone moyen est le reste de la division de la diagonale et du côté du grand, et sa diagonale est le côté du grand. On se retrouve donc dans la même configuration que la configuration initiale, à changement d'échelle près. Le caractère fractal de cette configuration montre que le processus ne s'arrêtera pas.

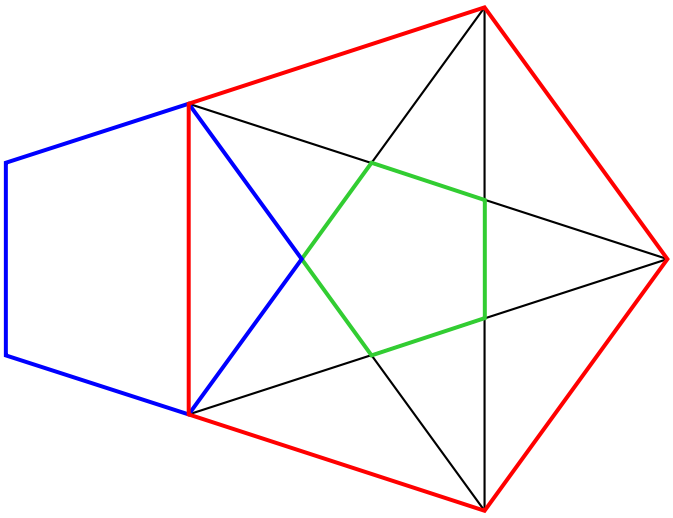


FIGURE 5.1 – Incommensurabilité du côté et de la diagonale du pentagone

I.6 Densité de $\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$ dans $\mathbb{R}$

On peut alors se demander s'il y a beaucoup de nombres irrationnels, et comment ils se répartissent entre les nombres rationnels pour former $\mathbb{R}$. Un élément de réponse est apporté par la propriété de densité, affirmant qu'il y a des rationnels et des irrationnels un peu partout dans $\mathbb{R}$: il n'existe pas dans $\mathbb{R}$ d'intervalle non vide ou non réduit à un singleton, aussi petit soit-il, ne possédant ni rationnel ni irrationnel.
Commençons par définir rigoureusement la propriété de densité :

Définition 5.1.14 (Densité dans $\mathbb{R}$)
Un sous-ensemble E de $\mathbb{R}$ est dense dans $\mathbb{R}$ si pour tout $(x, y) \in \mathbb{R}^2$ tel que $x < y$, il existe $z \in E$ tel que $x < z < y$.

Autrement dit, entre deux éléments quelconques de $\mathbb{R}$ (aussi proches soient-ils), il existe toujours un élément de E : les éléments de E vont s'infiltrer un peu partout.

Théorème 5.1.15 (Densité des rationnels et des irrationnels dans $\mathbb{R}$)
Les ensembles $\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$ sont denses dans $\mathbb{R}$.

Bref, il existe beaucoup de nombres irrationnels. Et en fait beaucoup plus que des rationnels. En effet $\mathbb{Q}$ est dénombrable, et comme $\mathbb{R}$ ne l'est pas, $\mathbb{R} \setminus \mathbb{Q}$ non plus, et, en admettant l'hypothèse du continu, il a donc la puissance du continu (*i.e.* le même cardinal que $\mathbb{R}$).

Nous avons vu précédemment que les nombres irrationnels peuvent eux-même être classés en nombres « peu irrationnels » et nombres « très irrationnels », ou plutôt, en adoptant une terminologie plus correcte, en nombres algébriques (solutions d'une équation polynomiale en $\mathbb{Q}$) et en nombres transcendants (les autres).

Note Historique 5.1.16

On connaît l'existence de nombres irrationnels depuis la Grèce classique. En revanche, la notion de nombres transcendants est beaucoup plus récente :

- Leibniz est le premier, en 1682, à envisager la possibilité de l'existence de nombres transcendants.
- Ce n'est qu'en 1844 que Liouville justifie l'existence de nombres transcendants, en construisant pour l'occasion et en montrant la transcendance du réel $c = \sum_{j=1}^{+\infty} 10^{-j!}$, appelé depuis « constante de Liouville ».
- Hermite prouve en 1873 la transcendance de e. C'est la première fois qu'on montre la transcendance d'un réel qui avait une existence antérieure.
- Lindemann montre en 1882 la transcendance de π, mettant ainsi fin à 3 millénaires de recherches infructueuses pour réaliser la quadrature du cercle.
- Les travaux de Cantor permettent de justifier l'existence de nombres transcendants sans avoir à en contruire, par simple considération des cardinaux.

II Les nombres réels

L'ensemble $\mathbb{R}$ peut être muni d'une relation d'ordre total, obtenu comme prolongement de la relation d'ordre sur $\mathbb{Q}$. La définition rigoureuse de cette relation d'ordre nécessiterait de se plonger dans la définition de $\mathbb{R}$ comme espace quotient. Nous l'admettrons donc.

II.1 Signe et inégalités dans $\mathbb{R}$ et $\mathbb{Q}$

Il est indispensable de bien savoir manipuler les inégalités. En effet, l'analyse peut se définir comme l'étude d'approximations infinitésimales, ces approximations s'obtenant souvent par majorations et minorations. Le caractère infinitésimal se traduit par le fait qu'on s'autorise une marge d'erreur ε, mais que ε peut devenir aussi petit qu'on veut.

Nous rappelons les règles usuelles suivantes :

Proposition 5.2.1 (Sommes et produits d'inégalité)

Soit a, b, c et b des réels.

- *Si $a \leqslant b$ et $c \leqslant d$, alors $a + c \leqslant b + d$, avec égalité si et seulement si $a = b$ et $c = d$.*
- *En particulier, si $a = b$, on obtient : $c \leqslant d \Longrightarrow a + c \leqslant a + d$.*
- *Si $0 < a \leqslant b$ et $0 < c \leqslant d$, alors $0 < ab \leqslant cd$, avec égalité si et seulement si $a = b$ et $c = d$. L'inégalité reste vraie pour des valeurs positives ou nulles, mais on perd alors le cas d'égalité.*
- *Si $a \leqslant b$ alors $-b \leqslant -a$.*
- *Si $a > 0$ et $b \leqslant c$, alors $ab \leqslant ac$, avec égalité si et seulement si $b = c$.*
- *Si $a < 0$ et $b \leqslant c$, alors $ab \geqslant ac$, avec égalité si et seulement si $b = c$.*
- *Pour toutes les autres situations de produit d'inégalité, raisonner d'abord sur la valeur absolue, puis ajouter le signe.*
- *Si $a \leqslant b$ et $c \leqslant d$, alors $a - d \leqslant b - c$*
- *Si $a \leqslant b$ et si a et b sont de même signe et non nuls, alors $\frac{1}{b} \leqslant \frac{1}{a}$.*
- *Pour quotienter deux inégalité, combiner une inversion (point précédent) et une multiplication.*

Définition 5.2.2 (Valeur absolue)

Soit $x \in \mathbb{R}$ La valeur absolue de x, notée $|x|$, est le réel obtenu de x en changeant si besoin son signe de sorte à obtenir une quantité positive :

$$|x| = \begin{cases} x & \text{si } x \geqslant 0 \\ -x & \text{si } x < 0. \end{cases}$$

Définition 5.2.3 (partie positive, partie négative d'un réel)

Soit $x \in \mathbb{R}$.

- On appelle *partie positive* de x, et on note x^+, le réel défini par :

$$x^+ = \max(0, x) = \begin{cases} x & \text{si } x \geqslant 0 \\ 0 & \text{si } x < 0 \end{cases}$$

- On appelle *partie négative* de x, et on note x^-, le réel défini par :

$$x^- = -\min(0, x) = \max(0, -x) = \begin{cases} -x & \text{si } x \leqslant 0 \\ 0 & \text{si } x > 0 \end{cases}$$

Propriétés 5.2.4 (propriétés des parties positives et négatives)

Soit x un réel. Alors :

- $x^+ \geqslant 0$ *et* $x^- \geqslant 0$;
- $x^+ = 0$ *ou* $x^- = 0$;
- $x = x^+ - x^-$;
- *l'égalité précédente est minimale dans le sens suivant : pour tout* $(y, z) \in \mathbb{R}_+$, *si* $x = y - z$ *alors* $y \geqslant x^+$ *et* $z \geqslant x^-$;
- $|x| = x^+ + x^- = \max(0, x) - \min(0, -x)$.
- $(-x)^+ = x^-$ *et* $(-x)^- = x^+$.

Corollaire 5.2.5 (inégalités triangulaires)

Soit x et y deux réels. Alors :

- $(x + y)^+ \leqslant x^+ + y^+$
- $(x + y)^- \leqslant x^- + y^-$
- $|x + y| \leqslant |x| + |y|$

Chacune de ces inégalités est une égalité si et seulement si x et y sont de même signe.

On donne ci-dessous deux inégalités classiques, utiles dans de nombreuses situations.

Théorème 5.2.6 (Inégalité de Cauchy-Schwarz numérique)

Soient $x_1, \ldots, x_n, y_1, \ldots, y_n$ des réels. On a alors :

$$\left| \sum_{i=1}^{n} x_i y_i \right|^2 \leqslant \left(\sum_{i=1}^{n} x_i^2 \right) \left(\sum_{i=1}^{n} y_i^2 \right),$$

avec égalité si et seulement si les vecteurs $(x_1, \ldots, x_n)$ et $(y_1, \ldots, y_n)$ sont colinéaires.

En notant, pour $X = (x_1, \dots, x_n)$ et $Y = (y_1, \dots, y_n)$

$$\langle X, Y \rangle = \sum_{i=1}^{n} x_i y_i$$

le produit scalaire canonique de $\mathbb{R}^n$, et

$$\|X\| = \sqrt{\sum_{i=1}^{n} x_i^2} = \sqrt{\langle X, X \rangle}$$

la norme euclidienne canonique, l'inégalité de Cauchy-Schwarz se réexprime de la sorte :

$$|\langle X, Y \rangle| \leqslant \|X\| \cdot \|Y\|.$$

Remarque 5.2.7

La démonstration n'utilise que le fait que pour tout X, $\langle X, X \rangle \geqslant 0$, avec égalité ssi $X = 0$, et la symétrie su produit scalaire. On définira plus tard dans l'année une notion générale de produit scalaire, vérifiant ces propriétés. Ainsi, la formule de Cauchy-Schwarz restera valable pour tout produit scalaire, la norme associée à ce produit scalaire se définissant comme on l'a fait pour la norme euclidienne à partir du produit scalaire canonique.

Théorème 5.2.8 (Inégalité arithmético-géométrique)

Pour tout $X = (x_1, \dots, x_n) \in (\mathbb{R}_+^*)^n$,

$$\frac{1}{n}(x_1 + \cdots + x_n) \geqslant \sqrt[n]{x_1 \dots x_n}.$$

Cette inégalité dit que la moyenne arithmétique est plus grande que la moyenne géométrique.

II.2 Partie entière, partie décimale

Nous étudions maintenant les représentations des réels dans la vie pratique. Pour cela, nous commençons par séparer la partie entière et la partie décimale, en définissant rigoureusement ces notions.

Proposition/Définition 5.2.9 (Partie entière)

Soit $x \in \mathbb{R}$. Il existe un unique entier relatif, noté $\lfloor x \rfloor$, vérifiant l'une (et donc chacune) des quatre propriétés équivalentes suivantes :

(i) $\lfloor x \rfloor = \max\{n \in \mathbb{Z} \mid n \leqslant x\}$;

(ii) $\lfloor x \rfloor = \min\{n \in \mathbb{Z} \mid n > x\} - 1$;

(iii) $\lfloor x \rfloor$ est l'unique entier tel que $\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1$;

(iv) $\lfloor x \rfloor$ est l'unique entier tel que $x - 1 < \lfloor x \rfloor \leqslant x$.

