Éléments de mathématiques pour le XXI^{e} siècle, volume 4

Du même auteur

- *Éléments de mathématiques pour le XXIe siècle, volume 1 : Fondements des mathématiques 1 (logique des propositions et des prédicats, systèmes déductifs formels, arithmétique de Peano, structures algébriques de base)*. 2019.
- *Éléments de mathématiques pour le XXIe siècle, volume 2 : Fondements des mathématiques 2 (théorie des ensembles, mathématiques discrètes, structures algébriques de base)*. 2019.
- *Éléments de mathématiques pour le XXIe siècle, volume 3 : Fondements des mathématiques 3 (théorie des ensembles, théorie des nombres, algèbre, théorie des modèles, théorie de la calculabilité, théorie des catégories et des topos)*. 2022.
- *Éléments de mathématiques pour le XXIe siècle, volume 5 : Fondements des mathématiques 5 (théorie univalente des types)*. À paraître (2026).
- *Citations mathématiques : Plus de 200 citations sourcées et vérifiées*. 2021.

Étienne Bonheur

Éléments de mathématiques pour le XXI^{e} siècle, volume 4

Fondements des mathématiques 4
(analyse combinatoire, théorie des graphes, théorie des nombres, algèbre linéaire, topologie, théorie des groupes et des anneaux)

Paysages Mathématiques

https://paysmaths.net

ISBN : 978-2-9569666-4-7
Dépôt légal : Décembre 2025

Table des matières

Introduction **1**

Vocabulaire, notations et rappels **5**

1 Compléments sur les anneaux **9**
1.1 Caractéristique d'un anneau . . . 9
1.2 Compléments sur les groupes et les anneaux ordonnés . . . 11

2 Analyse combinatoire **17**
2.1 Rappels et compléments . . . 17
2.2 *Twelvefold way* . . . 19
2.3 k-listes . . . 24
2.4 Arrangements et permutations . . . 27
2.5 Combinaisons, coefficients binomiaux . . . 32
2.6 Formule du binôme . . . 38
2.7 Permutations avec répétition et formule du multinôme . . . 42
2.8 Combinaisons avec répétition . . . 44
2.9 Dénombrement des surjections, des partitions d'un ensemble, nombres de Stirling de seconde espèce . . . 47
2.10 Dénombrement des partitions d'un entier . . . 51
2.11 Synthèse . . . 52

3 Compléments sur les groupes **55**
3.1 Ordre d'un groupe, indice d'un sous-groupe . . . 55
3.2 Sous-groupes engendrés, ordre d'un élément . . . 59
3.3 Groupes monogènes, groupes cycliques . . . 64
3.4 Groupes symétriques . . . 69
3.5 Action de groupe, orbite . . . 76
3.6 Cycles et générateurs de $\mathcal{S}_n$ . . . 83
3.7 Signature, groupe alterné . . . 89
3.8 Éléments d'ordre 1 ou 2 . . . 95
3.9 Compléments sur les sous-groupes normaux . . . 98

4 Compléments de théorie des nombres **101**
4.1 Triplets pythagoriciens . . . 101
4.2 Nombres de Mersenne . . . 105
4.3 Nombres de Fermat . . . 107
4.4 Généralités sur les fonctions arithmétiques . . . 109
4.5 Indicatrice d'Euler . . . 111

4.6 Somme des diviseurs, nombres parfaits . . . 116

5 Extension de la notion de nombre 121
5.1 Corps des fractions d'un anneau intègre . . . 121
5.2 Corps $\mathbb{Q}$ des nombres rationnels . . . 128
5.3 Corps premiers . . . 133
5.4 Corps archimédiens . . . 136
5.5 Compléments sur les suites . . . 144
5.6 Suites convergentes dans un corps archimédien . . . 146
5.7 Suites de Cauchy dans un corps archimédien . . . 158
5.8 Corps $\mathbb{R}$ des nombres réels (introduction) . . . 168
5.9 Construction de $\mathbb{R}$ par les coupures de Dedekind . . . 178
5.10 Construction de $\mathbb{R}$ par les suites de Cauchy . . . 192
5.11 Autres propriétés de $\mathbb{R}$ . . . 196
5.12 Droite réelle achevée . . . 212
5.13 Corps $\mathbb{C}$ des nombres complexes . . . 214

