Matthieu Garcin
Younes Kchia

MATHS : l'entrée en prépa sans faux pas

Cours et exercices corrigés
pour apprivoiser les mathématiques
des classes préparatoires

ellipses

Références sciences

Maths : l'entrée en prépa sans faux pas

Cours et exercices corrigés pour apprivoiser les mathématiques des classes préparatoires

Matthieu Garcin
Younes Kchia

ellipses

Avant-propos

Ce livre propose un cours et des exercices corrigés de mathématiques aux élèves de terminale scientifique motivés et qui veulent préparer au mieux la suite de leurs études. Il cherche à enseigner une façon rigoureuse de faire des mathématiques tout en utilisant des outils facilement compréhensibles pour des élèves de terminale. Le ton et l'esprit sont ceux d'un apprentissage gradué, parfois ludique, parfois proche de l'exhortation, encourageant le lecteur à s'adapter aux exigences des études supérieures : à ce titre, la succession des chapitres du livre suit une progression marquée, puisque la rigueur, le nombre et la densité des théorèmes sont dignes de la terminale dans le premier chapitre et évoluent au fil des pages vers une approche semblable à celle des études supérieures.

Ce livre aborde la logique (Chapitre 1), pierre indispensable à l'élaboration de tout raisonnement mathématique. Puis les auteurs ont choisi de traiter de thèmes qui permettent au lecteur d'établir un lien avec ses connaissances acquises au lycée, d'une part, et, d'autre part, de se familiariser avec des notions que le bachelier découvre en classes préparatoires et dont le caractère peut déconcerter au premier abord, mais que les auteurs ont veillé à bien expliquer, afin de rassurer le futur élève de classes préparatoires scientifiques. Ainsi, cet ouvrage contient des chapitres sur la théorie des ensembles (Chapitre 2), sur l'algèbre (Chapitre 3), sur les nombres réels (Chapitre 4) et sur les suites réelles (Chapitre 5). Ce choix des thèmes abordés ne reprend pas exhaustivement le programme de classes préparatoires : ce n'est pas le but de ce livre, dans lequel est simplement opérée une sélection de notions permettant au lecteur, au prix d'un effort modéré, d'avoir un rapide et fidèle aperçu de ce qu'est l'enseignement des mathématiques en classes préparatoires. Par conséquent, plutôt que de traiter tout le programme en accéléré, les auteurs ont préféré se concentrer sur un choix varié de chapitres et ont mis l'accent sur la qualité des démonstrations, sachant que ce point est primordial en classes préparatoires. Ils ont également cherché à développer l'intuition du lecteur en proposant de nombreux exemples et contre-exemples, soulignant la subtilité des théorèmes présentés.

Par ailleurs, les auteurs ont pensé bon de conclure cet ouvrage avec quelques pages de conseils au lecteur pour aborder sereinement ses débuts dans les études supérieures. Ces conseils s'appuient sur des avis recueillis auprès de plusieurs anciens étudiants – qu'ils soient ici remerciés.

Ce livre, pensé pour les élèves désireux d'entrer en classes préparatoires scientifiques, peut naturellement aussi intéresser tout élève de terminale voulant commencer des études supérieures scientifiques avec une forte composante en mathématiques, quelles qu'elles soient.

Matthieu Garcin tient à remercier Armelle G. pour son appui enthousiaste et François L. pour ses relectures.

Younes Kchia tient à remercier Mariem B. pour ses soutien et contributions à la réalisation de ce livre.

Table des matières

Chapitre 1

Logique

Nous commençons cet ouvrage par un chapitre sur la logique, laquelle définit la manière de raisonner en mathématiques. En effet, le discours régissant les objets mathématiques, c'est-à-dire les quantités et les ordres [1], doit respecter une certaine norme pour être compris de tous sans ambiguïté. Ceci justifie la position de ce chapitre en tête de livre. Ne cédez donc pas à la tentation de parcourir les autres chapitres avant d'avoir lu celui-ci en entier : sauter le présent chapitre ne vous éclairera pas plus vite sur ce que sont les mathématiques en prépa mais, au contraire, cela vous fera découvrir des concepts énoncés dans une langue que vous connaissez encore mal !

Pour saisir l'importance de la logique, il faut aussi que vous compreniez qu'un mathématicien, plus que tout autre scientifique, n'admet aucune assertion pour juste s'il n'est pas capable de prouver lui-même et de manière indiscutable qu'elle l'est. Or, le seul moyen de rendre un raisonnement indiscutable est de l'écrire dans une langue universellement compréhensible, avec des codes universellement admis, bref de respecter la logique. Bon, il ne faut pas que cet avertissement vous effraie plus que de raison : nous allons vous aider à apprendre progressivement la rigueur et même à l'aimer, puisque c'est le seul moyen de ne pas écrire des choses fausses. Présentée ainsi, la logique est plutôt attrayante, non ? Alors, commençons ce cours sans tarder !

Ah ! Encore un détail... Notez que, dans ce chapitre, vous trouverez certains exemples dont le titre est suivi d'une étoile ($\star$). Cela signifie que l'énoncé

1. C'est ainsi que *le Petit Robert* définit les mathématiques. On le comprend bien si l'on s'en tient à l'exemple des symboles d'égalité et d'inégalité, qui établissent un lien entre des objets, les quantifiant et les ordonnant, quels que soient ces objets : nombres, ensembles, suites et autres objets construits par une abstraction plus ou moins poussée.

peut dérouter les lecteurs qui ne connaissent pas encore certaines notions qui seront approfondies dans la suite du livre mais qui sont en principe au programme de terminale (au moins pour l'intuition). Il est en effet délicat de vous expliquer la logique en restreignant le propos à des exemples déconnectés des notions mathématiques que nous souhaitons vous faire découvrir dans cet ouvrage. Si ces exemples plus compliqués vous semblent trop obscurs, passez-les et réessayez de les lire quand vous aurez fini le livre ! Quoi qu'il en soit, des exemples plus simples vous seront aussi proposés pour bien comprendre chacune des notions présentées dans le présent chapitre.

1.1 Connecteurs logiques

En logique binaire, une assertion peut prendre deux valeurs : vrai ou faux. Pour simplifier, si une assertion A est vraie nous noterons $A \equiv V$ et si elle est fausse $A \equiv F$.

Exemple 1.1 *Les assertions considérées peuvent être de toutes sortes. Par exemple, nous pouvons noter A l'assertion « juillet est le mois juste après le mois d'avril ». Naturellement,* $A \equiv F$ *: pas besoin d'avoir fait d'études de mathématiques pour le savoir. Notons maintenant B une autre assertion, au contenu plus mathématique :* $1 - 1 = 0$. *Alors* $B \equiv V$.

Les assertions sont les éléments de base de tout raisonnement mathématique. Elles en sont même l'objet, dans le sens où notre objectif est de construire des assertions à partir de la connaissance d'autres assertions. Cela suppose donc que l'on sache manipuler plusieurs assertions afin de les transformer, d'intégrer les différentes informations qu'elles recèlent jusqu'à atteindre une nouvelle assertion qui répond à la question que l'on se pose. Dans l'exemple suivant, nous avons deux assertions en hypothèse et nous cherchons à établir une troisième assertion.

Exemple 1.2 ($\star$) *Vous connaissez l'ensemble des entiers naturels,* $\mathbb{N}$, *et l'ensemble des réels,* $\mathbb{R}$. *Supposez que l'on a également la connaissance des deux assertions suivantes :*

- *assertion A : «* $\mathbb{N}$ *n'a pas de borne supérieure finie » ;*
- *assertion B : « entre deux nombres entiers il existe une infinité de nombres réels ».*

La question que l'on se pose, et que l'on veut résoudre uniquement avec les deux assertions A et B, est la suivante : l'ensemble des nombres réels non entiers, $\mathbb{R}\backslash\mathbb{N}$, *admet-il une borne supérieure ? La réponse à cette question est négative et découle de l'utilisation conjointe des assertions A et B. Si nous notons P l'assertion*[1] *« l'ensemble des*

1. On peut indifféremment parler d'assertion ou de proposition, laquelle a ici prêté son initiale dans notre notation P.

nombres réels non entiers admet une borne supérieure finie », notre objectif est ainsi de prouver que $P \equiv F$.

Alors, voyez-vous pourquoi $P \equiv F$ dans cet exemple ? Tentez d'y répondre en manipulant les deux assertions A et B de toutes les manières possibles ! Ensuite, comparez votre travail avec le raisonnement détaillé ci-après.

Exemple 1.3 ($\star$) *Supposons que P soit vraie, c'est-à-dire que l'ensemble, noté $\mathbb{R}\backslash\mathbb{N}$, des nombres réels non entiers admette une borne supérieure finie. Alors, par l'assertion A*[1]*, il existe deux nombres entiers distincts, n et m, avec $n < m$, qui majorent $\mathbb{R}$. Par l'assertion B, il existe un réel non entier, x, tel que $n < x < m$. Tout nombre réel non entier y est inférieur ou égal à son majorant n, $y \leq n < x$, donc x n'appartient pas à l'ensemble des nombres réels non entiers, ce qui est contradictoire avec la définition de x. Ainsi, l'hypothèse P au début du raisonnement est fausse et nous pouvons maintenant affirmer que l'ensemble des nombres réels non entiers n'admet pas de borne supérieure finie.*

Très bien vous dites-vous, ce raisonnement est compréhensible et n'est rien d'autre qu'un raisonnement classique de mathématiques dans lequel la connaissance de ce qu'est une assertion n'est pas nécessaire. Certes, ce raisonnement est très classique, mais il abrège une série d'assertions, qui sont implicitement utilisées. Dans l'exemple suivant, on détaille toutes les assertions par lesquelles le raisonnement nous a fait passer. Attention, il est préférable d'écrire la preuve abrégée, comme dans l'exemple 1.3, car la décomposition de toutes les assertions est vraiment fastidieuse. Heureusement, c'est le seul exemple de ce livre où vous lirez autant de détails !

Exemple 1.4 ($\star$) *Rappelons que P est l'assertion : « l'ensemble des nombres réels non entiers admet une borne supérieure finie ». Nous avons montré dans l'exemple 1.3 que P était fausse. Nous pouvons maintenant détailler un peu plus les étapes du raisonnement en faisant la liste des assertions intermédiaires que nous avons implicitement utilisées :*

- *Assertion C : « si P est vraie, alors $\mathbb{R}\backslash\mathbb{N}$ admet un majorant entier », à cause de l'assertion A.*
- *Assertion D : « si $\mathbb{R}\backslash\mathbb{N}$ admet un majorant entier, alors $\mathbb{R}\backslash\mathbb{N}$ admet deux majorants entiers distincts », à cause de l'assertion A.*
- *Assertion E : « si $\mathbb{R}\backslash\mathbb{N}$ admet deux majorants entiers distincts, alors il y a une infinité de nombres réels entre ces deux majorants », à cause de l'assertion B.*
- *Assertion F, obtenue en ne gardant qu'une partie de l'information contenue dans l'assertion E : « si $\mathbb{R}\backslash\mathbb{N}$ admet deux majorants entiers distincts, alors il y a un nombre réel non entier strictement supérieur au plus petit de ces deux majorants ».*
- *Assertion G, obtenue en reformulant l'assertion F : « si $\mathbb{R}\backslash\mathbb{N}$ admet deux majorants entiers distincts, alors il y a un nombre réel non entier majorant $\mathbb{R}\backslash\mathbb{N}$ sans y appartenir ».*

1. Nous reprenons les assertions A et B de l'exemple 1.2.

– *Assertion H, obtenue en synthétisant la chaîne causale mise en évidence dans les assertions C, D et G : « si P est vraie, alors il y a un nombre réel non entier majorant $\mathbb{R}\backslash\mathbb{N}$ sans y appartenir ».*

Vous constatez que l'assertion H est construite de la manière suivante : si P, alors H' [1]. Or, H' est en contradiction avec P, donc on ne peut pas avoir P vraie, ce qui, par l'assertion H, entraînerait H' vraie. Par conséquent, $P \equiv F$ et cela répond à la question que nous nous posions : l'ensemble des nombres réels non entiers n'admet pas de borne supérieure finie.

Nous vous avions prévenu : le raisonnement de l'exemple précédent est très détaillé. Le but est de vous faire comprendre qu'il ne faut jamais s'éloigner des assertions dont on dispose et qu'il faut savoir les utiliser à bon escient et ne pas faire confiance qu'à une compréhension intuitive, dans laquelle l'idée générale des assertions prévaudrait sur l'utilisation précise de l'information qu'elles contiennent. En pratique, vous ne rédigerez pas autant vos raisonnements, sauf situation délicate, et vous vous contenterez d'écrire ce qui suffirait à convaincre une personne suffisamment intelligente pour comprendre immédiatement mais en faisant en sorte qu'elle n'ait pas à faire d'effort de raisonnement. Donc soyez rassurés : nous préférons aussi le raisonnement abrégé de l'exemple 1.3 !

Vous êtes habitué à faire des raisonnements abrégés, donc une étude de la logique peut vous sembler inutile. Néanmoins, une connaissance approfondie des connecteurs logiques (c'est-à-dire des différentes opérations que l'on peut faire sur des assertions) permet d'une part de ne pas se laisser aller à une erreur de raisonnement et d'autre part d'assimiler des connecteurs plus subtils et plus efficaces que ceux que l'on utilise inconsciemment.

1.1.1 Négation

Le premier connecteur à connaître est la négation. Notez que la définition d'un connecteur passe par les tables de vérité qui, à la valeur d'une assertion (V ou F), associent la valeur de l'assertion obtenue en appliquant le connecteur à l'assertion de base. Si cette phrase est un peu sibylline, lisez la définition suivante, qui devrait vous éclairer sur l'usage des tables de vérité.

Définition 1.1 *Soit A une assertion. La négation de A est notée $non(A)$ ou $\neg A$ et est définie par la table de vérité suivante :*

A	$non(A)$
V	F
F	V

1. Plus précisément, cela signifie : si P est vraie, alors H' est vraie.

qu'il faut comprendre ainsi : si A est vrai, alors $non(A)$ est faux; si A est faux, alors $non(A)$ est vrai.

Il nous semble inutile d'épiloguer sur le sens profond de la négation d'une assertion dans la mesure où celui-ci correspond à l'intuition : la négation d'une assertion affirme son contraire. Quelques exemples devraient éclairer ceux qui ont lu trop rapidement ce qui précède.

Exemple 1.5 *La négation de l'assertion « je suis plus âgé que toi » est « je suis plus jeune que toi ou bien nous avons le même âge ». Mais faites attention : la négation de l'assertion « ce livre est bleu » n'est pas « ce livre est rouge » ou « ce livre est blanc », mais simplement « ce livre n'est pas bleu » ! Dans un registre plus mathématique, pour $x \in \mathbb{R}$, on a $[non(x = 1)] \equiv [x \neq 1]$. Nous pouvons également écrire $[non(x < 1)] \equiv [x \geq 1]$.*

On peut déduire une propriété naturelle de la négation : la négation de la négation d'une assertion est cette assertion.

Proposition 1.1 *Soit A une assertion. Alors, $non(non(A)) \equiv A$, ce qui signifie que*

A	$non(non(A))$
V	V
F	F

Preuve. La preuve d'une telle proposition consiste à définir la table de vérité du connecteur de la double négation. Nous pouvons le faire dans un tableau ou simplement l'écrire avec du texte, comme nous allons le faire, ce qui revient au même :
- Si $A \equiv V$, alors $non(A) \equiv F$ par définition de la négation, puis, toujours par définition de la négation, $non(non(A)) \equiv V$.
- Si $A \equiv F$, alors $non(A) \equiv V$ par définition de la négation, puis, toujours par définition de la négation, $non(non(A)) \equiv F$.

V et F étant les deux seules valeurs possibles de l'assertion A, nous avons démontré que $non(non(A)) \equiv A$. ■

1.1.2 Disjonction et conjonction

Après avoir défini dans le paragraphe précédent un connecteur appliqué à une seule assertion, nous allons maintenant voir des connecteurs appliqués à deux assertions : la disjonction et la conjonction. Là encore, la définition passe par la table de vérité, laquelle n'aura plus seulement deux lignes (V et F pour l'assertion de départ), mais quatre lignes, ce qui correspond à tous les couples possibles pour les deux assertions de départ : (V,V), (V,F), (F,V) et (F,F).

Définition 1.2 *A et B sont deux assertions. La* **disjonction** *de A et B est notée [A ou B] et est définie par :*

A	B	A *ou* B
V	V	V
V	F	V
F	V	V
F	F	F

La disjonction est aussi communément appelée le *ou* logique. Concrètement, A *ou* B est vrai dès lors que l'une au moins des deux assertions est vraie. Définissons maintenant la notion cousine de la disjonction qu'est la conjonction :

Définition 1.3 *A et B sont deux assertions. La* **conjonction** *de A et B est notée [A et B] et est définie par :*

A	B	A *et* B
V	V	V
V	F	F
F	V	F
F	F	F

La conjonction est le *et* logique. A *et* B est vrai si à la fois A et B sont vrais. On pourrait aussi dire que A *et* B est faux dès lors que l'une au moins des deux assertions est fausse. Cela permet d'approcher la phrase que nous avons formulée pour expliquer la disjonction et, par conséquent, d'établir un lien entre conjonction et disjonction, lien qui est clair si l'on compare les deux tables de vérités.

Proposition 1.2 *Soient A et B deux assertions. Alors,*

$$\begin{cases} non(A \text{ ou } B) & \equiv & non(A) \text{ et } non(B) \\ non(A \text{ et } B) & \equiv & non(A) \text{ ou } non(B). \end{cases}$$

Preuve. Nous démontrons la première ligne et nous vous laissons ensuite démontrer vous-même la deuxième pour vous entraîner, sachant que la démarche est la même. Comme on l'a déjà écrit, ce genre de démonstration revient à construire la table de vérité de l'assertion étudiée. Cela peut être fait dans un tableau ou en écrivant un texte détaillant chaque ligne du tableau.

Nous pouvons encore aller un peu plus vite en ne détaillant que le cas vrai (le cas faux suivant implicitement comme nous allons l'expliquer dans quelques lignes) en écrivant que $non(A\ ou\ B)$ est vrai si et seulement si $(A\ ou\ B)$ est faux, puis en poursuivant le raisonnement comme nous allons le faire dans quelques lignes. Précisons d'abord que cette phrase signifie que $non(A\ ou\ B)$ est vrai si $(A\ ou\ B)$ est faux et que $non(A\ ou\ B)$ est faux si $(A\ ou\ B)$ est vrai. Ainsi, en écrivant « si et seulement si », on écrit une phrase qui correspond à deux cas de la table de vérité, jouant sur le fait que la logique que nous étudions est une logique binaire et que ce qui n'est pas vrai est donc nécessairement faux. Reprenons donc le raisonnement : $non(A\ ou\ B)$ vrai

- si et seulement si $(A\ ou\ B)$ faux ;
- si et seulement si A faux et B faux (si l'on se reporte à la définition de la disjonction) ;
- si et seulement si $non(A)$ vrai et $non(B)$ vrai ;
- si et seulement si $[non(A)\ et\ non(B)]$ vrai.

■

Exemple 1.6 *La négation de l'assertion « ce livre est bleu et je l'ai lu » est « ce livre n'est pas bleu ou je ne l'ai pas lu ». La négation de l'assertion « 10 est un nombre impair ou positif » est « 10 est un nombre pair et négatif », ce qui est notoirement faux. En revanche, la négation de l'assertion « 10 est un nombre impair <u>et</u> positif » est « 10 est un nombre pair <u>ou</u> négatif », ce qui, en l'occurrence, est vrai, car 10 est pair.*

Nous n'avons pas encore mentionné d'autres propriétés qui vont de soi si l'on s'en tient à la définition par les tables de vérité, raison pour laquelle nous n'avons pas rédigé de preuve pour la proposition suivante.

Proposition 1.3 *Soient A, B et C trois assertions. La disjonction et la conjonction sont commutatives, ce qui signifie que*

$$\begin{cases} A\ ou\ B \equiv B\ ou\ A \\ A\ et\ B \equiv B\ et\ A. \end{cases}$$

La disjonction et la conjonction sont associatives, ce qui signifie que

$$\begin{cases} (A\ ou\ B)\ ou\ C \equiv A\ ou\ (B\ ou\ C) \\ (A\ et\ B)\ et\ C \equiv A\ et\ (B\ et\ C). \end{cases}$$

Nous finissons cette partie sur la disjonction et la conjonction par une dernière propriété bien utile qui permet d'écrire, à partir de trois assertions et des deux connecteurs *ou* et *et*, une seule grosse assertion, en manipulant correctement les parenthèses, qui sont les marqueurs de la priorité des opérations.

Proposition 1.4 *Soient A, B et C trois assertions. La disjonction et la conjonction sont distributives, ce qui signifie que*

$$\begin{cases} A \textit{ et } (B \textit{ ou } C) \equiv (A \textit{ et } B) \textit{ ou } (A \textit{ et } C) \\ A \textit{ ou } (B \textit{ et } C) \equiv (A \textit{ ou } B) \textit{ et } (A \textit{ ou } C). \end{cases}$$

Preuve. Démontrons la première ligne en construisant, à partir des propositions et définitions précédentes, la table de vérité des deux assertions de part et d'autre du signe $\equiv$. Si ces tables sont identiques, alors on pourra affirmer que les deux assertions sont équivalentes. Comparons donc la dernière colonne de

A	B	C	B *ou* C	A *et* $(B$ *ou* $C)$
V	V	V	V	V
V	V	F	V	V
V	F	V	V	V
V	F	F	F	F
F	V	V	V	F
F	V	F	V	F
F	F	V	V	F
F	F	F	F	F

avec la dernière colonne de

A	B	C	A *et* B	A *et* C	$(A$ *et* $B)$ *ou* $(A$ *et* $C)$
V	V	V	V	V	V
V	V	F	V	F	V
V	F	V	F	V	V
V	F	F	F	F	F
F	V	V	F	F	F
F	V	F	F	F	F
F	F	V	F	F	F
F	F	F	F	F	F

Elles sont bien identiques, ce qui établit l'équivalence entre A *et* $(B$ *ou* $C)$ et $(A$ *et* $B)$ *ou* $(A$ *et* $C)$.

Vous pouvez vous tester et tenter de démontrer l'autre équivalence. Faites-le. Ensuite, revenez au livre et découvrez une autre manière de la prouver, laquelle utilise la première équivalence prouvée. En effet, en remplaçant A, B et C par leurs négations respectives, la première équivalence s'écrit

$$\begin{aligned} & \textit{non}(A) \textit{ et } (\textit{non}(B) \textit{ ou } \textit{non}(C)) \\ & \equiv (\textit{non}(A) \textit{ et } \textit{non}(B)) \textit{ ou } (\textit{non}(A) \textit{ et } \textit{non}(C)). \end{aligned}$$

Si nous prenons la négation des deux assertions de part et d'autre du signe $\equiv$, l'équivalence logique est conservée et on obtient

$$\begin{aligned}&non[non(A)\ et\ (non(B)\ ou\ non(C))]\\ &\equiv non[(non(A)\ et\ non(B))\ ou\ (non(A)\ et\ non(C))].\end{aligned}$$

En utilisant la Proposition 1.2, cela s'écrit

$$\begin{aligned}&non(non(A))\ ou\ non(non(B)\ ou\ non(C))\\ &\equiv non(non(A)\ et\ non(B))\ et\ non(non(A)\ et\ non(C)),\end{aligned}$$

puis, en utilisant encore une fois la Proposition 1.2,

$$\begin{aligned}&non(non(A))\ ou\ (non(non(B))\ et\ non(non(C)))\\ &\equiv (non(non(A))\ ou\ non(non(B)))\ et\ (non(non(A))\ ou\ non(non(C))).\end{aligned}$$

La Proposition 1.1 permet de simplifier cette expression et d'obtenir précisément celle que nous recherchons.

$$A\ ou\ (B\ et\ C) \equiv (A\ ou\ B)\ et\ (A\ ou\ C).$$

■

Dans la preuve que vous venez de lire, le fait que l'on ne démontre pas la deuxième ligne de l'énoncé en construisant une table de vérité, ce qui peut être fastidieux, mais en utilisant un raisonnement faisant appel à la première équivalence appelle quelques remarques :

- Ce n'est pas une astuce ! Ce que nous voulons vous dire est que vous devez être capable de penser vous-même à faire ce type de raisonnement qui a le mérite d'économiser votre temps. En l'occurrence, quand des assertions sont proches (ces deux formules se ressemblent fortement, non ? Il suffit de remplacer les *ou* par des *et* et *vice versa* pour passer de l'une à l'autre), il y a de fortes chances que la preuve de l'une puisse servir de support à la preuve de l'autre. Ici, connaissant l'impact de la négation sur la disjonction et la conjonction grâce à la Proposition 1.2, il est naturel de commencer le raisonnement comme nous l'avons fait. Au pire, vous avez le droit de réfléchir deux minutes avec un crayon et une feuille de brouillon avant de vous lancer... C'est même recommandé, comme il est recommandé de lire le cours avec ce même crayon et cette même feuille de brouillon et d'essayer de faire vous-même les démonstrations avant de les lire.
- L'autre remarque est à propos de la satisfaction que doit susciter chez vous cette démonstration : vous utilisez explicitement des résultats déjà prouvés par vous à la lecture de ce livre pour construire un nouveau résultat ; autrement dit, vous bâtissez votre connaissance et ce n'est qu'un début.

1.1.3 Implication

Allons un peu plus loin dans le monde des connecteurs logiques. Ce qui précédait correspondait normalement à votre intuition. La suite s'en écartera pour de nombreux lecteurs, car l'usage qui est intuitivement fait du connecteur que nous allons vous présenter est souvent maladroit.

Définition 1.4 *Soient A et B des assertions. L'**implication** de A vers B est notée $A \Rightarrow B$. On peut dire aussi A implique B. Cette assertion est définie par*

$$A \Rightarrow B \equiv non(A) \text{ ou } B.$$

Attention, $A \Rightarrow B$ ne signifie pas A donc B, comme beaucoup aiment à l'écrire. Beaucoup trop nombreux sont les raisonnements où est ainsi mise en exergue une chaîne causale, $A \Rightarrow B \Rightarrow \ldots \Rightarrow Z$, que l'étudiant auteur du raisonnement conclut en affirmant : « donc Z est vrai ». En réalité, cette chaîne causale permet uniquement de dire : « si A est vrai, alors Z est vrai ; mais si A est faux, alors on ne peut rien dire de Z, qui peut être vrai ou faux ». L'étudiant fautif aurait donc dû écrire « or A est vrai donc Z est vrai », ou remplacer la chaîne d'implications par « A est vrai, donc B est vrai, donc... donc Z est vrai ». Et l'on remarque ainsi qu'utiliser des symboles mathématiques ne dispense pas de s'exprimer avec des mots bien choisis. Peut-être l'écriture explicite de la table de vérité de l'implication vous aidera-t-elle à ne pas écrire le genre de bêtises que nous venons de mentionner :

A	B	$A \Rightarrow B$
V	V	V
V	F	F
F	V	V
F	F	V

Si vous regardez bien cette table, elle vous dit bien que si A est vrai, alors il faut que B le soit aussi pour que l'assertion $A \Rightarrow B$ soit vraie. Et elle vous dit également que si A est faux, alors, que B soit vrai ou faux, $A \Rightarrow B$ sera toujours vrai.

Comme pour la disjonction et la conjonction, il existe quelques propriétés ayant trait à l'utilisation conjointe de l'implication et d'autres connecteurs, comme la négation.

Proposition 1.5 *Soient A et B des assertions. Alors,*
- $[non(A \Rightarrow B)] \equiv [A \text{ et } non(B)]$;

- $[A \Rightarrow B] \equiv [non(B) \Rightarrow non(A)]$, *l'assertion* $non(B) \Rightarrow non(A)$ *étant ce que l'on appelle l'implication contraposée de* $A \Rightarrow B$.

Preuve.

- En utilisant successivement la Définition 1.4, puis la Proposition 1.2 et enfin la Proposition 1.1, on obtient

$$\begin{aligned} non(A \Rightarrow B) &\equiv non(non(A) \text{ ou } B) \\ &\equiv non(non(A)) \text{ et } non(B) \\ &\equiv A \text{ et } non(B). \end{aligned}$$

- Pour cette équivalence, nous vous proposons de partir de l'expression la plus compliquée afin de retomber sur l'expression la plus simple. Ainsi, en utilisant la Définition 1.4 puis la Proposition 1.1, cette formule s'écrit

$$\begin{aligned} non(B) \Rightarrow non(A) &\equiv non(non(B)) \text{ ou } non(A) \\ &\equiv B \text{ ou } non(A) \\ &\equiv non(A) \text{ ou } B, \end{aligned}$$

  par commutativité du connecteur de disjonction, comme nous vous l'avons énoncé dans la Proposition 1.3. Or, cette dernière ligne correspond à l'implication $A \Rightarrow B$, par définition. Donc, l'équivalence entre les deux formules est prouvée.

■

Exemple 1.7 *L'implication « s'il neige, alors je skie », signifie qu'il ne neige pas ou que je skie. Cela veut donc bien dire que cette assertion est aussi vraie au mois de décembre qu'au mois d'août : rien n'indique qu'il doive neiger pour que l'implication soit vraie. Cette implication est équivalente à l'assertion suivante : « si je ne skie pas, alors il ne neige pas ». Sa négation est alors : « il neige et je ne skie pas ».*

D'autres propriétés relatives aux implications vous seront présentées dans l'exercice 1.1

1.1.4 Équivalence

Voilà encore un symbole que de nombreux étudiants utilisent à tort et à travers ! Nous n'entrerons pas trop dans le détail des mésusages possibles qui sont semblables à ce que l'on a déjà relevé pour l'implication. Cela est d'ailleurs bien normal, dans la mesure où une équivalence entre deux assertions A et B signifie qu'il y a une implication de A vers B et une implication de B vers A.

Définition 1.5 *Soient A et B deux assertions. L'**équivalence** entre A et B est notée $A \Leftrightarrow B$. Elle est définie par*

$$A \Leftrightarrow B \equiv (A \Rightarrow B) \text{ et } (B \Rightarrow A).$$

En résumé, deux assertions sont équivalentes si elles sont toutes les deux vraies ou si elles sont toutes les deux fausses. Autrement dit, $A \Leftrightarrow B$ revient à affirmer que A est vrai si et seulement si B est vrai. En fin de compte, lorsque nous écrivons $A \equiv B$, nous affirmons simplement que $A \Leftrightarrow B$.

Comme dans les paragraphes précédents, on pourrait étudier de nombreuses formules logiques constituées de plusieurs connecteurs dont des équivalences, mais nous nous contenterons d'évoquer l'équivalence contraposée, notion cousine de l'implication contraposée, comme vous le verrez particulièrement dans la démonstration qui suit le proposition.

Proposition 1.6 *Soient A et B des assertions. Alors,*

$$(A \Leftrightarrow B) \equiv (non(A) \Leftrightarrow non(B)).$$

Preuve. Il suffit de décomposer l'équivalence en deux implications, comme dans la définition de l'équivalence,

$$(A \Rightarrow B) \text{ et } (B \Rightarrow A),$$

puis d'utiliser la propriété de contraposée de l'implication comme dans la Proposition 1.5

$$(non(B) \Rightarrow non(A)) \text{ et } (non(A) \Rightarrow non(B)).$$

On conclut en utilisant encore la définition de l'équivalence par deux implications : $(non(A) \Leftrightarrow non(B))$. ■

1.2 Quantificateurs

Nous avons étudié différentes manières de manipuler des assertions, c'est-à-dire de construire des assertions à partir de plusieurs assertions assemblées à l'aide de connecteurs logiques. Mais nous n'avons pas dit grand-chose sur les assertions. Qu'est-ce qu'une assertion ? C'est une affirmation, une proposition, un prédicat. Soit. Mais comment la définir proprement ?

Nous allons, en particulier, nous intéresser au cas d'assertions dépendant d'une quantité. En effet, vous vous rappelez ce que nous avons dit en début de chapitre à propos des mathématiques : ce sont des sciences qui ont pour objet la quantité et l'ordre. Nous abordons donc les différentes manières de quantifier dans des assertions. Pour une quantité x, nous définissons ainsi une assertion $A(x)$, dont la table de vérité dépend de x.

Exemple 1.8 ($\star$) *Nous avons déjà présenté, dans l'exemple 1.5, un cas d'assertion dépendant d'une quantité x. Nous pouvons donner ici un nouvel exemple. Du lycée, vous avez quelques connaissances sur les suites, même si celles-ci seront affermies dans le chapitre idoine. Nous pouvons donc vous présenter un exemple très simple sur le sujet. En l'occurrence, nous disons qu'une suite réelle $(u_n)_{n\in\mathbb{N}}$ converge vers une limite $x \in \mathbb{R}$ lorsque les termes u_n de la suite sont aussi proches que l'on veut de x à condition de choisir n suffisamment grand. Nous pouvons alors définir l'assertion $A(x)$ par : « la suite $(u_n)_{n\in\mathbb{N}}$ converge vers x ». Cette assertion dépend bien d'un objet x qui est ici un nombre réel. Rendons cet exemple un peu plus concret : si les termes de la suite sont définis par la formule $u_n = (1+n)^{-1}$, alors l'assertion $A(0)$ est vraie mais $A(x)$ est fausse pour toute valeur de x différente de 0.*

Nous utiliserons deux sortes de quantificateurs :

Définition 1.6 (Le quantificateur existentiel) *L'assertion $(\exists x, A(x))$ (lisez « il existe x tel que $A(x)$ ») est vraie si et seulement si il existe un objet x tel que $A(x)$ est vrai.*

Définition 1.7 (Le quantificateur universel) *L'assertion $(\forall x, A(x))$ (lisez « quel que soit x, on a $A(x)$ ») est vraie si et seulement si $A(x)$ est vrai pour tout objet x.*

Pour le quantificateur existentiel, vous rencontrerez dans certains énoncés $(\exists! x, A(x))$. L'ajout du signe ! derrière le symbole $\exists$ le transforme et l'énoncé devient : « il existe un unique objet x tel que $A(x)$ ».

Les deux quantificateurs, existentiel et universel, sont liés. Dans la proposition suivante, ne vous arrêtez pas aux symboles mais dites en français ce que signifient les différentes assertions : vous verrez que les propositions sont naturelles et que les retenir ne demande aucun effort.

Proposition 1.7 *Soit $A(x)$ une assertion dépendant d'un objet x. Alors, on a les deux équivalences suivantes :*
- $[non(\exists x, A(x))] \equiv (\forall x, non(A(x)))$;
- $[non(\forall x, A(x))] \equiv (\exists x, non(A(x)))$.

Exemple 1.9 *L'assertion « il existe un lecteur de ce livre portant le même prénom que moi » fait appel à un quantificateur existentiel. Sa négation fait donc appel à un quantificateur universel : « tous les lecteurs de ce livre portent un autre prénom que le mien ». Si l'on veut raisonner avec des chiffres, l'assertion « tout nombre réel x est supérieur à -2 » est fausse puisque sa négation* *est vraie : « il existe un nombre réel x inférieur à -2 », -3 étant un candidat convenable pour x, tout comme -5, -8.42, -π, etc.*

Nous pouvons également définir l'assertion $A(x,y)$, laquelle dépend de deux quantités, x et y. Nous pouvons même faire dépendre une assertion d'un nombre quelconque d'objets. L'usage de plusieurs quantificateurs est alors possible. Attention à l'écrire proprement, sans omettre la virgule par exemple, laquelle, après un quantificateur existentiel, signifie « tel que ».

Exemple 1.10 ($\star$) *Dans l'exemple 1.8, nous vous avons parlé de la limite d'une suite. Nous avions affirmé qu'une suite réelle $(u_n)_{n\in\mathbb{N}}$ convergeait lorsque les termes de cette suite étaient arbitrairement proches d'un certain $x \in \mathbb{R}$ à partir d'un certain rang. Nous nous étions bien gardés de formaliser cette définition de la convergence car il nous manquait alors la connaissance des quantificateurs et de leur imbrication. Voyons maintenant ce que cela donne :*

$$\exists x \in \mathbb{R}, \forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, |u_n - x| < \varepsilon,$$

ce qui se comprend ainsi : il existe un réel x (ce sera la limite), tel que, pour tout $\varepsilon > 0$ (sous-entendu arbitrairement petit, mais cela est valable pour tout $\varepsilon > 0$), il existe un entier N au-delà duquel (c'est-à-dire tel que pour tout $n \geq N$) les termes de la suite $(u_n)_{n\in\mathbb{N}}$ sont éloignés de x d'une distance inférieure à ε. Vous pouvez vous entraîner à lire ce genre de formules truffées de quantificateurs en choisissant celle que vous voulez dans une page de ce livre prise au hasard.

L'ordre des quantificateurs a son importance et, d'une manière générale, placer en premier un quantificateur existentiel puis un quantificateur universel ne revient pas à placer en premier un quantificateur universel puis un quantificateur existentiel. Dans certains cas seulement, ce sera identique, alors soyez prudents. En l'occurrence, la proposition suivante fixe la règle.

Proposition 1.8 *Soit $A(x,y)$ une assertion dépendant d'un objet x et d'un objet y. Alors,*

$$[\exists x, \forall y, A(x,y)] \Rightarrow [\forall y, \exists x, A(x,y)].$$

Lorsque l'on écrit $\exists x, \forall y$, l'objet x ne dépend pas de y. *A contrario*, lorsque l'on écrit $\forall y, \exists x$, l'objet x dépend de y et, concrètement, pour avoir $A(x,y)$ vraie, à chaque y peut correspondre un x différent, que nous pourrions noter x_y pour souligner une telle différence et éviter toute confusion.

Preuve. C'est une question de compréhension de texte. À gauche de l'implication, nous disons qu'il existe un objet x tel que, pour tout objet y, on a l'assertion $A(x,y)$. À droite de l'implication, on dit que, pour tout y, il existe un objet x (c'est le même que celui que nous mentionnions à gauche) tel que l'on ait $A(x,y)$. ■

Notez bien que nous n'avons qu'une implication, l'autre étant fausse. En effet, si $\forall y, \exists x, A(x,y)$, le x dont on affirme l'existence dépend de chaque objet y choisi (pour être plus clair, nous pourrions l'écrire x_y) : il n'y a alors pas un unique x qui convient à tous les y comme cela est le cas dans l'expression $\exists x, \forall y, A(x,y)$. Mais cela nécessite une explication un peu plus concrète, non ? Sauriez-vous trouver un contre-exemple ?

Exemple 1.11 *Faisons simple, fixons $A(x,y) \equiv (x = y)$, où $x, y \in \mathbb{R}$. Alors, l'assertion $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, A(x,y)$ est clairement fausse car sinon, pour le x en question, on aurait $x = y$ pour tout y, en particulier 0 et 1, ce qui mènerait à $x = 0$ et $x = 1$, donc $0 = 1$. En revanche, l'assertion $\forall y \in \mathbb{R}, \exists x \in \mathbb{R}, A(x,y)$ est bien vraie dans la mesure où, pour tout y, il existe bien un x tel que l'on ait $A(x,y)$; nous sommes même capables de préciser quel est cet x qui convient : il s'agit de y. Ainsi, comme avec cet exemple $\forall y \in \mathbb{R}, \exists x \in \mathbb{R}, A(x,y)$ est vrai et $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, A(x,y)$ est faux, on ne peut pas avoir l'implication $\forall y \in \mathbb{R}, \exists x \in \mathbb{R}, A(x,y) \Rightarrow \exists x \in \mathbb{R}, \forall y \in \mathbb{R}, A(x,y)$.*

D'une manière générale, en mathématiques, on n'utilise pas de symboles ou de lettres que l'on ne comprend pas ; il faut toujours introduire préalablement les objets dont on parle. Dans l'exemple 1.11, vous aurez remarqué que l'objet suivant le quantificateur existentiel est réutilisé tel quel dans la suite du raisonnement. En effet, lorsque l'on écrit $\exists x$, cette affirmation de l'existence de l'objet x équivaut à une introduction de cet objet dans notre raisonnement : il n'y a pas d'ambiguïté si l'on parle plus loin de x. En revanche, les objets suivant un quantificateur universel ne sont pas introduits de la même manière et on ne peut pas les réutiliser dans la suite du raisonnement sous risque d'être ambigu. En effet, si l'on écrit $\forall x \in \mathbb{R}, A(x)$, on ne peut pas évoquer plus loin ce x sans l'avoir introduit proprement (et puis de quel x parlerions-nous ? tous les $x \in \mathbb{R}$ semblent être des candidats possibles ; x vaut-il 0 ou 1 ou $\sqrt{5}$? c'est ambigu). Ainsi, après avoir écrit $\forall x \in \mathbb{R}, A(x)$, il faut écrire : « Soit $x \in \mathbb{R}$. » Alors seulement on peut utiliser x sans ambiguïté.

Pour finir notre propos sur les quantificateurs, une dernière propriété concernant la négation d'une assertion dépendant de deux quantités s'impose.

Proposition 1.9 *Soit $A(x,y)$ une assertion dépendant d'un objet x et d'un objet y. Alors,*

$$[non(\exists x, \forall y, A(x,y))] \equiv [\forall x, \exists y, non(A(x,y))].$$

Nous vous laissons démontrer vous-même ce point, sachant que cela consiste simplement à lire en français les symboles que vous voyez, comme pour la Proposition 1.7.

1.3 Raisonnements

Grâce à la logique, l'art de raisonner sans faute n'a maintenant plus de secret pour vous. Mais ne pas dire de bêtises ne vous garantit pas de dire la vérité si la complexité de celle-ci vous réduit au mutisme. En l'occurrence, il vous faut savoir raisonner, savoir quelle stratégie adopter pour résoudre un problème, savoir comment aborder une démonstration. Nous n'avons pas la prétention de tout vous apprendre sur le sujet car cela s'acquiert avec de la pratique, beaucoup de pratique. Ne lésinez donc pas sur les exercices pour vous familiariser avec l'art du raisonnement, ou plutôt des raisonnements car il s'agit d'un notion protéiforme. Nous vous présentons toutefois quelques stratégies bien utiles pour débuter.

1.3.1 Raisonnement direct ou par l'absurde

Supposons que l'on veuille prouver une assertion A. Le raisonnement direct nous fera travailler les hypothèses pour aboutir sans ambages à cette assertion A. Dans certains cas, la preuve ne vient pas aisément à l'esprit et l'on peut tenter une autre stratégie : le raisonnement par l'absurde. Celui-ci consiste à faire l'hypothèse que A est faux (ce qui revient aussi à $non(A)$ vrai) et à chercher une absurdité logique qui en découlerait. Nous allons vous présenter un exemple qui vous éclairera plus utilement qu'un long discours. Soulignons auparavant l'importance, lorsque l'on rédige une démonstration, de bien expliquer en amont le raisonnement que l'on va suivre et d'expliciter clairement l'objectif : « montrons que A est vrai », pour un raisonnement direct ; « supposons que A est faux et montrons que cela conduit à une absurdité », pour un raisonnement par l'absurde.

Pour reprendre un raisonnement déjà vu dans l'exemple 1.11, la fausseté de l'assertion $[\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, A(x,y)]$ est démontrée par l'absurde alors qu'un raisonnement direct est utilisé pour prouver que $[\forall y \in \mathbb{R}, \exists x \in \mathbb{R}, A(x,y)]$.

Écrivons un nouvel exemple pour illustrer le raisonnement par l'absurde.

Exemple 1.12 ($\star$) *Intéressons-nous à un théorème du chapitre sur les suites, le Théorème 5.2. Ce théorème stipule que si une suite $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ admet une limite, alors cette limite est unique. Vous avez vu dans l'exemple 1.10 la définition de la limite d'une suite, laquelle, à première vue, ne permet pas d'aboutir à la démonstration de l'unicité de cette limite. Ainsi, le raisonnement direct n'étant pas évident, nous pouvons tenter une autre stratégie et voir si celle-ci permet plus facilement d'aboutir : supposons donc qu'il existe deux limites distinctes l_1 et l_2 et cherchons une absurdité. Limitons-nous à une esquisse du raisonnement, plus de détails se trouvant dans la* *démonstration du Théorème 5.2 dans le chapitre idoine. En l'occurrence, en manipulant la définition de la limite, nous allons parvenir à nos fins. En effet, cette définition énonce que tous les termes a_n de la suite sont aussi proches que l'on veut de la limite, que celle-ci soit l_1 ou l_2, à condition de choisir n suffisamment grand. En fixant bien ce que l'on entend par « aussi proches que l'on veut » (choix de l'ε) et en définissant ainsi deux intervalles disjoints dans lesquels sont les termes de la suite, on aboutit à une absurdité : à partir d'un certain rang, les termes de la suite sont tous dans deux intervalles disjoints. Comme cela est impossible, on en déduit que l'hypothèse de l'existence de deux limites distinctes est fausse.*

1.3.2 Raisonnement par disjonction de cas

Dans certaines circonstances, l'objet étudié présente une hétérogénéité telle qu'il est difficile d'avoir un raisonnement efficace pour l'ensemble de l'objet. On coupe alors l'objet en morceaux et on raisonne sur tous ces morceaux, cherchant à prouver pour chacun d'eux la propriété recherchée. Attention, il ne faut oublier aucun morceau, sans quoi on ne peut aboutir à une propriété concernant l'objet entier. Là encore, un exemple sera bien utile.

Exemple 1.13 *Définissons la suite $(u_n)_{n\in\mathbb{N}}$ par l'expression du terme u_n, pour $n \in \mathbb{N}$:*

$$u_n = \begin{cases} 1 & \text{si } n-3 \text{ est multiple de } 4 \\ \sin\left(n\frac{\pi}{2}\right) & \text{sinon.} \end{cases}$$

Montrons que cette suite est constituée de termes positifs ou nuls. Comme cette suite est définie de manière hétérogène, montrons que tous les u_n, pour $n \in \mathbb{N}$, sont positifs ou nuls, par disjonction de cas :

- *si n est multiple de 4, alors il existe un entier k tel que $u_n = \sin(2k\pi) = 0 \geq 0$;*
- *si $n-1$ est multiple de 4, alors il existe un entier k tel que $u_n = \sin(2k\pi + \pi/2) = \sin(\pi/2) = 1 \geq 0$;*
- *si $n-2$ est multiple de 4, alors il existe un entier k tel que $u_n = \sin(2k\pi + \pi) = \sin(\pi) = 0 \geq 0$;*
- *si $n-3$ est multiple de 4, alors $u_n = 1 \geq 0$.*

Tous les cas possibles ont été envisagés : ils correspondent aux différents restes possibles de la division euclidienne par 4, à savoir 0, 1, 2 et 3. Ainsi, nous avons prouvé par disjonction de cas que la suite $(u_n)_{n\in\mathbb{N}}$ est constituée de termes positifs ou nuls.

1.3.3 Pour prouver des implications ou des équivalences

Si l'énoncé que vous cherchez à démontrer est une implication ou une équivalence, plusieurs stratégies tirant parti des propriétés de ces connecteurs s'offrent à vous. Pour ce qui concerne l'équivalence, il est souvent délicat de la prouver directement et le recours à une double implication est bien commode. Ainsi, pour deux assertions A et B, prouver $A \Leftrightarrow B$ revient à prouver $A \Rightarrow B$ et sa réciproque, $B \Rightarrow A$, ce qui est cohérent avec la Définition 1.5. Cette démarche peut aussi se justifier si une des deux implications est vraiment plus simple à résoudre que l'autre, ce qui permet de réduire le problème à une seule implication, comme cela est le cas dans l'exemple suivant.

Exemple 1.14 ($\star$) *Nous reprenons un énoncé du chapitre sur les suites, objets que vous connaissez déjà un peu grâce à vos cours de terminale. Nous voulons donc, sans trop entrer dans les détails, prouver le Théorème 5.12, lequel stipule que, pour une suite* $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ *et un réel* l[1]*, on a l'équivalence :*

$$(a_{2n})_{n\in\mathbb{N}} \text{ et } (a_{2n+1})_{n\in\mathbb{N}} \text{ convergent vers } l \Longleftrightarrow (a_n)_{n\in\mathbb{N}} \text{ converge vers } l.$$

L'implication de la droite vers la gauche est assez simple compte tenu du Théorème 5.2 que nous vous avons présenté dans l'exemple 1.12 et qui affirme qu'une suite ayant une limite ne peut avoir qu'une seule limite, ce qui suppose que deux sous-suites ont la même limite que la suite d'où elles sont extraites. L'autre implication nécessite le recours à d'autres outils et peut donc être démontrée séparément de la première : elle repose en l'occurrence sur l'exhaustivité de ces deux sous-suites ; en effet, tous les termes de la suite $(a_n)_{n\in\mathbb{N}}$ *sont dans* $(a_{2n})_{n\in\mathbb{N}}$ *ou* $(a_{2n+1})_{n\in\mathbb{N}}$ *; donc, la partie gauche de l'équivalence assure que tous les termes de la suite* $(a_n)_{n\in\mathbb{N}}$ *sont aussi proches que l'on veut de* l *à condition de choisir* n *suffisamment grand.*

Nous avons vu que nous pouvions scinder une équivalence en deux implications pour faciliter le raisonnement, mais démontrer une simple implication peut parfois être compliqué. L'utilisation de la contraposée telle qu'introduite dans la Proposition 1.5 peut alors éclairer la pensée.

Exemple 1.15 ($\star$) *Considérons une application* $f : [0,1] \to \mathbb{R}$ *telle que* $f(0) = -\pi$ *et* $f(1) = \pi$. *Nous cherchons à prouver l'implication suivante : si* $\forall x \in [0,1], f(x) \neq 0$, *alors* f *n'est pas continue. Il n'est pas très compliqué de se laisser convaincre par cette implication, mais trouver le raisonnement juste qui rendra la preuve irréfutable est bien plus simple si l'on considère l'implication contraposée, dans la mesure où celle-ci est une conséquence directe du théorème des valeurs intermédiaires. En effet, la contraposée s'écrit « si* f *est continue, alors* $\exists x \in [0,1], f(x) = 0$ *» ; comme* $f(0) = -\pi$ *et* $f(1) = \pi$ *et* $0 \in [-\pi, \pi]$, *le théorème des valeurs intermédiaires permet de conclure.*

1. Dans le Théorème 5.12, $l \in \mathbb{R} \cup \{+\infty, -\infty\}$, mais nous nous limitons ici à $l \in \mathbb{R}$ afin de ne pas embrouiller un exemple de logique avec trop de subtilités concernant les suites.

1.3.4 Raisonnement par récurrence

Pour finir cette liste non exhaustive de stratégies de raisonnements, nous évoquerons brièvement le raisonnement par récurrence, que vous connaissez normalement bien grâce au lycée. Ce type de raisonnement est utilisable si l'on veut prouver une assertion $A(n)$, pour tout $n \in \mathbb{N}$. On commence alors par prouver l'assertion $A(0)$: c'est l'initialisation de la récurrence. Puis on établit l'hérédité, qui consiste en la preuve que l'implication $(A(n) \Rightarrow A(n+1))$ est vraie pour tout $n \in \mathbb{N}$. Ces deux preuves intermédiaires permettent *in fine* de prouver $A(n)$ pour tout $n \in \mathbb{N}$. Vous rencontrerez souvent ce type de raisonnement dans ce livre. D'ailleurs, vous devez déjà être familier avec lui. Est-ce donc utile de vous fournir un exemple ? Peut-être pas... en tout cas nous vous en fournissons dans l'exercice 1.5, avec charge pour vous d'appliquer ce raisonnement.

De manière plus ludique, ce type de raisonnement est très efficace pour résoudre certaines énigmes, comme celle du jeu des allumettes, que vous trouverez dans l'exercice 1.7. Si vous doutiez de pouvoir vous amuser grâce aux mathématiques, allez vite vous y frotter [1] !

1.4 Exercices

Exercice 1.1 *Soient A, B et C des assertions. Montrez que*

(i) $A \Rightarrow (B \text{ et } C) \equiv (A \Rightarrow B) \text{ et } (A \Rightarrow C)$;

(ii) $A \Rightarrow (B \text{ ou } C) \equiv (A \text{ et non}(B)) \Rightarrow C$;

(iii) $A \Rightarrow (B \text{ ou } C) \equiv (A \text{ et non}(C)) \Rightarrow B$;

(iv) $[\text{non}(A \text{ ou non}(A \text{ ou } B)) \Rightarrow \text{non}(\text{non}(A) \text{ et } (B \Rightarrow A))] \equiv V$.

Exercice 1.2 *L'implication est-elle associative ? Autrement dit, pour des assertions A, B et C, a-t-on équivalence entre $[(A \Rightarrow B) \Rightarrow C]$ et $[A \Rightarrow (B \Rightarrow C)]$?*

Exercice 1.3 *Lequel des deux énoncés suivants est correct ?*

$$\begin{cases} \forall n \in \mathbb{N}, \exists k \in \mathbb{N}, n = 2k \text{ ou } n = 2k+1 \\ \exists k \in \mathbb{N}, \forall n \in \mathbb{N}, n = 2k \text{ ou } n = 2k+1 \end{cases}$$

Exercice 1.4 *Soit n un entier. Montrer que si n^2 est pair alors n est pair.*

1. Le « y » fait référence à l'exercice, pas aux allumettes...

Exercice 1.5 *Soit* $k \in \mathbb{N}$ *et* $n \in \mathbb{N}^\star$. *Montrer que la somme des* n *premiers entiers différents de zéro et multiples de* k *vaut* $\frac{kn(n+1)}{2}$.

Exercice 1.6 *Soit* $A(n)$ *une assertion définie pour tout entier* $n \in \mathbb{N}$. *Supposons que l'on a :*

(i) $A(1)$ *est vraie ;*

(ii) pour tout $n \in \mathbb{N}$, *l'implication* $A(n) \Rightarrow A(3n)$ *est vraie ;*

(iii) pour tout $n \in \mathbb{N}$, *l'implication* $A(n+1) \Rightarrow A(n)$ *est vraie.*

Montrez que $A(n)$ *est vraie pour tout* $n \in \mathbb{N}$.

Exercice 1.7 *Vous connaissez certainement ce jeu : deux joueurs (vous et votre adversaire) ont face à eux un certain nombre d'allumettes. Chacun joue à tour de rôle et a le droit de prendre 1, 2 ou 3 allumettes. Celui des deux joueurs qui prend la dernière allumette a perdu. Votre adversaire vous propose courtoisement de choisir si vous voulez commencer à jouer ou si vous lui laissez la main. Que choisissez-vous de faire (sachant que ce choix doit vous permettre de gagner à coup sûr) s'il y a 25 allumettes ? 1000 allumettes ?*

1.5 Solution des exercices

Solution 1.1 (de l'exercice 1.1) *(i) Utilisons la définition de l'implication (Définition 1.4), puis la distributivité de la conjonction et de la disjonction (Proposition 1.4) et enfin à nouveau la définition de l'implication :*

$$\begin{aligned} A \Rightarrow (B \text{ et } C) &\equiv \text{non}(A) \text{ ou } (B \text{ et } C) \\ &\equiv (\text{non}(A) \text{ ou } B) \text{ et } (\text{non}(A) \text{ ou } C) \\ &\equiv (A \Rightarrow B) \text{ et } (A \Rightarrow C). \end{aligned}$$

(ii) Le raisonnement est le même qu'au point précédent : écrire l'implication en termes de disjonction et de négation, utiliser des propriétés qui permettent de mettre l'assertion sous la forme désirée (ici, nous utilisons successivement l'associativité de la disjonction (Proposition 1.3) et la Proposition 1.2), puis réécrire cette assertion sous la forme d'une implication :

$$\begin{aligned} A \Rightarrow (B \text{ ou } C) &\equiv \text{non}(A) \text{ ou } (B \text{ ou } C) \\ &\equiv (\text{non}(A) \text{ ou } B) \text{ ou } C \\ &\equiv \text{non}(A \text{ et non}(B)) \text{ ou } C \\ &\equiv (A \text{ et non}(B)) \Rightarrow C. \end{aligned}$$

(iii) *Le raisonnement est encore plus rapide ici si nous faisons appel au résultat démontré juste avant : ainsi, nous utilisons successivement la commutativité de la disjonction (Proposition 1.3) puis le point (ii) appliqué à* (A, C, B) *au lieu de* (A, B, C) *:*

$$\begin{aligned} A \Rightarrow (B \text{ ou } C) &\equiv A \Rightarrow (C \text{ ou } B) \\ &\equiv (A \text{ et } non(C)) \Rightarrow B. \end{aligned}$$

(iv) *Voilà une grosse expression logique qu'il s'agit de simplifier. Ainsi :*

$$\begin{aligned} &[non(A \text{ ou } non(A \text{ ou } B)) \Rightarrow non(non(A) \text{ et } (B \Rightarrow A))] \\ &\equiv [non(non(A \text{ ou } non(A \text{ ou } B))) \text{ ou } non(non(A) \text{ et } (non(B) \text{ ou } A))] \\ &\equiv [(A \text{ ou } non(A \text{ ou } B)) \text{ ou } (A \text{ ou } non(non(B) \text{ ou } A))] \\ &\equiv [(A \text{ ou } (non(A) \text{ et } non(B))) \text{ ou } (A \text{ ou } (B \text{ et } non(A)))] \\ &\equiv [((A \text{ ou } non(A)) \text{ et } (A \text{ ou } non(B))) \\ &\quad \text{ ou } ((A \text{ ou } B) \text{ et } (A \text{ ou } non(A)))] \\ &\equiv [(V \text{ et } (A \text{ ou } non(B))) \text{ ou } ((A \text{ ou } B) \text{ et } V)] \\ &\equiv [(A \text{ ou } non(B)) \text{ ou } (A \text{ ou } B)] \\ &\equiv [A \text{ ou } (non(B) \text{ ou } B)] \\ &\equiv [A \text{ ou } V] \\ &\equiv V, \end{aligned}$$

où nous avons d'abord utilisé, pour passer à la deuxième ligne, la définition de l'implication (Définition 1.4), puis, pour passer aux lignes suivantes, les diverses propriétés vues concernant la négation, la conjonction et la disjonction (Propositions 1.1, 1.2, 1.3 et 1.4) et le fait que $(A \text{ ou } non(A)) \equiv V$.

Solution 1.2 (de l'exercice 1.2) *Les deux énoncés ne sont pas équivalents. En effet, d'après la Définition 1.4 et les propriétés élémentaires régissant le lien entre négations, conjonctions et disjonctions, nous pouvons écrire :*

$$\begin{aligned} (A \Rightarrow B) \Rightarrow C &\equiv (non(A) \text{ ou } B) \Rightarrow C \\ &\equiv non(non(A) \text{ ou } B) \text{ ou } C \\ &\equiv (A \text{ et } non(B)) \text{ ou } C \end{aligned}$$

et

$$\begin{aligned} A \Rightarrow (B \Rightarrow C) &\equiv A \Rightarrow (non(B) \text{ ou } C) \\ &\equiv non(A) \text{ ou } (non(B) \text{ ou } C) \\ &\equiv (non(A) \text{ ou } non(B)) \text{ ou } C. \end{aligned}$$

En prenant $(A, B, C) = (F, F, F)$*, la première assertion est fausse alors que la seconde est vraie : elle ne sont donc pas équivalentes.*

Solution 1.3 (de l'exercice 1.3) *Il suffit de lire les énoncés... Le premier est vrai : il affirme que tout nombre entier peut s'écrire sous la forme d'un nombre pair ou d'un nombre impair. Le deuxième est faux et recèle une absurdité : en effet, s'il était vrai, l'entier k en question serait tel que $k = 0$ (cas $n = 0$, qui est un nombre pair et donc $n = 2k$) et $k = 1$ (cas $n = 2$, qui est un nombre pair et donc $n = 2k$) ; on aurait ainsi $0 = 1$, ce qui est absurde.*

Solution 1.4 (de l'exercice 1.4) *Le raisonnement direct est-il aisé ? Si n^2 est pair, il existe un entier k tel que $n^2 = 2k$, donc $n = \sqrt{2k}$, ce qui ne nous avance pas à grand chose. Dans cet exercice, le raisonnement le plus simple est en fait la contraposée : supposons que n est impair ; montrons alors que n^2 est impair. Comme n est impair, il existe un entier k tel que $n = 2k + 1$, donc $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ est un nombre impair (puisqu'il va de soi que $2k^2+2k$ est un entier). Ayant ainsi prouvé l'implication contraposée, l'implication initiale est donc aussi démontrée.*

Solution 1.5 (de l'exercice 1.5) *Raisonnons par récurrence. Notons $A(n)$, pour $n \in \mathbb{N}^\star$, l'assertion $\sum_{j=1}^{n} jk = \frac{kn(n+1)}{2}$.*

- *Initialisation : l'assertion $A(1)$ est trivialement vraie car $\sum_{j=1}^{1} jk = k = \frac{k1(1+1)}{2}$.*
- *Hérédité : supposons que $A(n)$ soit prouvée pour un certain $n \in \mathbb{N}^\star$. Montrons alors que $A(n+1)$ est vraie. En l'occurrence, $\sum_{j=1}^{n+1} jk = (n+1)k + \sum_{j=1}^{n} jk$, ce qui, par hypothèse de récurrence, vaut $(n+1)k + \frac{kn(n+1)}{2} = (n+1)k[1 + \frac{n}{2}] = \frac{k(n+1)(n+2)}{2}$. Ainsi, nous avons prouvé $A(n+1)$.*
- *Conclusion : Par récurrence, comme nous avons prouvé $A(1)$ et $(A(n) \Rightarrow A(n+1))$ pour tout $n \in \mathbb{N}^\star$, nous avons prouvé que $A(n)$ est vraie pour tout $n \in \mathbb{N}^\star$.*

Solution 1.6 (de l'exercice 1.6) *Raisonnons par récurrence :*

- *En utilisant (i) et (iii), on prouve que $A(0)$ est vraie.*
- *Supposons que $A(k)$ est prouvée pour tous les entiers $k \leq n \in \mathbb{N}$ (c'est ce que l'on appelle une hypothèse de récurrence forte). Montrons alors que $A(n+1)$ est vraie. Pour ce faire, faisons une disjonction de cas :*
  - *Si $n+1$ est multiple de 3, alors $(n+1)/3$ est un entier inférieur à n, donc, par l'hypothèse de récurrence forte, $A((n+1)/3)$ est vraie, puis, en utilisant le point (ii), on démontre que $A(n+1)$ est vraie.*
  - *Si $n+2$ est multiple de 3, comme dans le cas précédent, on montre que $A(n+2)$ est vraie, puis, par le point (iii), on prouve que $A(n+1)$ est vraie.*
  - *Si n est multiple de 3, alors (nous faisons là encore une disjonction de cas) :*

- *Si* $n = 0$, *alors* $A(n+1)$ *est prouvée par l'hypothèse (i).*
- *Si* $n > 0$, *alors* $(n+3)/3$ *est un entier inférieur à* n, *donc, par l'hypothèse de récurrence forte,* $A((n+3)/3)$ *est vraie, puis, en utilisant le point (ii), on démontre que* $A(n+3)$ *est vraie. En ayant alors recours deux fois à l'hypothèse (iii), on démontre finalement que l'assertion* $A(n+1)$ *est vraie.*

Tous les cas ont bien été envisagés, donc $A(n+1)$ *est bien vraie*[1].
Le raisonnement par récurrence aboutit : $A(n)$ *est vraie pour tout* $n \in \mathbb{N}$.

Solution 1.7 (de l'exercice 1.7) *Implicitement, l'exercice impose de déterminer la stratégie qui fait gagner à coup sûr. Pour guider notre pensée et ne pas la perdre dans de grands nombres d'allumettes, comme 25 et 1000 dans l'énoncé, restreignons un peu le cadre :*

- *S'il y a une seule allumette, cas trivial qui ôte beaucoup d'intérêt au jeu, la stratégie ne fait aucun doute : vous avez intérêt à laisser la main à votre adversaire, qui perdra en étant contraint de prendre la seule et donc dernière allumette.*
- *S'il y a deux allumettes, vous avez intérêt à commencer, afin de prendre une allumette et de laisser l'allumette restante à votre adversaire.*
- *S'il y a trois allumettes, le cas est similaire : commencez par prendre deux allumettes, ce qui laisse la dernière à votre adversaire.*
- *S'il y a quatre allumettes : prenez-en trois et laissez la dernière à votre adversaire.*
- *S'il y a cinq allumettes : vous n'avez pas le droit de prendre plus de trois allumettes, donc la situation est différente de celle décrite aux trois points précédents. Toutefois, quel que soit le nombre d'allumettes que vous prenez, il en restera deux, trois ou quatre pour votre adversaire, qui pourra alors appliquer la stratégie gagnante décrite jusque là, s'il joue bien. Ainsi, si vous avez cinq allumettes et que vous commencez à jouer, vous n'êtes pas certain de gagner (c'est un euphémisme !). Laissez-donc la main à votre adversaire, qui, en jouant et en vous laissant deux, trois ou quatre allumettes, vous mettra dans une position favorable, dans laquelle vous êtes sûr de pouvoir gagner.*

Bon, ne poursuivons pas davantage cette itération : vous avez certainement compris comment cela fonctionne. Reste maintenant à répondre à l'énigme en construisant une démonstration solide. Celle-ci se fera par récurrence puisque le raisonnement que nous venons de mettre en exergue semble itératif. Pour

1. Un raisonnement alternatif accordant moins de place à la disjonction de cas est possible : il consiste, si $A(n)$ est prouvée pour $n > 0$, à prouver que $A(3n)$ est vraie par l'hypothèse (ii), puis à remarquer qu'en utilisant $2n-1$ fois l'hypothèse (iii), l'assertion $A(n+1)$ est vraie.

$n \in \mathbb{N}$, définissons $A(n)$ l'assertion : « Le joueur devant ôter des allumettes aux $4n+1$ encore en jeu n'est pas certain de gagner, son adversaire étant certain de gagner s'il joue bien ; s'il en reste $4n+2$, $4n+3$ ou $4n+4$, le joueur ayant la main est certain de pouvoir gagner. » Prouvons par récurrence que $A(n)$ est vraie pour tout n :

- *$A(0)$ est vraie, d'après le raisonnement préliminaire que nous avons donné.*
- *Supposons que $A(n)$ soit vraie pour un certain entier n. Montrons alors que $A(n+1)$ est aussi vraie. Différents cas doivent être traités :*
  - *S'il reste $4(n+1)+1 = 4n+5$ allumettes en jeu, le joueur ayant la main, en ôtant 1, 2 ou 3 allumettes, ne peut laisser que $4n+2$, $4n+3$ ou $4n+4$ allumettes à son adversaire, lequel, selon l'hypothèse de récurrence, est sûr de gagner s'il joue bien. Ainsi, le joueur ayant la main n'est-il pas certain de pouvoir gagner.*
  - *S'il reste $4(n+1)+k = 4n+(k+4)$ allumettes en jeu, pour $k \in \{2,3,4\}$, alors le joueur ayant la main, en choisissant d'enlever $k-1$ allumettes (nous vérifions au passage que $k-1 \in \{1,2,3\}$ comme l'impose la règle du jeu), laisse $4n+5$ allumettes à son adversaire, qui, comme on vient de l'expliquer, n'a pas d'autre choix que de jouer un coup qui laisse au joueur initial la possibilité de gagner avec certitude.*

  Nous avons donc prouvé l'assertion $A(n+1)$.

Le raisonnement par récurrence a abouti : $A(0)$ est vraie de même que l'implication $A(n) \Rightarrow A(n+1)$, pour $n \in \mathbb{N}$. Ainsi, $A(n)$ est vraie pour tout n. Mais, si cela met en place la stratégie gagnante, nous n'avons pas répondu à la question posée pour autant. C'est l'objet du paragraphe qui suit.

Soit N le nombre d'allumettes initial. Si N s'écrit sous la forme $4n+1$, alors vous êtes sûr de gagner si vous laissez la main à votre adversaire. A contrario, dans tous les autres cas (donc si N s'écrit sous la forme $4n+2$, $4n+3$ ou $4n+4$), vous êtes sûr de gagner si vous jouez en premier. Ainsi, le reste de la division euclidienne de N par 4 détermine votre choix. Si ce reste est 1, laissez la main, sinon jouez en premier. Les deux cas proposés dans l'énoncé, 25 et 1000, ne sont que des cas particuliers dont la résolution est aisée une fois connue la règle que nous venons d'énoncer. Ainsi, si $N = 25 = 4 \times 6 + 1$, laissez jouer votre adversaire en premier ; si $N = 1000 = 4 \times 250$, ne vous faites pas prier pour commencer !

Chapitre 2

Théorie des ensembles

Nous allons vous présenter la théorie des ensembles. Vous avez déjà, par vos connaissances de mathématiques du lycée, une connaissance intuitive de ce qu'est un ensemble, mais aussi de ce qu'est une application. Toutes ces connaissances intuitives sont utiles, mais il faut y mettre de l'ordre et démontrer rigoureusement ce qui doit l'être, ainsi qu'approfondir certains concepts. C'est ce que nous vous proposons de faire dans ce chapitre.

2.1 Définitions et opérations sur les ensembles

Un ensemble est, comme son nom l'indique, une collection d'objets. On ne peut pas vraiment définir plus précisément sans tomber dans la tautologie ou entrer dans des explications complexes qui s'écarteront fortement de la compréhension intuitive que vous avez d'un ensemble. Quelques exemples complèteront donc votre compréhension.

Exemple 2.1 *Les nombres entiers positifs ou nuls constituent un ensemble, l'ensemble des nombres entiers naturels, que l'on note* $\mathbb{N}$. *Les nombres entiers, qu'ils soient positifs, nuls ou négatifs, constituent l'ensemble des nombres entiers relatifs, que l'on note* $\mathbb{Z}$. *Ainsi,* $\mathbb{N}$ *est une partie de* $\mathbb{Z}$. *On peut même écrire :*

$$\mathbb{N} = \{x \in \mathbb{Z} | x \geq 0\},$$

écriture courante des ensembles, qui se lit ainsi : $\mathbb{N}$ *est l'ensemble constitué des éléments* x *de* $\mathbb{Z}$ *tels que* $x \geq 0$.

L'ensemble vide, que nous noterons $\emptyset$, est l'ensemble qui ne contient aucun élément.

Notons que les membres d'un ensemble sont nommés des éléments. On écrit alors, pour x élément de E :

$$x \in E.$$

Cette notation est à distinguer d'une autre, $\subset$, qui établit une relation d'inclusion entre deux ensembles. C'est l'objet de la définition suivante :

Définition 2.1 *Soient E et F deux ensembles. On dit que E est inclus dans F ou que E est un sous-ensemble de F, et on écrit $E \subset F$, si tous les éléments de E sont dans F. Formellement, cette condition s'écrit :*

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

Notez qu'on pourrait aussi écrire : $\forall x, (x \in E \Rightarrow x \in F)$. Par ailleurs, on peut également utiliser cette définition pour définir l'égalité entre deux ensembles :

Définition 2.2 *Soient E et F deux ensembles. On dit que E et F sont égaux, et on écrit $E = F$, si E est inclus dans F et réciproquement. Cette condition s'écrit aussi : $\forall x, (x \in E \Leftrightarrow x \in F)$.*

Définissons également le produit cartésien, auquel nous aurons recours lorsque nous définirons les applications :

Définition 2.3 *Soient E et F deux ensembles. On note $E \times F$ le produit cartésien de E et F, qui est l'ensemble défini par :*

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

Plus généralement, pour un entier $n \geq 2$, si E_1, E_2, ..., E_n sont des ensembles, on peut définir leur produit cartésien par :

$$E_1 \times E_2 \times ... \times E_n = \{(x_1, x_2, ..., x_n) | \forall i \in \{1, 2, ..., n\}, x_i \in E_i\}.$$

En un langage plus simple, le produit cartésien de deux ensembles est l'ensemble de tous les couples possibles décrits en prenant un élément dans chacun des deux ensembles. Par exemple, si le premier ensemble est un ensemble de formes géométriques (cercle et carré) et si le second ensemble est un ensemble de couleurs (rouge, jaune et bleu), alors le produit cartésien de ces deux ensembles est exactement constitué d'un cercle rouge, d'un cercle jaune, d'un cercle bleu, d'un carré rouge, d'un carré jaune et d'un carré bleu.