L'entier $\lfloor x \rfloor$ est appelé *partie entière de* x. On trouve aussi parfois les notations $[x]$ et $E(x)$.

On donne le graphe de la fonction partie entière : $x \mapsto \lfloor x \rfloor$ en figure 5.2

On définit parfois aussi la *partie entière par excès*, notée $\lceil x \rceil$, comme étant la plus petit entier supérieur ou égal à x :

$$\lceil x \rceil = \min\{n \in \mathbb{N} \mid n \geqslant x\}.$$

La partie entière par excès est alors caractérisée par son appartenance à n et l'un ou l'autre des encadrements suivants :

$$x \leqslant \lceil x \rceil < x + 1 \qquad \text{et} \qquad \lceil x \rceil - 1 < x \leqslant \lceil x \rceil.$$

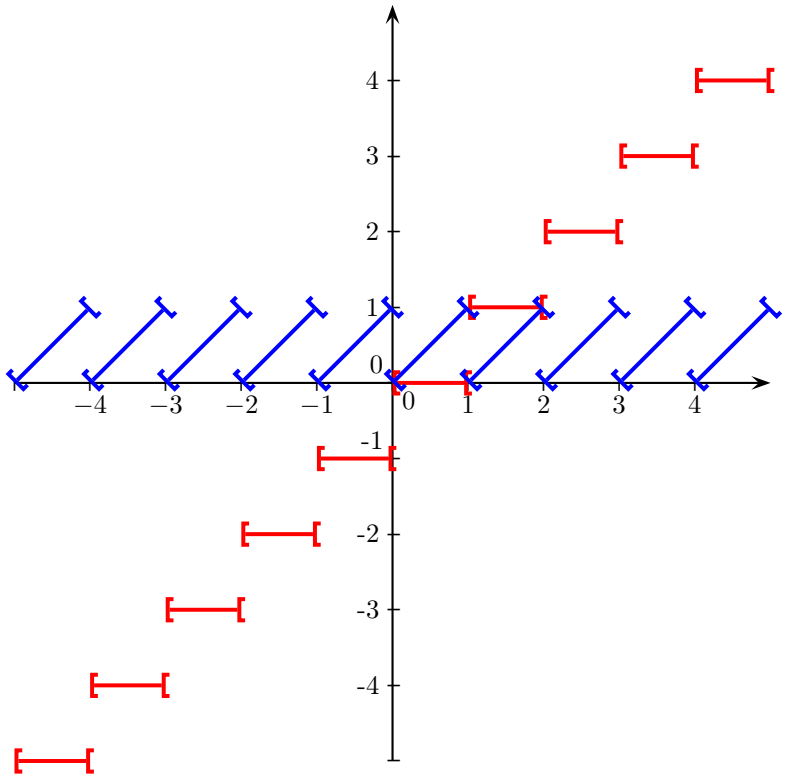


FIGURE 5.2 – Graphe de la partie entière et de la partie décimale

Propriétés 5.2.10 (propriétés de la partie entière)

1. $\forall x, y \in \mathbb{R},\ \lfloor x \rfloor + \lfloor y \rfloor + 1 \geqslant \lfloor x + y \rfloor \geqslant \lfloor x \rfloor + \lfloor y \rfloor$;
2. $\forall x, y \in \mathbb{R}_+,\ \lfloor xy \rfloor \geqslant \lfloor x \rfloor \cdot \lfloor y \rfloor$;
3. $\forall x \in \mathbb{R},\ \forall n \in \mathbb{Z},\ \lfloor x + n \rfloor = \lfloor x \rfloor + n$.

Définition 5.2.11 (Partie décimale, voir graphe 5.2)

La partie décimale de x est le réel $x - \lfloor x \rfloor$. Il s'agit du reste de la division euclidienne de x par 1. Intuitivement, c'est le réel obtenu en ne gardant que les chiffres après la virgule, mais cette interprétation n'est valable que pour les réels positifs.
La partie décimale de x est parfois notée $\{x\}$.

On a alors par définition même : $x = \lfloor x \rfloor + \{x\}$.

II.3 Représentation décimale

Note Historique 5.2.12 (petit aperçu historique de la représentation des nombres)

- Dès l'antiquité, les mathématiciens se rendent compte de la nécessité de rendre la notion de nombre indépendante de toute unité ou toute échelle. Ainsi, les Grecs définissent un nombre comme un rapport entre deux grandeurs de même type, par exemple entre deux longueurs. Ainsi, le théorème de Thalès (premier mathématicien grec important, début du 1er millénaire avant JC) s'exprime sous forme de rapports de longueur.
- Les premières représentations des entiers sont des numérations additives (on ajoute des symboles pour faire des nombres plus gros). Le premier système de numération connu est simplement une succession d'encoches dans un bout de bois ou un os. D'ailleurs, le mot « calcul » dérive du mot « calculus » signifiant caillou (pensez aux calculs rénaux !), car les bergers utilisaient des caillous pour compter leurs moutons.

- Beaucoup plus tard, il reste encore des vestiges de ce système de numération chez les romains, même s'ils disposent d'un système un peu plus sophistiqué (plusieurs symboles pour désigner différentes grandeurs, et notation soustractive).
- La numération de position (qui correspond à une numération dans une base donnée, la position d'un chiffre déterminant le coefficient multiplicatif qui lui sera appliqué) apparaît vraissemblablement à Babylone. Les nombres y sont représentés en base 60 (y compris pour les décimales) ; les « chiffres » de 1 à 60 sont représentés grâce à une numération additive, à l'aide de deux symboles de valeur 1 et 10. Le zéro n'existant pas encore, la position des chiffres n'est pas toujours très claire.
- Il reste d'ailleurs dans notre civilisation des vestiges de cette numération en base 60. Lesquels ?
- Les fractions apparaissent dès le 2e millénaire avant JC, à Babylone, où un calcul très complexe des fractions est mis en place. Imaginez-vous faire des opérations sur des fractions en base 60... Les règles calculatoires (sommes, produits) ne sont pas encore bien établies, et restent intuitive. La plupart des calculs sur les fractions sont faits à l'aide de tables.
- La découverte des nombres irrationnels date probablement de Pythagore (diagonale du carré), mais le secret est gardé. Hippase de Métaponte dévoile aux non initiés l'existence de grandeurs incommensurables (*i.e.* dont le rapport est irrationnel). Selon la légende, il est jeté du haut d'une falaise pour avoir révélé le secret pythagoricien. Quelle est la part de vérité dans cette histoire ? C'est dur à dire. Il est possible aussi que la découverte des irrationnels provienne de propriétés géométriques du pentagone : une construction fractale d'une suite de pentagones permet de montrer géométriquement que l'algorithme d'Euclide pour le rapport entre la diagonale et le côté ne se termine pas, ce qui équivaut à l'incommensurabilité de ces deux grandeurs.
- La numération actuelle est une numération en base 10, et une numération de position (l'un n'entraînant pas l'autre, la notation romaine n'est pas une numération de position, mais est bien une numération en base 10). La numération de position s'est imposée suite à la diffusion des ouvrage de Al Khwarizmi diffusant le système de numération indien. L'intermédiaire arabe de cette diffusion a eu pour conséquence la terminologie de « chiffres arabes », mais il s'agit bien de « chiffres indiens », même si la graphologie de ces chiffres a beaucoup changé. L'importance de l'apport est bien plus le système de numération par position (avec un symbole pour représenter 0) que la graphologie précise des chiffres.

Nous renvoyons au cours d'informatique pour les développements de réels en base b.

Notation 5.2.13 (nombres décimaux)

- Nous notons $\mathbb{D}$ l'ensemble des nombres décimaux, c'est à dire des réels x tels qu'il existe $n \in \mathbb{N}$ tel que $10^n x$ est entier.
- Étant donné $n \in \mathbb{N}$, nous notons $\mathbb{D}_n$ l'ensemble des nombres décimaux tels que $10^n x \in \mathbb{Z}$; Par exemple $\mathbb{D}_0 = \mathbb{Z}$, et $\mathbb{D}_1$ sont les décimaux s'écrivant avec au plus un chiffre après la virgule.

Proposition 5.2.14 (Approximations décimales d'un réel x)

Soit x un réel. Il existe un unique élément y de $\mathbb{D}_n$ tel que

$$y \leqslant x < y + 10^{-n}.$$

- *Le décimal y est appelé valeur approchée décimale à la précision 10^{-n} par défaut*
- *Le décimal $y + 10^{-n}$ est appelé valeur approchée décimale à la précision 10^{-n} par excès.*

De façon assez évidente, y est obtenu en tronquant le développement décimal *propre* de x après la n-ième décimale, et $y + 10^{-n}$ est obtenu en ajoutant 1 à la dernière décimale de y, avec propagation éventuelle de retenue.

Proposition 5.2.15 (Caractérisation des rationnels par leur développement décimal)

Un nombre x est rationnel si et seulement si son développement décimal est périodique à partir d'un certain rang.

II.4 Intervalles

Nous définissons les intervalles par leur propriété de convexité :

Définition 5.2.16 (ensemble convexe, figure 5.3)
Soit E un sous-ensemble de $\mathbb{R}^n$. On dit que E est convexe si et seulement si pour tout couple de points A et B de E, le segment $[AB]$ est entièrement inclus dans E.

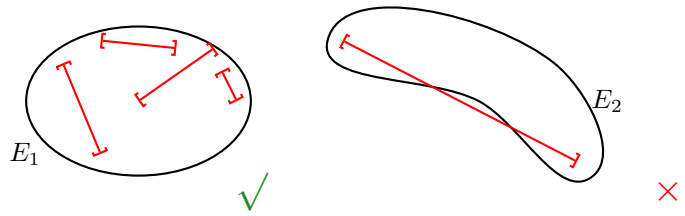


FIGURE 5.3 – Un sous-ensemble convexe E_1 et un sous-ensemble non convexe E_2 de $\mathbb{R}^2$

Définition 5.2.17 (Intervalle)
Un intervalle I de $\mathbb{R}$ est un sous-ensemble convexe I de $\mathbb{R}$, c'est-à-dire tel que :

$$\forall (a,b) \in I^2,\ \forall x \in \mathbb{R},\ a \leqslant x \leqslant b \Longrightarrow x \in I.$$

Intuitivement, « il n'y a pas de trou dans un intervalle ».

Théorème 5.2.18 (inventaire des intervalles)
Tout intervalle I de $\mathbb{R}$ est d'une des formes suivantes, pour certaines valeurs réelles a et b :

- $[a,b] = \{x \in \mathbb{R},\ a \leqslant x \leqslant b\}$, $a \leqslant b$;
- $]a,b[= \{x \in \mathbb{R},\ a < x < b\}$, $a < b$;
- $[a,b[= \{x \in \mathbb{R},\ a \leqslant x < b\}$, $a < b$;
- $]a,b] = \{x \in \mathbb{R},\ a < x \leqslant b\}$, $a < b$;
- $[a,+\infty[= \{x \in \mathbb{R},\ x \geqslant a\}$;
- $]a,+\infty[= \{x \in \mathbb{R},\ x > a\}$;
- $]-\infty,b] = \{x \in \mathbb{R},\ x \leqslant b\}$;
- $]-\infty,b[= \{x \in \mathbb{R},\ x < b\}$;
- $]-\infty,+\infty[= \mathbb{R}$;
- $\varnothing$.

Remarquez que le premier cas pour $a = b$ dit que tous les singletons $\{a\}$ sont des intervalles.
On définit de la même manière les intervalles de $\mathbb{Q}$ comme sous-ensemble convexes de $\mathbb{Q}$ (comme on reste dans $\mathbb{Q}$, les trous ne se voient pas dans la propriété de convexité)

Proposition 5.2.19 (description des intervalles de $\mathbb{Q}$)
Un sous-ensemble I de $\mathbb{Q}$ est un intervalle de $\mathbb{Q}$ si et seulement s'il existe un intervalle $I_{\mathbb{R}}$ de $\mathbb{R}$ tel que $I = I_{\mathbb{R}} \cap \mathbb{Q}$.