6 Algèbre linéaire 229
6.1 Modules et espaces vectoriels . . . 229
6.2 Combinaisons linéaires, sous-modules et sous-espaces vectoriels . . . 242
6.3 Morphismes de modules et d'espaces vectoriels (fonctions linéaires) . . . 249
6.4 Familles libres, familles génératrices, bases . . . 260
6.5 Algèbres . . . 274
6.6 Matrices et fonctions linéaires, algèbre des matrices carrées . . . 278

7 Séries formelles et polynômes 285
7.1 Algèbres des séries formelles et des polynômes . . . 285
7.2 Évaluation des polynômes . . . 299
7.3 Division euclidienne des polynômes . . . 304
7.4 Racines des polynômes . . . 307

8 Introduction à la théorie des graphes 313
8.1 Présentation informelle et exemples . . . 313
8.2 Formalisation de la notion de graphe et généralités . . . 316
8.3 Degré d'un sommet . . . 326
8.4 Chemins, cycles, connexité, et arbres . . . 329
8.5 Noyau d'un graphe orienté . . . 334
8.6 Distance, parcours en largeur et en longueur . . . 337
8.7 Graphes eulériens et hamiltoniens . . . 340
8.8 Coloration d'un graphe . . . 343

9 Structures topologiques 345
9.1 Espaces topologiques . . . 345
9.2 Topologie engendrée, base de topologie . . . 349
9.3 Topologie de l'ordre . . . 353
9.4 Espaces métriques et espaces vectoriels normés . . . 356
9.5 Topologie des espaces métriques . . . 370
9.6 Topologie produit . . . 377
9.7 Topologie induite . . . 380
9.8 Intérieur, adhérence . . . 384

9.9 Limites et continuité, homéomorphismes . . . 392
9.10 Limites et continuité de la restriction ou corestriction d'une fonction, prolongement par continuité . . . 407
9.11 Limites et continuité dans les espaces vectoriels normés . . . 413
9.12 Densité . . . 419
9.13 Convergence des suites dans les espaces topologiques . . . 424
9.14 Convergence des suites de fonctions dans les espaces topologiques . . . 430
9.15 Valeurs d'adhérence d'une suite . . . 432
9.16 Suites de Cauchy, espaces complets . . . 435
9.17 Espaces compacts . . . 442
9.18 Espaces vectoriels normés de dimension finie . . . 452
9.19 Espaces connexes, théorème des valeurs intermédiaires . . . 457

10 Fonctions à valeurs réelles **463**
10.1 Dérivabilité . . . 463
10.2 Extremums locaux, variations d'une fonction . . . 472

11 Séries **479**
11.1 Séries à valeurs dans un espace vectoriel normé . . . 479
11.2 Séries à valeurs réelles positives . . . 484
11.3 Séries à valeurs dans un espace de Banach . . . 491
11.4 Séries de fonctions . . . 501
11.5 Exponentielle dans une algèbre de Banach . . . 503
11.6 Exponentielle complexe, exponentielle réelle . . . 506

12 Compléments sur les corps $\mathbb{R}$ et $\mathbb{C}$ **511**
12.1 Fonctions trigonométriques . . . 511
12.2 Compléments sur l'exponentielle complexe . . . 518
12.3 Argument et forme polaire d'un complexe, racines n-ièmes de l'unité . . . 521
12.4 Théorème de d'Alembert-Gauss . . . 525

13 Arithmétique des anneaux **529**
13.1 Compléments sur les idéaux . . . 530
13.2 Anneaux principaux, anneaux euclidiens . . . 531
13.3 Idéaux premiers et maximaux, éléments premiers et irréductibles . . . 535
13.4 PGCD et PPCM . . . 544
13.5 Propriétés des PGCD et des PPCM dans un anneau principal . . . 547
13.6 Anneaux factoriels . . . 553

Liste des symboles **559**

Index des notions **563**

Index des noms propres **569**

Introduction

Ce livre est le quatrième volume d'une série qui doit, à terme, couvrir l'ensemble des notions du premier cycle universitaire en mathématiques, tout en débordant largement sur le deuxième cycle. Il sera donc utile aux étudiants en licence ou en classes préparatoires scientifiques, ainsi qu'aux étudiants en master, y compris ceux préparant le CAPES ou l'agrégation (dont les programmes sont également très largement couverts par cette série d'ouvrages)[1]. Les enseignants y trouveront aussi de nombreux éléments leur permettant de préparer leurs cours, ou de compléter leurs connaissances dans des domaines qui ne leur sont pas familiers.