Après les définitions d'appartenance, vous savez maintenant ce qu'est un élément d'un ensemble. Qu'en est-il si l'un de ces éléments est lui-même un ensemble ? Il n'y a à cela rien de contradictoire et un bon exemple d'un tel ensemble est l'ensemble des parties d'un ensemble.

Définition 2.4 *Soit E un ensemble. L'ensemble des parties de E, noté $\mathcal{P}(E)$ est l'ensemble des ensembles inclus dans E :*

$$\mathcal{P}(E) = \{A | A \subset E\}.$$

Si E est un ensemble non vide, $\mathcal{P}(E)$ est non vide et contient l'ensemble vide $\emptyset$ et l'ensemble E lui-même. Si E est un ensemble fini, la proposition suivante permet de connaître exactement le nombre d'éléments de l'ensemble des parties de E. D'une manière générale, le théorème de Cantor, hors programme, permet d'affirmer que, si E est non vide, alors E contient toujours strictement « moins » d'éléments que $\mathcal{P}(E)$. Cela est trivial si E est fini, en utilisant la proposition suivante, mais cela est moins évident si E est infini, raison pour laquelle nous avons mis « moins » entre guillemets : en effet, on ne peut déjà pas parler du nombre d'éléments d'un ensemble infini, donc on ne peut pas comparer deux ensembles infinis de la manière dont on compare deux ensembles finis. Nous reviendrons plus tard dans ce chapitre sur ce théorème de Cantor.

Proposition 2.1 *Soit E un ensemble fini à $n \in \mathbb{N}$ éléments. Alors, l'ensemble des parties de E contient 2^n éléments.*

Preuve. La preuve peut se faire par récurrence.
- La propriété est vraie pour $n = 0$ puisque l'ensemble vide n'a qu'un seul sous-ensemble, à savoir lui-même.
- Supposons la propriété vraie au rang $n \in \mathbb{N}$. Considérons E, ensemble de $n+1$ éléments dont un élément noté a. Notons F l'ensemble E privé de a. Ainsi, F a n éléments, et l'ensemble de ses parties, par hypothèse de récurrence, en a 2^n. Alors, l'ensemble des parties de E est constitué de deux ensembles disjoints : les sous-ensembles de E ne contenant pas a et les sous-ensembles de E contenant a. Or les premiers sont simplement les sous-ensembles de F, qui sont au nombre de 2^n, et les seconds sont ces mêmes sous-ensembles auxquels on a ajouté l'élément a (ils sont donc aussi au nombre de 2^n). Ainsi, l'ensemble des parties de E a $2^n + 2^n = 2^{n+1}$ éléments.

On a prouvé la proposition pour $n = 0$ et on a démontré la propriété de récurrence donc on a prouvé la proposition pour tout $n \in \mathbb{N}$. ∎

Vous avez donc vu un exemple d'ensemble contenant des ensembles. Imaginez ce nouvel ensemble-ci défini à partir d'ensembles : l'ensemble des ensembles n'appartenant pas à eux-mêmes. Cet ensemble appartient-il à lui-même ? Méditez un instant cet énoncé qui est celui du paradoxe de Russell. Nous le détaillerons juste après en avoir vu une version imagée peut-être plus simple à comprendre : le paradoxe du barbier.

Le paradoxe du barbier s'énonce comme une histoire. Dans un village, le conseil municipal, accablé par la mauvaise tenue de ses administrés, décide d'y remédier en promulguant une loi réquisitionnant l'unique barbier du village qui a, dès lors, obligation de raser tous les hommes qui ne se rasent pas eux-mêmes et seulement ces hommes-là. Le conseil municipal pense ainsi avoir trouvé la solution qu'aucun homme n'apparaisse avec une barbe. Néanmoins, qu'en est-il du barbier ? S'il ne se rase pas, alors, selon la nouvelle loi, le barbier, c'est-à-dire lui-même, est censé le raser, sauf que dans ce cas, il se rase lui-même, ce que la loi exclut des prérogatives du barbier : il y a donc contradiction. De même, s'il se rase, on aboutit à une contradiction. Une solution facétieuse est de faire occuper ce poste par une femme. Si l'un de nos lecteurs avisés intègre le conseil municipal, il peut aussi à juste titre évoquer le paradoxe de Russell et conclure qu'un tel barbier n'existe pas. En effet, l'ensemble des ensembles qui n'appartiennent pas à eux-même n'existe pas. C'est l'objet de l'exemple qui suit.

Exemple 2.2 *Soit E l'ensemble des ensembles n'appartenant pas à eux-mêmes. Cet ensemble E appartient-il à lui-même ? Tout d'abord, si $E \in E$, une contradiction apparaît, car, par définition de E, l'élément E n'appartient pas à lui-même. De même, si $E \notin E$, il y a aussi contradiction, car, si l'élément E n'est pas dans E, alors, par définition de E, E appartient à lui-même. Ainsi, il est faux d'affirmer que E appartient à lui-même, de même qu'il est faux de prétendre que E n'appartient pas à lui-même. C'est ce qu'on appelle le paradoxe de Russell. En fin de compte, on a simplement prouvé que E n'existe pas.*

Voilà pour les ensembles dont les éléments sont eux-mêmes des ensembles. Considérons maintenant plus simplement des ensembles quelconques, sans restriction sur la nature de leurs éléments. En particulier, nous allons tenter de manipuler ces ensembles comme n'importe quel objet mathématique. Vous savez probablement ce que cela implique, n'est-ce pas ? Non ? Lorsque vous manipulez des nombres réels, que faites-vous, concrètement ? Des additions, des multiplications, etc., bref, des opérations. Eh bien, nous allons faire de même avec les ensembles et définir des opérations : ce ne sera plus la somme de deux nombres mais l'union ou l'intersection de deux ensembles qui nous intéresse. De même que l'on définit un ensemble où les opérations sur les nombres réels sont définies, de même, nous devons définir un contexte où utiliser les opérations sur les ensembles. Ainsi, nous définissons les opérations sur les ensembles contenus dans $\mathcal{P}(E)$, où E est un ensemble.

Définition 2.5 *Soient A et B des ensembles appartenant à $\mathcal{P}(E)$. L'intersection de A et B, notée $A \cap B$, est l'ensemble des éléments appartenant à A*

et à B :

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

Définition 2.6 *Soient A et B des ensembles appartenant à $\mathcal{P}(E)$. L'union de A et B, notée $A \cup B$, est l'ensemble des éléments appartenant à A ou à B :*

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

Définition 2.7 *Soit A un ensemble appartenant à $\mathcal{P}(E)$. Le complémentaire de A dans E, noté $E \backslash A$, est l'ensemble des éléments appartenant à E et pas à A :*

$$E \backslash A = \{x \in E | x \notin A\}.$$

S'il ne peut y avoir d'ambiguïté sur E, on peut aussi écrire : $\overline{A}$.

De même que pour les nombres réels nous pouvons définir la soustraction, nous pouvons maintenant définir la différence d'ensembles :

Définition 2.8 *Soient A et B des ensembles appartenant à $\mathcal{P}(E)$. La différence de A et B, notée $A \backslash B$ et lue A privé de B, est l'ensemble des éléments appartenant à A et pas à B :*

$$A \backslash B = A \cap (E \backslash B).$$

Alors, le complémentaire de A dans E n'est que E privé de A, de même que l'opposé d'un nombre réel n'est que la soustraction de ce nombre à 0. Cela permet de comprendre le complémentaire d'un ensemble comme une analogie de l'opposé d'un nombre réel.

Nous illustrons les définitions précédentes dans la figure 2.1.

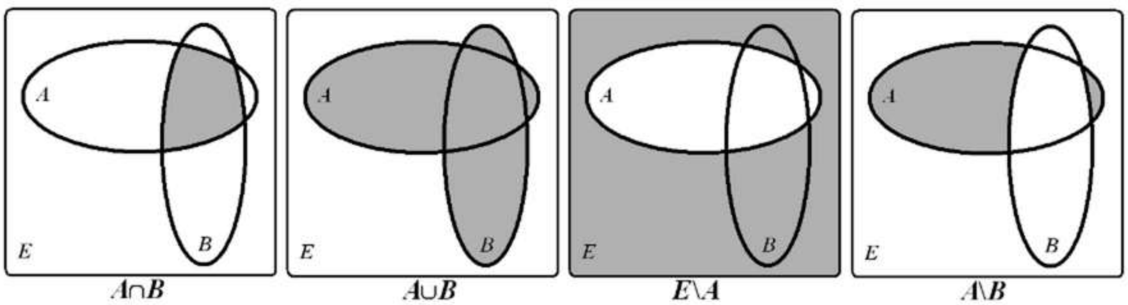

FIGURE 2.1 – Intersection, union, complémentaire et différence.

La définition de toutes ces opérations s'appuie fortement sur les connecteurs logiques : en effet, la conjonction logique (le *et*) devient l'intersection de deux ensembles, la disjonction (le *ou*) devient l'union et la négation s'apparente au complémentaire. Mais, rappelez-vous, parmi les connecteurs logiques, nous avions également défini l'implication et l'équivalence. Sauriez-vous continuer l'analogie avec la théorie des ensembles ? Reprenons un cas plus simple pour étudier le fonctionnement de cette analogie : l'intersection de deux ensembles A et B. On a

$$(x \in A \cap B) \Longleftrightarrow (x \in A \text{ et } x \in B)\,.$$

L'ensemble, que nous notons provisoirement C, défini par analogie avec l'implication logique, devrait donc s'écrire :

$$(x \in C) \Longleftrightarrow (x \in A \Rightarrow x \in B)\,.$$

Or, vous avez vu, dans le chapitre consacré à la logique, que $x \in A \Rightarrow x \in B$ signifie $x \notin A$ ou $x \in B$. Ainsi, cet ensemble noté C est égal à $\overline{A} \cup B$. Notez que si $A \subset B$, alors, $\forall x \in E$, on a l'implication $x \in A \Rightarrow x \in B$, ce qui permet de voir l'inclusion d'un ensemble dans un autre comme une autre manière de considérer l'analogie avec l'implication logique. Par ailleurs, l'ensemble C que nous avons juste défini a une propriété intéressante. En effet, l'intersection de A avec cet ensemble est contenue dans B, ce que vous aviez probablement deviné, car si x est dans C, alors $x \in A$ et $x \in B$, ce qui a pour conséquence que si, de plus, x est dans A, alors x est aussi dans B. Mais je sens que vous brûlez d'envie de le redémontrer rigoureusement. La solution est dans l'exemple 2.3. Mais avant de le faire, vous apprécierez certainement de connaître quelques propriétés héritées de l'analogie avec la logique.

Théorème 2.1 *Soient A et B des ensembles appartenant à $\mathcal{P}(E)$. Alors,*
- $A \subset (A \cup B)$ *;*
- $(A \cap B) \subset A$.

Preuve. Si l'on reprend la définition formelle de l'union et de l'intersection, la démonstration est triviale. Détaillons-la tout de même pour le premier point : pour tout $x \in A$, on a nécessairement $x \in A$ ou $x \in B$, donc, par définition de l'union, $x \in A \cup B$. Nous vous laissons démontrer le second point, en repassant par la définition de l'intersection. ■

Théorème 2.2 *Soient A, B et C des ensembles appartenant à $\mathcal{P}(E)$.*
- *l'union est une opération commutative, de même que l'intersection :*

$$\begin{cases} A \cup B = B \cup A \\ A \cap B = B \cap A\ ; \end{cases}$$

- *l'union est associative, de même que l'intersection :*

$$\begin{cases} (A \cup B) \cup C = A \cup (B \cup C) \\ (A \cap B) \cap C = A \cap (B \cap C)\ ; \end{cases}$$

– *l'union et l'intersection sont distributives l'une par rapport à l'autre :*

$$\begin{cases} A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \\ A \cap (B \cup C) = (A \cap B) \cup (A \cap C). \end{cases}$$

Ces propriétés sont héritées des mêmes propriétés concernant les connecteurs logiques. Vous vous laisserez aisément convaincre par les premiers points ; attelons-nous donc à démontrer le premier énoncé du dernier point, la démonstration du second énoncé nécessitant le recours aux mêmes types de raisonnement.

Preuve.

$$\begin{aligned} A \cup (B \cap C) &= \{x \in E | x \in A \text{ ou } x \in (B \cap C)\} \\ &= \{x \in E | x \in A \text{ ou } (x \in B \text{ et } x \in C)\} \\ &= \{x \in E | (x \in A \text{ ou } x \in B) \text{ et } (x \in A \text{ ou } x \in C)\} \\ &= \{x \in E | (x \in A \cup B) \text{ et } (x \in A \cup C)\} \\ &= (A \cup B) \cap (A \cup C). \end{aligned}$$

■

La clef de cette démonstration réside dans le passage de la deuxième à la troisième ligne, lorsque les connecteurs logiques sont distribués selon les propriétés que vous avez vues dans le chapitre idoine.

Théorème 2.3 *Soient A, B et C des ensembles appartenant à $\mathcal{P}(E)$. Alors,*
– $(A \cup B) \subset C$ *si et seulement si* $A \subset C$ *et* $B \subset C$ *;*
– $C \subset (A \cap B)$ *si et seulement si* $C \subset A$ *et* $C \subset B$.

Démontrons la première équivalence ; nous vous laissons la deuxième en exercice car le type de raisonnement est similaire : c'est une bonne occasion de vérifier que vous avez bien compris comment conduire ce genre de démonstrations.

Preuve. Une démarche organisée pour démontrer une équivalence consiste à la scinder en deux démonstrations, chacune correspondant à l'une des deux implications formant l'équivalence. Supposons ainsi, en premier lieu, que $(A \cup B) \subset C$. D'après le Théorème 2.1, on a $A \subset (A \cup B)$ et $B \subset (A \cup B)$, donc, par transitivité de l'inclusion, comme $(A \cup B) \subset C$, on a $A \subset C$ et $B \subset C$. Ainsi, $(A \cup B) \subset C \Rightarrow A \subset C$ et $B \subset C$. Pour démontrer l'autre implication, supposons que $A \subset C$ et $B \subset C$. Soit $x \in A \cup B$. Cela signifie que $x \in A$ ou $x \in B$. Ainsi, si $x \in A$, alors, comme $A \subset C$, on a *a fortiori* $x \in C$. *A contrario*, si $x \notin A$, alors $x \in B$ et, comme $B \subset C$, on a encore $x \in C$. Dans tous les cas (la réunion de $x \in A$ et $x \notin A$ représentant la totalité des cas possibles), on a $x \in C$. Ainsi, $A \subset C$ et $B \subset C \Rightarrow (A \cup B) \subset C$. La démonstration des deux implications suffit à prouver l'équivalence : $A \subset C$ et $B \subset C$. Ainsi, $(A \cup B) \subset C \iff A \subset C$ et $B \subset C$. ∎

Théorème 2.4 *Soit A un ensemble appartenant à $\mathcal{P}(E)$. Alors,*
(i) $\overline{\overline{A}} = A$ *;*
(ii) $A \cap \overline{A} = \emptyset$ *;*
(iii) $A \cup \overline{A} = E$.

Ces propriétés ressemblent beaucoup à des propriétés que vous avez déjà rencontrées à propos du chapitre sur la logique. Vous devriez donc être capables de démontrer aisément ces trois points. Vérifiez que c'est bien le cas avant de lire les trois démonstrations que nous vous proposons. Il y a d'ailleurs plusieurs manières de procéder, c'est pourquoi nous avons choisi trois raisonnements bien différents, tous valables. Attention, certains raisonnements sont plus adaptés à certains types de théorèmes à démontrer, et le choix d'un type de raisonnement pourrait être artificiel et plus difficile à comprendre dans certains cas, le but d'une démonstration étant avant tout de prouver un énoncé en peu de lignes et de manière claire : c'est ce que l'on appelle une démonstration élégante.

Preuve.
(i) Par définition, on a l'équivalence

$$\begin{aligned} x \in \overline{\overline{A}} &\iff x \in E \text{ et } x \notin \overline{A} \\ &\iff x \in E \text{ et } x \in A \\ &\iff x \in A \end{aligned}$$

car $A \subset E$.

(ii) Démontrons par l'absurde que $A \cap \overline{A} = \emptyset$. Supposons ainsi, hypothèse fausse, que $A \cap \overline{A}$ n'est pas vide et trouvons une incohérence. L'hypothèse que $A \cap \overline{A}$ n'est pas vide revient à affirmer qu'il existe $x \in A \cap \overline{A}$. Par le Théorème 2.1, $A \cap \overline{A} \subset A$ et $A \cap \overline{A} \subset \overline{A}$. Donc $x \in A$ et $x \in \overline{A}$, c'est-à-dire $x \in A$ et $x \notin A$, ce qui est absurde. Ainsi, notre raisonnement par l'absurde conduit à la négation de notre hypothèse : on peut donc conclure que $A \cap \overline{A} = \emptyset$.

(iii) Une égalité d'ensembles peut se montrer par double inclusion. C'est ce que nous faisons ici. Tout d'abord, tous les ensembles étudiés, A et $\overline{A}$, étant des sous-ensembles de E, leur réunion l'est aussi : $A \cup \overline{A} \subset E$. Pour l'autre inclusion, considérons $x \in E$. Alors, soit $x \in A$ soit $x \notin A$, donc $x \in A \cup \overline{A}$. Cela nous permet d'écrire que $E \subset A \cup \overline{A}$. Ces deux inclusions reviennent à écrire que $A \cup \overline{A} = E$.

∎

Théorème 2.5 *Soient A et B deux ensembles appartenant à $\mathcal{P}(E)$. Alors,*
(i) $\overline{A \cup B} = \overline{A} \cap \overline{B}$ *;*
(ii) $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Preuve.
(i) Soit $x \in \overline{A \cup B}$. Alors, par définition, $x \notin (A \cup B)$, c'est-à-dire $x \notin A$ et $x \notin B$. Donc, $\overline{A \cup B} \subset \overline{A} \cap \overline{B}$. Le raisonnement inverse peut être fait pour démontrer l'autre inclusion, donc, en fin de compte, on a montré que $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
(ii) En appliquant le point précédent à $\overline{A}$ et $\overline{B}$, on obtient $\overline{\overline{A} \cup \overline{B}} = \overline{\overline{A}} \cap \overline{\overline{B}}$. Puis, en prenant le complémentaire de ces deux ensembles, on peut écrire $\overline{\overline{\overline{A} \cup \overline{B}}} = \overline{\overline{\overline{A}} \cap \overline{\overline{B}}}$. On conclut par le point (i) du Théorème 2.4 : $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
■

Nous pouvons utiliser le Théorème 2.5 pour prouver un résultat que nous avons déjà prouvé, d'une autre manière, dans le Théorème 2.4, à savoir que $A \cup \overline{A} = E$. Voyez-vous comment procéder ? L'idée permet de faire une démonstration très brève utilisant d'autres résultats démontrés par ailleurs, c'est-à-dire que cette démonstration est élégante, comme on vous l'a déjà expliqué. Partez d'un autre résultat du Théorème 2.4 : $A \cap \overline{A} = \emptyset$. Vous ne voyez toujours pas ? Pourtant il suffit maintenant de prendre le complémentaire dans E des deux ensembles de part et d'autre de l'égalité : $\overline{A \cap \overline{A}} = \overline{\emptyset}$, ce qui revient, en utilisant le Théorème 2.5, à $\overline{A} \cup A = E$, puis, en ayant recours à la commutativité énoncé dans le Théorème 2.2, au résultat recherché, à savoir $A \cup \overline{A} = E$.

Théorème 2.6 *Soient A et B deux ensembles appartenant à $\mathcal{P}(E)$. Alors,*
(i) $A \subset B \Longleftrightarrow \overline{B} \subset \overline{A}$ *;*
(ii) $A \cap B = \emptyset \Longleftrightarrow A \subset \overline{B}$ *;*
(iii) $A \cup B = E \Longleftrightarrow \overline{A} \subset B$.

En termes de logique, le point (i) est analogue à la contraposée : en effet, cela saute aux yeux si vous vous rappelez le lien entre implication logique et inclusion d'ensembles déjà évoqué. Prouvons maintenant ce théorème.

Preuve.
(i) On a les équivalences suivantes :

$$\begin{aligned} A \subset B &\Longleftrightarrow (\forall x \in E, x \in A \Rightarrow x \in B) \\ &\Longleftrightarrow (\forall x \in E, x \notin B \Rightarrow x \notin A) \\ &\Longleftrightarrow (\forall x \in E, x \in \overline{B} \Rightarrow x \in \overline{A}) \\ &\Longleftrightarrow \overline{B} \subset \overline{A} \end{aligned}$$

ce qui prouve le premier point.

(ii) On démontre d'abord l'implication de droite à gauche : supposons que $A \subset \overline{B}$. Alors $A \cap B \subset \overline{B} \cap B = \emptyset$ d'après le Théorème 2.4. Ainsi $A \cap B \subset \emptyset$, donc $A \cap B = \emptyset$. Nous démontrons maintenant l'autre implication, ce qui, avec ce que nous venons de démontrer, suffira à démontrer l'équivalence : supposons que A et B sont disjoints, c'est-à-dire que $A \cap B = \emptyset$. Soit $x \in A$. Comme $A \cap B = \emptyset$, $x \notin B$. Par ailleurs, $x \in E$ car $A \subset E$. Donc $x \in \overline{B}$, ce qui conclut la preuve.

(iii) Appliquons le point (ii) du présent théorème à $\overline{A}$ et $\overline{B}$ au lieu de A et B :

$$\overline{A} \cap \overline{B} = \emptyset \Longleftrightarrow \overline{A} \subset \overline{\overline{B}}.$$

Par ailleurs, en passant au complémentaire à gauche et à droite du signe d'égalité, on peut écrire, grâce au Théorème 2.5 :

$$\overline{A} \cap \overline{B} = \emptyset \Longleftrightarrow A \cup B = E.$$

Comme $\overline{\overline{B}} = B$, on peut alors conclure que :

$$A \cup B = E \Longleftrightarrow \overline{A} \subset B.$$

■

Nous vous laissons démontrer quelques propriétés de la différence de deux ensembles dans l'exercice 2.1.

Maintenant que nous avons énoncé tous ces résultats importants et bien pratiques concernant les opérations sur les ensembles, retournons un instant à l'ensemble $C = \overline{A} \cup B$ qui nous permettait de faire une analogie avec l'implication logique.

Exemple 2.3 *Soient A et B deux ensembles et $C = \overline{A} \cup B$. Montrons que $A \cap C \subset B$. Si l'on reprend l'analogie avec la logique, cela signifierait que si l'implication $A \Rightarrow B$ est vraie et si A est vrai, alors B est vrai. Cela se montre facilement en utilisant la définition de C puis le Théorème 2.2 :*

$$\begin{aligned} A \cap C &= A \cap (\overline{A} \cup B) \\ &= (A \cap \overline{A}) \cup (A \cap B) \\ &= \emptyset \cup (A \cap B) \\ &= (A \cap B) \subset B. \end{aligned}$$

2.2 Applications

Lors de vos cours de mathématiques de lycée, vous avez souvent entendu parler d'applications, les utilisant même abondamment. Ce que nous appelons ici application porte aussi le nom de fonction : il s'agit du même objet que celui que vous connaissez, mais vous avez en fait encore beaucoup à apprendre sur le sujet. Cette partie est donc intéressante pour vous : elle vous permet d'approfondir vos connaissances et intuitions de terminale au point qui est exigé de vous en classes préparatoires.

Dans cette partie, E, F, G et H sont des ensembles quelconques.

Une application f de E dans F est un objet qui lie à tout élément x de E un unique élément y de F. E est l'ensemble de départ, F l'ensemble d'arrivée. Ces deux ensembles peuvent être éventuellement vides. y est appelé image de x par f et est noté $f(x)$. x est un antécédent de y par f ; ce n'est pas l'antécédent mais bien <u>un</u> antécédent : un élément y de F peut parfaitement avoir un, plusieurs ou même aucun antécédent par f. La notion d'injection et de surjection, que vous découvrirez dans la suite de ce chapitre, permettra d'être plus précis à ce sujet.

Par ailleurs, on notera : $f : E \to F, x \mapsto f(x)$.

Ces quelques explications permettent de confirmer ce que vous savez déjà d'une application. Donnons toutefois une définition plus formelle :

Définition 2.9 *Une application f est un triplet (E, F, Γ), où E et F sont des ensembles et $\Gamma \subset E \times F$, tel que $\forall x \in E, \exists! y \in F, (x, y) \in \Gamma$, ce qui se lit : pour tout élément x de E, il existe un unique élément y de F, tel que le couple (x, y) soit élément de l'ensemble Γ, que l'on appelle graphe de l'application f.*

Si vous avez lu attentivement le début de ce chapitre sur les ensembles, vous aurez alors apprécié l'apparition d'un produit cartésien dans la définition d'une application ! Peut-être, au contraire, le produit cartésien n'avait-il fait qu'effleurer un coin de votre œil sans vraiment entrer dans votre mémoire. Il est vrai que nous n'avions pas dit grand chose au sujet de ce produit cartésien, qui justifiait principalement sa présence dans ce livre par la définition que vous venez de lire sur les applications. N'hésitez pas, alors, à relire cette définition du produit cartésien : ce sera l'occasion de la retenir définitivement.

Par ailleurs, on fait souvent la confusion, en terminale, entre une application et son graphe, c'est-à-dire entre f et Γ selon l'écriture utilisée dans la Définition 2.9 que vous venez de lire. Mais, si vous relisez cette définition, vous vous rendez bien compte que cette confusion est fausse et que deux applications de même graphe ne sont pas nécessairement égales. Avez-vous un exemple ? Il y en a plein !

Exemple 2.4 *Les applications $f : [0, 1] \to [0, 1], x \mapsto x$ et $g : [0, 1] \to \mathbb{R}, x \mapsto x$ ne sont pas égales car elles n'ont pas le même ensemble d'arrivée. Contrai-*

rement à ce qu'une vision simplifiée pourrait laisser croire, il ne suffit pas de vérifier que les graphes sont égaux, c'est-à-dire que $\forall x \in [0,1]$, $f(x) = g(x)$, propriété qui est pourtant bien observée ici : il faut non seulement l'égalité entre les graphes mais aussi l'égalité entre les deux espaces de départ, d'une part, et entre les deux espaces d'arrivée, d'autre part.

Dans l'exemple 2.4, f est ce que l'on appelle l'application identité de $[0,1]$. On peut aisément généraliser cette notion à tout ensemble :

Définition 2.10 *L'application* ***identité*** *de E, notée Id_E, est l'application définie par : $Id_E : E \to E, x \mapsto x$.*

Maintenant que nous avons défini ce qu'est une application et que nous nous sommes attardés sur le cas particulier de l'identité, il est temps de voir ce que l'on peut faire avec plusieurs applications. En l'occurrence, nous définissons maintenant la composée de deux applications, qui est une nouvelle application.

Définition 2.11 *Soit $f : E \to F$ et $g : F \to G$ deux applications. La* ***composée*** *de f et g est l'application $h : E \to G, x \mapsto g(f(x))$. On note $h = g \circ f$.*

Vous pouvez le vérifier : la composée est bien une application. En effet, si vous reprenez la Définition 2.9, il faut que pour tout élément de $x \in E$, l'image de x par h existe et soit unique. Or, comme f et g sont des applications, l'image de x par f existe et est unique : c'est $f(x) \in F$. Par ailleurs, l'image de $f(x)$ par g, dont l'ensemble de départ, F, contient $f(x)$, existe et est unique : c'est $g(f(x))$. Donc l'image de x par $h = g \circ f$ existe et est unique. Notez bien qu'il faut que l'ensemble de départ de g corresponde à l'ensemble d'arrivée de f, sans quoi la composition ne peut se faire. Ce point n'est pas une lubie comme vous pouvez vous en rendre compte dans l'exemple suivant :

Exemple 2.5 *Soit $f : \mathbb{R} \to \mathbb{R}, x \mapsto x$. Autrement dit, $f = Id_{\mathbb{R}}$. Soit $g : [0,+\infty[\to [0,+\infty[, x \mapsto \sqrt{x}$. On ne peut pas composer f et g : $g \circ f$ n'a pas de sens car la racine carrée de nombres négatifs n'en a pas. En revanche, on peut composer g avec $Id_{[0,+\infty[}$, ce qui donne : $g \circ Id_{[0,+\infty[} = g$.*

Si vous n'avez pas suivi l'ordre du livre et que vous avez abordé le chapitre sur l'algèbre, vous savez que l'application identité est l'élément neutre pour la loi interne de composition. Cela signifie simplement que toute application f composée avec l'identité (identité définie sur le bon ensemble, selon que l'on compose à droite ou à gauche) est égale à l'application f. Comme nous avons pu le voir dans l'exemple 2.5, l'adéquation des ensembles de départ et d'arrivée est primordiale. Nous le soulignons dans la proposition que nous énonçons maintenant :

Proposition 2.2 *Soit $f : E \to F$. Alors $f \circ Id_E = Id_F \circ f = f$.*

Preuve. $Id_E : E \to E$ et $f : E \to F$, donc la coïncidence de l'ensemble d'arrivée de Id_E avec l'ensemble de départ de f permet de définir la composition des deux applications : $f \circ Id_E : E \to F$. Cette application composée a le même ensemble de départ et le même ensemble d'arrivée que f. Pour montrer que ces deux applications sont égales, il ne reste donc qu'à montrer que l'image de tout $x \in E$ par chacune de ces deux applications est bien égale, ce qui est trivial : $f \circ Id_E(x) = f(Id_E(x)) = f(x)$. Ce raisonnement peut être aussi suivi pour démontrer que $Id_F \circ f = f$, ce qui termine la démonstration du théorème. ■

Par ailleurs, une composée est une application, donc on peut la composer avec une autre application, du moment que les ensembles de départ et d'arrivée de celle-ci sont bien choisis. La proposition suivante permet ainsi de composer plusieurs applications : vous verrez que l'ordre de priorité dans lequel on compose les applications n'est pas important.

Proposition 2.3 *La composition est associative : pour $f : E \to F$, $g : F \to G$ et $h : G \to H$, $h \circ (g \circ f) = (h \circ g) \circ f$. Cette application peut être notée $h \circ g \circ f$.*

Nous vous laissons la démonstration de cette proposition en exercice. Rappelez-vous simplement ce point primordial : pour démontrer l'égalité de deux applications, il faut montrer qu'elles ont le même ensemble de départ, le même ensemble d'arrivée et le même graphe.

Dans l'exemple 2.4, tous les éléments de l'ensemble d'arrivée de $g : [0,1] \to \mathbb{R}, x \mapsto x$ ne sont pas atteignables, autrement dit il existe des éléments de cet ensemble d'arrivée n'ayant pas d'antécédent par g. Pour autant, g n'en est pas moins une application. Et, comme nous l'avons expliqué, elle est différente de l'application $f : [0,1] \to [0,1], x \mapsto x$, pour laquelle l'ensemble d'arrivée, $[0,1]$, admet un antécédent en chacun de ses points. Pour cette raison, f est ce que l'on appelle une surjection ou une application surjective.

Définition 2.12 *Une application $f : E \to F$ est* ***surjective*** *si*

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

ce qui se lit : pour tout élément de l'ensemble d'arrivée de f, il existe un antécédent par f dans son ensemble de départ.

Comme vous venez de lire précédemment quelques lignes à propos de la composition de plusieurs applications, vous vous demandez certainement (ou peut-être pas, mais alors nous répondrons tout de même à la question que vous ne vous posez pas !) ce qu'il advient de la composée de deux applications surjectives. Intuitivement, la première application surjective va permettre d'atteindre tous les éléments de son ensemble d'arrivée, donc tous les éléments de l'ensemble de départ de la deuxième application, puis la deuxième application surjective permettra aussi d'atteindre tous les éléments de l'ensemble d'arrivée de cette même deuxième application, donc tous les éléments de l'ensemble d'arrivée de la composée. Dit plus clairement : le composée sera surjective.

Théorème 2.7 *Soit $f : E \to F$ et $g : F \to G$ deux applications surjectives. Alors $g \circ f$ est aussi surjective.*

Nous vous avons donné l'intuition de la démonstration avant d'énoncer le théorème : vous devriez être capable de le prouver proprement, non ? Essayez puis comparez avec notre version.

Preuve. Utilisons la Définition 2.12 pour montrer la surjectivité de $g \circ f : E \to G$. Soit $y \in G$. Comme $g : F \to G$ est surjective, il existe $z \in F$ tel que $g(z) = y$. Par ailleurs, comme $f : E \to F$ est surjective, il existe $x \in E$ tel que $f(x) = z$. Donc $g(f(x)) = y$. Ainsi, pour tout $y \in G$, il existe $x \in E$ tel que $g \circ f(x) = y$, ce qui prouve la surjectivité de $g \circ f$. ∎

Notez que la réciproque du Théorème 2.7 est fausse. Pouvez-vous trouver un contre-exemple ?

Exemple 2.6 *Allez, nous vous aidons un peu... Nous cherchons f et g avec au moins l'une des deux non-surjective mais $g \circ f$ surjective. Comme $g \circ f$ est surjective, il faut nécessairement que g le soit également, car pour tout $y \in G$ il existe $x \in E$ tel que $g \circ f(x) = y$, autrement dit il existe z, valant précisément $f(x)$, tel que $g(z) = y$, ce qui correspond à la définition de la surjectivité de g. Pour le contre-exemple que nous cherchons, l'application non-surjective devra donc être f. Notons F' l'ensemble des éléments de F que f atteint, autrement dit F' est l'image de E par f. Alors, pour que $g \circ f$ soit surjective, il suffira que l'image par g de tout élément de F soit aussi l'image par g d'un élément de $F' \subset F$. Vous devriez maintenant avoir une idée, non ? Par exemple, si g est périodique et que f ne permet de décrire que les éléments d'une période, le tour est joué. Prenez donc $f : [-1,1] \to \mathbb{R}, x \mapsto \arcsin(x) + \pi/2$ et $g : \mathbb{R} \to [-1,1], x \mapsto \cos(x)$, par exemple[1]. f n'est pas surjective puisque l'image de $[-1,1]$ par f est $[0,\pi]$. Or l'image de $[0,\pi]$ par g est $[-1,1]$, ce qui assure que $g \circ f$ est surjective. Vous pouvez aussi le vérifier directement en notant que $g \circ f$ est simplement $-Id_{[-1,1]}$.*

1. L'application arc sinus associe à un nombre compris entre -1 et 1 l'unique mesure d'angle, dans $[-\pi/2, \pi/2]$, dont le sinus vaut ce nombre. Ainsi, pour $x \in [-1,1]$, $\sin(\arcsin(x)) = x$.

Maintenant que vous maîtrisez l'idée que nous avons développée, vous pouvez imaginer d'autres exemples et pas seulement pour des applications périodiques. Prenez par exemple pour f une application valeur absolue $f : [-1,1] \to [-1,1], x \mapsto |x|$ et pour g une application carré $g : [-1,1] \to [0,1], x \mapsto x^2$. La composée est bien surjective mais f ne l'est pas.

Considérons maintenant deux autres applications distinctes, quoique définies par la même expression : $f : [0,1] \to [0,1], x \mapsto x^2$ et $g : [-1,1] \to [0,1], x \mapsto x^2$. Ces deux applications sont toutes les deux des applications carré mais leur ensemble de départ diffère, ce qui suffit pour affirmer que ces deux applications sont différentes. En revanche, leur ensemble d'arrivée est identique et l'on peut même affirmer que ces deux applications sont surjectives. En effet, pour tout $y \in [0,1]$, $\sqrt{y}$ est un antécédent de y par f et par g. Pour f, cet antécédent est même unique, alors que pour g, $-\sqrt{y}$ est un autre antécédent possible lorsque $y \neq 0$. Cette propriété de f est très utile. On dira que f est une injection ou une application injective, ce qui signifie que deux éléments de son ensemble de départ ne peuvent avoir la même image.

Définition 2.13 *Une application $f : E \to F$ est* ***injective*** *si*

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

ce qui se lit : deux éléments quelconques de l'ensemble de départ de f ont une même image par f seulement si ces deux éléments sont égaux.

À l'image du Théorème 2.7 énonçant que la composée de deux applications surjectives est une application surjective, la composée de deux applications injectives est une application injective :

Théorème 2.8 *Soient $f : E \to F$ et $g : F \to G$ deux applications injectives. Alors $g \circ f$ est aussi injective.*

Essayez de démontrer ce théorème en utilisant la définition de l'injectivité. Si vous bloquez, la réponse suit.

Preuve. Utilisons la Définition 2.13 pour montrer l'injectivité de $g \circ f : E \to G$: autrement dit, pour $x, x' \in E$ tels que $g \circ f(x) = g \circ f(x')$, montrons que $x = x'$. Comme $g : F \to G$ est injective et que l'on suppose que $g(f(x)) = g(f(x'))$, on déduit que $f(x) = f(x')$. Alors, comme f est également injective, on déduit de $f(x) = f(x')$ que $x = x'$. Cela prouve l'injectivité de $g \circ f$. ■

Là encore, la réciproque du Théorème 2.8 est fausse : la composée de deux applications, dont l'une au moins n'est pas injective, peut être injective. En guise de contre-exemple vous pouvez reprendre les mêmes applications que dans l'exemple 2.6 ! En effet, $f : [-1, 1] \to \mathbb{R}, x \mapsto \arcsin(x) + \pi/2$ est bien injective alors que $g : \mathbb{R} \to [-1, 1], x \mapsto \cos(x)$ ne l'est pas et que leur composée, $-Id_{[-1,1]}$, l'est.

D'ailleurs, que se passe-t-il si une application est à la fois surjective et injective, comme cela est le cas pour $-Id_{[-1,1]}$? On dira alors qu'elle est bijective ou que c'est une bijection. Dans ce cas, tout élément de son ensemble d'arrivée a un et un seul antécédent.

Définition 2.14 *Une application $f : E \to F$ est* ***bijective*** *si et seulement si elle est injective et bijective. On peut aussi écrire qu'une application est bijective si*

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

ce qui se lit : pour tout élément de l'ensemble d'arrivée de f, il existe un unique antécédent par f dans son ensemble de départ.

Cette définition de la bijectivité doit vous faire penser à la définition d'une application : $\forall x \in E,\ \exists! y \in F,\ y = f(x)$. La similitude entre ces deux définitions est en effet frappante et revient à une inversion de l'ensemble de départ avec l'ensemble d'arrivée. Ainsi, cette définition de la bijectivité permettrait de définir une nouvelle application $g : F \to E$ telle que si $y = f(x)$, alors $g(y) = x$. Cette application g est l'application réciproque de f et elle est définie si et seulement si f est bijective. Vous commencez donc à comprendre l'intérêt de définir ce qu'est la bijectivité, mais aussi l'injectivité et la surjectivité ! Pour parler simplement, g va faire l'inverse de ce que fait f, et si f permet de passer de x à y, alors g permet de faire le chemin inverse, c'est-à-dire de passer de y à x (ainsi, en composant ces deux applications, on obtient une application identité). Cela n'est bien sûr possible que si f est bijective, sinon g ne peut pas être une application car elle pourrait avoir plusieurs images pour un seul antécédent (si f n'est pas injective) ou même aucune image pour un antécédent donné (si f n'est pas surjective).

Théorème 2.9 *Soit $f : E \to F$ une application bijective. Alors il existe une unique application $g : F \to E$ telle que $\forall (x, y) \in E \times F,\ y = f(x) \Leftrightarrow x = g(y)$. Par ailleurs g est telle que $f \circ g = Id_F$ et $g \circ f = Id_E$. g est appelée application* ***réciproque*** *de f et est notée $g = f^{-1}$.*

Nous avons déjà démontré succinctement ce théorème dans le paragraphe précédent, mais vous aurez les idées plus nettes si nous structurons un peu cette preuve :

Preuve. Plusieurs points sont à démontrer :
- il faut déjà montrer que g est bien une application ;

– il faut ensuite vérifier que g est unique ;
– enfin, il faut vérifier que $f \circ g = Id_F$ et $g \circ f = Id_E$.
La bijectivité de f implique que $\forall y \in F,\ \exists! x \in E,\ y = f(x)$, donc $g : F \to E$ telle que si $y = f(x)$ alors $g(y) = x$ est bien définie comme une application (ensemble de départ, ensemble d'arrivée et image unique).

Cette application g est unique car elle est définie explicitement par $\forall (x, y) \in E \times F$, $y = f(x) \Leftrightarrow x = g(y)$: ainsi, à toute image $x \in E$, il existe un unique antécédent $y \in F$ par g, lequel vaut précisément $f(x)$.

Pour ce qui concerne les compositions, l'adéquation croisée entre ensemble de départ et ensemble d'arrivée de f et g assure l'existence des deux composées. Par ailleurs, pour $x \in E$, $g \circ f(x) = x$ car $g(f(x))$ est par définition l'antécédent de $f(x)$ par f. Enfin, pour $x \in F$, $f \circ g(x) = x$ par la définition que l'on a donnée de g. ■

Outre l'application identité, beaucoup d'applications usuelles sont bijectives et admettent donc une inverse :

– $[0, 1] \to [0, 1], x \mapsto x^2$ est bijective d'inverse $[0, 1] \to [0, 1], x \mapsto \sqrt{x}$, alors que $\mathbb{R} \to \mathbb{R}, x \mapsto x^2$ n'est pas bijective ;
– $\mathbb{R} \to \mathbb{R}, x \mapsto x^3$ est bijective d'inverse $\mathbb{R} \to \mathbb{R}, x \mapsto x^{1/3}$;
– $\mathbb{R} \to [0, +\infty[, x \mapsto \exp(x)$ est bijective d'inverse $[0, +\infty[\to \mathbb{R}, x \mapsto \log(x)$;
– $[0, \pi] \to [-1, 1], x \mapsto \cos(x)$ est bijective d'inverse $[-1, 1] \to [0, \pi], x \mapsto \arccos(x)$.

Toutefois, l'identité est une application bijective un peu particulière dans la mesure où elle est sa propre inverse.

Définition 2.15 *Soit f une application bijective dont l'application réciproque est f. Alors f est ce que l'on appelle une* ***involution****.*

L'identité n'est pas le seul exemple d'involution. En voyez-vous d'autres ?

Exemple 2.7 *Un exemple très simple consiste en l'application $x \mapsto -x$. Un autre exemple se trouve grâce à une application monôme, qui a l'avantage de se composer facilement. En effet, pour $(a, b) \in \mathbb{Z}^2$ et pour des ensembles E et F que nous définirons plus tard, les applications $f_a : E \to F, x \mapsto x^a$ et $f_b : F \to E, x \mapsto x^b$ ont pour composée $f_b \circ f_a : E \to E, x \mapsto x^{ab}$, qui vaut Id_E si et seulement si $ab = 1$. Dans le cas d'une involution, on a $a = b$ donc, nécessairement, $a = 1$ ou $a = -1$. Si $a = 1$, f_a est l'application identité. Si $a = -1$ on a une autre application. Il suffit alors de choisir soigneusement E et F. On peut par exemple, pour $c \in]0, 1]$, définir l'involution $[c, 1/c] \to [c, 1/c], x \mapsto 1/x$.*

Pour compléter cet aperçu sur les applications, nous allons ajouter deux énoncés. Le premier stipule que l'inverse d'une inverse est l'application initiale. L'autre, à l'instar de ce que nous avons fait sur les applications surjectives et sur les applications injectives, nous permettra d'affirmer que la composée de deux applications bijectives est bijective.

Proposition 2.4 *Soit $f : E \to F$ une application bijective. Alors, son application inverse, $f^{-1} : F \to E$, est bijective d'inverse $(f^{-1})^{-1} = f$.*

Preuve. Comme $f \circ f^{-1} = Id_F$ et $f^{-1} \circ f = Id_E$, f^{-1} est bijective et son inverse est f. ■

Théorème 2.10 *Soient $f : E \to F$ et $g : F \to G$ deux applications bijectives. Alors $g \circ f$ est aussi bijective et son inverse est $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Preuve. Comme f et g sont bijectives :
- elles sont *a fortiori* injectives, donc le Théorème 2.8 assure que $g \circ f$ est injective ;
- elles sont *a fortiori* surjectives, donc le Théorème 2.7 assure que $g \circ f$ est surjective.

Ainsi, $g \circ f$ est bijective. Par ailleurs, comme on a vu que la position des parenthèses n'importait pas pour la composition des applications, on trouve que :

$$\begin{aligned}(g \circ f) \circ (f^{-1} \circ g^{-1}) &= g \circ (f \circ f^{-1}) \circ g^{-1} \\ &= g \circ Id_F \circ g^{-1} \\ &= g \circ g^{-1} \\ &= Id_G.\end{aligned}$$

Comme $g \circ f$ est bijective, on a prouvé que $f^{-1} \circ g^{-1}$ est son inverse. ■

Notez, dans la démonstration qui précède, que, contrairement à ce qu'indique la définition de l'application réciproque, on montre seulement $(g \circ f) \circ (f^{-1} \circ g^{-1}) = Id_G$ et pas $(f^{-1} \circ g^{-1}) \circ (g \circ f) = Id_E$. Si vous aviez relevé ce point, bravo ! Toutefois, ce n'est pas un oubli de notre part. En effet, pour éviter quelques lignes fastidieuses pour prouver la seconde inégalité (ce n'est pas difficile mais on aime gagner du temps quand on fait des mathématiques ! c'est presque une question d'esthétique...), nous avons eu recours à l'argument selon lequel $g \circ f$ est bijective, ce qui assure, grâce au Théorème 2.9, que son inverse à gauche est égal à son inverse à droite.

Jusqu'à maintenant, nous nous étions intéressés à l'image, par une application, de l'élément d'un ensemble. Ainsi, si $f : E \to F$, nous avions pu parler de $f(x)$ où $x \in E$, les deux ensembles E et F justifiant l'étude des applications dans un chapitre sur la théorie des ensembles. Mais la pertinence de l'évocation des applications dans le présent chapitre s'impose davantage que par la simple définition d'un ensemble de départ et d'un ensemble d'arrivée, dans la mesure où nous pouvons également étudier l'image d'un sous-ensemble par cette même application. Nous parlerons alors d'image directe de A pour $f(A)$, où $A \subset E$.

Définition 2.16 *Soit $f : E \to F$. Soit $A \subset E$. Alors l'**image directe** de A par f est l'ensemble :*

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

Littéralement, c'est l'ensemble constitué des images par f de chaque élément du sous-ensemble A.

Nous avons déjà introduit l'image de f, $Im(f)$, qui n'est autre que l'image directe de l'ensemble de départ de f : $Im(f) = f(E)$.

De même que nous avons défini l'inverse d'un point par une application bijective, de même nous pourrons parler d'image réciproque d'un sous-ensemble par cette même application.

Définition 2.17 *Soit $f : E \to F$. Soit $B \subset F$. Alors l'**image réciproque** de B par f est l'ensemble :*

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

Littéralement, c'est l'ensemble des éléments de E dont l'image par f est dans le sous-ensemble B.

Si f est bijective, alors f^{-1} l'est aussi et vous aurez donc remarqué que l'image réciproque de B par f est simplement l'image directe de B par f^{-1} ! Toutefois, dans la définition de l'image réciproque d'un sous-ensemble, il n'est nul besoin de la bijectivité de l'application. Nous avons donc bien là deux notions distinctes : la réciproque d'une application, appliquée à l'élément d'un ensemble, ce qui nécessite la bijectivité, et l'image réciproque d'un sous-ensemble, qui ne nécessite pas la bijectivité. Par exemple, si $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$, alors f n'est pas bijective et l'on ne pourra pas écrire $f^{-1}(1)$. Pourtant, on pourra définir l'image réciproque du sous-ensemble singleton[1] $\{1\}$: $f^{-1}(\{1\}) = \{-1; 1\}$. Cette image réciproque d'un singleton a deux éléments : cela illustre bien la non-bijectivité de f. Mais, même si l'image réciproque du singleton $\{0\}$ par f est aussi un singleton, on ne pourra qu'écrire $f^{-1}(\{0\}) = \{0\}$ alors que $f^{-1}(0)$ n'aura aucun sens puisque f n'est pas bijective.

1. Un singleton est un ensemble constitué d'un unique élément.

Naturellement, comme nous manipulons des ensembles grâce à ces applications, nous devons nous poser la question de l'image directe et de l'image réciproque d'ensembles formés par une réunion ou une intersection d'ensembles. Pour vous rafraîchir la mémoire, vous pouvez relire les définitions concernant l'union et l'intersection au début de ce chapitre.

Théorème 2.11 *Soit $f : E \to F$ et A et B des parties de E. Alors :*

(i) l'image directe d'une union est l'union des images directes : $f(A \cup B) = f(A) \cup f(B)$;

(ii) l'image directe d'une intersection est incluse dans l'intersection des images directes : $f(A \cap B) \subset f(A) \cap f(B)$.

(iii) De plus, si f est injective, alors $f(A \cap B) = f(A) \cap f(B)$.

Preuve.

(i) Nous introduisons un élément y de F et nous montrons que son appartenance à $f(A \cup B)$ est équivalente à son appartenance à $f(A) \cup f(B)$, ce qui revient à prouver que ces deux ensembles sont égaux. Notons que cette démonstration nécessite des rudiments de logique pour la manipulation des *ou* et des *et* :

$$\begin{aligned}
& y \in f(A \cup B) \\
\Leftrightarrow\ & \exists x \in A \cup B, f(x) = y \\
\Leftrightarrow\ & \exists x \in E, (\exists x \in A \text{ ou } \exists x \in B) \text{ et } f(x) = y \\
\Leftrightarrow\ & \exists x \in E, (\exists x \in A \text{ et } f(x) = y) \text{ ou } (\exists x \in B \text{ et } f(x) = y) \\
\Leftrightarrow\ & (\exists x \in A, f(x) = y) \text{ ou } (\exists x \in B, f(x) = y) \\
\Leftrightarrow\ & y \in f(A) \text{ ou } y \in f(B) \\
\Leftrightarrow\ & y \in f(A) \cup f(B).
\end{aligned}$$

(ii) Soit $y \in f(A \cap B)$. Alors il existe $x \in A \cap B$ tel que $f(x) = y$. Ainsi, il existe $x \in A$ tel que $f(x) = y$ et il existe $x \in B$ tel que $f(x) = y$. Donc $y \in f(A)$ et $y \in f(B)$, autrement dit $y \in f(A) \cap f(B)$. Nous avons alors montré que $f(A \cap B) \subset f(A) \cap f(B)$.

(iii) L'assertion *(ii)* du Théorème 2.11 démontrant l'une des deux inclusions, il ne reste plus qu'à montrer que $f(A) \cap f(B) \subset f(A \cap B)$. Soit $y \in f(A) \cap f(B)$. Il existe donc $x_A \in A$ et $x_B \in B$ tels que $f(x_A) = y$ et $f(x_B) = y$. Ainsi, $f(x_A) = f(x_B)$. Or, par hypothèse, f est injective, donc $x_A = x_B$. Par conséquent, nous pouvons affirmer que $x_A \in A \cap B$. Ainsi, $y \in f(A \cap B)$, ce qui prouve $f(A) \cap f(B) \subset f(A \cap B)$ et finalement $f(A \cap B) = f(A) \cap f(B)$.

■

Pour prouver l'assertion *(i)* du Théorème 2.11, nous aurions pu procéder en démontrant successivement l'inclusion de $f(A \cup B)$ dans $f(A) \cup f(B)$, puis l'inclusion de $f(A) \cup f(B)$ dans $f(A \cup B)$. Toutefois, en faisant de la sorte, nous aurions doublé nos efforts dans la mesure où la démonstration des deux inclusions présente les mêmes difficultés et qu'un raisonnement par équivalence est tout à fait possible dans la mesure où il ne camoufle pas de difficulté particulière. Pour vous assurer qu'il est effectivement légitime de raisonner par équivalence, relisez la série d'équivalences dans la preuve à partir de la fin !

Par ailleurs, notez bien que si f n'est pas injective alors l'égalité $f(A \cap B) = f(A) \cap f(B)$ n'est pas nécessairement vraie. Prenez une feuille et un crayon et trouvez un contre-exemple convaincant ! Bien comprendre le rôle de l'injectivité dans ce cas précis vous permettra de mieux retenir ou retrouver le sens de l'inclusion qui fonctionne sans une telle hypothèse, à savoir $f(A \cap B) \subset f(A) \cap f(B)$ et non pas $f(A) \cap f(B) \subset f(A \cap B)$.

Exemple 2.8 *L'exemple le plus simple est une application constante, laquelle, si son ensemble de départ est constitué d'au moins deux éléments, n'est pas injective. Prenons par exemple* $f : \{0; 1\} \to \{1\}, x \mapsto 1$. *Considérons l'image directe de deux singletons distincts :* $f(\{0\}) = \{1\}$ *et* $f(\{1\}) = \{1\}$. *Ainsi,* $f(\{0\}) \cap f(\{1\}) = \{1\}$, *alors que* $f(\{0\} \cap \{1\}) = f(\emptyset) = \emptyset$. *Il est donc clair que l'on a* $f(\{0\} \cap \{1\}) \subset f(\{0\}) \cap f(\{1\})$ *mais que l'autre inclusion est fausse.*

Maintenant que vous maîtrisez tout ce qui concerne l'image directe d'une union ou d'une intersection grâce au Théorème 2.11, vous allez pouvoir développer des résultats similaires pour les images réciproques dans le théorème suivant :

Théorème 2.12 *Soit* $f : E \to F$ *et* A *et* B *des parties de* F. *Alors :*

(i) l'image réciproque d'une union est l'union des images réciproques : $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$ *;*

(ii) l'image réciproque d'une intersection est l'intersection des images réciproques : $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$ *;*

(iii) l'image réciproque d'un complémentaire est le complémentaire de l'image réciproque : $f^{-1}(F \backslash A) = E \backslash f^{-1}(A)$.

Vous remarquez que l'énoncé du Théorème 2.12 est plus simple à retenir que celui du Théorème 2.11. En particulier, aucune condition d'injectivité ou de surjectivité n'est ici demandée pour avoir l'égalité entre l'image réciproque d'une intersection et l'intersection des images réciproques. Ceci est possible car la définition de l'image réciproque est plus simple que celle de l'image directe. Nous vous rappelons que $f^{-1}(B) = \{x \in E | f(x) \in B\}$ alors que $f(A) = \{y \in$

$F|\exists x \in A, y = f(x)\}$. Ainsi, la définition de l'image directe stipule l'existence d'un élément aux caractéristiques précises (son image par f vaut y), or prouver l'existence est souvent ce qui peut poser des problèmes dans un raisonnement mathématique. Saurez-vous donc démontrer ce théorème ?

Preuve. **(i)** La démonstration de ce point est similaire à ce que l'on a fait dans la démonstration du Théorème 2.11 à propos de l'image directe d'une union :

$$\begin{array}{ll} & x \in f^{-1}(A \cup B) \\ \Leftrightarrow & f(x) \in A \cup B \\ \Leftrightarrow & (f(x) \in A \text{ ou } f(x) \in B) \\ \Leftrightarrow & x \in f^{-1}(A) \text{ ou } x \in f^{-1}(B) \\ \Leftrightarrow & x \in f^{-1}(A) \cup f^{-1}(B). \end{array}$$

Ceci prouve que $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

(ii) La difficulté qui apparaissait dans le Théorème 2.11 pour l'intersection n'est pas présente ici, et l'on peut raisonner directement par équivalence :

$$\begin{array}{ll} & x \in f^{-1}(A \cap B) \\ \Leftrightarrow & f(x) \in A \cap B \\ \Leftrightarrow & (f(x) \in A \text{ et } f(x) \in B) \\ \Leftrightarrow & x \in f^{-1}(A) \text{ et } x \in f^{-1}(B) \\ \Leftrightarrow & x \in f^{-1}(A) \cap f^{-1}(B). \end{array}$$

Alors $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.

(iii) Là encore le raisonnement par équivalence prévaut :

$$\begin{array}{ll} & x \in f^{-1}(F \backslash A) \\ \Leftrightarrow & f(x) \in F \backslash A \\ \Leftrightarrow & (f(x) \in F \text{ et } f(x) \notin A). \end{array}$$

Sachant que $f(x) \in F$ est toujours vrai par définition de l'application f qui a F pour ensemble d'arrivée, nous pouvons poursuivre le raisonnement :

$$\begin{array}{ll} & (f(x) \in F \text{ et } f(x) \notin A) \\ \Leftrightarrow & \text{non } (f(x) \in A) \\ \Leftrightarrow & \text{non } (x \in f^{-1}(A)). \end{array}$$

Comme $x \in E$ par hypothèse (en effet, E est l'ensemble de départ de f), cette dernière ligne est équivalente à $x \in E \backslash f^{-1}(A)$. Ainsi, nous avons prouvé que $f^{-1}(F \backslash A) = E \backslash f^{-1}(A)$. ■

Retournons quelques instants à la définition que nous avons donnée pour les applications. Vous vous rappelez que, outre le graphe, il faut aussi l'ensemble de départ et l'ensemble d'arrivée pour caractériser une application. Ainsi, les applications $f : [0,1] \to [0,1], x \mapsto x^2$ et $g : [-1,1] \to [0,1], x \mapsto x^2$ sont-elles différentes car d'ensembles de départ distincts. Toutefois, dans les deux cas, l'habitude nous les fait désigner indistinctement sous le vocable d'application carré ; cette imprécision n'a pas sa place dans un raisonnement mathématique mais il faut reconnaître que ces deux applications ne sont pas sans rapport l'une pour l'autre. En fait, f est ce que l'on appelle la restriction de g au segment $[0,1]$, alors que g est un prolongement de f à $[-1,1]$. Nous allons maintenant définir rigoureusement ces deux notions qui permettent de jouer sur l'ensemble de départ d'une application.

Définition 2.18 *Soit $f : E \to F$ une application. Soit A une partie de E et B un ensemble contenant E.*
- *La **restriction** de f à A est l'application $f_{|A} : A \to F, x \mapsto f(x)$.*
- *Un **prolongement** de f à B est une application $g : B \to F$ telle que $g_{|E} = f$, c'est-à-dire telle que $\forall x \in E, g(x) = f(x)$.*

Les termes de la définition sont très clairs en français : la restriction correspond à l'utilisation d'un ensemble de départ plus petit alors qu'un prolongement désigne l'agrandissement de l'ensemble de départ. Par ailleurs, pour une application donnée, la restriction est unique, d'où l'article défini dans *la restriction. A contrario*, pour une application donnée, il peut y avoir plusieurs prolongements, d'où l'article indéfini dans *un prolongement*. En effet, l'application $[0,1[\to \mathbb{R}, x \mapsto 0$ admet par exemple, comme prolongements à $\mathbb{R}$, une infinité d'applications, dont :
- $\mathbb{R} \to \mathbb{R}, x \mapsto 0$;
- $\mathbb{R} \to \mathbb{R}, x \mapsto \max\{n \in \mathbb{Z} | n \leq x\}$, qui est l'application partie entière.

Rappelez-vous le début de cette partie du cours sur les applications : nous avions déjà évoqué ces deux applications carré $f : [0,1] \to [0,1], x \mapsto x^2$ et $g : [-1,1] \to [0,1], x \mapsto x^2$ pour illustrer l'injectivité. En effet, de ces deux applications *a priori* similaires, une seule est injective : c'est f. Ainsi, en jouant simplement sur l'ensemble de départ, nous avions deux applications dont l'une seulement avait cette agréable propriété d'injectivité. Naturellement, c'était l'application dont l'ensemble de départ était inclus dans l'autre qui était injective, la situation inverse étant de fait exclue par la contraposée de la proposition suivante.

Proposition 2.5 *Soit $f : E \to F$ et A une partie de E. Alors, si f est injective, $f_{|A}$ est aussi injective.*

Preuve. Supposons que f est injective. Montrons que $f_{|A}$ l'est aussi. Soient $x, y \in A \subset E$, tels que $f_{|A}(x) = f_{|A}(y)$. Pour prouver l'injectivité de $f_{|A}$, montrons que $x = y$. Nous avons $f_{|A}(x) = f_{|A}(y)$, c'est-à-dire, par définition de la restriction, $f(x) = f(y)$. Comme f est injective, nous avons $x = y$. Ainsi $f_{|A}$ est bien injective. ■

Notez que cette proposition est fausse pour la surjectivité : si f est surjective, $f_{|A}$ n'est pas nécessairement surjective. Essayez de trouver un contre-exemple !

Exemple 2.9 *Pensez à une application surjective très simple, comme l'identité. Si vous restreignez son ensemble de départ sans toucher à son ensemble d'arrivée, vous n'avez plus l'identité et vous n'avez plus non plus la surjectivité. Vérifiez-le ! Un autre exemple, très radical, consiste à considérer n'importe quelle application f surjective, définie entre deux ensembles non vides. La restriction de cette application à l'ensemble vide n'est clairement pas surjective. Attention toutefois à bien avoir f définie entre deux ensembles non vides ! En effet, si l'ensemble d'arrivée de f, que nous noterons F, est l'ensemble vide, alors f et sa restriction à n'importe quel ensemble sont nécessairement surjectives, car la condition commençant par $\forall y \in F = \emptyset$ que vous pouvez lire dans la définition de la surjectivité sera toujours vraie.*

Si la restriction d'une application surjective n'est pas nécessairement surjective, un prolongement d'une application surjective, en revanche, l'est, comme le stipule la proposition qui suit :

Proposition 2.6 *Soit $f : E \to F$ et A une partie de E. Alors, si $f_{|A}$ est surjective, f est aussi surjective.*

Là encore, la preuve est simple et se résume à une bonne analyse de la situation et de la définition de la surjectivité. Essayez de démontrer cette proposition avant de vérifier que votre démarche est bonne en lisant la suite.

Preuve. Supposons que $f_{|A}$ est surjective. Montrons que f l'est aussi. Soit $y \in F$. Pour prouver la surjectivité de f, montrons qu'il existe $x \in E$ tel que $f(x) = y$. Comme $f_{|A}$ est surjective, il existe par définition $z \in A$ tel que $f_{|A}(z) = y$. Posons $x = z$. Comme $A \subset E$, nous avons bien $x \in E$. Par ailleurs, $f(x) = f(z) = f_{|A}(z) = y$, donc f est bien surjective. ■

Comme vous l'aurez compris, la propriété d'injectivité est conservée lors d'une restriction alors que pour un prolongement c'est la propriété de surjectivité qui reste. Ainsi, vous pouvez vous douter que nous ne pouvons pas transcrire cette dernière proposition pour l'injectivité : si $f_{|A}$ est injective, f n'est pas nécessairement injective. Pour en être totalement convaincu, un contre-exemple est bien utile !

Exemple 2.10 *Vous devez à l'évidence percevoir que l'application identité est injective. En revanche, aucun prolongement de cette application ne peut être* *injectif (sauf pour un unique cas que les esprits malicieux auront détecté : si on prolonge Id_E à E on obtient Id_E, qui est bien injective, certes). En effet, si f est un prolongement de Id_E à un ensemble A distinct de E et tel que $E \subset A$ (sans cette inclusion, la prolongation n'a pas de sens), il n'est pas difficile de montrer que f n'est pas injective. Comme $A\backslash E \neq \emptyset$, nous pouvons considérer $x \in A\backslash E$. Notons y l'image de x par f. E étant l'ensemble d'arrivée de Id_E et de tous ses prolongements, f compris, nous savons que $y \in E$. Or, cet élément a au moins deux antécédents distincts par f, à savoir x (par hypothèse) et y (car f est un prolongement de l'identité). Nous sommes bien certains que ces deux antécédents sont distincts car $x \in A\backslash E$ et $y \in E$. Donc f n'est pas injective !*

2.3 Relations binaires

A ce stade du chapitre, vous savez ce qu'est un ensemble et vous êtes capable d'effectuer de multiples opérations dessus : des intersections, des unions, etc. Nous allons maintenant nous intéresser à une échelle plus microscopique, c'est-à-dire non pas à l'ensemble en tant que tel mais aux relations qui lient les éléments constituant cet ensemble. Par exemple, pour être très concret, considérons l'ensemble B_a des élèves admis au baccalauréat une année a. Si vous vous intéressez à l'échelle macroscopique, vous pouvez par exemple faire l'union de ces ensembles correspondant à des années différentes : vous obtiendrez l'ensemble $B = \bigcup_i B_{a_i}$ de la population diplômée du baccalauréat, sans distinction d'année d'obtention du diplôme. Mais si vous vous intéressez aux élèves qui constituent cet ensemble B_a, donc à l'échelle microscopique, vous pouvez faire un peu de tri. Vous pouvez par exemple classer ces élèves en fonction de la mention obtenue : vous définirez alors une relation d'équivalence (les élèves $x, y \in B_a$ sont équivalents s'ils ont la même mention). S'il n'y a pas d'ex-aequo, vous pouvez aussi les trier par ordre croissant de moyenne obtenue : c'est ce que l'on appelle une relation d'ordre. Nous allons maintenant définir plus rigoureusement ces deux notions de relation d'équivalence et de relation d'ordre et voir ce que les mathématiques nous en disent.

Dans cette partie, E désigne un ensemble non vide.

Tout d'abord, ces deux relations dérivent d'une même définition qui est celle de la relation binaire.

Définition 2.19 *Une assertion $\mathcal{R}(x, y)$ dépendant de deux éléments $x, y \in E$, ou aussi parfois écrite $x\mathcal{R}y$, est une* ***relation binaire*** *sur E.*

Notez bien que l'ordre des éléments a son importance et que si l'on a $\mathcal{R}(x, y)$, on n'a pas nécessairement $\mathcal{R}(y, x)$.

L'ensemble de tous les couples liés par une relation binaire donnée est le graphe de cette relation : $\Gamma_{\mathcal{R}} = \{(x, y) \in E^2 | x\mathcal{R}y\}$. Vous connaissez déjà ce terme de graphe que nous avions introduit pour les applications. Vous aviez alors lu qu'une application était définie par un ensemble de départ, un ensemble d'arrivée et un graphe. Mieux que définie, elle était même caractérisée par la donnée de ces trois éléments, ce qui signifie que si deux applications ont le même ensemble de départ, le même ensemble d'arrivée et le même graphe, alors elles sont égales. Nous pouvons faire une analogie avec les relations binaires, lesquelles sont caractérisées par un ensemble et un graphe. Mais applications et relations binaires ne sont pas une même chose, vous devez vous en douter.

- Ainsi, toute application n'est pas nécessairement une relation binaire. Toutefois, si une application a pour ensemble de départ et ensemble d'arrivée un même ensemble, $f : E \to E$, alors cette application définit une relation binaire sur l'ensemble E, de graphe $\{(x, y) \in E^2 | f(x) = y\}$.
- Symétriquement, toute relation binaire n'est pas nécessairement une application. Voyez-vous pourquoi ? Si l'on voulait construire une application f à partir d'une relation binaire $\mathcal{R}$ sur E, l'ensemble de départ et l'ensemble d'arrivée ne poseraient pas de problème : ce serait E. En revanche, pour $x \in E$, on ne pourrait pas toujours définir une image y par f en prenant y tel que $x\mathcal{R}y$, car un tel y n'existe pas nécessairement ou bien il peut être multiple, alors que dans la définition d'une application, il doit exister et être unique. Pour pouvoir définir une application à partir de cette méthode inspirée par l'intuition, il faudrait la condition : $\forall x \in E, \exists! y, x\mathcal{R}y$.

Cette dernière condition ne sera jamais remplie par un certain type de relation que nous avons abordé brièvement en introduction, la relation d'ordre, dès lors que cette relation établit au moins un lien entre éléments distincts. Définissons d'abord ce type de relation et voyons ensuite pourquoi nous n'aurons jamais $\forall x \in E, \exists! y, x\mathcal{R}y$ si $\mathcal{R}$ établit au moins un lien entre éléments distincts.

2.3.1 Relations d'ordre

Définition 2.20 *Une relation binaire $\mathcal{R}$ sur E est une* **relation d'ordre** *sur E, si :*
- *$\mathcal{R}$ est réflexive, ce qui signifie que $\forall x \in E, x\mathcal{R}x$;*
- *$\mathcal{R}$ est antisymétrique, ce qui signifie que $\forall (x, y) \in E^2, (x\mathcal{R}y \text{ et } y\mathcal{R}x) \Rightarrow x = y$;*
- *$\mathcal{R}$ est transitive, ce qui signifie que $\forall (x, y, z) \in E^3, (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$.*

Revenons un instant sur la condition $\forall x \in E, \exists! y, x\mathcal{R}y$, nécessaire pour bâtir une application à partir d'une relation selon la méthode que nous avons définie précédemment. Supposons que $\mathcal{R}$ soit une relation d'ordre. Raisonnons en supposant que $\forall x \in E, \exists! y, x\mathcal{R}y$. Soit $x \in E$. Comme une relation d'ordre est réflexive, nous savons déjà que $x\mathcal{R}x$. Par ailleurs, par hypothèse, l'élément $y \in E$ tel que $x\mathcal{R}y$ est unique ; c'est donc x et l'on peut écrire $\forall y \neq x, \mathrm{non}(x\mathcal{R}y)$. Ainsi, avec cette hypothèse, la relation d'ordre n'établit aucun lien entre éléments distincts. C'est le seul cas possible où, avec la méthode proposée, nous saurons construire une application à partir d'une relation d'ordre. Dans un contexte plus général, où l'on ne se limite pas à ce cas très particulier de relation d'ordre, on ne pourra donc pas définir d'application à partir d'une relation d'ordre. Cela justifie l'originalité d'un tel objet, bien différent de ce que vous avez vu dans le début du chapitre à propos des applications.

Pour bien comprendre à quoi correspondent les propriétés de réflexivité, d'antisymétrie et de transitivité, appuyons-nous sur un exemple très simple que vous connaissez : l'ordre naturel de comparaison des nombres réels.

Exemple 2.11 *Nous notons $\leq$ la relation d'ordre naturel de comparaison des nombres réels.*

- *C'est une relation binaire : cela est évident car elle concerne toujours la comparaison de deux éléments, mais il est toujours bon de vérifier toutes les conditions de la définition, et la binarité en fait partie.*
- *C'est une relation réflexive, car pour tout réel x on peut écrire $x \leq x$: x est inférieur ou égal à x, en l'occurrence égal.*
- *C'est une relation antisymétrique car si $x \leq y \leq x$, vous savez que $x = y$.*
- *C'est une relation transitive car si $x \leq y \leq z$, vous savez également que $x \leq z$.*

L'inégalité large est une relation d'ordre. Pensez-vous que l'inégalité stricte soit aussi une relation d'ordre ?