Les intervalles de $\mathbb{Q}$ n'admettent pas de description de la forme $]a,b[$ intrinsèque à $\mathbb{Q}$: on ne peut pas exprimer les bornes des intervalles sans sortir de $\mathbb{Q}$. Par exemple, $]0,\sqrt{2}[\cap\mathbb{Q}$ n'admet pas de borne supérieure dans $\mathbb{Q}$.

Remarque 5.2.20

L'inventaire des intervalles de $\mathbb{R}$ est strictement équivalente à la propriété de la borne supérieure, et pourrait être considérée comme propriété fondamentale de $\mathbb{R}$ en lieu et place de la propriété de la borne supérieure : un réel est alors une classe d'équivalence d'intervalles de $\mathbb{Q}$ de même borne supérieure dans $\mathbb{R}$ (cette notion d'égalité étant à définir intrinsèquement à $\mathbb{Q}$, pour que la définition soit valide).

Un intervalle est donc délimité par deux réels (ou les infinis), et chacune des deux bornes, si elle est finie, peut être ou ne pas être dans l'intervalle (une borne infinie est toujours exclue de l'intervalle, l'infini n'étant pas un réel). L'appartenance ou non des bornes à l'intervalle nous incite à donner un classement des intervalles :

Définition 5.2.21 (intervalles ouverts, fermés, semi-ouverts)

- On dit qu'un intervalle est ouvert s'il est de la forme $]a, b[$, $]a, +\infty[$, $]-\infty, b[$, $\mathbb{R}$ ou $\varnothing$.
- On dit qu'un intervalle est fermé s'il est de la forme $[a, b]$, $[a, +\infty[$, $]-\infty, b]$, $\mathbb{R}$ ou $\varnothing$.
- On dit qu'un intervalle est semi-ouvert s'il est de la forme $[a, b[$ ou $]a, b]$.

Remarquez qu'il existe des intervalles à la fois ouverts et fermés ($\mathbb{R}$ et $\varnothing$)

II.5 Intervalles et topologie

La notion d'intervalle est en fait liée à des notions de « topologie » plus générales (la topologie étant l'étude des sous-ensembles « ouverts » et « fermés » d'un ensemble). Nous nous limitons à une brève introduction de ces notions dans $\mathbb{R}^n$, la distance que nous utilisons étant la distance euclidienne canonique : si $X = (x_1, \ldots, x_n)$ et $Y = (y_1, \ldots, y_n)$, la distance entre X et Y est :

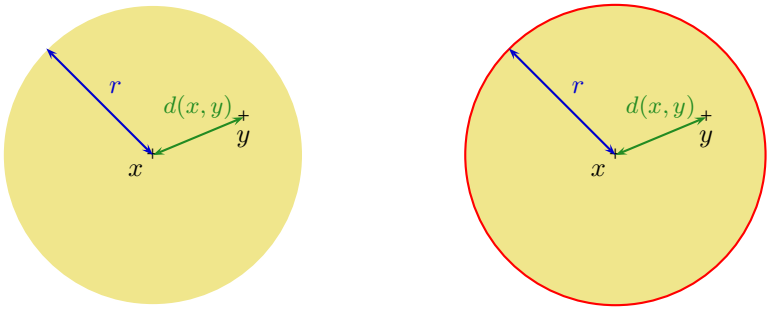
$$d(X, Y) = \sqrt{\sum_{i=1}^{n} (y_i - x_i)^2}.$$

En particulier, si $x, y \in \mathbb{R}^1 = \mathbb{R}$, $d(x, y) = |y - x|$.
Ces notions se généralisent dans des espaces muni de distances plus générales (espaces métriques).

Définition 5.2.22 (Boule dans $\mathbb{R}^n$, figure 5.4)

Soit $x \in \mathbb{R}^n$ et $r \in \mathbb{R}_+$.

1. La boule ouverte de centre x et de rayon r est : $B(x, r) = \{y \in \mathbb{R}^n \mid d(y, x) < r\}$
2. La boule fermée de centre x et de rayon r est : $\overline{B}(x, r) = \{y \in \mathbb{R}^n \mid d(y, x) \leqslant r\}$



$B(x, r)$ $\overline{B}(x, r)$

Figure 5.4 – Boules dans $\mathbb{R}^n$

Exemple 5.2.23

Dans $\mathbb{R}$, les boules sont des intervalles (voir figure 5.5) :

- $B(x,r) =]x-r, x+r[$
- $\overline{B}(x,r) = [x-r, x+r]$

En fait, tout intervalle borné ouvert est une boule ouverte, tout intervalle borné fermé est une boule fermée :

- $]a,b[= B\left(\frac{a+b}{2}, \frac{b-a}{2}\right)$,
- $[a,b] = \overline{B}\left(\frac{a+b}{2}, \frac{b-a}{2}\right)$

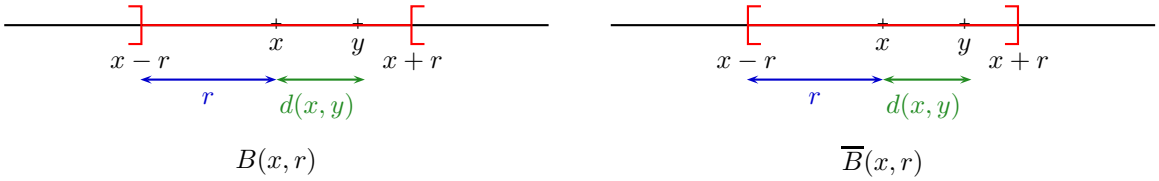


FIGURE 5.5 – Boule ouverte, boule fermée dans $\mathbb{R}$

Définition 5.2.24 (voisinage, figure 5.6)

Soit $x \in \mathbb{R}^n$. Un *voisinage* V de x est un sous-ensemble V de $\mathbb{R}^n$ tel qu'il existe une boule ouverte centrée en x entièrement contenue dans V :

$$\exists \varepsilon > 0,\ B(x,\varepsilon) \subset V, \qquad \text{i.e.} \qquad \exists \varepsilon > 0,\ \forall y \in E,\ d(y,x) < \varepsilon \Longrightarrow y \in V.$$

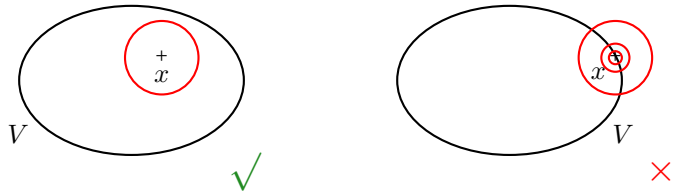


FIGURE 5.6 – Voisinage de x

En gros, V est un voisinage de x si x est « à l'intérieur de V », et non sur un bord. En s'éloignant un peu de x, on ne sort pas de V.

Exemple 5.2.25 (Voisinages dans $\mathbb{R}$)

- Dans $\mathbb{R}$, un voisinage de x est un ensemble contenant un intervalle $]a,b[$ tel que $x \in]a,b[$.
- Par extension et commodité, on dit parfois qu'un ensemble contenant un intervalle $]a,+\infty[$ est un voisinage de $+\infty$. Version symétrique pour $-\infty$.

Définition 5.2.26 (sous-ensemble ouvert)

- Un *ouvert* U de $\mathbb{R}^n$ est un sous-ensemble U de $\mathbb{R}^n$ qui est voisinage de tous ses points
- De manière équivalente, $U \subset \mathbb{R}^n$ est ouvert ssi :

$$\forall x \in U, \exists \varepsilon > 0,\ B(x,\varepsilon) \subset U.$$

Intuitivement, un ouvert est en ensemble dont le « bord » est flou : on peut s'en approcher, mais jamais l'atteindre en restant dans U. Ainsi, l'image qu'il faut en garder est qu'un ouvert est un ensemble ne contenant pas son bord. Évidemment, n'ayant pas défini la notion de bord, ceci reste une image.

Définition 5.2.27 (sous-ensemble fermé)

Un sous-ensemble F de $\mathbb{R}^n$ est *fermé* si son complémentaire $\complement_E F$ est ouvert.

Cette fois, intuitivement, c'est le complémentaire qui ne contient pas son bord, donc F, lui contient tout son bord.

Exemples 5.2.28

1. Les intervalles ouverts sont des sous-ensembles ouverts de $\mathbb{R}$.
2. Les intervalles fermés sont des sous-ensembles fermés de $\mathbb{R}$.
3. Les intervalles semi-ouverts ne sont ni ouverts ni fermés.
4. $\mathbb{R}$ et $\varnothing$ sont des sous-ensembles à la fois fermés et ouverts de $\mathbb{R}$.
5. On peut montrer que les sous-ensembles ouverts de $\mathbb{R}$ sont les unions disjointes d'intervalles ouverts.

Proposition 5.2.29 (union, intersection d'ouverts et de fermés)

1. *Toute union quelconque d'ouverts est un ouvert ;*
2. *Toute intersection d'un nombre* fini *d'ouverts est un ouvert ;*
3. *Toute intersection quelconque de fermés est un fermé ;*
4. *Toute union d'un nombre* fini *de fermés est un fermé.*

Exemples 5.2.30

Voici deux contre-exemples à bien garder en tête :

1. Contre-exemple pour une intersection infinie d'ouverts : $\displaystyle\bigcap_{n=1}^{+\infty} \left]-\frac{1}{n}, 1\right[= [0,1[$.
2. Contre-exemple pour une union infinie de fermés : $\displaystyle\bigcup_{n=1}^{+\infty} \left[\frac{1}{n}, 1\right] =]0,1]$.

III Droite achevée $\overline{\mathbb{R}}$

Par commodité, il est parfois intéressant de pouvoir considérer les deux infinis comme des éléments comme les autres. Cela permet en particulier d'unifier certains énoncés et certaines démonstrations, qui sinon, nécessiteraient une disjonction de cas.

Définition 5.3.1 (droite achevée réelle)

La droite achevée réelle, notée $\overline{\mathbb{R}}$, est l'ensemble $\mathbb{R} \cup \{-\infty, +\infty\}$.

Définition 5.3.2 (relation d'ordre sur $\overline{\mathbb{R}}$)

On peut prolonger l'ordre de $\mathbb{R}$ en un ordre sur $\overline{\mathbb{R}}$ en posant :

$$\forall x \in \overline{\mathbb{R}}, \quad -\infty \leqslant x \leqslant +\infty.$$

Définition 5.3.3 (règles calculatoires dans $\overline{\mathbb{R}}$)

On peut prolonger partiellement les opérations de $\mathbb{R}$ sur $\overline{\mathbb{R}}$, en posant :
- $-(+\infty) = -\infty$
- $\forall x \in \overline{\mathbb{R}} \setminus \cup\{-\infty\}, \quad x + (+\infty) = +\infty$
- $\forall x \in \overline{\mathbb{R}} \setminus \{+\infty\}, \quad x + (-\infty) = -\infty$
- $\frac{1}{+\infty} = \frac{1}{-\infty} = 0$
- $\forall x \in \mathbb{R}_+^*, \quad x \times (+\infty) = +\infty, \quad x \times (-\infty) = -\infty,$
- $\forall x \in \mathbb{R}_-^*, \quad x \times (+\infty) = -\infty, \quad x \times (-\infty) = +\infty.$

En revanche, certaines opérations ne peuvent pas être définies de façon cohérente, comme le montre l'étude des formes indéterminées dans le calcul des limites.

Définition 5.3.4 (formes indéterminées)

Les opérations suivantes ne sont pas définies, et définissent les formes indéterminées de la somme et du produit dans $\overline{\mathbb{R}}$:
- $-\infty + (+\infty)$
- $0 \times (+\infty)$
- $0 \times (-\infty)$.