De manière plus générale, cette série d'ouvrages pourra être utile à toute personne s'intéressant aux mathématiques actuelles (les *mathématiques du XXI^e siècle* auxquelles fait référence le titre[2]). Elle devrait, *en théorie*, être accessible même sans connaissance préalable. En effet, les mathématiques sont prises à leur début et les différents concepts progressivement construits, chaque définition, théorème et démonstration ne faisant appel qu'à ce qui a été défini précédemment. Ce principe général aura cependant quelques exceptions : je pourrai, pour des raisons didactiques (notamment dans les remarques et exemples), ou par volonté de synthèse, être parfois amené à faire référence à des notions postérieures. À noter aussi que je suivrai un ordre me permettant d'enchaîner logiquement les différentes notions, mais qui n'est pas nécessairement l'ordre que l'on pourrait trouver dans un cursus universitaire, c'est-à-dire, par exemple, que certains éléments apparaissant dans les premiers volumes peuvent être enseignés traditionnellement dans des classes de troisième année de licence, voire au-delà. Néanmoins les chapitres peuvent être largement indépendants, et la compréhension d'un chapitre donné n'est pas toujours nécessaire à la compréhension de ceux qui suivent. Par ailleurs, lorsque cela peut être utile, les prérequis principaux seront indiqués au début d'un chapitre ou d'une section[3][4].

Chaque ouvrage se veut à la fois

- didactique, avec des preuves très détaillées, des explications informelles, et de nombreux exemples et contre-exemples ;
- complet, voire encyclopédique, avec un exposé de nombreuses notions, des théorèmes tous démontrés, et de nombreux détails historiques (notamment sur l'origine des notations et du vocabulaire mathématique) ;
- synthétique, avec en particulier la volonté de multiplier les points de vue ; par exemple, les sujets pourront être abordés de façon à la fois formelle et informelle, et il pourra arriver que je donne plusieurs définitions équivalentes d'un même concept, ou plusieurs preuves d'un même théorème.

J'ai décidé de ne pas inclure de bibliographie, qui ne serait qu'une très longue liste de documents, et dont l'intérêt serait limité, sachant que dans cet ouvrage, tous les termes sont définis, tous les théorèmes sont prouvés, et mon lectorat peut ainsi vérifier par lui-même tous les résultats. Les affirmations non justifiées (par exemple les remarques historiques) et certaines démonstrations sont directement sourcées dans les notes de bas de page. Cependant, pour les remarques portant sur l'origine du vocabulaire et des notations, je n'indiquerai pas à chaque fois mes sources principales, qui sont

1. Ou des cursus équivalents, pour mon lectorat francophone non français.

2. Le début du titre faisant par ailleurs référence aux *Éléments* d'Euclide, et aux *Éléments de Mathématique* de Bourbaki, deux œuvres partageant avec la présente série la volonté d'exposition des savoirs selon un ordre logique précis, à partir d'axiomes donnés.

3. Une section est un sous-chapitre.

4. Les différents prérequis indiqués ne correspondent ni à un minimum ni à un maximum à connaître pour comprendre la section en cours, mais doivent être pris comme une aide pour identifier, parmi les notions abordées précédemment, celles pouvant être utiles.

- Jeff MILLER. *Earliest Uses of Some Words of Mathematics*. URL : `https://mathshistory.st-andrews.ac.uk/Miller/mathword/`
- Jeff MILLER. *Earliest Uses of Various Mathematical Symbols*. URL : `https://mathshistory.st-andrews.ac.uk/Miller/mathsym/`
- Florian CAJORI. *A history of mathematical notations*. The Open Court Publishing Co., 1928-1929

Je précise que les sources indiquées ne sont pas nécessairement exhaustives (je peux par exemple donner uniquement une source simple d'accès, ce qui est le cas des précédentes), et que, dans la mesure du possible, je vérifie et recoupe toutes les informations, y compris les références données par ces différentes sources. Par ailleurs, les citations issues de textes non francophones feront automatiquement l'objet d'une traduction personnelle, sans que je le précise non plus à chaque fois.