Exemple 2.12 *Non ! L'inégalité stricte ne constitue pas une relation d'ordre. Certes, l'antisymétrie et la transitivité sont bien vérifiées pour cette relation binaire ; notez au passage que la condition ($x\mathcal{R}y$ et $y\mathcal{R}x$) n'est jamais vraie, ce qui garantit l'antisymétrie (rappelez-vous le chapitre sur la logique : pour deux assertions A et B, l'assertion $A \Rightarrow B$ signifie (B ou non(A))). Mais l'inégalité stricte n'est pas réflexive. En effet, pour tout réel x, on ne peut avoir $x < x$, laquelle assertion implique que $x \neq x$.*

Voici un autre exemple, qui évoquera des définitions lues au début de ce chapitre sur la théorie des ensembles : l'ordre sur $\mathcal{P}(E)$, défini par l'inclusion :

pour $A, B \in \mathcal{P}(E)$, $A \subset B$ si $\forall x \in E, x \in A \Rightarrow x \in B$. Nous vous laissons vérifier rigoureusement que cette relation est bien une relation d'ordre.

Une différence notoire entre l'ordre naturel de comparaison des nombres réels et l'ordre d'inclusion sur $\mathcal{P}(E)$ est que la première relation d'ordre permet de classer tous les éléments sur lesquels la relation s'applique alors que ce n'est pas toujours le cas pour la deuxième relation. C'est la distinction entre ordre total et ordre partiel :

Définition 2.21 *Une relation d'ordre sur E est* ***totale*** *si*

$$\forall (x,y) \in E^2, x\mathcal{R}y \text{ ou } y\mathcal{R}x,$$

c'est-à-dire si les éléments de E sont deux à deux comparables. E muni de la relation $\mathcal{R}$ est alors un ensemble totalement ordonné. Une relation d'ordre qui n'est pas totale est dite ***partielle****.*

Si le fait que l'ordre naturel de comparaison des nombres réels soit total saute aux yeux, l'ordre d'inclusion sur $\mathcal{P}(E)$ n'est total que si E a au plus un élément. En effet, dans le cas contraire, si E a au moins deux éléments distincts x et y, on ne peut pas utiliser la relation d'inclusion pour comparer entre eux les ensembles singletons $\{x\}$ et $\{y\}$.

Nous avons donc défini la relation d'ordre. Vous êtes donc capable de classer des éléments d'un ensemble selon une telle relation. Dans certains cas, vous serez même en mesure de trouver un minorant d'un ensemble. Par exemple, selon l'ordre naturel, 0 est un minorant des réels positifs ou nuls. C'est aussi le cas, à plus forte raison, de -1. En revanche vous aurez quelques difficultés à définir un minorant pour cet ordre sur l'ensemble des réels, positifs et négatifs...

Définition 2.22 *Soit $F \subset E$.*
- *On dit que $x \in E$ est un* ***minorant*** *de F si $\forall y \in F, x\mathcal{R}y$.*
- *On dit que $x \in E$ est un* ***majorant*** *de F si $\forall y \in F, y\mathcal{R}x$.*

Si un minorant (respectivement un majorant) existe pour F, alors F est minoré (respectivement majoré). Si F est à la fois minoré et majoré, on dit qu'il est ***borné****.*

Dans cette définition, le majorant ou le minorant n'appartient pas nécessairement au sous-ensemble considéré. Il peut même y avoir plusieurs minorants ou majorants. En revanche, si un sous-ensemble admet un minorant ou un majorant en son sein, celui-ci est unique. Il est appelé le min, ou le max.

Définition 2.23 *Soit $F \subset E$.*
- *On dit que $x \in E$ est le plus petit élément de F si $x \in F$ et x minore F. On note alors $x = \min F$.*

– *On dit que $x \in E$ est le plus grand élément de F si $x \in F$ et x majore F. On note alors $x = \max F$.*

Proposition 2.7 *Soit $F \subset E$. Le plus petit élément (respectivement le plus grand élément) de F, s'il existe, est unique.*

Preuve. Montrons-le pour le plus grand élément, le cas du plus petit élément étant similaire. Supposons que F admette deux plus grands éléments, x et y. Montrons que ces deux éléments ne sont pas différents l'un de l'autre. Comme y est le plus grand élément de F, $y \in F$. Aussi, comme x est le plus grand élément de F, $z\mathcal{R}x$ pour tout élément $z \in F$. Donc $y\mathcal{R}x$. Nous pouvons aussi montrer que $x\mathcal{R}y$ en utilisant les propriétés du plus grand élément pour x et y. Comme la relation d'ordre est antisymétrique et que l'on a $y\mathcal{R}x$ et $x\mathcal{R}y$, nous pouvons conclure que $x = y$, ce qui prouve l'unicité du plus grand élément. ■

Nous avons montré que le plus petit (ou le plus grand) élément d'un ensemble est unique si ce plus petit élément (ou ce plus grand élément) existe. Mais rien ne le garantit *a priori*. En particulier, vous avez déjà constaté que pour l'ordre naturel $\mathbb{R}$ n'admet pas de plus petit élément, au contraire de $[0, \infty[$. Dans certains cas, cependant, un théorème bien utile nous permettra d'affirmer que le min et le max d'un sous-ensemble existent.

Théorème 2.13 *Soit $F \subset E$ <u>fini</u> et <u>non vide</u>. Si $\mathcal{R}$ est un ordre total sur F, alors $\min F$ et $\max F$ existent.*

Dans le Théorème 2.13, vous avez lu comme hypothèse que le sous-ensemble devait être non vide. Que se passe-t-il si un sous-ensemble est vide ? Naturellement, l'ensemble vide ne contenant aucun élément et $\min F$ et $\max F$ faisant partie de l'ensemble F, l'ensemble vide n'a pas de min ni de max. Dit plus simplement, l'ensemble vide n'a pas de plus petit ni de plus grand élément puisqu'il n'a pas d'éléments. En revanche, si E est non vide, l'ensemble vide est borné. En effet, tout élément de E minore et majore l'ensemble vide. Si vous n'êtes pas convaincu, pour que $x \in E$ (x existe bien car nous avons imposé $E \neq \emptyset$) minore l'ensemble vide, $\emptyset$, il faut que $\forall y \in \emptyset, x\mathcal{R}y$. Or la condition $\forall y \in \emptyset$ implique que la suite de l'assertion est nécessairement vraie puisque $x\mathcal{R}y$ doit être vérifiée pour tout $y \in \emptyset$, c'est-à-dire pour aucun y. Ainsi, tout $x \in E$ minore $\emptyset$. Nous vous laissons raisonner par vous-même pour vérifier que c'est aussi le cas pour la majoration.

Prouvons maintenant le Théorème 2.13. Voyez-vous comment commencer cette démonstration ? La remarque précédente a souligné l'importance d'avoir F non vide. Ce point aura certainement une place centrale dans la démonstration. L'autre hypothèse relative à F indique que cet ensemble est fini, ce qui signifie que vous serez capable de compter ses éléments, de les indexer par un entier naturel. Toujours pas d'idée ? Dans ce cas, on peut essayer d'ajouter une hypothèse pour rendre l'énoncé très simple à prouver. Si l'on impose par exemple un très faible nombre d'éléments dans F, le raisonnement vous semblera peut-être plus clair. Supposons donc un instant que F a un unique élément. Rien de plus simple alors ! Grâce à la réflexivité de la relation d'ordre, cet élément est à la fois le min et le max de F. Et si l'on complique un peu l'énoncé en ajoutant un autre élément à F, qui en compte maintenant deux, la résolution ne sera pas beaucoup plus compliquée puisque vous pourrez comparer directement ce nouvel élément avec le plus petit et le plus grand élément que vous aviez pour F avant l'ajout de son deuxième élément. Bon, vous devez commencer à comprendre : un raisonnement par récurrence devrait vous permettre de démontrer le Théorème 2.13.

Preuve. Raisonnons donc par récurrence :

- Pour initialiser cette récurrence, il faut faire l'hypothèse que F n'a qu'un seul élément, $x \in F \subset E$. F est donc fini et non vide, ce qui est en accord avec les hypothèses du Théorème 2.13. Comme $\mathcal{R}$ est une relation d'ordre, elle est en particulier réflexive. Donc $x\mathcal{R}x$. Or x est le seul élément de F, donc $\forall y \in F$, $x\mathcal{R}y$ et $y\mathcal{R}x$: x majore et minore F. Comme, de plus, $x \in F$, alors x est à la fois le min de F et son max. La propriété est démontrée si F a un unique élément.
- Itérons maintenant le raisonnement : nous supposons que l'on a démontré le théorème pour tout sous-ensemble F contenant exactement $n > 0$ éléments. Montrons-le pour un sous-ensemble contenant $n + 1$ éléments. Soit, donc, F un sous-ensemble de E tel que F contient $n + 1$ éléments. Soit $x \in F$ et $G = F \backslash \{x\}$. G contient n éléments (il est donc, fini, non vide, inclus dans E car $G \subset F \subset E$ et $\mathcal{R}$ est un ordre total sur G car si les éléments de F sont comparables deux à deux, ceux de G le sont *a fortiori*), donc, par hypothèse, $\min G$ et $\max G$ existent. Comme l'ordre est total sur F, on a $x\mathcal{R}(\min G)$ ou bien $(\min G)\mathcal{R}x$. Dans le premier cas, par transitivité, x minore G ; de plus, par réflexivité, x minore $F = G \cup \{x\}$, donc, comme $x \in F$, x est le min de F. Dans le second, cas, si $(\min G)\mathcal{R}x$, alors, par définition, $\min G$ minore G puis, car $(\min G)\mathcal{R}x$, $\min G$ minore $F = G \cup \{x\}$; de plus $(\min G) \in G \subset F$, donc $\min G$ est également le min de F. Le même raisonnement peut être conduit pour le max et l'on a ainsi montré que si le théorème est vrai au rang n alors il l'est aussi au rang $n + 1$.

Conclusion : le théorème est vrai si F contient un unique élément. De plus, si le théorème est vrai pour un ensemble contenant $n > 0$ éléments, alors il est vrai pour un ensemble contenant $n + 1$ éléments. Ainsi, le théorème est-il prouvé pour tout ensemble $F \subset E$ fini et non vide. ■

Pour ne pas utiliser le Théorème 2.13 à mauvais escient, frottez-vous aux exemples suivant :

Exemple 2.13 *Des ensembles suivants, munis de l'ordre naturel de comparaison des nombres, lesquels ont un min et un max :* $\mathbb{N}$, $\mathbb{Z}$, $]0,1[$, $[0,1]$ *?*

- $\mathbb{N}$ *est un ensemble infini, donc le Théorème 2.13 ne permet pas de conclure. Vous savez pourtant bien que* $\min \mathbb{N} = 0$ *et un raisonnement simple vous affranchira du recours au moindre théorème. Néanmoins, si l'on définit, pour* $n > 0$*, l'ensemble* N_n *par* $\{m \in \mathbb{N} | m \leq n\}$*, alors* N_n *est fini, non vide et muni d'un ordre total. Son min et son max existent donc d'après le Théorème 2.13 : vous relèverez simplement que ce sont 0 et* n*.*
- *De même,* $\mathbb{Z}$, $]0,1[$, $[0,1]$ *sont des ensembles infinis donc le Théorème 2.13 ne permet pas d'affirmer l'existence d'un min ou d'un max. En l'occurrence, parmi ces trois ensembles, seul* $[0,1]$ *a un min et un max : 0 et 1. Notez bien que, pour l'intervalle ouvert* $]0,1[$*, 0 et 1 ne sont pas un min et un max mais simplement le plus grand minorant et le plus petit majorant.*

2.3.2 Relations d'équivalence

L'autre type de relation binaire que nous vous proposons de découvrir est la relation d'équivalence. Elle se distingue de la relation d'ordre par l'une de ses propriétés : au lieu d'être antisymétrique, elle est symétrique :

Définition 2.24 *Une relation binaire* $\mathcal{R}$ *sur* E *est une* ***relation d'équivalence*** *sur* E*, si :*

- $\mathcal{R}$ *est réflexive, ce qui signifie que* $\forall x \in E, x\mathcal{R}x$ *;*
- $\mathcal{R}$ *est symétrique, ce qui signifie que* $\forall (x,y) \in E^2, (x\mathcal{R}y \iff y\mathcal{R}x)$ *;*
- $\mathcal{R}$ *est transitive, ce qui signifie que* $\forall (x,y,z) \in E^3, (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$*.*

Notez que l'on raisonne parfois par classe d'équivalence, qui sont des ensembles dont tous les éléments sont liés par la même relation d'équivalence. Ainsi, cela peut justifier l'usage d'une notation alternative dans laquelle $\mathcal{R}(x)$ désigne l'ensemble des éléments de E équivalents à x, pour $x \in E$:

Définition 2.25 *Soit* $\mathcal{R}$ *une relation d'équivalence sur* E *et soit* $x \in E$*. Alors, l'ensemble* $\mathcal{R}(x) = \{y \in E, y\mathcal{R}x\}$ *est la classe d'équivalence de* x *selon* $\mathcal{R}$*. Un élément de cette classe d'équivalence est appelé un représentant de la classe.*

On utilise cette notation de classe d'équivalence dans le théorème suivant :

Théorème 2.14 *Soient* $x, y \in E$*. Alors :*

1. $\mathcal{R}(x) = \mathcal{R}(y) \iff x\mathcal{R}y$ *;*
2. $\mathcal{R}(x) \cap \mathcal{R}(y) \neq \emptyset \implies \mathcal{R}(x) = \mathcal{R}(y)$*.*

Pour la démonstration du premier point, il s'agit de prouver une équivalence. Vous connaissez maintenant bien la principale méthode pour prouver une équivalence : il faut prouver chacune des deux implications qui la constituent, l'une après l'autre. Sinon, la preuve n'a aucune difficulté mais requiert que vous utilisiez certaines caractéristiques de la relation d'équivalence. Ce sera donc l'occasion de vérifier que vous en connaissez bien la définition.

Preuve.

1. – Montrons dans un premier temps l'implication de gauche à droite. On suppose que $\mathcal{R}(x) = \mathcal{R}(y)$. Comme, par définition, $\mathcal{R}$ est réflexive, on peut écrire $x \in \mathcal{R}(x)$. Par hypothèse, $\mathcal{R}(x) = \mathcal{R}(y)$, donc $x \in \mathcal{R}(y)$, ce qui s'écrit aussi $x\mathcal{R}y$.
   – Montrons maintenant l'implication droite gauche, ce qui, en l'invoquant conjointement avec le point précédent, reviendra à prouver l'équivalence de l'énoncé. Supposons donc que $x\mathcal{R}y$. Nous voulons montrer que $\mathcal{R}(x) = \mathcal{R}(y)$, ce que nous pouvons faire en montrant successivement les deux inclusions : $\mathcal{R}(x) \subset \mathcal{R}(y)$ et $\mathcal{R}(y) \subset \mathcal{R}(x)$. Or, la relation d'ordre est symétrique, donc si l'on suppose $x\mathcal{R}y$, on a symétriquement $y\mathcal{R}x$, ce qui justifie que démontrer l'une des deux inclusions suffit pour prouver l'égalité entre les ensembles $\mathcal{R}(x)$ et $\mathcal{R}(y)$. Montrons donc que $\mathcal{R}(x) \subset \mathcal{R}(y)$. Pour ce faire, considérons $z \in \mathcal{R}(x)$ et prouvons que $z \in \mathcal{R}(y)$. Or, nous avons supposé que $z\mathcal{R}x$ et que $x\mathcal{R}y$. Ainsi, par transitivité de la relation d'équivalence, on obtient $z\mathcal{R}y$, c'est-à-dire $z \in \mathcal{R}(y)$. Cela termine cette preuve.
2. Comme $\mathcal{R}(x) \cap \mathcal{R}(y)$ n'est pas vide, il existe un élément $z \in \mathcal{R}(x) \cap \mathcal{R}(y)$. Cela signifie que $z\mathcal{R}x$ et que $z\mathcal{R}y$. Par transitivité (et en utilisant implicitement la symétrie pour écrire $x\mathcal{R}z$ au lieu de $z\mathcal{R}x$), on obtient $x\mathcal{R}y$. Le précédent point du théorème stipule l'équivalence entre cette assertion et $\mathcal{R}(x) = \mathcal{R}(y)$, ce qui permet de conclure.

■

Avez-vous en tête quelques exemples de relations d'équivalence ?

Exemple 2.14 *La relation d'égalité $x\mathcal{R}y$, définie par $x = y$, est une relation d'équivalence. Vous ne tarderez pas à être convaincus après avoir prouvé les quatre points suivants : c'est une relation binaire, réflexive, symétrique et transitive. Vous pourrez aussi prouver ces quatre points pour montrer que la relation $x\mathcal{R}y$, définie par $(x \geq 0$ et $y \geq 0)$ ou $(x < 0$ et $y < 0)$, est aussi une relation d'équivalence.*

L'une des propriétés les plus intéressantes des classes d'équivalences sur un ensemble E est qu'elles forment une partition de E, c'est-à-dire qu'à tout élément de E correspond une et unique classe d'équivalence. Avant d'énoncer cette propriété, définissons clairement ce qu'est une partition :

Définition 2.26 *Soit $\mathcal{E} \subset \mathcal{P}(E)$, c'est-à-dire un ensemble de parties de E.*
– *$\mathcal{E}$ est un* ***recouvrement*** *de E si $\forall x \in E, \exists X \in \mathcal{E}, x \in X$.*
– *$\mathcal{E}$ est une* ***partition*** *de E si les trois conditions suivantes sont réunies :*

1. *$\emptyset \notin \mathcal{E}$;*
2. *$\mathcal{E}$ est un recouvrement de E ;*
3. *les éléments de $\mathcal{E}$ sont deux à deux disjoints, ce qui signifie que*

$$\forall (F, G) \in \mathcal{E}^2, F \neq G \Rightarrow F \cap G = \emptyset.$$

La condition de recouvrement peut aussi s'écrire $E \subset \bigcup_{X \in \mathcal{E}} X$. Comme l'autre inclusion est évidente par définition de $\mathcal{E}$, car chaque élément de $\mathcal{E}$ est un sous-ensemble de E, on a alors $E = \bigcup_{X \in \mathcal{E}} X$. La compréhension intuitive d'un recouvrement est que tout élément de E est contenu dans un des ensembles constituant le recouvrement $\mathcal{E}$; il n'y a pas d'élément de E oublié par $\mathcal{E}$. Néanmoins, un élément de E peut appartenir à plusieurs éléments du recouvrement. Cela n'est plus possible pour une partition. En effet, un élément de E possède un et unique ensemble de $\mathcal{E}$ le contenant. On peut alors penser au découpage d'une feuille de papier. Les morceaux obtenus par ce découpage forment une partition de la feuille initiale : il ne peut pas y avoir un élément de la feuille appartenant à deux morceaux différents.

Pour un exemple de recouvrement qui ne soit pas une partition, on peut penser au découpage d'une ville en fonction de la proximité d'une station de métro. Ainsi, pour une ville comme Paris, si nous définissons des disques d'un kilomètre de rayon autour de chaque station de métro, nous obtenons un recouvrement de Paris, dans la mesure où chaque habitation de la ville sera dans l'un de ces disques. Mais certaines habitations seront dans le disque de deux ou trois stations de métro, voire plus. Ce recouvrement n'est donc pas une partition. Par ailleurs, si les disques ne font plus que 100 mètres de rayon, alors certaines habitations ne seront plus dans le disque d'influence d'une station de métro : l'ensemble des disques n'est pas un recouvrement et *a fortiori* pas une partition.

Après ces exemples intuitifs, voici quelques exemples plus abstraits :

Exemple 2.15 *Soit F un ensemble non vide et soit f une application $f : E \to F$. Définissons l'ensemble $\mathcal{E}$ par $\mathcal{E} = \{f^{-1}(\{y\}) | y \in Im(f)\}$: c'est l'ensemble des images réciproques par f des singletons contenus dans l'image de f, autrement dit chaque ensemble inclus dans $\mathcal{E}$ regroupe les éléments de E qui ont même image par f. Nous allons montrer que $\mathcal{E}$ est une partition de E.*

Reprenons la définition d'une partition. Tout d'abord, $\mathcal{E}$ est bien un ensemble de parties de E.

1. *Il faut d'abord montrer que l'ensemble vide n'est pas élément de $\mathcal{E}$. Cela se vérifie aisément par définition de $\mathcal{E}$. En effet, en raisonnant par l'absurde, si l'ensemble vide était élément de $\mathcal{E}$, on aurait l'existence d'un élément $y \in Im(f)$ tel que $f^{-1}(\{y\}) = \emptyset$. Or, comme $y \in Im(f)$, par définition de l'image directe, il existe $x \in E$ tel que $f(x) = y$. Donc $x \in f^{-1}(\{y\})$, ce qui est contradictoire avec l'hypothèse $f^{-1}(\{y\}) = \emptyset$: absurde !*
2. *Il faut ensuite vérifier que $\mathcal{E}$ est un recouvrement de E. Soit $x \in E$. Existe-t-il $X \in \mathcal{E}$ tel que $x \in X$? Oui, l'ensemble $X = f^{-1}(\{f(x)\})$ convient.*
3. *La dernière propriété à vérifier est la disjonction des éléments de $\mathcal{E}$. Faisons-le par contraposée. Soit $(F, G) \in \mathcal{E}^2$, vérifiant $F \cap G \neq \emptyset$. Montrons donc que $F = G$. Soit $(y_F, y_G) \in Im(f)^2$ tel que $F = f^{-1}(\{y_F\})$ et $G = f^{-1}(\{y_G\})$. Par hypothèse, $F \cap G \neq \emptyset$, donc il existe $x \in f^{-1}(\{y_F\}) \cap f^{-1}(\{y_G\})$. Autrement dit, $x \in f^{-1}(\{y_F\})$ et $x \in f^{-1}(\{y_G\})$, donc $f(x) = y_F$ et $f(x) = y_G$, donc, l'image d'un même élément par une application étant unique, $y_F = y_G$. Par conséquent, les ensembles F et G sont définis comme l'image réciproque par f d'un même point. Donc $F = G$, ce qui prouve la disjonction.*

Finalement, les trois propriétés sont vérifiées : $\mathcal{E}$ est bien une partition de E.

En réalité, cet exemple théorique correspond à quelque chose de très pratique et qui vous est familier s'il vous arrive de regarder une carte géographique : c'est en effet ainsi que l'on définit des courbes de niveau. Si f associe à un point de la carte une altitude, $f^{-1}(\{y\})$ est l'ensemble des points de la carte à l'altitude y.

En lisant cet exposé sur les partitions, vous aurez certainement pensé à un point commun avec les relations d'équivalence. En effet, les deux permettent de diviser un ensemble en sous-ensembles, sans redondances. En fin de compte, ces deux objets mathématiques sont très proches, au point que l'on peut énoncer la proposition suivante :

Proposition 2.8 *Soit $\mathcal{R}$ une relation d'équivalence sur E et $\mathcal{E}_{\mathcal{R}}$ l'ensemble de toutes les classes d'équivalence de $\mathcal{R}$. Alors $\mathcal{E}_{\mathcal{R}}$ est une partition de E.*

$\mathcal{E}_{\mathcal{R}}$ est ce que l'on appelle la partition de E associée à $\mathcal{R}$. Nous avons déjà montré comment prouver qu'un ensemble de parties de E était une partition, vous êtes donc probablement capable de prouver la proposition que nous venons d'énoncer. Vous devrez prouver chacune des propriétés définissant une partition. Pour aller plus vite, vous pouvez même faire référence directement au Théorème 2.14.

Preuve. $\mathcal{E}_{\mathcal{R}} = \{\mathcal{R}(x)|x \in E\}$ est bien un ensemble de parties de E, par définition de $\mathcal{R}$. Il nous reste trois propriétés à vérifier :

1. $\emptyset \notin \mathcal{E}_{\mathcal{R}}$, par réflexivité de la relation d'équivalence.
2. $\mathcal{E}_{\mathcal{R}}$ recouvre E, car, pour $x \in E$, il existe au moins un élément de $\mathcal{E}_{\mathcal{R}}$ contenant x, à savoir $\mathcal{R}(x)$.
3. Les éléments de $\mathcal{E}_{\mathcal{R}}$ sont disjoints deux à deux grâce au deuxième point du Théorème 2.14.

■

Naturellement, à partir d'une partition, on peut définir une relation d'équivalence, chaque classe d'équivalence étant définie comme l'appartenance à un même élément de la partition. Vous pouvez le vérifier en reprenant la définition de la relation d'équivalence.

2.4 Dénombrement et cardinalité

Nous avons vu ce qu'était un ensemble et vous avez appris à les manipuler, à créer des applications entre différents ensembles, à classer les éléments d'un même ensemble par des relations binaires. Pour compléter votre connaissance des ensembles, nous allons maintenant aborder le dénombrement, qui est l'art de déterminer le nombre d'éléments d'un ensemble. Ce nombre peut être fini (comme pour l'ensemble des entiers naturels inférieurs à 10) ou infini (comme pour l'ensemble des entiers naturels). Nous évoquerons surtout la première de ces deux catégories, les ensembles finis, avant d'ouvrir le chapitre sur les ensembles infinis, lesquels ne sont pas inscrits au programme de première année de prépa mais ont culturellement leur place dans ce chapitre.

2.4.1 Ensembles finis

Définition 2.27 *Un ensemble E est un* ***ensemble fini*** *si $\exists n \in \mathbb{N}$ tel que E et l'intervalle d'entiers $[\![1, n]\!]$ sont en bijection (deux ensembles en bijection sont dits* ***équipotents****). Alors, n est unique et est appelé le* **cardinal** *de E. Il est noté $Card(E)$.*

Cela va sans dire que ce que l'on désigne par l'expression « ensemble infini » est un ensemble qui n'est pas un ensemble fini, donc pour lequel il n'existe pas de bijection avec $[\![1, n]\!]$, quel que soit $n \in \mathbb{N}$.

Le cardinal d'un ensemble fini n'est rien d'autre que son nombre d'éléments. Par ailleurs, le recours à la bijection avec un intervalle d'entiers naturels s'explique intuitivement. En effet, cette bijection tient lieu d'indexation de tous les éléments de l'ensemble. Par exemple, si nous considérons un ensemble de personnes rassemblées dans une pièce et que nous voulons les compter, nous allons attribuer un numéro à chacune, en commençant par 1 et en incrémentant d'une unité à chaque nouvelle personne jusqu'à atteindre, pour la dernière personne, le nombre de personnes présentes, disons 12. Il y a ainsi une personne correspondant à chaque entier compris entre 1 et 12 (ne serait-ce donc pas une surjection ?) et à chacun de ces entiers ne correspond jamais plus d'une personne (et voilà une injection... et une application qui est à la fois injection et surjection est une bijection).

Notez que la Définition 2.27 affirme l'unicité du cardinal. Prenons la peine de justifier ce point. Supposons que le cardinal vaut à la fois n et p. Alors E est en bijection avec $[\![1,n]\!]$, par une application f_n, et avec $[\![1,p]\!]$, par une application f_p, ce que l'on pourrait écrire schématiquement

$$[\![1,n]\!] \xleftarrow{f_n} E \xrightarrow{f_p} [\![1,p]\!].$$

Ainsi, $[\![1,n]\!]$ et $[\![1,p]\!]$ seraient reliés par la bijection $f_n^{-1} \circ f_p : [\![1,n]\!] \to [\![1,p]\!]$. Cela signifie deux choses :
- $f_n^{-1} \circ f_p$ est injective, ce qui veut dire que deux éléments distincts de $[\![1,n]\!]$ n'ont pas la même image dans $[\![1,p]\!]$, ce qui n'est possible que si $p \geq n$;
- $f_n^{-1} \circ f_p$ est surjective, ce qui veut dire que tous les éléments de $[\![1,p]\!]$ ont un antécédent dans $[\![1,n]\!]$, ce qui n'est possible que si $p \leq n$.

Alors, $p = n$ et le cardinal est bien unique. Au passage, il est bon de relever que dans notre explication nous avons utilisé, sans le citer explicitement, le principe des tiroirs. La compréhension de ce principe est très simple mais permet de mettre un nom sur un raisonnement que l'on peine autrement à expliquer sans utiliser de longues périphrases. Le **principe des tiroirs** stipule que si vous voulez ranger n chemises dans p tiroirs, avec $n > p$, alors au moins deux chemises se trouveront dans le même tiroir. Mettons maintenant un peu les formes pour énoncer ce principe bien utile et très imagé :

Proposition 2.9 (Principe des tiroirs) *Soient E et F deux ensembles finis et f une application de E vers F, $f : E \to F$. On a alors l'implication*

$$Card(F) < Card(E) \Rightarrow (f \text{ n'est pas injective}),$$

ou, de manière équivalente, la contraposée

$$(f \text{ est injective}) \Rightarrow Card(F) \geq Card(E).$$

Quelques propriétés découlent de la Définition 2.27. Pour la première d'entre elles, on énonce simplement qu'un ensemble inclus dans un autre sera fini si le deuxième ensemble est fini ; il aura même moins ou autant d'éléments.

Proposition 2.10 *Soit E un ensemble fini et $F \subset E$. Alors, F est fini et $Card(F) \leq Card(E)$, avec égalité si et seulement si $F = E$.*

Preuve. Comme E est fini, il existe par définition une bijection $f : E \to [\![1, Card(E)]\!]$. Comme F est une partie de E, par la Proposition 2.5, $f_{|F} : F \to [\![1, Card(E)]\!]$ est injective. Alors, par la contraposée du principe des tiroirs,

$$Card(F) \leq Card([\![1, Card(E)]\!]) = Card(E).$$

Nous vous laissons étudier vous-même le cas d'égalité. ■

Dans la proposition suivante, on se rend compte que les applications sont un outil intéressant pour comparer le cardinal d'ensembles finis, ce qui n'est que justice dans la mesure où, dans la définition du cardinal, nous avons recours à la notion de bijectivité.

Proposition 2.11 *Soient E et F des ensembles finis et $f : E \to F$. Alors :*
- *si f est injective, alors $Card(E) \leq Card(F)$, avec égalité si et seulement si f est bijective ;*
- *si f est surjective, alors $Card(E) \geq Card(F)$, avec égalité si et seulement si f est bijective.*

Plus concrètement, s'il existe une injection de E vers F, alors E n'a pas plus d'éléments que F. Au contraire, s'il existe une surjection de E vers F, alors E n'a pas moins d'éléments que F. Une bijection indique qu'il y a autant d'éléments entre les deux ensembles, ce qui est cohérent avec la Définition 2.27.

Preuve.
- Supposons que f est injective. Soit $g : E \to f(E)$ la bijection induite par f. On sait que $f(E) \subset F$ et que F est fini, donc, d'après la Proposition 2.10, $f(E)$ est fini et $Card(f(E)) \leq Card(F)$, avec égalité si et seulement si $f(E) = F$, c'est-à-dire si et seulement si f est surjective (laquelle surjectivité est équivalente à la bijectivité de f dans la mesure où l'injectivité est en hypothèse). Nous avons donc presque prouvé l'énoncé et il ne reste plus qu'à établir le lien entre $Card(E)$ et $Card(f(E))$; or, $g : E \to f(E)$ est une bijection dans la mesure où f est une injection, donc $Card(E) = Card(f(E))$. En utilisant cette égalité conjointement avec l'inégalité $Card(f(E)) \leq Card(F)$, on aboutit bien au résultat et même à la condition d'égalité équivalente à la bijectivité de f.

– Supposons que f est surjective. Alors, il existe $g : F \to E$ injective tel que $f \circ g = Id_F$. L'application du point précédent à g permet de conclure.

■

Attention ! Ne succombez pas à la tentation de généraliser tous ces résultats à des ensembles quelconques, car ce qui est vrai pour des ensembles finis ne l'est pas nécessairement pour des ensembles infinis, comme on peut le constater dans l'exemple qui suit.

Exemple 2.16 *Soit* $f : [0,1] \to [0,2], x \mapsto 2x$. *$f$ est bijective, vous pouvez le vérifier vous-même. De plus,* $[0,1] \subset [0,2]$. *Vous pourriez dès lors être tenté de faire le raisonnement suivant, qui est absolument faux : « Par la Proposition 2.11, sans trop faire attention aux hypothèses, on affirme que* $[0,1]$ *et* $[0,2]$ *ont même cardinal car f est bijective ; or,* $[0,1] \subset [0,2]$, *donc, en utilisant la Proposition 2.10, on peut conclure que* $[0,1] = [0,2]$. *» Naturellement, ce résultat est faux ! La raison à cela est que l'on a utilisé les deux propositions mentionnées sans vérifier l'hypothèse selon laquelle les ensembles étudiés devaient être finis, ce qui n'était pas le cas des intervalles* $[0,1]$ *et* $[0,2]$. *De plus, dans notre cas précis, les énoncés des propositions n'avaient aucun sens : en effet, qu'est-ce que le cardinal d'un ensemble infini ? Rappelez-vous la définition que nous avons donnée d'un cardinal. Bon, n'insistons pas trop car, dans ce livre, nous voulons avant tout vous expliquer ce qu'il faut faire plutôt que vous raconter dans le détail pourquoi tel ou tel raisonnement n'a ni queue ni tête, d'autant qu'il y a mille manières de se tromper et que nous n'avons pas l'ambition de les aborder toutes. Retenez néanmoins que la vérification des hypothèses, donc leur connaissance, est primordiale.*

Dans les parties précédentes, après avoir présenté un concept lié à un ensemble, comme l'image directe d'un ensemble par une application, nous avons voulu étendre l'étude à des opérations sur les ensembles, ce qui, par exemple, nous a fait aborder l'image directe de l'union ou de l'intersection de deux ensembles. Vous allez finir par être familier avec ce procédé cartésien consistant à partir d'un problème simple vers des formes plus complexes de celui-ci... Nous vous proposons donc maintenant d'évoquer le cardinal d'un ensemble défini par une opération sur plusieurs ensembles. Commençons donc par le cardinal de l'union de deux éléments finis disjoints. Par exemple, le cardinal de l'ensemble des étudiants (c'est-à-dire le nombre d'étudiants) candidats au baccalauréat en 2014 est égal à la somme du cardinal de l'ensemble des étudiants obtenant le baccalauréat en 2014 et du cardinal de l'ensemble des étudiants échouant au baccalauréat la même année, car ces deux ensembles sont disjoints (ce qui signifie qu'aucun étudiant n'appartient simultanément aux deux ensembles mentionnés). Ceci illustre le théorème suivant :

Théorème 2.15 *Soient A et B des ensembles finis disjoints (la disjonction de A et B signifie que $A \cap B = \emptyset$). Alors, $Card(A \cup B) = Card(A) + Card(B)$.*

La démonstration de ce théorème est intéressante : nous vous conseillons de vous y frotter un peu seul avant de la lire. Si vous avez du mal à conduire votre raisonnement, voici un conseil permettant de comprendre l'intuition du théorème : notez que, si l'on a le cardinal d'un ensemble fini, A par exemple, on a une bijection entre cet ensemble et $[\![1, Card(A)]\!]$. On est donc capable de compter, de 1 à $Card(A)$, pour indexer chaque élément de A. Nous pouvons faire la même chose pour B. Mais si nous voulons compter les éléments de A puis ajouter ceux de B, nous allons développer une manière particulière de compter, en comptant normalement les éléments de A puis en commençant à $1+Card(A)$ pour le premier élément de B et en continuant par des incréments de 1. Si, si, faites-le, utilisez vos doigts et comptez : il n'y a rien de plus simple ! Reste alors à prouver que cette manière de compter a les propriétés requises, à savoir que nous avons formé une application et que celle-ci est bijective.

Preuve. A et B étant finis, il existe deux bijections $f_A : A \to [\![1, Card(A)]\!]$ et $f_B : B \to [\![1, Card(B)]\!]$. Définissons une application f sur l'ensemble $A \cup B$ par

$$f : x \in A \cup B \mapsto \begin{cases} f_A(x) & \text{si } x \in A \\ f_B(x) + Card(A) & \text{si } x \in B. \end{cases}$$

f est bien une application car, à tout élément de $A \cup B$, correspond une unique image par f, grâce à la disjonction entre A et B[1]. L'ensemble de départ de f est $A \cup B$ et son ensemble d'arrivée $[\![1, Card(A) + Card(B)]\!]$. Pour prouver que cette application est bijective, vous pouvez montrer qu'elle admet une application réciproque[2] en la construisant proprement ou bien vous pouvez montrer qu'elle est injective et surjective en revenant aux définitions d'injectivité et de surjectivité et en utilisant le fait que f_A et f_B sont bijectives. Cela vous fournit assez d'éléments pour terminer vous-même cette démonstration, non ?
■

Le corollaire qui suit découle du Théorème 2.15 : dans le théorème, nous nous intéressions à l'union de deux ensembles disjoints ; nous abordons maintenant le cas de l'union d'un nombre fini d'ensembles disjoints. En particulier, ce corollaire permet d'aboutir à l'assertion suivante : l'union d'un nombre fini d'ensembles finis est nécessairement finie. La seule difficulté pour passer du corollaire à cette assertion réside dans la disjonction des ensembles dans le corollaire. Vous pouvez contourner cet écueil en découpant chaque ensemble

1. S'il existait $y \in A \cap B$, alors il y aurait une ambiguïté pour définir $f(y)$, qui pourrait valoir $f_A(y)$ ou $f_B(y) + Card(A)$.
2. C'est-à-dire une application g telle que $f \circ g = Id_{[\![1, Card(A)+Card(B)]\!]}$ et $g \circ f = Id_{A \cup B}$.

en un sous-ensemble d'éléments n'appartenant à aucun des autres ensembles et plusieurs autres sous-ensembles définis par les intersections avec les autres ensembles. Cette manière de faire correspond en fait à la formule du crible, que vous découvrirez dans l'Exercice 2.9.

Corollaire 2.1 *Soit $n \in \mathbb{N}^\star$ et $(A_i)_{1\leq i\leq n}$ une famille d'ensembles finis deux à deux disjoints. Alors,*

$$Card\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} Card(A_i).$$

Si vous avez bien lu le livre jusqu'à ce point, la démonstration doit jaillir dans votre esprit ! En effet, nous avons prouvé un théorème qui s'applique à deux ensembles [1] et nous voulons maintenant l'étendre à un nombre fini d'ensembles. Donc, le théorème est un cas particulier. L'étendre à trois ensembles n'est pas bien compliqué, et ainsi de suite jusqu'à atteindre n'importe quel nombre fini n d'ensembles. Cela suggère un raisonnement par récurrence.

Preuve.

- Le corollaire est vrai pour $n = 1$: $Card(A_1) = Card(A_1)$. Le Théorème 2.15 nous dit même explicitement qu'il est vrai pour $n = 2$.
- Supposons le corollaire vrai pour un certain $n \in \mathbb{N}^\star$. Montrons qu'il est également vrai pour $n+1$. Soit $(A_i)_{1\leq i\leq n+1}$ une famille d'ensembles finis deux à deux disjoints. Notons $B = \bigcup_{i=1}^{n} A_i$. D'une part, $(A_i)_{1\leq i\leq n}$ est une famille d'ensembles finis deux à deux disjoints, donc, par l'hypothèse de récurrence, $Card(B) = \sum_{i=1}^{n} Card(A_i)$. D'autre part, B et A_{n+1} sont disjoints, donc, en utilisant le Théorème 2.15, $Card(A_{n+1} \cup B) = Card(A_{n+1}) + Card(B)$. Ainsi, $Card\left(\bigcup_{i=1}^{n+1} A_i\right) = \sum_{i=1}^{n+1} Card(A_i)$.
- Le corollaire a été prouvé pour $n = 1$ et on a démontré la propriété de récurrence, donc on a prouvé le corollaire pour tout $n \in \mathbb{N}^\star$.

$\blacksquare$

Notez que l'hypothèse de disjonction des ensembles dans le Théorème 2.15 et son corollaire est primordiale, comme vous l'avez peut-être remarqué dans la preuve que nous avons donnée pour le Théorème 2.15. Reprenons l'exemple des ensembles d'étudiants candidats au baccalauréat. Notons M l'ensemble des étudiants ayant obtenu une note inférieure à 10 en mathématiques au baccalauréat et B l'ensemble des étudiants ayant obtenu le baccalauréat cette même année. Alors, $Card(M \cup B) \neq Card(M) + Card(B)$. En effet, certains étudiants ont eu moins de 10 en mathématiques tout en obtenant le baccalauréat : il sont donc comptés une fois dans $Card(M \cup B)$ mais deux fois dans

1. Il s'agit du Théorème 2.15.

$Card(M)+Card(B)$. La proposition suivante permet de travailler avec des ensembles qui ne sont pas nécessairement disjoints, en ôtant le double comptage des éléments dans l'intersection des deux ensembles.

Proposition 2.12 *Soient A et B des ensembles finis. Alors, $Card(A \cup B) = Card(A) + Card(B) - Card(A \cap B)$.*

Preuve. Il s'agit d'utiliser les résultats que nous connaissons déjà, afin de gagner un peu de temps et de ne pas démontrer plus laborieusement cette proposition. En l'occurrence, le Théorème 2.15 et son corollaire semblent être nos armes les plus prometteuses, mais, pour les utiliser, il faut se rapporter à des ensembles disjoints. Pour ce faire, il suffit de considérer, d'une part, l'intersection de A et B et, d'autre part, A amputé de son intersection avec B et symétriquement. En effet, $A \cap B$, $A \backslash B$ et $B \backslash A$ sont des ensembles disjoints. En utilisant le corollaire du Théorème 2.15, on peut écrire :

$$\begin{aligned} Card(A \cup B) &= Card([A \cap B] \cup [A \backslash B] \cup [B \backslash A]) \\ &= Card(A \cap B) + Card(A \backslash B) + Card(B \backslash A). \end{aligned}$$

$Card(A \cap B)$ apparaît dans la formule que nous voulons montrer, donc nous sommes rassurés ; en revanche, $Card(A \backslash B)$ et son symétrique n'y apparaissent pas. Qu'à cela ne tienne ! Réfléchissez un instant à la manière dont nous pouvons approcher $A \backslash B$ d'ensembles que nous connaissons, à savoir A, B et leur intersection ou leur union. La bonne piste est d'écrire A comme l'union des deux ensembles disjoints que sont $A \backslash B$ et $A \cap B$. Alors, par le Théorème 2.15, $Card(A) = Card(A \backslash B) + Card(A \cap B)$, formule que vous pouvez renverser pour obtenir $Card(A \backslash B) = Card(A) - Card(A \cap B)$. Symétriquement, $Card(B \backslash A) = Card(B) - Card(A \cap B)$. Reprenons alors la formule du cardinal de $A \cup B$ là où nous l'avions laissée :

$$\begin{aligned} Card(A \cup B) &= Card(A \cap B) + Card(A \backslash B) + Card(B \backslash A) \\ &= Card(A \cap B) + Card(A) - Card(A \cap B) \\ &\quad + Card(B) - Card(A \cap B), \end{aligned}$$

ce qui fournit le résultat escompté après rassemblement des $Card(A \cap B)$.
■

Vous pouvez également retourner la formule de la Proposition 2.12 pour obtenir le cardinal d'une intersection de deux ensembles finis : $Card(A \cap B) = Card(A) + Card(B) - Card(A \cup B)$. Mais un résultat plus intéressant obtenu à partir de cette proposition consiste en son extension à un nombre fini quelconque d'ensembles. C'est ce que l'on appelle la formule du crible, que nous vous présentons à l'exercice 2.9.

2.4.2 Ensembles infinis

Nous venons d'étudier la cardinalité d'ensembles finis. Or, ces ensembles finis ne constituent qu'une vision partielle de tous les ensembles : nous ne vous apprendrons rien en vous annonçant qu'il existe des ensembles infinis, c'est-à-dire composés d'un nombre infini d'éléments. Cependant, quelques surprises se cachent derrière cette notion d'infini. Vous avez probablement grandi dans la certitude que l'infini était une sorte de concept monolithique : « L'infini est plus grand que n'importe quel nombre fini, mais l'infini c'est l'infini, il n'y a qu'un seul infini, il n'y a pas d'infini plus grand qu'un autre infini, raison pour laquelle on utilise d'ailleurs un seul symbole : ∞. » Certes, tel était aussi le point de vue des mathématiciens à la fin du XIXe siècle lorsque Cantor et d'autres ont commencé à faire des distinctions entre diverses sortes d'infinis, précisément grâce à la théorie des ensembles. En effet, pour tout ensemble infini, Cantor a montré qu'il existait un autre ensemble infini strictement plus *grand*[1] que l'ensemble initial : cet ensemble est l'ensemble de ses parties. Mais comment classer ces infinis entre eux ? Dans le monde infini, par analogie avec le principe des tiroirs, dire que l'ensemble F est plus grand que l'ensemble E signifie qu'il n'y a pas de surjection de E dans F. On pourrait aussi dire que cela signifie qu'il n'y a pas d'injection de F dans E.

Théorème 2.16 (Théorème de Cantor) *Soit E un ensemble quelconque, c'est-à-dire fini ou infini. Alors, la cardinalité de $\mathcal{P}(E)$ est strictement plus grande que celle de E, ce qui signifie qu'il n'existe pas de surjection de E dans $\mathcal{P}(E)$.*

Tiens, tiens, ce théorème ne vous évoque-t-il rien ? Nous en avons en fait déjà parlé lorsque vous avez lu, au début du chapitre, une proposition permettant de prouver le théorème de Cantor restreint au cas particulier des ensembles finis : c'était la Proposition 2.1. Relisez-la et voyez que cela permet bien de prouver le théorème de Cantor dans le cas fini. Il n'est d'ailleurs pas innocent de notre part de faire référence au début du chapitre que nous sommes en train de clore : d'une part, la lecture de ces quelques pages vous a beaucoup appris et vous a enseigné des notions que vous êtes capable d'appliquer pour élargir certains résultats ; d'autre part, une petite révision vous permet de vérifier que tout est bien intégré dans votre esprit ; enfin, cela vous permet d'apprécier le lien qui unit tous les concepts engrangés – ensembles, applications, relations binaires, cardinal... Nous allons même pousser plus loin la réutilisation de notions déjà présentées en tout début de chapitre puisque la démonstration du Théorème 2.16 s'appuie sur la même idée que le paradoxe de

1. Le sens de cet adjectif est précisé dans le Théorème 2.16.

Russell. Ne vous rappelez-vous pas ce paradoxe ? C'était l'histoire du barbier qui devait raser tous les hommes ne se rasant pas eux-mêmes et uniquement ceux-ci : il se trouvait embêté quant au sort à réserver à sa propre barbe. Plus mathématiquement parlant, le paradoxe de Russell énonce que l'ensemble constitué des ensembles n'appartenant pas à eux-mêmes n'existe pas. C'était l'objet de l'exemple 2.2. Maintenant que votre mémoire a été rafraîchie, nous pouvons nous lancer dans la preuve du théorème de Cantor.

Preuve. Soit une application $f : E \to \mathcal{P}(E)$. Il faut montrer que f n'est pas surjective. En l'occurrence, nous allons raisonner par l'absurde, donc nous supposons que f est surjective, c'est-à-dire que, pour tout ensemble $Y \in \mathcal{P}(E)$, il existe un élément $x \in E$ tel que $Y = f(x)$; cette hypothèse doit aboutir à une contradiction. Définissons alors l'ensemble $R \in \mathcal{P}(E)$ par

$$R = \{x \in E | x \notin f(x)\},$$

que vous pourrez appeler ensemble de Russell car il mène à un raisonnement identique à celui développé dans le paradoxe de Russell. Nous avons supposé, pour initier ce raisonnement par l'absurde, qu'il existait $e \in E$ tel que $R = f(e)$. Ceci mène à une contradiction dans le mesure où :
- si $e \in f(e)$, alors, comme $f(e) = R$ et par définition de R, $e \notin f(e)$;
- si $e \notin f(e)$, alors, comme $f(e) = R$ et par définition de R, $e \in f(e)$;

ce qui revient à écrire l'absurdité $e \in f(e) \Leftrightarrow e \notin f(e)$. Le théorème est ainsi démontré, par l'absurde. ■

Comment faut-il comprendre le recours à l'ensemble de Russel dans cette démonstration ? Simplement, à tous les éléments x de E correspond un ensemble singleton $\{x\}$ élément de $\mathcal{P}(E)$; mais il reste alors tous les autres éléments de $\mathcal{P}(E)$, dont l'ensemble de Russel peut être un exemple. Si cette explication ne vous a pas aidé, si vous avez du mal à voir à quoi ressemble R ou encore si vous doutez que R existe ou appartient à $\mathcal{P}(E)$, quelques exemples peuvent être utiles.

Exemple 2.17 *Prenons quelques exemples pour l'application f de la preuve du théorème de Cantor :*
- *Si f est l'application « identité » $x \mapsto \{x\}$ (ce n'est pas exactement ce que nous avons défini comme une application identité puisque l'ensemble de départ et l'ensemble d'arrivée diffèrent, mais vous devez voir l'analogie, non ?), alors l'ensemble de Russell est l'ensemble vide, lequel est bien élément de $\mathcal{P}(E)$. Ainsi, et cela éclaire peut-être l'explication du paragraphe précédent, en plus de tous les singletons, $\mathcal{P}(E)$ contient l'ensemble vide. Si E est réduit à un seul élément, l'ensemble vide est d'ailleurs le seul autre élément de $\mathcal{P}(E)$ et alors $Card(E) = 1$ et $Card(\mathcal{P}(E)) = 2$.*

- *Si f est une application constante $x \mapsto F$ où $F \subset E$, alors l'ensemble de Russell est le complémentaire de F dans E. En particulier, si $F = E$, alors $R = \emptyset$ et, si $F = \emptyset$, alors $R = E$. Dans tous ces cas, R est bien élément de $\mathcal{P}(E)$.*

Le rapprochement avec le paradoxe de Russell ne doit pas vous faire peur. Ce paradoxe présente un ensemble qui en fin de compte n'existe pas, mais cet ensemble n'est pas ce que nous avons appelé ensemble de Russell. En l'occurrence, il va de soi que R est un élément de $\mathcal{P}(E)$, puisque, par définition, c'est un ensemble constitué d'éléments de E ou bien c'est l'ensemble vide si la condition $x \notin f(x)$ n'est vérifiée pour aucun $x \in E$.

Voyez-vous la conséquence fabuleuse de ce Théorème 2.16 ? Il y a une infinité d'infinis ! Si E est un ensemble infini, alors $\mathcal{P}(E)$ est aussi infini mais strictement plus *grand* (dans le sens du Théorème 2.16) que E. $\mathcal{P}(E)$ est donc l'ensemble infini ayant le plus d'éléments, nous direz-vous ? Que nenni, $\mathcal{P}(\mathcal{P}(E))$ contient davantage d'éléments ! Et ainsi de suite... Dès lors, il n'existe pas de plus grand cardinal et personne ne pourra vous présenter l'ensemble le plus grand imaginable puisqu'en prenant simplement l'ensemble de ses parties vous trouverez un ensemble encore plus grand. De même, l'ensemble contenant tous les ensembles ne peut pas exister.

Mais s'il n'existe pas de plus grand cardinal infini, peut-être peut-on avoir une idée de ce qu'est le plus petit infini ? On peut en effet approcher cette notion grâce aux ensembles dénombrables.

Définition 2.28 *Soit E un ensemble. E est dit* **dénombrable** *s'il est équipotent à $\mathbb{N}$, c'est-à-dire s'il existe une bijection entre E et $\mathbb{N}$.*

Le théorème suivant permet de confirmer que la dénombrabilité correspond à la plus petite notion d'infini puisqu'aucun autre infini ne vient s'intercaler entre ce qui est fini et ce qui est dénombrable.

Théorème 2.17 *Toute partie de $\mathbb{N}$ est finie ou dénombrable.*

Preuve. Soit F une partie infinie de $\mathbb{N}$. Il nous faut montrer que F est dénombrable et donc construire une bijection avec $\mathbb{N}$. Pour ce faire, rangeons les éléments de F par ordre croissant : $x_0 = \min(F)$, $x_1 = \min(F \backslash \{x_0\})$, $x_2 = \min(F \backslash \{x_0, x_1\})$, etc. Alors, l'application $\phi : \mathbb{N} \to F, n \mapsto x_n$ est strictement croissante, donc injective. ϕ est aussi surjective puisqu'elle parcourt entièrement F : en effet, pour $n \in F$, on a nécessairement $n \in \{x_0, \ldots, x_n\}$, car sinon il y aurait $n+1$ entiers naturels $(x_0, \ldots, x_n)$ strictement inférieurs à n, ce qui est impossible. Donc, l'application ϕ étant à la fois injective et surjective, elle est bijective. ■

On peut étendre ce résultat en remplaçant $\mathbb{N}$ par n'importe quel ensemble dénombrable. Cela revient à utiliser l'équipotence. En effet, si E est dénombrable, il existe une bijection f de E dans $\mathbb{N}$. Alors, toute partie $F \subset E$ est équipotente à $f(F) \subset \mathbb{N}$. Or, par le Théorème 2.17, $f(F)$ est finie ou dénombrable, donc F également.

Corollaire 2.2 *Toute partie d'un ensemble dénombrable est finie ou dénombrable.*

Arrivé à ce point, vous connaissez des ensembles finis, des ensembles infinis les plus petits possibles, c'est-à-dire des ensembles dénombrables, et vous savez comment augmenter la cardinalité d'un ensemble grâce au théorème de Cantor. Mais peut-être voulez-vous, pour finir le cours sur la théorie des ensembles, un exemple d'ensemble infini non dénombrable ? Très bien, prenons l'exemple des nombres réels, $\mathbb{R}$. Un argument astucieux, développé par Cantor, encore lui, permet de démontrer que $\mathbb{R}$ est indénombrable. C'est ce que nous présentons dans cette dernière proposition.

Proposition 2.13 *L'ensemble $\mathbb{R}$ des nombres réels est indénombrable.*

Preuve. Pour démontrer cette proposition, il faut vérifier qu'il n'existe pas de surjection de $\mathbb{N}$ dans $\mathbb{R}$, donc il suffit de constater qu'il n'existe pas de surjection de $\mathbb{N}$ dans $[0,1[$. Pour le prouver, nous allons utiliser ce que l'on appelle l'argument diagonal de Cantor. Soit $f : \mathbb{N} \to [0,1[$. Écrivons chaque réel $f(n)$, pour $n \in \mathbb{N}$, en écriture décimale :

$$\begin{array}{ccccccccc}
f(0) & = & 0, & r_{00} & r_{01} & r_{02} & \dots & r_{0n} & \dots \\
f(1) & = & 0, & r_{10} & r_{11} & r_{12} & \dots & r_{1n} & \dots \\
f(2) & = & 0, & r_{20} & r_{21} & r_{22} & \dots & r_{2n} & \dots \\
\vdots & & & & & & & & \\
f(n) & = & 0, & r_{n0} & r_{n1} & r_{n2} & \dots & r_{nn} & \dots \\
\vdots & & & & & & & &
\end{array}$$

On définit alors un autre réel $x = 0, x_0x_1x_2...x_n...$, où, $\forall i \in \mathbb{N}$, $x_i = 1$ si $r_{ii} = 0$ et $x_i = 0$ sinon. Cela permet d'avoir $\forall i \in \mathbb{N}$, $x_i \neq r_{ii}$ et donc $x \neq f(i)$ car x diffère de $f(i)$ par au moins un chiffre dans son écriture décimale (celui en position i : x_i et r_{ii}). Ainsi f n'est-elle pas surjective, ce qui suffit à prouver que $\mathbb{R}$ est indénombrable. ■

2.5 Exercices

2.5.1 Ensembles

Exercice 2.1 *Soient A, B et C des ensembles inclus dans un autre ensemble, nommé E. Montrer les points suivants :*
(1) $(A\backslash B) \cup (A \cap B) = A$;
(2) $(A\backslash B) \cup B = A \cup B$;
(3) $E\backslash(A\backslash B) = (E\backslash A) \cup B$;
(4) $A \cap (B\backslash C) = (A \cap B)\backslash C$. *L'égalité reste-t-elle vraie si l'on remplace les signes $\cap$ par des signes $\cup$?*

Exercice 2.2 *Soient A et B des ensembles inclus dans un autre ensemble, nommé E. Définissons l'opération $\star$ par $A \star B = \overline{A \cap B}$. Montrer que l'on peut écrire $\overline{A}$, $A \cap B$ et $A \cup B$ en utilisant uniquement l'opération $\star$.*

2.5.2 Applications

Exercice 2.3 *Les applications suivantes sont-elles injectives, surjectives, bijectives ?*
(1) $f : \mathbb{N} \to \mathbb{N}, x \mapsto x + 1$
(2) $g : \mathbb{Z} \to \mathbb{Z}, x \mapsto x + 1$

Exercice 2.4 *Soient E, F, G, H quatre ensembles et $f : E \to F$, $g : F \to G$, $h : G \to H$ trois applications telles que $g \circ f$ et $h \circ g$ sont bijectives. Montrer que f, g et h sont bijectives.*

Exercice 2.5 *Soient E un ensemble et $f : E \to E$ une application telle que $f \circ f = f$. Montrer que si f est injective ou surjective alors $f = Id_E$.*

Exercice 2.6 *Soient E et F deux ensembles et $f : E \to F$ une application. Montrer que, pour tous $A \subset E$ et $B \subset F$, $f(A \cap f^{-1}(B)) = f(A) \cap B$.*

2.5.3 Relations binaires

Exercice 2.7 *Montrer que la relation de divisibilité des entiers est une relation d'ordre partiel sur $\mathbb{N}$. Que dire si l'on définit cette relation sur $\mathbb{Z}$?*

Exercice 2.8 *Soit $\mathcal{R}$ la relation binaire sur $\mathbb{Z} \times \mathbb{N}^*$ définie par*

$$(m, n)\mathcal{R}(p, q) \Leftrightarrow mq = np,$$

pour tous (m,n) et (p,q) dans $\mathbb{Z}\times\mathbb{N}^*$. Montrer que $\mathcal{R}$ est une relation d'équivalence.

2.5.4 Dénombrement et cardinalité

Exercice 2.9 (Formule du crible) *Soit $n \in \mathbb{N}^\star$ et $(A_i)_{1\leq i\leq n}$ une famille d'ensembles finis. Montrer la formule du crible, qui est l'équation suivante :*

$$Card\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{k=1}^{n}\left((-1)^{k+1}\sum_{1\leq i_1<\ldots<i_k\leq n} Card\left(\bigcap_{p=1}^{k} A_{i_p}\right)\right).$$

Exercice 2.10 (Dénombrabilité) *Pour montrer la dénombrabilité d'un ensemble, il faut montrer qu'il est en bijection avec $\mathbb{N}$.*
(1) Trouver une bijection de $\mathbb{N}$ dans $\mathbb{Z}$.
(2) Trouver une bijection de $\mathbb{N}\times\mathbb{N}$ dans $\mathbb{N}$.

2.5.5 Problèmes corrigés

Problème 2.1 (Intégrande de l'application Gamma) *On appelle application Gamma l'application $\Gamma : \mathbb{R}^+\backslash\{0\} \to \mathbb{R}^+\backslash\{0\}, x \mapsto \int_0^{+\infty} t^{x-1}e^{-t}dt$. L'étude des intégrales n'est pas abordée dans ce livre et nous ne la ferons pas non plus dans ce problème. Vous rencontrerez en revanche cette application Gamma au cours de vos études et vous pouvez dès à présent noter que, pour tout $n\in\mathbb{N}$, on a $\Gamma(n+1) = n!$ et, pour tout réel $x > 0$, $\Gamma(x+1) = x\Gamma(x)$, ce qui fait de cette application Gamma une sorte de prolongement de la factorielle aux réels positifs. Voilà pour votre culture mathématique. Dans le problème qui suit, nous nous intéresserons uniquement à l'intégrande de cette application, à savoir :*

$$f : \mathbb{R}^+\backslash\{0\} \to \mathbb{R}^+\backslash\{0\}, t \mapsto t^{\alpha-1}e^{-t},$$

pour $\alpha \in \mathbb{R}$.
(1) Caractériser les intervalles I pour lesquels la restriction de f à I est injective.
(2) Pour quelles valeurs du paramètre α f est-elle bijective ?
(3) Même question concernant la bijectivité pour l'application $g : \mathbb{R}^+\backslash\{0\} \to \mathbb{R}^+\backslash\{0\}, t \mapsto t^{(\alpha-1)^2}\exp\left[-(\alpha-1)t - t^{\alpha-1}e^{-t}\right]$.
Soit $\alpha\in\mathbb{R}$. Soit $\mathcal{R}$ la relation définie pour $(x,y)\in(\mathbb{R}^+\backslash\{0\})^2$ par $x\mathcal{R}y$ si et seulement si $(x/y)^{\alpha-1} = e^{x-y}$.
(4) Montrer que $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{R}^+\backslash\{0\}$.
(5) Pour $x\in\mathbb{R}^+\backslash\{0\}$, quel est le nombre de représentants de la classe de x ?

2.6 Solution des exercices

Solution 2.1 (de l'exercice 2.1) *(1) Par définition,*

$$\begin{aligned}(A\backslash B)\cup(A\cap B) &= (A\cap(E\backslash B))\cup(A\cap B)\\ &= A\cap((E\backslash B)\cup B)\\ &= A\cap E\\ &= A,\end{aligned}$$

en utilisant la propriété de distributivité, en factorisant, pour le passage à la deuxième ligne.

(2) On a

$$\begin{aligned}(A\backslash B)\cup B &= (A\cap(E\backslash B))\cup B\\ &= (A\cup B)\cap((E\backslash B)\cup B)\\ &= (A\cup B)\cap E\\ &= A\cup B,\end{aligned}$$

en utilisant la propriété de distributivité pour le passage à la deuxième ligne.

(3) On a

$$\begin{aligned}E\backslash(A\backslash B) &= E\backslash(A\cap(E\backslash B))\\ &= (E\backslash A)\cup E\backslash E\backslash B\\ &= (E\backslash A)\cup B,\end{aligned}$$

où l'on a utilisé le Théorème 2.5

(4) $A\cap(B\backslash C) = A\cap(B\cap(E\backslash C)) = (A\cap B)\backslash C$*, par associativité. Le résultat est naturellement faux si l'on remplace* $\cap$ *par* $\cup$*. Pour le prouver, un contre-exemple suffit. Prenons trois ensembles réduits à un seul élément, avec* A *et* C *confondus : soient* $a, b \in E$ *tels que* $A = C = \{a\}$ *et* $B = \{b\}$*. Alors,* $A\cup(B\backslash C) = \{a, b\}$ *et* $(A\cup B)\backslash C = \{b\}$*, ce qui forme deux ensembles différents. Si vous ne comprenez pas pourquoi nous avons choisi ce contre-exemple et quelle intuition se cache sous ce raisonnement, voici une petite explication : l'union permet de créer un ensemble plus grand à partir de deux ensembles, alors que l'intersection et la différence en créent un plus petit (la différence n'est rien d'autre qu'une intersection) ; ainsi, lorsque l'on écrit* $A\cup(B\backslash C)$*, on réduit d'abord la taille de* B *puis on l'augmente en ajoutant* A*, lequel contient éventuellement des éléments déjà enlevés à* B *ou, du moins, exclus par la différence avec* C *(autrement dit : des éléments de* C*, enlevés par différence avec* B*, sont ensuite ajoutés s'ils sont dans* A*) ; au contraire, en écrivant* $(A\cup B)\backslash C$*, c'est au grand ensemble, consistant en l'union de* A *et de* B*, que l'on enlève* C *(il ne reste donc plus aucun élément de* C *dans l'ensemble ainsi constitué).*

Solution 2.2 (de l'exercice 2.2) *On remarque déjà que* $A \star A = \overline{A \cap A} = \overline{A}$. *Ensuite,* $\overline{A \star B} = A \cap B$. *Or, on vient de voir comment écrire le complémentaire en utilisant l'opération* $\star$, *donc* $A \cap B = (A \star B) \star (A \star B)$. *Pour finir, on peut écrire, par le Théorème 2.5,* $A \star B = \overline{A} \cup \overline{B}$, *donc, par ce qui précède à propos du complémentaire,* $A \cup B = (A \star A) \star (B \star B)$.

Solution 2.3 (de l'exercice 2.3) *(1)* $0 \in \mathbb{N}$ *n'a pas d'antécédent par* f, *donc* f *n'est pas surjective et a fortiori pas bijective. En revanche, elle est injective trivialement, car, pour* $x, y \in \mathbb{N}$, *si* $x + 1 = y + 1$, *alors* $x = y$.

(2) Pour la même raison que f, g *est injective. Elle est aussi surjective, car, pour tout* $y \in \mathbb{Z}$, $y - 1 \in \mathbb{Z}$ *est un antécédent de* y *par* g. *Comme* g *est injective et surjective, elle est aussi bijective.*

Solution 2.4 (de l'exercice 2.4) *Raisonnons en trois temps. Nous allons d'abord montrer que* g *est surjective puis injective, ce qui permettra aisément de prouver que* f *et* h *sont aussi bijectives.*

- $g \circ f$ *étant bijective, elle est en particulier surjective. Mais alors,* g *aussi est surjective. En effet, pour tout* $z \in G$, *par hypothèse il existe* $x \in E$ *tel que* $z = g \circ f(x)$, *donc il existe* $y \in F$ *(en l'occurrence,* $y = f(x)$ *fonctionne) tel que* $z = g(y)$.
- $h \circ g$ *étant bijective, elle est en particulier injective. Mais alors,* g *aussi est injective. En effet, pour tout* $x, y \in F$, *tel que* $g(x) = g(y)$, $h \circ g(x) = h \circ g(y)$, *donc* $x = y$ *par hypothèse d'injectivité de* $h \circ g$.
- g *étant injective et surjective, elle est bijective. Alors, son application réciproque existe et est bijective (Proposition 2.4) et on peut écrire* $f = g^{-1} \circ (g \circ f)$ *et* $h = (h \circ g) \circ g^{-1}$, *qui, en tant que composées d'applications bijectives, sont bijectives d'après le Théorème 2.10.*

Solution 2.5 (de l'exercice 2.5) f *et* Id_E *ont même ensemble de départ et d'arrivée. Il suffit donc (après avoir préalablement souligné ce point primordial) de vérifier qu'elles ont même graphe.*

- *Si* f *est injective, alors* $\forall x, y \in E$ *tel que* $f(x) = f(y)$, *on a* $x = y$. *En particulier, pour tout* $x \in E$, *on a* $f(x) = f(f(x))$ *par hypothèse, donc, en prenant* $y = f(x) \in E$ *dans la définition de l'injectivité, on a* $x = f(x)$, *donc* $f = Id_E$.
- *Si* f *est surjective, alors, pour tout* $y \in E$, *il existe* $x \in E$ *tel que* $f(x) = y$. *En composant de part et d'autre de l'équation par* f, *on obtient* $f(f(x)) = f(y)$, *donc, par l'hypothèse* $f \circ f = f$, *cela devient* $x = f(y)$. *Ainsi, en remplaçant* x *par* $f(y)$ *dans l'équation* $f(x) = y$, *on obtient* $f(f(y)) = y$, *ce qui, par hypothèse, équivaut à* $f(y) = y$. *Donc* $f = Id_E$.

Solution 2.6 (de l'exercice 2.6) *Soient* $A \subset E$ *et* $B \subset F$. *Comme à l'accoutumée, nous allons montrer la double inclusion.*

D'abord, $f(A \cap f^{-1}(B)) \subset f(A) \cap B$ est assez simple. En effet, si y appartient à l'ensemble $f(A \cap f^{-1}(B))$, alors il existe $x \in A \cap f^{-1}(B)$ tel que $y = f(x)$. Comme $x \in f^{-1}(B)$, il s'ensuit que $y \in B$. Par ailleurs, comme $x \in A$, $y = f(x) \in f(A)$. Donc $y \in f(A) \cap B$.

Maintenant, si $y \in f(A) \cap B$, alors $y \in f(A)$ et il existe donc $x \in A$ tel que $y = f(x)$. Mais, comme $y \in B$, il en découle que $x \in f^{-1}(B)$. Finalement, $x \in A \cap f^{-1}(B)$ et donc $y \in f(A \cap f^{-1}(B))$, ce qui conclut la preuve.

Solution 2.7 (de l'exercice 2.7)

1. *La relation de divisibilité des entiers naturels signifie que, pour $x, y \in \mathbb{N}$, $x\mathcal{R}y$ si x divise y, c'est-à-dire si $\exists n \in \mathbb{N}$, $y = n \times x$. On note souvent $x|y$. Cette relation sur $\mathbb{N}$ est :*
   - *binaire ;*
   - *réflexive car tout entier naturel est son propre diviseur ;*
   - *antisymétrique : soient $x, y \in \mathbb{N}$, tels que $x\mathcal{R}y$ et $y\mathcal{R}x$; alors, il existe des entiers n et m tels que $y = n \times x$ et $x = m \times y$; donc $y = n \times m \times y$; donc $y = 0$ ou bien $n \times m = 1$; si $y = 0$, alors $x = m \times y = 0 = y$; si $n \times m = 1$, comme n et m sont des entiers, alors $n = m = 1$ et $y = m \times x = x$; dans tous les cas $x = y$;*
   - *transitive : soient $x, y, z \in \mathbb{N}$, tels que $x\mathcal{R}y$ et $y\mathcal{R}z$; alors, il existe des entiers n et m tels que $y = n \times x$ et $z = m \times y$; soit $p = n \times m$; alors $p \in \mathbb{N}$ et $z = p \times x$, donc $x\mathcal{R}z$.*

   Donc, $\mathcal{R}$ est une relation d'ordre sur $\mathbb{N}$. Par ailleurs, deux nombres premiers distincts ne se divisent pas, donc, par exemple, on n'a ni $2\mathcal{R}5$ ni $5\mathcal{R}2$. Ainsi, cette relation d'ordre est partielle.

2. *La relation de divisibilité des entiers relatifs signifie que, pour $x, y \in \mathbb{Z}$, $x\mathcal{R}y$ si x divise y, c'est-à-dire si $\exists n \in \mathbb{Z}$, $y = n \times x$. Elle n'est pas une relation d'ordre car elle n'est pas antisymétrique. En effet, 1 divise -1 et -1 divise 1.*

Solution 2.8 (de l'exercice 2.8) *La relation $\mathcal{R}$ sur $\mathbb{Z} \times \mathbb{N}^*$ est :*
- *binaire ;*
- *réflexive car, pour tout $(m, n) \in \mathbb{Z} \times \mathbb{N}^*$, $mn{=}nm$;*
- *symétrique : soient (m, n) et (p, q) dans $\mathbb{Z} \times \mathbb{N}^*$, tels que $(m, n)\mathcal{R}(p, q)$; alors $mq = np$ et donc $pn = qm$, d'où $(p, q)\mathcal{R}(m, n)$;*
- *transitive : soient (m, n), (p, q) et (r, s) des éléments de $\mathbb{Z} \times \mathbb{N}^*$ tels que $(m, n)\mathcal{R}(p, q)$ et $(p, q)\mathcal{R}(r, s)$; alors $mq = np$ et $ps = qr$. Comme q est non nul,*
  $$ms = mq\frac{s}{q} = np\frac{s}{q} = \frac{n}{q}ps = \frac{n}{q}qr = nr,$$
  et donc $(m, n)\mathcal{R}(r, s)$.