Pour l'étude des limites, ces formes donnent également des formes indéterminées pour les puissances, par passage à l'exponentielle (voir le chapitre sur les suites).
Les intervalles de $\overline{\mathbb{R}}$ étant définis comme ceux de $\mathbb{R}$ par la propriété de convexité, on obtient la description suivante :

Proposition 5.3.5 (inventaire des intervalles de $\overline{\mathbb{R}}$)

Les intervalles de $\overline{\mathbb{R}}$ sont les intervalles de $\mathbb{R}$, et les intervalles de la forme $]a, +\infty]$, $[a, +\infty]$, $[-\infty, a[$, $[-\infty, a]$, $]-\infty, +\infty]$, $[-\infty, +\infty[$, et $[-\infty, +\infty] = \overline{\mathbb{R}}$, pour $a \in \mathbb{R}$.

6

Le corps $\mathbb{C}$ des complexes

Au reste, tant les vraies racines que les fausses ne sont pas toujours réelles, mais quelquefois seulement imaginaires, c'est à dire qu'on peut bien toujours en imaginer autant que j'ai dit en chaque équation, mais qu'il n'y a quelquefois aucune quantité qui corresponde à celles qu'on imagine ; comme encore qu'on puisse en imaginer trois en celle-ci :

$$x^3 - 6x^2 + 13x - 10 = 0,$$

il n'y en a toutefois qu'une réelle qui est 2, et pour les deux autres, quoiqu'on les augmente ou diminue, ou multiplie en la façon que je viens d'expliquer, on ne saurait les rendre autres qu'imaginaires.

(René Descartes)

Ce que nous nommons temps imaginaire est en réalité le temps réel, et ce que nous nommons temps réel n'est qu'une figure de notre imagination.

(Stephen Hawking)

Les nombres complexes sont nés de l'étude des solutions des équations du troisième degré. Dans un premier temps, ils ont été utilisés sans se préoccuper de leur donner un sens précis : ils étaient des outils abstraits, imaginaire pourrait-on dire, pour accéder aux solutions, pouvant elles être bien réelles, des équations considérées.

I Les nombres complexes : définition et manipulations

I.1 Définition, forme algébrique

Note Historique 6.1.1

- Les nombres complexes ont été introduits par Cardan et Bombelli au 16-ième siècle, comme moyen d'exprimer certaines racines de polynômes de degrés 3 ou 4. A cette époque, l'introduction des nombres imaginaires (*via* des racines de réels négatifs) est un pur artifice.
- Ainsi, dès leur origine, les nombres complexes sont introduits pour pallier au fait que certains polynômes à coefficients réels n'ont pas de racines dans $\mathbb{R}$, comme par exemple $X^2 + 1$.
- La notation i est introduite par Euler en 1777 pour remplacer la notation $\sqrt{-1}$.

D'un point de vue formel, $\mathbb{C}$ est défini comme le plus petit sur-corps de $\mathbb{R}$ dans lequel le polynôme X^2+1 admet une racine (c'est ce qu'on appelle un corps de rupture du polynôme X^2+1, correspondant dans ce cas au corps de décomposition, le plus petit corps dans lequel le polynôme peut se factoriser en polynômes de degré 1).

Ainsi, il s'agit d'un ensemble contenant un élément i, racine de X^2+1, vérifiant donc $\mathrm{i}^2=-1$, et muni d'une addition et d'un produit prolongeant celles de $\mathbb{R}$, avec les mêmes propriétés. En fait, la relation $\mathrm{i}^2=-1$ et les propriétés de commutativité, associativité et distributivité déterminent entièrement les opérations sur $\mathbb{C}$. Nous donnons la définition suivante :

Définition 6.1.2 (ensemble $\mathbb{C}$ des nombres complexes)

L'ensemble des nombres complexes $\mathbb{C}$ est l'ensemble $\mathbb{R}^2$, muni des opérations suivantes :
- $(a,b)+(a',b')=(aa',bb')$;
- $(a,b)\times(a',b')=(aa'-bb',ab'+a'b)$.

Pour tout réel λ et tout complexe $z=(a,b)$, on peut définir λz par $\lambda z=(\lambda a,\lambda b)$.

Définition 6.1.3 (définition de la forme algébrique ; partie réelle, partie imaginaire)
- On note $1=(1,0)$, et $\mathrm{i}=(0,1)$
- On a alors, pour tout $z=(a,b)\in\mathbb{C}$, $z=a+\mathrm{i}\,b$. C'est la *forme algébrique* du nombre complexe z.
- Soit $z=a+\mathrm{i}\,b$, avec $a,b\in\mathbb{R}$.
  - Le réel a est appelé *partie réelle de z*, et est noté $\mathrm{Re}(z)$;
  - Le réel b est appelé *partie imaginaire de z*, et est noté $\mathrm{Im}(z)$
- Un nombre $z\in\mathbb{C}$ (disons $z=a+\mathrm{i}\,b$, $(a,b)\in\mathbb{R}$) tel que $\mathrm{Im}(z)=0$ (donc $z=a$) est identifié au réel a. Ainsi, l'ensemble des nombres complexes de partie imaginaire nulle est égal à l'ensemble des nombres réels. En particulier, on a une inclusion $\mathbb{R}\subset\mathbb{C}$.
- Un nombre $z\in\mathbb{C}$ tel que $\mathrm{Re}(z)=0$ est appelé *nombre imaginaire pur*.

Proposition 6.1.4 (propriétés liées au produit)

1. $\mathrm{i}^2=-1$
2. *Le produit $(a+\mathrm{i}\,b)(a'+\mathrm{i}\,b')$ est simplement obtenu par utilisation des règles de distributivité et par la relation $\mathrm{i}^2=-1$.*
3. *Si $z\neq 0$, alors z et inversible, et, si $z=a+\mathrm{i}\,b$ avec $(a,b)\in\mathbb{R}^2$, on a l'expression de l'inverse :*

$$z^{-1}=\frac{a-\mathrm{i}\,b}{a^2+b^2}.$$

Théorème 6.1.5 (structure de $\mathbb{C}$)

L'ensemble $\mathbb{C}$ muni des opérations ci-dessus est un corps.

Dans la pratique, un nombre complexe est représenté sous sa forme algébrique $a+\mathrm{i}\,b$, ou sa forme trigonométrique que nous rappellerons plus loin. On perd un peu de vue le point de vue initial du couple (d'ailleurs, on peut introduire $\mathbb{C}$ de façon différente). Nous donnons dans la définition suivante la démarche inverse, permettant de revenir de $\mathbb{C}$ à $\mathbb{R}^2$. Cette interprétation est fructueuse pour la geométrie du plan, pouvant ainsi être étudiée sous l'angle des nombres complexes.

Définition 6.1.6 (affixe d'un point du plan)

Soit $A=(a,b)$ un point de $\mathbb{R}^2$. L'*affixe* du point A est le nombre complexe $z_A=a+\mathrm{i}\,b$.

Désormais, nous abandonnons la notation d'un complexe sous forme d'un couple, et nous représenterons un nombre complexe sous la forme $a+\mathrm{i}\,b$.
Remarquons que la construction de $\mathbb{C}$ à partir de $\mathbb{R}$ est un cas particulier d'une construction plus générale d' « extensions monogènes d'un corps $\mathbb{K}$ », à la base de la théorie de Galois : étant donné une racine x d'une

équation polynomiale P à coefficients dans $\mathbb{K}$, $\mathbb{K}[x]$ est l'ensemble de toutes les sommes, produits, quotients qu'on peut former à partir des éléments de $\mathbb{K}$ et de x. Par exemple $\mathbb{Q}[\sqrt{2}] = \{(a + b\sqrt{2}), (a, b) \in \mathbb{Q}^2\}$, et $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2,\ (a, b, c) \in \mathbb{Q}^3\}$ (on peut montrer que tout quotient peut s'exprimer ainsi aussi).
De ce point de vue, $\mathbb{C} = \mathbb{R}[\mathrm{i}]$.

Nous avons donc défini $\mathbb{C}$ comme un corps de rupture sur $\mathbb{R}$ du polynôme $X^2 + 1$, et même un corps de décomposition, puisqu'on a alors la factorisation suivante : $X^2 + 1 = (X + \mathrm{i})(X - \mathrm{i})$. En fait, cette propriété est beaucoup plus générale, ainsi que le prouve le théorème suivant, d'une importance capitale :

Théorème 6.1.7 (d'Alembert-Gauss)

Tout polynôme non constant à coefficients complexes admet au moins une racine dans $\mathbb{C}$.

On démontrera plus tard que ceci implique que tout polynôme à coefficient complexe se factorise en polynômes de degré 1.
Le théorème de d'Alembert-Gauss se réexprime ainsi : $\mathbb{C}$ est algébriquement clos, ce qui signifie qu'il n'existe pas d'autre nombre algébrique sur $\mathbb{C}$ que les nombres complexes eux-mêmes.
Le théorème de d'Alembert-Gauss, restreint aux polynômes à coefficients réels, allié au fait que $\mathbb{C}$ est par définition le plus petit corps dans lequel $X^2 + 1$ admet une racine, s'exprime en disant que $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$.

Note Historique 6.1.8

Le théorème de d'Alembert-Gauss est d'une importance capitale, puisque c'est ce résultat qui motive la construction de $\mathbb{C}$.

- Il est conjecturé depuis longtemps déjà lorsque d'Alembert en propose une preuve en 1743. Cette preuve n'est pas satisfaisante, Gauss va jusqu'à la qualifier de *petitio principii*, puisqu'elle part de l'hypothèse de l'existence de racines « fictives ».
- La première preuve complète et rigoureuse revient à Gauss, au 19-ième siècle.

Nous voyons maintenant quelques notions directement liées à la forme algébrique des nombres complexes

Définition 6.1.9 (conjugué d'un nombre complexe)

Soit $z = a + \mathrm{i}\,b$ (avec $(a, b) \in \mathbb{R}^2$) un nombre complexe. Le *conjugué* de z est le nombre complexe

$$\overline{z} = a - \mathrm{i}\,b.$$

Propriétés 6.1.10 (propriétés de la conjugaison dans $\mathbb{C}$)

Soit z et z' deux nombres complexes. Alors :

1. $\overline{\overline{z}} = z$ *(autrement dit, la conjugaison est une involution) ;*
2. $z = \overline{z} \iff z \in \mathbb{R}$ *;*
3. $z = -\overline{z} \iff z$ *imaginaire pur ;*
4. $\mathrm{Re}(z) = \frac{z+\overline{z}}{2}$ *et* $\mathrm{Im}(z) = \frac{z-\overline{z}}{2\,\mathrm{i}}$ *;*
5. $\overline{z + z'} = \overline{z} + \overline{z'}$ *et* $\overline{zz'} = \overline{z} \cdot \overline{z'}$ *;*

I.2 Module

Nous définissons maintenant quelques notions liées à la structure euclidienne de $\mathbb{R}^2$, donc aux propriétés métriques.

Définition 6.1.11 (module d'un nombre complexe)
Soit $(a, b) \in \mathbb{R}^2$, et $z = a + \mathrm{i}\, b$. Le *module* de z est le réel positif défini par

$$|z| = \sqrt{a^2 + b^2}.$$

Remarque 6.1.12
Via la correspondance entre $\mathbb{C}$ et $\mathbb{R}^2$ le module d'un nombre complexe correspond à la norme des vecteurs. Ainsi, si A est le point d'affixe z et O l'origine, alors $|z| = \|\overrightarrow{OA}\|$.

Exemples 6.1.13
1. Décrire l'ensemble des nombres complexes z tels que $|z - a| = r$, où $a \in \mathbb{C}$ et $r \in \mathbb{R}_+^*$.
2. Même question avec l'inéquation $|z - a| \leqslant r$.