On notera aussi qu'aucun paragraphe ne commence par « exercice », ce qui ne veut pas dire que les lecteurs ne disposent d'aucun matériel pour s'exercer : les exemples ainsi que les nombreux théorèmes peuvent être considérés comme autant d'exercices corrigés (beaucoup d'énoncés que l'on trouve fréquemment dans la littérature sous l'intitulé *exercice* se trouvent ici sous l'intitulé *théorème*). Ainsi, chaque théorème étant suivi d'une démonstration complète[5], il n'y aura pas, dans cette série d'ouvrages, d'expressions comme « la preuve est laissée en exercice », « le lecteur prouvera lui-même que… », et autres « on démontre facilement que… ».

Le premier volume traite essentiellement de la notion de logique mathématique, le deuxième de la théorie des ensembles de Zermelo-Fraenkel, et le troisième aborde notamment la théorie des modèles, la théorie de la calculabilité, et la théorie des catégories et des topos (je présente dans ce cadre la *théorie élémentaire de la catégorie des ensembles* (ou ETCS) de William Lawvere). On trouve aussi dans les trois premiers volumes une introduction aux structures algébriques de base et à la théorie des nombres (divisibilité, PGCD et PPCM, entiers modulo n…).

Au programme de ce quatrième volume :

- des compléments de mathématiques discrètes : théorie des nombres (chapitre 4), analyse combinatoire (chapitre 2), introduction à la théorie des graphes (chapitre 8) ;
- des compléments sur les groupes et les anneaux (chapitres 1, 3 et 13) ;
- la suite de la construction des ensembles classiques de nombres, et l'étude de leurs propriétés (chapitre 5 et 12) : ensemble $\mathbb{Q}$ des rationnels, ensemble $\mathbb{R}$ des réels (construction par les coupures de Dedekind, et par les suites de Cauchy), ensemble $\mathbb{C}$ des complexes ;
- une introduction à l'algèbre linéaire par la présentation de quelques structures (modules, espaces vectoriels, algèbres) et de quelques exemples usuels (chapitres 6 et 7) : espaces $\mathbb{K}^n$, matrices, polynômes, séries formelles…
- la présentation de structures topologiques (espaces topologiques, espaces métriques, espaces vectoriels normés), et de quelques notions associées (chapitres 9 à 11) : limite, continuité, convergence de suites et séries, compacité…

Le cinquième volume sera consacré à l'introduction de la *théorie univalente des types* (ou *théorie des types univalents*[6]), qui permet un fondement formel alternatif des mathématiques[7]. Il sera par ailleurs accompagné d'une formalisation complète sur l'assistant de preuves *Agda*[8]. Ce cinquième volume terminera une première partie consacrée aux fondements modernes des mathématiques. Comme on a pu le constater dans les premiers volumes, je prends cette expression dans un sens un peu général : au-delà de son acception

5. À l'exception de certains théorèmes, qui peuvent ne pas être suivis d'une preuve explicite, dans deux cas : s'ils sont une conséquence immédiate du théorème précédent, ou si la preuve a déjà été donnée dans un commentaire précédant le théorème.

6. On parle aussi de *fondements univalents*, de *théorie homotopique des types*, ou *théorie des types d'homotopie* (en anglais *Univalent Type Theory*, *Univalent Foundations*, ou *Homotopy Type Theory*).

7. Il était initialement prévu de faire figurer cette partie dans ce quatrième volume, mais la taille importante de l'ensemble m'a conduit à le partager en deux.

8. Fichiers accessibles en ligne, indépendamment du livre.

la plus usuelle (comprenant, pour faire simple, la logique mathématique et la théorie des ensembles), j'inclus d'autres sujets comme la construction des ensembles classiques de nombres (ensemble $\mathbb{N}$ des entiers naturels, ensemble $\mathbb{R}$ des nombres réels…) ou l'introduction de certaines structures de base : structures algébriques simples (groupes, anneaux…), structures linéaires (espaces vectoriels…), structures topologiques (espaces métriques…), etc.