Donc $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{Z} \times \mathbb{N}^*$.

Solution 2.9 (de l'exercice 2.9) *Raisonnons par récurrence.*

- *L'énoncé est trivialement vrai pour* $n = 1$: $Card(A_1) = Card(A_1)$.
- *Soit* $n \geq 1$. *Supposons l'énoncé vrai pour* n. *Montrons qu'il reste vrai en* $n+1$. *Soit* $(A_i)_{1 \leq i \leq n+1}$ *une famille d'ensembles finis. Notons* $B = \bigcup_{i=1}^{n} A_i$.
  D'une part, $(A_i)_{1 \leq i \leq n}$ *est une famille d'ensembles finis, donc, par l'hypothèse de récurrence,*

$$Card\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{k=1}^{n}\left((-1)^{k+1} \sum_{1 \leq i_1 < \ldots < i_k \leq n} Card\left(\bigcap_{p=1}^{k} A_{i_p}\right)\right).$$

D'autre part, en considérant les deux ensembles finis B *et* A_{n+1}, *on peut utiliser la Proposition 2.12 :* $Card(A_{n+1} \cup B) = Card(A_{n+1}) + Card(B) - Card(A_{n+1} \cap B)$. *Ainsi,*

$$\begin{aligned} Card\left(\bigcup_{i=1}^{n+1} A_i\right) &= \sum_{k=1}^{n}\left((-1)^{k+1} \sum_{1 \leq i_1 < \ldots < i_k \leq n} Card\left(\bigcap_{p=1}^{k} A_{i_p}\right)\right) \\ &\quad + Card(A_{n+1}) - Card\left(A_{n+1} \cap \left(\bigcup_{i=1}^{n} A_i\right)\right). \end{aligned}$$

Or, par distributivité de l'union et de l'intersection, comme énoncé dans le Théorème 2.2 :

$$Card\left(A_{n+1} \cap \left(\bigcup_{i=1}^{n} A_i\right)\right) = Card\left(\bigcup_{i=1}^{n} (A_{n+1} \cap A_i)\right).$$

Donc, en appliquant l'hypothèse de récurrence aux n *ensembles* $(A_{n+1} \cap A_i)_{1 \leq 1 \leq n}$, *on obtient :*

$$\begin{aligned} &Card\left(A_{n+1} \cap \left(\bigcup_{i=1}^{n} A_i\right)\right) \\ &= \sum_{k=1}^{n}\left((-1)^{k+1} \sum_{1 \leq i_1 < \ldots < i_k \leq n} Card\left(\bigcap_{p=1}^{k} (A_{n+1} \cap A_{i_p})\right)\right) \\ &= \sum_{k=1}^{n}\left((-1)^{k+1} \sum_{1 \leq i_1 < \ldots < i_k < i_{k+1} = n+1} Card\left(\bigcap_{p=1}^{k+1} A_{i_p}\right)\right) \\ &= \sum_{k=2}^{n+1}\left((-1)^{k} \sum_{1 \leq i_1 < \ldots < i_k = n+1} Card\left(\bigcap_{p=1}^{k} A_{i_p}\right)\right), \end{aligned}$$

où le passage à la dernière ligne s'effectue en translatant l'indice k *d'une unité. Alors, en notant que* $-(-1)^k = (-1)^{k+1}$ *et que* $Card(A_{n+1})$ *correspond au terme en* $k = 1$ *de la somme précédente, on peut écrire :*

$$\begin{aligned} &Card(A_{n+1}) - Card\left(A_{n+1} \cap \left(\bigcup_{i=1}^{n} A_i\right)\right) \\ &= Card(A_{n+1}) + \sum_{k=2}^{n+1}\left((-1)^{k+1} \sum_{1 \leq i_1 < \ldots < i_k = n+1} Card\left(\bigcap_{p=1}^{k} A_{i_p}\right)\right) \\ &= \sum_{k=1}^{n+1}\left((-1)^{k+1} \sum_{1 \leq i_1 < \ldots < i_k = n+1} Card\left(\bigcap_{p=1}^{k} A_{i_p}\right)\right) \end{aligned}$$

puis :

$$\begin{aligned}
&Card\left(\bigcup_{i=1}^{n+1} A_i\right)\\
&=\sum_{k=1}^{n}\left((-1)^{k+1}\sum_{1\leq i_1<\ldots<i_k<n+1} Card\left(\bigcap_{p=1}^{k} A_{i_p}\right)\right)\\
&\ +\sum_{k=1}^{n+1}\left((-1)^{k+1}\sum_{1\leq i_1<\ldots<i_k=n+1} Card\left(\bigcap_{p=1}^{k} A_{i_p}\right)\right)\\
&=\sum_{k=1}^{n+1}\left((-1)^{k+1}\sum_{1\leq i_1<\ldots<i_k\leq n+1} Card\left(\bigcap_{p=1}^{k} A_{i_p}\right)\right).
\end{aligned}$$

Nous pouvons justifier plus précisément le passage à la dernière ligne : la condition $i_k \leq n+1$ correspond à la disjonction logique (le ou) entre $i_k = n+1$, ce qui est équivalent à la deuxième somme, et $i_k < n+1$; à première vue, ce dernier cas diffère de la première somme, laquelle est indexée de $k = 1$ à $k = n$ et non pas $k = n + 1$; néanmoins, le cas $i_k < n + 1$ correspond bien à la première somme dans la mesure où l'écriture $1 \leq i_1 < \ldots < i_k < n + 1$ suppose que $k \leq n$ (c'est le principe des tiroirs : il y a n entiers [les tiroirs] entre 1 et $n + 1$ où $n + 1$ est exclu ; on ne peut donc mettre strictement plus de n entiers distincts dedans [c'est-à-dire des chemises dans des tiroirs distincts]). Ceci prouve l'énoncé en $n + 1$.

- *L'énoncé a été prouvé pour $n = 1$ et on a démontré la propriété de récurrence donc on a prouvé l'énoncé pour tout $n \in \mathbb{N}^\star$.*

Solution 2.10 (de l'exercice 2.10) *(1) On cherche à montrer que $\mathbb{Z}$ est dénombrable, on doit donc être capable de compter ses éléments comme ceux de $\mathbb{N}$. Faisons cela en prenant successivement un nombre positif puis un nombre négatif : $0, -1, 1, -2, 2, -3, \cdots$*

Ainsi, nous sommes certains de parcourir tous les entiers naturels et tous leurs opposés, donc $\mathbb{Z}$ en entier. Nous avons ainsi construit une application de comptage f, telle que

$$f(0) = 0, f(1) = -1, f(2) = 1, f(3) = -2, f(4) = 2, f(5) = -3, \cdots$$

Voyez-vous la formule qui définit f ? Remarquez que les entiers naturels pairs ont pour image les entiers naturels et que les impairs ont pour image les entiers négatifs. Notre application f est tout simplement

$$f(2m) = m \quad \text{et} \quad f(2m + 1) = -m - 1 \qquad \text{pour tout } m \in \mathbb{N}.$$

Il est immédiat de vérifier que f est une bijection de $\mathbb{N}$ dans $\mathbb{Z}$.

(2) Comptons maintenant les paires (p, q) de $\mathbb{N} \times \mathbb{N}$. Procédons en nous intéressant aux paires dont la somme des éléments, $p+q$, vaut 0, puis 1, puis 2, etc. Notons qu'il y a $n + 1$ paires (p, q) dont la somme des éléments, $p + q$, vaut n : p peut varier de 0 à n et, une fois p choisi, q est connu et vaut $n - p$.

- *Pour* $n = 0$*, la seule paire est (0,0). Numérotons-la* 0.
- *Pour* $n = 1$*, les deux paires sont (0,1) et (1,0). Numérotons-les* 1 *et* 2.
- *Pour* $n = 2$*, les trois paires sont (0,2), (1,1) et (2,0). Numérotons-les* 3, 4 *et* 5.
- *Pour* $n = 3$*, les quatre paires sont (0,3), (1,2), (2,1) et (3,0). Numérotons-les* 6, 7, 8 *et* 9.
- *Ainsi de suite, pour* n *quelconque, les* $n+1$ *paires dont la somme des éléments est égale à* n *sont* $(0,n),(1,n-1),\cdots,(n-1,1)$ *et* $(n,0)$*. Graphiquement, ces paires représentent les points d'intersection de* $\mathbb{N}\times\mathbb{N}$ *et de la droite* $x+y=n$*, lues de bas en haut, comme on peut le voir sur la figure 2.2.*
  Comme nous avons déjà numéroté $n(n+1)/2$ *paires*[1]*, les indices de ces nouvelles* $(n+1)$ *paires dont la somme des éléments vaut* n *seront notés* $\frac{n(n+1)}{2}+k$ *pour* k *allant de* 0 *à* n*, comme on le voit sur la figure 2.3.*

	0	1	2	3
0	0	1	2	3
1	1	2	3	
2	2	3		
3	3			

FIGURE 2.2 – Solutions de $p+q=n$, $n \in \{0,1,2,3,\dots\}$.

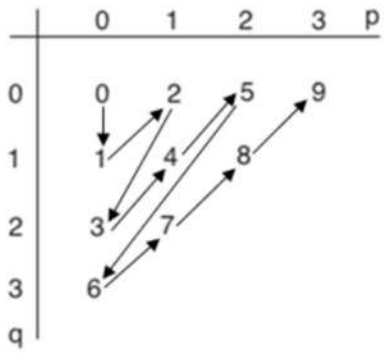

FIGURE 2.3 – Bijection de $\mathbb{N}\times\mathbb{N}$ dans $\mathbb{N}$.

Il est maintenant facile de voir que l'application de $\mathbb{N}\times\mathbb{N}$ *dans* $\mathbb{N}$ *ainsi construite est*

$$f(p,q) = \frac{(p+q)(p+q+1)}{2} + p.$$

Vous pouvez vous amuser à montrer rigoureusement que f *est effectivement une bijection de* $\mathbb{N}\times\mathbb{N}$ *dans* $\mathbb{N}$.

Notez que cela permet de montrer que $\mathbb{Q}$ *est dénombrable. En effet,* $\mathbb{Q}$ *peut facilement être mis en bijection avec* $\mathbb{Z}\times\mathbb{N}^*$*. Or, nous avons déjà mis* $\mathbb{Z}$ *et* $\mathbb{N}\times\mathbb{N}$ *en bijection avec* $\mathbb{N}$*. En composant correctement ces bijections, on peut donc aussi mettre* $\mathbb{Q}$ *en bijection avec* $\mathbb{N}$.

1. Le nombre de paires indiqué provient du fait que $\sum_{k=0}^{n-1}(k+1) = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

2.7 Solution des problèmes corrigés

Solution 2.11 (du problème 2.1) *(1) Pour répondre à cette question, il faut avoir une connaissance précise des variations de cette application f. f étant dérivable en tout point, on peut donc représenter un tableau de variations de f, chose que vous avez apprise à faire au lycée. Soit $\alpha \in \mathbb{R}$ et $t \in \mathbb{R}^+ \backslash \{0\}$. La dérivée de f en t s'écrit :*

$$f'(t) = t^{\alpha-2}e^{-t}(\alpha - 1 - t).$$

On a ainsi plusieurs variations possibles, selon la valeur du paramètre α. Ainsi, si $\alpha \leq 1$, l'application f est strictement décroissante, avec une limite à 0 lorsque $t \to \infty$ et une limite à 1 (respectivement $+\infty$) lorsque $t \to 0$ pour $\alpha = 1$ (respectivement $\alpha < 1$). Par ailleurs, si $\alpha > 1$, on a le tableau de variations suivant :

t	0		$\alpha - 1$		$+\infty$
$f'(t)$		+	|	-	
$f(t)$	0	$\nearrow$	$f(\alpha - 1)$	$\searrow$	0

Pour ce qui est de l'injectivité, f est injective sans restriction de son ensemble de départ si $\alpha \leq 1$ car elle est strictement décroissante[1]. Il va de soi que toute restriction de f à un intervalle inclus dans $\mathbb{R}^+ \backslash \{0\}$ est aussi strictement monotone donc injective. Mais ce problème, sans grande difficulté de raisonnement, peut aussi être l'occasion de passer en revue certains résultats démontrés dans ce cours : vous pouvez donc conclure de la même manière en utilisant la Proposition 2.5 qui stipule que toute restriction d'une application injective est aussi une application injective.

Dans l'autre cas, où $\alpha > 1$, il y a un changement de monotonie. La restriction de f à $]0, \alpha - 1]$ ou à $[\alpha - 1, +\infty[$ ainsi qu'à tous les intervalles inclus dans chacun de ces deux intervalles est strictement monotone donc injective. Attention cependant à ne pas affirmer trop vite qu'il n'y a pas d'autre intervalle pouvant convenir : par exemple, la restriction de l'application

$$\mathbb{R} \to \mathbb{R}, x \mapsto \begin{cases} 1/x & \text{si } x < 0 \\ x & \text{sinon} \end{cases}$$

à tout intervalle est injective (prenez une feuille et un crayon et dessinez le graphe de cette application : cela devrait suffire à vous convaincre et à

1. Relisez la Définition 2.13 si le lien entre stricte monotonie et injectivité n'est pas clair : $\forall s < t$, la stricte décroissance implique que $f(s) > f(t)$ donc *a fortiori* $f(s) \neq f(t)$.

vous faire sentir les raisons qui distinguent injectivité et monotonie), alors même que cette application est décroissante puis croissante. D'une manière générale, le théorème des valeurs intermédiaires garantit qu'une application non monotone n'est pas injective si elle est continue. Dans notre problème particulier, considérons un intervalle I contenant un certain $x \in \mathbb{R}$ et un certain $y \in \mathbb{R}$, tels que $x < \alpha - 1 < y$. Montrons que $f_{|I}$ n'est pas injective. Si $f(x) = f(y)$, comme $x \neq y$ et $x, y \in I$, par définition $f_{|I}$ n'est pas injective. Supposons alors que $f(x) \neq f(y)$. Cela signifie donc que $f(x) < f(y)$ ou bien $f(y) < f(x)$. Intéressons-nous au premier cas, le deuxième étant démontrable de la même manière : ainsi nous supposons que $f(x) < f(y)$. D'après le tableau de variations de f, le maximum de l'application f est atteint en $\alpha - 1$. f étant continue sur $[x, \alpha - 1]$ et $f(y)$ appartenant à l'image directe de $[x, \alpha - 1]$ par f, le théorème des valeurs intermédiaires affirme qu'il existe $z \in [x, \alpha - 1]$ tel que $f(z) = f(y)$. Or, $z \leq \alpha - 1 < y$, donc $z \neq y$. Comme $f(z) = f(y)$ et $z, y \in I$, ceci prouve que $f_{|I}$ n'est pas injective. Donc, les seuls intervalles pour lesquels la restriction de f est injective sont ceux déjà cités : $]0, \alpha - 1]$, $[\alpha - 1, +\infty[$ ainsi que tous les intervalles inclus dans chacun de ces deux intervalles.

(2) L'étude des variations de f, faite à la question précédente, permet de répondre. L'injectivité de f n'est vraie que pour $\alpha \leq 1$. Concernant la surjectivité, comme l'ensemble d'arrivée est $\mathbb{R}^+ \backslash \{0\}$, l'étude des variations de f nous enseigne que $\alpha < 1$ est le seul cas qui convienne. Attention toutefois : si dans l'énoncé l'ensemble d'arrivée de f avait été $\mathbb{R}^+$, aucune valeur du paramètre α n'aurait permis à f d'être surjective dans la mesure où $f^{-1}(\{0\}) = \emptyset$ pour tout $\alpha \in \mathbb{R}$. Donc, f est bijective si et seulement si $\alpha < 1$.

(3) Notez que $g = f \circ f$. Le Théorème 2.10 permet de conclure que, pour tout α tel que f est bijective, alors g est bijective. Ceci fournit une condition suffisante de bijectivité de g : $\alpha < 1$. Mais ce n'est pas une condition nécessaire et nous devons maintenant nous demander s'il n'existe pas un α tel que g est bijective mais pas f. En l'occurrence, si nous supposons que g est bijective alors g est a fortiori surjective. Or, nous avons expliqué dans l'exemple 2.6 que la composée $u \circ v$ de deux applications u et v est surjective seulement si u est aussi surjective. Ainsi, dans notre problème, la surjectivité de g implique la surjectivité de f. Comme nous l'avons mentionné dans notre réponse à la question précédente, f est surjective si et seulement si $\alpha < 1$. Ainsi $\alpha < 1$ est une condition nécessaire de bijectivité de g. Nous avions déjà montré que c'était une condition suffisante, donc nous pouvons caractériser la bijectivité de g par la condition $\alpha < 1$.

(4) On peut réécrire la relation $\mathcal{R}$, pour $(x, y) \in (\mathbb{R}^+ \backslash \{0\})^2$, par $x\mathcal{R}y$ si et seulement si $f(x) = f(y)$. Pour montrer que $\mathcal{R}$ est une relation d'équiva-

lence sur $\mathbb{R}^+\backslash\{0\}$, *il faut vérifier les quatre conditions citées dans la Définition 2.24 : binaire, réflexive, symétrique, transitive. Cette vérification est triviale, mais il faut tout de même faire cet effort minimal de citer ces quatre conditions (si le reste de votre réponse au problème n'est pas entièrement juste, le correcteur s'attend même à voir plus qu'un simple rappel de la définition), sans quoi la personne vous lisant pourrait croire que vous usez d'un subterfuge pour camoufler une méconnaissance supposée de la définition d'une relation d'équivalence : être rapide ne dispense pas d'être rigoureux !*

(5) *Soit* $x \in \mathbb{R}^+\backslash\{0\}$ *et* $y \in \mathcal{R}(x)$. *Alors,* $f(x) = f(y)$. *Deux cas se présentent, selon la valeur prise par* α *(on utilisera notre réponse à la question (1)) :*
- *Si* $\alpha \leq 1$, *alors* f *est injective, donc* $f(x) = f(y) \Rightarrow x = y$. *Ainsi, la classe d'équivalence* $\mathcal{R}(x)$ *est réduite au singleton* $\{x\}$.
- *Si* $\alpha > 1$, *alors* f *n'est pas injective. Là encore, plusieurs cas sont possibles, selon la valeur de* x *:*
  - *Si* x *correspond au point maximisant* f, *c'est-à-dire si* $x = \alpha - 1$, *alors la classe d'équivalence* $\mathcal{R}(x)$ *est réduite au singleton* $\{x\}$. *En effet, comme la restriction de* f *à* $]0, \alpha - 1]$ *ou à* $[\alpha - 1, +\infty[$ *est injective, alors, pour* $y \in \mathcal{R}(x)$, *si* $y \in]0, \alpha - 1]$, $f(\alpha - 1) = f(y) \Rightarrow \alpha - 1 = y$ *par injectivité de* $f_{|]0,\alpha-1]}$, *et si* $y \in [\alpha - 1, +\infty[$, $f(\alpha - 1) = f(y) \Rightarrow \alpha - 1 = y$ *par injectivité de* $f_{|[\alpha-1,+\infty[}$.
  - *Si* $x < \alpha - 1$, *alors la classe d'équivalence* $\mathcal{R}(x)$ *est constituée de deux éléments. En effet, par injectivité de* $f_{|]0,\alpha-1]}$, *il n'existe pas d'élément de la classe de* x *autre que* x *dans* $]0, \alpha - 1]$. *Or, d'après notre étude des variations de* f, *on note que* $f(x) \in f(]0, \alpha - 1[) = f(]\alpha - 1, +\infty[)$. *Donc, il existe* $y \in]\alpha - 1, +\infty[$ *tel que* $f(x) = f(y)$. *Par hypothèse,* $x \neq y$, *donc* y *est un élément de la classe de* x *distinct de* x. *C'est d'ailleurs le seul appartenant à l'intervalle* $]\alpha - 1, +\infty[$ *par injectivité de* $f_{|]\alpha-1,+\infty[}$.
  - *Si* $x > \alpha - 1$, *alors la classe d'équivalence* $\mathcal{R}(x)$ *est constituée de deux éléments. Le raisonnement est symétrique à celui fait pour le cas* $x < \alpha - 1$.

Chapitre 3

Introduction à l'algèbre générale

Nous nous intéressons dans ce chapitre aux structures algébriques, structures généralement composées d'un *ensemble* et d'une ou de plusieurs *lois de composition* satisfaisant certains *axiomes*. Les structures de base auxquelles vous allez souvent être confrontés sont les groupes, les anneaux et les corps. Mais avant de nous lancer dans l'étude de ces structures algébriques, définissons le seul mot clé qui vous est encore étranger, à savoir les *lois de composition*.

3.1 Lois de composition

Soient E et K deux ensembles donnés. Une loi de composition est une application de $E \times K$ dans E. Si $K = E$, la loi est dite interne ; si $K \neq E$, la loi est dite externe.

3.1.1 Lois de composition internes

Définition 3.1 *Soit E un ensemble. On appelle loi de composition interne toute application $*$ de $E \times E$ dans E.*

Bien qu'étant une application, on utilise généralement les notations $*$, $\cdot$, $+$, $\times$, $\circ$, T, $\ldots$ pour les lois de composition, au lieu des notations usuelles f, g, ... Dans l'ensemble des entiers naturels, l'addition $+$ et la multiplication $\times$ sont des lois de composition interne.

Un ensemble E muni d'une loi de composition interne $*$ sera noté $(E, *)$. On n'omettra de préciser la loi de composition que s'il n'y a aucune ambiguïté sur celle-ci.

3.1.2 Associativité et commutativité

Vous avez déjà l'habitude de manipuler les lois de composition internes $+$ et $\times$ sur les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, probablement sans vous en rendre compte ! Vous savez par exemple que $a+(b+c) = (a+b)+c$ et $a+b = b+a$. Le fait de pouvoir placer les parenthèses où vous voulez sans modifier le résultat est une propriété de certaines lois de composition internes que l'on appelle l'associativité. Aussi, le fait de pouvoir permuter les éléments a et b sans affecter le résultat s'appelle la commutativité. Ces propriétés ne sont pas caractéristiques de l'addition et de la multiplication de nombres, mais sont des axiomes que l'on exigera des lois de composition pour pouvoir définir plusieurs structures algébriques de base.

Définition 3.2 *Soit E un ensemble muni d'une loi de composition interne $*$. On dit que :*
– *$*$ est associative si, pour tout $(x, y, z) \in E^3$, $x * (y * z) = (x * y) * z$,*
– *$*$ est commutative si, pour tout $(x, y) \in E^2$, $x * y = y * x$.*

Avant d'aller plus loin, donnons quelques exemples de telles lois.

Exemple 3.1 *Sur tous les ensembles de nombres que vous connaissez ($\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$), les lois de composition internes $+$ et $\times$ sont associatives et commutatives. Mais les lois de composition ne sont pas définies uniquement sur les ensembles de nombres. Par exemple, si E est un ensemble non vide, l'union $\cup$ et l'intersection $\cap$ sont des lois de composition internes sur $\mathcal{P}(E)$, l'ensemble des parties de E. Ces deux lois sont associatives et commutatives dans $\mathcal{P}(E)$. Cela a été démontré dans le cours sur la théorie des ensembles. Souvenez-vous, nous avions vu que pour tous A, B et C appartenant à $\mathcal{P}(E)$,*

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

Ceci correspond à l'associativité et à la commutativité de l'union. Il en est de même pour l'intersection car

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

Vous utilisez depuis votre maternelle la commutativité sans y réfléchir. Maintenant que les lois auxquelles vous serez confronté ne seront pas toutes commutatives, vous devez faire attention aux règles de calcul que vous appliquez.

Par exemple, si x et y sont deux éléments d'un ensemble E muni d'une loi de composition interne non commutative $*$, alors $x * y * x$ peut être différent de $x^2 * y$!

Construisons justement un exemple d'ensemble muni d'une loi non commutative en utilisant les notions acquises dans le chapitre sur les ensembles et les applications.

Exemple 3.2 *Considérons E un ensemble non vide et $\mathcal{F}(E)$ l'ensemble de toutes les applications de E dans E. Dans $\mathcal{F}(E)$, la loi de composition des applications $\circ$ est associative mais n'est pas commutative ! Prenons par exemple $E = [0, 1]$, l'application f constante nulle sur E et l'application g constante sur E égale à 1. Alors pour tout $x \in E$, $(f \circ g)(x) = f(1) = 0$ est différent de $(g \circ f)(x) = g(0) = 1$. Ainsi, dans $(\mathcal{F}(E), \circ)$, les applications f et g ne commutent pas.*

De même, vous pouvez construire des exemples d'ensembles munis de lois non associatives. Dans un premier exemple, considérons un ensemble à deux éléments distincts $G = \{a, b\}$ et définissons dessus une loi non associative.

Exemple 3.3 *Soit $*$ la loi définie sur G par $b*a = b*b = a$ et $a*b = a*a = b$. Il est plus facile de visualiser comment la loi $*$ opère sur G en explicitant sa table de composition*

$*$	a	b
a	b	b
b	a	a

Remarquez d'abord que $*$ est bien une loi de composition interne. Toutefois, elle n'est pas associative. En effet,

$$a * (b * a) = a * a = b \qquad \text{et} \qquad (a * b) * a = b * a = a$$

ne sont pas égaux.

Nous trouvons en géométrie des exemples plus intéressants.

Exemple 3.4 *Le produit vectoriel sur $\mathbb{R}^3$, défini, pour $(x, y, z) \in \mathbb{R}^3$ et pour $(u, v, w) \in \mathbb{R}^3$, par*

$$(x, y, z) \wedge (u, v, w) = (yw - vz, -xw + uz, xv - uy),$$

est une loi de composition interne non associative.

Considérons l'élément nul $0_{\mathbb{R}^3} = (0, 0, 0)$. Remarquez que pour tout $X = (x, y, z) \in \mathbb{R}^3$, le produit vectoriel de X avec lui-même est l'élément nul,

$X \wedge X = 0_{\mathbb{R}^3}$. Introduisons aussi les éléments $e_1 = (1,0,0)$, $e_2 = (0,1,0)$ et $e_3 = (0,0,1)$. La famille (e_1, e_2, e_3) forme ce que vous appellerez plus tard la base canonique de $\mathbb{R}^3$. Nous pouvons maintenant utiliser la définition du produit vectoriel et calculer

$$e_2 \wedge (e_2 \wedge e_3) = e_2 \wedge e_1 = -e_3 \qquad \textit{et} \qquad (e_2 \wedge e_2) \wedge e_3 = 0_{\mathbb{R}^3} \wedge e_3 = 0_{\mathbb{R}^3}.$$

Ceci prouve que le produit vectoriel $\wedge$ n'est pas une loi associative sur $\mathbb{R}^3$.

Si la loi est associative, comme le résultat ne dépend pas de l'emplacement des parenthèses, on peut définir, pour tout x dans E et tout n dans $\mathbb{N}^*$, $x^n = x * \cdots * x$ où $*$ est appliquée n fois. Il en découle le petit lemme suivant :

Lemme 3.1 *Soit E un ensemble muni d'une loi de composition interne associative $*$. Soient $x \in E$ et $(n, m) \in \mathbb{N}^* \times \mathbb{N}^*$. On a*

$$x^n * x^m = x^{n+m} \qquad \textit{et} \qquad (x^n)^m = x^{nm}$$

De plus, si la loi de composition interne est à la fois associative et commutative, le résultat du produit de n éléments ne dépend ni de l'emplacement des parenthèses ni de l'ordre des éléments dans la multiplication. Autrement dit, on peut permuter arbitrairement les éléments x_i dans $x_1 * x_2 * \cdots * x_n$ sans changer le résultat !

3.1.3 Élément neutre

L'addition de 0 et d'un nombre quelconque ne change pas ce nombre-là. De même, la multiplication de 1 et d'un nombre quelconque ne modifie pas ce dernier. Nous ne vous apprenons rien de nouveau jusque là ! On dit que 0 est un élément neutre pour l'addition dans $\mathbb{N}$ et que 1 est un élément neutre pour la multiplication dans $\mathbb{N}$. Êtes-vous prêt pour un peu plus de formalisme ?

Définition 3.3 *Soit E un ensemble non vide muni d'une loi de composition interne $*$. On dit que $e \in E$ est élément neutre pour la loi $*$ si, pour tout $x \in E$,*

$$x * e = e * x = x.$$

Vous savez que 0 est le seul élément de $(\mathbb{N}, +)$ à satisfaire cette propriété. C'est donc l'élément (et non pas un élément) neutre de $(\mathbb{N}, +)$. Cela vaut aussi pour 1 dans $(\mathbb{N}, \times)$. Ce résultat est vrai de manière plus générale.

Théorème 3.1 *Soit E un ensemble non vide muni d'une loi de composition interne $*$. Il existe au plus un élément neutre $e \in E$ pour la loi $*$.*

Preuve. Supposons que l'on ait deux éléments neutres e_1 et e_2 pour $*$ dans E. On a alors, en choisissant $x = e_1$ et $e = e_2$ dans la Définition 3.3,

$$e_1 * e_2 = e_2 * e_1 = e_1,$$

et, en choisissant $x = e_2$ et $e = e_1$ dans la même définition,

$$e_2 * e_1 = e_1 * e_2 = e_2.$$

Cela prouve alors que $e_1 = e_2$ et l'unicité de l'élément neutre, dès qu'il existe.
■

Revenons sur les ensembles et lois vus dans les exemples précédents.

Exemple 3.5 *Soit E un ensemble non vide.*
(i) L'ensemble vide $\emptyset$ est l'élément neutre pour $(\mathcal{P}(E), \cup)$ car, pour tout A dans $\mathcal{P}(E)$,

$$A \cup \emptyset = \emptyset \cup A = A.$$

(ii) L'ensemble E est l'élément neutre pour $(\mathcal{P}(E), \cap)$ car, pour tout A dans $\mathcal{P}(E)$,

$$A \cap E = E \cap A = A.$$

(ii) L'identité est l'élément neutre pour $(\mathcal{F}(E), \circ)$. Toute application de E dans E composée à droite ou à gauche avec Id_E est égale à elle-même.

Lorsque la loi $*$ admet un élément neutre e dans E, on conviendra que pour tout $x \in E$, $x^0 = e$. Souvenez-vous que c'est exactement la convention que vous utilisez pour les nombres, x^0 valant 1 pour tout $x \in \mathbb{R}$.

3.2 Groupes

Nous avons maintenant tous les ingrédients nécessaires à la définition de votre première structure algébrique : les groupes.

Définition 3.4 *Soit G un ensemble muni d'une loi de composition interne $*$. On dit que le couple $(G, *)$ est un groupe si*
(i) la loi $*$ est associative,
(ii) $(G, *)$ admet un élément neutre, c'est-à-dire

$$\exists e \in G, \quad \forall x \in G, \quad x * e = e * x = x$$

(iii) et tout élément de G admet un symétrique, c'est-à-dire

$$\forall x \in G, \quad \exists y \in G, \quad x * y = y * x = e.$$

Si la loi $*$ est aussi commutative, on dit que le groupe $(G, *)$ est commutatif (ou encore abélien).

Insistons sur le fait que l'on ne peut parler de groupe que si la loi de composition est précisée ! Cela n'a pas de sens de dire qu'un ensemble G est un groupe ! Au risque de nous répéter, un groupe est un couple (ensemble, loi de composition interne).

Remarquez que les propriétés d'associativité et de commutativité de la loi $*$ n'ont pas la même importance dans cette définition. L'associativité est requise pour pouvoir parler d'un groupe, la commutativité, elle, est optionnelle.

Avant d'aller plus loin, donnons quelques exemples de groupes et quelques contre-exemples.

Exemple 3.6 *L'ensemble des entiers relatifs muni de l'addition $(\mathbb{Z}, +)$ est un groupe abélien, dont l'élément neutre est 0. Chaque élément $x \in \mathbb{Z}$ admet un symétrique que l'on appelle usuellement opposé et que l'on note $-x$ au lieu de x^{-1}. Cela découle de la notation usuelle $x + (-x) = 0$. De manière générale, la notation du symétrique x^{-1} est réservée à la notation multiplicative de la loi, $*$ ou $\times$, et la notation $-x$ est réservée à la notation additive de la loi, $+$.*

Exemple 3.7 *L'ensemble des entiers naturels muni de l'addition $(\mathbb{N}, +)$ n'est pas un groupe : mis à part 0, l'élément neutre de la loi $+$, aucun autre élément de $\mathbb{N}$ n'admet de symétrique (ou opposé). Les opposés des entiers naturels non nuls vivent dans $\mathbb{Z}$ privé de $\mathbb{N}$.*

De même, l'ensemble des entiers relatifs non nuls muni de la multiplication $(\mathbb{Z}^*, \times)$ n'est pas un groupe car les seuls éléments de $\mathbb{Z}^*$ admettant un symétrique, appelé aussi inverse dans le cas multiplicatif, sont 1 et -1. Les inverses des entiers relatifs non nuls vivent dans $\mathbb{Q}$. Plus précisément, si $p \in \mathbb{Z}^*$ tel que $p \neq 1$ et $p \neq -1$, alors $\frac{1}{p}$ appartient à $\mathbb{Q}$ privé de $\mathbb{Z}$.

Exemple 3.8 *L'ensemble des réels non nuls muni de la loi de multiplication $(\mathbb{R}^*, \times)$ est un groupe. Ce groupe est abélien. Son élément neutre est 1. Bien entendu, l'ensemble des réels muni de la loi de multiplication n'est pas un groupe, car l'élément 0 n'admet pas de symétrique (ou d'inverse) : l'inverse d'un réel x est x^{-1} ou encore $\frac{1}{x}$ et on ne peut pas diviser par 0 !*

Aventurons-nous maintenant à donner des exemples hors des ensembles de nombres. Travaillons par exemple sur un ensemble d'ensembles.

Exemple 3.9 *Soient E un ensemble non vide et $\mathcal{P}(E)$ l'ensemble de ses parties. Muni de la différence symétrique, définie par*

$$\forall (A, B) \in \mathcal{P}(E) \times \mathcal{P}(E), \quad A \Delta B = (A \cup B) \backslash (A \cap B),$$

$(\mathcal{P}(E), \Delta)$ est un groupe. La figure 3.1 permet de visualiser cette définition.

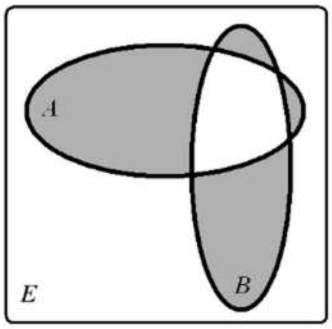

FIGURE 3.1 – Différence symétrique de A et B dans E.

Vous pouvez vérifier à la main l'associativité de la loi Δ en utilisant celle des lois d'union et d'intersection d'ensembles. Faites-le ! Notons au passage que la commutativité des lois $\cup$ et $\cap$ implique que Δ est aussi commutative.

Ensuite, il est facile de vérifier que l'ensemble vide $\emptyset$ est l'élément neutre pour la loi Δ car, pour tout $A \subset E$, on a

$$A\Delta\emptyset = (A \cup \emptyset)\backslash(A \cap \emptyset) = A\backslash\emptyset = A \cap \overline{\emptyset} = A \cap E = A.$$

Et, par commutativité de Δ, on conclut que $\emptyset\Delta A = A\Delta\emptyset = A$.

Il ne reste plus qu'à vérifier que tout élément A de $\mathcal{P}(E)$ admet un symétrique, c'est-à-dire qu'il existe $B \in \mathcal{P}(E)$ tel que $A\Delta B = B\Delta A = \emptyset$. L'ensemble A lui-même satisfait bien ces propriétés. En effet,

$$A\Delta A = (A \cup A)\backslash(A \cap A) = A\backslash A = A \cap \overline{A} = \emptyset.$$

Ceci prouve que $(\mathcal{P}(E), \Delta)$ est bien un groupe.

Les ensembles d'applications sont aussi une source inépuisable d'exemples.

Exemple 3.10 *Soit E un ensemble non vide. L'ensemble des bijections de E muni de la loi de composition des applications est un groupe. Faites un effort pour démontrer ce petit résultat par vous-même. Cela vous fera une bonne révision sur les applications !*

Remarquez d'abord que la composition des applications constitue bien une loi de composition interne sur l'ensemble des bijections de E, la composition de deux applications bijectives sur E étant elle-même une bijection de E. De plus, vous savez déjà que cette loi est associative. Aussi, elle admet clairement un élément neutre qui n'est autre que l'application bijective Id_E, l'application identité sur E. Enfin, toute bijection ϕ sur E admet une bijection réciproque

ϕ^{-1} satisfaisant $\phi(\phi^{-1}(x)) = x = \phi^{-1}(\phi(x))$ pour tout $x \in E$, ce qui prouve que $\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = Id_E$. Dit autrement, toute bijection ϕ sur E est inversible[1] *pour la loi de composition et son symétrique est ϕ^{-1}. Ceci conclut la preuve. En revanche, la loi de composition n'étant pas commutative, ce groupe n'est pas abélien.*

Maintenant que vous savez ce qu'est un groupe, regardons de plus près cette structure algébrique.

Théorème 3.2 *Soit $(G, *)$ un groupe. Les assertions suivantes sont vraies :*
(i) $(G, *)$ admet un unique élément neutre, que l'on note e.
(ii) Pour tout $x \in G$, x admet un unique symétrique, que l'on notera x^{-1}.
(iii) L'élément neutre est son propre symétrique,

$$e^{-1} = e.$$

(iv) Le symétrique du symétrique d'un élément $x \in G$ est l'élément x lui-même,

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

(v) Pour tout $(x, y) \in G^2$, $(x * y)^{-1} = y^{-1} * x^{-1}$.
(vi) Pour tout $(x, y, z) \in G^3$, si $x * y = x * z$ alors $y = z$.

Si vous avez assimilé le début de ce chapitre, vous réussirez à démontrer ces résultats élémentaires. Cela requiert une gymnastique de l'esprit que vous devez nécessairement développer. En cas de difficultés, voici une preuve pour vous aider à assimiler ces techniques.

Preuve. (i) Par définition, $(G, *)$ admet un élément neutre et par le Théorème 3.1, il en admet au plus un, d'où l'unicité affirmée au point (i).

(ii) Soit $x \in G$. Supposons que x admette deux symétriques y_1 et y_2. Comme e est l'élément neutre, $y_1 = y_1 * e$. Et comme y_2 est un symétrique de x, $e = x * y_2 = y_2 * x$. Donc

$$y_1 = y_1 * e = y_1 * (x * y_2) = (y_1 * x) * y_2 = e * y_2 = y_2.$$

La troisième égalité découle de l'associativité de la loi $*$, la quatrième du fait que y_1 est un symétrique de x et la dernière de la définition de e. Ceci démontre que x admet un unique symétrique, que l'on notera x^{-1}.

(iii) Par définition du symétrique de e, on a $e * e^{-1} = e^{-1} * e = e$. Mais par définition de e, on a également $e * e^{-1} = e^{-1}$. Donc $e = e^{-1}$ et e est son propre symétrique.

1. C'est-à-dire : admet un symétrique.

(iv) La succession des égalités suivantes démontre ce point :

$$(x^{-1})^{-1} = (x^{-1})^{-1} * e = (x^{-1})^{-1} * (x^{-1} * x) = \left((x^{-1})^{-1} * x^{-1}\right) * x = e * x = x.$$

La deuxième égalité découle de la définition du symétrique de x, la troisième de l'associativité de la loi $*$ et la quatrième de la définition du symétrique de x^{-1}.

(v) Comme le symétrique de $(x * y)$ est unique, vérifions qu'il est donné par $(y^{-1} * x^{-1})$. Il suffit donc de calculer

$$(x * y) * (y^{-1} * x^{-1}) = x * (y * y^{-1}) * x^{-1} = x * (e * x^{-1}) = x * x^{-1} = e.$$

(vi) Cette dernière assertion est simple à démontrer. Il vous suffit de composer à gauche par x^{-1} et de vous souvenir de la définition de e pour obtenir

$$y = e * y = (x^{-1} * x) * y = x^{-1} * (x * y) = x^{-1} * (x * z) = (x^{-1} * x) * z = e * z = z.$$

■

Insistons sur quelques points du théorème précédent. D'abord, nous avions mentionné l'importance de l'associativité dans la définition d'un groupe. Entre autres, elle garantit l'unicité des symétriques.

Exemple 3.11 *Soit $G = \{0, a, b\}$ un ensemble à 3 éléments distincts et T la loi de composition interne définie par*

(i) $0\ T\ a = a\ T\ 0 = a$ *et* $0\ T\ b = b\ T\ 0 = b$ *et* $0\ T\ 0 = 0$.
(ii) $a\ T\ b = b\ T\ a = a\ T\ a = b\ T\ b = 0$.

La table de composition de T aide à mieux visualiser toutes ces équations.

T	0	a	b
0	0	a	b
a	a	0	0
b	b	0	0

Le point (i) dit que 0 *est l'élément neutre de* (G, T). *Le point (ii) assure que a et b admettent des symétriques, mais que ces symétriques ne sont pas uniques. En effet, a et b sont symétriques l'un pour l'autre et chacun est aussi son propre symétrique. Par le point (ii) de notre théorème,* (G, T) *ne pourrait être un groupe. Comme vous l'avez sans doute deviné, l'hypothèse manquante est l'associativité de la loi T. En effet*

$$(a\ T\ b)\ T\ b = 0\ T\ b = b \qquad et \qquad a\ T\ (b\ T\ b) = a\ T\ 0 = a$$

ne sont pas égaux.

Les exemples suivants vous permettront d'éviter de fausses interprétations ou mauvaises lectures des hypothèses nécessaires aux points (v) et (vi) du théorème.

Exemple 3.12 *Le point (v) dit que le symétrique du produit de x et de y est le produit dans le sens inverse des symétriques y^{-1} et x^{-1}. Si le groupe n'est pas commutatif, l'ordre dans lequel le produit des symétriques est fait est très important. Dans ce cas,*

$$x * y * x^{-1} * y^{-1} \neq e.$$

Par contre, si le groupe est abélien, on obtient que

$$x * y * x^{-1} * y^{-1} = (x * y) * (y^{-1} * x^{-1}) = (x * y) * (x * y)^{-1} = e.$$

Ici, la première égalité découle de la commutativité du groupe et la deuxième du point (v) du Théorème 3.2. La dernière est une conséquence du point (iii) de la Définition 3.4, concernant le symétrique d'un élément du groupe.

Cet exemple démontre que la prudence doit être de rigueur : vos réflexes de calcul algébrique peuvent s'avérer trompeurs !

Exemple 3.13 *Dans le même esprit que celui de l'exemple ci-dessus, il faut faire attention à l'ordre des éléments dans le point (vi) du théorème. Si x, y et z sont des éléments du groupe $(G, *)$ tels que $x * y = z * x$, on ne peut pas en déduire l'égalité $y = z$, à moins bien sûr que le groupe soit abélien !*

Exemple 3.14 *Il est crucial dans la Définition 3.4 que tous les éléments de G soient inversibles. Sans cela, le point (vi) du Théorème 3.2 devient faux, par exemple. Dans $\mathbb{R}$, $xy = xz$ implique $y = z$ uniquement si x est non nul, car simplifier par x revient à composer à gauche par le symétrique x^{-1} qui n'existe que si x est différent de 0.*

Théorème 3.3 *Soit $(G, *)$ un groupe. Pour tout $x \in G$ et tout $n \in \mathbb{N}^*$,*

$$(x^n)^{-1} = (x^{-1})^n.$$

Preuve. Démontrons ce théorème par récurrence. Soit $x \in G$. La proposition est trivialement vérifiée pour $n = 1$. Supposons que $(x^{n-1})^{-1} = (x^{-1})^{n-1}$. On a alors

$$(x^{-1})^n * x^n = x^{-1} * \left((x^{-1})^{n-1} * x^{n-1}\right) * x = x^{-1} * e * x = x^{-1} * x = e.$$

On conclut alors par unicité du symétrique démontrée dans le point *(ii)* du Théorème 3.2. ■

On notera x^{-n} pour $(x^n)^{-1}$, pour tout $x \in E$ et $n \in \mathbb{N}$. Souvenez-vous de la convention $x^0 = e$. Ceci permet de définir x^m pour tout $m \in \mathbb{Z}$. On a alors les relations suivantes, vraies pour tout $(m, n) \in \mathbb{Z}^2$ et tout $x \in E$:

$$(x^m)^n = x^{nm} \qquad \text{et} \qquad x^m * x^n = x^{m+n}.$$

3.3 Sous-groupes

Un groupe peut contenir beaucoup d'éléments et la compréhension de sa structure peut être délicate. La stratégie *séparer pour régner* s'impose de fait. Au lieu d'étudier directement le groupe dans son ensemble, il sera très utile de s'intéresser à des sous-ensembles de notre groupe qui, munis de la loi du groupe, gardent la structure de groupe ; nous avons nommé les sous-groupes.

3.3.1 Définitions et exemples

Définition 3.5 *Soit $(G, *)$ un groupe et $H \subset G$ un sous-ensemble non vide de G. On dit que H est un sous-groupe de G si la restriction de $*$ à $H \times H$ confère à H une structure de groupe, c'est-à-dire que la restriction de la loi $*$ à $H \times H$ est une loi de composition interne, associative (cela est vrai car elle l'est sur G), admettant un élément neutre et pour laquelle tout élément de H est inversible dans H.*

De manière équivalente, cette définition peut s'écrire comme suit :

Définition 3.6 *Soit $(G, *)$ un groupe d'élément neutre e et H un sous-ensemble de G. H est un sous-groupe de G si*
(i) $e \in H$,
(ii) pour tout $(x, y) \in H^2$, $x * y \in H$,
(iii) et pour tout $x \in H$, $x^{-1} \in H$.

Les conditions ci-dessus peuvent être remplacées par celles données par le théorème suivant :

Théorème 3.4 *Un sous-ensemble H d'un groupe G est un sous-groupe de G si et seulement si H est non vide et*

$$\forall x \in H, \quad \forall y \in H, \quad x * y^{-1} \in H.$$

Preuve. Supposons que H soit un sous-groupe de G. Donc $e \in H$ et H est non vide. Soient x et y deux éléments de H. On a alors $y^{-1} \in H$ par le point (iii) de la Définition 3.6, et donc $x * y^{-1} \in H$ par le point (ii).

Supposons maintenant que H est non vide et que pour tous $x, y \in H$, $x * y^{-1} \in H$. Soit $x \in H$, on a alors $e = x * x^{-1} \in H$. Aussi, $x^{-1} = e * x^{-1} \in H$, ce qui démontre le point (iii). Finalement, le point (ii) découle du fait que $x * y = x * (y^{-1})^{-1} \in H$ pour tous x et y dans H. ■

Pour réfléchir un peu à ces définitions, essayez de construire des exemples de sous-groupes pour chacun de vos groupes favoris. N'ayez aucune inquiétude ! Si cela vous semble encore mystérieux, nous vous proposons aussi une multitude d'exemples.

Exemple 3.15 *Etant donné un groupe $(G, *)$, d'élément neutre e, les deux exemples les plus simples de sous-groupes sont :*
(i) Le groupe G lui-même !
(ii) Le sous-groupe $H = (\{e\}, *)$ qui ne contient que l'élément neutre e de G.
Vous pouvez facilement vérifier qu'ils satisfont l'une des deux (et donc les deux !) définitions ci-dessus, ou la condition nécessaire et suffisante du Théorème 3.4.

Exemple 3.16 *Les groupes de nombres que vous connaissez si bien regorgent d'exemples.*
(i) $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$.
(ii) $(\mathbb{Q}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.
(iii) Si H est un sous-groupe de K et si K est un sous-groupe de G, alors H est un sous-groupe de G.

Passons maintenant à des exemples plus intéressants.

Exemple 3.17 *Soit $m \in \mathbb{Z}$. Introduisons l'ensemble des multiples de m, à savoir*

$$m\mathbb{Z} = \{mn | n \in \mathbb{Z}\}.$$

Muni de la loi d'addition, $(m\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$. Vérifions ce point ensemble. D'abord l'ensemble $m\mathbb{Z}$ contient clairement l'élément neutre 0 de $(\mathbb{Z}, +)$, car $0 = m \cdot 0$, et est donc non vide. Soient x, y deux éléments de $m\mathbb{Z}$, c'est-à-dire que $x = mp$ et $y = mq$ où p et q sont deux entiers relatifs. Souvenez-vous que le symétrique pour la loi additive $+$ est l'opposé usuel. On a alors

$$x + y^{-1} = x + (-y) = mp - mq = m(p - q) \in m\mathbb{Z}.$$

On peut donc conclure par le Théorème 3.4 que $(m\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$.

L'exemple suivant est plus élaboré et introduit le concept de centre d'un groupe G, qui est le sous-groupe des éléments de G qui commutent avec tous les autres éléments de G.

Exemple 3.18 *Soit $(G, *)$ un groupe. Le centre de G est défini par*

$$Z(G) = \{h \in G \mid h * g = g * h, \ \forall g \in G\}.$$

Muni de la loi $*$, $Z(G)$ est un sous-groupe de G. Démontrez-le ! Au besoin, vous trouverez une preuve ci-dessous.

Théorème 3.5 *Soit $(G, *)$ un groupe. Son centre $(Z(G), *)$ en est un sous-groupe.*

Preuve. Montrons que $Z(G)$ est un sous-groupe de G.

L'élément neutre de G commute par définition avec tous les éléments de G et appartient par conséquent à $Z(G)$.

Soient h et k dans $Z(G)$. Montrons que $h * k \in Z(G)$. Soit g un élément quelconque de G. Comme $k \in Z(G) \subset G$, on a $k * g \in G$ et comme $h \in Z(G)$,

$$(h * k) * g = h * (k * g) = (k * g) * h = k * (g * h).$$

De même, $g * h \in G$. Comme $k \in Z(G)$ et par associativité de la loi $*$, on a

$$k * (g * h) = (g * h) * k = g * (h * k),$$

ce qui prouve que $(h * k) * g = g * (h * k)$ et donc $h * k \in Z(G)$.

Il ne reste plus qu'à montrer la stabilité du symétrique. Soit $h \in Z(G)$ et $g \in G$. On a

$$(h^{-1} * g)^{-1} = g^{-1} * h = h * g^{-1},$$

car $g^{-1} \in G$ et $h \in Z(G)$. En prenant le symétrique, on obtient que

$$h^{-1} * g = (h * g^{-1})^{-1} = g * h^{-1}.$$

Ainsi $h^{-1} \in Z(G)$ et $Z(G)$ est bien un sous-groupe de G. ■

Vous pouvez aussi vérifier que $Z(G)$ est un groupe abélien et que, si le groupe G est lui-même abélien, G et son centre $Z(G)$ sont égaux !

Si vous n'avez pas fait l'exercice proposé ci-dessus, arrêtez-vous là et retournez à vos plumes ! De manière générale, étudier des démonstrations est très formateur car cela permet entre autres de découvrir des méthodes de raisonnement, des astuces et des exemples d'utilisation de théorèmes pour obtenir de nouveaux résultats. Néanmoins, il faut prendre le temps de réfléchir par soi-même et apprendre à mettre en œuvre les techniques que vous avez vues en cours pour mieux les assimiler. Lire et étudier un cours est primordial mais loin d'être suffisant.

3.3.2 Intersection, union et produit

Après cette petite leçon de morale, poursuivons notre série d'exemples et intéressons-nous à la création de nouveaux sous-groupes par le biais de sous-groupes existants en utilisant les opérations d'ensembles. Il est légitime de se demander si les opérations usuelles sur les ensembles (intersection, union) conservent la propriété de sous-groupe.

Pour l'intersection, la réponse est toujours affirmative, comme le démontre le Théorème suivant.

Théorème 3.6 *Étant donné un groupe $(G, *)$ et H et K deux sous-groupes de G, l'intersection $H \cap K$ est un sous-groupe de G.*

Preuve. Notons e l'élément neutre de G. On a $e \in H$ et $e \in K$, donc $e \in H \cap K$, qui est donc un ensemble non-vide. Soient x et y deux éléments de $H \cap K$. Alors, x et y appartiennent à H et à K. Et comme H et K sont des sous-groupes de G, on sait que $x * y^{-1} \in H$ et $x * y^{-1} \in K$. Donc $x * y^{-1} \in H \cap K$. Cela prouve que $H \cap K$ est un sous-groupe de G par le Théorème 3.4. ∎

A votre avis, étant donné un groupe $(G, *)$, l'union, $H \cup K$, de deux sous-groupes H et K de G est-elle encore un sous-groupe de G ? Réfléchissez-y bien avant de lire la suite ! Nous tenons à vous prévenir : le cas de l'union est plus délicat que celui de l'intersection !

Exemple 3.19 *Dans le cas général, la réponse est négative ! La condition de groupe qui manquera est la stabilité. Considérons par exemple les groupes $G = (\mathbb{Z}, +)$, $H = (2\mathbb{Z}, +)$ et $K = (3\mathbb{Z}, +)$. On sait par l'Exemple 3.17 que H et K sont des sous-groupes de G. On a alors $2 \in H \cup K$ car $2 \in H$ et $3 \in H \cup K$ car $3 \in K$. Mais $2 + 3 = 5$ n'appartient ni à H ni à K (car 5 n'est ni un multiple de 2 ni un multiple de 3) ! Donc $H \cup K$ ne saurait être un groupe !*

Bien sûr, il y a des exemples où l'union de deux sous-groupes reste un sous-groupe. Prenez par exemple le cas où $K \subset H$. Alors $H \cup K = H$ est un sous-groupe de G ! En fait, l'inclusion d'un sous-groupe dans l'autre est l'unique cas où l'union de deux sous-groupes est un groupe. Essayez de démontrer ce résultat par vous-même. Nous avons déjà démontré la première implication ! Pour démontrer l'implication restante, utilisez un raisonnement par l'absurde.

Théorème 3.7 *Soit $(G, *)$ un groupe et H et K deux sous-groupes de G. L'union $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.*

Preuve. Supposons que $H \cup K$ est un sous-groupe de G et supposons par l'absurde que H n'est pas inclus dans K et que K n'est pas inclus dans H.

Cela veut dire qu'il existe un élément $h \in H$ tel que $h \notin K$ et qu'il existe un élément $k \in K$ tel que $k \notin H$. Mais alors $h \in H \cup K$ et $k \in H \cup K$, et comme $H \cup K$ est un sous-groupe de G par hypothèse, il suit que $h * k^{-1} \in H \cup K$. Distinguons alors deux cas :

(i) Si $h * k^{-1} \in K$, comme $k \in K$ et K est un groupe, $h * k^{-1} * k \in K$, et donc $h \in K$. Absurde !
(ii) Si $h * k^{-1} \in H$, comme $h \in H$ et H est un groupe, $h^{-1} * h * k^{-1} \in H$. Donc $k^{-1} \in H$ et son symétrique aussi : $k \in H$. Absurde !

Dans les deux cas, on aboutit à une contradiction, ce qui achève la preuve. ∎

Nous vous proposons un dernier exemple sur la création de sous-groupes en utilisant des opérations sur des sous-groupes existants. On considère à nouveau un groupe $(G, *)$ et deux sous-groupes H et K de G. On définit l'ensemble, noté HK, de tous les produits d'un élément quelconque de H par un élément quelconque de K :

$$HK = \{h * k \mid h \in H,\ k \in K\}.$$

La question est la suivante : quand HK est-il un sous-groupe de G ?

Théorème 3.8 *Soit $(G, *)$ un groupe et H et K deux sous-groupes de G. Alors HK est un sous-groupe de G si et seulement si $HK = KH$.*

Avant d'entamer la preuve, souvenez-vous que l'ordre dans lequel le produit est effectué est important si le groupe G n'est pas commutatif ! Ainsi, dans le cas général, $KH = \{k * h \mid h \in H,\ k \in K\}$ est différent de HK.

Preuve. Supposons que HK est un sous-groupe de G. Montrons l'égalité entre ensembles $HK = KH$. Pour cela, il suffit de démontrer la double inclusion $HK \subset KH$ et $KH \subset HK$. Soit $x \in HK$. Comme HK est un groupe, x^{-1} appartient à HK et il existe donc $h \in H$ et $k \in K$ tel que $x^{-1} = h * k$. Les règles du symétrique permettent de calculer

$$x = (x^{-1})^{-1} = k^{-1} * h^{-1}.$$

Mais comme K est un groupe, on a $k^{-1} \in K$. De même, $h^{-1} \in H$ et donc $x \in KH$. Ainsi $HK \subset KH$. Il ne nous reste plus qu'à prouver l'inclusion contraire. Attention, on ne sait pas si KH est un sous-groupe, donc la méthode diffère légèrement. Considérons $x \in KH$: il existe $h \in H$ et $k \in K$ tel que $x = k * h$. H et K étant des groupes, h et k admettent chacun un symétrique, $h^{-1} \in H$ et $k^{-1} \in K$, donc on a $y = h^{-1} * k^{-1} \in HK$. Comme HK est un groupe, y admet un symétrique dans HK, $y^{-1} = k * h = x$. Donc ce symétrique de y, x, appartient à HK, ce qui prouve que $KH \subset HK$ et *in fine* $HK = KH$.

Démontrons maintenant l'implication inverse. Pour cela, supposons que $KH = HK$. On sait que $e = e * e \in HK$. Soient x et y deux éléments de HK. Il existe h_1 et h_2 dans H, et k_1 et k_2 dans K tels que $x = h_1 * k_1$ et $y = h_2 * k_2$. On a alors

$$x * y^{-1} = h_1 * k_1 * k_2^{-1} * h_2^{-1}.$$

Or, $k_1 * k_2^{-1} \in K$ et donc $k_1 * k_2^{-1} * h_2^{-1} \in KH = HK$. Il existe donc h_3 et k_3 tels que

$$k_1 * k_2^{-1} * h_2^{-1} = h_3 * k_3.$$

Il en découle alors que

$$x * y^{-1} = h_1 * (k_1 * k_2^{-1} * h_2^{-1}) = h_1 * (h_3 * k_3) = (h_1 * h_3) * k_3,$$

qui appartient finalement à HK, car $h_1 * h_3 \in H$ et $k_3 \in K$. ■

Nous sommes conscients que ces exemples peuvent sembler compliqués au premier abord mais nous vous recommandons fortement de bien les étudier avant de progresser dans ce chapitre. Nous les trouvons particulièrement représentatifs des techniques à assimiler pour commencer à bien manipuler les structures de groupes.

3.3.3 Sous-groupe engendré par une partie

Dans cette sous-section, on se donne un groupe $(G, *)$ et A un sous-ensemble non vide de G.

Définition 3.7 *On appelle sous-groupe engendré par A l'intersection de tous les sous-groupes de G qui contiennent A. On le note*

$$\langle A \rangle = \bigcap_{H \in S_A} H$$

où S_A est l'ensemble des sous-groupes de G contenant A. Notez que l'ensemble S_A sur lequel l'intersection est prise n'est pas vide car il contient au moins l'ensemble G, et l'ensemble $\langle A \rangle$ est donc bien défini.

La démonstration du Théorème 3.6 sur le caractère de groupe de l'intersection de deux sous-groupes peut s'étendre sans problème à l'intersection d'un nombre infini de sous-groupes et $\langle A \rangle$ est donc bien un sous-groupe de G.

Le Théorème suivant donne une caractérisation du sous-groupe engendré par A :

Théorème 3.9 *Soit $(G, *)$ un groupe et A un sous-ensemble non vide de G. Alors $\langle A\rangle$ est le plus petit sous-groupe de G contenant A. De manière équivalente,*
(i) $\langle A\rangle$ est un sous-groupe de G contenant A,
(ii) si H est un autre sous-groupe de G contenant A, alors $\langle A\rangle \subset H$.

Preuve. $\langle A\rangle$ est un sous-groupe de G comme intersection de sous-groupes de G et contient A par définition, car chaque élément de S_A contient A! Si H est un autre sous-groupe de G contenant A, alors $H \in S_A$ et donc $\langle A\rangle = \bigcap_{K\in S_A} K \subset H$. ∎

Définition 3.8 *Soit $(G, *)$ un groupe et A un sous-ensemble non vide de G. On dit que A est un système générateur de G, ou encore que A engendre G, si le sous-groupe engendré par A est égal à G, c'est-à-dire si $\langle A\rangle = G$.*

On dit que A est un système générateur minimal s'il n'existe pas de sous-ensemble B de G dont le cardinal est plus petit que celui de A et tel que $\langle B\rangle = G$.

Cette notion de système générateur minimal est très importante car, dès lors que l'on a pu identifier un système générateur le plus petit possible, on acquiert une bonne connaissance de G. Cela découle du fait que l'on a une description précise de tous les éléments du sous-groupe engendré par un ensemble, laquelle description est possible grâce au théorème suivant :

Théorème 3.10 *Soit $(G, *)$ un groupe et A un sous-ensemble non vide de G. Soit $x \in G$. Alors $x \in \langle A\rangle$ si et seulement s'il existe $n \in \mathbb{N}$ et $(y_i)_{1\leq i\leq n}$ tels que pour tout $1 \leq i \leq n$, soit $y_i \in A$ soit $y_i^{-1} \in A$ et*

$$x = y_1 * \cdots * y_n.$$

Preuve. Considérons l'ensemble de tous les éléments x de G qui s'écrivent comme produit d'éléments de A ou de symétriques d'éléments de A. Notons cet ensemble H. Il peut s'écrire :

$$H=\{x\in G \mid \exists n\in\mathbb{N},\ \exists(y_i)_{1\leq i\leq n}\in A^n,\ \exists(\varepsilon_i)_{1\leq i\leq n}\in\{-1,1\}^n,\ x=y_1^{\varepsilon_i}*\cdots*y_n^{\varepsilon_n}\}.$$

Il nous faut montrer que $H = \langle A\rangle$. D'abord, H est un sous-groupe de G (vérifiez-le en utilisant par exemple le Théorème 3.4) contenant A. En effet, si $a \in A$, on peut voir que a appartient à H en prenant $n = 1$, $y_1 = a \in A$ et $\varepsilon_1 = 1$.

Il s'ensuit que $\langle A\rangle$, qui est l'intersection de tous les sous-groupes de G contenant A, est en particulier contenue dans H, ou encore $\langle A\rangle \subset H$.

Montrons maintenant l'inclusion inverse $H \subset \langle A \rangle$. Si un sous-groupe de G contient le sous-ensemble A, alors il contient aussi tous les symétriques des éléments de A et il contient donc le sous-groupe H, qui est obtenu par la composition de tels éléments. Donc, H est inclus dans l'intersection de tous les sous-groupes de G contenant A, ou encore $H \subset \langle A \rangle$. Nous avons ainsi démontré que $H = \langle A \rangle$. ■

Le Théorème 3.10 fournit une recette permettant de construire le sous-groupe engendré par une partie : c'est l'ensemble obtenu par toutes les compositions possibles de tous les éléments et symétriques d'éléments de ce sous-ensemble.

Quelques exemples de groupes engendrés par une partie s'imposent.

Exemple 3.20 *On travaille ici dans $(\mathbb{Z}, +)$. On considère le sous-groupe $\langle \{2\} \rangle$, engendré par le singleton $\{2\}$. Ce sous-groupe est le groupe des entiers relatifs pairs. Pour voir cela, il suffit d'appliquer le Théorème 3.10 avec $(G, *) = (\mathbb{Z}, +)$ et $A = \{2\}$. Alors $\langle \{2\} \rangle$ n'est autre que l'ensemble de toutes les sommes possibles de 2 et de son opposé -2, à savoir*

$$\langle \{2\} \rangle = \{x \in \mathbb{Z} \mid \exists n \in \mathbb{N},\ \exists (y_i)_{1 \leq i \leq n} \in \{2, -2\}^n,\ x = y_1 + \cdots + y_n\}.$$

Dans chacune de ces sommes, notons i le nombre de y_k valant 2. Le nombre de y_k valant -2 est alors $n - i$. Donc

$$\langle \{2\} \rangle = \{x \in \mathbb{Z} \mid \exists n \in \mathbb{N},\ \exists i \in [0, n],\ x = i * 2 + (n - i) * (-2)\}.$$

Les éléments de $\langle \{2\} \rangle$ s'écrivent donc sous la forme $2 * (2i - n)$ avec $n \in \mathbb{N}$ et $0 \leq i \leq n$. Il en découle enfin que

$$\begin{aligned} \langle \{2\} \rangle &= \{x \in \mathbb{Z} \mid \exists n \in \mathbb{N},\ \exists k \in [-n, n],\ x = k * 2\} \\ &= \{x \in \mathbb{Z} \mid \exists k \in \mathbb{N},\ x = k * 2\}, \end{aligned}$$

qui n'est autre que l'ensemble des entiers relatifs pairs.

Plusieurs parties peuvent engendrer le même groupe. En effet, le singleton $\{1\}$ engendre le groupe $(\mathbb{Z}, +)$, mais l'ensemble $\{2, 3\}$ engendre aussi ce même groupe :

$$\langle \{2, 3\} \rangle = \mathbb{Z} = \langle \{1\} \rangle.$$

Exemple 3.21 *On peut étendre l'Exemple 3.20 comme suit. Soit $m \in \mathbb{Z}$. Le groupe $(m\mathbb{Z}, +)$, introduit dans l'Exemple 3.17, est le sous-groupe de $(\mathbb{Z}, +)$ engendré par le singleton $\{m\}$. On peut aussi écrire $m\mathbb{Z} = \langle \{m\} \rangle$, ou plus simplement $m\mathbb{Z} = \langle m \rangle$.*

De manière plus générale, si $(G, +)$ un groupe additif et $x \in G$, le sous-groupe engendré par x est donné par $H = \{nx \mid n \in \mathbb{Z}\}$.

Exemple 3.22 *En notation multiplicative, le résultat de l'exemple précédent se traduit comme suit. Soit* $(G, *)$ *un groupe et* $x \in G$. *Le sous-groupe engendré par* x *est donné par* $H = \{x^n \mid n \in \mathbb{Z}\}$. *Ce groupe jouera un rôle important dans l'étude de l'ordre d'un élément d'un groupe. Cette notion étant importante et étudiée en classe prépa, vous aurez le plaisir de la découvrir dans les exercices proposés.*

L'exemple suivant requiert des connaissances de base concernant les nombres complexes. Nous ne consacrons aucun chapitre de ce livre aux nombres complexes, que vous connaissez probablement déjà. Mais nous vous recommandons fortement de relire un cours sur le sujet si l'exemple ci-dessous vous pose des difficultés.

Exemple 3.23 *Rappelons que pour deux nombres complexes* $z = x + iy$ *et* $w = u + iv$, *les lois d'addition* $+$ *et de multiplication* $\cdot$ *sont définies comme suit*

$$z + w = (x + u) + i \cdot (y + v) \qquad et \qquad z \cdot w = (xu - yv) + i \cdot (xv + yu).$$

Soit U *l'ensemble des nombres complexes de module égal à 1 :*

$$U = \{z \in \mathbb{C}, |z| = 1\}.$$

Muni de la loi de multiplication des nombres complexes, $(U, \cdot)$ *est un groupe abélien dont l'élément neutre est* 1. *Pour démontrer cela (nous vous laissons le faire vous-même), souvenez-vous que pour deux nombres complexes* z *et* w, *on a* $|z \cdot w| = |z| \times |w|$ *et* $\left|\frac{1}{z}\right| = \frac{1}{|z|}$ *si* z *est non nul.*

Soit $n \in \mathbb{N}^*$. *On considère les nombres complexes solutions de l'équation* $z^n = 1$. *Ses racines*[1] *sont* $\left(e^{\frac{2k\pi}{n}i}\right)_{1 \leq k \leq n}$ *et sont bien sûr de module 1. On appelle ces nombres les racines n-ièmes de l'unité.*

Considérons alors l'ensemble de ces racines. Muni de la loi de multiplication $\cdot$, *il forme un sous-groupe de* $(U, \cdot)$, *que l'on notera* $(U_n, \cdot)$. *En effet, l'élément neutre de* $(U, \cdot)$ *appartient à* U_n *car* $1 = e^{2i\pi} = e^{\frac{2n\pi}{n}i} \in U_n$ *et si* $e^{\frac{2k\pi}{n}i}$ *et* $e^{\frac{2l\pi}{n}i}$ *sont deux éléments de* U_n *avec* $1 \leq k \leq n$ *et* $1 \leq l \leq n$, *on a, si* $k \leq l$,

$$e^{\frac{2l\pi}{n}i} \cdot \left(e^{\frac{2k\pi}{n}i}\right)^{-1} = e^{\frac{2l\pi}{n}i} \cdot e^{-\frac{2k\pi}{n}i} = e^{\frac{2(l-k)\pi}{n}i} \in U_n$$

ou, si $l \leq k$,

$$e^{\frac{2l\pi}{n}i} \cdot \left(e^{\frac{2k\pi}{n}i}\right)^{-1} = e^{\frac{2(l-k)\pi}{n}i} = 1 \cdot e^{\frac{2(l-k)\pi}{n}i} = e^{\frac{2(n+k-l)\pi}{n}i} \in U_n.$$

1. C'est-à-dire les solutions de cette équation.

Comme on connaît la forme explicite de tous les éléments de U_n, il est immédiat de voir que $\{e^{\frac{2\pi}{n}i}\}$ est un système générateur minimal de $(U_n, \cdot)$. Autrement dit, $U_n = \langle e^{\frac{2\pi}{n}i} \rangle$.

3.4 Morphismes

Nous nous sommes intéressés dans un chapitre précédent à l'action d'applications sur des ensembles. Nous allons maintenant étudier un type particulier d'applications qui agissent sur des groupes. Ces applications envoient le produit de deux éléments du groupe de départ sur le produit des images des éléments du groupe d'arrivée et sont connues sous le nom de morphismes de groupes.

3.4.1 Définitions et premiers résultats

Définition 3.9 *Soient $(G, *)$ et $(H, \circ)$ deux groupes. Soit f une application de G dans H. On dit que f est un morphisme de groupes si et seulement si*

$$f(x * y) = f(x) \circ f(y) \qquad \text{pour tout } (x, y) \in G^2.$$

La définition suivante introduit plus de terminologie. Les cas où les ensembles de départ et d'arrivée sont identiques et/ou les cas où le morphisme est bijectif se voient réserver un intérêt particulier.

Définition 3.10 *Soient $(G, *)$ et $(H, \circ)$ deux groupes. Soit f un morphisme de G dans H.*
(i) Si $H = G$, on dit que f est un ***endomorphisme****.*
(ii) Si f est une application bijective, on dit que f est un ***isomorphisme****.*
(iii) Si $H = G$ et f est une bijection, on dit que f est un ***automorphisme****.*

Donnons à présent quelques exemples de morphismes de groupes.