Propriétés 6.1.14 (propriétés du module)
Soit z et z' deux nombres complexes. Alors :
1. $z = 0 \iff |z| = 0$;
2. $|\mathrm{Re}(z)| \leqslant |z|$ *et* $|\mathrm{Im}(z)| \leqslant |z|$;
3. $|zz'| = |z| \cdot |z'|$ *et si* $z' \neq 0$, $\left|\frac{z}{z'}\right| = \frac{|z|}{|z'|}$ *(multiplicativité du module)*
4. $|z + z'| \leqslant |z| + |z'|$ *(inégalité triangulaire, ou sous-additivité du module).*
   L'égalité est vérifiée si et seulement si $z = 0$ ou s'il existe $\lambda \in \mathbb{R}_+$ tel que $z' = \lambda z$.
5. $|z|^2 = z\overline{z}$ *(expression du module à l'aide du conjugué)*
6. $|z| = |\overline{z}|$ *(invariance du module par conjugaison)*

On en déduit notamment une méthode pour exprimer sous forme algébrique un quotient de deux complexes donnés sous forme algébrique (pour les autres opérations, cela ne pose aucune difficulté).

Méthode 6.1.15 (Expression algébrique d'un quotient)
Soit z_1 et z_2 deux nombres complexes donnés sous forme algébrique, avec $z_2 \neq 0$. Pour trouver la forme algébrique du quotient $\dfrac{z_1}{z_2}$, multipliez le dénominateur et le numérateur par $\overline{z_2}$, c'est-à-dire considérez l'expression $\frac{z_1 \cdot \overline{z_2}}{z_2 \cdot \overline{z_2}}$
De la sorte, le dénominateur est maintenant un réel.

II Trigonométrie

II.1 Cercle trigonométrique, formules de trigonométrie

Littéralement, « trigonométrie » signifie « mesure des trois angles », donc se rapporte aux propriétés des angles d'un triangle. On fait donc ainsi référence aux interprétations géométriques usuelles des fonctions trigonométriques.

Note Historique 6.2.1
- La trigonométrie (l'étude des mesures dans le triangle) existe depuis l'antiquité (Égypte, Babylone, Grèce), et est développée en rapport avec l'astronomie.

- Le sinus, sous sa forme actuelle, a été introduit par les indiens aux alentours de 500 ap JC, pour l'étude des angles célestes. La première table connue date de 499, et est attribuée au mathématicien indien Aryabhata. En 628, Brahmagupta construit une approximation de la fonction sinus par interpolation.
- Ces notions nous sont parvenus grâce aux travaux de synthèse des mathématiciens arabes des 9^{e} et 10^{e} siècles (essentiellement basés dans les actuelles Irak, Iran et Khazakstan)
- Auparavant, les grecs utilisaient plutôt la mesure de la corde, ce qui est moins commode, mais assez équivalent.
- Le nom de « sinus » provient d'un mot sanscrit signifiant « arc », apparaissant dans l'ouvrage de Aryabhata, et transcrit phonétiquement en arabe, puis déformé en un mot proche signifiant « repli de vêtement ». Il a été traduit en latin au 12^{e} siècle par le mot « sinus » signifiant « pli ».

Définition 6.2.2 (cercle trigonométrique)

Le cercle trigonométrique (ou cercle unité) est le sous-ensemble de $\mathbb{C}$, noté $\mathbb{U}$ (comme « unité »), constitué des nombres complexes de module 1 :

$$\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}.$$

Le cercle trigonométrique correspond dans l'interprétation géométrique des complexes au cercle de centre $(0, 0)$ et de rayon 1 de $\mathbb{R}^2$.

Définition 6.2.3 (fonctions trigonométriques, figure 6.1)

Soit $x \in \mathbb{R}$. Soit z le point du cercle trigonométrique tel que le rayon correspondant du cercle trigonométrique forme avec l'axe des réels un angle (orienté dans le sens direct) de x. On définit alors les fonctions cosinus, sinus et tangente par :

$$\cos(x) = \mathrm{Re}(z), \qquad \sin(x) = \mathrm{Im}(z) \qquad \text{et} \qquad \tan(x) = \frac{\sin(x)}{\cos(x)} \text{ si } \cos(x) \neq 0.$$

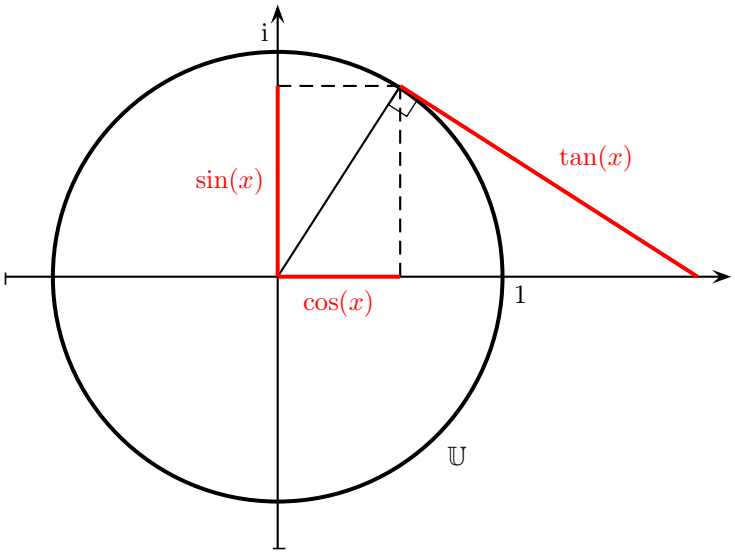


FIGURE 6.1 – Fonctions trigonométriques

On retrouve facilement l'interprétation usuelle sur les triangles (définitions données au collège), pour un angle $\alpha \in]0, \frac{\pi}{2}[$: si ABC est un triangle rectangle en A, et d'angle en B égal à α, alors :

$$\sin(x) = \frac{\text{côté opposé}}{\text{hypothénuse}}, \qquad \cos(x) = \frac{\text{côté adjacent}}{\text{hypothénuse}}, \qquad \tan(x) = \frac{\text{côté opposé}}{\text{côté adjacent}}.$$

On utilise parfois une autre fonction trigonométrique, version symétrique de la tangente :

Définition 6.2.4 (cotangente)

Soit $x \in \mathbb{R}$. La cotangente est définie, pour tout x tel que $\sin(x) \neq 0$, par :

$$\operatorname{cotan}(x) = \frac{\cos(x)}{\sin(x)}.$$

Ainsi, en tout point en lequel à la fois $\sin(x) \neq 0$ et $\cos(x) \neq 0$, on a $\operatorname{cotan}(x) = \frac{1}{\tan(x)}$.

Proposition 6.2.5 (domaines de définition des fonctions trigonométriques)

1. *Les fonctions* sin *et* cos *sont définies sur* $\mathbb{R}$.
2. *La fonction* tan *est définie sur* $\bigcup_{n\in\mathbb{Z}} \left]-\frac{\pi}{2}+n\pi, \frac{\pi}{2}+n\pi\right[= \mathbb{R} \setminus \left\{\frac{\pi}{2}+n\pi,\ n \in \mathbb{Z}\right\}$.
3. *La fonction* cotan *est définie sur* $\bigcup_{n\in\mathbb{Z}}]n\pi, (n+1)\pi[= \mathbb{R} \setminus \{n\pi,\ n \in \mathbb{Z}\}$.

Les propriétés suivantes sont à bien comprendre sur le cercle trigonométrique.

Proposition 6.2.6 (Symétries de sin et cos)

1. sin *et* cos *sont* 2π*-périodiques ;*
2. sin *est impaire et* cos *est paire ;*
3. $\forall x \in \mathbb{R}$, $\cos(\pi + x) = -\cos(x)$, *et* $\sin(\pi + x) = -\sin(x)$.
4. $\forall x \in \mathbb{R}$, $\cos(\pi - x) = -\cos(x)$, *et* $\sin(\pi - x) = \sin(x)$.
5. $\forall x \in \mathbb{R}$, $\cos\left(\frac{\pi}{2} - x\right) = \sin(x)$, *et* $\sin\left(\frac{\pi}{2} - x\right) = \cos(x)$.
6. $\forall x \in \mathbb{R}$, $\cos\left(\frac{\pi}{2} + x\right) = -\sin(x)$, *et* $\sin\left(\frac{\pi}{2} + x\right) = \cos(x)$.

Proposition 6.2.7 (symétries de tan et cotan)

1. tan *et* cotan *sont* π*-périodiques ;*
2. tan *et* cotan *sont impaires ;*
3. *pour tout* x *dans le domaine de* tan, $\tan(\pi - x) = -\tan(x)$ *;*
4. *pour tout* x *dans le domaine de* cotan, $\operatorname{cotan}(\pi - x) = -\operatorname{cotan}(x)$ *;*
5. *pour tout* $x \in \mathbb{R} \setminus \left\{\frac{n\pi}{2},\ n \in \mathbb{Z}\right\}$, $\tan\left(\frac{\pi}{2} - x\right) = \operatorname{cotan}(x)$ *et* $\operatorname{cotan}\left(\frac{\pi}{2} - x\right) = \tan(x)$ *;*
6. *pour tout* $x \in \mathbb{R} \setminus \left\{\frac{n\pi}{2},\ n \in \mathbb{Z}\right\}$, $\tan\left(\frac{\pi}{2} + x\right) = -\operatorname{cotan}(x)$ *et* $\operatorname{cotan}\left(\frac{\pi}{2} + x\right) = -\tan(x)$ *;*

Nous rappelons :

Proposition 6.2.8 (Valeurs particulières des fonctions trigonométriques)

Voici un tableau des valeurs particulières à bien connaître, entre 0 *et* $\frac{\pi}{2}$ *(les autres s'obtiennent par les symétries) :*

	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$
sin	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1
cos	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0
tan	0	$\frac{1}{\sqrt{3}}$	1	$\sqrt{3}$	–
cotan	–	$\sqrt{3}$	1	$\frac{1}{\sqrt{3}}$	0

Nous obtenons les graphes des fonctions trigonomtriques, les variations pouvant être obtenues par des considérations purement géométriques (voir figure 6.2).

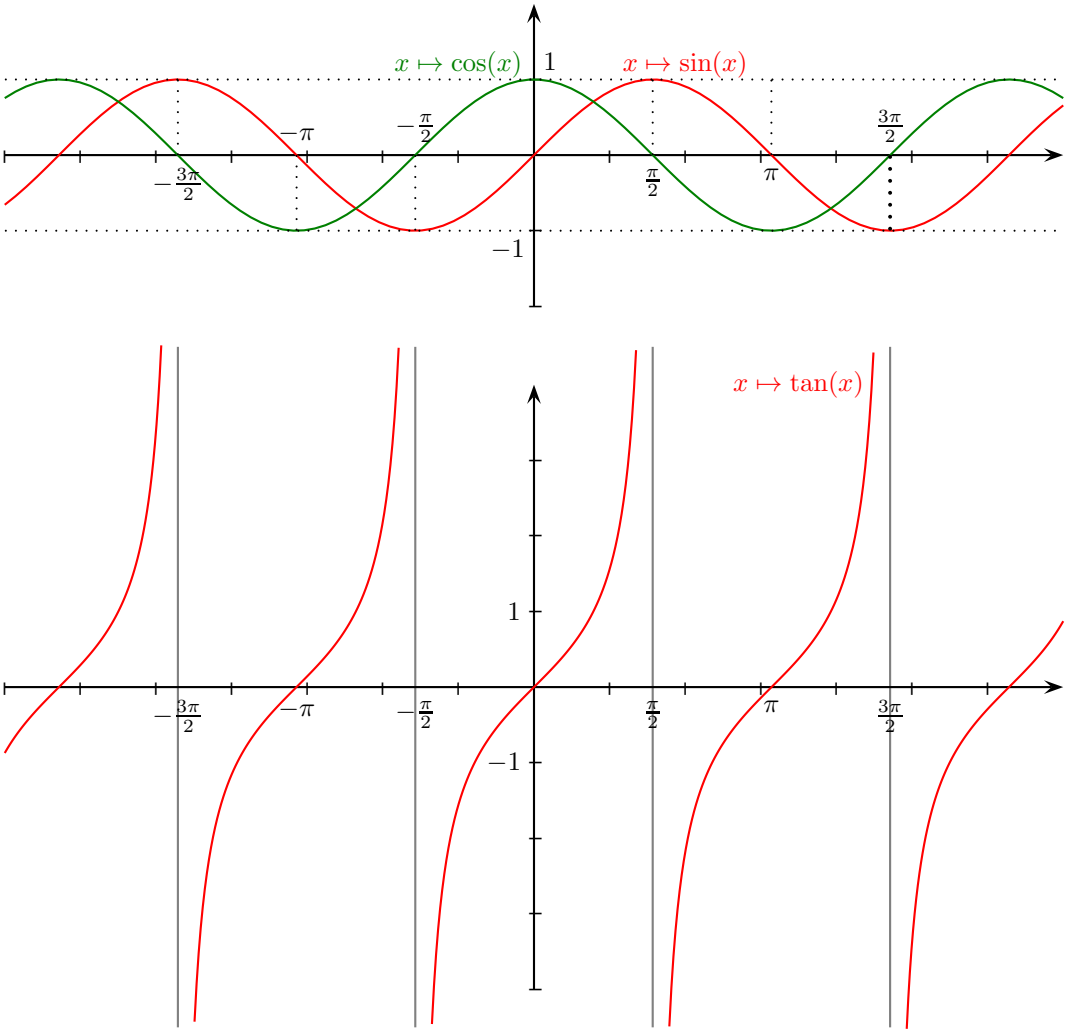


FIGURE 6.2 – Graphe des fonctions trigonométriques

Et voici les inévitables formules à retenir...