Vocabulaire, notations et rappels

Je renvoie mon lectorat au premier volume pour quelques remarques introductives concernant le vocabulaire et les notations. Je ne rappellerai ici que quelques usages qui peuvent être peu répandus, voire personnels (les notations classiques ne feront pas l'objet d'un rappel systématique, mais peuvent être trouvées dans la liste des symboles à la fin de cet ouvrage), ainsi que quelques principes vus dans les volumes précédents.

1. L'égalité ayant en mathématiques un sens parfois subtil, je fais la distinction entre *égalité* et *égalité par définition*[9] :
   - égalité :
   $$A = B \qquad (\text{« A est égal à B »})$$
   signifie : les objets A et B sont identiques.
   - égalité par définition :
   $$A \overset{\text{def}}{\equiv} B \qquad (\text{« A est égal, par définition, à B »})$$
   signifie : on donne par définition, à l'objet B, le nom A.
2. Le symbole $\equiv$ désigne l'équivalence (sémantique ou syntaxique) de deux formules, dans le sens suivant : si Γ est une théorie donnée (en général implicite), $\mathscr{F} \equiv \mathscr{G}$ signifie $\Gamma \vdash \mathscr{F} \iff \mathscr{G}$ (autrement dit la théorie Γ permet de prouver que $\mathscr{T}$ est équivalent à $\mathscr{G}$). Cette formulation me permet en particulier de noter
   $$\mathscr{F} \equiv \mathscr{G} \equiv \mathscr{H}$$
   pour signifier
   $$\Gamma \vdash (\mathscr{F} \iff \mathscr{G}) \qquad \text{et} \qquad \Gamma \vdash (\mathscr{G} \iff \mathscr{H})$$
   (autrement dit $\mathscr{F}$ est équivalent à $\mathscr{G}$ et $\mathscr{G}$ est équivalent à $\mathscr{H}$, d'où l'on déduit que $\mathscr{F}$ est équivalent à $\mathscr{H}$).
3. Je note $\subseteq$ la relation d'inclusion et $\subset$ la relation d'inclusion stricte : pour tous les ensembles A et B
   $$A \subseteq B \overset{\text{def}}{\equiv} \forall x \in A, x \in B \qquad \text{et} \qquad A \subset B \overset{\text{def}}{\equiv} A \subseteq B \text{ et } A \neq B$$
   Si $A \subseteq B$ (respectivement $A \subset B$), on dit que A est un *sous-ensemble* (respectivement un *sous-ensemble strict*, ou un *sous-ensemble propre*), ou une *partie* (respectivement une *partie stricte*, ou une *partie propre*), de B.
4. Je peux écrire « pour tout $x\ y \in A$ », ou
   $$\forall x\ y \in A$$
   comme raccourci pour
   $$\forall x \in A, \forall y \in A$$
   ce qui équivaut à
   $$\forall (x, y) \in A^2$$
   De même pour d'autres relations, par exemple
   $$\forall x\ y \geqslant z \qquad \text{est un raccourci pour} \qquad \forall x \geqslant z, \forall y \geqslant z$$

9. Pour simplifier, je n'utilise plus l'égalité par affectation, qui était équivalente à l'égalité par définition (la différence n'étant que subjective).

5. Je désigne les intervalles de tout ensemble ordonné A par la même notation que les intervalles classiques de $\mathbb{R}$, en indiquant éventuellement l'ensemble (A) en indice en cas d'ambiguïté. Par exemple :

$$[a,b]_A \overset{\text{def}}{\equiv} \{x \in A\ ;\ a \leqslant x \text{ et } x \leqslant b\} \quad [a,b[_A \overset{\text{def}}{\equiv} \{x \in A\ ;\ a \leqslant x \text{ et } x < b\} \quad]-\infty,b]_A \overset{\text{def}}{\equiv} \{x \in A\ ;\ x \leqslant b\}$$