Exemple 3.24 *Soit $(G, *)$ un groupe. Introduisons l'application identité $Id_G : G \to G$ définie par $Id_G(x) = x$ pour tout $x \in G$. Alors Id_G est un endomorphisme. Id_G étant aussi une bijection, c'est donc un automorphisme.*

Exemple 3.25 *Soient $a \in \mathbb{R}$ un réel fixé et f_a l'application définie par $f_a(x) = a \cdot x$. Pour tout $(x, y) \in \mathbb{R}^2$, on a*

$$f_a(x + y) = a \cdot (x + y) = a \cdot x + a \cdot y = f_a(x) + f_a(y).$$

Donc f_a est un endomorphisme du groupe $(\mathbb{R}, +)$.

Exemple 3.26 *Considérons l'application* $f : (\mathbb{R}, +) \to (\mathbb{R}^{+*}, \cdot)$ *définie par* $f(x) = e^x$*, pour tout* $x \in \mathbb{R}$*. On a, pour tout* $(x, y) \in \mathbb{R}^2$*,*

$$f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$$

et f *est donc un morphisme de groupes. Comme la fonction exponentielle est une bijection de* $\mathbb{R}$ *dans* $\mathbb{R}^{+*}$*,* f *est en fait un isomorphisme.*

Exemple 3.27 *Rappelons la notation du groupe unitaire* $(U, \cdot)$ *des nombres complexes de module unité et considérons l'application* $f : (\mathbb{R}, +) \to (U, \cdot)$ *définie par* $f(x) = e^{ix}$*, pour tout* $x \in \mathbb{R}$*. On a pour tout* $(x, y) \in \mathbb{R}^2$*,*

$$f(x+y) = e^{i(x+y)} = e^{ix} \cdot e^{iy} = f(x) \cdot f(y)$$

et f *est donc un morphisme de groupes.*

Remarquez que dans l'Exemple 3.26, l'élément neutre de $(\mathbb{R}, +)$, qui n'est autre que 0, a pour image $f(0) = e^0 = 1$, qui n'est autre que l'élément neutre de $(\mathbb{R}^{+*}, \cdot)$. Il en est de même dans l'Exemple 3.27. Ce résultat est en fait très général : l'image par un morphisme de groupes de l'élément neutre du groupe de départ est égale à l'élément neutre du groupe d'arrivée.

Dans le reste de cette sous-section, si G est un groupe, on notera e_G son élément neutre.

Théorème 3.11 *Soient* $(G, *)$ *et* $(H, \circ)$ *deux groupes et* f *un morphisme de* G *dans* H*. On a alors*

$$f(e_G) = e_H.$$

Preuve. En prenant $x = y = e_G$ dans la définition 3.9, on obtient

$$f(e_G) = f(e_G * e_G) = f(e_G) \circ f(e_G).$$

En multipliant par le symétrique de $f(e_G)$ (dans H bien sûr), on a

$$e_H = \big(f(e_G)\big)^{-1} \circ f(e_G) = \big(f(e_G)\big)^{-1} \circ f(e_G) \circ f(e_G) = e_H \circ f(e_G) = f(e_G).$$

■

On peut facilement en déduire que le symétrique de l'image d'un élément du groupe de départ est égal à l'image du symétrique de cet élément.

Corollaire 3.1 *Soient* $(G, *)$ *et* $(H, \circ)$ *deux groupes et* f *un morphisme de* G *dans* H*. On a alors*

$$\big(f(x)\big)^{-1} = f(x^{-1}) \qquad \textit{pour tout } x \in G.$$

Preuve. Soit $x \in G$. En choisissant $y = x^{-1}$, le symétrique de x dans G, puis en inversant les rôles de x et de y, on obtient

$$\begin{aligned} & f(e_G) = f(x * x^{-1}) = f(x) \circ f(x^{-1}) \\ \text{et} \qquad & f(e_G) = f(x^{-1} * x) = f(x^{-1}) \circ f(x). \end{aligned}$$

Souvenons-nous maintenant que $e_H = f(e_G)$ et donc $e_H = f(x) \circ f(x^{-1}) = f(x^{-1}) \circ f(x)$. Ceci prouve que $\big(f(x)\big)^{-1} = f(x^{-1})$. ■

Concluons cette sous-section par un exemple simple sur les isomorphismes.

Exemple 3.28 *Soient $(G, *)$ et $(H, \circ)$ deux groupes et $f : G \to H$ un isomorphisme. Comme f est une application bijective, sa bijection réciproque $f^{-1} : H \to G$ est bien définie et est en fait un isomorphisme. Pourquoi ? Comme la bijectivité de f^{-1} est déjà garantie, il vous suffit de vérifier la propriété de morphisme de groupes.*

Voici une démonstration pour les moins téméraires des lecteurs ! Ou peut-être voulez-vous uniquement vérifier votre méthodologie ? Soient x et y deux éléments de H. Montrons que $f^{-1}(x \circ y) = f^{-1}(x) * f^{-1}(y)$. Comme $f^{-1}(x)$ et $f^{-1}(y)$ sont dans G et f est un morphisme de G dans H, on a

$$f\big(f^{-1}(x) * f^{-1}(y)\big) = f\big(f^{-1}(x)\big) \circ f\big(f^{-1}(y)\big) = x \circ y.$$

En composant l'équation précédente par f^{-1} et en se souvenant que, pour tout $z \in G$, $f^{-1}(f(z)) = z$, on peut conclure que

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

Ainsi f^{-1} est bien un isomorphisme.

Que se passe-t-il maintenant lorsque l'on fait agir un morphisme de groupes sur un sous-groupe du groupe de départ ? Vous l'avez deviné, on obtient un sous-groupe du groupe d'arrivée ! De même, qu'en est-il de l'image réciproque d'un sous-groupe du groupe d'arrivée par un morphisme de groupes ? Il ne faut pas être devin : c'est un sous-groupe du groupe de départ. Bien que simples, ces résultats sont pourtant cruciaux et nous permettront d'introduire deux notions très importantes pour l'étude d'un morphisme de groupes : son image et son noyau.

3.4.2 Image et noyau d'un morphisme de groupes

Cette sous-section introduit deux sous-groupes particulièrement importants que l'on appelle image et noyau d'un morphisme de groupes. Concentrons-nous d'abord sur le cas de l'image. L'image de f fait partie d'une famille plus générale de sous-groupes de H définie dans le Théorème ci-après.

Théorème 3.12 *Soient $(G, *)$ et $(H, \circ)$ deux groupes et f un morphisme de G dans H. Soit K un sous-groupe de G. Alors $f(K)$ est un sous-groupe de H.*

Preuve. Ce type de démonstration doit être quasi-mécanique pour vous à ce stade du chapitre. Vous avez deux propriétés à vérifier. Au boulot !

Le premier point est immédiat : $e_G \in K$ et, d'après le Théorème 3.11, $e_H = f(e_G)$, donc $e_H \in f(K)$.

Le second point à démontrer est la stabilité par composition et symétrique. Soient x et y dans $f(K)$. Il existe donc deux éléments h et k dans K tels que $x = f(h)$ et $y = f(k)$. Par le Corollaire 3.1,

$$x \circ y^{-1} = f(h) \circ \big(f(k)\big)^{-1} = f(h) \circ f(k^{-1}).$$

Comme f est un morphisme, $x \circ y^{-1} = f(h * k^{-1})$. Comme K est un sous-groupe de G, $h * k^{-1} \in K$ (souvenez de la propriété caractéristique d'un sous-groupe) et donc

$$x \circ y^{-1} = f(h) \circ f(k^{-1}) = f(h * k^{-1}) \in f(K),$$

ce qui conclut la preuve. ■

Le cas où K est égal au groupe G définit l'image de f. Comme vous le verrez plus loin, ce sous-groupe joue un rôle particulier dans l'étude de la surjectivité de l'application f.

Corollaire 3.2 *Soient $(G, *)$ et $(H, \circ)$ deux groupes et f un morphisme de G dans H. Alors $f(G)$ est un sous-groupe de H, appelé image de f.*

Si le Théorème 3.12 a introduit une famille de sous-groupes de H dont fait partie l'image de f, le Théorème ci-après introduit quant à lui une famille de sous-groupes de G à laquelle appartient le noyau de f, notion qui vous sera définie juste ensuite.

Théorème 3.13 *Soient $(G, *)$ et $(H, \circ)$ deux groupes et f un morphisme de G dans H. Soit K un sous-groupe de H. Alors l'image réciproque de K par f,*

$$f^{-1}(K) = \{x \in G \mid f(x) \in K\}$$

munie de la loi de composition interne $*$, est un sous-groupe de G.

Preuve. Comme K est un sous-groupe de H, $e_H \in K$. Par le Théorème 3.11, $e_H = f(e_G)$ et donc $e_G \in f^{-1}(K)$.

Soient h et k deux éléments de $f^{-1}(K)$. Montrons que $h * k^{-1} \in f^{-1}(K)$. Pour cela, il suffit de vérifier que $h * k^{-1} \in G$ et $f(h * k^{-1}) \in K$. Le premier point est immédiat car h et k sont dans $f^{-1}(K) \subset G$ et G est un groupe. Montrons donc le second point. On a

$$f(h * k^{-1}) = f(h) \circ f(k^{-1}) = f(h) \circ \big(f(k)\big)^{-1}$$

Comme h et k sont dans $f^{-1}(K)$, on sait que $f(h) \in K$ et $f(k) \in K$. Et comme K est un sous-groupe de H, on peut conclure que $f(h) \circ \big(f(k)\big)^{-1} \in K$. D'où $h * k^{-1} \in f^{-1}(K)$, ce qu'il nous fallait démontrer. ∎

Le cas particulier où le sous-groupe K est le sous-groupe trivial de H, à savoir $(\{e_H\}, \circ)$, joue un rôle particulièrement important dans l'étude d'un morphisme de groupes. Le sous-groupe obtenu dans ce cas s'appelle le noyau de f, notion que le corollaire suivant définit de manière précise.

Corollaire 3.3 *Soient $(G, *)$ et $(H, \circ)$ deux groupes et f un morphisme de G dans H. Alors l'image réciproque du singleton élément neutre de H munie de la loi $*$, $\Big(f^{-1}(\{e_H\}), *\Big)$, est un sous-groupe de G. On le note $Ker f = f^{-1}(\{e_H\})$ et on l'appelle noyau de f.*

En d'autres termes, le noyau de f est l'ensemble de tous les éléments de G dont l'image par f est l'élément neutre de H. Muni de la loi de composition interne $*$, il forme un sous-groupe de G. La notation Ker vient du mot allemand *Kern* dont la traduction est noyau.

Exemple 3.29 *Reprenons le morphisme de l'Exemple 3.26 :*

$$f : (\mathbb{R}, +) \to (\mathbb{R}^{+*}, \cdot), x \mapsto e^x.$$

On a $Ker f = f^{-1}(\{1\}) = \{0\}$.

Exemple 3.30 *Reprenons le morphisme de l'Exemple 3.27 :*

$$f : (\mathbb{R}, +) \to (U, \cdot), x \mapsto e^{ix}.$$

L'élément neutre de $(U, \cdot)$ est à nouveau 1. Pour déterminer $Ker f$, il suffit de résoudre $e^{ix} = 1$ dans $\mathbb{R}$. Il est bien connu que les solutions de cette équation sont les multiples de 2π. Donc $Ker f = f^{-1}(\{1\}) = 2\pi\mathbb{Z}$.

Le noyau de f joue un rôle particulier dans l'étude de l'injectivité de f. Remarquez que, comme $Ker f$ est un sous-groupe de G, $Ker f$ n'est jamais vide et contient au moins e_G. Le fait que $Ker f$ soit un singleton (réduit alors à l'élément neutre e_G) est équivalent à l'injectivité de f.

Théorème 3.14 *Soient $(G, *)$ et $(H, \circ)$ deux groupes et f un morphisme de G dans H. On a alors l'équivalence entre les deux propositions suivantes :*
(i) l'application f est injective ;

(ii) le noyau de f est réduit à l'élément neutre de G : $Kerf = \{e_G\}$.

Preuve. Supposons d'abord que f soit injective. Soient $x \in Kerf$ et $y \in Kerf$. On a alors $f(x) = e_H = f(y)$. Par injectivité de f, on en déduit que $x = y$. Donc $Kerf$ contient au plus un élément. D'autre part, on sait que $e_G \in Kerf$, et donc $Kerf = \{e_G\}$.

Réciproquement, supposons que $Kerf$ soit réduit à e_G. Soient x et y deux éléments de G tels que $f(x) = f(y)$. Nous cherchons à montrer que $x = y$. Si vous ne savez pas comment vous y prendre, remarquez que cela revient à démontrer que $x * y^{-1} = e_G$. Voyez-vous maintenant ?

En utilisant le fait que f est un morphisme de groupes, nous pouvons calculer :

$$f(x * y^{-1}) = f(x) \circ f(y^{-1}) = f(x) \circ \big(f(y)\big)^{-1} = f(x) \circ \big(f(x)\big)^{-1} = e_H.$$

Donc $x * y^{-1} \in Kerf$, et donc $x * y^{-1} = e_G$, d'où $x = y$. ■

Exemple 3.31 *Nous avons montré dans l'exemple 3.30 que le morphisme $f : (\mathbb{R}, +) \to (U, \cdot)$ défini par $f(x) = e^{ix}$, pour tout $x \in \mathbb{R}$, a pour noyau $Kerf = f^{-1}(\{1\}) = 2\pi\mathbb{Z}$. $Kerf$ n'est donc pas réduit à l'élément neutre de $(\mathbb{R}, +)$, à savoir 0. Le Théorème 3.14 permet de conclure que f n'est pas injectif.*

Dans le cas de groupes finis de même cardinal, l'injectivité devient équivalente à la bijectivité. La réduction du noyau du morphisme à l'élément neutre devient alors caractéristique de la bijectivité du morphisme.

Corollaire 3.4 *Soient $(G, *)$ et $(H, \circ)$ deux groupes finis de même cardinal et f un morphisme de G dans H. Alors f est un isomorphisme si et seulement si $Kerf = \{e_G\}$.*

Les notions exposées jusqu'ici sont la base de l'algèbre générale. Consolidez ces acquis avant d'aller plus loin. Le reste de ce chapitre s'intéresse à des notions plus élaborées. On étudie notamment le groupe des automorphismes d'un groupe et on définit des structures algébriques plus complexes telles que les anneaux et les corps. Le corps des réels en est un exemple important et se voit réservé tout le chapitre suivant.

3.4.3 Groupe des automorphismes d'un groupe

Soit $(G, *)$ un groupe. On s'intéresse ici à l'ensemble des automorphismes de G (isomorphismes de G dans G). Notons cet ensemble $A(G)$.

Théorème 3.15 *Muni de la loi de composition des applications,* $\big(A(G), \circ\big)$ *est un groupe.*

Preuve. Vous connaissez maintenant parfaitement la définition d'un groupe. Nous avons trois points à vérifier. D'abord, l'identité Id_G est un élément de $A(G)$, comme souligné dans l'Exemple 3.24. C'est en fait l'élément neutre de $\big(A(G), \circ\big)$, car pour tout $f \in A(G)$, pour tout $x \in G$,

$$(f \circ Id_G)(x) = f(Id_G(x)) = f(x) = Id_G(f(x)) = (Id_G \circ f)(x).$$

Et donc $f \circ Id_G = Id_G \circ f = f$.

Deuxièmement, la loi de composition des applications $\circ$ est associative. Nous ne vous apprenons rien de nouveau ici !

Finalement, tout élément $f \in A(G)$ est inversible et son symétrique est la bijection réciproque de f. En effet, si $f \in A(G)$, alors sa bijection réciproque f^{-1} est aussi un automorphisme et $f \circ f^{-1} = f^{-1} \circ f = Id_G$. Replongez dans l'Exemple 3.28 si cela n'est pas aussi clair que de l'eau de source ! ■

Ceci achève cette section consacrée à la structure de groupe. Ne vous empressez pas d'étudier les autres structures algébriques si vous ne vous sentez pas totalement à l'aise avec les groupes. Prenez votre temps pour méditer la multitude de résultats et la variété d'exemples que nous vous avons concoctés dans cette section. Vous n'en serez que mieux armés pour attaquer l'étude des anneaux et des corps et résoudre les exercices et problèmes que nous vous proposons en fin de chapitre. Notamment, dans le problème corrigé 3.3, nous vous proposons d'étudier en profondeur un sous-groupe de ce groupe des automorphismes d'un groupe : le sous-groupe des automorphismes intérieurs. Ce serait pour vous l'occasion de vérifier votre compréhension de ce qu'est un groupe.

3.5 Anneaux

La structure d'anneau vient enrichir celle de groupe et nécessite non pas une, mais deux lois de composition internes que l'on notera $+$ et $\times$ dans le reste de cette section.

3.5.1 Structure d'anneau

Pour pouvoir définir la structure d'anneau, nous devons d'abord définir un nouvel axiome que peuvent satisfaire les lois de composition internes.

Définition 3.11 *Soit A un ensemble non vide muni de deux lois de composition internes $+$ et $\times$. On dit que la loi $\times$ est* ***distributive*** *par rapport à la loi $+$ si pour tout $(x, y, z) \in A^3$,*

$$x \times (y + z) = x \times y + x \times z \qquad \text{et} \qquad (y + z) \times x = y \times x + z \times x.$$

Ce n'est pas la première fois que vous rencontrez cette propriété : elle est satisfaite par l'addition et la multiplication usuelles dans tous les ensembles de nombres que vous connaissez, en particulier dans $(\mathbb{R}, +, \cdot)$. C'est cette propriété qui vous aide à effectuer le calcul algébrique comme vous avez l'habitude de le faire, en particulier en ce qui concerne le développement et la factorisation.

Procédons maintenant à la définition de la structure d'anneau.

Définition 3.12 *Soit $(A, +, \times)$ un ensemble non vide muni de deux lois de composition internes. $(A, +, \times)$ est un anneau si et seulement si*
(i) $(A, +)$ est un groupe commutatif,
(ii) la loi $\times$ est associative,
(iii) la loi $\times$ est distributive par rapport à la loi $+$,
(iv) il existe un élément neutre pour la loi $\times$, appelé aussi élément unité.
Si, de plus, la loi $\times$ est commutative, on dit que l'anneau $(A, +, \times)$ est commutatif.

Comme vous vous en doutez, $(\mathbb{Z}, +, \cdot)$ est un anneau commutatif. Il en est de même pour $(\mathbb{R}, +, \cdot)$.

Dans un anneau [1] $(A, +, \times)$, l'élément unité est unique et on le note 1_A ou 1 s'il n'y a pas de confusion possible.

Dans le reste de cette section, on notera 0 l'élément neutre pour la loi $+$. Dans les ensembles de nombres, vous savez que si l'on multiplie un nombre quelconque par 0, on obtient à nouveau 0. Aussi 0 est-il le seul nombre à avoir cette propriété. Nous ne vous apprenons rien de nouveau jusqu'à présent. Mais, saviez-vous que ces propriétés ne sont pas propres aux ensembles de nombres ? En fait, elles restent vraies dans tous les anneaux !

Théorème 3.16 *Soit $(A, +, \times)$ un anneau. Alors,*
(i) Pour tout $x \in A$, $x \times 0 = 0 \times x = 0$. On dit que 0 est un élément absorbant.
(ii) 0 est le seul élément absorbant de $(A, +, \times)$.

1. On parle parfois d'anneau unitaire pour souligner l'existence d'un élément unité.

Preuve. Soit $x \in A$. Comme $(A, +)$ est un groupe d'élément neutre 0, on a $x+0=x$. Aussi, comme la loi $\times$ est distributive par rapport à la loi $+$,

$$x \times x = x \times (x+0) = x \times x + x \times 0.$$

Mais $x \times x \in A$ car $\times$ est une loi de composition interne et $x \times x$ est inversible dans le groupe $(A, +)$ de symétrique $-(x \times x)$. Donc

$$0 = x \times x - (x \times x) = x \times x + x \times 0 - (x \times x) = x \times 0.$$

L'égalité $0 \times x = 0$ se démontre de manière similaire.

Démontrons le point (ii). Soient 0_1 et 0_2 deux éléments absorbants de $(A, +, \times)$. Alors $0_1 \times 0_2 = 0_2 \times 0_1 = 0_1$ et $0_2 \times 0_1 = 0_1 \times 0_2 = 0_2$. Il est alors immédiat de voir que $0_1 = 0_2$. Et comme l'élément neutre 0 de $(A, +)$ est absorbant, on peut conclure que c'est l'unique élément absorbant de l'anneau A. ■

Exemple 3.32 *Le théorème ci-dessus démontre alors des règles de calcul classiques. Soit $(x, y) \in A^2$, alors l'opposé de $x \times y$ est donné par*

$$-(x \times y) = (-x) \times y = x \times (-y).$$

En effet, en utilisant la distributivité de $\times$ par rapport à $+$, on voit que

$$x \times y + (-x) \times y = (x + (-x)) \times y = 0 \times y = 0,$$

et

$$x \times y + x \times (-y) = x \times (y + (-y)) = x \times 0 = 0.$$

Dans les ensembles de nombres, l'addition a pour élément neutre 0, et la multiplication a pour élément neutre 1. Mais tous les anneaux ne sont pas nécessairement des ensembles de nombres. Sauriez-vous de quelles lois munir $\mathbb{Z}^2$ pour en faire un anneau ?

Exemple 3.33 *Introduisons l'ensemble $\mathbb{Z}^2 = \{(x, y) \mid x \in \mathbb{Z}, y \in \mathbb{Z}\}$ muni des lois d'addition et de multiplication terme à terme : pour tous (x, y) et (u, v) dans $\mathbb{Z}^2$,*

$$(x, y) + (u, v) = (x+u, y+v) \qquad \text{et} \qquad (x, y) \times (u, v) = (x \times u, y \times v).$$

On peut facilement vérifier que $(\mathbb{Z}^2, +, \times)$ est un anneau. L'élément neutre pour la loi $+$ est $0_{\mathbb{Z}^2} = (0, 0)$ et l'élément neutre pour la loi $\times$ est $1_{\mathbb{Z}^2} = (1, 1)$.

3.5.2 Anneau intègre

Une propriété intéressante de certains anneaux est l'absence de diviseur de zéro : le produit de deux éléments de l'anneau est nul si et seulement si l'un des deux éléments est nul. Ceci est le cas par exemple dans les ensembles de nombres munis des lois d'addition et de multiplication usuelles. Mais soyez attentifs, cette propriété n'est pas forcément vraie dans toutes les structures algébriques ! Lorsqu'un anneau satisfait cette propriété, on dit que c'est un anneau intègre.

Définition 3.13 *Soit $(A, +, \times)$ un anneau commutatif. On dira que l'anneau $(A, +, \times)$ est intègre si*

$$\forall x \in A, \quad \forall y \in A, \quad xy = 0 \quad \Rightarrow \quad x = 0 \quad ou \quad y = 0.$$

Exemple 3.34 *L'anneau $\mathbb{Z}^2$ de l'exemple 3.33 n'est pas un anneau intègre. En effet, les éléments $(1, 0)$ et $(0, 1)$ de $\mathbb{Z}^2$ sont non nuls, pourtant*

$$(1, 0) \times (0, 1) = (0, 0).$$

3.5.3 Groupe des éléments inversibles d'un anneau

Soit $(A, +, \times)$ un anneau. Soit $x \in A$. On dit que x est un élément inversible s'il admet un symétrique pour la loi $\times$, c'est-à-dire

$$\exists y \in A, \quad x \times y = y \times x = 1_A.$$

Exemple 3.35 *Voici quelques exemples d'éléments inversibles et non inversibles.*

(i) L'élément neutre 1_A est un élément inversible ! Son symétrique est lui-même.

(ii) Aucun diviseur de zéro n'est inversible ! Si ce n'était pas le cas, il existerait x diviseur de 0 (ce qui implique l'existence de $z \neq 0$ tel que $z \times x = 0$), tel que x serait inversible de symétrique noté y ; alors, on aurait

$$z = z \times 1_A = z \times (x \times y) = (z \times x) \times y = 0 \times y = 0,$$

ce qui est contradictoire avec nos hypothèses : absurde !

On note A^* l'ensemble de tous les éléments inversibles de A. Lorsque l'on munit A^* de la loi $\times$, on obtient le groupe des éléments inversibles de A. Vous verrez dans l'exemple 3.36 que cette notation avec une étoile vous est déjà familière.

Théorème 3.17 *Soit $(A, +, \times)$ un anneau. Alors, $(A^*, \times)$ est un groupe.*

Preuve. D'après l'Exemple 3.35, $1_A \in A^*$. Aussi, tout élément de A^* admet un symétrique dans A^* par définition. Il ne reste plus qu'à démontrer la stabilité pour $\times$. Soient x et y deux éléments de A^*. Il existe alors x^{-1} et y^{-1} tels que

$$x \times x^{-1} = x^{-1} \times x = 1_A \qquad \text{et} \qquad y \times y^{-1} = y^{-1} \times y = 1_A.$$

On a alors

$$(x \times y) \times (y^{-1} \times x^{-1}) = x \times 1_A \times x^{-1} = x \times x^{-1} = 1_A.$$

Et de même, $(y^{-1} \times x^{-1}) \times (x \times y) = 1_A$. Donc $x \times y \in A^*$, ce qui achève la preuve. ■

Exemple 3.36 *Dans l'anneau $(\mathbb{R}, +, \times)$, le groupe des inversibles est $(\mathbb{R}^*, \times)$: tous les nombres réels non nuls sont inversibles !*

3.6 Corps

La structure de corps nécessite aussi deux lois de composition internes et vient enrichir la structure d'anneau en y ajoutant deux axiomes : l'inversibilité de tous les éléments non nuls et la commutativité de la seconde loi.

Définition 3.14 *Soit K un ensemble muni de deux lois de composition internes $+$ et $\times$. Soit K^* l'ensemble K privé de 0, l'élément neutre pour la loi $+$ dans K. On dit que $(K, +, \times)$ est un corps si*
(i) $(K, +, \times)$ est un anneau commutatif et
(ii) K^* est non vide et tous ses éléments admettent un symétrique pour la loi $\times$.

Partant de ces deux points, on voit aussi que $(K, +, \times)$ est un corps si $(K, +, \times)$ est un anneau et $(K^*, \times)$ est un groupe commutatif.

On voit aussi que dans un corps, il n'y a aucun diviseur de zéro, tous les éléments non nuls étant inversibles. Il s'ensuit qu'un corps est en particulier un anneau intègre.

Enfin, on voit aussi qu'un corps K est un anneau commutatif dont l'ensemble des éléments inversibles est K privé de l'élément neutre pour la loi $+$. Au passage, cela justifie que l'on ait gardé la même notation que celle que l'on avait introduite pour l'ensemble des éléments inversibles K^*.

Vous trouverez ci-après des exemples classiques de corps. Les premiers exemples vous sont très familiers !

Exemple 3.37 *(i) Munis des lois d'addition et de multiplication usuelles, $(\mathbb{Q},+,\times)$ et $(\mathbb{R},+,\times)$ sont des corps.*

(ii) Muni des lois d'addition et de multiplication pour les nombres complexes, $(\mathbb{C},+,\times)$ est un corps.

3.7 Exercices

Exercice 3.1 *Soit G un ensemble fini muni d'une loi de composition interne $*$ associative. On suppose que tout $a \in G$ satisfait les propriétés suivantes : pour tout $(x,y) \in G^2$,*

$$a * x = a * y \Rightarrow x = y \qquad \text{et} \qquad x * a = y * a \Rightarrow x = y.$$

(1) Montrer que $(G,*)$ est un groupe.

Voici quelques indications pour vous aider. Soit $a \in G$. Vous pouvez montrer les points suivants :

(a) Il existe un élément $e \in G$ tel que $a * e = a$.

(b) e est en fait un élément neutre.

(c) Vous saurez ensuite ce qu'il vous reste à faire pour prouver que $(G,*)$ est un groupe !

(2) Ce résultat reste-t-il vrai si G n'est pas fini ?

Exercice 3.2 *Soit G un ensemble muni d'une loi de composition interne $*$ associative tel que*

$$\exists e \in G, \forall x \in G, e * x = x \qquad \text{et} \qquad \forall x \in G, \exists y \in G, y * x = e.$$

Ces deux hypothèses peuvent se lire : $(G,*)$ admet un élément neutre à gauche e et tout élément de G possède un symétrique à gauche.

Montrer que $(G,*)$ est un groupe. Pour cela, vous pouvez d'abord montrer que :

(a) pour tout $(x,y) \in G^2$, $x * y = e \Rightarrow y * x = e$,

(b) l'élément neutre à gauche est unique,

(c) e est en fait l'élément neutre de $(G,*)$.

Conclure maintenant que $(G,*)$ est un groupe

Exercice 3.3 *Soit $(G,*)$ un groupe d'élément neutre e et tel que pour tout $x \in G$, $x^2 = e$. Montrer que $(G,*)$ est un groupe abélien.*

Exercice 3.4 *Soient $(G, *)$ un groupe et H et K deux sous-groupes de G. On suppose qu'il existe $(a, b) \in G^2$ tel que $Ha \subset Kb$ où*

$$Ha = \{h * a \mid h \in H\} \qquad \text{et} \qquad Kb = \{k * b \mid k \in K\}.$$

Montrer que H est un sous-groupe de K.

Exercice 3.5 *Soit H une partie non vide d'un groupe $(G, *)$. Montrer que H est un sous-groupe de G si et seulement si pour tout $a \in H$, $Ha = H$.*

Exercice 3.6 *Déterminer tous les morphismes surjectifs du groupe $(\mathbb{Z}, +)$.*

3.8 Problèmes corrigés

Problème 3.1 (Ordre d'un élément d'un groupe) *Un groupe est dit fini si le nombre de ses éléments est fini. Dans ce cas, on appelle ordre d'un groupe son cardinal. Soit $(G, *)$ un groupe non trivial d'élément neutre e.*

(1) Soit $x \in G$. Montrer que les assertions suivantes sont équivalentes.
(i) Le groupe $\langle x \rangle$ est fini.
(ii) Un sous-groupe fini de G contient x.
(iii) Il existe $n \in \mathbb{N}^*$ tel que $x^n = e$.
Si l'une de ces conditions est vérifiée, on dit que l'élément x est d'ordre fini. On appelle alors ordre de x l'ordre du groupe $\langle x \rangle$.

(2) Soit $x \in G$. Montrer que l'ordre de x est le plus petit entier non nul n tel que $x^n = e$.

(3) Soit $x \in G$ d'ordre d. Montrer l'équivalence suivante : un entier k satisfait $x^k = e$ si et seulement si d divise k.

(4) Montrer que si $x \in G$ est d'ordre mn alors x^m est d'ordre n.

(5) Supposons que G soit un groupe d'ordre pair. Montrer qu'il existe $x \in G$ tel que $x \neq e$ et $x^2 = e$.

(6) Supposons que G soit un groupe d'ordre impair. Montrer que $x^2 = e$ admet une unique solution, qui est donc $x = e$.

Problème 3.2 (Groupes finis et Théorème de Lagrange) *Le but de ce problème est de démontrer le résultat suivant connu sous le nom de Théorème de Lagrange. Soient $(G, *)$ un groupe d'ordre fini et H un sous-groupe de G. Alors le cardinal de H divise le cardinal de G.*

Pour cela, introduisons, pour tout $g \in G$, l'ensemble gH de tous les produits de g par un élément de H, c'est-à-dire $gH = \{g * h \mid h \in H\}$.

(1) Soit $k \in gH$. Montrer que $gH = kH$.

(2) Soient k et g deux éléments de G. Montrer que les ensembles gH et kH sont soit égaux soit disjoints.

(3) Montrer que pour tout $g \in G$, H et gH sont de même cardinal.

(4) Montrer qu'il existe $I \subset G$ tel que

$$G = \bigcup_{g \in I} gH \qquad \text{et} \qquad \forall (g,k) \in I^2,\ gH \cap kH = \emptyset.$$

(5) En déduire finalement que le cardinal de H divise le cardinal de G.

Ceci achève la démonstration du Théorème de Lagrange, mais il serait dommage d'omettre le corollaire qui suit. Là encore, G est un groupe d'ordre fini.

6) Démontrer que l'ordre de tout élément de G divise l'ordre de G.

Problème 3.3 (Automorphismes intérieurs) *Soit $(G, *)$ un groupe et a un élément de G. Introduisons l'application (appelée automorphisme intérieur de G) $I_a : G \to G$ définie par*

$$I_a(x) = a * x * a^{-1} \qquad \text{pour tout } x \in G.$$

(1) Montrer que I_a est un automorphisme de G.

(2) Montrer que la bijection réciproque d'un automorphisme intérieur de G est aussi un automorphisme intérieur de G.

(3) Soit $I(G)$ l'ensemble de tous les automorphismes intérieurs de G, c'est-à-dire $I(G) = \{I_a \mid a \in G\}$. Muni de la loi de composition des applications, vous avez montré à la question (2) que $I(G)$ est stable par inversion. Mais $\big(I(G), \circ\big)$ est-il un sous-groupe de $\big(A(G), \circ\big)$?

3.9 Solution des exercices

Solution 3.1 (de l'exercice 3.1) *(1) Montrons que $(G, *)$ est un groupe.*

(a) La technique suivante vous est familière maintenant, nous l'avons déjà utilisée à plusieurs reprises. Introduisons l'application $f : G \to G$ définie par $f(x) = a * x$ pour tout $x \in G$. Par hypothèse, f est injective. Et

comme G est fini, elle est aussi surjective. Il existe donc $e \in G$ tel que $f(e) = a$, c'est-à-dire $a * e = a$.

(b) Soit $x \in G$. Montrons que $e * x = x * e = x$. On a

$$a * (e * x) = (a * e) * x = a * x.$$

Il s'ensuit que $e * x = x$, d'après la propriété satisfaite par tout élément de G. En particulier $e * a = a$. Aussi,

$$(x * e) * a = x * (e * a) = x * a.$$

D'où $x * e = x$. Cela prouve que e est un élément neutre de $(G, *)$.

(c) Pour conclure que $(G, *)$ est un groupe, il ne reste plus qu'à démontrer que tout élément de G est inversible.
Soit $y \in G$. Introduisons l'application g_y définie de G dans G par $g_y(x) = y * x$ pour tout $x \in G$. Elle est injective par hypothèse et donc surjective car G est fini. Il existe donc $x \in G$ tel que $g_y(x) = e$, ou encore $y * x = e$. De plus,

$$(x * y) * x = x * (y * x) = x * e = x = e * x.$$

Et alors $x * y = e$ d'après la propriété de l'énoncé. Finalement $x * y = e = y * x$ et x est donc symétrique à y. Ceci achève la preuve.

(2) Non ! L'hypothèse G est fini est cruciale ici. Pour preuve, $(\mathbb{N}, +)$ n'est pas un groupe et satisfait pourtant la propriété de l'énoncé.

Solution 3.2 (de l'exercice 3.2) ***(a)*** *Soit $(x, y) \in G^2$ tel que $x * y = e$ et soit z un symétrique à gauche de x, $z * x = e$. On a alors*

$$y*x = e*y*x = (z*x)*y*x = z*(x*y)*x = z*e*x = z*(e*x) = z*x = e.$$

(b) *Soient e et f deux éléments neutres à gauche. Pour tout $x \in G$, $f * x = x$. En particulier $f * e = e$. Mais alors d'après la question précédente, on a aussi $e * f = e$. Aussi, pour tout $x \in G$, $e * x = x$ et en particulier $e * f = f$. Ainsi $e = f$.*

(c) *Montrons que e est aussi un élément neutre à droite de $(G, *)$. Soit $x \in G$ et z son symétrique à gauche. On a $z * x = e$ et donc aussi $x * z = e$ par la première question.*

$$x * e = x * (z * x) = (x * z) * x = e * x = x.$$

Donc e est élément neutre. Finalement, il est alors immédiat de voir que tout élément de x est inversible et que donc $(G, *)$ est un groupe.

Solution 3.3 (de l'exercice 3.3) *Soit $(x, y) \in G^2$. On a $(x * y)^2 = e$. Il s'ensuit que*

$$x * y * x * y = e.$$

En multipliant à droite par y et à gauche par x, on obtient

$$x * (x * y * x * y) * y = x * e * y = x * y.$$

En utilisant l'associativité de la loi $*$ et le fait que $x^2 = e = y^2$, on obtient

$$y * x = e * y * x * e = x^2 * (y * x) * y^2 = x * (x * y * x * y) * y = x * y.$$

Ceci prouve que $(G, *)$ est commutatif.

Solution 3.4 (de l'exercice 3.4) *Il suffit de montrer que $H \subset K$. Soit h un élément de H. On a $h*a \in Ha \subset Kb$. Il existe donc $k \in K$ tel que $h*a = k*b$. Et alors $h = k * b * a^{-1}$.*

Aussi, comme e est un élément de H, on a $e * a \in Kb$ et il existe donc $l \in K$ tel que $a = e * a = l * b$. D'où $b * a^{-1} = l^{-1}$. Finalement $h = k * l^{-1} \in K$ car K est un sous-groupe de G, ce qui achève la preuve.

Solution 3.5 (de l'exercice 3.5) *Supposons que H soit un sous-groupe de G. Soit $a \in H$. Soit $h \in H$. On a $h * a^{-1} \in H$ car H est un groupe et donc*

$$h = h * e = h * (a^{-1} * a) = (h * a^{-1}) * a \in Ha.$$

D'où $H \subset Ha$. Démontrons maintenant l'inclusion inverse. Soit $x \in Ha$. Il existe donc $h \in H$ tel que $x = h * a$. Mais alors $x \in H$ car a et h sont deux éléments du groupe H. Finalement $H = Ha$ pour tout $a \in H$.

Réciproquement, supposons que pour tout $a \in H$, $H = Ha$. Et montrons que H est un sous-groupe de G. Soit $(x, y) \in H^2$. Comme $y \in H$, on a $H = Hy$, et alors $x \in Hy$ et il existe $h \in H$ tel que $x = h * y$. D'où $x * y^{-1} = h \in H$ et H est bien un sous-groupe de G.

Solution 3.6 (de l'exercice 3.6) *Nous allons résoudre cet exercice en deux étapes. Nous caractériserons d'abord les morphismes du groupe $(\mathbb{Z}, +)$ puis nous nous intéresserons à ceux d'entre eux qui sont surjectifs.*

(a) *Soit f un morphisme de $(\mathbb{Z}, +)$. Montrons que $f(n) = nf(1)$ pour tout $n \in \mathbb{Z}$.*

Remarquons d'abord que $f(0) = 0$ car 0 est l'élément neutre de $(\mathbb{Z}, +)$ et f est un morphisme de ce groupe. Donc la propriété est satisfaite pour $n = 0$.

Montrons maintenant par récurrence que $f(n) = nf(1)$ pour tout $n \geq 1$. Cette propriété est trivialement vraie pour $n = 1$. Supposons-la vraie au rang n. On a alors

$$f(n+1) = f(n) + f(1) = nf(1) + f(1) = (n+1)f(1).$$

où la première égalité découle du fait que f est un morphisme de groupes. Cela achève la preuve par récurrence.

Il reste maintenant à montrer que $f(n) = nf(1)$ pour tout $n \leq -1$. Soit $n \leq -1$. On a alors $-n \geq 1$ et donc $f(-n) = -nf(1)$. Aussi

$$0 = f(0) = f(n + (-n)) = f(n) + f(-n) = f(n) - nf(1).$$

Et donc $f(n) = nf(1)$ pour tout $n \in \mathbb{Z}$. Réciproquement, ces applications sont clairement des morphismes de $(\mathbb{Z}, +)$.

***(b)** Caractérisons maintenant les morphismes surjectifs de $(\mathbb{Z}, +)$. Soit f un tel morphisme. On sait que $f(n) = nf(1)$ pour tout $n \in \mathbb{Z}$. Comme f est surjectif, pour tout $p \in \mathbb{Z}$, il existe $n \in \mathbb{Z}$ tel que $nf(1) = f(n) = p$. Et donc $f(1)$ divise p. Cela vaut pour tout $p \in \mathbb{Z}$. Les seuls entiers qui divisent tous les autres entiers sont 1 et -1. Donc, si f est un morphisme surjectif de $(\mathbb{Z}, +)$, alors $f(n) = n$ pour tout $n \in \mathbb{Z}$ ou $f(n) = -n$ pour tout $n \in \mathbb{Z}$. Réciproquement, ces deux applications sont clairement des morphismes surjectifs de $(\mathbb{Z}, +)$ et nous avons ainsi identifiés tous les morphismes surjectifs du groupe $(\mathbb{Z}, +)$.*

3.10 Solution des problèmes corrigés

Solution 3.7 (du problème 3.1) *(1) Soit $x \in G$. Pour montrer ces équivalences, nous allons démontrer que $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$.*

La première implication est immédiate car $\langle x \rangle$ est un sous-groupe de G qui contient x. Montrons alors la deuxième implication : supposons qu'un sous-groupe fini de G contient x. Appelons-le H. Comme $x \in H$, H contient aussi toutes les puissances de x, c'est-à-dire $x^n \in H$, pour tout $n \in \mathbb{Z}$. Comme H est fini, ces puissances ne sont pas deux à deux distinctes. Il existe alors $m > p$ tels que $x^m = x^p$. On en déduit que $x^{m-p} = e$. En particulier, en posant $n = m - p$, on conclut qu'il existe $n > 0$ tel que $x^n = e$.

Il ne reste plus que l'implication $(iii) \Rightarrow (i)$ à démontrer. Supposons que $x^n = e$ pour un certain $n > 0$. Soit $m \in \mathbb{Z}$. Effectuons la division euclidienne de m par n. Il existe donc $q \in \mathbb{Z}$ et $0 \leq r < n$ tels que $m = qn + r$. On a alors

$$x^m = x^{qn+r} = x^{qn} * x^r = (x^n)^q * x^r = e^q * x^r = e * x^r = x^r.$$

On en conclut que $\langle x \rangle$ *contient au plus les éléments* $\{e, x, \cdots, x^{n-1}\}$ *et est par conséquent fini. Ceci achève la preuve du premier point.*

(2) Soit $x \in G$ *d'ordre* n*. On cherche à montrer que* n *est le plus petit entier non nul tel que* $x^n = e$*. Si vous n'avez pas d'idée, pensez à introduire l'ensemble*

$$E = \{k \in \mathbb{N}^* \mid x^k = e\},$$

et montrez que n *en est le plus petit élément.*

Faisons la démonstration ensemble. Remarquons d'abord que E *est non vide (car* $n \in E$*) et comme* E *est un sous-ensemble de* $\mathbb{N}$*, il admet un plus petit élément, que l'on notera* m*. Comme* $n \in E$*,* $n \geq m$*. Montrons maintenant l'inégalité inverse* $m \geq n$*. Soit* $k \in \mathbb{Z}$*. Utilisons à nouveau la division euclidienne de* k *par* m *: on sait qu'il existe* $q \in \mathbb{Z}$ *et* $0 \leq r < m$ *tels que* $k = qm+r$*. On a* $x^k = x^{qm+r} = x^r$ *et donc* $\langle x \rangle \subset \{e, x, \cdots, x^{m-1}\}$*. L'ensemble de droite étant de cardinal inférieur ou égal à* m*, on en conclut que le cardinal de* $\langle x \rangle$*, qui n'est autre que* n*, est inférieur ou égal à* m*. D'où* $m \geq n$*. Finalement, nous avons montré que* $n = m$*.*

(3) Soit $x \in G$ *d'ordre* d*. Soit* k *tel que* $x^k = e$*. Montrons que* d *divise* k*. La technique est maintenant classique. Effectuons la division euclidienne de* k *par* d *:* $k = qd + r$ *où* $0 \leq r < d$*, et* $e = x^k = x^{qd+r} = x^r$*. Mais souvenez-vous du résultat de la question précédente. Comme* $r < d$*,* r *est forcément nul et alors* $k = qd$*. Autrement dit,* d *divise* k*. Réciproquement, si* d *divise* k*,* k *s'écrit* $k = qd$*, avec* $q \in \mathbb{Z}$*, et alors*

$$x^k = x^{qd} = (x^d)^q = e^q = e.$$

(4) Soit $x \in G$ *d'ordre* mn*. Montrons que* x^m *est d'ordre* n*. Pour cela nous allons utiliser intensivement les résultats des questions précédentes. On a* $(x^m)^n = x^{mn} = e$*. Donc* x^m *est d'ordre fini,* d*, et* d *divise* n*. Et comme* x^m *est d'ordre* d*, on a aussi* $x^{md} = (x^m)^d = e$*. Et comme* x *est d'ordre* mn*, on en déduit que* mn *divise* md*, c'est-à-dire qu'il existe* $p \in \mathbb{Z}$*, tel que* $md = pmn$*, ou encore* $d = pn$*. Donc* n *divise aussi* d*. Cela prouve que* $d = n$ *et que* x^m *est d'ordre* n*.*

(5) Supposons que G *soit un groupe d'ordre pair. Supposons par l'absurde que pour tout* $x \in G$ *tel que* $x \neq e$*, on ait* $x^2 \neq e$*. Alors, pour tout* $x \neq e$*,* x *et son symétrique* x^{-1} *sont différents. Groupons alors chaque* $x \neq e$ *avec son symétrique, cela donne l'ensemble à deux éléments* $\{x, x^{-1}\}$*. On a alors*

$$G = \bigcup_{x \neq e} \{x, x^{-1}\} \cup \{e\}.$$

Cela prouve alors que G est d'ordre impair. Ceci contredit notre hypothèse et il existe donc un élément $x \neq e$ tel que $x^2 = e$.

(6) Supposons que G soit un groupe d'ordre impair. Cet ordre est donc égal à $2n + 1$ pour un certain $n \in \mathbb{N}$. Introduisons l'application f définie de G dans G par $f(x) = x^2$, pour tout $x \in G$. Montrons que f est bijective.

Soit $x \in G$. Comme G est d'ordre $2n + 1$, on sait que $x^{2n+1} = e$. Et donc $x^{2n+2} = x$, ce qui s'écrit encore $(x^{n+1})^2 = x$, ou enfin $f(x^{n+1}) = x$. Nous avons ainsi démontré que pour tout $x \in G$, il existe $y = x^{n+1} \in G$ tel que $x = f(y)$. Ceci n'est rien d'autre que la définition de la surjectivité de f. Et comme G est fini, f est bijective. Donc il existe un unique élément $x \in G$ tel que $x^2 = f(x) = e$. Comme e satisfait clairement cette équation, e est l'unique solution de $x^2 = e$ dans un groupe d'ordre impair.

Solution 3.8 (du problème 3.2) *(1) Soit $k \in gH$. Il existe donc $h \in H$ tel que $k = g * h$. Comme H est un groupe, h est inversible et*

$$g = k * h^{-1} \qquad \text{et} \qquad k = g * h.$$

Montrons alors, par double inclusion, que $gH = kH$. Soit $f = g * l$ avec $l \in H$ un élément quelconque de gH. On a alors

$$f = g * l = (k * h^{-1}) * l = k * (h^{-1} * l) \in kH.$$

Donc $gH \subset kH$. De même, si $k * l$, avec $l \in H$, est un élément quelconque de kH, alors $k * l = (g * h) * l = g * (h * l) \in gH$. Donc $gH = kH$.

(2) Soient $k \in G$ et $g \in G$. Supposons que $gH \cap kH$ soit non vide et soit f un élément dans cette intersection. Il existe donc $(h_1, h_2) \in H^2$ tel que $f = g * h_1 = k * h_2$. Donc $k = g * h_1 * h_2^{-1} \in gH$. Mais alors, par la question précédente, $gH = kH$. Ceci prouve que les ensembles gH et kH sont soit égaux soit disjoints.

(3) Soit $g \in G$. Pour montrer que H et gH sont de même cardinal, essayez de construire une application bijective de H dans gH.

Soit l'application $f : H \to gH$ définie par $f(h) = g * h$ pour tout $h \in H$. L'application f est surjective par construction. Il ne faut donc montrer que son injectivité. Pour cela, donnons nous h_1 et h_2 dans H tels que $f(h_1) = f(h_2)$. On alors $g * h_1 = g * h_2$. Mais g est inversible et donc, en multipliant à gauche par g^{-1}, on obtient $h_1 = h_2$. Donc f est une bijection et H et gH sont de même cardinal.

(4) Comme G est d'ordre fini, il existe $(g_i)_{1\leq i\leq n}$ tel que $G = \bigcup_{i=1}^{n}\{g_i\}$. Comme $g_i = g_i * e \in g_iH$, il s'ensuit aussi que

$$G = \bigcup_{i=1}^{n} g_iH.$$

Mais d'après les questions précédentes, g_iH et g_jH sont soit égaux soit disjoints. Il existe donc un sous ensemble K de $[1, n]$ tel que $G = \bigcup_{i\in K} g_iH$ et les g_iH, pour $i \in K$, sont deux à deux disjoints. Introduisons maintenant $I = \{g_i \mid i \in K\}$. On a alors

$$G = \bigcup_{g\in I} gH \qquad et \qquad \forall(g,k) \in I^2,\ gH \cap kH = \emptyset.$$

Une démonstration plus élégante consisterait à prouver que la relation $\mathcal{R}$ définie par

$$\forall(x,y) \in G^2, \qquad x\mathcal{R}y \quad \text{si et seulement si} \quad x * y^{-1} \in H,$$

est une relation d'équivalence sur G. Il suffit ensuite de voir que les ensembles gH sont des classes d'équivalence de $\mathcal{R}$ pour déduire qu'ils forment une partition de G. C'est l'occasion rêvée d'utiliser vos acquis de la section relative aux classes d'équivalence ! A vous de jouer !

***(5)** Nous avons tous les ingrédients maintenant pour démontrer le Théorème de Lagrange. On a*

$$|G| = |\bigcup_{g\in I} gH| = \sum_{g\in I} |gH| = \sum_{g\in I} |H| = |I| \cdot |H|.$$

La deuxième égalité découle du fait que les gH sont deux à deux disjoints, la troisième est le résultat de la question (3). La dernière égalité est triviale étant donné que la quantité $|H|$ ne dépend pas de l'indice de sommation g.

Nous avons donc démontré que $|H|$ divise $|G|$, ou, dit autrement, l'ordre du sous-groupe H divise l'ordre du groupe G.

***(6)** Soit $x \in G$. Comme G est d'ordre fini et que $\langle x\rangle$ est un sous-groupe de G, le Théorème de Lagrange affirme que l'ordre de x, qui n'est autre que l'ordre du sous-groupe $\langle x\rangle$, divise l'ordre de G.*

Solution 3.9 (du problème 3.3) ***(1)** Démontrons que I_a est un endomorphisme de G. La partie endo découle du fait que pour tout $x \in G$, $I_a(x) \in G$, car $a \in G$ et G est un groupe (donc $a^{-1} \in G$ et $a * x * a^{-1} \in G$ par stabilité* *par application de la loi $*$). Montrons donc que I_a est un morphisme. Soient x et y dans G. On a*

$$\begin{aligned} I_a(x*y) &= a*(x*y)*a^{-1} = a*(x*e_G*y)*a^{-1} \\ &= a*(x*a^{-1}*a*y)*a^{-1} \\ &= (a*x*a^{-1})*(a*y*a^{-1}) \\ &= I_a(x)*I_a(y). \end{aligned}$$

Pour conclure, il ne nous reste plus qu'à prouver que I_a est une bijection. Soit $x \in KerI_a$. On a alors $I_a(x) = e_G = a*x*a^{-1}$ et donc, en multipliant à gauche par a^{-1} et à droite par a, on obtient $a^{-1}*e_G*a = x$, c'est-à-dire $e_G = x$. Donc $KerI_a = \{e_G\}$ et I_a est injective. Soit $y \in G$ et définissons $x = a^{-1}*y*a$. On a alors

$$\begin{aligned} I_a(x) &= I_a(a^{-1}*y*a) \\ &= a*(a^{-1}*y*a)*a^{-1} \\ &= (a*a^{-1})*y*(a*a^{-1}) \\ &= e_G*y*e_G = y. \end{aligned}$$

Donc I_a est surjective. Et comme I_a est aussi injective, c'est une bijection. Joint au fait que I_a est un endomorphisme de G, ceci prouve que $I_a \in A(G)$.

(2) Comme $I_a \in A(G)$ et $(A(G), \circ)$ est un groupe, on sait que I_a est inversible. De plus, son symétrique est donnée par sa bijection réciproque.

Soit $y \in G$. On a

$$\begin{aligned} y = I_a(x) &\Leftrightarrow y = a*x*a^{-1} \\ &\Leftrightarrow a^{-1}*y*a = a^{-1}*(a*x*a^{-1})*a \\ &\Leftrightarrow a^{-1}*y*a = (a^{-1}*a)*x*(a^{-1}*a) = e_G*x*e_G \\ &\Leftrightarrow a^{-1}*y*a = x. \end{aligned}$$

Ainsi, $I_a(x) = y$ équivaut à $I_a^{-1}(y) = x = a^{-1}*y*a = I_{a^{-1}}(y)$, pour tout $y \in G$. Cela prouve que I_a^{-1} est aussi un automorphisme intérieur de G et $(I_a)^{-1} = I_{a^{-1}}$.

(3) L'identité Id_G appartient à $I(G)$, car pour tout $x \in G$,

$$Id_G(x) = x = e_G*x*e_G^{-1} = I_{e_G}(x).$$

Donc $Id_G = I_{e_G} \in I(G)$. Soient I_a et I_b deux éléments de $I(G)$. Montrons que $I_a \circ (I_b)^{-1} \in I(G)$. Soit $x \in G$. D'après la réponse à la question (2),

$(I_b)^{-1} = I_{b^{-1}}$ *et donc*

$$\begin{aligned}\big(I_a \circ (I_b)^{-1}\big)(x) &= \big(I_a \circ I_{b^{-1}}\big)(x) = I_a(I_{b^{-1}}(x)) \\ &= I_a(b^{-1} * x * b) = a * (b^{-1} * x * b) * a^{-1} \\ &= (a * b^{-1}) * x * (b * a^{-1}) = (a * b^{-1}) * x * (a * b^{-1})^{-1}.\end{aligned}$$

Ainsi, $I_a \circ (I_b)^{-1} = I_{a*b^{-1}} \in I(G)$ *et* $(I(G), \circ)$ *est un sous-groupe de* $(A(G), \circ)$.

Chapitre 4

Corps des réels $\mathbb{R}$

De votre maternelle à la fin de vos études secondaires, vous avez construit plusieurs ensembles de nombres, en grossissant naturellement l'un pour obtenir l'autre.

Rappelez-vous le premier ensemble que l'on vous a enseigné, celui des entiers naturels, $\mathbb{N}$. Sachant que la différence de deux entiers naturels n'est pas forcément un entier naturel, vous avez construit l'ensemble des entiers relatifs, $\mathbb{Z}$, en ajoutant à $\mathbb{N}$ tous les opposés de ses propres éléments.

Ensuite, pour pouvoir faire des divisions, vous avez créé à partir de ces deux ensembles l'ensemble $\mathbb{D}$ des nombres décimaux, ces nombres avec une virgule et un nombre fini de chiffres après la virgule. Étant donné un nombre décimal d, il suffit de le multiplier par une puissance de 10 pour qu'il devienne entier. Prenons par exemple le nombre décimal $d = 0,2014$. On a bien $10^4 d = 2014$, qui est élément de $\mathbb{Z}$. En fait $\mathbb{D}$ n'est autre que l'ensemble

$$\mathbb{D} = \left\{ \frac{p}{10^k} \,\middle|\, k \in \mathbb{N}, p \in \mathbb{Z} \right\}.$$

On voit ainsi que le produit de deux nombres décimaux

$$\frac{p_1}{10^{k_1}} \times \frac{p_2}{10^{k_2}} = \frac{p_1 p_2}{10^{k_1+k_2}}$$

est encore décimal. Cependant, l'inverse d'un nombre décimal non nul n'est pas forcément décimal. En revanche, il sera rationnel. Souvenez-vous, l'ensemble des nombres rationnels $\mathbb{Q}$ est défini comme étant l'ensemble de tous les quotients de nombres entiers, ou plus précisément :

$$\mathbb{Q} = \left\{ \frac{p}{q} \,\middle|\, p \in \mathbb{Z}, q \in \mathbb{N}^* \right\}.$$

Notez que tous les nombres décimaux sont rationnels, mais l'inverse n'est évidemment pas vrai. Par exemple $\frac{1}{2} = 0,5$ est décimal (et aussi rationnel) mais $\frac{1}{3} = 0,333\ldots$ est rationnel mais n'est pas décimal ! Ainsi, jusqu'à présent, vous avez les inclusions d'ensembles

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{D} \subset \mathbb{Q}.$$

Compter avec ces nombres fait partie du savoir mathématique depuis plusieurs siècles avant notre ère. Mais nos ancêtres savaient aussi que les nombres rationnels ne suffisent pas pour répondre à des questions aussi simples que celle-ci : quelle est la longueur x de la diagonale d'un carré de côté de longueur 1 ? Ce problème est décrit dans la figure 4.1.

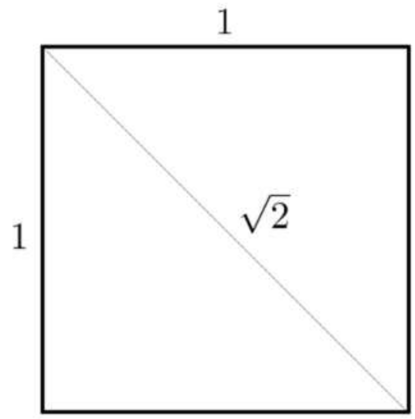

FIGURE 4.1 – La diagonale d'un carré de côté de longueur 1 vaut $\sqrt{2}$.

D'après le théorème de Pythagore, $x^2 = 1 + 1 = 2$ et donc $x = \sqrt{2}$. Nos ancêtres savaient cela. Ils savaient aussi que ce nombre $\sqrt{2}$ ne peut pas s'écrire sous la forme rationnelle $\frac{p}{q}$. Mais, bien que comprendre et même démontrer que des nombres irrationnels existent soit un grand pas, il faudra attendre plus de deux millénaires pour que l'ensemble de ces nombres ne voit complètement le jour.

En effet, la construction de l'ensemble des nombres réels, $\mathbb{R}$, est relativement récente dans l'histoire des mathématiques. Ce n'est que dans les années 1860 qu'une construction complète en est donnée. Celle-ci est basée sur les suites de Cauchy et dépasse malheureusement largement le cadre de ce cours. Gardez néanmoins en tête qu'il y a un saut énorme entre $\mathbb{Q}$ et $\mathbb{R}$. Nous admettrons donc l'existence de $\mathbb{R}$ et nous nous attarderons plutôt sur quelques-unes de ses propriétés fondamentales.

4.1 Bornes supérieures, bornes inférieures

Nous avons déjà abordé les notions de majorant / minorant, borne supérieure / borne inférieure sur un ensemble muni d'une relation d'ordre totale. Mais aviez-vous anticipé l'importance de ces notions dans la construction de $\mathbb{R}$? Rappelons d'abord brièvement ces concepts pour des parties de $\mathbb{R}$.

Définition 4.1 *Soit A une partie de $\mathbb{R}$ et $a \in \mathbb{R}$. On dit que*
(i) a est un majorant de A si pour tout $x \in A$, $x \leq a$.
(ii) A est une partie majorée si elle possède un majorant.
(iii) a est un minorant de A si pour tout $x \in A$, $x \geq a$.
(iv) A est une partie minorée si elle possède un minorant.

Notez l'utilisation de l'article indéfini *un* et non de l'article défini *le*. L'assertion *a est le majorant de A* n'a pas de sens, car il n'y a pas unicité du majorant ! En effet si a majore une partie A alors $a+2014$ majore aussi A. En revanche, si un majorant a est aussi un élément de A, on dit que a est *le* plus grand élément de A, le plus grand élément étant quant à lui unique. On le note $\max A$. De même, si un minorant a est aussi un élément de A, on dit que a est *le* plus petit élément de A et on le note $\min A$.

Lemme 4.1 *Soit A une partie de $\mathbb{R}$. Si A possède un plus grand élément, alors celui-ci est unique.*

Preuve. Raisonnons par l'absurde et supposons que A admet deux plus grands éléments a et b. Alors a est un majorant de A et, comme $b \in A$, on a $b \leq a$. Mais b est aussi un majorant de A et $a \in A$ donc $a \leq b$. Ceci prouve que $a = b$, contredisant ainsi notre hypothèse. ■

Ainsi, le plus grand élément d'une partie, lorsqu'il existe, est unique. Souvenez vous maintenant du théorème suivant sur l'existence du plus grand élément d'une partie de $\mathbb{Z}$.

Théorème 4.1 *Toute partie non vide et majorée de $\mathbb{Z}$ admet un plus grand élément et toute partie non vide et minorée de $\mathbb{Z}$ admet un plus petit élément.*

Ce résultat devient faux dans $\mathbb{R}$ et une partie de $\mathbb{R}$, même majorée, peut ne pas avoir de plus grand élément. Un exemple s'impose !

Exemple 4.1 *Soit $E = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$. E est une partie majorée de $\mathbb{R}$, 1 étant clairement un de ses majorants. Mais $1 \notin E$ et 1 n'est donc pas le plus grand élément de E. Néanmoins, c'est bien le plus petit des majorants de E. En effet on peut choisir $x < 1$ aussi proche que l'on veut de 1, ce x là ne sera pas un majorant de E car on trouvera toujours un autre réel y strictement* *plus grand que x et plus petit que 1, par exemple $x < y = x + \frac{1-x}{2} < 1$ comme vous pouvez vous en rendre compte dans la figure 4.2.*

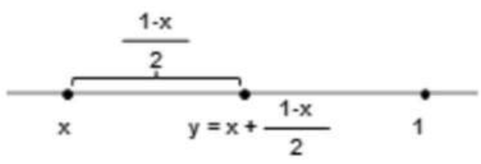

FIGURE 4.2 – Elément y entre x et 1.

On voit donc que 1 joue ici un rôle particulier, bien que E n'admette pas de plus grand élément. Pour remédier à la non-existence du plus grand élément, nous allons introduire la notion de borne supérieure.

Définition 4.2 *Soit A une partie de $\mathbb{R}$. On dit que S est la borne supérieure de A si S est un majorant de A et si*

$$\forall \varepsilon > 0, \exists a \in A, S - \varepsilon < a \leq S.$$

De même, on dit que m est la borne inférieure de A si m est un minorant de A et si

$$\forall \varepsilon > 0, \exists a \in A, m \leq a < m + \varepsilon.$$

Pour que le Théorème 4.1 devienne vrai dans $\mathbb{R}$, il suffit de remplacer *un plus grand élément* par *une borne supérieure.* Le résultat modifié se lirait :

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

Cette modification, simple en apparence, est en fait très profonde. En effet, cette propriété est à la base de la construction de $\mathbb{R}$. Cette construction est délicate et dépasse le cadre de ce cours, mais vous avez tout maintenant pour admettre et comprendre, à défaut de démontrer, l'existence de $\mathbb{R}$.

Théorème 4.2 *Il existe un ensemble, noté $\mathbb{R}$, muni de deux lois de composition interne commutatives, notées $+$ et $\times$, telles que $\times$ est distributive par rapport à $+$, et d'une relation d'ordre total sur $\mathbb{R}$, notée $\leq$, tels que*
(i) $(\mathbb{R}, +)$ est un groupe commutatif d'élément neutre 0 ;
(ii) $(\mathbb{R}, \times)$ est un groupe commutatif d'élément neutre 1 ;
(iii) toute partie non vide et majorée de $\mathbb{R}$ admet une borne supérieure.

On appellera l'assertion *(iii)* du Théorème 4.2 *propriété de la borne supérieure.* De même, toute partie non vide et minorée de $\mathbb{R}$ admet une borne inférieure. Étudions maintenant plus en détail les propriétés caractéristiques de la borne supérieure.

Théorème 4.3 *Soit A une partie de $\mathbb{R}$ admettant une borne supérieure S. Alors*
(i) S est le plus petit des majorants de A ;
(ii) S est l'unique borne supérieure de A.

Preuve. Supposons que A admette deux bornes supérieures $S' < S$. Posons $\varepsilon = S - S' > 0$. Il existe donc $a \in A$ tel que $S' = S - \varepsilon < a \leq S$. Mais cela est en contradiction avec $a \leq S'$ et A admet une unique borne supérieure. ■

Étant donnée son unicité, on notera $\sup A$ la borne supérieure d'une partie A de $\mathbb{R}$. De même, la borne inférieure de A est unique si elle existe et sera notée $\inf A$.

Vous noterez alors que si A admet un borne supérieure, alors $\sup A$ est un majorant de A et A est donc majorée. Il découle ainsi de la propriété caractéristique de $\mathbb{R}$ (c'est-à-dire la propriété de la borne supérieure) et du Théorème ci-avant qu'une partie non vide de $\mathbb{R}$ admet une borne supérieure si et seulement si elle est majorée. Et, comme vous vous en doutez aussi, une partie non vide de $\mathbb{R}$ admet une borne inférieure si et seulement si elle est minorée.

Nous avons vu qu'une partie non vide et majorée de $\mathbb{R}$ admet toujours une borne supérieure mais peut ne pas avoir de plus grand élément. Clarifions maintenant davantage le lien entre borne supérieure et maximum d'une partie de $\mathbb{R}$.

Théorème 4.4 *Soit A une partie non vide de $\mathbb{R}$.*
(i) Si A admet un plus grand élément, alors A admet une borne supérieure et $\max A = \sup A$.
(ii) Si A admet une borne supérieure $\sup A$ *qui appartient à A, alors A admet un plus grand élément et* $\sup A = \max A$.

Avant d'aller plus loin, regardons ensemble quelques exemples de parties bornées de $\mathbb{R}$ et déterminons leurs bornes supérieures et inférieures.

Exemple 4.2 *Soit $p \geq 2$ un entier naturel. Considérons l'ensemble*

$$A = \left\{ \frac{1}{p^n} \middle| n \in \mathbb{N} \right\}.$$

On a $p^n \geq 1$, donc, pour tout $a \in A$, $a \leq 1$ et 1 est un majorant de A. Il est atteint car $1 = p^0 \in A$, c'est donc le plus grand élément et la borne supérieure de A. Qu'en est-il de la borne inférieure ?

Notons d'abord que 0 *est un minorant de* A *car* $\frac{1}{p^n} > 0$ *pour tout* $n \in \mathbb{N}$. *Nous allons montrer que* 0 *est la borne inférieure de* A. *Notez alors que* A *n'a pas de plus petit élément car* $0 \notin A$. *Soit* $\varepsilon > 0$. *D'après la Définition 4.2, la question à se poser est la suivante : existe-t-il un élément* $a = \frac{1}{p^n}$ *de* A *tel que* $0 \leq \frac{1}{p^n} < \varepsilon$ *? Cela revient à chercher un entier naturel* n *tel que* $\frac{1}{\varepsilon} < p^n = e^{n\ln(p)}$ *ou encore* $\ln(\frac{1}{\varepsilon}) < n\ln(p)$. *Finalement notre* n *doit satisfaire*

$$-\frac{\ln(\varepsilon)}{\ln(p)} < n.$$

Donc, on choisit n *suffisamment grand (strictement plus grand que le plus grand entier inférieur à* $-\ln(\varepsilon)/\ln(p)$ *comme le montre la figure 4.3) pour que* $\frac{1}{p^n} < \varepsilon$ *;* 0 *est ainsi bien la borne inférieure de* A.

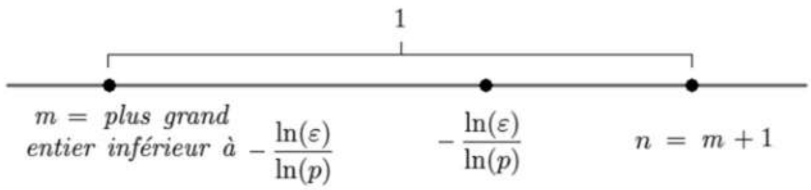

FIGURE 4.3 – Choix de n.

Exemple 4.3 *Un autre exemple très classique est celui de la partie*

$$A = \{x \in \mathbb{Q} \mid 0 \leq x < 1\}$$

qui n'est autre que l'intersection de l'intervalle $[0, 1[$ *et de* $\mathbb{Q}$. *Le plus petit élément de* A *est trivial à identifier ! C'est* 0. *Qu'en est-il de son plus grand élément ou de sa borne supérieure ? Clairement* 1 *est un majorant. Montrons que c'est la borne supérieure de* A. *La recette est encore la même. Soit* $\varepsilon > 0$. *Cherchons un rationnel* q *de* A *satisfaisant*

$$1 - \varepsilon < q < 1.$$

Trouver des réels entre $1 - \varepsilon$ *et* 1 *n'est pas difficile,* $1 - \frac{\varepsilon}{2}$ *faisant l'affaire. Mais rien ne garantit que* $1 - \frac{\varepsilon}{2} \in \mathbb{Q}$. *Pour garantir que le nombre* q *que l'on construit soit rationnel, nous allons choisir* q *de la forme* $q = 1 - \frac{1}{n} < 1$, *où* n *est tel que* $1 - \varepsilon < 1 - \frac{1}{n}$. *Pour cela, il suffit que* $\varepsilon > \frac{1}{n}$ *ou encore*

$$n > \frac{1}{\varepsilon}.$$

On a donc montré que $\sup A = 1$ *et que* $\max A$ *n'existe pas car* $1 \notin A$.

Nous avons admis que la propriété de la borne supérieure caractérise $\mathbb{R}$, c'est-à-dire que $\mathbb{R}$ vérifie cette propriété et est le seul ensemble à la vérifier. Pouvez vous alors vérifier que $\mathbb{Q}$ ne vérifie pas cette propriété ? Pour cela, essayez de trouver une partie non vide et majorée de $\mathbb{Q}$ mais qui n'admet pas de borne supérieure dans $\mathbb{Q}$.

Exemple 4.4 *Soit $A = \{a \in \mathbb{Q}, a^2 < 2\}$. A est bien une partie non vide (elle contient 0) et majorée (2 est un majorant !) de $\mathbb{Q}$. Supposons par l'absurde que A admette une borne supérieure S. Alors S vérifierait $S^2 = 2$. S étant un rationnel positif, on peut l'écrire sous la forme d'une fraction $S = \frac{p}{q}$ avec p et q des entiers naturels premiers entre eux. En d'autres termes, la fraction $\frac{p}{q}$ est irréductible. On a alors*

$$S^2 = 2 \Leftrightarrow p^2 = 2q^2 \Rightarrow 2 \textit{ divise } p^2$$

mais si p^2 est pair, alors p est aussi pair, car si $p = 2k+1$ est impair, alors $p^2 = 4k^2 + 4k + 1$ serait aussi impair. Continuons donc notre démonstration.

$$S^2 = 2 \Rightarrow 2 \textit{ divise } p \Rightarrow 4 \textit{ divise } p^2 = 2q^2 \Rightarrow 2 \textit{ divise } q^2 \Rightarrow 2 \textit{ divise } q.$$

On a ainsi prouvé que p et q sont pairs, ce qui contredit l'irréductibilité de la fraction $\frac{p}{q}$. Ainsi, A ne peut admettre de borne supérieure. Nous venons de démontrer au passage que $\sqrt{2}$ est irrationnel, c'est-à-dire que $\sqrt{2} \notin \mathbb{Q}$!