Proposition 6.2.9 (identité remarquable, ou théorème de Pythagore)
Pour tout $x \in \mathbb{R}$, $\sin^2 x + \cos^2 x = 1$.

Proposition 6.2.10 (formules d'addition)
Soit a *et* b *deux réels. Alors :*

(i) $\sin(a+b) = \sin a \cos b + \sin b \cos a$

(ii) $\sin(a-b) = \sin a \cos b - \sin b \cos a$

(iii) $\cos(a+b) = \cos a \cos b - \sin a \sin b$

(iv) $\cos(a-b) = \cos a \cos b + \sin a \sin b$

(v) Pour tout $(a,b) \in \mathbb{R}^2$ *tel que* $\tan(a)$, $\tan(b)$ *et* $\tan(a+b)$ *soient définis :*
$$\tan(a+b) = \frac{\tan a + \tan b}{1 - \tan a \tan b}$$

(vi) Pour tout $(a,b) \in \mathbb{R}^2$ *tel que* $\tan(a)$, $\tan(b)$ *et* $\tan(a-b)$ *soient définis :*
$$\tan(a-b) = \frac{\tan a - \tan b}{1 + \tan a \tan b}$$

Proposition 6.2.11 (formules de duplication des angles)
Soit a *un réels. Alors :*

(i) $\sin 2a = 2 \sin a \cos a$

(ii) $\cos 2a = \cos^2 a - \sin^2 a = 1 - 2\sin^2 a = 2\cos^2 a - 1$.

(iii) $\tan 2a = \dfrac{2 \tan a}{1 - \tan^2 a}$

Proposition 6.2.12 (formules de linéarisation des carrés, ou formules de Carnot)
Soit $a \in \mathbb{R}$ *:*

(i) $\cos^2 a = \dfrac{1 + \cos 2a}{2}$

(ii) $\sin^2 a = \dfrac{1 - \cos 2a}{2}$

Proposition 6.2.13 (formules de développement, ou transformation de produit en somme)
Soit a *et* b *deux réels.*

(i) $\sin a \sin b = \dfrac{1}{2}[\cos(a-b) - \cos(a+b)]$

(ii) $\cos a \cos b = \dfrac{1}{2}[\cos(a-b) + \cos(a+b)]$

(iii) $\sin a \cos b = \dfrac{1}{2}[\sin(a+b) + \sin(a-b)]$

Proposition 6.2.14 (formules de factorisation, ou formules de Simpson)
Soit p *et* q *deux réels.*

(i) $\sin p + \sin q = 2 \sin \dfrac{p+q}{2} \cos \dfrac{p-q}{2}$

(ii) $\sin p - \sin q = 2 \cos \dfrac{p+q}{2} \sin \dfrac{p-q}{2}$

(iii) $\cos p + \cos q = 2\cos\dfrac{p+q}{2}\cos\dfrac{p-q}{2}$

(iv) $\cos p - \cos q = -2\sin\dfrac{p+q}{2}\sin\dfrac{p-q}{2}$

Proposition 6.2.15 (formules de l'arc moitié)

Soit x un réel tel que $t = \tan\left(\frac{x}{2}\right)$ soit défini. Alors :

(i) $\sin x = \dfrac{2t}{1+t^2}$

(ii) $\cos x = \dfrac{1-t^2}{1+t^2}$

(iii) $\tan x = \dfrac{2t}{1-t^2}$ *si* $t \neq \pm 1$.

Proposition 6.2.16 (formule de factorisation de $a\cos x + b\sin x$)

Soit a, b et x trois réels, $a \neq 0$. Alors

$$a\cos x + b\sin x = \frac{a}{\cos\varphi}\cos(x-\varphi), \quad \text{où } \tan(\varphi) = \frac{b}{a}.$$

En physique, $\dfrac{a}{\cos(\varphi)}$ est appelé *amplitude* et φ est appelé la *phase*.

II.2 L'exponentielle complexe et applications à la trigonométrie

Définition 6.2.17 (exponentielle complexe)

On définit l'exponentielle complexe sur les nombres imaginaires purs par :

$$\forall \theta \in \mathbb{R}, \quad \mathrm{e}^{\mathrm{i}\,\theta} = \cos\theta + \mathrm{i}\sin\theta.$$

Proposition 6.2.18

La fonction $\theta \mapsto \mathrm{e}^{\mathrm{i}\,\theta}$ est surjective de $\mathbb{R}$ sur $\mathbb{U}$. Plus précisément, c'est une bijection de tout intervalle $]\alpha, \alpha+2\pi]$ sur $\mathbb{U}$, ainsi que de tout intervalle $[\alpha, \alpha+2\pi[$ sur $\mathbb{U}$.

Corollaire 6.2.19

La fonction de $\mathbb{R}_+^* \times]-\pi, \pi]$ sur $\mathbb{C}^*$ définie par $(r,\theta) \mapsto r\mathrm{e}^{\mathrm{i}\,\theta}$ est bijective.

Définition 6.2.20 (forme trigonométrique)

- Ainsi, tout nombre complexe z s'écrit sous la forme $z = r\mathrm{e}^{\mathrm{i}\,\theta}$ appelée forme trigonométrique de z, avec $r > 0$;
- r est unique, égal au module de z ;
- θ est unique *modulo* 2π, appelé argument de z.
- L'unique argument θ de l'intervalle $]-\pi, \pi]$ est appelé *argument principal* de z et est noté $\arg(z)$.

Proposition 6.2.21 (formules d'Euler)

Soit $\theta \in \mathbb{R}$. Alors :

$$\cos(\theta) = \frac{e^{i\,\theta} + e^{-i\,\theta}}{2} \qquad et \qquad \sin(\theta) = \frac{e^{i\,\theta} - e^{-i\,\theta}}{2\,i}.$$

Théorème 6.2.22 (formules trigonométriques d'addition)

Pour tout $(\theta, \theta') \in \mathbb{R}^2$, $e^{i(\theta+\theta')} = e^{i\,\theta} e^{i\,\theta'}$.

Corollaire 6.2.23 (Formule de (De) Moivre, 1707)

Pour tout $\theta \in \mathbb{R}$ et $n \in \mathbb{N}$:

$$e^{i\,n\theta} = (e^{i\,\theta})^n \qquad soit: \qquad \cos(n\theta) + i\sin(n\theta) = (\cos\theta + i\sin\theta)^n.$$

Note Historique 6.2.24

- Abraham de Moivre était un mathématicien ami des physiciens et astronomes Newton et Halley. Il faudrait théoriquement dire « formule de De Moivre », (selon la règle de conservation de la particule onomastique pour les noms d'une syllabe, comme de Gaulle), mais on dit plus souvent « formule de Moivre ».
- La version démontrée par Moivre est la version donnée avec les fonctions sin et cos, le lien avec les propriétés de l'exponentielle n'ayant été découvertes que plus tard par Euler (19^e siècle), qui est à l'origine de la notation exponentielle $e^{i\,\theta}$.

L'utilisation des exponentielles complexes permet de simplifier un certain nombre de calculs liés à la trigonométrie. Nous présentons ci-dessous quelques méthodes à connaître.

Méthode 6.2.25 (Principe de symétrisation des arguments)

Cette méthode permet d'exprimer une somme ou une différence de deux exponentielles à l'aide des fonctions trigonométriques. C'est notamment intéressant pour obtenir la partie réelle et la partie imaginaire sous forme factorisée. Soit a et b deux réels. Alors :

- $e^{i\,a} + e^{i\,b} = e^{i\,\frac{a+b}{2}} \left(e^{i\,\frac{a-b}{2}} + e^{-i\,\frac{a-b}{2}}\right) = 2\cos\left(\frac{a-b}{2}\right) e^{i\,\frac{a+b}{2}}$.
- $e^{i\,a} - e^{i\,b} = e^{i\,\frac{a+b}{2}} \left(e^{i\,\frac{a-b}{2}} - e^{-i\,\frac{a-b}{2}}\right) = 2\,i\sin\left(\frac{a-b}{2}\right) e^{i\,\frac{a+b}{2}}$.

Remarquez que c'est une façon commode de retenir ou retrouver les formules de factorisation des fonctions trigonométriques (transformation d'une somme en produit).

Exemple 6.2.26

Factoriser $1 + e^{i\,a}$.

Méthode 6.2.27 (Linéarisation)

Le but est d'exprimer $\cos^n\theta$ ou $\sin^n\theta$ en fonction de $\cos(k\theta)$ et $\sin(k\theta)$, $k \in \mathbb{N}$. Principe du calcul :

1. Exprimer $\cos\theta$ (ou $\sin\theta$) à l'aide des formules d'Euler ;
2. Développer à l'aide de la formule du binôme de Newton ;
3. Regrouper dans le développement les exponentielles conjuguées et les réexprimer à l'aide des fonctions sin et cos en utilisant la formule d'Euler dans l'autre sens.

Exemple 6.2.28

1. Linéariser $\cos^4(x)$
2. Linéariser $\sin^5(x)$. En déduire $\displaystyle\int_0^\pi \sin^5(x)\,\mathrm{d}x$.

Méthode 6.2.29 (« délinéarisation », ou les polynômes de Tchébychev)

Il s'agit de la méthode inverse, consistant à écrire $\cos(n\theta)$ ou $\sin(n\theta)$ en fonction des puissances de $\cos(x)$ et/ou $\sin(x)$. Le principe du calcul :

1. On utilise la formule de Moivre pour exprimer $\cos(n\theta)$ ou $\sin(n\theta)$ comme partie réelle ou imaginaire de $(\cos(\theta)+\mathrm{i}\sin(\theta))^n$.
2. On développe cette expression à l'aide de la formule du binôme de Newton
3. On utilise l'identité remarquable $\sin^2 x+\cos^2 x=1$ pour exprimer la partie réelle (ou imaginaire) sous forme d'un polynôme en $\cos(x)$ (pour $\cos(n\theta)$) ou le produit de $\cos(x)$ par un polynôme en $\sin(x)$ (pour $\sin(n\theta)$)

Remarque 6.2.30

Les polynômes obtenus ainsi s'appelle polynômes de Tchébychev, de première espèce pour les cosinus, et de seconde espèce pour les sinus. On peut définir ces polynômes par récurrence et redémontrer directement à l'aide de ces relations de récurrence et des formules de trigonométrie le fait qu'ils assurent la délinéarisation de $\cos(n\theta)$ et $\sin(n\theta)$. La méthode ci-dessus permet alors d'obtenir une expression explicite de ces polynômes.