6. Une fonction $A \xrightarrow{f} B$ est définie entièrement sur A (*fonction* est synonyme d'*application*, terme que je n'utilise pas). L'ensemble A s'appelle le domaine de la fonction, et B son codomaine. Si le domaine de ce que j'ai appelé une *relation fonctionnelle* peut être strictement inclus dans A, il s'agit alors d'une *fonction partielle* de A dans B.
7. Je note $A \longrightarrow B$ ou B^A l'ensemble des fonctions de A dans B.
8. Pour tous les ensembles A, B, C, il est équivalent de se donner une fonction de $A \longrightarrow (B \longrightarrow C)$ ou une fonction de $(A \times B) \longrightarrow C$ (ces deux ensembles sont en bijection). Ce principe porte le nom de *curryfication* (plus précisément, la *curryfication* est la transformation d'une fonction de $(A \times B) \longrightarrow C$ en une fonction de $A \longrightarrow (B \longrightarrow C)$, et la *décurryfication* est la transformation inverse, mais je peux utiliser le terme *curryfication* pour désigner ce principe d'équivalence).
9. Une famille $(a_i)_{i\in I}$ d'éléments d'un ensemble E est une fonction $I \xrightarrow{a} E$ (et une suite est une famille indexée par l'ensemble des entiers naturels, c'est-à-dire telle que $I = \mathbb{N}$), d'où les deux notations équivalentes pour l'image de i par a :

$$a_i \qquad \text{et} \qquad a(i)$$

   Par ailleurs, on dit qu'une famille $(a_i)_{i\in I}$ est finie (respectivement infinie, dénombrable, non dénombrable, vide) lorsque l'ensemble I est fini (respectivement infini, dénombrable, non dénombrable, vide).
10. Le produit (ou produit cartésien) d'une famille $(A_i)_{i\in I}$ d'ensembles, noté $\prod_{i\in I} A_i$, est l'ensemble des familles $(a_i)_{i\in I}$ telles que pour tout $i \in I$, $a_i \in A_i$.
    - Dans le cas où la famille $(A_i)_{i\in I}$ est constante, c'est-à-dire que les A_i sont égaux à un même ensemble E, le produit est l'ensemble des fonctions de I dans E :

$$\prod_{i\in I} E = I \longrightarrow E$$

    - Dans le cas où I est un ensemble fini de cardinal n, on peut identifier une famille indexée par I et une n-liste (ou n-uplet) : si pour tout $i \in [1,n]$, $a_i \in A_i$, je pourrai noter indifféremment

$$(a_1, \dots, a_n) \qquad \text{ou} \qquad (a_i)_{i\in[1,n]} \qquad \text{ou} \qquad a$$

      ce qui représente à la fois la n-liste $(a_1, \dots, a_n)$ de $A_1 \times \cdots \times A_n$, la famille $(a_i)_{i\in[1,n]}$ de $\prod_{i\in[1,n]} A_i$, ou la fonction a qui, à un élément $i \in [1,n]$, associe un élément $a_i \in A_i$. Si de plus la famille $(A_i)_{i\in I}$ est constante, égale à un ensemble E, on a donc

$$E^n = \underbrace{E \times \cdots \times E}_{n \text{ fois}} = \prod_{i\in[1,n]} E = [1,n] \longrightarrow E$$

11. Pour toute fonction $A \xrightarrow{f} B$ je note respectivement $\underset{\rightarrow}{f}$ et $\underset{\leftarrow}{f}$ les fonctions suivantes :

$$\underset{\rightarrow}{f} : \begin{cases} \mathscr{P}(A) \longrightarrow \mathscr{P}(B) \\ X \longmapsto \{f(x)\ ;\ x \in X\} \end{cases} \qquad \text{et} \qquad \underset{\leftarrow}{f} : \begin{cases} \mathscr{P}(B) \longrightarrow \mathscr{P}(A) \\ Y \longmapsto \{x \in A\ ;\ f(x) \in Y\} \end{cases}$$

$\vec{f}(X)$ représente donc l'image directe de l'ensemble X par la fonction f, autrement dit ce qui est noté plus classiquement $f(X)$; et $\overleftarrow{f}(Y)$ représente donc l'image réciproque de l'ensemble Y par la fonction f, autrement dit ce qui est noté plus classiquement $f^{-1}(Y)$. L'image d'une fonction est l'image directe de son domaine :

$$\mathrm{Im}(f) \overset{\text{def}}{=\!=} \vec{f}(A) \overset{\text{def}}{=\!=} \{f(x)\,;\ x \in A\}$$

Et puisqu'une suite est une fonction particulière, l'image de la suite $(u_n)_{n\in\mathbb{N}}$ est donc l'ensemble $\left\{u_n\,;\ n \in \mathbb{N}\right\}$.