4.2 Valeur absolue

Souvenez-vous que l'ensemble $\mathbb{R}$ est muni d'une relation d'ordre total $\leq$. Plus vous maîtriserez les inégalités classiques sur $\mathbb{R}$, plus vous aurez une artillerie à votre disposition pour résoudre vos problèmes d'analyse réelle. Nous allons donc introduire dans cette section quelques inégalités super importantes ! Pour cela, définissons la fonction valeur absolue, dont vous pouvez voir le graphe sur la figure 4.4.

Définition 4.3 *Soit $x \in \mathbb{R}$. La valeur absolue de x est définie par $|x| = \max(x, -x)$, c'est-à-dire $|x| = x$ si $x \geq 0$ et $|x| = -x$ sinon.*

Ainsi, pour tout $x \in \mathbb{R}$, $|x| \geq 0$. Notez aussi que la fonction valeur absolue est paire, c'est-à-dire $|x| = |-x|$ pour tout $x \in \mathbb{R}$. Voici d'autres propriétés élémentaires de la valeur absolue que vous devez absolument maîtriser :

(i) Pour tout $x \in \mathbb{R}$, $x \leq |x|$ et $-x \leq |x|$.
(ii) Pour $a > 0$ et $x \in \mathbb{R}$, on a l'équivalence $|x| \leq a \Leftrightarrow -a \leq x \leq a$.

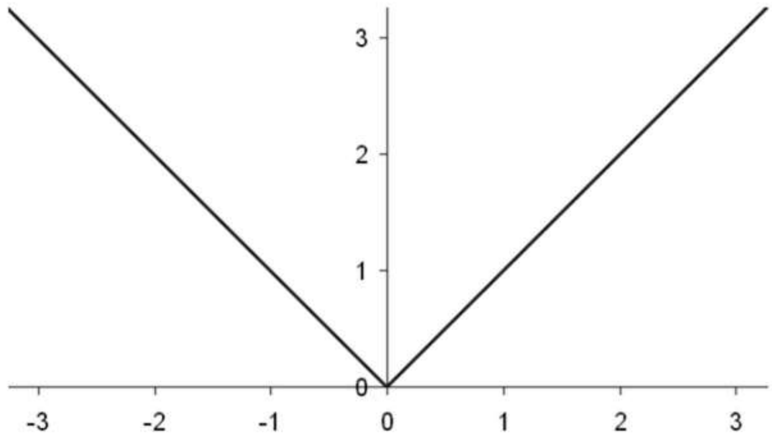

FIGURE 4.4 – Graphe de la fonction valeur absolue.

(iii) Plus généralement, pour deux réels x et y, et pour $a > 0$, on a les équivalences

$$|x - y| \leq a \Leftrightarrow -a \leq x - y \leq a \Leftrightarrow y - a \leq x \leq y + a.$$

(iv) Pour tout $x \in \mathbb{R}$, $\sqrt{x^2} = |x|$.

Le point (iv) mérite de l'attention : un piège classique est de simplifier $\sqrt{x^2}$ en x mais cela n'est vrai que si $x \geq 0$. Pour $x < 0$, $\sqrt{x^2} = |x| = -x$.

L'inégalité suivante est très utile et est connue sous le nom d'inégalité triangulaire.

Théorème 4.5 *Soient x et y deux réels. Alors*

$$|x + y| \leq |x| + |y|.$$

Preuve. Soient x et y deux réels. On a $x \leq |x|$ et $y \leq |y|$. Donc $x+y \leq |x|+|y|$. Mais on a aussi $-x \leq |x|$ et $-y \leq |y|$, donc $-(x + y) \leq |x| + |y|$. Or, $|x + y|$ est égal soit à $x + y$ soit à $-(x + y)$. Dans les deux cas, cette valeur absolue reste inférieure à $|x| + |y|$. ∎

Une vision géométrique de la valeur absolue est aussi utile. Sur la droite réelle, $|x - y|$ représente la distance entre les réels x et y comme le montre la figure 4.5.

En particulier, $|x|$ est la distance entre 0 et x comme vous pouvez le voir dans la figure 4.6.

Exemple 4.5 *Quand avons-nous l'égalité entre $|x + y|$ et $|x| + |y|$? Aucune idée ? Eh bien, celle-ci n'a lieu que si x et y sont de même signe.*

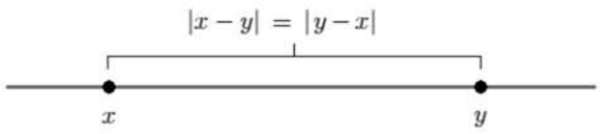

FIGURE 4.5 – La distance entre x et y est $|x-y|$.

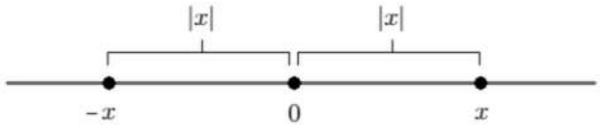

FIGURE 4.6 – $|x|$ est la distance entre x et 0.

Supposons que $|x+y| = |x| + |y|$. En élevant au carré, on obtient

$$x^2 + 2xy + y^2 = x^2 + 2|x| \cdot |y| + y^2.$$

Il en découle $xy = |x| \cdot |y| = |xy|$. Ceci implique que $xy \geq 0$, ce qui ne peut avoir lieu que si x et y sont de même signe.

L'inégalité triangulaire peut être généralisée au cas de n réels.

Théorème 4.6 *Soit $n \in \mathbb{N}^*$ et $(x_1, \cdots, x_n) \in \mathbb{R}^n$. On a*

$$|x_1 + \cdots + x_n| \leq |x_1| + \cdots + |x_n|.$$

En notation plus compacte, $\left|\sum_{i=1}^n x_i\right| \leq \sum_{i=1}^n |x_i|$.

Preuve. Un raisonnement par récurrence est la route naturelle à suivre. Pour $n = 1$, il n'y a rien à démontrer. Le cas $n = 2$ a été démontré auparavant, dans le Théorème 4.5. Supposons alors le résultat vrai pour un certain $n \geq 2$. Démontrons-le pour $n+1$. Soit $(x_1, \cdots, x_{n+1}) \in \mathbb{R}^{n+1}$. Soit $X = \sum_{i=1}^n x_i$. On a alors

$$\left|\sum_{i=1}^{n+1} x_i\right| = \left|\sum_{i=1}^{n} x_i + x_{n+1}\right| = |X + x_{n+1}| \leq |X| + |x_{n+1}|.$$

On a utilisé ici l'inégalité triangulaire classique du Théorème 4.5 (cas de deux réels X et x_{n+1}). Or l'hypothèse de récurrence implique que

$$|X| = \left|\sum_{i=1}^{n} x_i\right| \leq \sum_{i=1}^{n} |x_i|.$$

Ainsi, $|\sum_{i=1}^{n+1} x_i| \leq \sum_{i=1}^{n} |x_i| + |x_{n+1}| = \sum_{i=1}^{n+1} |x_i|$. Le résultat est donc démontré en $n+1$ et donc pour tout $n \in \mathbb{N}^*$, par récurrence. ■

L'inégalité suivante s'avérera aussi utile.

Théorème 4.7 *Soient x et y deux réels. Alors*

$$\big||x| - |y|\big| \leq |x+y| \leq |x| + |y|.$$

Preuve. Il n'y a que la première inégalité à prouver, l'autre correspondant directement à l'inégalité triangulaire. Appliquons justement l'inégalité triangulaire à $x = (x-y) + y$ et à $y = (y-x) + x$. Cela donne

$$|x| \leq |x-y| + |y| \qquad \text{et} \qquad |y| \leq |y-x| + |x|.$$

Il en découle que $|x| - |y| \leq |x-y|$ et $|y| - |x| \leq |y-x| = |x-y|$. Ceci signifie exactement que $\big||x| - |y|\big| \leq |x-y|$. ■

4.3 Partie entière

La fonction partie entière, E, est définie de $\mathbb{R}$ dans $\mathbb{Z}$ et envoie un réel x sur le plus grand entier inférieur ou égal à x.

Exemple 4.6 *Pour tout $n \in \mathbb{Z}$, $E(n) = n$. Pour tout $n \in \mathbb{Z}$ et pour tout réel x tel que $n \leq x < n+1$, on a $E(x) = n$, ainsi $E(\frac{3}{2}) = 1$ et $E(-\frac{3}{2}) = -2$. Si vous vous amusez à tracer le graphe de cette fonction, vous verrez qu'elle ressemble à un escalier, où l'on change de marche à chaque entier. Regardez le graphe de la figure 4.7.*

Les plus curieux d'entre vous peuvent continuer la lecture de cette sous-section qui prouve l'existence de cette fonction partie entière. Cela découle du caractère archimédien de $\mathbb{R}$: pour deux réels distincts $0 < a < b$, il existe toujours un multiple entier n du plus petit a, supérieur au plus grand b. La restriction $a < b$ n'est pas nécessaire, car $na < b$ est alors satisfaite avec $n = 1$.

Théorème 4.8 *L'ensemble $\mathbb{R}$ est archimédien, c'est-à-dire*

$$\forall a > 0, \quad \forall b \geq 0, \quad \exists n \in \mathbb{N}^*, \quad na > b.$$

Preuve. Soient $a > 0$ et $b \geq 0$ deux réels. Supposons par l'absurde que, pour tout $n \in \mathbb{N}^*$, $na \leq b$. L'ensemble $A = \{na \mid n \in \mathbb{N}^*\}$ est alors une partie non-vide de $\mathbb{R}$. C'est aussi une partie majorée, b étant un majorant par

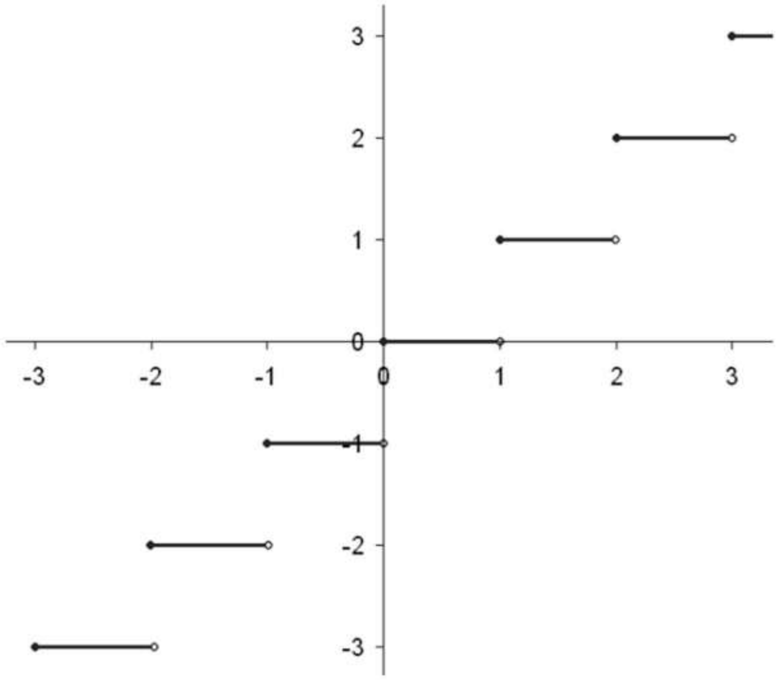

FIGURE 4.7 – Graphe de la fonction partie entière.

notre hypothèse. A admet donc une borne supérieure $\sup A$. Or, si $n \in \mathbb{N}^*$, alors $n+1 \in \mathbb{N}^*$ aussi et donc $(n+1)a \in A$. Ainsi, pour tout $n \in \mathbb{N}^*$, $(n+1)a \leq \sup A$, ou encore $na \leq \sup A - a$. Cela implique que $\sup A - a$ est un majorant de A. Mais $\sup A - a < \sup A$. Cela est en contradiction avec le fait que $\sup A$ soit le plus petit des majorants de A. Notre hypothèse est donc absurde et il existe $n \in \mathbb{N}^*$ tel que $na > b$. ∎

Remarquez l'importance de l'hypothèse $a > 0$ dans ce théorème. Le résultat devient faux si a est nul. Dans ce cas, pour tout $n \in \mathbb{N}^*$, $na = 0 \leq b$ et notre raisonnement par l'absurde ne pourra évidemment pas fonctionner ! Mais où avons-nous utilisé l'hypothèse $a > 0$ dans la preuve ci-dessus ? Vous ne voyez pas ? En fait, l'argument qui n'est plus valable est dans l'inégalité stricte $\sup A - a < \sup A$ car $\sup A - a = \sup A - 0 = \sup A$.

De cette propriété d'Archimède de $\mathbb{R}$, on démontre l'existence et l'unicité de la partie entière de tout réel x, ce qui permet de définir proprement la fonction partie entière.

Théorème 4.9 *Soit $x \in \mathbb{R}$. Il existe un unique $n \in \mathbb{Z}$ tel que $n \leq x < n+1$. Cet entier n est appelé partie entière de x et est noté $E(x)$.*

Preuve. Soit $x \in \mathbb{R}$. Clairement, si $x \in \mathbb{Z}$, le seul entier satisfaisant les inégalités du théorème est $n = x$. Supposons donc que $x \notin \mathbb{Z}$. Nous distinguons deux sous-cas : $x > 0$ et $x < 0$.

Supposons, pour commencer, que $x > 0$ et appliquons la propriété d'Archimède avec $a = 1$ et $b = x$. Il existe donc $m \in \mathbb{N}^*$ tel que $m > x$. L'ensemble

$$A = \{n \in \mathbb{N}^* \mid n > x\}$$

est alors non vide (car il contient m) et minoré (par 1). Il admet donc un plus petit élément p satisfaisant $p > x$ et $p-1 \leq x$. L'entier $n = p-1$ satisfait alors les inégalités du théorème. Nous vous laissons en exercice le cas $x < 0$.

Démontrons maintenant ensemble l'unicité. Supposons que deux entiers n et m satisfont les inégalités du théorème. Alors

$$n \leq x < n+1 \qquad \text{et} \qquad -m-1 < -x \leq -m$$

donc $n - m - 1 < 0 < n - m + 1$ ou encore $-1 < m - n < 1$. Mais comme $m - n$ est un entier et que 0 est le seul entier entre -1 et 1, on conclut que $n = m$. La fonction partie entière est donc bien définie. ■

Vous aurez l'occasion de manipuler la partie entière dans les exercices que nous vous proposons en fin de chapitre, mais vous pouvez déjà vous amuser à démontrer ces propriétés élémentaires données en guise d'exemples.

Exemple 4.7 *Soit $x \in \mathbb{R}$.*

(i) x est un entier relatif si et seulement si x et sa partie entière sont égaux.
(ii) Pour tout $n \in \mathbb{Z}$, $E(x+n) = E(x) + n$.
Ceci n'est pas vrai si l'entier n est remplacé par un réel. Ainsi pour $y \in \mathbb{R}$, $E(x+y)$ peut être différent de $E(x) + E(y)$. Par exemple,

$$E(1,7 + 1,5) = E(3,2) = 3 > E(1,7) + E(1,5) = 1 + 1 = 2.$$

(iii) Attention ! $E(nx)$ peut être différent de $nE(x)$ même si $n \in \mathbb{N}$. Par exemple,

$$E(2 * 1,5) = E(3) = 3 > 2 * E(1,5) = 2 * 1 = 2.$$

4.4 Densité

Du caractère archimédien de $\mathbb{R}$ découle aussi la propriété de densité de $\mathbb{Q}$ dans $\mathbb{R}$ qui reflète l'idée que l'on peut approcher autant que l'on veut un réel avec des nombres rationnels. Par analogie avec un usage du mot densité que vous connaissez, si nous considérons un point précis d'un territoire, plus la densité démographique du territoire en question est élevée, moins loin se trouvera l'habitant le plus proche de ce point. Si nous retournons à la densité de $\mathbb{Q}$ dans $\mathbb{R}$, on écrira de manière plus formelle :

pour tout $x \in \mathbb{R}$ et pour tout $\varepsilon > 0$, il existe $q \in \mathbb{Q}$ tel que $x - \varepsilon < q < x + \varepsilon$.

Cela revient aussi à dire qu'entre deux réels distincts quelconques $x \neq y$ il existe un rationnel $q \in \mathbb{Q}$.

Théorème 4.10 *Soient $x < y$ deux réels distincts. Il existe $q \in \mathbb{Q}$ tel que $x < q < y$.*

Preuve. Soient $x < y$ deux réels distincts. Comme $y - x > 0$, d'après la propriété d'Archimède de $\mathbb{R}$, il existe $n \in \mathbb{N}^*$ tel que $n(y - x) > 1$ (il suffit de prendre $a = y - x$ et $b = 1$ dans le Théorème 4.8). Soit p la partie entière de nx. On a alors $p \leq nx < p + 1$. Il en découle que

$$\frac{p}{n} \leq x < \frac{p+1}{n}.$$

Souvenez-vous maintenant que $n(y - x) > 1$. Donc $y > \frac{1}{n} + x \geq \frac{1}{n} + \frac{p}{n} = \frac{p+1}{n}$. Nous avons donc bien trouvé un rationnel, $\frac{p+1}{n}$, entre x et y. ∎

Pour prouver que $\mathbb{Q}$ est dense dans $\mathbb{R}$, il suffit d'appliquer ce théorème à $x - \varepsilon$ et $x + \varepsilon$. On obtient alors

$$\forall x \in \mathbb{R}, \forall \varepsilon > 0, \exists q \in \mathbb{Q}, x - \varepsilon < q < x + \varepsilon.$$

Vous pouvez facilement déduire du Théorème 4.10 que l'on peut trouver une infinité de rationnels entre deux réels $x < y$. Pour cela, donnons-nous $n \in \mathbb{N}^*$ et partitionnons l'intervalle $]x, y[$ en n sous-intervalles. Introduisons $x_i = x + i\frac{y-x}{n}$ pour tout $0 \leq i \leq n$. On a alors

$$]x, y[= \bigcup_{i=0}^{n-1}]x_i, x_{i+1}[.$$

Et comme $x_i < x_{i+1}$, il existe un rationnel q_i tel que $x \leq x_i < q_i < x_{i+1} \leq y$. Les intervalles $]x_i, x_{i+1}[$ étant deux à deux disjoints, nous avons trouvé n rationnels entre x et y. Ceci étant vrai pour tout $n \in \mathbb{N}^*$, nous avons la preuve qu'il y a une infinité de rationnels entre x et y.

Nous venons de voir qu'il y a beaucoup de rationnels dans $\mathbb{R}$, mais qu'en est-il des irrationnels ? Vous avez rencontré $\sqrt{2}$ pour le moment mais peut-être pensez-vous qu'il est difficile de construire d'autres nombres irrationnels ? Cette pensée est trompeuse, car en fait l'ensemble des irrationnels, c'est-à-dire $\mathbb{R} \backslash \mathbb{Q}$, est aussi dense dans $\mathbb{R}$.

Théorème 4.11 *Soient $x < y$ deux réels distincts. Il existe $r \notin \mathbb{Q}$ tel que $x < r < y$.*

Preuve. On sait déjà qu'il y a un rationnel entre deux réels quelconques. Translatons alors l'intervalle $]x, y[$ de $-\sqrt{2}$ et prenons un rationnel q dans $]x - \sqrt{2}, y - \sqrt{2}[$. Le réel $r = q + \sqrt{2}$ est donc, dans notre intervalle de départ, $]x, y[$. Aussi, r est irrationnel, car s'il ne l'était pas, $\sqrt{2}$ ne le serait pas non plus.

Notez au passage que l'on peut aussi démontrer qu'il y a en fait une infinité d'irrationnels entre x et y. Pour cela il vous suffit d'utiliser le même argument précédant ce théorème en remplaçant le mot rationnel par irrationnel ! ■

Il y a donc une infinité de rationnels et d'irrationnels dans $\mathbb{R}$. Néanmoins, il faut garder à l'esprit que $\mathbb{R}$ est *beaucoup plus grand* que $\mathbb{Q}$. En d'autres termes, il y a beaucoup plus d'irrationnels que de rationnels ! Ces propos manquent clairement de rigueur mais vous reviendrez sur ces points en classes préparatoires. Vous verrez notamment que $\mathbb{Q}$ peut être mis en bijection avec $\mathbb{N}$. Pour ceux qui se souviennent des notions introduites à la fin du chapitre 2, cela implique que $\mathbb{Q}$ est dénombrable, alors que $\mathbb{R}$ est indénombrable. Nous ne vous en disons pas plus pour le moment !

L'importance de cette notion de densité de $\mathbb{Q}$ dans $\mathbb{R}$ découle du fait qu'elle implique que tout réel est limite d'une suite de rationnels. Cela vous permettra souvent d'étendre des résultats vrais sur $\mathbb{Q}$ à $\mathbb{R}$ tout entier. N'ayant toujours pas introduit la notion de limite d'une suite, nous n'esquissons que brièvement ce résultat. Nous vous recommandons néanmoins de réviser votre cours de Terminale sur les suites avant d'approfondir la notion de densité. Cette révision vous sera aussi utile pour poursuivre l'étude de cet ouvrage, le prochain chapitre portant sur les suites réelles.

Théorème 4.12 *Tout réel est limite d'une suite de rationnels.*

Preuve. Soient x un réel et n un entier naturel fixés. En appliquant le Théorème 4.10 avec x et $y = x + \frac{1}{n+1}$, on sait qu'il existe un rationnel r_n tel que $x < r_n < x + \frac{1}{n+1}$. Ceci définit bien une suite de rationnels $(r_n)_{n \in \mathbb{N}}$ qui converge vers x d'après le Théorème des gendarmes [1].

Il est très utile de remarquer que cette suite de rationnels $(r_n)_{n \in \mathbb{N}}$ approche x par le haut, r_n étant toujours supérieur à x. Nous pouvons tout aussi bien approcher x par le bas par une suite de rationnels et construire ainsi pour

1. Vous pouvez trouver ce théorème dans le chapitre sur les suites réelles : il s'agit du Théorème 5.14.

chaque $n \in \mathbb{N}$, un rationnel s_n tel que $x - \frac{1}{n+1} < s_n < x$. Le Théorème des gendarmes implique aussi que s_n converge vers x. ■

Cette notion de densité et les résultats ci-avant ne sont pas propres à $\mathbb{Q}$. En effet, on peut se demander si une partie quelconque de $\mathbb{R}$ est dense dans $\mathbb{R}$ au sens de la définition suivante :

Définition 4.4 *Soit A une partie de $\mathbb{R}$. On dit que A est dense dans $\mathbb{R}$ si et seulement si*

$$\forall x \in \mathbb{R}, \forall \varepsilon > 0, \exists a \in A, x - \varepsilon < a < x + \varepsilon.$$

Dit autrement, A est dense dans $\mathbb{R}$ si et seulement si $]x - \varepsilon, x + \varepsilon[\cap A$ est non vide pour tous $x \in \mathbb{R}$ et $\varepsilon > 0$.

Cette définition implique clairement qu'une partie A de $\mathbb{R}$ est dense dans $\mathbb{R}$ si et seulement si, pour tous réels $x < y$,

$$]x, y[\cap A \neq \emptyset.$$

Comme on l'a fait lors de l'étude de la densité de $\mathbb{Q}$ dans $\mathbb{R}$, on peut obtenir de cette caractérisation epsilonesque de la densité d'une partie de $\mathbb{R}$ la caractérisation séquentielle suivante :

Théorème 4.13 *Soit A une partie de $\mathbb{R}$. A est dense dans $\mathbb{R}$ si et seulement si tout réel x est limite d'une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de A.*

4.5 Exercices

Exercice 4.1 *Soient A et B deux parties non vides et majorées de $\mathbb{R}$. Montrer que*
1) si $A \subset B$ alors $\sup A \leq \sup B$;
2) $\sup(A \cup B) = \max(\sup A, \sup B)$.

Exercice 4.2 *Trouver les bornes supérieures et inférieures des parties de $\mathbb{R}$ qui suivent :*
(i) $E = \left\{1 - \frac{1}{n} \middle| n \in \mathbb{N}^*\right\}$,
(ii) $F = \left\{\frac{(-1)^n n}{n+1} \middle| n \in \mathbb{N}\right\}$.

Exercice 4.3 *Soit E une partie non vide et majorée de $\mathbb{R}$. Supposons que E n'admet pas de maximum et notons S sa borne supérieure. Montrer que pour tout $\varepsilon > 0$, l'intersection $E\cap]S - \varepsilon, S[$ contient une infinité d'éléments.*

Exercice 4.4 *Montrer que $\sqrt{2}$, $\sqrt{3}$ et $\frac{\ln 3}{\ln 2}$ sont irrationnels.*

Exercice 4.5 *Cet exercice simple a pour but de vous faire manipuler quelques propriétés de la fonction partie entière. À vous de jouer!*
(i) $\forall x \in \mathbb{R}$, $\forall n \in \mathbb{N}^*$, $E\left(\frac{E(nx)}{n}\right) = E(x)$.
(ii) Si $x \in \mathbb{R}$, *que vaut* $E(x) + E(-x)$ *?*

4.6 Problèmes corrigés

Problème 4.1 (Sous-groupes additifs de $\mathbb{R}$ et nombres irrationnels) *Ce problème donne une caractérisation des sous-groupes additifs de* $\mathbb{R}$ *et quelques caractérisations de l'irrationalité d'un réel.*

1) Montrer le théorème suivant :

Théorème 4.14 *Soit* G *un sous-groupe de* $(\mathbb{R}, +)$. *Soit* α *la borne inférieure de* $G \cap]0, +\infty[$.
(i) Si $\alpha \neq 0$, *alors* $G = \alpha\mathbb{Z}$.
(ii) Si $\alpha = 0$, *alors* G *est dense dans* $\mathbb{R}$.

2) Ce résultat a plusieurs corollaires très intéressants dont le suivant qui caractérise l'irrationalité d'un réel et que l'on vous demande de démontrer :

Corollaire 4.1 *Un réel* θ *est irrationnel si et seulement si l'ensemble*

$$H_\theta = \{p + \theta q \mid (p, q) \in \mathbb{Z} \times \mathbb{Z}\}$$

est dense dans $\mathbb{R}$.

3) Ce corollaire mène à son tour à une autre caractérisation de l'irrationalité d'un réel θ. *En utilisant ce corollaire, prouver le théorème suivant :*

Théorème 4.15 *Soit* θ *un réel donné. Montrer que* θ *est irrationnel si et seulement s'il existe deux suites d'entiers relatifs* $(p_n)_{n\in\mathbb{N}}$ *et* $(q_n)_{n\in\mathbb{N}}$ *telles que*
(i) pour tout $n \in \mathbb{N}$, $p_n - \theta q_n \neq 0$,
(ii) la suite $(p_n - \theta q_n)_{n\in\mathbb{N}}$ *converge vers* 0.

Problème 4.2 (Endomorphismes monotones de $\mathbb{R}$) *1) Soit* f *un endomorphisme de* $(\mathbb{R}, +)$. *Supposons que* f *soit monotone. Montrer qu'il existe* $a \in \mathbb{R}$ *tel que pour tout* $x \in \mathbb{R}$, $f(x) = ax$.

2) En déduire que si g *est une application monotone de* $\mathbb{R}^{+*}$ *dans lui-même telle que*

$$\forall x > 0, \forall y > 0, g(xy) = g(x)g(y),$$

alors g *est une fonction puissance : il existe* $a \in \mathbb{R}$ *tel que pour tout* $x \in \mathbb{R}^{+*}$, $g(x) = x^a$.

4.7 Solution des exercices

Solution 4.1 (de l'exercice 4.1) *1) Soit $x \in A$. Comme $A \subset B$, on a $x \in B$ et par définition de la borne supérieure, $x \leq \sup B$. Ceci vaut pour tout $x \in A$, donc $\sup B$ est un majorant de A. Comme $\sup A$ est le plus petit des majorants de A, il en résulte que $\sup A \leq \sup B$.*

Notez que si $A \subset B$ alors on a aussi $\inf B \leq \inf A$. En effet, pour tout $x \in A$, on a $x \in B$ et $x \geq \inf B$, ce qui implique que $\inf B$ est un minorant de A. Enfin, $\inf B \leq \inf A$, $\inf A$ étant le plus grand des minorants de A.

2) Soit $x \in A \cup B$.
(i) Si $x \in A$, alors $x \leq \sup A \leq \max(\sup A, \sup B)$.
(ii) Sinon, $x \in B$ et alors $x \leq \sup B \leq \max(\sup A, \sup B)$.
Il en découle que $\sup(A \cup B) \leq \max(\sup A, \sup B)$.

Montrons maintenant l'inégalité inverse. On sait que $A \subset A \cup B$ et $B \subset A \cup B$. Par la question précédente, on a alors

$$\sup A \leq \sup(A \cup B) \qquad \textit{et} \qquad \sup B \leq \sup(A \cup B).$$

Donc $\max(\sup A, \sup B) \leq \sup(A \cup B)$. L'égalité demandée en résulte.

Solution 4.2 (de l'exercice 4.2) *(i) Remarquez bien d'abord que, pour tout $n \geq 1$, $1 - \frac{1}{n} \geq 0$ donc 0 est un minorant de E. Aussi, en prenant $n = 1$, on voit que $0 = 1 - \frac{1}{1} \in E$. Donc 0 est le minimum de E.*

Aussi, il est immédiat de voir que tous les éléments de E sont majorés par 1. L'ensemble E admet donc une borne supérieure. Montrons que 1 est précisément la borne supérieure de E. Soit $\varepsilon > 0$. Montrons qu'il existe $x = 1 - \frac{1}{n} \in E$ tel que $1 - \varepsilon < x < 1$. Pour cela il suffit de choisir n tel que

$$1 - \varepsilon < 1 - \frac{1}{n}$$

ou encore $\varepsilon > \frac{1}{n}$, c'est-à-dire $n > \frac{1}{\varepsilon}$. Il suffit donc de prendre $n = E(\frac{1}{\varepsilon}) + 1$ où $E(\frac{1}{\varepsilon})$ est la partie entière de $\frac{1}{\varepsilon}$. Ceci prouve que $\sup E = 1$, mais comme $1 \notin E$, car pour tout $n \geq 1$ $1 - \frac{1}{n} < 1$, E n'admet pas de maximum.

(ii) Déterminons maintenant les bornes supérieures et inférieures de

$$F = \left\{ \frac{(-1)^n n}{n+1} \middle| n \in \mathbb{N} \right\}.$$

Soit $x = \frac{(-1)^n n}{n+1} \in F$. Alors

$$x = (-1)^n \frac{n+1-1}{n+1} = (-1)^n \left(1 - \frac{1}{n+1}\right) = (-1)^n + \frac{(-1)^n}{n+1}.$$

L'ensemble F peut donc être vu comme l'union des sous-ensembles

$$F_p = \left\{ 1 + \frac{1}{2k+1} \middle| k \in \mathbb{N} \right\} \qquad et \qquad F_i = \left\{ -1 - \frac{1}{2k+2} \middle| k \in \mathbb{N} \right\},$$

où F_p représente les éléments de F pour n pair et F_i représente les éléments de F pour n impair. Pour tout $x \in F_p$, $x \leq 2$ et $2 = 1 + \frac{1}{2\times 0+1}$ est atteint en $k = 0$. Aussi, pour tout $x \in F_i$, $x < -1 < 2$. Ainsi 2 est le maximum de F.

Notons maintenant que F_p est minoré par 0 et donc aussi par tout réel négatif. Soit $x \in F_i$. Il existe alors $k \in \mathbb{N}$ tel que $x = -1 - \frac{1}{2k+2} \geq -\frac{3}{2}$. L'égalité ayant lieu si $k = 0$, on obtient que $\min F = \min F_i = -\frac{3}{2}$.

Solution 4.3 (de l'exercice 4.3) *Soit $\varepsilon > 0$. Comme S est la borne supérieure de E, il existe $x_0 \in E$ tel que $S - \varepsilon < x_0 \leq S$. Mais, comme $S \notin E$, x_0 ne peut être égal à S et l'inégalité large est en fait stricte :*

$$S - \varepsilon < x_0 < S.$$

En utilisant encore le fait que S est la borne supérieure de E avec $S \notin E$ et en choisissant maintenant $\varepsilon_1 = S - x_0 > 0$, on déduit qu'il existe $x_1 \in E$ tel que

$$x_0 = S - (S - x_0) = S - \varepsilon_1 < x_1 < S.$$

Par récurrence, on peut construire une suite strictement croissante $(x_n)_{n\geq 0}$ dans l'intervalle $]S - \varepsilon_0, S[$. En effet, supposons construits les n premiers termes de la suite et choisissons $\varepsilon_{n+1} = S - x_n > 0$. Il existe alors $x_{n+1} \in E$ tel que

$$x_n = S - (S - x_n) = S - \varepsilon_{n+1} < x_{n+1} < S.$$

Ceci démontre qu'il y a une infinité d'éléments de E dans l'intervalle $]S-\varepsilon, S[$ dès que $S \notin E$.

Remarquez l'importance de l'hypothèse $S \notin E$ dans cet exercice. Le résultat devient en fait faux si la borne supérieure est un maximum. Prenons par exemple l'ensemble $E = \{1\}$. Cet ensemble est non vide et majoré ; sa borne supérieure est 1 et elle appartient clairement à E. Mais E étant un singleton, dans tous les intervalles de la forme $]1 - \varepsilon, 1]$, il n'y aura jamais que 1 comme élément de E, et dans l'intervalle ouvert $]1 - \varepsilon, 1[$, il n'y a aucun élément de E. Soyez donc attentifs à toutes les hypothèses de vos théorèmes, elles sont toujours là pour une bonne raison !

Solution 4.4 (de l'exercice 4.4) *Nous avons déjà montré, dans le cadre de l'Exemple 4.4, que $\sqrt{2}$ est irrationnel. Montrons maintenant que $\sqrt{3}$ est irrationnel. Supposons par l'absurde que $\sqrt{3} \in \mathbb{Q}$. Il s'écrit donc sous la forme* *d'une fraction irréductible* $\frac{p}{q}$

$$\sqrt{3} = \frac{p}{q} \qquad \text{où} \qquad q \in \mathbb{N}^* \qquad \text{et} \qquad p \in \mathbb{N}.$$

En élevant au carré, on obtient $3q^2 = p^2$. *Donc* 3 *divise* p^2. *Par conséquent,* 3 *divise aussi* p. *En effet, si* 3 *ne divisait pas* p, *alors* p *s'écrirait*
(i) soit sous la forme $3k+1$ *et dans ce cas* $p^2 = 9k^2+6k+1 = 3(3k^2+2k)+1$ *ne serait pas divisible par* 3,
(ii) soit sous la forme $3k+2$ *et dans ce cas* $p^2 = 9k^2+12k+4 = 3(3k^2+4k+1)+1$ *ne serait pas divisible par* 3.
Il s'ensuit que $p = 3k$ *pour un certain* $k \in \mathbb{N}$. *Alors*

$$3q^2 = p^2 = (3k)^2 = 9k^2.$$

En simplifiant par 3, *on a* $q^2 = 3k^2$ *et donc* 3 *divise* q^2. *Par le même raisonnement que celui appliqué à* p, *on en déduit que* 3 *divise également* q. *Ainsi, on a prouvé que* 3 *est un diviseur commun à* p *et à* q. *Cela vient en contradiction avec le fait que la fraction* $\frac{p}{q}$ *est irréductible et démontre que* $\sqrt{3} \notin \mathbb{Q}$.

Qu'en est-il de $\frac{\ln 3}{\ln 2}$ *? La démarche est toujours la même. Si c'était un nombre rationnel, il s'écrirait sous la forme d'une fraction irréductible* $\frac{p}{q}$, *avec* $q \in \mathbb{N}^*$ *et* $p \in \mathbb{N}$. *Et donc* $q \ln 3 = p \ln 2$. *En utilisant l'exponentielle, on obtient*

$$3^q = e^{q \ln 3} = e^{p \ln 2} = 2^p.$$

Si $p \geq 1$, *l'égalité ci-dessus impliquerait que* 2 *divise* 3^q *et donc* 2 *divise* 3 *(car nous avons imposé à* q *d'être un entier strictement positif), ce qui est absurde ! Donc* $p = 0$ *et alors* $q \ln 3 = p \ln 2 = 0$. *Donc* q *est aussi nul, ce qui contredit notre hypothèse* $q \in \mathbb{N}^*$. *Ce raisonnement par l'absurde prouve que* $\frac{\ln 3}{\ln 2} \notin \mathbb{Q}$.

Solution 4.5 (de l'exercice 4.5) *(i) Soient* $x \in \mathbb{R}$ *et* $n \in \mathbb{N}^*$. *On sait que* $E(x) \leq x < E(x)+1$, *donc*

$$nE(x) \leq nx < nE(x) + n.$$

Mais aussi $E(nx) \leq nx$, *donc*

$$E(nx) \leq nx < nE(x) + n.$$

Il en découle que

$$\frac{E(nx)}{n} \leq x < E(x) + 1.$$

D'autre part, comme $nE(x)$ est un entier plus petit que nx et comme $E(nx)$ est le plus grand entier plus petit que nx, on peut affirmer que

$$nE(x) \leq E(nx).$$

Et donc $E(x) \leq \frac{E(nx)}{n}$. Finalement, nous avons montré que

$$E(x) \leq \frac{E(nx)}{n} < E(x) + 1.$$

Comme $E\Big(\frac{E(nx)}{n}\Big)$ est l'unique entier p tel que $p \leq \frac{E(nx)}{n} < p+1$ et comme $E(x)$ est un entier satisfaisant ces inégalités, on peut conclure que $E\Big(\frac{E(nx)}{n}\Big) = E(x)$.

(ii) *Soit $x \in \mathbb{R}$. Si $x \in \mathbb{Z}$, alors $E(x) = x$ et $E(-x) = -x$. Donc*

$$\forall x \in \mathbb{Z}, \quad E(x) + E(-x) = 0.$$

Supposons maintenant que $x \in \mathbb{R}\backslash\mathbb{Z}$. On sait que $E(x) \leq x < E(x)+1$. Mais comme x n'est pas un entier, la première inégalité est en fait stricte. Il est alors facile d'obtenir

$$x-1 < E(x) < x < E(x)+1 \qquad \textit{et} \qquad -x-1 < E(-x) < -x < E(-x)+1.$$

En sommant terme à terme, on obtient

$$-2 < E(x) + E(-x) < 0.$$

Comme $E(x) + E(-x)$ est lui-même un entier et que le seul entier entre -2 et 0 est -1, on conclut que $E(x) + E(-x) = -1$.

4.8 Solution des problèmes corrigés

Solution 4.6 (du problème 4.1) *1) Démontrons d'abord le théorème 4.14.*

Nous allons démontrer l'égalité entre les deux ensembles G et $\alpha\mathbb{Z}$ par double inclusion. L'ensemble $G \cap \mathbb{R}^{+*}$ jouera un rôle fondamental dans cette démonstration. Le cas où G est réduit à l'élément neutre, $G = \{0\}$, ne présente aucun intérêt car dans ce cas G s'écrit trivialement sous la forme $0\mathbb{Z}$.

Supposons donc que G n'est pas réduit à 0. Remarquons que, dans ce cas, l'ensemble $G \cap \mathbb{R}^{+*}$ est non vide et minoré par 0. Il admet donc une borne inférieure. Soit $\alpha = \inf G \cap]0, +\infty[$ cette borne inférieure.

1-a) *Supposons que α est non nul. Dans ce cas, $\alpha > 0$. Par définition de la borne inférieure, on sait qu'il existe une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de $G\cap]0,+\infty[$ qui converge vers α. Nous reviendrons dans le chapitre suivant sur la convergence de suites réelles. Cependant, vous savez déjà que la suite (x_n) converge vers α si, pour toute erreur $\varepsilon > 0$, il existe un rang N suffisamment grand à partir duquel tous les termes de la suite x_n sont proches de α à ε près. Plus rigoureusement,*

$$\forall\varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N |x_n - \alpha| \leq \varepsilon.$$

En choisissant $\varepsilon = \frac{\alpha}{2}$ qui est strictement positif par hypothèse, on sait qu'il existe $N \in \mathbb{N}$ tel que, pour tout $n \geq N$, $|x_n - \alpha| \leq \frac{\alpha}{2}$. Il en découle que

$$\frac{\alpha}{2} \leq x_n \leq \frac{3\alpha}{2}.$$

Mais, comme $x_n \in G$, on peut raffiner l'encadrement :

$$\alpha \leq x_n \leq \frac{3\alpha}{2}.$$

Soit $n \geq N$ et $p \geq N$. Pour clarifier les idées, supposons que $x_n \leq x_p$. On a alors

$$0 \leq x_p - x_n \leq \frac{\alpha}{2} < \alpha.$$

Or, comme x_p et x_n sont deux éléments du groupe G, $x_p - x_n \in G$. Mais, comme α est la borne inférieure de $G\cap]0,+\infty[$, cela n'est possible que si $x_p = x_n$. Cela vaut pour tout $n \geq N$ et tout $p \geq N$. On a donc démontré que la suite $(x_n)_{n\in\mathbb{N}}$ est stationnaire à partir d'un certain rang. Comme elle converge vers α, alors $x_n = \alpha$ à partir d'un certain rang et donc $\alpha \in G$. Il en découle alors que, pour tout $n \in \mathbb{Z}$, $n\alpha \in G$ et donc

$$\alpha\mathbb{Z} \subset G.$$

1-b) *Montrons maintenant l'inclusion réciproque. Soit $x \in G$. Souvenez-vous que $\alpha \neq 0$. On peut donc définir n la partie entière de $\frac{x}{\alpha}$. On a alors $n \leq \frac{x}{\alpha} < n+1$. Donc*

$$n\alpha \leq x < (n+1)\alpha.$$

Mais $n\alpha \in \alpha\mathbb{Z} \subset G$ et G est un groupe, donc $x - n\alpha \in G$ et

$$0 \leq x - n\alpha < \alpha.$$

Cela ne peut avoir lieu que si $x - n\alpha = 0$ étant donné que α est la borne inférieure de $G\cap]0,+\infty[$. Donc $x = n\alpha \in \alpha\mathbb{Z}$. Cela valant pour tout $x \in \mathbb{G}$, on a bien $G \subset \alpha\mathbb{Z}$, ce qui achève la preuve.

1-c) *Supposons maintenant que $\alpha = 0$. Montrons que G est dense dans $\mathbb{R}$. Pour cela, considérons deux réels $a < b$ et montrons qu'il existe $z \in G$ tel que $a < z < b$. Comme $0 = \inf G \cap \mathbb{R}^{+*}$, il existe $x \in G \cap \mathbb{R}^{+*}$ tel que*

$$0 < x < b - a.$$

Comme $x > 0$, on peut diviser par x et on obtient

$$1 < \frac{b}{x} - \frac{a}{x}.$$

Cela prouve que l'intervalle $]\frac{a}{x}, \frac{b}{x}[$ contient au moins un entier! Considérons alors un entier n dans cet intervalle, et posons $z = nx$. On a

$$a < z < b \qquad \text{et} \qquad z \in G.$$

Ceci complète la preuve.

2) Déduisons maintenant du Théorème 4.14 le corollaire demandé. Remarquons d'abord que si l'on munit l'ensemble H_θ de la loi d'addition usuelle, nous obtenons un sous-groupe de $\mathbb{R}$. En utilisant le Théorème 4.14, nous pouvons affirmer que H_θ est soit de la forme $\alpha\mathbb{Z}$, soit dense dans $\mathbb{R}$.

2-a) *Supposons d'abord que $\theta \notin \mathbb{Q}$. Supposons par l'absurde que H_θ soit de la forme $\alpha\mathbb{Z}$, pour un certain réel $\alpha > 0$. Comme*

$$1 = 1 + \theta \times 0 \qquad \text{et} \qquad \theta = 0 + \theta \times 1,$$

il est clair que $1 \in H_\theta$ et $\theta \in H_\theta$. Cela implique que l'on peut trouver deux entiers relatifs p et q tels que

$$1 = p\alpha \qquad \text{et} \qquad \theta = q\alpha.$$

Donc $\alpha = \frac{1}{p} \in \mathbb{Q}$ et $\theta = \frac{q}{p} \in \mathbb{Q}$. Ceci contredit notre hypothèse de départ selon laquelle $\theta \notin \mathbb{Q}$ et H_θ est donc dense dans $\mathbb{R}$.

2-b) *Pour montrer l'autre implication, nous allons utiliser un raisonnement par contraposée. Supposons donc que $\theta \in \mathbb{Q}$ et montrons que H_θ n'est pas dense dans $\mathbb{R}$. Au vu du Théorème 4.14, cela revient à démontrer que H_θ est de la forme $\alpha\mathbb{Z}$.*

Comme $\theta \in \mathbb{Q}$, θ s'écrit sous la forme d'une fraction $\theta = \frac{p}{q}$ avec p et q premiers entre eux.

Soit $h \in H_\theta$, alors il existe p_h et q_h tels que

$$h = p_h + \theta q_h = p_h + \frac{p}{q} q_h = \frac{1}{q}(p_h q + p q_h) \in \frac{1}{q}\mathbb{Z}.$$

Donc $H_\theta \subset \frac{1}{q}\mathbb{Z}$. Comme $\frac{1}{q}\mathbb{Z}$ est un ensemble discret (non dense), il est alors clair que H_θ ne saurait être dense dans $\mathbb{R}$. Ceci achève la preuve du Corrollaire 4.1.

Pour les plus téméraires d'entre vous, sachez que l'on peut déterminer H_θ explicitement. Nous allons en fait montrer que $H_\theta = \frac{1}{q}\mathbb{Z}$.

Soit maintenant $h \in \frac{1}{q}\mathbb{Z}$. Il existe alors $m_h \in \mathbb{Z}$ tel que $h = \frac{m_h}{q}$. Comme p et q sont premiers entre eux, le Théorème de Bézout (l'aviez-vous oublié ? Si tel est le cas, jetez un coup d'œil à votre cours d'arithmétique de Terminale !) assure l'existence d'entiers r et s tels que

$$rp + sq = 1.$$

Donc $m_h = (rm_h)p + (sm_h)q$ et alors

$$h = \frac{m_h}{q} = \frac{1}{q}\big((rm_h)p + (sm_h)q\big) = rm_h\theta + sm_h = p_h + q_h\theta$$

où on a posé $p_h = sm_h$ et $q_h = rm_h$. Ainsi $h \in H_\theta$ et on a prouvé que $\frac{1}{q}\mathbb{Z} \subset H_\theta$. On a donc montré la double inclusion ! Finalement $H_\theta = \frac{1}{q}\mathbb{Z}$.

3) Démontrons enfin le Théorème 4.15.

***3-a)** Supposons d'abord que $\theta \notin \mathbb{Q}$. On sait, d'après le Corollaire 4.1, que H_θ est dense dans $\mathbb{R}$. Tout réel est donc limite d'une suite d'éléments de H_θ. En particulier, il existe une suite $(h_n = p_n - \theta q_n)_{n\in\mathbb{N}}$ de H_θ qui converge vers 0. Ainsi les deux suites d'entiers relatifs $(p_n)_{n\in\mathbb{N}}$ et $(q_n)_{n\in\mathbb{N}}$ satisfont bien le second point*

$$\lim_{n\to\infty} p_n - \theta q_n = 0.$$

Comme vous l'aviez vu lors de l'étude de la densité de $\mathbb{Q}$ dans $\mathbb{R}$, nous pouvons choisir la suite h_n de manière à approcher 0 par le haut et dans ce cas $p_n - \theta q_n > 0$, pour tout n, ce qui entraîne le premier point.

***3-b)** Démontrons maintenant la réciproque et supposons par l'absurde que θ soit rationnel. Écrivons $\theta = \frac{p}{q}$ sous sa forme irréductible. On a alors, pour tout $n \in \mathbb{N}$,*

$$p_n q - p q_n \neq 0.$$

Mais, comme $p_n q - p q_n$ est un entier, il s'ensuit que

$$|p_n q - p q_n| \geq 1.$$

Et donc $|p_n - \theta q_n| = \frac{1}{q}|p_n q - p q_n| \geq \frac{1}{q}$ ne peut converger vers 0, ce qui contredit la seconde hypothèse de l'énoncé. Ainsi, θ est irrationnel.

Solution 4.7 (du problème 4.2) *1) Ce résultat est très classique et la démarche pour l'obtenir ne l'est pas moins. On établit la propriété demandée d'abord sur $\mathbb{N}$ puis on l'étend pas à pas à $\mathbb{R}$ en passant d'abord par $\mathbb{Z}$ et $\mathbb{Q}$.*

1-a) *Montrons d'abord qu'il existe $a \in \mathbb{R}$ tel que, pour tout $n \in \mathbb{N}$, $f(n) = an$. Comme f est un endomorphisme de $(\mathbb{R}, +)$, pour tous réels x et y,*

$$f(x+y) = f(x) + f(y).$$

En particulier, en prenant $x = n$ et $y = 1$, on obtient $f(n+1) = f(n) + f(1)$. On aboutit alors immédiatement à

$$f(n) = nf(1) \quad \text{pour tout } n \geq 1.$$

Utilisez un raisonnement par récurrence pour démontrer cela rigoureusement. En prenant alors $a = f(1)$, on a démontré notre résultat pour tout $n \in \mathbb{N}^*$. Pour $n = 0$, il suffit de prendre $x = y = 0$ pour obtenir

$$f(0) = f(0+0) = f(0) + f(0) = 2f(0).$$

Ceci implique que $f(0) = 0 = 0 \times a$ et le résultat est vrai sur $\mathbb{N}$.

1-b) *Étendons maintenant le résultat à $\mathbb{Z}$. Pour cela, remarquez que, pour tout $x \in \mathbb{R}$, on a*

$$0 = f(0) = f(x + (-x)) = f(x) + f(-x).$$

Il en résulte que $f(-x) = -f(x)$ et f est donc impaire. Ainsi, pour tout entier relatif négatif $-n$, on a

$$f(-n) = -f(n) = -an = a \times (-n).$$

Ainsi, le résultat est vrai sur $\mathbb{Z}$.

1-c) *Soit $x = \frac{p}{q} \in \mathbb{Q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$. Remarquons d'abord que, pour tout $y \in \mathbb{R}$, on a*

$$f(qy) = qf(y).$$

Si vous avez un doute, démontrez cela par récurrence en revenant à la définition d'un endomorphisme. En choisissant $y = \frac{p}{q}$, on a alors

$$f(p) = f\left(q \times \frac{p}{q}\right) = qf\left(\frac{p}{q}\right).$$

Comme $f(p) = pa$, il en découle que $f(x) = f\left(\frac{p}{q}\right) = \frac{f(p)}{q} = a\frac{p}{q} = ax$. Ceci achève l'extension du résultat à $\mathbb{Q}$.

1-d) *Souvenez vous de notre commentaire sur la densité de $\mathbb{Q}$ dans $\mathbb{R}$; elle sert souvent à étendre des résultats vérifiés sur $\mathbb{Q}$ à $\mathbb{R}$ tout entier, ce qui est exactement ce qu'il nous reste à faire.*

Soit $x \in \mathbb{R}$. Comme $\mathbb{Q}$ est dense dans $\mathbb{R}$ et comme cela a été fait dans la preuve du Théorème 4.12, on peut construire deux suites de rationnels $(r_n)_{n\geq 0}$ et $(s_n)_{n\geq 0}$ qui convergent vers x et qui sont telles que

$$r_n \leq x \leq s_n \qquad \textit{pour tout } n \in \mathbb{N}.$$

Remarquez que nous n'avons toujours pas utilisé l'hypothèse de monotonie de f. Considérez cela comme un indice que cette hypothèse doit nous servir maintenant. Si vous ne voyez toujours pas comment procéder, pensez à utiliser le théorème des gendarmes tel que vous pouvez le lire dans le chapitre sur les suites réelles, Théorème 5.14. Pour fixer les idées, nous supposerons que f est croissante. La preuve est analogue dans le cas où f est décroissante. Pour tout $n \in \mathbb{N}$,

$$r_n a = f(r_n) \leq f(x) \leq f(s_n) = s_n a,$$

où les inégalités sont vraies grâce à la croissance de f. En passant à la limite, on obtient $xa \leq f(x) \leq xa$ et par conséquent $f(x) = ax$. Ceci achève la démonstration. Ainsi les seuls endomorphismes monotones de $(\mathbb{R}, +)$ sont les applications linéaires.

Pour ceux dont les souvenirs sur les suites réelles semblent lointains, n'ayez pas d'inquiétude, elles constituent l'objet du chapitre suivant.

2) Soit g une application monotone de $\mathbb{R}^{+*}$ dans lui-même telle que pour tous réels x et y, $g(xy) = g(x)g(y)$. Soit l'application h de $\mathbb{R}$ dans $\mathbb{R}^{+*}$ définie par $h(x) = g(e^x)$ pour tout $x \in \mathbb{R}$. Soit $(x, y) \in \mathbb{R}^2$. On a

$$h(x+y) = g(e^{x+y}) = g(e^x e^y) = g(e^x)g(e^y) = h(x)h(y).$$

Introduisons alors l'application f définie de $\mathbb{R}$ dans $\mathbb{R}$ par $f(x) = \ln(h(x))$, pour tout $x \in \mathbb{R}$. On a alors, pour tout réel x,

$$f(x+y) = \ln(h(x+y)) = \ln(h(x)h(y)) = \ln(h(x)) + \ln(h(y)) = f(x) + f(y).$$

Ainsi f est un endomorphisme de $(\mathbb{R}, +)$. Aussi, comme g est monotone et que la fonction exponentielle est croissante, $h = g \circ \exp$ est aussi monotone. Enfin, comme la fonction logarithme est aussi croissante, $f = \ln \circ h$ est également monotone. On peut alors utiliser le résultat précédent qui nous assure l'existence de $a \in \mathbb{R}$ tel que

$$\ln(h(y)) = f(y) = ay \qquad \textit{pour tout } y \in \mathbb{R}.$$

En passant à l'exponentielle, il en résulte que, pour tout réel y*,* $g(e^y) = h(y) = e^{ay}$*. Soit* $x \in \mathbb{R}^{+*}$*. Comme l'exponentielle est une fonction bijective de* $\mathbb{R}$ *dans* $\mathbb{R}^{+*}$ *dont la bijection réciproque n'est autre que la fonction logarithme, il existe un unique* $y \in \mathbb{R}$ *tel que* $x = e^y$ *et* $y = \ln(x)$*. Finalement,*

$$g(x) = g(e^y) = h(y) = e^{ay} = e^{a \ln x} = x^a.$$

Ainsi les seules applications monotones de $\mathbb{R}^{+*}$ *satisfaisant la relation de l'énoncé sont les fonctions puissances.*

Chapitre 5

Suites réelles

5.1 Définitions et propriétés de base

Définition 5.1 *Une* ***suite réelle*** $(a_n)_{n\in\mathbb{N}}$ *est une famille d'éléments de* $\mathbb{R}$ *indexée par* $\mathbb{N}$ *ou, dit autrement, une application de* $\mathbb{N}$ *dans* $\mathbb{R}$. *On note l'ensemble des suites réelles* $\mathbb{R}^{\mathbb{N}}$.

Il faut bien distinguer le n-ième terme de la suite a_n et la suite elle-même, que l'on peut aussi bien noter a que $(a_n)_{n\in\mathbb{N}}$.

Notation 5.1 *Soient* $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$. *On définit l'addition et le produit de deux suites par l'addition et le produit terme à terme :*
(i) $(c_n)_{n\in\mathbb{N}} = (a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}}$ *signifie que* $\forall n \in \mathbb{N}$, $c_n = a_n + b_n$ *;*
(ii) $(c_n)_{n\in\mathbb{N}} = (a_n)_{n\in\mathbb{N}} \times (b_n)_{n\in\mathbb{N}}$ *signifie que* $\forall n \in \mathbb{N}$, $c_n = a_n \times b_n$.

Soit $\lambda \in \mathbb{R}$. *On définit aussi le produit d'une suite par un scalaire de manière naturelle, comme suit :*
(iii) $(d_n)_{n\in\mathbb{N}} = \lambda \cdot (a_n)_{n\in\mathbb{N}}$ *signifie que* $\forall n \in \mathbb{N}$, $d_n = \lambda \cdot a_n$.

Ainsi, l'ensemble des suites réelles $\mathbb{R}^{\mathbb{N}}$ est muni des deux lois de composition interne $+$ et $\times$ et d'une loi de composition externe $\cdot$.

Ces notations permettent d'écrire le théorème suivant, dont le sens ne sera clair que si vous avez déjà parcouru le chapitre de ce livre consacré à l'algèbre. Toutefois, la compréhension immédiate de ce théorème n'est pas nécessaire pour lire sereinement la suite de ce chapitre dédié aux suites réelles.

Théorème 5.1 $(\mathbb{R}^{\mathbb{N}}, +, \times)$ *est un anneau commutatif non intègre.*

Il est facile de vérifier que $(\mathbb{R}^{\mathbb{N}}, +, \times)$ satisfait chacune des propriétés définissant un anneau commutatif, exercice que nous vous laissons le soin de faire ! Maintenant, pourquoi est-ce un anneau non intègre ? Pour démontrer ce point, il vous suffit de trouver deux suites non nulles dont le produit est nul. À vous de jouer !

Exemple 5.1 *Considérons la suite réelle a définie par $a_{2n} = 0$ et $a_{2n+1} = 2n+1$ pour tout $n \in \mathbb{N}$. Tous ses termes d'indices pairs sont nuls. Introduisons aussi la suite b dont tous les termes d'indices impairs sont nuls $b_{2n} = 2n$ et $b_{2n+1} = 0$, pour tout $n \in \mathbb{N}$. On a alors $a_n b_n = 0$ pour tout $n \in \mathbb{N}$, mais aucune des deux suites a et b n'est nulle !*

Introduisons maintenant la relation binaire $\leq$ sur $\mathbb{R}^{\mathbb{N}}$.

Définition 5.2 *La relation binaire $\leq$ est telle que pour toutes suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$, $(a_n)_{n\in\mathbb{N}} \leq (b_n)_{n\in\mathbb{N}}$ si pour tout $n \in \mathbb{N}$, $a_n \leq b_n$.*

Lemme 5.1 *La relation $\leq$ de la Définition 5.2 est une relation d'ordre sur $\mathbb{R}^{\mathbb{N}}$.*

Toutes les relations d'ordre ne sont pas totales. Alors, la relation $\leq$ est-elle une relation d'ordre total sur $\mathbb{R}^{\mathbb{N}}$?

Exemple 5.2 *La réponse est non. Les suites dont le terme général est défini par $a_n = (-1)^n$ et $b_n = (-1)^{n+1}$ forment un contre-exemple. En effet, lorsque n est pair, on a $b_n \leq a_n$, alors que, lorsque n est impair, on a au contraire $a_n \leq b_n$. On ne peut donc écrire ni $(a_n)_{n\in\mathbb{N}} \leq (b_n)_{n\in\mathbb{N}}$ ni $(b_n)_{n\in\mathbb{N}} \leq (a_n)_{n\in\mathbb{N}}$.*

Rappelons maintenant la notion de suites monotones.

Définition 5.3 *Une suite $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ est :*

(i) ***stationnaire*** *si elle est constante à partir d'un certain rang, c'est-à-dire s'il existe $p \in \mathbb{N}$ tel que $\forall n \geq p$, $a_n = a_p$;*

(ii) ***croissante*** *si $\forall n, m \in \mathbb{N}$, $n \geq m \Rightarrow a_n \geq a_m$;*

(iii) ***décroissante*** *si $\forall n, m \in \mathbb{N}$, $n \geq m \Rightarrow a_n \leq a_m$.*

Une suite est alors dite monotone si elle est croissante ou décroissante. De la définition 5.3, il est facile de voir qu'une suite a est croissante si et seulement si pour tout $n \in \mathbb{N}$, $a_{n+1} \geq a_n$. De même, une suite a est décroissante si et seulement si pour tout $n \in \mathbb{N}$, $a_{n+1} \leq a_n$. Cela est clair, mais démontrez-le malgré tout.

Quand les inégalités ci-dessus sont strictes, on parle de suites strictement monotones, ce que précise la définition suivante :

Définition 5.4 *Une suite* $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ *est :*
(i) ***strictement croissante*** *si* $\forall n \in \mathbb{N},\ a_{n+1} > a_n$ *;*
(ii) ***strictement décroissante*** *si* $\forall n \in \mathbb{N},\ a_{n+1} < a_n$.

Allez, encore quelques définitions de base avant d'entamer le cœur de ce chapitre :

Définition 5.5 *Une suite* $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ *est :*
(i) ***majorée*** *si* $\exists M \in \mathbb{R},\ \forall n \in \mathbb{N},\ a_n \leq M$ *;*
(ii) ***minorée*** *si* $\exists m \in \mathbb{R},\ \forall n \in \mathbb{N},\ a_n \geq m$ *;*
(iii) ***bornée*** *si elle est majorée et minorée.*

Insistons que pour une suite a majorée, le M dans la définition 5.5 est un majorant et non pas <u>le</u> majorant. Finissons cette partie introductive avec un résultat assez simple à démontrer si vous avez bien lu la définition 5.5.

Lemme 5.2 *La suite* $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ *est bornée si et seulement si la suite* $(|a_n|)_{n\in\mathbb{N}}$ *est majorée.*

5.2 Limite et convergence

5.2.1 Convergence d'une suite

Définition 5.6 *Soit* $l \in \mathbb{R}$. *Une suite* $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ ***converge*** *vers* l, *appelée limite de* $(a_n)_{n\in\mathbb{N}}$, *si*

$$\forall \varepsilon > 0, \exists p \in \mathbb{N}, \forall n \geq p, |a_n - l| \leq \varepsilon.$$

On note alors $(a_n)_{n\in\mathbb{N}} \to l$. *Si* $(a_n)_{n\in\mathbb{N}}$ *n'est pas convergente,* $(a_n)_{n\in\mathbb{N}}$ *est alors dite divergente.*

Cela peut être paraphrasé comme suit : pour toute erreur $\varepsilon > 0$ que l'on se donne, aussi petite soit elle, il existe un rang, p, à partir duquel a est à une distance au plus ε de l. Autrement dit, à partir de ce rang, tous les éléments de la suite a (i.e. tous les termes a_n, pour $n \geq p$) seront compris dans l'intervalle $[l - \varepsilon, l + \varepsilon]$. N'hésitez pas à faire des dessins pour mieux visualiser cela.

Remarque 5.1 *De la Définition 5.6, il est clair que la suite* a *converge vers* l *si et seulement si la suite* b, *définie par* $\forall n \in \mathbb{N}, b_n = a_n - l$, *converge vers 0.*

Étant donné une suite convergente a, le Théorème 5.2, ci-après, justifie que l'on puisse parler de la limite (et non pas d'<u>une</u> limite) de a.

Théorème 5.2 (Unicité de la limite) *Si une suite* $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ *admet une limite, alors cette limite est unique.*

Preuve. Raisonnons par l'absurde : supposons que $(a_n)_{n\in\mathbb{N}}$ converge vers une limite $\lambda \in \mathbb{R}$ et une limite $\mu \in \mathbb{R}$, telles que $\lambda \neq \mu$. L'idée est que la suite ne pourra pas se rapprocher simultanément de λ et de μ. En prenant ε suffisamment petit, de sorte que les intervalles $[\lambda-\varepsilon, \lambda+\varepsilon]$ et $[\mu-\varepsilon, \mu+\varepsilon]$ ne se coupent pas, on pourra aboutir à une contradiction : les termes a_n devront être dans ces deux intervalles à partir d'un certain rang mais cela est impossible car les deux intervalles sont disjoints !

Le choix $\varepsilon = |\lambda - \mu|/3 > 0$ convient. Par définition, il existe $p, q \in \mathbb{N}$, tels que $\forall n \geq p$, $|a_n - \lambda| \leq \varepsilon$ et tels que $\forall n \geq q$, $|a_n - \mu| \leq \varepsilon$. Soit $n \geq \max(p, q)$. Par inégalité triangulaire dans la deuxième ligne ci-après, on obtient :

$$\begin{array}{rcl} |\lambda - \mu| & = & |(\lambda - a_n) - (\mu - a_n)| \\ & \leq & |\lambda - a_n| + |\mu - a_n| \\ & \leq & 2\varepsilon. \end{array}$$

Comme on a posé $\varepsilon = |\lambda-\mu|/3$ et que $|\lambda-\mu| \neq 0$, cela revient à écrire $1 \leq 2/3$, ce qui est absurde et prouve donc le théorème. ∎

Attention à ne pas mal interpréter la phrase de la Définition 5.6 « si $(a_n)_{n\in\mathbb{N}}$ n'est pas convergente, $(a_n)_{n\in\mathbb{N}}$ est alors dite divergente ». Cela ne signifie pas forcément qu'elle diverge vers $+\infty$ ou $-\infty$. Ces notions seront définies de manière précise dans la section 5.2.3, mais l'intuition que vous avez de la divergence vers l'infini est suffisante pour se rendre compte qu'une suite peut ne pas converger sans pour autant diverger vers l'infini. Alors, avez-vous un exemple en tête ? Non ?

Exemple 5.3 *La suite dont le terme général est défini par* $a_n = (-1)^n$ *ne converge pas et ne diverge pas vers l'infini : elle oscille sans cesse entre -1 et 1, comme le montre la figure 5.1, et n'est donc pas convergente mais, étant bornée, elle ne peut pas tendre vers l'infini ! Pour ce type de suite, on dit qu'elle diverge grossièrement.*

Gardez en tête que les suites qui alternent de signe, telle que celle construite dans l'exemple 5.3, sont très utiles pour construire des contre-exemples dans ce cours.

La suite de l'exemple ci-dessus est une suite bornée qui n'est pas convergente. Mais alors, y a-t-il un lien quelconque entre convergence et caractère borné ? Une première réponse, positive, est donnée par le théorème suivant.

Théorème 5.3 *Toute suite convergente est bornée.*

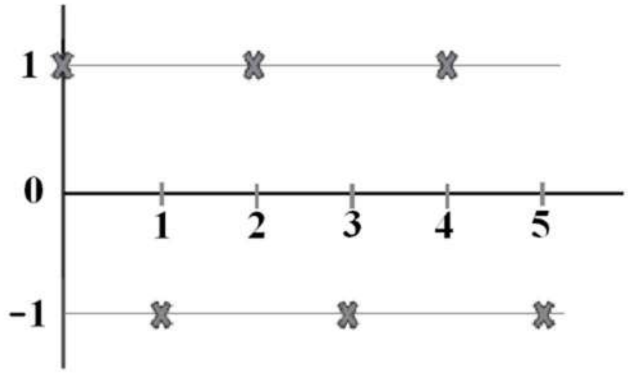

FIGURE 5.1 – Premiers termes de la suite de terme général $(-1)^n$.

Preuve. Soit a une suite convergeant vers $l \in \mathbb{R}$. Prenons $\varepsilon = 1$ dans la Définition 5.6, il existe alors $p \in \mathbb{N}$ tel que pour tout $n \geq p$, $l-1 \leq a_n \leq l+1$. Les premiers termes de la suite étant bornés par $m = \max_{0 \leq k \leq p-1} |a_k|$, il suffit de poser $M = \max\{m, |l-1|, |l+1|\}$ pour obtenir que $a_n \leq M$ pour tout $n \in \mathbb{N}$. ■

On a déjà vu que la réciproque est fausse. Néanmoins, de toute suite bornée on peut extraire une sous-suite qui converge. Mais, avant de vous embarquer dans les sous-suites (voir Section 5.2.4), vous devez d'abord vous exercer à manipuler la Définition 5.6 et les Théorèmes 5.2 et 5.3. Pour cela, nous vous encourageons fortement à démontrer les résultats usuels d'opérations sur les limites que vous avez déjà beaucoup utilisés et que nous vous présentons dans le paragraphe suivant. Essayez par vous-même avant de lire les démonstrations proposées.

5.2.2 Opérations usuelles sur les limites

Théorème 5.4 *Soient a et b deux suites réelles tendant respectivement vers les réels l_1 et l_2. Soit $\lambda \in \mathbb{R}$. Alors,*
(1) la suite $a+b$ converge vers $l_1 + l_2$;
(2) la suite $\lambda \cdot a$ converge vers $\lambda\, l_1$.

Preuve. On se donne $\varepsilon > 0$. On cherche à démontrer qu'il existe $p > 0$ tel que pour tout $n \geq p$, $|a_n + b_n - (l_1 + l_2)| \leq \varepsilon$. Mais comme a converge vers l_1,

$$\forall \eta > 0, \exists N > 0, \forall n \geq N, |a_n - l_1| \leq \eta.$$

En particulier, si l'on choisit $\eta = \frac{\varepsilon}{2}$, il existe $N_1 > 0$ tel que pour tout $n \geq N_1$, $|a_n - l_1| \leq \frac{\varepsilon}{2}$. De même, il existe N_2 tel que pour tout $n \geq N_2$, $|b_n - l_2| \leq \frac{\varepsilon}{2}$.

Maintenant, il suffit que n soit plus grand que $p = \max(N_1, N_2)$ pour que

$$|a_n + b_n - (l_1 + l_2)| \leq |a_n - l_1| + |b_n - l_2| \leq \varepsilon,$$

où la première inégalité est la fameuse inégalité triangulaire. Ce qui démontre le premier point. Nous vous laissons le soin de démontrer le second point. ∎

Qu'en est-il de la limite du produit de deux suites convergentes ? Pour démontrer qu'elle existe et qu'elle est égale au produit des limites des deux suites, on a besoin du résultat suivant, qui est simple (mais utile) et que vous devez savoir démontrer les yeux fermés.

Lemme 5.3 *Soient a et b deux suites réelles telles que a est bornée et b converge vers 0. Alors la suite $a \times b$ converge vers 0.*

Preuve. Soit $\varepsilon > 0$ fixé. Comme a est bornée, il existe $M > 0$ tel que $|a_n| \leq M$ pour tout $n \in \mathbb{N}$. Comme b converge vers 0, il existe $p \in \mathbb{N}$, $\forall n \geq p$, $|b_n| \leq \frac{\varepsilon}{M}$. Alors,

$$\forall n \geq p, |a_n b_n| \leq |a_n||b_n| \leq M\frac{\varepsilon}{M} \leq \varepsilon.$$

∎

Théorème 5.5 *Soient a et b deux suites réelles tendant respectivement vers les réels l_1 et l_2. La suite $a \times b$ converge alors vers $l_1 l_2$.*

L'idée de la démonstration est simple. Moralement, comme a_n est proche de l_1, on pense à écrire $a_n b_n = l_1 b_n + (a_n - l_1)b_n$. Voyez vous comment conclure maintenant ?

Preuve. On a $a_n b_n = l_1 b_n + (a_n - l_1)b_n$. Comme b converge vers l_2, $l_1 b_n$ tend vers $l_1 l_2$ par le Théorème 5.4 (2). Comme a converge vers l_1, $a_n - l_1$ tend vers 0 ; comme b converge, elle est bornée, par le Théorème 5.3 ; donc $(a_n - l_1)b_n$ tend vers 0 par le Lemme 5.3. D'où le résultat. ∎

Et pour le quotient de deux suites ? Le passage de la limite au quotient est-il légitime ? Pour répondre rigoureusement à cette question, une digression sur le passage des inégalités à la limite est nécessaire.