Méthode 6.2.31 (Sommes de sin et cos)

Le principe général est d'écrire une somme de sin (ou de cos) sous forme de partie imaginaire (ou réelle) d'une somme d'exponentielles. On peut alors souvent exploiter le caractère géométrique du terme $\mathrm{e}^{\mathrm{i}\,n\theta}$, par utilisation des propriétés des sommes géométriques, ou de la formule du binôme etc.

Exemple 6.2.32 (noyau de Dirichlet)

Soit a et b deux réels et

$$C=\cos a+\cos(a+b)+\cos(a+2b)+\cdots+\cos(a+nb)=\sum_{k=0}^{n}\cos(a+kb).$$

Alors $C=\cos\left(a+\dfrac{bn}{2}\right)\cdot\dfrac{\sin\left(\frac{n+1}{2}\cdot b\right)}{\sin\frac{b}{2}}$.

Nous terminons ce paragraphe par une présentation rapide de l'exponentielle complexe générale.

Définition 6.2.33 (Exponentielle complexe)

Soit z un nombre complexe. On définit alors $\mathrm{e}^z=\mathrm{e}^{\mathrm{Re}(z)}\times\mathrm{e}^{\mathrm{i}\,\mathrm{Im}(z)}$.

Si z est réel ou imaginaire pur, on retrouve respectivement l'exponentielle réelle et l'exponentielle définie sur les imaginaires purs.

Théorème 6.2.34 (propriété d'addition)
Soit $(z, z') \in \mathbb{C}^2$. *Alors* $\mathrm{e}^{z+z'} = \mathrm{e}^z e^{z'}$.

Proposition 6.2.35 (cas d'égalité)
Soit $(z, z') \in \mathbb{C}^2$. *On a* $\mathrm{e}^z = \mathrm{e}^{z'}$ *si et seulement si* $\mathrm{Re}(z) = \mathrm{Re}(z')$ *et* $\mathrm{Im}(z) \equiv \mathrm{Im}(z') \mod 2\pi$.

Proposition 6.2.36 (recherche de l'image réciproque)
Soit $a \in \mathbb{C}^2$. *Alors :*
- *si* $a = 0$, *l'équation* $\mathrm{e}^z = a$ *n'a pas de solution ;*
- *si* $a \neq 0$, *l'équation* $\mathrm{e}^z = a$ *a une infinité de solutions, décrites par :*

$$\mathrm{Re}(z) = \ln|a| \qquad et \qquad \mathrm{Im}(z) \equiv \arg(a) \mod 2\pi.$$

III Racines d'un nombre complexe

III.1 Racines n-ièmes

Définition 6.3.1 (racines n-ièmes, groupe $\mathbb{U}_n$)
- Soit $n \in \mathbb{N}^*$ et $z \in \mathbb{C}$. Une racine n-ième de z est une racine (complexe) du polynôme $X^n - z$, donc un nombre complexe ω tel que $\omega^n = z$
- Une racine n-ième de l'unité est une racine n-ième de 1.
- L'ensemble des racines n-ièmes de l'unité est noté $\mathbb{U}_n$.

Nous verrons plus tard que cet ensemble $\mathbb{U}_n$ possède une structure de *groupe* (notion définie plus tard).

Proposition 6.3.2 (Explicitation des racines de l'unité)
Le groupe $\mathbb{U}_n$ *des racines n-ièmes de l'unité est constitué de n éléments deux à deux distincts et donnés par :*

$$\mathbb{U}_n = \{\omega_k = \mathrm{e}^{\mathrm{i}\frac{2\pi k}{n}}, k \in [\![0, n-1]\!]\}.$$

Ces racines se répartissent de façon régulière sur le cercle trigonométrique, de façon à former les sommets d'un polygône régulier à n côtés (figure 6.3)

Proposition 6.3.3 (racines n-ièmes de z, figure 6.4)
Soit $z = r\mathrm{e}^{\mathrm{i}\,\theta}$ *un nombre complexe. Alors :*

(i) Une racine n-ième particulière de z est $z_0 = \sqrt[n]{r} \cdot \mathrm{e}^{\mathrm{i}\frac{\theta}{n}}$

(ii) z possède exactement n racines n ièmes, données par :

$$\xi_k = z_0\omega_k, \quad k \in [\![0, n-1]\!],$$

où $\omega_0, \ldots, \omega_{n-1}$ *sont les racines n-ièmes de l'unité.*

(iii) Ainsi, pour $z = r\mathrm{e}^{\mathrm{i}\,\theta}$, *on obtient la description explicite des racines n-ièmes :*

$$\xi_k = \sqrt[n]{r} \cdot \mathrm{e}^{\mathrm{i}\left(\frac{\theta+2k\pi}{n}\right)}, \quad k \in [\![0, n-1]\!].$$

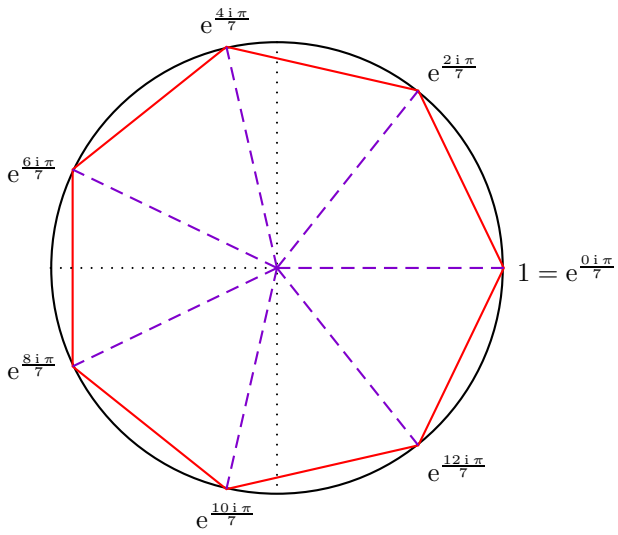


Figure 6.3 – Répartition des racines de l'unité sur le cercle trigonométrique

Proposition 6.3.4
Soit $k \in [\![1, n-1]\!]$. *Alors* $\sum_{i=0}^{n-1} \omega_k^i = 0$.

En particulier, puisque pour tout $k \in [\![0, n]\!]$, $\omega_k = \omega_1^k$, on obtient :

Corollaire 6.3.5 (somme des racines n-ièmes de l'unité)
Soit $\{\omega_0, \ldots, \omega_{n-1}\}$ *l'ensemble des racines* n*-ièmes de* 1, *alors* $\sum_{k=0}^{n-1} \omega_k = 0$.

Corollaire 6.3.6 (somme des racines n-ièmes de z)
Soit $\{\xi_0, \ldots, \xi_{n-1}\}$ *l'ensemble des racines* n*-ièmes de* z, *alors* $\sum_{k=0}^{n-1} \xi_k = 0$.

Remarque 6.3.7
Ce résultat est un cas particulier des relations entre coefficients et racines d'un polynôme.

III.2 Cas des racines carrées : expression sous forme algébrique

Les racines carrées z peuvent être obtenues par la méthode général décrite ci-dessus, lorsqu'on connaît z sous forme trigonométrique : Si $z = re^{i\theta}$, z possède deux racines carrées :

$$z_1 = \sqrt{r}e^{i\frac{\theta}{2}} \qquad \text{et} \qquad z_2 = -\sqrt{r}e^{i\frac{\theta}{2}}.$$

Dans le cas particulier des racines carrées, on dispose également d'une méthode permettant d'obtenir facilement l'expression algébrique des racines carrées de z lorsque z est donné lui-même sous forme algébrique.

Méthode 6.3.8 (recherche des racines carrées sous forme algébrique)
Soit $z = a + ib$ un nombre complexe sous forme algébrique ($a, b \in \mathbb{R}$). Pour trouver les racines carrées sous forme algébrique :

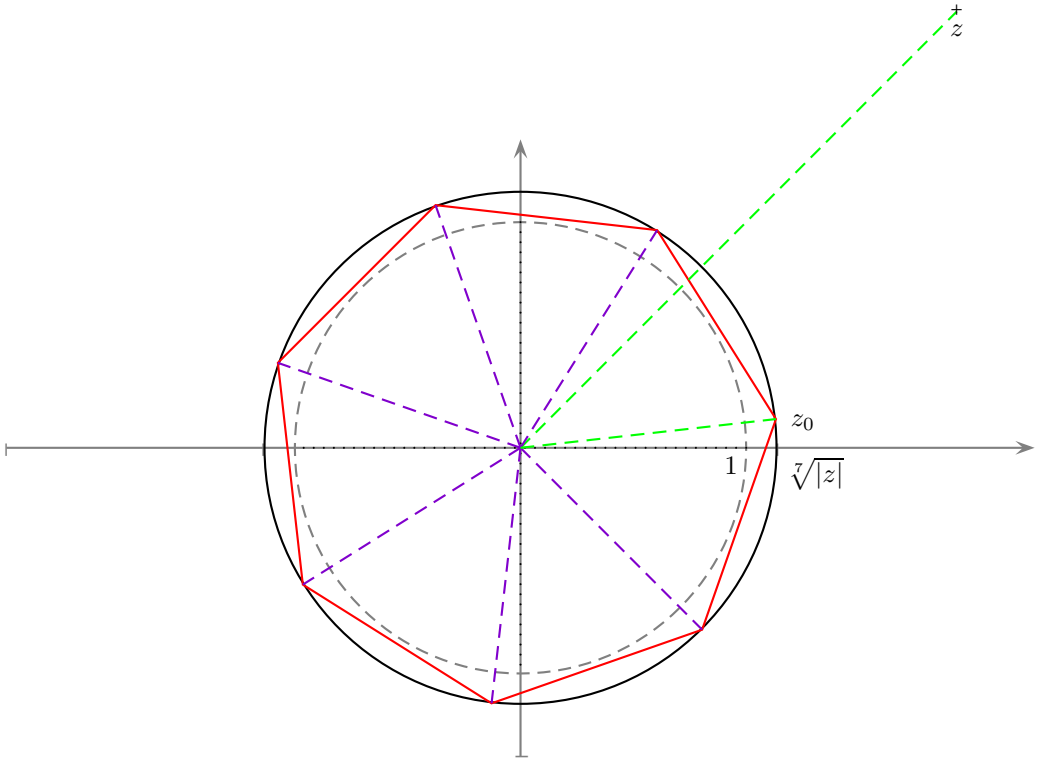


FIGURE 6.4 – Répartition des racines de z dans le plan complexe

1. Considérer une racine $z' = c + \mathrm{i}\, d$
2. Identifier les parties imaginaires et réelles dans l'égalité $(z')^2 = z$: en retenir essentiellement la valeur de $c^2 - d^2$ et le signe de cd.
3. Donner l'égalité des modules de $(z')^4$ et de z^2. Cela donne la valeur de $c^2 + d^2$.
4. Résoudre le système en c^2 et d^2 donné par les équations ci-dessus.
5. Des quatre solutions pour le couple (c, d), garder les deux seules qui donnent le bon signe de cd.

On peut aussi s'en sortir sans utiliser l'égalité des modules, en constatant que l'étape 2 donne la valeur de la somme et du produit de c^2 et $-d^2$, donc une équation du second degré dont ces réels sont les solutions.