12. Pour tout ensemble A, $|A|$ représente le *cardinal* de A. Pour tous les ensembles A et B, $|A| = |B|$ si et seulement si A et B sont en bijection, et $|A| \leqslant |B|$ si et seulement si il existe une injection de A dans B. Le cardinal d'un ensemble fini est son nombre d'éléments. En particulier pour tout entier naturel n

$$|[0, n[| = |[1, n]| = n$$

Un ensemble A est ∞-*dénombrable* lorsqu'il est en bijection avec $\mathbb{N}$, et *dénombrable* lorsqu'il existe une injection de A dans $\mathbb{N}$ (donc lorsqu'il est fini ou en bijection avec $\mathbb{N}$). Le cardinal de $\mathbb{N}$ étant noté $\aleph_0$, un ensemble A est

- fini si et seulement si $|A| < \aleph_0$;
- dénombrable si et seulement si $|A| \leqslant \aleph_0$;
- ∞-dénombrable si et seulement si $|A| = \aleph_0$.
- non-dénombrable si et seulement si $|A| > \aleph_0$.

13. La loi d'un groupe peut être notée indifféremment par un symbole de type $*$ ou $\times$ (l'élément neutre étant alors généralement noté e ou 1), ou par un symbole $+$ (l'élément neutre étant alors généralement noté 0), la notation additive $(+)$ étant le plus souvent réservée aux groupes commutatifs (mais pas de façon systématique).

14. L'expression $A \simeq B$ signifie, selon le contexte, que les ensembles A et B sont en bijection, ou que l'ensemble A, muni d'une certaine structure, et l'ensemble B, muni de la même structure, sont isomorphes. Par exemple si $(G, *, e)$ et $(G', \star, e')$ sont deux groupes,

$$(G, *, e) \simeq (G', \star, e') \qquad \text{ou juste} \qquad G \simeq G'$$

signifie que les deux groupes sont isomorphes.

15. En ce qui concerne les définitions de quelques structures algébriques de base :

- les *anneaux* sont toujours unitaires (autrement dit la multiplication dispose toujours d'un élément neutre) ;
- les *anneaux intègres* et les *corps* sont non triviaux (autrement dit le neutre pour l'addition et le neutre pour la multiplication sont des éléments distincts), et toujours commutatifs (autrement dit la multiplication est commutative, l'addition étant toujours commutative par définition d'un anneau) [10].

10. Un anneau non trivial dans lequel tout élément non nul a un inverse s'appelle un *anneau à division*, ou un *corps gauche*. Un corps est donc un anneau à division commutatif.

Chapitre 1

Compléments sur les anneaux

Prérequis
Les anneaux et les anneaux ordonnés (sections 8.4 et 8.5 du volume 1, section 2.9 du volume 2, chapitre 2 du volume 3).

1.1 Caractéristique d'un anneau

Je rappelle que pour tout élément x d'un groupe commutatif $(G, +, 0)$, et pour tout $n \geqslant 0$, nx est l'addition itérée

$$\underbrace{x + x + \cdots + x}_{n \text{ termes}}$$

définie par la récurrence

$$\begin{cases} 0x = 0 \\ (n+1)x = nx + x \end{cases}$$

(voir la section 4.7 du volume 2), et pour tout $n < 0$

$$nx \overset{\text{def}}{=\!=} -(-nx)$$

Cette opération vérifie notamment les propriétés suivantes : si x et y sont des éléments de G, alors pour tous les entiers relatifs n et p

$$\begin{cases} (n+p)x = nx + px \\ (np)x = n(px) \\ n(x+y) = nx + ny \end{cases}$$

et si x et y sont des éléments d'un anneau A

$$\begin{cases} (nx)y = n(xy) = x(ny) \\ (n1_A)x = nx = x(n1_A) \end{cases}$$

Définition 1.1.1 (Caractéristique d'un anneau)
Pour tout anneau A, la fonction

$$f : \begin{cases} \mathbb{Z} \longrightarrow A \\ n \longmapsto n1_A \end{cases}$$

est le seul morphisme d'anneaux de $\mathbb{Z}$ dans A.