Théorème 5.6 (Passage des inégalités à la limite) *Soit a une suite réelle à valeurs positives (i.e. pour tout $n \in \mathbb{N}, a_n \geq 0$). Si a converge vers l, alors $l \geq 0$.*

Raisonnez par l'absurde pour démontrer cela. Supposez $l < 0$ et essayez d'obtenir une contradiction avec les hypothèses du théorème. L'idée est que les termes u_n finissent par tous se retrouver dans une bande autour de l, une bande aussi fine que vous le désirez, et donc tous ces termes finissent par se retrouver notamment entre $\frac{3l}{2}$ et $\frac{l}{2}$. Ils seront alors tous strictement négatifs car $\frac{l}{2} < 0$ selon l'hypothèse que vous avez faite pour ce raisonnement.

Preuve. Supposons $l < 0$. On choisit $\varepsilon = -\frac{l}{2} > 0$ dans la Définition 5.6. Il existe $p \in \mathbb{N}$ tel que pour tout $n \geq p$, $|a_n - l| \leq -\frac{l}{2}$, et donc

$$\frac{l}{2} \leq a_n - l \leq -\frac{l}{2},$$

ce qui démontre que $\frac{3l}{2} \leq a_n \leq \frac{l}{2} < 0$ pour tout $n \geq p$. Cela contredit le fait que a est une suite à valeurs positives et prouve que la limite l est forcément positive. ■

Réfléchissez un instant au cas où l'on remplace l'inégalité large par une inégalité stricte dans l'énoncé du théorème ci-dessus, c'est à dire au cas où a est une suite convergente à valeurs strictement positives. Que peut-on dire de sa limite l ?

Si vous êtes en train d'essayer de démontrer que $l > 0$, vous pouvez arrêter maintenant ! En fait, on ne peut rien dire de plus. La limite l peut être positive ou nulle. Avez-vous un contre-exemple ?

Exemple 5.4 *Soit a la suite de terme général $a_n = \frac{1}{n}$. On a bien $a_n > 0$ pour tout $n \in \mathbb{N}$ et pourtant a_n converge vers 0.*

Corollaire 5.1 *Soient a et b deux suites qui convergent respectivement vers l_1 et l_2 et telles que $a_n \leq b_n$ pour tout $n \in \mathbb{N}$. Alors $l_1 \leq l_2$.*

Preuve. Il suffit d'appliquer le Théorème 5.6 à la suite à termes positifs $b - a$. ■

Le résultat suivant, analogue au Théorème 5.6, peut s'avérer très utile. Il peut s'énoncer comme suit : si a est une suite réelle qui converge vers une limite non nulle, alors a garde un signe constant à partir d'un certain rang.

Théorème 5.7 *Soit a une suite réelle qui converge vers l.*
(1) Si $l > 0$, alors il existe $p \in \mathbb{N}$ tel que $a_n > 0$ pour tout $n \geq p$.
(2) Si $l < 0$, alors il existe $p \in \mathbb{N}$ tel que $a_n < 0$ pour tout $n \geq p$.

L'idée est encore la même : pour $l > 0$, par exemple, les termes a_n finissent par se retrouver entre $\frac{l}{2}$ et $\frac{3l}{2}$ et finiront donc par être tous strictement positifs car $\frac{l}{2} > 0$.

Preuve. Commençons par (1). On choisit $\varepsilon = \frac{l}{2} > 0$ dans la Définition 5.6. Il existe $p \in \mathbb{N}$ tel que pour tout $n \geq p$, $|a_n - l| \leq \frac{l}{2}$, et donc

$$-\frac{l}{2} \leq a_n - l \leq \frac{l}{2},$$

ce qui démontre que $0 < \frac{l}{2} \leq a_n \leq \frac{3l}{2}$ pour tout $n \geq p$. Le point (2) découle du point (1) car si a converge vers $l < 0$ alors la suite $(-a)$ converge vers $-l > 0$. ■

Peut-on obtenir le même type de conclusion si $l = 0$?

Exemple 5.5 *Évidemment, on ne peut rien conclure si la limite l est nulle. Pensez à nouveau à la suite alternée $\big((-1)^n\big)_{n\in\mathbb{N}}$ de l'Exemple 5.3, et essayez de la transformer en une suite qui converge vers 0. Pour cela, il suffit par exemple de diviser le terme général par $n+1$. Définissons $a = \big(\frac{(-1)^n}{n+1}\big)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$. La suite a converge vers 0 tout en alternant de signe sans arrêt.*

Néanmoins, il y a un cas intéressant où l'on peut déterminer le signe de la suite a même dans le cas où elle tend vers 0. Que pouvez-vous ainsi dire du signe d'une suite décroissante qui tend vers 0 ?

Lemme 5.4 *Soit a une suite réelle décroissante tendant vers 0. Alors $\forall n \in \mathbb{N}$, $a_n \geq 0$.*

Preuve. Comme a est décroissante, pour tous n et m dans $\mathbb{N}$, $n \leq m \Rightarrow a_n \geq a_m$, d'après la Définition 5.3. Par passage à la limite lorsque m tend vers $+\infty$, et comme a converge vers 0, on obtient bien que pour tout $n \in \mathbb{N}$, $a_n \geq 0$. ■

Cette digression achevée, on peut à présent énoncer le résultat sur la limite de l'inverse d'une suite convergente.

Théorème 5.8 *Soit a une suite réelle qui converge vers $l \in \mathbb{R}^*$. Alors, les deux assertions suivantes sont vraies.*
(1) Il existe $p \in \mathbb{N}$ tel que $\forall n \geq p$, $a_n \neq 0$.
(2) La suite $\left(\frac{1}{a_n}\right)_{n\geq p}$ converge vers $\frac{1}{l}$.

Nous vous donnons l'idée de la démonstration et allez y réfléchir un peu. Écrivez

$$\left|\frac{1}{a_n} - \frac{1}{l}\right| = \frac{|l - a_n|}{|la_n|}.$$

Il vous sera immédiat de majorer le numérateur. Minorer le dénominateur est légèrement moins évident.

Preuve. Le point (1) est une conséquence immédiate du Théorème 5.7 car soit $l > 0$ et dans ce cas il existe un rang p à partir duquel les termes de la suite a seront tous strictement positifs et donc non nuls ; soit $l < 0$ et il existe alors un rang à partir duquel ces termes seront tous strictement négatifs (et donc non nuls). La suite $\left(\frac{1}{a_n}\right)_{n\geq p}$ est ainsi bien définie.

Démontrons le point (2). Quitte à remplacer a par son opposée, nous pouvons supposer que $l > 0$, ce que nous faisons pour fixer les idées. Comme a converge vers l, et avec le choix $\varepsilon = \frac{l}{2} > 0$ dans la Définition 5.6, on obtient

$$\exists N_1 \in \mathbb{N}, \forall n \geq N_1, |a_n - l| \leq \frac{l}{2}.$$

Il s'ensuit que pour tout $n \geq N_1$, $0 < \frac{l}{2} \leq a_n$. Soit $\varepsilon > 0$. Toujours par convergence de a, il existe un autre rang $N_2 \in \mathbb{N}$, tel que pour tout $n \geq N_2$, $|a_n - l| \leq \varepsilon$. Et alors, pour tout $n \geq \max(N_1, N_2)$,

$$\left|\frac{1}{a_n} - \frac{1}{l}\right| = \frac{|l - a_n|}{|la_n|} \leq \frac{2\varepsilon}{l^2},$$

ce qui prouve que $\left(\frac{1}{a_n}\right)_{n\geq p}$ converge vers $\frac{1}{l}$. ■

Remarque 5.2 *Notez que si vous vouliez finir avec ε au second membre de la dernière inégalité de la preuve ci-dessus, il aurait suffi de choisir $\frac{\varepsilon l^2}{2}$ au lieu de ε lorsque l'on a défini le rang N_2. Vous avez maintenant vu suffisamment d'exemples de ce type de preuves pour que l'on vous épargne ces découpages de ε.*

5.2.3 Divergence d'une suite vers l'infini

Définition 5.7 *Une suite $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$* ***diverge (ou tend)*** *vers $+\infty$ si*

$$\forall A > 0, \exists p \in \mathbb{N}, \forall n \geq p, a_n \geq A.$$

On note alors $(a_n)_{n\in\mathbb{N}} \to +\infty$. On dit aussi que la suite a diverge vers $-\infty$ si la suite $(-a)$ diverge vers $+\infty$.

En d'autres termes, une suite diverge vers $+\infty$ s'il suffit d'aller suffisamment loin pour que tous ses termes soient aussi grands que l'on veut. Encore une fois, visualisez cela sur un dessin.

Remarque 5.3 *De la Définition 5.7, on voit qu'une suite a diverge vers $-\infty$ si*

$$\forall A < 0, \exists p \in \mathbb{N}, \forall n \geq p, a_n \leq A.$$

Les premières conséquences de cette définition sont les suivantes :

Lemme 5.5 *Soit $a \in \mathbb{R}^{\mathbb{N}}$. Supposons que a diverge vers $+\infty$. Alors*
(1) a est strictement positive à partir d'un certain rang ;
(2) a n'est pas majorée.

Preuve. Le point (1) découle simplement du choix de la constante $A = 1$, par exemple, dans la Définition 5.7. Démontrons (2) par l'absurde et supposons donc que a est majorée. Notons $M > 0$ un majorant. Alors, pour tout $n \in \mathbb{N}$, $a_n \leq M$. Choisissons alors $A = M + 1$ dans la Définition 5.7 pour obtenir notre contradiction. ∎

La réciproque du point (2) est-elle vraie ? Une suite non majorée diverge-t-elle forcément vers l'infini ? La réponse est non ! Réfléchissez bien par vous-même à un contre-exemple avant de lire celui que nous vous proposons.

Exemple 5.6 *Rappelez-vous que les suites qui alternent de signe aident souvent à construire des contre-exemples. Réfléchissez à nouveau dans ce sens si vous n'avez pas encore trouvé et relisez l'Exemple 5.3 pour vous rafraîchir les idées.*

Définissons $a = ((-1)^n n)_{n\in\mathbb{N}}$. La suite a n'est pas majorée et la suite $|a|$ diverge vers $+\infty$ (remarquez que pour tout $n \in \mathbb{N}$, $|a_n| = n$). Mais la suite a, elle-même, ne diverge pas vers $+\infty$. On peut le prouver en utilisant le point (1) du précédent lemme. Cette suite, a, n'arrête pas de changer de signe, car $a_{2n} = 2n > 0$ et $a_{2n+1} = -(2n + 1) < 0$, et a ne peut donc pas devenir strictement positive à partir d'un certain rang.

Pouvons-nous appliquer les opérations usuelles sur les limites, établies pour les suites convergentes, dans le cas de suites divergentes ? La réponse est généralement oui, mais tout n'est pas permis ! Il faut bien faire attention à ce que l'on fait. Commençons par énoncer les résultats concernant l'addition, la multiplication et l'inverse. Nous vous laissons le soin de faire les démonstrations. Bien que tous ces résultats soient très intuitifs, les démontrer rigoureusement est un exercice formateur que nous vous recommandons fortement de faire.

Théorème 5.9 *Soient a et b deux éléments de $\mathbb{R}^{\mathbb{N}}$.*
(1) Si a et b diverge vers $+\infty$, alors $a + b$ aussi ;
(2) Si a converge et b diverge vers $+\infty$, alors $a + b$ diverge vers $+\infty$;
(3) Si a et b diverge vers $+\infty$, alors ab diverge vers $+\infty$;
(4) Si a converge vers $l > 0$ et b diverge vers $+\infty$, alors ab diverge vers $+\infty$.
(5) Si a diverge vers $+\infty$ alors il existe un rang p à partir duquel a est strictement positive et $\left(\frac{1}{a}\right)_{n\geq p}$ converge vers 0.

(6) Si a converge vers 0 et est strictement positive à partir d'un certain rang p, alors $\left(\frac{1}{a}\right)_{n\geq p}$ diverge vers $+\infty$.

Quelques généralisations et contre-exemples s'imposent. Commençons par les points (1) et (2).

Exemple 5.7 *A-t-on un résultat similaire au point (1) si a diverge vers $+\infty$ et b diverge vers $-\infty$? La réponse est non ! Prenez par exemple $a_n = n$ et $b_n = -n$. La suite $(a+b)$ est identiquement nulle et converge trivialement vers 0.*

Dans le point (2), la convergence de a n'est pas le point clé : il suffit de supposer que a est minorée pour obtenir le même résultat.

Donnons aussi quelques détails concernant le produit de limites, points (3) et (4).

Exemple 5.8 *Dans (3), et contrairement à l'addition, le produit de deux suites divergeant l'une vers $+\infty$ et l'autre vers $-\infty$ diverge vers $-\infty$.*

Dans (4), l'hypothèse l non nul est cruciale. Donnez un exemple où a converge vers 0 et b diverge vers $+\infty$ mais ab ne diverge pas vers $+\infty$. Aucune idée ? Le choix $a_n = \frac{1}{n}$ et $b_n = n$ satisfait l'hypothèse mais ab est la suite constante égale à 1.

Dans le point (4) encore, la convergence de a n'est pas le point clé ici non plus : il suffit de supposer que a est minorée à partir d'un certain rang par un réel ***strictement*** *positif pour obtenir le même résultat. Démontrez-le !*

5.2.4 Suites extraites

Comme promis en début de chapitre, nous revenons maintenant en détail sur la notion de sous-suite.

Définition 5.8 *Une* ***suite extraite****, ou* ***sous-suite****, d'une suite $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ est une suite de la forme $(a_{\phi(n)})_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$, où ϕ est une application strictement croissante de $\mathbb{N}$ vers $\mathbb{N}$.*

L'application ϕ de la Définition 5.8 s'appelle une extraction. Les extractions les plus communément utilisées sont les suivantes :

(1) L'application $\phi(n) = n + p$ où p est un entier fixé. Elle correspond à la suite décalée de p indices, i.e. $\forall n \in \mathbb{N}$, $a_{\phi(n)} = a_{n+p}$.
(2) L'application $\phi(n) = 2n$. Elle correspond à la suite des termes d'indices pairs de la suite d'origine a, i.e. $\forall n \in \mathbb{N}$, $a_{\phi(n)} = a_{2n}$.

(3) L'application $\phi(n) = 2n+1$. Elle correspond à la suite des termes d'indices impairs de la suite d'origine a, i.e. $\forall n \in \mathbb{N}$, $a_{\phi(n)} = a_{2n+1}$.

Les sous-suites étant définies, nous pouvons maintenant énoncer le résultat suivant :

Théorème 5.10 (Bolzano-Weierstrass) *Toute suite réelle bornée admet une sous-suite convergente.*

Cet énoncé constitue un résultat important d'analyse connu sous le nom de Théorème de Bolzano-Weierstrass. Vous le démontrerez pas à pas dans le problème corrigé 5.2, bien que hors programme en classes préparatoires. En attendant, profitons de cette section pour vous familiariser davantage avec les suites extraites.

Exemple 5.9 *Nous avons déjà rencontré la suite alternée définie par $u_n = (-1)^n$. Cette suite ne converge pas. Néanmoins elle est bornée. D'après le Théorème 5.10, elle admet donc une sous-suite convergente. Il est immédiat de voir que les sous-suites $u_{2n} = 1$ et $u_{2n+1} = -1$ sont constantes, donc convergentes.*

Exemple 5.10 *Soient $p \in \mathbb{N}^*$ et u la suite de terme général $u_n = \cos(n\frac{\pi}{p})$. Pour tout n, $|u_n| \leq 1$. La suite u est bornée et admet donc une sous-suite convergente. Pouvez-vous en trouver une ?*

Introduisons l'extraction $\phi(n) = 2pn$ et la suite de terme général $v_n = u_{\phi(n)}$. La suite v est une sous-suite convergente de u. En effet, en utilisant le fait que la fonction $\cos$ est 2π-périodique, on voit que pour tout $n \geq 0$

$$v_n = u_{2pn} = \cos(2pn\frac{\pi}{p}) = \cos(2n\pi) = \cos(0) = 1.$$

De même, la sous-suite $(u_{(2n+1)p})_{n\in\mathbb{N}}$ est convergente car

$$u_{(2n+1)p} = \cos((2n+1)p\frac{\pi}{p}) = \cos\big((2n+1)\pi\big) = \cos(\pi) = -1.$$

Le résultat ci-dessous montre que la convergence ou divergence vers l'infini d'une suite détermine complètement le comportement de toutes ses sous-suites.

Théorème 5.11 *Soit $a = (a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ telle que $(a_n)_{n\in\mathbb{N}} \to l \in \mathbb{R} \cup \{+\infty, -\infty\}$. Soit $(b_n)_{n\in\mathbb{N}}$ une sous-suite de a. Alors $(b_n)_{n\in\mathbb{N}} \to l$.*

Pour démontrer ce théorème, nous avons besoin du lemme suivant.

Lemme 5.6 *Soit ϕ une application strictement croissante de $\mathbb{N}$ vers $\mathbb{N}$. Alors pour tout $n \in \mathbb{N}$, on a $\phi(n) \geq n$.*

Vous souvenez-vous du principe de récurrence ? Ce petit lemme est l'occasion de vous rafraîchir les idées. A vos crayons et papiers !

Preuve. Soit $n \in \mathbb{N}$ et (H_n) l'assertion $\phi(n) \geq n$. Cette assertion est vraie pour $n = 0$, car $\phi(0) \in \mathbb{N}$ et est donc positif. Fixons $n \in \mathbb{N}$ et supposons (H_n) vraie. Démontrons (H_{n+1}). Comme ϕ est strictement croissante, $\phi(n+1) > \phi(n) \geq n$. Donc $\phi(n+1) > n$. Mais comme $\phi(n+1)$ est un entier, alors forcément, $\phi(n+1) \geq n+1$. Ceci prouve (H_{n+1}) et conclut le raisonnement. ∎

Preuve. (Théorème 5.11). Décryptons les hypothèses de ce théorème. Supposons tout d'abord que la suite a converge vers $l \in \mathbb{R}$. Soit $\varepsilon > 0$. Par la Définition 5.6, on sait que

$$\exists p \in \mathbb{N}, \forall n \geq p, |a_n - l| \leq \varepsilon.$$

Par ailleurs, comme on l'a vu dans la Définition 5.8, il existe une fonction ϕ strictement croissante de $\mathbb{N}$ vers $\mathbb{N}$ telle que, pour tout $n \in \mathbb{N}$, on peut écrire $b_n = a_{\phi(n)}$. L'application ϕ étant strictement croissante, on a ainsi, d'après le Lemme 5.6,

$$\forall n \in \mathbb{N}, \phi(n) \geq n.$$

Il ne reste alors plus qu'à utiliser ces deux équations. Considérons $n \geq p$. Alors $\phi(n) \geq n \geq p$. Donc :

$$|b_n - l| = |a_{\phi(n)} - l| \leq \varepsilon$$

et le tour est joué, pensez-vous. Attention, ce n'est pas totalement fini, car nous avons fait l'hypothèse, dans cette démonstration, que a convergeait, mais l'énoncé du théorème est plus général. Allez, en utilisant la Définition 5.7, vous devriez bien réussir à démontrer ce résultat dans le cas où a diverge vers l'infini, n'est-ce pas ? Alors, seulement, vous aurez prouvé le théorème en entier. ∎

Le Théorème 5.11 fournit alors une méthode pour démontrer qu'une suite diverge grossièrement. Sans le dire, nous avons déjà vaguement utilisé cela dans l'Exemple 5.3.

Corollaire 5.2 *Soit $a \in \mathbb{R}^{\mathbb{N}}$. Si a admet deux sous-suites qui tendent vers deux limites différentes l_1 et l_2 de $\mathbb{R} \cup \{+\infty, -\infty\}$, alors a n'admet pas de limite dans $\mathbb{R} \cup \{+\infty, -\infty\}$.*

Reprenons maintenant l'Exemple 5.3. La suite $a = ((-1)^n)_{n\in\mathbb{N}}$ diverge grossièrement car les sous-suites $(a_{2n})_{n\in\mathbb{N}}$ et $(a_{2n+1})_{n\in\mathbb{N}}$ convergent respectivement vers 1 et -1. La suite $u = \left(\cos(n\frac{\pi}{p})\right)_{n\in\mathbb{N}}$ de l'Exemple 5.10 est aussi grossièrement divergente car les sous-suites $(u_{2np})_{n\in\mathbb{N}}$ et $(u_{(2n+1)p})_{n\in\mathbb{N}}$ convergent respectivement vers 1 et -1.

Notons que le Corollaire 5.2 prouve que la connaissance des comportements de quelques sous-suites permet parfois de tirer des conclusions sur le comportement de la suite elle-même.

Théorème 5.12 *Soit $a \in \mathbb{R}^{\mathbb{N}}$ et $l \in \mathbb{R} \cup \{+\infty, -\infty\}$. Les deux assertions suivantes sont équivalentes :*
(1) les suites $(a_{2n})_{n\in\mathbb{N}}$ et $(a_{2n+1})_{n\in\mathbb{N}}$ tendent vers la même limite l ;
(2) la suite a tend vers l.

Preuve. L'implication (2) $\Rightarrow$ (1) est une conséquence immédiate du Théorème 5.11.

Démontrons donc l'implication (1) $\Rightarrow$ (2). Supposons $l \in \mathbb{R}$ et fixons $\varepsilon > 0$. Par hypothèse, $\exists N_1 \in \mathbb{N}, \forall n \geq N_1, |a_{2n} - l| \leq \varepsilon$ et $\exists N_2 \in \mathbb{N}, \forall n \geq N_2, |a_{2n+1} - l| \leq \varepsilon$. Il suffit alors de définir $N = \max(2N_1, 2N_2 + 1)$ pour que pour tout $n \geq N$, $|a_n - l| \leq \varepsilon$. Les cas de limites infinies vous sont laissés en exercice. ■

5.2.5 Moyenne de Cesàro

On appelle **moyenne de Cesàro** d'une suite a la suite dont le terme général de rang n est obtenu en effectuant la moyenne arithmétique des n premiers termes de la suite a. Le Théorème de Cesàro précise alors que lorsque la suite a admet une limite, sa moyenne de Cesàro admet la même limite.

Théorème 5.13 (Cesàro) *Soit a une suite réelle. Soit b la suite dont le terme général est donné par*

$$b_n = \frac{1}{n+1} \sum_{k=0}^{n} a_k.$$

Si a tend vers $l \in \mathbb{R}$ alors b aussi.

Preuve. Remarquons qu'il nous suffit seulement de prouver le résultat dans le cas $l = 0$. En effet, supposons que l'on ait démontré le théorème pour $l = 0$. Soit maintenant une suite a qui converge vers $l \in \mathbb{R}^*$. Introduisons la suite auxiliaire $u = a - l$, qui converge vers 0. La suite de terme général

$$\frac{1}{n+1} \sum_{k=0}^{n} u_k = \frac{1}{n+1} \sum_{k=0}^{n} (a_k - l) = \frac{1}{n+1} \sum_{k=0}^{n} a_k - \frac{1}{n+1} \sum_{k=0}^{n} l = b_n - l$$

converge alors vers 0, ce qui démontre que b converge effectivement vers l. Nous pouvons donc tranquillement nous concentrer sur le cas $l = 0$.

Soit $\varepsilon > 0$ fixé. Comme a converge vers 0, d'après la Définition 5.6 que vous maîtrisez maintenant (si ce n'est pas le cas, relisez toute la partie 5.2 sur la convergence, sans quoi ce qui suit vous semblera abscons) on sait qu'il existe $p \in \mathbb{N}$ tel que pour tout $n \geq p$, $|a_n| \leq \frac{\varepsilon}{2}$. Découpons $|b|$ en deux sommes dont chacune sera majorée par $\frac{\varepsilon}{2}$ à partir d'un certain rang. La somme sera donc majorée par ε à partir du même rang. Soit $n \geq p$, on écrit alors

$$b_n = \frac{1}{n+1} \sum_{k=0}^{p-1} a_k + \frac{1}{n+1} \sum_{k=p}^{n} a_k$$

et en utilisant l'inégalité triangulaire, on obtient

$$|b_n| \leq \frac{1}{n+1} \left| \sum_{k=0}^{p-1} a_k \right| + \frac{1}{n+1} \left| \sum_{k=p}^{n} a_k \right|.$$

Réappliquons l'inégalité triangulaire aux $(n-p+1)$ termes de la deuxième somme

$$|b_n| \leq \frac{1}{n+1} \left| \sum_{k=0}^{p-1} a_k \right| + \frac{1}{n+1} \sum_{k=p}^{n} |a_k|.$$

Maintenant, vu que $\forall n \geq p$, $|a_n| \leq \varepsilon$, on peut majorer la deuxième somme par $\frac{1}{n+1} \sum_{k=p}^{n} \varepsilon = \frac{n-p+1}{n+1} \frac{\varepsilon}{2} \leq \frac{\varepsilon}{2}$ et donc, pour le moment, nous avons démontré que

$$\forall n \geq p, \qquad |b_n| \leq \frac{1}{n+1} \left| \sum_{k=0}^{p-1} a_k \right| + \frac{\varepsilon}{2}. \tag{5.1}$$

Comme p est un nombre fixé, la somme $\left| \sum_{k=0}^{p-1} a_k \right|$ est une simple constante positive, que l'on peut noter A. La suite de terme général $\frac{1}{n+1} \left| \sum_{k=0}^{p-1} a_k \right| = \frac{A}{n+1}$ converge alors vers 0, et il existe donc $p_0 \in \mathbb{N}$ tel que

$$\forall n \geq p_0, \qquad 0 \leq \frac{1}{n+1} \left| \sum_{k=0}^{p-1} a_k \right| \leq \frac{\varepsilon}{2}. \tag{5.2}$$

Mettant bout à bout les inégalités (5.1) et (5.2), nous obtenons pour tout $n \geq \max(p, p_0)$, $|b_n| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$, ce qui conclut la preuve. ■

Remarque 5.4 *Le résultat reste vrai en cas de divergence vers l'infini : si a diverge vers $+\infty$ ou $-\infty$, il en sera de même pour b. Nous vous recommandons fortement d'essayer de reproduire la preuve dans ces deux cas.*

Vous aurez encore l'occasion de vous entraîner à faire ces démonstrations *à la Cesàro* dans l'Exercice 5.3, où une formulation plus générale du Théorème 5.13 est proposée. Dans ce type d'exercice, la recette est toujours la même : réussir à découper la somme en deux termes, le premier étant majoré par une petite quantité ε grâce à un dénominateur qui le fait tendre vers 0 (c'était le $n+1$ dans la preuve ci-dessus) et la convergence du second terme découlant généralement de la convergence de la suite a à partir de laquelle la moyenne que vous étudiez a été construite.

Notons que la réciproque du Théorème de Cesàro est fausse. Il existe des suites n'admettant pas de limite, mais pour lesquelles la moyenne de Cesàro est convergente. Le moyen le plus simple de construire de telles suites est de penser à une suite a qui diverge grossièrement mais telle que la suite $(\sum_{k=0}^{n} a_k)_{n\in\mathbb{N}}$ soit bornée. Pour une telle suite la moyenne de Cesàro converge vers 0.

Exemple 5.11 *Considérons la suite divergente $a = ((-1)^n)_{n\in\mathbb{N}}$ que nous avons rencontrée à maintes reprises précédemment. La somme $\sum_{k=0}^{n}(-1)^k$ vaut 1 si n est pair et 0 si n est impair. Elle est donc bornée par 1. Il s'ensuit que pour tout $n \in \mathbb{N}$,*

$$\frac{1}{n+1}\left|\sum_{k=0}^{n}(-1)^k\right| \leq \frac{1}{n+1}$$

et la moyenne de Cesàro $\left(\frac{1}{n+1}\sum_{k=0}^{n}(-1)^k\right)_{n\in\mathbb{N}}$ converge vers 0.

Pouvez-vous maintenant construire un exemple d'une suite a où cette fois-ci la moyenne de Cesàro de a converge vers une limite non nulle sans que a admette une limite ?

Exemple 5.12 *Soit a la suite de terme général $a_n = \frac{1}{2}((-1)^n + 1)$. Cela donne $a_{2n} = 1$ et $a_{2n+1} = 0$ pour tout $n \in \mathbb{N}$. La suite a diverge grossièrement par le Corollaire 5.2. Sa moyenne de Cesàro converge vers $\frac{1}{2}$. En effet, pour tout $n \in \mathbb{N}$,*

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

La première somme tend vers 0 par l'Exemple 5.11. La seconde vaut $\frac{1}{2}$, comme annoncé.

Finalement, on peut aussi avoir des suites n'admettant pas de limite et dont la moyenne de Cesàro diverge vers l'infini. Un exemple ? Si vous n'en avez pas trouvé, nous vous proposons celui-ci.

Exemple 5.13 *Soit a la suite de terme général défini par $a_{2p} = 2p$ et $a_{2p+1} = 0$, pour tout $p \in \mathbb{N}$. Autrement dit, a_n est nulle si n est impair et égal à n si n est pair. En utilisant le Théorème 5.12, montrez que la moyenne de Cesàro de a diverge vers $+\infty$.*

Toujours rien ? Bon, notons $b_n = \frac{1}{n+1}\sum_{k=0}^{n} a_n$ et calculons les limites des deux suites extraites $(b_{2n})_{n\in\mathbb{N}}$ et $(b_{2n+1})_{n\in\mathbb{N}}$. On a pour tout $n \in \mathbb{N}$,

$$b_{2n} = \frac{1}{2n+1}\sum_{k=0}^{2n} a_k = \frac{1}{2n+1}\sum_{p=0}^{n} a_{2p},$$

où la dernière égalité a lieu car tous les termes impairs sont nuls ! Et alors

$$\begin{array}{rcl} b_{2n} & = & \frac{1}{2n+1}\sum_{p=0}^{n} 2p \\ & = & \frac{2}{2n+1}\frac{n(n+1)}{2} \\ & = & \frac{n(n+1)}{2n+1} \end{array}$$

et $(b_{2n})_{n\in\mathbb{N}}$ diverge vers $+\infty$. Étudions maintenant la sous-suite des termes impairs.

$$\begin{array}{rcl} b_{2n+1} & = & \frac{1}{2n+2}\sum_{k=0}^{2n+1} a_k \\ & = & \frac{1}{2n+2}\sum_{p=0}^{n} a_{2p} \\ & = & \frac{1}{2n+2}\sum_{p=0}^{n} 2p \\ & = & \frac{2}{2n+2}\frac{n(n+1)}{2} \\ & = & \frac{n}{2} \end{array}$$

et $(b_{2n+1})_{n\in\mathbb{N}}$ diverge aussi vers $+\infty$. On peut donc conclure que b diverge vers $+\infty$.

5.3 Théorèmes de convergence

Souvent, le recours à la Définition 5.6 n'est pas nécessaire pour démontrer la convergence d'une suite. Les maniements d'ε vous semblaient fastidieux ? Soyez donc rassurés ! Des théorèmes sont là pour vous permettre de démontrer aisément qu'une suite converge. Nous présentons et démontrons ci-dessous les plus classiques de ces théorèmes.

5.3.1 Théorèmes de comparaison

Le théorème suivant, appelé couramment théorème des gendarmes, est aussi connu sous le nom de théorème d'encadrement, ces deux noms traduisant la même idée d'une suite encadrée par deux autres suites, comme une escorte de deux gendarmes de part et d'autre d'un bandit.

Théorème 5.14 (Des gendarmes) *Soient a, b et c trois suites réelles telles que a et c convergent vers la même limite l et satisfaisant $\forall n \in \mathbb{N}$, $a_n \leq b_n \leq c_n$. Alors b est convergente, de limite l.*

Preuve. Soit $\varepsilon > 0$. Comme a et c convergent vers l, $\exists N_a \in \mathbb{N}, \forall n \geq N_a, |a_n - l| \leq \varepsilon$ et $\exists N_c \in \mathbb{N}, \forall n \geq N_c, |c_n - l| \leq \varepsilon$. Choisissons $N = \max(N_a, N_c)$. Alors pour tout $n \geq N$,

$$-\varepsilon \leq a_n - l \leq b_n - l \leq c_n - l \leq \varepsilon,$$

ce qui démontre le résultat. ■

Le cas des limites infinies se traduit comme suit :

Théorème 5.15 *Soient a et b deux suites réelles telles que $\forall n \in \mathbb{N}$, $a_n \leq b_n$. Si a tend vers $+\infty$, alors b aussi. A contrario, si b tend vers $-\infty$, alors a aussi.*

5.3.2 Théorème de la limite monotone

Le théorème suivant est un résultat fondamental d'analyse réelle. Sa preuve repose sur le théorème de la borne supérieure vu dans le chapitre sur le corps des réels.

Théorème 5.16 (Limite monotone) *Soit a une suite réelle supposée croissante. Alors, l'une des deux assertions suivantes est vraie :*
(1) soit a est majorée et a est alors convergente ;
(2) soit a diverge vers $+\infty$.

Preuve. Soit a une suite croissante. Supposons d'abord que a n'est pas majorée, i.e.

$$\forall M \in \mathbb{R}, \exists N \in \mathbb{N}, a_N \geq M.$$

Soit $M > 0$. Il existe alors $N \in \mathbb{N}$, tel que $a_N \geq M$. Mais comme a est croissante, pour tout $n \geq N$, $a_n \geq a_N \geq M$, ce qui, par la Définition 5.7, démontre que a diverge vers $+\infty$ et prouve le point (2). Supposons maintenant que a est majorée. On considère l'ensemble

$$A = \{a_n, n \in \mathbb{N}\}.$$

L'ensemble A est non vide et majoré (car a l'est) et admet donc une borne supérieure que l'on note l. Soit $\varepsilon > 0$ fixé. Par définition de la borne supérieure d'un ensemble, on a

$$\forall x \in A, x \leq l \qquad \text{et} \qquad \exists x \in A, l - \varepsilon < x \leq l.$$

Ceci s'écrit, en termes de la suite a :

$$\forall n \in \mathbb{N}, a_n \leq l \qquad \text{et} \qquad \exists N \in \mathbb{N}, l - \varepsilon < a_N \leq l.$$

Mais comme a est croissante, on a alors que pour tout $n \geq N$,

$$l - \varepsilon \leq a_N \leq a_n \leq l \leq l + \epsilon.$$

Donc $|a_n - l| \leq \varepsilon$ pour tout $n \geq N$ et a converge vers l, ce qui achève la preuve. ■

Nous avons un résultat analogue pour les suites décroissantes.

Corollaire 5.3 *Soit a une suite réelle décroissante. Alors l'une des deux assertions suivantes est vraie :*
(1) soit a est minorée et a est alors convergente ;
(2) soit a diverge vers $-\infty$.

Ce corollaire s'obtient trivialement en appliquant le Théorème 5.16 à la suite croissante $(-a)$. Les suites positives étant naturellement minorées par 0, on obtient immédiatement le corollaire suivant, bien utile en pratique.

Corollaire 5.4 *Soit a une suite réelle décroissante et positive. Alors a est convergente.*

Les applications de ces résultats sont très nombreuses et vous en verrez quelques-unes dans les exercices et problèmes corrigés. Patience ! Mais avant cela, nous vous en proposons immédiatement deux mises en œuvre. La première est élémentaire et fournit un exemplaire d'hypothèse supplémentaire sous laquelle la réciproque du Théorème de Cesàro devient vraie. La seconde, à propos des suites *adjacentes*, est bien plus importante et se verra ainsi réserver toute la sous-section suivante.

Théorème 5.17 (Une *réciproque* au Théorème de Cesàro) *Soit a une suite réelle, avec b sa moyenne de Cesàro et $l \in \mathbb{R} \cup \{+\infty, -\infty\}$. On suppose que a est monotone. On a alors l'équivalence*

$$a \text{ tend vers } l \Leftrightarrow b \text{ tend vers } l.$$

Preuve. L'implication $(\Rightarrow)$ est le Théorème de Cesàro même et ne requiert pas l'hypothèse de monotonie de a. Il n'y a donc que la réciproque $(\Leftarrow)$ à démontrer.

Supposons que b tend vers l et supposons par l'absurde que a ne tend pas vers l. Comme a est monotone, on sait par le Théorème 5.16 et son Corollaire 5.3 que soit a converge, soit a diverge vers $\pm\infty$ et donc a admet une limite $\lambda \in \mathbb{R} \cup \{+\infty, -\infty\}$, différente de l. Mais alors, d'après le Théorème de Cesàro, b a le même comportement que a et tend vers λ, ce qui contredit l'hypothèse de convergence de b vers $l \neq \lambda$. ■

5.3.3 Suites adjacentes

Définition 5.9 *Soient a et b deux suites réelles. On dit que a et b sont adjacentes si*
(1) l'une de ces deux suites est croissante ;
(2) l'autre suite est décroissante ;
(3) la suite $(b - a)$ converge vers 0.

On trouve souvent dans la définition des suites adjacentes la condition supplémentaire suivante : si a est la suite croissante, pour tout $n \in \mathbb{N}$, $a_n \leq b_n$. Cette condition est toutefois une simple conséquence des trois autres conditions. Démontrez-la ! Si vous n'y arrivez pas, ne vous inquiétez pas, elle sera démontrée dans la preuve du Théorème 5.18 ci-après.

Théorème 5.18 (Suites adjacentes) *Soient a et b deux suites réelles adjacentes, avec a la suite croissante. Alors*
(1) a et b convergent vers la même limite l ;
(2) $a_n \leq l \leq b_n$ pour tout $n \in \mathbb{N}$.

Preuve. Comme a est croissante et b décroissante, $b - a$ est décroissante. Si cela n'est pas immédiat pour vous, introduisez la suite $c = b - a$ et étudier le signe de $c_{n+1} - c_n$. Vous voyez mieux maintenant ? Aussi par hypothèse, $b - a$ converge vers 0, ce qui implique que $b - a$ est positive par le Lemme 5.4, i.e. pour tout $n \in \mathbb{N}$, $a_n \leq b_n$.

La suite a est croissante et majorée par b_0 car $a_n \leq b_n \leq b_0$ par décroissance de b. Donc a converge par le Théorème de la limite monotone. Notons l sa limite. Mais puisque $b = (b - a) + a$ et que $b - a$ converge vers 0, on en déduit que b converge et que sa limite est aussi l.

Démontrons maintenant l'encadrement du point (2). Soit $n \in \mathbb{N}$ fixé. Soit $p \geq n$. On a $a_p \leq b_p \leq b_n$, d'où $a_p \leq b_n$ et, en faisant tendre p vers l'infini tout en gardant n fixé, on obtient $l \leq b_n$, pour tout $n \in \mathbb{N}$, ce qui démontre l'inégalité de droite. Toujours pour n fixé, on a pour tout $q \geq n$, $a_n \leq a_q \leq b_q$, d'où $a_n \leq b_q$ et, en faisant tendre cette fois q vers l'infini, on obtient que $a_n \leq l$, ce qui conclut la preuve. ■

On verra deux applications très classiques du Théorème 5.18 dans les exercices 5.6 et 5.7.

5.4 Relations de comparaison

Nous avons déjà introduit la relation d'ordre sur les suites et vous avez pu remarquer que, cet ordre étant partiel, nous pouvions rarement utiliser cet outil. Il existe un autre moyen de comparer les suites et c'est ce que nous vous dévoilons maintenant.

Définition 5.10 *Soient a et b deux suites réelles. On dit que a est* ***dominée*** *par b, ce que l'on écrit $a_n = O(b_n)$, s'il existe une suite réelle bornée u telle qu'il existe $N \in \mathbb{N}$ tel que $\forall n \geq N$, $a_n = u_n b_n$.*

Définition 5.11 *Soient a et b deux suites réelles. On dit que a est* ***négligeable*** *devant b, ce que l'on écrit $a_n = o(b_n)$, s'il existe une suite réelle u convergeant vers 0 telle qu'il existe $N \in \mathbb{N}$ tel que $\forall n \geq N$, $a_n = u_n b_n$.*

Exemple 5.14 *La suite $a = (\frac{1}{n^2})_{n\in\mathbb{N}}$ est négligeable devant la suite $b = (\frac{1}{n})_{n\in\mathbb{N}}$ car pour tout $n \geq 1$,*

$$a_n = \frac{1}{n^2} = \frac{1}{n} \times \frac{1}{n} = \frac{1}{n} b_n,$$

et $\frac{1}{n} \to 0$.

Définition 5.12 *Soient a et b deux suites réelles. On dit que a est* ***équivalente*** *à b, ce que l'on écrit $a_n \sim b_n$, s'il existe une suite réelle u convergeant vers 1 telle qu'il existe $N \in \mathbb{N}$ tel que $\forall n \geq N$, $a_n = u_n b_n$.*

Exemple 5.15 *Les suites u et v définies par $u_n = n$ et $v_n = n + 1$ sont toutes deux divergentes vers $+\infty$. En l'infini, n domine 1 et v_n et u_n sont équivalentes. Pour démontrer cela, il suffit de factoriser par le terme prédominant :*

$$v_n = n + 1 = n(1 + \frac{1}{n}) = u_n(1 + \frac{1}{n}).$$

L'équivalence de u et v découle de la convergence de $(1 + \frac{1}{n})_{n\in\mathbb{N}}$ vers 1.

Notez que si les termes de la suite b sont non nuls à partir d'un certain rang, alors ces définitions peuvent être écrites plus simplement en considérant le rapport de a par b. Par exemple, toujours si les termes de la suite b sont non nuls à partir d'un certain rang N, on a l'équivalence logique :

$$a_n = o(b_n) \Longleftrightarrow \left(\frac{a_n}{b_n}\right)_{n\geq N} \to 0.$$

Par ailleurs, l'équivalence de deux suites est bien une relation d'équivalence, mais les caractères de suite négligeable ou dominée ne sont ni des relations d'ordre ni des relations d'équivalence; toutes les deux sont transitives et la domination est réflexive. Voyez-vous pourquoi la domination n'est pas une relation d'équivalence?

Exemple 5.16 *Rappelez-vous : une relation d'équivalence est binaire, réflexive, transitive et symétrique. Or, pour la domination, il manque la symétrie. En effet, si l'on considère simplement que a est la suite constante égale à 0 et que b est la suite constante égale à 1, alors $a_n = O(b_n)$ mais il est faux d'écrire $b_n = O(a_n)$.*

Théorème 5.19 *Soient a et b deux suites réelles.*
(1) Si $a_n = o(b_n)$, alors $a_n + b_n \sim b_n$.
(2) Si $a_n \sim b_n$, alors $a_n - b_n = o(b_n)$.
(3) Si $a_n = o(b_n)$, alors $a_n = O(b_n)$.
Soient c et d deux autres suites réelles.
(4) Supposons que $a_n \sim b_n$ et $c_n \sim d_n$. Alors $a_nc_n \sim b_nd_n$.

Preuve. La démonstration réutilise simplement les Définitions 5.11 et 5.12.
(1) Si $a_n = o(b_n)$, alors il existe une suite réelle u convergeant vers 0 telle qu'il existe $N \in \mathbb{N}$ tel que $\forall n \geq N$, $a_n = u_nb_n$. Ainsi, pour $n \geq N$, $a_n + b_n = (u_n + 1)b_n$. Comme $(u_n + 1)$ converge vers 1, on peut conclure que $a_n + b_n \sim b_n$.
(2) Si $a_n \sim b_n$, alors il existe une suite réelle u convergeant vers 1 telle qu'il existe $N \in \mathbb{N}$ tel que $\forall n \geq N$, $a_n = u_nb_n$. Ainsi, pour $n \geq N$, $a_n - b_n = (u_n - 1)b_n$. Comme $(u_n - 1)$ converge vers 0, on peut conclure que $a_n - b_n = o(b_n)$.
(3) Nous montrons ici que si a est négligeable devant b, alors a est dominée par b. Si $a_n = o(b_n)$, alors il existe une suite réelle u convergeant vers 0 telle qu'il existe $N \in \mathbb{N}$ tel que $\forall n \geq N$, $a_n = u_nb_n$. Mais, comme u converge, alors u est bornée et donc $a_n = O(b_n)$.
(4) Il existe deux suites réelles u et v convergeant vers 1 telles qu'il existe $N_u \in \mathbb{N}$ et $N_v \in \mathbb{N}$ tel que $\forall n \geq N_u$, $a_n = u_nb_n$ et $\forall n \geq N_v$, $c_n = v_nd_n$. On a alors, pour tout $n \geq \max(N_u, N_v)$, $(ac)_n = (uv)_n(bd)_n$. Comme uv tend vers 1, on conclut que $a_nc_n \sim b_nd_n$.

■

Notons que si les équivalents passent au produit sans problème, on ne peut pas appliquer toutes les opérations usuelles aux équivalents comme on le ferait avec des limites. Pour résumer, et de manière générale, on ne somme pas des équivalents! On ne passe pas aux logarithmes dans des équivalents! ni aux exponentielles d'ailleurs! Des règles spécifiques seront à appliquer dans ces cas-là, comme nous le verrons plus loin.

Exemple 5.17 *Soient a, b et c trois suites telles que $a_n \sim b_n + c_n$. Alors, on n'a pas forcément $a_n - b_n \sim c_n$. Par exemple, si $a_n = n$, $b_n = n$ et $c_n = 1$, on a bien $\frac{a_n}{b_n+c_n} = \frac{n}{n+1} = \frac{1}{1+\frac{1}{n}}$ tend vers 1. Mais la suite nulle $a - b$ n'est pas équivalente à la suite c, constante égale à 1.*

L'exemple ci-dessus encourage fortement à ne regarder que les termes prédominants lorsque l'on étudie les équivalents. Supposons que, dans l'expression $a_n \sim b_n + c_n$, b et c ne sont pas du même ordre. Supposons aussi, pour fixer les idées, que $c_n = o(b_n)$. Il n'est d'aucune utilité de garder le terme négligeable c et il vaut mieux écrire $a_n \sim b_n$.

Théorème 5.20 *Soient a et b des suites réelles.*
(1) Supposons que a et b sont équivalentes. Si a converge vers $l \in \mathbb{R}$ ou si a diverge vers $+\infty$ ou $-\infty$, alors b aussi.
(2) Supposons que a et b convergent vers $l \in \mathbb{R} \setminus \{0\}$. Alors a et b sont équivalentes.

Preuve. Nous nous limitons à la démonstration du *(1)*, la démonstration de l'autre point n'étant pas bien différente et pouvant constituer un bon exercice pour vous. Supposons donc que a et b sont équivalentes. En utilisant la Définition 5.12, il existe une suite réelle u convergeant vers 1 telle qu'il existe $N \in \mathbb{N}$ tel que $\forall n \geq N$, $b_n = u_n a_n$. Alors, si a converge vers l, comme u converge vers 1, b converge vers l par le Théorème 5.5. Si a diverge vers l'infini (disons $+\infty$, l'autre cas étant symétrique), comme u converge vers $1 > 0$, b diverge vers $+\infty$ d'après le Théorème 5.9. ∎

La condition $l \neq 0$ est très importante dans le point *(2)* du Théorème 5.20. Voyez-vous pourquoi ?

Exemple 5.18 *Considérons a et b les suites définies, pour $n > 0$, par $a_n = \frac{1}{n}$ et $b_n = -\frac{1}{n}$. Alors, a et b convergent l'une et l'autre vers 0, mais il est faux de dire qu'elles sont équivalentes. En effet, la suite u de la Définition 5.12 est alors la suite constante valant -1, qui ne converge pas du tout vers 1. Plus généralement, deux suites équivalentes auront toujours le même signe à partir d'un certain rang. Attention ! Nous ne prétendons pas qu'elles seront de signe constant mais nous affirmons simplement que pour chaque n supérieur à un certain N, le signe de a_n est le même que celui de b_n.*

On a alors un bon moyen de comparer de nombreuses suites très simples. Vous verrez aussi en cours des équivalences moins évidentes à démontrer, comme la formule de Stirling, par exemple. Pour l'heure, essayez déjà de montrer que, pour tout réel k, $k^n = o(n!)$. Si vous n'avez pas d'idée, commencez par écrire que $\frac{k^n}{n!} = \frac{k}{1}\frac{k}{2}\cdots\frac{k}{n}$.

Exemple 5.19 *Soit $K = E(2|k|)+1$, où $E(.)$ est la partie entière. Soit $n \in \mathbb{N}$ tel que $n > K$. Alors*

$$\frac{k^n}{n!} = A \prod_{j=K}^{n} \frac{k}{j},$$

où A est le réel $\prod_{j=1}^{K-1} \frac{k}{j}$ ne dépendant pas de n. Alors

$$\left|\frac{k^n}{n!}\right| \leq A \prod_{j=K}^{n} \left|\frac{k}{j}\right| \leq A \prod_{j=K}^{n} \left|\frac{1}{2}\right| \leq A \left(\frac{1}{2}\right)^{n-K+1} \longrightarrow 0.$$

Donc $k^n = o(n!)$.

Les équivalents de suites constituent un outil que vous utiliserez abondamment, il est donc utile d'en connaître quelques règles d'opérations bien commodes.

Théorème 5.21 *Soient a et b deux suites à termes strictement positifs tels que a et b soient équivalentes et convergent vers 0 ou divergent vers l'infini. Alors $\ln(a_n) \sim \ln(b_n)$.*

Preuve. Si a et b divergent vers l'infini, on peut écrire le quotient $\frac{\ln(a_n)}{\ln(b_n)}$ qui est bien défini à partir d'un certain rang. Alors

$$\frac{\ln(a_n)}{\ln(b_n)} = 1 + \frac{\ln(\frac{a_n}{b_n})}{\ln(b_n)}.$$

Le numérateur du quotient de droite converge car a et b sont équivalentes et le dénominateur diverge vers l'infini, donc le quotient converge vers 0. Ainsi $\frac{\ln(a_n)}{\ln(b_n)}$ converge vers 1, ce qui assure que $\ln(a_n) \sim \ln(b_n)$.

Il reste à démontrer le théorème dans le cas où a et b convergent vers 0. Vous avez certainement une idée astucieuse pour le faire rapidement, n'est-ce pas ? Il suffit effectivement d'appliquer le travail déjà effectué au sein de cette démonstration à l'inverse des deux suites. Nous vous laissons le soin de le faire. ■

Il est important de vérifier la condition de convergence vers 0 ou de divergence vers l'infini dans le théorème précédent. Avez-vous un exemple de suites, même convergentes, ne respectant pas cette hypothèse ni la conclusion du théorème ?

Exemple 5.20 *Considérons les suites de terme général $a_n = e^{1/n}$ et $b_n = e^{2/n}$ pour $n \geq 1$. Alors, ces deux suites convergent vers 1 et sont donc équivalentes. En revanche, $\ln(a_n) = \frac{1}{n}$ et $\ln(b_n) = \frac{2}{n}$ ne sont clairement pas équivalentes car leur quotient est constant et égal à $\frac{1}{2}$.*

Après les logarithmes, peut-on dire quelque chose sur les exponentielles ? Oui, c'est le but du théorème suivant.

Théorème 5.22 *Soient a et b deux suites réelles. On a alors l'équivalence logique :*

$$e^{a_n} \sim e^{b_n} \Longleftrightarrow (a_n - b_n) \to 0.$$

Preuve. Supposons que $e^{a_n} \sim e^{b_n}$. Cela signifie, par la Définition 5.12 et par non nullité de e^{b_n}, que $e^{a_n - b_n}$ converge vers 1, donc, en passant au logarithme dans la limite (ce qui contrairement à l'équivalence, a bien un sens), on obtient $(a_n - b_n) \to 0$.

Démontrons l'autre implication. Supposons que $(a_n - b_n) \to 0$. Alors, en passant à l'exponentielle dans la limite, on obtient que $e^{a_n - b_n}$ converge vers 1. Puis, toujours en utilisant la Définition 5.12, on aboutit à $e^{a_n} \sim e^{b_n}$. ■

Là encore, il faut manipuler cet outil avec attention. En particulier, si a et b sont équivalentes, il n'y a pas nécessairement équivalence entre (e^{a_n}) et (e^{b_n}). Trouvez un contre-exemple !

Exemple 5.21 *Pour $n \in \mathbb{N}$, posons $a_n = n + 1$ et $b_n = n$. Alors, a et b sont équivalentes mais leur différence ne tend pas vers 0 puisqu'elle est constante égale à 1. Ainsi, en utilisant le théorème précédent, il n'y aura pas équivalence entre (e^{a_n}) et (e^{b_n}). Pour s'en convaincre encore plus, remarquez simplement que $\frac{e^{a_n}}{e^{b_n}} = e \neq 1$.*

Nous nous arrêtons à ce stade dans ce livre introductif et nous vous laissons le plaisir de mettre en œuvre ces relations plus tard, en cours, dans des études asymptotiques de suites et des développements limités.

5.5 Suites définies par une relation de récurrence

Avant de plonger dans l'étude générale des suites définies par une relation de récurrence $u_{n+1} = f(u_n)$ où f est une application continue, donnons deux exemples classiques de telles suites : les suites arithmétiques et les suites géométriques.

5.5.1 Suites arithmétiques et suites géométriques

Définition 5.13 *Une suite $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ est **arithmétique** s'il existe un réel r, appelé raison de a, tel que le terme général de la suite a est défini par la* *relation de récurrence, pour* $n \in \mathbb{N}$ *:* $a_{n+1} = a_n + r$*. Ceci équivaut à écrire* $a_n = a_0 + nr$*.*

Définition 5.14 *Une suite* $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ *est* ***géométrique*** *s'il existe un réel* r*, appelé raison de* a*, tel que le terme général de la suite* a *est défini par la relation de récurrence, pour* $n \in \mathbb{N}$ *:* $a_{n+1} = ra_n$*. Ceci équivaut à écrire* $a_n = r^n a_0$*.*

Remarque 5.5 *On voit des Définitions 5.13 et 5.14 que les suites arithmétiques correspondent au cas où l'application* f *est la fonction linéaire* $f(x) = x + r$ *et que les suites géométriques correspondent au cas où* $f(x) = r\ x$*. Les suites définies par la relation de récurrence* $a_{n+1} = f(a_n)$ *où* $f(x) = q\ x + r$*, avec* $(q, r) \in \mathbb{R}^2$*, sont appelées suites arithmético-géométriques. Le cas* $q = 1$ *redonne les suites arithmétiques, et le cas* $r = 0$ *redonne les suites géométriques. Mais plus généralement, remarquez que l'étude de ces suites se ramène toujours à celle des suites arithmétiques et géométriques. En effet, supposons que* q *est différent de* 1 *et introduisons* l*, l'unique solution de l'équation* $l = q\ l + r$*, qui n'est rien d'autre que* $l = \frac{r}{1-q}$*. On a alors*

$$a_{n+1} - l = f(a_n) - l = q\ a_n + r - l = q\ a_n + r - ql - r = q\ (a_n - l).$$

La suite auxiliaire b*, définie par* $b_n = a_n - l = a_n - \frac{r}{1-q}$ *pour tout* $n \in \mathbb{N}$*, satisfait alors* $b_{n+1} = q\ b_n$ *et est donc une suite géométrique de raison* q*. Il vous sera alors très simple d'étudier la suite* $a = b + l$ *dès lors que vous saurez étudier* b*.*

Théorème 5.23 (Convergence d'une suite arithmétique) *Soient* $r \in \mathbb{R}$ *et* a *une suite réelle arithmétique de raison* r*. Supposons que* $a_0 > 0$*. Alors,*
(1) si $r = 0$*, la suite est constante ;*
(2) si $r > 0$*, la suite diverge vers* $+\infty$ *;*
(3) si $r < 0$*, la suite diverge vers* $-\infty$*.*

Si les suites arithmétiques n'offrent pas une grande variété de comportements à l'infini comme vous l'avez vu dans le Théorème 5.23, les suites géométriques peuvent converger, diverger vers l'infini ou même diverger grossièrement. Ce comportement dépend évidemment de la raison ; voyez-vous comment ?

Théorème 5.24 (Convergence d'une suite géométrique) *Soient* $r \in \mathbb{R}$ *et* a *une suite réelle géométrique de raison* r*. Alors, si* $a_0 \neq 0$ *:*
(1) si $r \leq -1$*, la suite* a *diverge grossièrement ;*
(2) si $|r| < 1$*, la suite* a *converge vers 0 ;*
(3) si $r = 1$*, la suite* a *est constante ;*
(4) si $r > 1$ *et* $a_0 > 0$*, la suite* a *diverge vers* $+\infty$ *;*
(5) si $r > 1$ *et* $a_0 < 0$*, la suite* a *diverge vers* $-\infty$*.*

Les Théorèmes 5.23 et 5.24 sont vraiment faciles à prouver. Si vous ne voyez pas comment commencer, rappelez-vous que l'on écrit simplement, pour une suite géométrique, $a_n = r^n a_0$. La limite est vite trouvée, non ?

Nous vous faisons à titre d'exemple la démonstration du point (2).

Preuve. Le cas $r = 0$ est trivial. Supposons donc $0 < |r| < 1$. Soit $\varepsilon > 0$ et $n \in \mathbb{N}$. On a les équivalences suivantes :

$$|r^n| \leq \varepsilon \Leftrightarrow |r|^n \leq \varepsilon \Leftrightarrow e^{n \ln |r|} \leq \varepsilon \Leftrightarrow n \ln |r| \leq \ln \varepsilon \Leftrightarrow n \geq \frac{\ln \varepsilon}{\ln |r|}.$$

Pour la dernière inégalité, souvenez-vous que $0 < |r| < 1$ et donc $\ln |r| < 0$. Définissons maintenant $N = \max\left(0, \left[\frac{\ln \varepsilon}{\ln |r|}\right] + 1\right) \in \mathbb{N}$. Alors, pour tout $n \geq N \geq \frac{\ln \varepsilon}{\ln |r|}$, on a $|r^n| \leq \varepsilon$, ce qui prouve le résultat. ■

Un exemple bien connu de suite géométrique apparaît en géométrie fractale dans ce qui est joliment appelé le flocon de Koch. Reportez-vous à l'Exercice 5.8 si vous voulez en savoir plus. Par ailleurs, dans cet exercice, vous aurez besoin de connaître la somme partielle d'une suite géométrique, c'est-à-dire la suite dont le terme général de rang n est la somme des n premiers termes de la suite initiale. Le théorème suivant y pourvoit.

Théorème 5.25 *Soient $r \in \mathbb{R}$ et a une suite réelle géométrique de raison r. Notons A la somme partielle de a, définie pour tout $n \in \mathbb{N}$ par :*

$$A_n = \sum_{k=0}^{n} a_k.$$

Alors

$$A_n = \begin{cases} (n+1)a_0 & \text{si } r = 1 \\ a_0 \frac{1-r^{n+1}}{1-r} & \text{sinon.} \end{cases}$$

Preuve. Le cas $r = 1$ est trivial, tous les termes de la suite a étant égaux à a_0. Nous démontrons l'autre cas et supposons donc que $r \neq 1$. Alors, pour $n \in \mathbb{N}$:

$$\begin{aligned} (1-r)A_n &= a_0 \sum_{k=0}^{n} r^k - a_0 \sum_{k=0}^{n} r^{k+1} \\ &= a_0 \sum_{k=0}^{n} r^k - a_0 \sum_{k=1}^{n+1} r^k \\ &= a_0 \left(r^0 - r^{n+1}\right), \end{aligned}$$

ce qui, en divisant le tout par $(1-r) \neq 0$, prouve le Théorème 5.25. ■

La manipulation, dans la preuve ci-avant, qui permet de passer de deux sommes à deux simples termes est appelée télescopage et est très fréquente dès lors que l'on étudie des sommes partielles. Pensez-y : vous en rencontrerez dans nos exercices ! Plus précisément, si vous avez à étudier une somme de la forme $\sum_{k=m}^{n}(a_{k+1}-a_k)$, pour une suite a quelconque et $m,n\in\mathbb{N}$ avec $m\leq n$, vous pouvez écrire :

$$\begin{array}{rcl}\sum_{k=m}^{n}(a_{k+1}-a_k) & = & \sum_{k=m}^{n}a_{k+1}-\sum_{k=m}^{n}a_k\\ & = & \sum_{k=m+1}^{n+1}a_k-\sum_{k=m}^{n}a_k\\ & = & \left(a_{n+1}+\sum_{k=m+1}^{n}a_k\right)-\left(a_m+\sum_{k=m+1}^{n}a_k\right)\\ & = & a_{n+1}-a_m+\sum_{k=m+1}^{n}(a_k-a_k)=a_{n+1}-a_m.\end{array}$$

À votre avis, est-il possible de démontrer un résultat semblable au Théorème 5.25 pour les suites arithmétiques ? La réponse est oui.

Théorème 5.26 *Soient $r\in\mathbb{R}$ et a une suite réelle arithmétique de raison r. Notons A la somme partielle de a, définie pour tout $n\in\mathbb{N}$ par :*

$$A_n=\sum_{k=0}^{n}a_k.$$

Alors

$$A_n=(n+1)\left(a_0+\frac{nr}{2}\right).$$

Preuve. On remarque simplement que

$$A_n=\sum_{k=0}^{n}(a_0+kr)=(n+1)a_0+r\sum_{k=0}^{n}k.$$

Or, vous savez certainement que $\sum_{k=0}^{n}k=\frac{n(n+1)}{2}$, ce qui conclut la démonstration. Si vous n'êtes pas convaincu par cette dernière équation, notez alors que

$$\begin{array}{rcl}2\sum_{k=0}^{n}k & = & \sum_{k=0}^{n}k+\sum_{k=0}^{n}(n-k)\\ & = & \sum_{k=0}^{n}n=n(n+1).\end{array}$$

Dans la première ligne, vous aurez simplement écrit $\sum_{k=0}^{n}k$ de deux manières distinctes, une fois telle quelle et l'autre en inversant l'ordre des termes de la somme. ■

5.5.2 Suites récurrentes et applications continues

Soient I un intervalle non vide de $\mathbb{R}$, f une application de I dans I et $\lambda\in I$. Il existe alors une unique suite a telle que $a_0=\lambda$ et $a_{n+1}=f(a_n)$, pour tout $n\in\mathbb{N}$. L'objet de cette sous-section est d'étudier la convergence de a sous différentes hypothèses sur f (continuité, monotonie). Mais avant d'entamer cette étude, rappelons brièvement ce qu'est une application continue.

Définition 5.15 *Soit f une application d'un intervalle $I \subset \mathbb{R}$ dans $\mathbb{R}$. Soit $a \in I$. On dit que f est continue en a si et seulement si*

$$\forall \varepsilon > 0, \exists \eta > 0, \forall x \in I, |x - a| < \eta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

En français, cela peut se lire de la manière suivante : pour toute erreur $\varepsilon > 0$ que l'on se donne, aussi petite soit-elle, on peut trouver un voisinage de a, tel que pour tout point x dans ce voisinage, son image $f(x)$ est à moins de ε de l'image $f(a)$ de a. Remarquez que ce voisinage n'est rien d'autre que l'intervalle $]a - \eta, a + \eta[$ dans la Définition 5.15.

Revenons à notre problème d'étude de la convergence des suites récurrentes, et commençons par nous intéresser au cas où la suite $(a_n)_{n\in\mathbb{N}}$ converge vers $a \in I$. Que peut-on dire sur sa limite ?

Théorème 5.27 *Soient f une application définie d'un intervalle non vide $I \subset \mathbb{R}$ dans $\mathbb{R}$ et $a \in I$ tels que f soit continue en a. Soit $(a_n)_{n\in\mathbb{N}}$ une suite réelle qui converge vers a et telle que pour tout $n \in \mathbb{N}$, $a_n \in I$. Alors, $\big(f(a_n)\big)_{n\in\mathbb{N}}$ converge vers $f(a)$.*

Preuve. Soit $\varepsilon > 0$. Comme f est continue en a, il existe $\eta > 0$ tel que pour tout $x \in I$ tel que $|x - a| < \eta$, on a $|f(x) - f(a)| < \varepsilon$.

Mais aussi, comme $\lim_{n\to\infty} a_n = a$, il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$, $|a_n - a| < \eta$. Et comme $a_n \in I$, on obtient alors que pour tout $n \geq N$, $|f(a_n) - f(a)| < \varepsilon$. ■

On déduit le corollaire suivant caractérisant la limite d'une suite a convergente définie par une relation de récurrence de la forme $a_{n+1} = f(a_n)$ sous l'hypothèse importante de continuité de f.

Corollaire 5.5 *Soient $I \subset \mathbb{R}$ un segment non vide et f une application continue de I dans $f(I) \subset I$. Soit $(a_n)_{n\in\mathbb{N}}$ une suite définie par $a_{n+1} = f(a_n)$ pour tout $n \in \mathbb{N}$ et telle que $a_0 \in I$. Supposons que $(a_n)_{n\in\mathbb{N}}$ converge vers a. Alors a est un point fixe de l'application f, c'est à dire que $f(a) = a$.*

Remarque 5.6 *Notons au passage que l'hypothèse que I est un segment et non un intervalle quelconque est importante. Elle garantit que la limite a appartient encore à I et on peut donc appliquer le Théorème 5.27.*

On voit que l'ensemble des points fixes de f joue un rôle important dans l'étude de la convergence de a. En effet, le Corollaire 5.5 nous permet déjà de conclure qu'une condition nécessaire pour que a converge est que l'ensemble E des points fixes de f, défini par

$$E = \{x \in I \mid f(x) = x\},$$

soit non vide. On peut alors déduire un critère simple sous lequel ces suites récurrentes divergent vers l'infini.

Corollaire 5.6 *Soient $I \subset \mathbb{R}$ un segment non vide et f une application continue de I dans $f(I) \subset I$ telle que $f(x) > x$ pour tout $x \in I$. Soit $(a_n)_{n\in\mathbb{N}}$ une suite définie par $a_{n+1} = f(a_n)$ pour tout $n \in \mathbb{N}$ et telle que $a_0 \in I$. Alors a diverge vers $+\infty$.*

Preuve. Pour cela, montrez que la suite a est croissante et non majorée. Faîtes-le !

Il suffit d'écrire $u_{n+1} - u_n = f(u_n) - u_n > 0$ pour tout $n \in \mathbb{N}$. Donc a est croissante. Par le Théorème de la limite monotone, soit a est majorée et auquel cas elle converge, soit a diverge vers $+\infty$. Si a est majorée, sa limite est un point fixe de f. Mais E est vide, f n'ayant aucun point fixe car $f(x) > x$ pour tout $x \in I$. Donc a n'est pas majorée et diverge vers $+\infty$. ∎

Exemple 5.22 *Choisissons $f(x) = e^x$ qui satisfait naturellement $f(x) > x$ pour tout $x \in \mathbb{R}$. Pour tout $\lambda \in \mathbb{R}$, la suite a^λ, définie par $a_0^\lambda = \lambda$ et $a_{n+1}^\lambda = e^{a_n^\lambda}$ pour tout $n \in \mathbb{N}$, diverge vers $+\infty$. Il en est de même pour la suite $b_{n+1} = b_n + \frac{1}{b_n^2}$ pour tout $n \in \mathbb{N}$ et $b_0 > 0$. À vous de nous dire pourquoi !*

Évidemment, la réciproque du Corollaire 5.5 est fausse, dans le sens où l'existence d'un point fixe de f n'implique pas forcément que la suite récurrente a converge !

Exemple 5.23 *Pour s'en convaincre doublement, considérons une fonction f avec non pas un mais deux points fixes : $f(x) = x^2$, qui admet 0 et 1 pour points fixes. Définissons ensuite les suites récurrentes a et b par : $a_0 = \frac{1}{2}$, $a_{n+1} = f(a_n)$, $b_0 = 2$ et $b_{n+1} = f(b_n)$ pour tout $n \in \mathbb{N}$. Cela revient à écrire : $\forall n \in \mathbb{N}$, $a_n = \frac{1}{2^{2^n}}$ et $b_n = 2^{2^n}$. Alors, a converge certes vers 0, point fixe de f, mais b diverge vers $+\infty$. La Figure 5.2 donne une intuition de la convergence de a vers 0.*

Affranchissons-nous maintenant de l'hypothèse de convergence de a. Vous verrez qu'il est possible de conclure à la convergence ou à la divergence de a si l'application f est supposée non seulement continue mais aussi monotone sur I. Comme dans le Corollaire 5.5 et l'Exemple 5.22, l'idée sous-jacente est que la monotonie de f implique celle de a et le Théorème de la limite monotone jouera alors un rôle important dans l'étude du comportement asymptotique de a. Les détails de cette étude dépassent le cadre de l'introduction que nous voulons vous donner sur les suites et nous vous laissons donc un peu de surprise pour la prochaine rentrée scolaire. Néanmoins, le lemme suivant est un

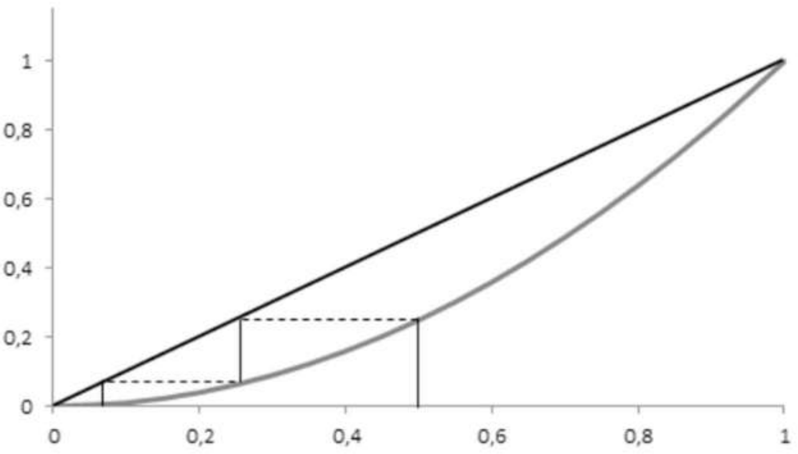

FIGURE 5.2 – Convergence de a vers 0.

avant-goût des ingrédients qui vous seront nécessaires pour mener à bien cette étude.

Lemme 5.7 *Soit a une suite récurrente définie par $a_0 \in I$ et $\forall n \in \mathbb{N}, a_{n+1} = f(a_n)$ où f est une application monotone de I, intervalle de $\mathbb{R}$, dans $f(I) \subset I$. Alors :*

(i) si f est croissante, a est monotone, et a est croissante si et seulement si $f(a_0) \geq a_0$;

(ii) si f est décroissante, les suites extraites $(a_{2n})_{n\in\mathbb{N}}$ et $(a_{2n+1})_{n\in\mathbb{N}}$ sont monotones de monotonies contraires, et $(a_{2n})_{n\in\mathbb{N}}$ est croissante si et seulement si $f\big(f(a_0)\big) \geq a_0$.

Preuve. Commençons par le point *(i)*. Pour tout $n \geq 1$, on a $a_{n+1} - a_n = f(a_n) - f(a_{n-1})$, et par croissance de f, le signe de $f(a_n) - f(a_{n-1})$ est le même que celui de $a_n - a_{n-1}$. Par récurrence, on voit alors que le signe de $a_{n+1} - a_n$ est celui de $a_1 - a_0$, pour tout $n \in \mathbb{N}$, ce qui permet de conclure.