Exemple 6.3.9

1. Rechercher les racines carrées de $3 + 5\,\mathrm{i}$.
2. Trouver les solutions de l'équation du second degré : $(2 + \mathrm{i})z^2 - \mathrm{i}\, z + 1 = 0$

La méthode de résolution ci-dessus montre que les racines (réelles ou complexes) d'un polynôme de degré 2 peuvent être exprimées à l'aide de radicaux (*i.e.* les parties réelles et imaginaires peuvent être exprimées à l'aide des 4 opérations usuelles à partir des nombres rationnels, des coefficients de l'équation, et des fonctions « racine » définies sur $\mathbb{R}_+$, ici la racine carrée).

Note Historique 6.3.10

- La résolution d'équations polynomiales par radicaux a motivé une part importante de la recherche mathématique, jusqu'à ce que Niels Abel prouve l'impossibilité de résoudre l'équation général du 5-ième degré par radicaux. Peu de temps après, Évariste Galois élucide complètement le problème, dans un mémoire rédigé peu avant sa mort prématurée en 1832, et dans une lettre rédigée à la hâte à un ami, la veille du duel qui

devait lui être fatal (il avait alors 20 ans). Dans ce mémoire, on y trouve en particulier les balbutiements de la théorie des groupes.
- Carl Friedrich Gauss montre que les racines de $X^n - 1$ (donc les racines n-ièmes de l'unité), peuvent s'exprimer par radicaux si n est premier.
- Il va plus loin, en montrant que si n est un entier premier de la forme $2^{2^k} + 1$, alors les solutions peuvent s'exprimer sous forme de radicaux carrés. Ce résultat amène la constructibilité à la règle et au compas du pentagone (déjà connu depuis bien longtemps), de l'heptadécagone, *i.e.* le polygone à 17 côtés (Gauss en donne une construction) puis des polygônes à 257 et 65537 côtés. On ne connaît pas à ce jour d'autre nombre premier de la forme $2^{2^k} + 1$ (nombres de Fermat). On ne sait pas s'il y en a d'autres.
- Pierre-Laurent Wantzel montre la réciproque en 1837 : les seuls polygônes constructibles sont les polygônes dont le nombre de côtés est un nombre premier de la forme $2^{2^k} + 1$, ou des nombres ayant comme uniques facteurs (qui doivent être simples) ces nombres premiers ou 2 (en multiplicité quelconque). Ce théorème est connu sous le nom de théorème de Gauss-Wantzel.

IV Nombres complexes et géométrie

Nous terminons cette étude des nombres complexes par un bref aperçu de l'efficacité de l'utilisation des nombres complexes pour l'étude de la géométrie du plan. Nous rappelons que, par la construction que nous avons donnée, $\mathbb{C}$ s'identifie au plan $\mathbb{R}^2$. Nous rappelons :

Définition 6.4.1 (affixe)

1. L'affixe d'un point $(a, b) \in \mathbb{R}^2$ est le complexe $z = a + \mathrm{i}\, b$.
2. L'affixe d'un vecteur $\overrightarrow{u} = \begin{pmatrix} a \\ b \end{pmatrix}$ de $\mathbb{R}^2$ est le complexe $a + \mathrm{i}\, b$.

On commence par traduire sous forme complexe certaines propriétés géométriques :

Proposition 6.4.2 (affixe d'un vecteur défini par un bipoint)

Soit A et B deux points d'affixe z_A et z_B. Alors l'affixe du vecteur $\overrightarrow{AB}$ est $z_B - z_A$

Proposition 6.4.3 (norme d'un vecteur)

Soit $\overrightarrow{u}$ un vecteur de $\mathbb{R}^2$ d'affixe z. Alors $\|\overrightarrow{u}\| = |z|$.

Proposition 6.4.4 (traduction de l'alignement, du produit scalaire, de l'orthogonalité)

1. *Soit $\overrightarrow{u}$ et $\overrightarrow{v}$ deux vecteurs de $\mathbb{R}^2$ d'affixes z_u et z_v. Alors $\overrightarrow{u}$ et $\overrightarrow{v}$ sont colinéaires si et seulement si* $\mathrm{Im}(z_u\overline{z_v}) = 0$.
2. *Soit A, B et C trois points distincts de $\mathbb{R}^2$ d'affixe z_A, z_B et z_C. Alors A, B et C sont alignés si et seulement si* $\mathrm{Im}((z_C - z_A)(\overline{z_C} - \overline{z_B})) = 0$.
3. *Soit $\overrightarrow{u}$ et $\overrightarrow{v}$ deux vecteurs de $\mathbb{R}^2$ d'affixes z_u et z_v. Alors le produit scalaire (usuel) de $\overrightarrow{u}$ et $\overrightarrow{v}$ est donné par :*
$$\langle \overrightarrow{u}, \overrightarrow{v} \rangle = \mathrm{Re}(z_u\overline{z_v}).$$
4. *En particulier, $\overrightarrow{u}$ et $\overrightarrow{v}$ sont orthogonaux si et seulement si* $\mathrm{Re}(z_u\overline{z_v}) = 0$.

Proposition 6.4.5 (interprétation géométrique de $\frac{b-a}{c-a}$.)

Soit a, b et c trois complexes, et A, B et C les points de $\mathbb{R}^2$ d'affixe a, b et c. Alors

$$\arg\left(\frac{b-a}{c-a}\right) = (\overrightarrow{AC}, \overrightarrow{AB})$$

Enfin, les transformations usuelles du plan peuvent être traduites par des fonctions simples de $\mathbb{C}$ dans $\mathbb{C}$, ce qui simplifie souvent leur étude ou leur utilisation.

Proposition 6.4.6 (Interprétation complexe des transformations usuelles du plan)

1. *Soit $\overrightarrow{u}$ un vecteur du plan, d'affixe z_u. La translation de vecteur $\overrightarrow{u}$ correspond dans $\mathbb{C}$ à la fonction $z \mapsto z + z_u$.*
2. *Soit A un point du plan, d'affixe z_A, et θ un réel. La rotation de centre A et d'angle θ (dans le sens trigonométrique, ou direct) correspond dans $\mathbb{C}$ à la fonction $z \mapsto z_A + e^{i\,\theta}(z - z_A)$.*
3. *Soit A un point du plan, d'affixe z_A, et λ un réel. L'homothétie de centre A et de rapport λ correspond dans $\mathbb{C}$ à la fonction $z \mapsto z_A + \lambda(z - z_A)$.*
4. *Soit D une droite passant par le point A d'affixe z_A, et de vecteur directeur unitaire $\overrightarrow{u}$, d'affixe z_U. La symétrie orthogonale d'axe D est donnée par la fonction $z \mapsto z_u^2(\overline{z} - \overline{z_A}) + z_A$*

Remarquez dans le 4 qu'on a supposé que $\overrightarrow{u}$ est unitaire, donc que z_u est de la forme $e^{i\,\theta}$. Ainsi, la multiplication par $\overline{z_u}$ correspond à une rotation qui nous ramène à un axe horizontal. Si cet axe passe par 0, la symétrie correspond alors à la conjugaison (ce qui fait partir la barre du coefficient multiplicatif z_u).
Attention, le caractère unitaire de $\overrightarrow{u}$ est important ici.

Proposition 6.4.7 (compositions de rotations et translations)

Toute transformation obtenue par composition de translations et de rotations (d'angle total θ) est :

- *soit une rotation d'angle θ, si $\theta \not\equiv 0 \mod 2\pi$*
- *soit une translation, si $\theta \equiv 0 \mod 2\pi$.*

Proposition 6.4.8 (composition de rotations, translations et homothéties)

Toute transformation obtenue par composition de translations, de rotations (d'angle total θ), et d'homothéties (dont le produit des rapports est λ) est

- *soit la composition d'une rotation d'angle θ et d'une homothétie de rapport λ si $\theta \not\equiv 0 \mod 2\pi$*
- *soit une homothétie de rapport λ si $\theta \equiv 0 \mod 2\pi$ et $\lambda \neq 1$*
- *soit une translation si $\theta \equiv 0 \mod 2\pi$ et $\lambda = 1$.*

La propriété commune de toutes les transformations étudiées ici est qu'elles conservent les longueurs (rotations, translations), ou qu'elles multiplient toutes les longueurs par un même coefficient (homothéties). Elles font donc partie d'une même famille de fonctions que nous définissons ci-dessous.

Définition 6.4.9 (isométries et similitudes)

Soit $F : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ une application.

1. On dit que F est une isométrie affine si F conserve les longueurs, donc si pour tout $(A, B) \in (\mathbb{R}^2)^2$, $\|f(A)f(B)\| = \|AB\|$.
2. On dit que F est une isométrie vectorielle si F est une isométrie affine telle que $F(O) = O$, où $O = (0, 0)$.

3. On dit que F est une similitude affine s'il existe $\lambda \in \mathbb{R}_+^*$ tel que pour tout $(A,B) \in (\mathbb{R}^2)^2$, $\|f(A)f(B)\| = \lambda \|AB\|$.
4. On dit que F est une similitude vectorielle si F est une similitude affine telle que $F(O) = O$.

Lemme 6.4.10

1. *Une isométrie tansforme un triangle en un triangle semblable*
2. *En particulier, une isométrie conserve les angles*
3. *Notamment, une isométrie conserve l'alignement et l'orthogonalité.*
4. *Une similitude conserve les angles, donc aussi l'alignement et l'orthogonalité.*

Lemme 6.4.11

1. *Une similitude affine (donc aussi une isométrie affine) est entièrement déterminée par l'image de 3 points non alignés.*
2. *Une similitude vectorielle (donc aussi une isométrie vectorielle) est entièrement déterminée par l'image des points* $(0,1)$ *et* $(1,0)$ *; l'application* $f : \mathbb{C} \mapsto \mathbb{C}$ *est donc entièrement déterminée par la connaissance de* $f(1)$ *et* $f(\mathrm{i})$.

Proposition 6.4.12 (Caractérisation des isométries et des similitude vectorielles)

1. *Les isométries vectorielles de* $\mathbb{R}^2$ *correspondent exactement aux applications complexes* $f : z \mapsto az$ *ou* $f : z \mapsto a\overline{z}, \quad a \in \mathbb{U}$.
2. *Les similitudes vectorielles de* $\mathbb{R}^2$ *correspondent exactement aux applications complexes* $f : z \mapsto az$ *ou* $f : z \mapsto a\overline{z}, \quad a \in \mathbb{C}^*$.

Définition 6.4.13 (isométrie, similitude directe, indirecte)

- Une isométrie (*resp.* similitude) vectorielle de type $z \mapsto az$ est appelée isométrie (*resp.* similitude) directe. Il s'agit des rotations (*resp. homothéties-rotations*).
- Une isométrie (*resp.* similitude) vectorielle de type $z \mapsto a\overline{z}$ est appelée isométrie (*resp.* similitude) indirecte. Il s'agit des symétries axiales (*resp* homothéties-symétries)

Proposition 6.4.14 (Caractérisation des isométries et des similitude affines directes)

1. *Les isométries affines de* $\mathbb{R}^2$ *correspondent exactement aux applications complexes* $f : z \mapsto az + b$ *ou* $f : z \mapsto a\overline{z} + b, \quad a \in \mathbb{U}, b \in \mathbb{C}$.
2. *Les similitudes affines de* $\mathbb{R}^2$ *correspondent exactement aux applications complexes* $f : z \mapsto az + b$ *ou* $f : z \mapsto a\overline{z} + b, \quad a \in \mathbb{C}^*, b \in \mathbb{C}$.

On définit de même que dans le cas vectoriel les isométries et similitudes affines directes et indirectes.

Exemples 6.4.15

1. Une similitude affine directe $z \mapsto az + b$ est la composition d'une rotation et d'une homothétie vectorielles, suivies d'une translation.
2. Une similitude directe est soit une rotation affine, soit une homothétie affine, soit une translation, soit une composée de deux tranformations de ce type exactement ; s'il s'agit d'une composée d'une homothétie et d'une rotation, on peut s'arranger pour les choisir de même centre.

3. À quelles isométries correspondent les applications $z \mapsto \overline{z}$ et $z \mapsto \mathrm{i}\,\overline{z}$?