Démontrons maintenant le point *(ii)*. Comme suggéré par le résultat, introduisons la fonction composée $g = f \circ f$. Comme f est décroissante, g est croissante (oui oui ! Si vous avez un doute, vérifiez-le en prenant $x \leq y$ et en comparant $g(x)$ à $g(y)$). Introduisons les sous-suites $b_n = a_{2n}$ et $c_n = a_{2n+1}$, pour tout $n \in \mathbb{N}$. On a alors

$$\forall n \in \mathbb{N}, \qquad b_{n+1} = a_{2n+2} = f(a_{2n+1}) = f\big(f(a_{2n})\big) = g(a_{2n}) = g(b_n)$$

et

$$\forall n \in \mathbb{N}, \qquad c_{n+1} = a_{2n+3} = f(a_{2n+2}) = f\big(f(a_{2n+1})\big) = g(a_{2n+1}) = g(c_n).$$

Comme g est croissante et satisfait aussi $g(I) \subset I$, on conclut grâce au point (i) que b et c sont monotones. En particulier b est croissante si et seulement si $f\big(f(a_0)\big) = g(b_0) \geq b_0 = a_0$ et comme f est décroissante, cela équivaut à $g(c_0) \leq c_0$ qui est aussi équivalent à la décroissance de c par *(i)*. ∎

S'il est facile d'imaginer comment le cas où f est croissante sera utilisé en pratique, le cas où f est décroissante est plus abstrus. Pour éclaircir le problème, considérons ce cas où f décroît et introduisons, comme dans la preuve ci-avant, la fonction $g = f \circ f$ et la sous-suite d'indices pairs b et celle d'indices impairs c. Remarquez d'abord que tous les points fixes de f sont aussi points fixes de g. En effet, si l est un point fixe de f, alors $g(l) = f\big(f(l)\big) = f(l) = l$. Donc tout ce que vous verrez dans le cas f croissante pourra s'appliquer indépendamment aux suites extraites b et c. Souvenez-vous ensuite du Théorème 5.12. Les comportements asymptotiques de b et c vous donneront des informations sur la convergence de la suite a. Voici un tel exemple d'application :

Exemple 5.24 *Supposons que $I = [\alpha, \beta]$ est un segment de $\mathbb{R}$ et f une application de I dans I, continue et décroissante. On définit les suites a, b et c par $a_0 \in I$ et $a_{n+1} = f(a_n)$, $b_n = a_{2n}$ et $c_n = a_{2n+1}$ pour tout $n \in \mathbb{N}$. Par l'illustre Théorème des valeurs intermédiaires, on sait que f admet un point fixe $l \in I$. L'ensemble E_g des points fixes de la fonction $g = f \circ f$ contient l selon la discussion ci-avant et est donc non-vide. Supposons de plus que E_g soit un singleton : $E_g = \{l\}$. Comme b et c sont monotones par le Lemme 5.7 et bornées car appartenant au segment $[\alpha, \beta]$, elles convergent par le Théorème de la limite monotone et leurs limites sont égales, car toutes deux égales à l'unique point fixe l de g, par le Corollaire 5.5. Cela prouve donc que la suite a converge aussi vers l, d'après le Théorème 5.12.*

L'exemple est-il clair ? Si ce n'est pas le cas, relisez-le bien autant de fois que nécessaire ! N'hésitez pas à vous reporter aux différents résultats auxquels il se réfère. C'est une bonne opportunité pour les méditer un peu plus.

Dernier point, mais non des moindres, un autre résultat important d'analyse réelle, connu sous le nom de Théorème du point fixe, garantit que des suites récurrentes convergent, sous une hypothèse différente pour la fonction f. Nous ne vous en disons pas plus pour le moment : faites le problème 5.3 pour de plus abondants détails.

5.6 Exercices

5.6.1 Suites extraites

Exercice 5.1 *Soit $a \in \mathbb{R}^{\mathbb{N}}$ telle que $(a_{2n})_{n\in\mathbb{N}}$, $(a_{2n+1})_{n\in\mathbb{N}}$ et $(a_{3n})_{n\in\mathbb{N}}$ convergent. Montrer que a converge.*

Exercice 5.2 *Montrer que la suite $(\sin n)_{n\in\mathbb{N}}$ diverge grossièrement.*

5.6.2 Applications du Théorème de Cesàro et Généralisations

Exercice 5.3 (Moyenne de Cesàro généralisée) *On fixe une suite $a = (a_n)_{n\in\mathbb{N}}$ de réels strictement positifs telle que la suite A, définie par $A_n = \sum_{k=0}^{n} a_k$ pour tout $n \in \mathbb{N}$, tend vers $+\infty$. On peut alors associer à une suite u donnée, la suite $v = (v_n)_{n\in\mathbb{N}}$ de ses moyennes barycentriques selon la suite a, définie par :*

$$v_n = \frac{1}{A_n}\sum_{k=0}^{n} a_k u_k \qquad \text{pour tout } n \in \mathbb{N}.$$

Montrer que si u tend vers $l \in \mathbb{R} \cup \{-\infty, \infty\}$, alors v aussi.

Remarque 5.7 *Le Théorème de Cesàro est un cas particulier du résultat ci-dessus : il suffit de définir la suite a comme étant la suite constante égale à 1. Dans ce cas,*

$$A_n = \sum_{k=0}^{n} 1 = n + 1$$

diverge bien vers $+\infty$ et on obtient le Théorème de Cesàro tel qu'il est énoncé dans le cours.

Exercice 5.4 *On suppose que $a \in \mathbb{R}^{\mathbb{N}}$ est une suite réelle à termes strictement positifs et converge vers $l \in \mathbb{R}^+$.*

(a) Montrer que la suite de terme général $\left(\prod_{k=1}^{n} a_k\right)^{\frac{1}{n}}$ converge et déterminer sa limite.

(b) Montrer que la suite de terme général $\left(\prod_{k=1}^{n} a_k^k\right)^{\frac{1}{n^2}}$ converge et déterminer sa limite.

Exercice 5.5 (Théorème de Stolz-Cesàro) *Cet exercice donne un critère de convergence du quotient de deux suites et fournit une généralisation du Théorème de Cesàro.*

(a) Soient a et b deux suites réelles telles que b est une suite strictement croissante et non majorée et telles que la limite $\lim_{n\to\infty} \frac{a_{n+1}-a_n}{b_{n+1}-b_n}$ *existe et est finie. Notons alors l cette limite. Montrer que la suite* $\left(\frac{a_n}{b_n}\right)_{n\in\mathbb{N}}$ *converge vers l.*

(b) Montrer que le Théorème de Cesàro (dans le cas d'une limite réelle uniquement) est un cas particulier du résultat ci-dessus.

5.6.3 Application des suites adjacentes

Exercice 5.6 (Définition et irrationalité de e) *Soient a et b les suites de termes généraux*

$$a_n = \sum_{k=0}^{n} \frac{1}{k!} \qquad \text{et} \qquad b_n = a_n + \frac{1}{n \cdot n!}.$$

(a) Montrer que a et b convergent vers la même limite. Cette limite commune n'est rien d'autre que le nombre e, mais cela est admis pour le moment.

(b) Les sous-questions suivantes visent à vous aider à démontrer que e est irrationnel.

(b.1) Montrer que pour tout $n \in \mathbb{N}$*, il existe* $u_n \in \mathbb{N}$ *tel que* $a_n = \frac{u_n}{n!}$.

(b.2) En déduire que pour tout $n > 1$, $u_n < e\, n! < u_n + \frac{1}{n}$.

(b.3) Conclure que $e \notin \mathbb{Q}$ *en raisonnant par l'absurde.*

Exercice 5.7 (Théorème des segments emboîtés) *Soient deux suites réelles, a et b, satisfaisant les trois propriétés suivantes :*

(1) pour tout $n \in \mathbb{N}$, $a_n \leq b_n$ *;*

(2) pour tout $n \in \mathbb{N}$, $[a_{n+1}, b_{n+1}] \subset [a_n, b_n]$ *;*

(3) la suite $(b - a)$ *tend vers* 0.

Montrer que

(a) l'ensemble $\bigcap_{n\in\mathbb{N}} [a_n, b_n]$ *est un singleton ;*

(b) le résultat ci-dessus ne reste pas vrai si les segments $[a_n, b_n]$ *sont remplacés par des intervalles ouverts* $]a_n, b_n[$.

5.6.4 Suites récurrentes

Exercice 5.8 (Flocon de Koch) *Le flocon de Koch est une figure géométrique définie de manière récursive. Nous partons d'une figure* K_0 *qui consiste en un simple triangle équilatéral de côtés de longueur* $L > 0$*. Supposons définie la figure* K_n*, où* $n \in \mathbb{N}$*. Alors* K_{n+1} *est obtenue en faisant subir à* K_n *la transformation suivante :*

(1) chaque segment de la figure K_n est coupé en trois parties égales : $[AB]$, $[BC]$ et $[CD]$;
(2) les deux parties extrêmes, $[AB]$ et $[CD]$, restent inchangées ;
(3) deux segments apparaissent de sorte à former un triangle équilatéral BCE pointant vers l'extérieur de la figure ;
(4) la partie centrale, $[BC]$, est effacée.
Notons P la suite dont le terme général, P_n, est le périmètre de K_n et notons S la suite dont le terme général, S_n, est la superficie de K_n, pour $n \in \mathbb{N}$. Les suites P et S convergent-elles ?

5.6.5 Relations de comparaison

Exercice 5.9 *Nous avons déjà vu dans le cours que $k^n = o(n!)$, pour tout $k \in \mathbb{R}$. Nous étendons ici ce résultat et démontrons des relations de comparaison entre certaines suites usuelles.*
(1) Soit u une suite réelle telle que $\frac{u_{n+1}}{u_n}$ converge vers $0 \leq l < 1$. Montrer que u converge vers 0.
(2) Soient $0 \leq a < 1$, $b < 0$, $c > 0$ et $d > 1$. Montrer que
(2-i) $a^n = o(n^b)$,
(2-ii) $n^c = o(d^n)$,
(2-iii) $n! = o(n^n)$.

5.7 Problèmes corrigés

Problème 5.1 (Série harmonique) *Le but de ce problème est d'étudier la série harmonique. Soit $s_n = \frac{1}{n}$ et S sa somme partielle, c'est-à-dire $S_n = \sum_{k=1}^{n} \frac{1}{k}$ pour tout $n \geq 1$. Nous allons déterminer un développement asymptotique de la suite S.*
(1) Montrez que S diverge vers $+\infty$. Pour cela montrez d'abord que, pour tout $n \geq 1$, $\ln(n+1) \leq S_n$.
(2) Montrez que $S_n \sim \ln(n)$.
(3) Montrez que $\big(S_n - \ln(n)\big)_{n \geq 1}$ converge vers un certain $\gamma \in \mathbb{R}$. On appelle constante d'Euler ce γ.

Problème 5.2 (Th. de Bolzano-Weierstrass) *Dans ce problème, vous allez pouvoir démontrer le Théorème 5.10, lequel affirme que toute suite réelle bornée admet une sous-suite convergente. Introduisons donc une suite réelle a bornée. Notons $I = \{n \in \mathbb{N}, \forall p > n, a_p \geq a_n\}$.*

(1) Supposons que I est infini. Montrer que a admet une sous-suite convergente.

(2) Supposons que I est fini. Montrer que a admet une sous-suite convergente.

La démonstration de ces deux points suffit pour démontrer le Théorème de Bolzano-Weierstrass.

Problème 5.3 (Suites de Cauchy et point fixe) *Avant d'énoncer le théorème du point fixe, introduisons la notion de suite de Cauchy. On dit que $a \in \mathbb{R}^{\mathbb{N}}$ est une suite de Cauchy si et seulement si*

$$\forall \varepsilon > 0, \quad \exists\, N \in \mathbb{N}, \quad \forall p \geq N, \quad \forall k \geq 0, \quad |a_{p+k} - a_p| \leq \varepsilon.$$

Cela peut se réécrire de manière équivalente de la manière suivante :

$$\forall \varepsilon > 0, \quad \exists\, N \in \mathbb{N}, \quad \forall p \geq N, \quad \forall q \geq N, \quad |a_q - a_p| \leq \varepsilon.$$

Intuitivement cela veut dire que les termes de la suite a se rapprochent uniformément les uns des autres en l'infini. Cette uniformité est davantage précisée par l'équivalence qui suit :

$$a \in \mathbb{R}^{\mathbb{N}} \text{ est de Cauchy si et seulement si } \lim_{n\to\infty} \sup_{p,q \geq n} |a_q - a_p| = 0.$$

Remarquez l'ordre des quantificateurs dans les définitions ci-dessus. L'uniformité de la convergence (c'est le suprémum des différences qui converge vers 0) est d'une importance cruciale. Le rang N ne dépend que de l'erreur ε et l'inégalité doit alors être vérifiée pour tous les p et q au delà du rang N simultanément.

(1-i) Démontrer que toute suite convergente est de Cauchy.

(1-ii) Démontrer que toute suite de Cauchy est bornée.

Dans $\mathbb{R}$, la réciproque de (1-i) est vraie.

(2) En utilisant le Théorème de Bolzano-Weierstrass, démontrer le théorème suivant :

Théorème 5.28 *Une suite réelle converge si et seulement si elle est de Cauchy.*

Munis de ce théorème, vous êtes désormais armé pour démontrer le Théorème du point fixe :

Théorème 5.29 (Théorème du point fixe) *On suppose que I est un intervalle fermé non vide de $\mathbb{R}$ et que $f : I \to I$ est une application contractante, i.e.*

$$\exists\, k \in [0,1[\quad \text{tel que} \quad \forall x \in I,\ \forall y \in I,\ |f(x) - f(y)| \leq k\,|x - y|.$$

Alors f admet un unique point fixe l, et toute suite a définie par $a_0 \in I$ et $a_{n+1} = f(a_n)$, pour tout $n \in \mathbb{N}$, converge vers ce point fixe l.

Pour cela, nous vous proposons le cheminement suivant. On se donne f et a quelconques, comme dans le théorème.
(3-i) Démontrer que, pour tout $n \in \mathbb{N}$, $|a_{n+1} - a_n| \leq k^n |a_1 - a_0|$.
(3-ii) En déduire que la suite a est de Cauchy et qu'elle converge donc. Notons l sa limite.
(3-iii) Montrer finalement que l est l'unique point fixe de f.

5.8 Solution des exercices

Solution 5.1 (de l'exercice 5.1) *Soient a une suite et l_1, l_2 et l_3 les limites respectives de ses sous-suites $(a_{2n+1})_{n\in\mathbb{N}}$, $(a_{2n})_{n\in\mathbb{N}}$ et $(a_{3n})_{n\in\mathbb{N}}$. $(a_{6n})_{n\in\mathbb{N}}$ est une suite extraite de $(a_{2n})_{n\in\mathbb{N}}$, donc elle converge vers l_2 par le Théorème 5.11. Elle est aussi une suite extraite de $(a_{3n})_{n\in\mathbb{N}}$, donc elle converge vers l_3. Par unicité de la limite, $l_2 = l_3$.*

De même, en utilisant $(a_{6n+3})_{n\in\mathbb{N}}$, extraite à la fois de $(a_{2n+1})_{n\in\mathbb{N}}$ et de $(a_{3n})_{n\in\mathbb{N}}$, on trouve que $l_1 = l_3$. Alors $l_1 = l_2$ et le Théorème 5.12 permet de conclure que la suite a converge.

Solution 5.2 (de l'exercice 5.2) *Si vous n'avez aucune idée de la manière par laquelle résoudre cet exercice, nous vous suggérons de raisonner par l'absurde et de penser à utiliser les relations trigonométriques.*

Si vous n'avez aucun souvenir de ces relations, une petite piqûre de rappel s'impose. Soient $(a, b) \in \mathbb{R}^2$. Il vous suffit de retenir cette première formule

$$\sin(a + b) = \sin(a)\cos(b) + \cos(a)\sin(b) \tag{5.3}$$

pour en retrouver plusieurs. Notamment, en se souvenant que cos *est une fonction paire et* sin *une fonction impaire, on obtient en remplaçant b par $(-b)$ dans (5.3)*

$$\sin(a - b) = \sin(a)\cos(b) - \cos(a)\sin(b). \tag{5.4}$$

En sommant (5.3) et (5.4), on a aussi

$$2\sin(a)\cos(b) = \sin(a + b) + \sin(a - b). \tag{5.5}$$

Finalement, en posant $u = a + b$ et $v = a - b$, i.e. $a = \frac{u+v}{2}$ et $b = \frac{u-v}{2}$, l'équation (5.5) se réécrit, pour tout $(u, v) \in \mathbb{R}^2$

$$\sin(u) + \sin(v) = 2\sin\left(\frac{u+v}{2}\right)\cos\left(\frac{u-v}{2}\right). \tag{5.6}$$

Une fois ce petit rappel bien assimilé (et ces formules retenues une bonne fois pour toutes !), retournez démontrer que $(\sin n)_{n\in\mathbb{N}}$ *diverge.*

La fonction sin *étant bornée par* 1*, la divergence vers* $\pm\infty$ *est automatiquement écartée. Donc, soit la suite converge vers un réel, soit elle diverge grossièrement. Supposons par l'absurde qu'elle converge vers* $l \in \mathbb{R}$*. En utilisant la formule (5.6) avec* $u = n+2$ *et* $v = n$*, on obtient*

$$\sin(n+2) + \sin(n) = 2\sin(n+1)\cos(1), \qquad \forall n \in \mathbb{N}.$$

Comme $(\sin n)_{n\in\mathbb{N}}$ *est supposée converger vers* l*, toutes ses sous-suites convergent aussi vers* l*. En passant alors à la limite dans l'équation ci-avant, on obtient*

$$l + l = 2\ l\cos 1.$$

Ceci se simplifie en $l(1-\cos 1) = 0$*, i.e.* $l = 0$ *ou* $\cos 1 = 0$*. Mais* $\cos 1$ *ne peut pas valoir* 0 *car la fonction* cos *est strictement décroissante sur* $[0, \frac{\pi}{2}]$ *et donc* $0 = \cos(\frac{\pi}{2}) < \cos(1) < \cos(0) = 1$*. Ceci prouve que* $l = 0$*. Mais alors, comme d'après (5.3)*

$$\sin(n+1) = \sin(n)\cos(1) + \cos(n)\sin(1), \qquad \forall n \in \mathbb{N}$$

et comme $\sin(1) \neq 0$*, cela prouve que la suite* $(\cos n)_{n\in\mathbb{N}}$ *converge aussi vers* 0*. Mais il est bien connu que* $\sin^2(n) + \cos^2(n) = 1$*, pour tout* $n \in \mathbb{N}$*. Donc, par passage à la limite dans cette égalité, on obtient que* $0 = 1$ *; ce qui est absurde. Donc,* $(\sin n)_{n\in\mathbb{N}}$ *diverge.*

Vous pouvez vous amuser à démontrer que la suite $(\cos n)_{n\in\mathbb{N}}$ *diverge en usant des mêmes techniques. Pour vous aider, nous récapitulons d'autres formules de trigonométrie qui peuvent vous être utiles et qui, de toute manière, sont à connaître.*

Soit $(a,b) \in \mathbb{R}^2$*. Il vous suffit encore de retenir la formule suivante :*

$$\cos(a+b) = \cos(a)\cos(b) - \sin(a)\sin(b). \tag{5.7}$$

Les autres en découlent simplement. On obtient, en remplaçant b *par* $(-b)$ *dans (5.7),*

$$\cos(a-b) = \cos(a)\cos(b) + \sin(a)\sin(b). \tag{5.8}$$

En sommant (5.7) et (5.8), on a aussi

$$2\cos(a)\cos(b) = \cos(a+b) + \cos(a-b). \tag{5.9}$$

En prenant la différence entre (5.8) et (5.7), on obtient

$$2\sin(a)\sin(b) = \cos(a-b) - \cos(a+b). \tag{5.10}$$

Finalement, en posant $u = a + b$ *et* $v = a - b$, *i.e.* $a = \frac{u+v}{2}$ *et* $b = \frac{u-v}{2}$, *l'équation (5.9) se réécrit, pour tout* $(u, v) \in \mathbb{R}^2$

$$\cos(u) + \cos(v) = 2\cos\left(\frac{u+v}{2}\right)\cos\left(\frac{u-v}{2}\right). \tag{5.11}$$

À vous de jouer maintenant ! Montrez que $(\cos n)_{n\in\mathbb{N}}$ *diverge.*

Solution 5.3 (de l'exercice 5.3) *Nous démontrons séparément le cas d'une limite* l *finie du cas où elle est infinie.*

Cas $l \in \mathbb{R}$ *: On commence par le cas où* u *converge vers* $l \in \mathbb{R}$ *et on se donne* $\varepsilon > 0$. *On sait qu'il existe* $N_1 \in \mathbb{N}$ *tel que pour tout* $n \geq N_1$, $|u_n - l| \leq \frac{\varepsilon}{2}$. *Soit donc* $n \geq N_1$. *Suivons pas à pas les idées utilisées dans la preuve du Théorème de Cesàro.*

$$\begin{aligned}
|v_n - l| &= \Big|\frac{1}{A_n}\sum_{k=0}^{n} a_k u_k - l\Big| = \Big|\frac{1}{A_n}\sum_{k=0}^{n} a_k u_k - l\frac{1}{A_n}\sum_{k=0}^{n} a_k\Big| \\
&= \Big|\frac{1}{A_n}\sum_{k=0}^{N} a_k(u_k - l)\Big| \leq \frac{1}{A_n}\sum_{k=0}^{N} a_k|u_k - l|,
\end{aligned}$$

où la dernière inégalité est une application de l'inégalité triangulaire (souvenez-vous que a *est à termes strictement positifs). Pour contrôler* $|v_n - l|$, *on découpe à nouveau la somme ci-dessus en deux.*

$$\begin{aligned}
|v_n - l| &\leq \frac{1}{A_n}\Big(\sum_{k=0}^{N_1-1} a_k|u_k - l| + \sum_{k=N_1}^{n} a_k|u_k - l|\Big) \\
&\leq \frac{1}{A_n}\Big(\sum_{k=0}^{N_1-1} a_k|u_k - l| + \frac{\varepsilon}{2}\sum_{k=N_1}^{n} a_k\Big).
\end{aligned}$$

Comme les termes a_k *sont tous strictement positifs, on a* $\sum_{k=N_1}^{n} a_k \leq A_n$. *Aussi, la somme* $\sum_{k=0}^{N_1-1} a_k|u_k - l|$ *est une constante indépendante de* n, *que l'on va noter* C. *On a alors*

$$|v_n - l| \leq \frac{C}{A_n} + \frac{\varepsilon}{2}.$$

Finalement, comme A *tend vers* $+\infty$, *la suite* $\left(\frac{C}{A_n}\right)_{n\in\mathbb{N}}$ *converge vers* 0. *Il existe donc* $N \geq N_1$ *tel que pour tout* $n \geq N$, $0 \leq \frac{C}{A_n} \leq \frac{\varepsilon}{2}$. *On a ainsi démontré que pour tout* $n \geq N$,

$$|v_n - l| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Ceci achève la preuve du cas d'une limite finie.

Cas $l \in \{+\infty, -\infty\}$ ***:*** *Il suffit de démontrer le cas $l = +\infty$, l'autre découlant trivialement de celui-ci en considérant la suite $(-u)$. Supposons donc que u diverge vers $+\infty$. Soit $M > 0$. Il existe alors $N_1 \in \mathbb{N}$ tel que pour tout $n \geq N_1$, $u_n \geq M + 1$. On a alors*

$$\begin{aligned} v_n &= \frac{1}{A_n} \sum_{k=0}^{N_1-1} a_k u_k + \frac{1}{A_n} \sum_{k=N_1}^{n} a_k u_k \geq \frac{1}{A_n} \sum_{k=0}^{N_1-1} a_k u_k + \frac{M+1}{A_n} \sum_{k=N_1}^{n} a_k \\ &\geq (M+1) + \frac{1}{A_n} \left(\sum_{k=0}^{N_1-1} a_k u_k - (M+1) \sum_{k=0}^{N_1-1} a_k \right). \end{aligned}$$

La constante $C = \sum_{k=0}^{N_1-1} a_k u_k - (M+1) \sum_{k=0}^{N_1-1} a_k$ ne dépend pas de n et $\frac{C}{A_n}$ tend vers 0. Il existe donc $N \geq N_1$ tel que pour tout $n \geq N$, $\frac{C}{A_n} \geq -1$. Finalement, pour tout $n \geq N$,

$$v_n \geq (M+1) + \frac{C}{A_n} \geq (M+1) - 1 = M,$$

ce qui prouve que v diverge aussi vers $+\infty$.

Solution 5.4 (de l'exercice 5.4) ***(a)*** *Soit b la suite de terme général $b_n = \ln(a_n)$ pour $n \in \mathbb{N}$. Par continuité du logarithme et car a converge vers $l > 0$, on peut affirmer que b converge vers $\ln(l)$. Alors, par le Théorème de Cesàro, la suite de terme général $\frac{1}{n} \sum_{k=1}^{n} b_k$ converge aussi vers $\ln(l)$. Donc, la suite c de terme général $c_n = \exp\left(\frac{1}{n} \sum_{k=1}^{n} b_k\right)$ converge par continuité de la fonction exponentielle et sa limite vaut l. Or, pour $n \in \mathbb{N}$,*

$$c_n = \exp\left(\frac{1}{n} \sum_{k=1}^{n} \ln(a_k)\right) = \left(\prod_{k=1}^{n} a_k\right)^{\frac{1}{n}},$$

qui est simplement le terme général de la suite dont nous cherchons le comportement. Nous avons donc répondu à la question.

(b) *Comme pour* ***(a)****, vous devez avoir le réflexe de passer à l'exponentielle dès lors que vous vous retrouvez face à des quantités du type $a^x = e^{x \ln a}$, avec $a > 0$.*

$$\begin{aligned} \left(\Pi_{k=1}^{n} a_k^k\right)^{\frac{1}{n^2}} &= \exp\left(\tfrac{1}{n^2} \ln\left(\Pi_{k=1}^{n} a_k^k\right)\right) \\ &= \exp\left(\tfrac{1}{n^2} \sum_{k=1}^{n} \ln(a_k^k)\right) \\ &= \exp\left(\tfrac{1}{n^2} \sum_{k=1}^{n} k \ln(a_k)\right). \end{aligned}$$

La somme dans l'exposant de l'exponentielle ressemble beaucoup à la somme introduite dans l'exercice 5.3, n'est-ce pas ? Introduisons donc la suite $b_k = k$

dont la somme partielle est donnée par $B_n = \frac{n(n+1)}{2}$. *On écrit alors*

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

Comme $\ln(a)$ *converge vers* $\ln(l)$, b *est à termes strictement positifs et* B *tend vers l'infini, on conclut alors que* $\frac{1}{B_n}\sum_{k=1}^{n} b_k \ln(a_k)$ *converge aussi vers* $\ln(l)$, *par le résultat de l'exercice 5.3. Finalement,*

$$\left(\Pi_{k=1}^{n} a_k^k\right)^{\frac{1}{n^2}} = \exp\left(\frac{n(n+1)}{2n^2}\frac{1}{B_n}\sum_{k=1}^{n} b_k \ln(a_k)\right)$$

converge vers $e^{\frac{1}{2}\ln(l)} = \sqrt{l}$, *par continuité de la fonction exponentielle.*

Solution 5.5 (de l'exercice 5.5) *(a) Soient* a *et* b *deux suites réelles telles que* b *est une suite strictement croissante et non majorée et* $\lim_{n\to\infty} \frac{a_{n+1}-a_n}{b_{n+1}-b_n} = l \in \mathbb{R}$ *existe. Soit* $\varepsilon > 0$. *Il existe alors* $N \in \mathbb{N}$ *tel que pour tout* $p \geq N$,

$$l - \varepsilon \leq \frac{a_{p+1} - a_p}{b_{p+1} - b_p} \leq l + \varepsilon.$$

Comme $b_{p+1} - b_p > 0$ *par stricte croissance de* b, *on a, pour tout* $p \geq N$,

$$(l-\varepsilon)(b_{p+1} - b_p) \leq a_{p+1} - a_p \leq (l+\varepsilon)(b_{p+1} - b_p).$$

On se donne maintenant $n \geq N$ *et on somme les inégalités ci-dessus pour tout* p *entre* N *et* n. *Cela donne*

$$(l-\varepsilon)(b_{n+1} - b_N) \leq a_{n+1} - a_N \leq (l+\varepsilon)(b_{n+1} - b_N). \tag{5.12}$$

Ces inégalités sont-elles mystérieuses pour vous ? Souvenez-vous du petit rappel sur les sommes télescopiques :

$$\sum_{p=N}^{n}(b_{p+1} - b_p) = (b_{n+1} - b_n) + (b_n - b_{n-1}) + \cdots + (b_{N+1} - b_N).$$

Tous les termes se simplifient sauf ceux des deux extrémités, à savoir b_{n+1} *et* b_N. *Si vous estimez qu'avec des* $\cdots$, *on ne peut pas appeler cela une démonstration, c'est tout à votre honneur de rédiger la preuve plus convenablement. Pensez à découper la somme et réarrangez les termes. Pour tout* $n \geq N$, *on a*

$$\begin{aligned}\sum_{p=N}^{n}(b_{p+1} - b_p) &= \sum_{p=N}^{n} b_{p+1} - \sum_{p=N}^{n} b_p = \sum_{p=N+1}^{n+1} b_p - \sum_{p=N}^{n} b_p \\ &= \left(b_{n+1} + \sum_{p=N+1}^{n} b_p\right) - \left(b_N + \sum_{p=N+1}^{n} b_p\right) = b_{n+1} - b_N.\end{aligned}$$

Retournons maintenant à notre démonstration. Nous en étions aux inégalités (5.12). Comme b est strictement croissante et non majorée, on sait par le Théorème de la limite monotone que b tend vers $+\infty$. Il existe donc un rang $N_1 \in \mathbb{N}$ tel que pour tout $n \geq N_1$, $b_{n+1} > 0$. Il nous est alors permis de diviser par b_{n+1} et on obtient, pour tout $n \geq \max(N_1, N)$,

$$(l-\varepsilon)\Big(1-\frac{b_N}{b_{n+1}}\Big) \leq \frac{a_{n+1}}{b_{n+1}} - \frac{a_N}{b_{n+1}} \leq (l+\varepsilon)\Big(1-\frac{b_N}{b_{n+1}}\Big).$$

Cela se réécrit, pour tout $n \geq \max(N_1, N)$,

$$(l-\varepsilon)\Big(1-\frac{b_N}{b_{n+1}}\Big) + \frac{a_N}{b_{n+1}} \leq \frac{a_{n+1}}{b_{n+1}} \leq (l+\varepsilon)\Big(1-\frac{b_N}{b_{n+1}}\Big) + \frac{a_N}{b_{n+1}}.$$

Souvenez-vous alors que N est fixé et que b diverge vers $+\infty$. Vous pouvez donc conclure que $\left(\frac{a_n}{b_n}\right)_{n\in\mathbb{N}}$ converge vers l.

Comment pouvez-vous maintenant utiliser ce résultat pour démontrer le Théorème de Cesàro dans le cas d'une limite réelle ?

***(b)** On se donne une suite réelle $(u_n)_{n\in\mathbb{N}}$ qui converge vers $l \in \mathbb{R}$. Soit V sa moyenne de Cesàro, i.e.*

$$V_n = \frac{1}{n+1}\sum_{k=0}^{n} u_k, \qquad \forall n \in \mathbb{N}.$$

Voyez-vous apparaître les suites a et b du résultat précédent ? Réfléchissez bien avant de lire la suite de la solution !

Il suffit de définir $b_n = n+1$ et $a_n = \sum_{k=0}^{n} u_k$ pour tout $n \in \mathbb{N}$. On a alors $V_n = \frac{a_n}{b_n}$ et

$$\frac{a_{n+1}-a_n}{b_{n+1}-b_n} = \frac{u_{n+1}}{1} = u_{n+1} \to l \in \mathbb{R} \quad \textit{quand} \quad n \to +\infty.$$

Donc $\lim_{n\to\infty} V_n = \lim_{n\to\infty} \frac{a_n}{b_n} = l$. Ce qui achève la démonstration du Théorème de Cesàro.

Solution 5.6 (de l'exercice 5.6) ***(a)** La suite a est clairement strictement croissante. Soit $n \in \mathbb{N}$.*

$$\begin{aligned} b_{n+1} - b_n &= a_{n+1} + \frac{1}{(n+1)(n+1)!} - a_n - \frac{1}{nn!} \\ &= \frac{1}{(n+1)!} + \frac{1}{(n+1)(n+1)!} - \frac{1}{nn!} \\ &= \frac{n(n+1)+n-(n+1)^2}{n(n+1)(n+1)!} = \frac{-1}{n(n+1)(n+1)!} < 0. \end{aligned}$$

Donc b est strictement décroissante. De plus, pour tout $n \in \mathbb{N}$, $b_n - a_n = \frac{1}{nn!}$. La suite $(b - a)$ tend alors clairement vers 0 et les suites a et b sont donc adjacentes. D'après le Théorème 5.18, elles convergent vers une même limite, qui est e, d'après l'énoncé.

(b) Pour démontrer le point (b.1), il suffit de réduire la somme $a_n = \sum_{k=0}^{n} \frac{1}{k!}$ au même dénominateur. Ce dénominateur commun n'est rien d'autre que $n!$, car chaque terme de la somme s'écrit

$$\frac{1}{k!} = \frac{1}{1 \times \cdots \times k} = \frac{(k+1) \times \cdots \times n}{1 \times \cdots \times k \times \cdots \times n} = \frac{(k+1) \times \cdots \times n}{n!}$$

et on peut réécrire

$$a_n = \sum_{k=0}^{n} \frac{1}{k!} = \frac{1}{n!} \sum_{k=0}^{n} \frac{n!}{k!} = \frac{1}{n!} \sum_{k=0}^{n} \prod_{i=k+1}^{n} i.$$

On pose $u_n = \sum_{k=0}^{n} \prod_{i=k+1}^{n} i$, pour tout $n \in \mathbb{N}$. On a alors pour tout $n \in \mathbb{N}$, $u_n \in \mathbb{N}$ et $a_n = \frac{u_n}{n!}$.

Montrons (b.2), i.e. $\forall n > 1$, $u_n < e\, n! < u_n + \frac{1}{n}$. Comme a et b sont adjacentes de limite commune e, que a est strictement croissante et que b est strictement décroissante, le Théorème 5.18 guarantit que pour tout $n \in \mathbb{N}$,

$$a_n < a_{n+1} \leq e \leq b_{n+1} < b_n.$$

Cela implique que $\frac{u_n}{n!} < e < \frac{u_n}{n!} + \frac{1}{nn!}$. Remarquez les inégalités strictes qui résultent de la stricte monotonie des suites a et b. Il suffit alors de multiplier par $n!$ pour obtenir les inégalités demandées.

Nous pouvons maintenant montrer que e est irrationnel. Pour cela, raisonnons par l'absurde comme proposé à la question (b.3) et supposons que $e \in \mathbb{Q}$. Il existe donc des entiers p et q tels que $e = \frac{p}{q}$. Et d'après (b.2) appliqué à $n = q$, $u_q < \frac{p}{q}\, q! < u_q + \frac{1}{q}$, i.e.

$$u_q < p\,(q-1)! < u_q + \frac{1}{q} \leq u_q + 1.$$

Cela implique que l'entier $p\,(q-1)!$ est strictement (c'est ici où vous pouvez vous rendre compte de l'importance des inégalités strictes à la question précédente !) compris entre les deux entiers consécutifs u_q et $u_q + 1$, ce qui est évidemment absurde. D'où $e \notin \mathbb{Q}$.

Solution 5.7 (de l'exercice 5.7) *(a) Les hypothèses impliquent que a et b sont des suites adjacentes, la croissance de a et décroissance de b découlant du* *fait que les segments sont emboîtés, par l'hypothèse (2). Par le Théorème 5.18, elles convergent vers la même limite $l \in \mathbb{R}$, et pour tout $n \in \mathbb{N}$, $a_n \leq l \leq b_n$. La seconde assertion peut se réécrire*

$$l \in \bigcap_{n\in\mathbb{N}} [a_n, b_n].$$

Cela prouve que l'ensemble $\bigcap_{n\in\mathbb{N}}[a_n, b_n]$ est non vide. Montrons maintenant qu'il est réduit à l'élément l. Soit $x \in \bigcap_{n\in\mathbb{N}}[a_n, b_n]$. On a alors, pour tout $n \in \mathbb{N}$, $a_n \leq x \leq b_n$ et, par passage à la limite, on obtient

$$l \leq x \leq l.$$

Cela implique évidemment que $x = l$ et prouve que $\bigcap_{n\in\mathbb{N}}[a_n, b_n] = \{l\}$ est bien un singleton.

***(b)** Dans ce théorème, l'hypothèse que les intervalles (a_n, b_n) sont des segments (c'est-à-dire des intervalles fermés et bornés) est cruciale. Considérons par exemple la suite d'intervalles ouverts $I_n =]1 - \frac{1}{n}, 1[$, pour tout $n \geq 1$. Toutes les autres hypothèses du théorème sont satisfaites et pourtant, dans ce cas, on a $\bigcap_{n\in\mathbb{N}} I_n = \emptyset$.*

Solution 5.8 (de l'exercice 5.8) *Intéressons-nous d'abord au périmètre du flocon de Koch, dont vous pouvez voir la construction sur la Figure 5.3. Le passage de K_n à K_{n+1}, pour $n \in \mathbb{N}$ consiste à passer de trois segments égaux, $[AB]$, $[BC]$ et $[CD]$, à quatre segments de même longueur : $[AB]$, $[BE]$, $[EC]$ et $[CD]$. Le périmètre est donc multiplié par $\frac{4}{3}$ à chaque itération. P est donc une suite géométrique de raison $\frac{4}{3} > 1$ et $P_0 = 3L > 0$, donc, d'après le Théorème 5.24, la suite P diverge vers $+\infty$.*

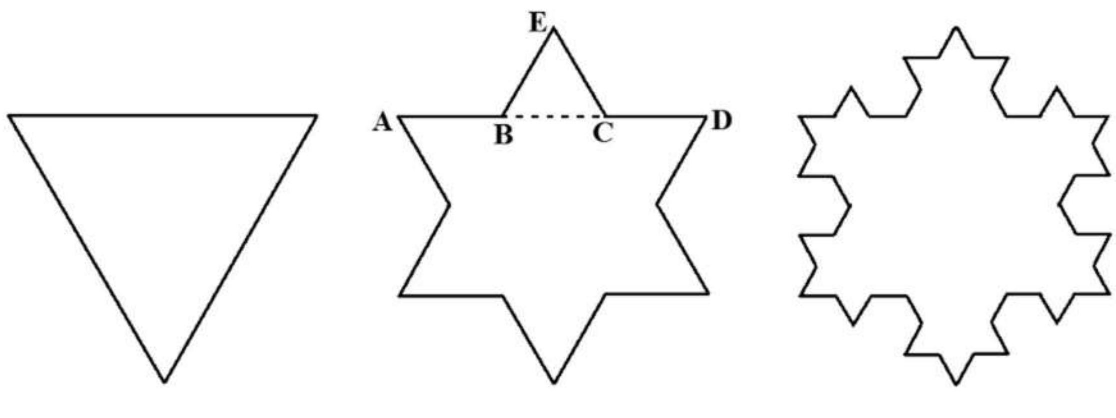

FIGURE 5.3 – K_0, K_1 et K_2. À vous de dessiner K_n, pour $n \geq 3$!

Avant de nous intéresser à la superficie du flocon de Koch, notons que, pour $n \in \mathbb{N}$, la figure K_n est composée de segments ayant tous la même longueur, à *savoir* L_n. *Plus précisément,* $L_n = \frac{L}{3^n}$ *et* L *est une suite géométrique de raison* $\frac{1}{3}$ *qui converge donc vers 0 d'après le Théorème 5.24. Par ailleurs, le nombre de segments de longueur* L_n *formant* K_n *est simplement* $N_n = \frac{P_n}{L_n} = 3 \times 4^n$.

Pour $n \in \mathbb{N}$, *la superficie de* K_{n+1} *est la superficie de* K_n *à laquelle il faut ajouter la superficie de* N_{n+1} *triangles équilatéraux de côtés de longueur* L_{n+1}. *Une simple application du théorème de Pythagore vous permettra de trouver que la superficie d'un triangle équilatéral de côtés de longueur* L_{n+1} *vaut* $\frac{\sqrt{3}L_{n+1}^2}{8}$. *Ainsi*

$$S_{n+1} = S_n + N_{n+1}\frac{\sqrt{3}L_{n+1}^2}{8} = S_n + \frac{3\sqrt{3}L^2}{8}\left(\frac{4}{9}\right)^{n+1}.$$

Notons $T = \frac{3\sqrt{3}L^2}{8}$. *Alors*

$$S_n = S_0 + T\sum_{k=0}^{n-1}\left(\frac{4}{9}\right)^{k+1} = S_0 + T\frac{\left(\frac{4}{9}\right) - \left(\frac{4}{9}\right)^{n+1}}{1 - \left(\frac{4}{9}\right)}.$$

Comme $\left|\frac{4}{9}\right| < 1$, *la superficie converge et sa limite vaut*

$$S_0 + T\frac{4}{5} = \frac{\sqrt{3}L^2}{8}\left(1 + \frac{12}{5}\right).$$

Remarquez que cette figure vous a permis de délimiter une surface finie non nulle grâce à un trait de longueur infinie.

Solution 5.9 (de l'exercice 5.9) *(1) Soit* $\varepsilon = \frac{1-l}{2} > 0$. *Il existe* $N \in \mathbb{N}$ *tel que, pour tout* $n \geq N$, $\left|\frac{u_{n+1}}{u_n} - l\right| \leq \varepsilon$. *Alors,* $0 < \frac{u_{n+1}}{u_n} \leq l + \varepsilon = \frac{1+l}{2} < 1$ *pour tout* $n \geq N$. *Donc, pour tout* $n \geq N$,

$$u_{n+1} \leq \frac{1+l}{2}u_n.$$

En procédant par récurrence à partir de ces inégalités, nous obtenons, pour tout $p \in \mathbb{N}$,

$$0 < u_{N+p} \leq \left(\frac{1+l}{2}\right)^p u_N.$$

Souvenez-vous que N *est fixé et que la suite géométrique* $\left(\frac{1+l}{2}\right)^p$ *tend vers* 0 *quand* $p \to +\infty$ *car* $0 < \frac{1+l}{2} < 1$. *Il ne reste plus qu'à faire tendre* p *vers l'infini pour conclure.*

(2-i) Soit $u_n = \frac{a^n}{n^b}$ *pour tout* $n \in \mathbb{N}$. *On a*

$$\frac{u_{n+1}}{u_n} = \frac{a^{n+1}n^b}{(n+1)^b a^n} = a\left(\frac{n}{n+1}\right)^b,$$

qui tend clairement vers a, avec $0 \leq a < 1$. Donc u tend vers 0 selon la première partie de l'exercice ou, autrement dit, $a^n = o(n^b)$.

(2-ii) *On utilise la même idée et on définit $u_n = \frac{n^c}{d^n}$. On a*

$$\frac{u_{n+1}}{u_n} = \frac{d^n(n+1)^c}{n^c d^{n+1}} = \frac{1}{d}\left(1+\frac{1}{n}\right)^c,$$

qui tend vers $\frac{1}{d}$, avec $0 < \frac{1}{d} < 1$. La question (1) permet de conclure à nouveau.

(2-iii) *Considérons maintenant $u_n = \frac{n!}{n^n}$. On a*

$$\frac{u_{n+1}}{u_n} = \frac{(n+1)!}{(n+1)^{n+1}}\frac{n^n}{n!} = (n+1)\frac{n^n}{(n+1)^{n+1}} = \left(\frac{n}{n+1}\right)^n.$$

Il faut faire très attention ici quant au calcul de la limite de $\left(\frac{n}{n+1}\right)^n$. La forme $1^{+\infty}$ est indéterminée et non égale à 1. Le calcul doit se faire comme suit :

$$\left(\frac{n}{n+1}\right)^n = \left(\frac{1}{1+\frac{1}{n}}\right)^n = \frac{1}{\left(1+\frac{1}{n}\right)^n}$$

et l'on écrit alors

$$\left(1+\frac{1}{n}\right)^n = e^{n\ln\left(1+\frac{1}{n}\right)}.$$

Souvenez-vous maintenant de vos limites usuelles :

$$\lim_{x\to 0^+}\frac{\ln(1+x)}{x} = 1$$

et donc $n\ln\left(1+\frac{1}{n}\right)$ tend vers 1, car $\frac{1}{n}$ tend vers 0. On en déduit alors, par continuité de l'exponentielle, que $\left(1+\frac{1}{n}\right)^n$ tend vers $e^1 = e$. Finalement, $\frac{u_{n+1}}{u_n}$ tend vers $0 < \frac{1}{e} < 1$. On conclut donc que $u_n = \frac{n!}{n^n}$ tend vers 0, ou encore $n! = o(n^n)$.

5.9 Solution des problèmes corrigés

Solution 5.10 (du problème 5.1) *La technique utilisée dans cette correction est très classique et connue sous le nom de comparaison série-intégrale. Vous reviendrez dessus en détail en cours, mais retenez pour le moment qu'elle est applicable lorsque l'on s'intéresse au comportement d'une somme partielle d'une suite dont le terme général est de la forme $f(k)$ où f est monotone. La* *somme* $\sum_{k=1}^{n} f(k)$ *est alors comparable à l'intégrale* $\int_1^n f(x)dx$, *mais l'étude de l'intégrale peut s'avérer beaucoup plus simple que celle de la somme.*

(1) Remarquons d'abord que S *est strictement croissante comme somme partielle d'une suite à termes strictement positifs. Donc, par le Théorème de la limite monotone, soit* S *converge soit elle diverge vers* $+\infty$.

La somme partielle $S_n = \sum_{k=1}^{n} \frac{1}{k}$ *est de la forme ci-dessus avec* $f(x) = \frac{1}{x}$ *qui est décroissante sur* $\mathbb{R}^{+*}$. *Une primitive de* f *est donnée par la fonction logarithme qui apparaît dans l'inégalité que l'on vous suggère de démontrer. Essayons donc de mettre en œuvre la comparaison série-intégrale. Soit* $k \in \mathbb{N}^*$ *et* $k \leq x \leq k+1$. *On a alors* $\frac{1}{k+1} \leq \frac{1}{x} \leq \frac{1}{k}$. *On intègre entre* k *et* $k+1$ *et on obtient, pour tout* $k \geq 1$,

$$\frac{1}{k+1} = \int_k^{k+1} \frac{dx}{k+1} \leq \int_k^{k+1} \frac{dx}{x} \leq \int_k^{k+1} \frac{dx}{k} = \frac{1}{k}.$$

Cela donne

$$\frac{1}{k+1} \leq \ln(k+1) - \ln(k) \leq \frac{1}{k}.$$

Soit $n \in \mathbb{N}^*$. *On somme ces inégalités pour* k *allant de* 1 *à* n. *En remarquant que la somme au centre est télescopique, on obtient :*

$$\sum_{k=1}^{n} \frac{1}{k+1} \leq \ln(n+1) \leq \sum_{k=1}^{n} \frac{1}{k} = S_n.$$

Comme $\ln(n+1)$ *diverge vers* $+\infty$, *il en est de même pour* S_n.

(2) Reprenons l'inégalité démontrée ci-dessus : $\sum_{k=1}^{n} \frac{1}{k+1} \leq \ln(n+1) \leq S_n$. *La première somme n'est rien d'autre que* $S_{n+1} - 1$, *donc*

$$S_{n+1} - 1 \leq \ln(n+1) \leq S_n.$$

Cela implique que, pour tout $n \in \mathbb{N}^*$, $\ln(n+1) \leq S_n \leq \ln(n) + 1$. *Alors, pour tout* $n \geq 2$,

$$\frac{\ln(n+1)}{\ln(n)} \leq \frac{S_n}{\ln(n)} \leq 1 + \frac{1}{\ln(n)}.$$

Les suites $\frac{\ln(n+1)}{\ln(n)}$ *et* $1 + \frac{1}{\ln(n)}$ *tendent clairement vers* 1. *Le Théorème des gendarmes prouve alors que* $\frac{S_n}{\ln(n)}$ *tend aussi vers* 1, *ce qui prouve que* $S_n \sim \ln(n)$.

(3) Soit $u_n = S_n - \ln(n)$. *Montrons que* u *converge. Nous savons déjà que pour tout* $n \geq 1$, $\ln(n+1) \leq S_n \leq S_{n+1}$, *et donc, pour tout* $n \geq 2$, $\ln(n) \leq S_n$.

Notons que cette inégalité est clairement vérifiée pour $n = 1$ et donc $(u_n)_{n\geq 1}$ est positive (et donc minorée par 0). Montrons que u est décroissante. Par le Théorème de la limite monotone, cela démontrera que u est convergente. Soit $n \geq 1$.

$$u_{n+1} - u_n = \frac{1}{n+1} - \ln(n+1) + \ln(n) = \frac{1}{n+1} + \ln\left(1 - \frac{1}{n+1}\right).$$

Mais pour tout $x > -1$, $\ln(1+x) \leq x$. Avec $x = -\frac{1}{n+1} > -1$, on a alors $u_{n+1} - u_n \leq 0$, ce qui démontre bien la décroissance de u et achève la preuve. La limite de la suite $\Big(S_n - \ln(n)\Big)_{n\geq 1}$ est généralement notée γ et est appelée constante d'Euler.

Solution 5.11 (du problème 5.2) ***(1)*** *Si I est infini, nous pouvons indexer ses éléments par $\mathbb{N}$, autrement dit, il existe une sous-suite de a, que nous notons $(a_{\phi(k)})_{k\in\mathbb{N}}$, avec ϕ une fonction strictement croissante, telle que $\forall k \in \mathbb{N}$, $\phi(k) \in I$. Alors, par définition de I, pour tout $k \in \mathbb{N}$, comme $\phi(k+1) > \phi(k)$, $a_{\phi(k+1)} \geq a_{\phi(k)}$. Ainsi, $(a_{\phi(k)})_{k\in\mathbb{N}}$ est une suite croissante. Par ailleurs, comme a est bornée, $(a_{\phi(k)})_{k\in\mathbb{N}}$ est aussi bornée et a fortiori majorée. Étant croissante et majorée, la suite $(a_{\phi(k)})_{k\in\mathbb{N}}$ converge.*

(2) *Si I est fini, alors I possède un élément maximum, que nous notons N. Posons $\phi(0) = N + 1$. Ainsi, $\phi(0) \notin I$ et, par définition de I, il existe $\phi(1) > \phi(0)$ tel que $a_{\phi(1)} < a_{\phi(0)}$ et, comme $\phi(1) > \phi(0) > N$, $\phi(1) \notin I$. Nous construisons alors par récurrence une sous-suite $(a_{\phi(k)})_{k\in\mathbb{N}}$ décroissante. En effet, pour tout $k \in \mathbb{N}$, tel que $\phi(k) \notin I$, il existe $\phi(k+1) > \phi(k)$ tel que $a_{\phi(k+1)} < a_{\phi(k)}$ et $\phi(k+1) \notin I$: la relation de récurrence est claire grâce à la définition de I et nous l'avons déjà démontrée pour n_0 ; nous avons donc construit une sous-suite décroissante de a. Par ailleurs, cette sous-suite est bornée donc a fortiori minorée. Ainsi, la suite $(a_{\phi(k)})_{k\in\mathbb{N}}$ converge.*

Solution 5.12 (du problème 5.3) ***(1-i)*** *Soient $(a_n)_{n\in\mathbb{N}}$ une suite convergente de limite $l \in \mathbb{R}$ et $\varepsilon > 0$. Alors, $\exists N \in \mathbb{N}$, $\forall p \geq N$, $|a_p - l| \leq \frac{\varepsilon}{2}$. Soit $k \geq 0$. On a alors, par l'inégalité triangulaire, pour tout $p \geq N$ et $k \geq 0$,*

$$|a_{p+k} - a_p| = |(a_{p+k} - l) - (a_p - l)| \leq |a_{p+k} - l| + |a_p - l| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

ce qui prouve bien que a est de Cauchy.

(1-ii) *Soit $(a_n)_{n\in\mathbb{N}}$ une suite de Cauchy. Choisissons $\varepsilon = 1$ dans la définition. Alors $\exists N \in \mathbb{N}$, $\forall p \geq N$, $\forall k \geq 0$, $|a_{p+k} - a_p| \leq 1$. En particulier, en choisissant $p = N$, on a, pour tout $k \geq 0$, $|a_{N+k} - a_N| \leq 1$, ce qui implique que $|a_{N+k}| \leq |a_N| + 1$, encore par l'inégalité triangulaire ! Croyez-nous, il vaut mieux bien la* *retenir et penser souvent à l'utiliser. Vous pouvez maintenant voir que, pour tout $p \in \mathbb{N}$,*

$$|a_p| \leq \max\left(\max_{0\leq k\leq N} |a_k|, |a_N| + 1\right),$$

ce qui démontre que la suite a est bornée puisque le terme de droite ne dépend pas de p. Ces quelques manipulations des suites de Cauchy étant assimilées, vous pouvez démontrer à présent le Théorème du point fixe.

(2) *On a déjà démontré à la question (1-i) que toute suite convergente est de Cauchy. Il ne reste donc plus qu'une implication à prouver.*

Soit a une suite réelle de Cauchy. Montrons que a converge. Comme a est une suite de Cauchy, a est bornée d'après la question (1-ii). Par le théorème de Bolzano-Weierstrass, on peut en extraire alors une sous-suite qui converge. Il existe donc une application $\phi : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que la suite extraite $(u_{\phi(n)})_{n\in\mathbb{N}}$ converge vers un certain $l \in \mathbb{R}$. Soit $\varepsilon > 0$. Il existe alors $N_1 \in \mathbb{N}$ tel que pour tout $n \geq N_1$,

$$|u_{\phi(n)} - l| \leq \varepsilon.$$

Mais, comme u est de Cauchy, il existe $N_2 \in \mathbb{N}$ tel que pour tout $p \geq q \geq N_2$, $|u_p - u_q| \leq \varepsilon$. En particulier, comme ϕ est strictement croissante, on peut prendre $q = n$ et $p = \phi(n) \geq n$ pour obtenir que pour tout $n \geq N_2$,

$$|u_n - u_{\phi(n)}| \leq \varepsilon.$$

Il ne reste plus qu'à utiliser l'inégalité triangulaire pour obtenir que, pour tout $n \geq \max(N_1, N_2)$,

$$|u_n - l| = |u_n - u_{\phi(n)} + u_\phi(n) - l| \leq |u_n - u_{\phi(n)}| + |u_\phi(n) - l| \leq 2\varepsilon,$$

ce qui prouve bien que u converge vers l.

(3-i) *Nous montrons l'inégalité demandée par récurrence. Pour $n = 0$, l'assertion est trivialement vérifiée, car $k^0 = 1$ et donc $|a_1 - a_0| \leq k^0|a_1 - a_0|$. Supposons maintenant que l'assertion soit vraie à un rang n. On a alors*

$$|a_{n+2} - a_{n+1}| = |f(a_{n+1}) - f(a_n)| \leq k|a_{n+1} - a_n| \leq kk^n|a_1 - a_0| = k^{n+1}|a_1 - a_0|$$

qui est exactement l'assertion au rang $n+1$. Donc, pour tout $n \in \mathbb{N}$, $|a_{n+1} - a_n| \leq k^n|a_1 - a_0|$.

(3-ii) *Soit $\varepsilon > 0$, $p \in \mathbb{N}$ et $m \in \mathbb{N}$. On a*

$$\begin{aligned}
|a_{p+m} - a_p| &= \left| \sum_{n=p}^{p+m-1} a_{n+1} - a_n \right| \leq \sum_{n=p}^{p+m-1} |a_{n+1} - a_n| \\
&= \sum_{n=p}^{p+m-1} k^n |a_1 - a_0| = k^p \frac{1-k^m}{1-k} |a_1 - a_0| \\
&\leq \frac{k^p}{1-k} |a_1 - a_0|,
\end{aligned}$$

où la première inégalité résulte encore d'une application de l'inégalité triangulaire, et la dernière égalité n'est rien d'autre que la formule de somme de m termes consécutifs d'une suite géométrique.

Remarquez que le majorant $\frac{k^p}{1-k}|a_1 - a_0|$ ne dépend pas de m et converge donc uniformément en m vers 0 lorsque p tend vers l'infini car $0 \leq k < 1$, par le théorème 5.24. On en déduit donc que la suite a est de Cauchy. Elle converge donc par le Théorème admis dans l'énoncé. Notons l sa limite.

(3-iii) *Comme $a_n \in I$ pour tout $n \in \mathbb{N}$ et comme I est fermé, la limite l de a appartient aussi à I. On peut alors utiliser le Théorème 5.27 pour conclure que $f(l) = l$, i.e. l est un point fixe de f. Supposons maintenant par l'absurde que f admette deux points fixes différents l et l'. On a alors*

$$0 < |l - l'| = |f(l) - f(l')| \leq k|l - l'|.$$

Mais comme $k < 1$, cela implique forcément que $l = l'$. Absurde ! Donc l est l'unique point fixe de f.

Quelques conseils pour réussir en prépa

Voilà un titre bien ambitieux et ceci pour plusieurs raisons. Tout d'abord, à travers une enquête réalisée auprès d'anciens préparationnaires ayant intégré des écoles prestigieuses, nous avons pu constater que des étudiants appliquant des méthodes différentes avaient des résultats similaires, ce qui rend illégitimes certains conseils trop pressants. L'exemple le plus flagrant est le temps travaillé : des bourreaux de travail, misant sur une connaissance très approfondie des programmes, peuvent très bien être meilleurs, ou moins bons, que des élèves faisant le pari d'une vie saine dans laquelle l'heure du coucher est érigée en règle immuable. Les premiers auront plus de savoir, mais seront moins lucides et efficaces que les seconds. Pour vous, il s'agit de trouver l'équilibre qui vous convient. Autrement dit, vous devez adapter à votre personnalité les conseils que nous pourrions donner. Néanmoins, certains d'entre eux sont valables pour tous et cela justifie les quelques propositions que nous faisons pour mieux travailler.

« Réussir en prépa » : voilà l'autre raison de l'audace de ce court chapitre, tant cela recouvre de nombreuses notions. Nous avons essayé de les regrouper par thème, en allant du plus général (la vie en prépa) au plus particulier (travailler son intuition en mathématiques), en passant par des considérations d'efficacité quant à l'organisation du travail.

Bien vivre le passage en prépa

Anticipez !

En entrant en classe préparatoire, vous devez être conscient de la grande différence de niveau demandé par rapport au lycée. Cela signifie qu'il faut travailler davantage, mais aussi que vous pouvez vous rassurer en anticipant cette transition, qui, en fin de compte, n'est pas insurmontable. C'est d'ailleurs l'objet de ce livre. N'hésitez pas à regarder ainsi ce qui est demandé en mathématiques dans des ouvrages comme celui-ci : vous y apprendrez une méthode plus évoluée que celle que vous utilisiez jusqu'au baccalauréat et vous découvrirez de nouveaux concepts qui risquent de transformer la vision quelque peu calculatoire que l'on peut parfois avoir des mathématiques avant les études supérieures.

« La plus grande gloire n'est pas de ne jamais tomber, mais de se relever à chaque chute. » - Confucius

Une fois les premières semaines de prépa passées, vous risquez de mal vivre le premier devoir, avec éventuellement une note très basse par rapport à ce que vous connaissiez en terminale. Ne désespérez pas, mais utilisez au contraire cet échec relatif pour vous motiver à structurer votre travail personnel et à entrer plus en profondeur dans le cours et les exercices. La plupart des élèves passent par cette étape peu agréable, ce qui ne les empêche pas de réussir par la suite.

Ce n'est pas un sprint mais un marathon !

Gardez également un mode de vie sain, en pratiquant un peu de sport (ce qui ne vous sera pas inutile si vous prétendez intégrer une école comme Polytechnique, qui présente des épreuves sportives à son concours), en soignant votre alimentation et surtout votre sommeil. Pour ce dernier point, deux techniques sont possibles et nous les avons déjà évoquées : miser sur la quantité de travail en sacrifiant le sommeil (ne faites cependant pas cela à l'approche des concours !), ou privilégier la fraicheur d'esprit apportée par de bonnes nuits complètes pour être plus efficace dans le travail. À vous de voir ce qui vous convient le mieux.

Il ne faut pas mettre tous ses œufs dans le même panier !

Vous devez être assez complet si vous voulez réussir et vous ne devez donc pas concentrer votre travail uniquement sur les mathématiques : nous avons évoqué le sport mais ceci est vrai à plus forte raison pour d'autres matières telles que la physique, la chimie, le français, les langues. Combien de temps accorder à chacune de ces matières ? Cela dépend des facilités de chacun, mais ne faites aucune impasse. Naturellement, il y a des matières plus importantes que d'autres : les coefficients accordés à chaque matière aux différents concours, ou le nombre d'heures de cours par matière, vous permettent d'avoir une idée de hiérarchie.

Organiser son travail

Dans l'apprentissage des mathématiques se cache un grand danger : il s'agit de la trop grande confiance que l'on accorde à notre compréhension à la lecture d'un théorème. Pour pleinement saisir toutes les subtilités d'un tel énoncé et être en mesure de savoir en quelles circonstances il peut être un outil efficace, il est nécessaire d'étayer la lecture du cours par de nombreux exercices (sans négliger le cours pour autant, bien entendu ! La connaissance du cours, c'est-à-dire des énoncés *et* de leur démonstration, est fondamentale.). Ces exercices permettent en effet de mieux apprécier les résultats contenus dans votre cours, de vous familiariser avec eux et de vous habituer à recourir à eux de manière opportune. La démarche est similaire à l'apprentissage de la conduite : vous pouvez lire tous les livres que vous voulez, vous n'aurez jamais autant confiance au volant que lorsque vous aurez pu vous entraîner à conduire des kilomètres, sur autoroute, en ville, en campagne. Pour les exercices, c'est la même chose : variez les types d'exercices et ne lésinez pas sur la quantité. Par chance, les ouvrages rassemblant des exercices ou des sujets de concours corrigés ne manquent pas sur les rayons des bibliothèques et des librairies ! Utilisez-les, ne vous limitez pas aux énoncés donnés par votre professeur. Certaines personnes passées par la prépa recommandent, pour x heures passées à relire le cours, de passer $2x$ heures à faire des exercices. Il ne s'agit pas non plus de lire l'exercice avec sa solution, il s'agit vraiment de lire l'énoncé et de tenter de le résoudre avec une feuille et un crayon : pour filer la métaphore, vous apprendrez mieux à conduire en étant derrière le volant qu'en regardant quelqu'un conduire tout en étant confortablement assis dans le siège du passager.

Nous vous encourageons donc à bien travailler en profondeur, mais ne mettez pas non plus la barre trop haut : il vous sera difficile de faire tous les exercices des livres que vous aurez dans votre bibliothèque ; le temps de la prépa est court, donc il ne faut pas perdre le rythme et vouloir trop en faire risquerait de vous faire prendre un retard conséquent sur le cours tel qu'il sera développé par votre professeur.

Développer l'intuition

Ne lisez pas les définitions de notions ou les hypothèses de théorèmes comme des litanies de conditions tombées du ciel. Vous devez vraiment comprendre chacune de ces conditions en vous les appropriant. Pourquoi a-t-on mis telle hypothèse dans un théorème ? Posez-vous la question de ce que deviendrait le théorème en question sans une telle hypothèse : construisez des contre-exemples simples, qui vous soient familiers et qui vous permettent d'apprécier pourquoi le théorème ne fonctionne plus sans l'hypothèse en question. En faisant de la sorte :

- vous retiendrez plus facilement toutes ces conditions,
- vous serez capable de les retrouver si vous les oubliez,
- vous penserez à faire appel au théorème idoine lorsque vous rencontrerez dans un exercice ces conditions qui vous seront devenues familières.

Ce qui vaut pour les théorèmes vaut aussi pour les définitions et, si vous vous posez par exemple la question « que devient une relation d'équivalence si elle n'est plus transitive ou réflexive ? », alors vous aurez mieux compris ce qu'est une relation d'équivalence.

Nous venons d'affirmer que le contre-exemple doit vous permettre de mieux comprendre les hypothèses d'un théorème. En fait, vous devez utiliser abondamment les exemples et les contre-exemples. Les premiers vous permettent de tester un théorème et de vous laisser convaincre en plus de la démonstration, donc de vous rendre ce théorème plus naturel ; les seconds, en tentant de montrer les limites d'un théorème déshabillé de certaines de ses hypothèses, vous permettent de mieux comprendre dans quel cadre il faut utiliser ce théorème. Cela peut aussi être une méthode à suivre pour résoudre un exercice : commencer sa réflexion en se limitant à un cas particulier de l'énoncé permet de réduire la difficulté et de tester des idées de raisonnement ; en l'occurrence, si un raisonnement ne fonctionne pas sur un cas particulier de l'énoncé, il n'y a aucune chance pour que ce raisonnement fonctionne dans le cadre plus général de l'énoncé. En faisant de la sorte, vous gagnez du temps en évitant d'emprunter de fausses voies et vous raisonnez sur des objets plus simples à manipuler. Attention toutefois à ne pas vous laisser abuser par l'étude du cas particulier trivial qui vide l'énoncé de toute la subtilité de raisonnement qu'il nécessite : testez-donc plusieurs cas particuliers et confrontez-les ! Un dessin tracé sur votre feuille de brouillon peut aussi bien vous aider : ne négligez aucun mode de raisonnement !

À la lecture de l'énoncé d'un exercice, il est primordial de repérer précisément les hypothèses ainsi que de bien identifier ce qu'il est demandé de montrer.

Lorsque l'on est déconcerté par un exercice, ignorant totalement comment le résoudre, c'est souvent à cause d'une mauvaise compréhension de son énoncé. La liste exhaustive des hypothèses vous permettra de distinguer quels théorèmes vous pourriez être en droit d'utiliser, cette étape n'étant vraiment efficace que si vous connaissez parfaitement votre cours. De plus, passer par des formules avec des symboles plutôt que par du texte peut aussi vous aider à mieux comprendre l'enjeu d'un exercice ; encore faut-il s'être suffisamment entraîné pour être familier avec cette manière d'écrire les mathématiques ! Prenons un exemple trivial : soit $f : E \to E$ une application injective ; il s'agit de montrer que la restriction de f à tout ensemble F distinct de E n'est pas surjective. Si cet énoncé vous laisse pantois, cela peut-être dû au mélange d'écriture symbolique et d'assertions littéraires. Reformuler l'énoncé de manière symbolique permettra une vision plus synthétique du problème. Montrer que $f_{|F} : F \to E$ n'est pas surjective, revient à montrer que

$$\exists v \in E, \forall u \in F, f_{|F}(u) \neq v.$$

Les hypothèses à disposition sont les suivantes :
- $F \subset E$ avec $E \neq F$, ce qui signifie que $\exists x \in E, x \notin F$;
- f est injective : $\forall (x,y) \in E^2, f(x) = f(y) \Rightarrow x = y$.

La première hypothèse nous incite à choisir un élément $x \in E$ tel que $x \notin F$. La deuxième hypothèse indique, par contraposée, que, pour tout y différent de x (par exemple pour tout $y \in F$), $f(y) \neq f(x)$. Vous devez commencer à voir comment cela fonctionne... Mettons en forme le raisonnement en faisant référence à ce que nous cherchons à montrer. En l'occurrence, nous cherchons un élément v vérifiant une certaine condition. $v = f(x)$ semble être le candidat idéal et ce problème ne présente plus de difficulté. En effet, $f(x) \in E$ et nous avons noté que, pour tout $y \in F$, $f(y) \neq f(x)$, c'est-à-dire $f_{|F}(y) = f(y) \neq f(x) = v$.

Pour conclure, nous laissons maintenant la parole à d'autres anciens élèves de classes préparatoires. Méditez leurs conseils.

Conseils d'anciens aux futurs bizuts

Accrochez-vous ! Le jeu en vaut la chandelle !

Ali, Supélec

Quand on a déjà des méthodes de travail, ne pas tout abandonner sans réfléchir, mais regarder ce qui convient et ce qui ne convient plus. *Tabula rasa* peut être catastrophique !

Charles, X

Prenez des moments de repos (une demie journée par semaine, quelques jours pendant les vacances). Utilisez les vacances entre la sup et la spé à bon escient !

Guillaume, X

Travaillez régulièrement, accrochez-vous et ne baissez pas les bras ! Consacrez aussi quelques heures par semaine pour faire le vide (sport, loisirs).

Mohamed, Centrale Paris

Ne vous laissez pas décourager par les premières difficultés et tâchez de progresser tout au long des deux ans de prépa. Personnellement, les progrès se sont accélérés au moment des révisions des concours ; j'étais constamment en retard pour assimiler le cours et les méthodes mais j'ai fini par tout assimiler à mon rythme et cela a payé pour les concours.

Hugues, X

Keep cool ! Ce ne sont que des études :)

Jean-François, ENSIMAG

Travaillez régulièrement et préparez-vous psychologiquement !

Ali, ESTP

Trois choses me semblent importantes. D'abord, ne pas se donner l'impression de travailler. Il faut savoir distinguer les phases où l'on travaille efficacement et où l'on apprend vraiment de celles où l'on se donne bonne conscience. L'archétype de ce genre de moments, c'est lorsqu'on lit des exercices en lisant pratiquement immédiatement la correction. Ensuite, savoir se reposer, le soir comme le week-end. Enfin, bien connaître son cours. L'accumulation d'exercices ne remplace pas vraiment la connaissance précise et maîtrisée des principaux concepts du cours, de leur enchaînement, s'il y en a un.

Anonyme, X

Éclatez-vous et faites du sport !

Benoît, X

Ne croyez pas être seul à souffrir ! Et acceptez *a contrario* que certains ne souffriront simplement pas !

Toan, X

Index

MATHS : l'entrée en prépa sans faux pas

Vous êtes en terminale S ou vous en sortez juste, et vous envisagez de poursuivre vos études en classe préparatoire scientifique à la rentrée prochaine, mais :

- vous avez entendu beaucoup de choses sur l'écart de niveau entre les programmes de mathématiques en terminale et en prépa, si bien que vous voulez vous rassurer ;
- vous êtes impatient de vous familiariser avec les maths de prépa, l'art de la démonstration et de prendre un peu d'avance sur le programme ;
- vous vous ennuyez et cherchez une saine occupation.

Alors ce livre de mathématiques a été conçu pour vous ! Il vous permettra, par la judicieuse sélection des thèmes, de passer progressivement du raisonnement de terminale (acceptation de théorèmes parfois sans remise en question) à celui des études supérieures (questionnement constructif visant à saisir la subtilité des théorèmes), en alternant cours et exercices corrigés. Vous trouverez également à la fin du livre quelques pages de conseils pratiques pour réussir vos études en classe préparatoire.

Matthieu Garcin a intégré l'École polytechnique après avoir suivi la classe préparatoire du lycée Marcelin Berthelot, où il a été colleur en mathématiques par la suite. Il a également obtenu un doctorat en mathématiques à l'université Paris 1 Panthéon-Sorbonne. Actuellement, il travaille en tant qu'ingénieur financier.

Younes Kchia est docteur et ingénieur de l'École polytechnique, qu'il a intégrée après ses classes préparatoires au lycée Louis Le Grand, où il a été colleur. Il a été chargé de TD de mathématiques à l'université Pierre et Marie Curie. Il travaille actuellement en tant qu'ingénieur financier.

9 782340 003637

www.editions-ellipses.fr