- On appelle *caractéristique* de A l'unique entier naturel p tel que

$$\mathrm{Ker}(f) = p\mathbb{Z}$$

  c'est-à-dire tel que pour tout $n \in \mathbb{Z}$, $n1_A = 0$ si et seulement si n est un multiple de p.
- L'image de f est donc un sous-anneau de A isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
- En particulier, si $p = 0$ alors l'image de f est isomorphe à $\mathbb{Z}$ et A est infini.

Preuve
- La fonction indiquée est bien un morphisme d'anneaux, car $f(1) = 1_A$, et pour tous les éléments n et p de $\mathbb{Z}$

$$\begin{cases} f(n+p) = (n+p)1_A = n1_A + p1_A = f(n) + f(p) \\ f(n \times p) = (n \times p)1_A = n(p1_A) = (n1_A) \times (p1_A) = f(n) \times f(p) \end{cases}$$

- Il y a de plus unicité, car si g est un morphisme de $\mathbb{Z}$ dans A, on a $f(1) = 1_A = g(1)$, et par conséquent f et g sont deux morphismes d'anneaux (donc aussi de groupes) qui coïncident sur une partie génératrice du groupe $(\mathbb{Z}, +)$ (car 1 est générateur), donc $f = g$.
- Enfin, on sait que le noyau de f est un idéal de $\mathbb{Z}$, qui est donc nécessairement de la forme $p\mathbb{Z}$, avec $p \in \mathbb{N}$. On en déduit que l'image de f est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ (premier théorème d'isomorphisme pour les anneaux).

Exemple 1.1.2
- Dans un anneau de caractéristique 2, comme $\mathbb{Z}/2\mathbb{Z}$, on a $1 + 1 = 0$.
- Dans un anneau de caractéristique 3, comme $\mathbb{Z}/3\mathbb{Z}$, on a $1 + 1 + 1 = 0$.
- Un anneau est de caractéristique 1 si et seulement si c'est un anneau trivial (c'est-à-dire si et seulement si $1 = 0$).
- $\mathbb{Z}$ est un anneau de caractéristique nulle.

Remarque 1.1.3 : On notera en particulier qu'un anneau de caractéristique nulle (c'est-à-dire tel que $n1 = 0$ si et seulement si $n = 0$) est infini, et contient un sous-anneau isomorphe à $\mathbb{Z}$ (et par contraposition, un anneau fini est de caractéristique non nulle).

Remarque 1.1.4 : Si a est un élément d'un anneau de caractéristique $p > 0$, alors $pa = 0$ (car $pa = (p1) \times a$).

Remarque 1.1.5 : Si a est un élément d'un anneau intègre de caractéristique nulle, et $n \in \mathbb{Z}$, alors

$$na = 0 \iff (n = 0) \text{ ou } (a = 0)$$

car $na = (n1)a$. On en déduit aussi que si $p \in \mathbb{Z}$

$$na = pa \iff (n = p) \text{ ou } (a = 0)$$

car $na = pa$ si et seulement si $(n - p)a = 0$.

Théorème 1.1.6

1. Pour tout ensemble E et tout anneau A, la caractéristique de l'anneau $E \longrightarrow A$ est celle de A.
2. Un sous-anneau d'un anneau A a la même caractéristique que A.
3. La caractéristique d'un anneau non trivial sans diviseur de zéro (ce qui est notamment le cas d'un anneau intègre ou d'un corps) est soit 0 soit un nombre premier.

Preuve

On considère un anneau A de caractéristique p.

1. L'élément unité de l'anneau $E \longrightarrow A$ est la fonction constante égale à 1, notons-la k, et pour tout $n \in \mathbb{Z}$, nk est la fonction nulle si et seulement si $n1 = 0$.
2. Si A' est un sous-anneau de A, alors pour tout entier relatif n, $n1$ est un élément de A', donc la caractéristique de A' est celle de A.
3. Si A est non trivial (donc $p \neq 1$) et n'a pas de diviseur de zéro, c'est aussi le cas de l'image de la fonction $n \longmapsto n1$, qui est un sous-anneau de A isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On en déduit que $\mathbb{Z}/p\mathbb{Z}$ est intègre, donc soit $p = 0$ soit p est premier. On pouvait aussi démontrer directement le résultat : si A est de caractéristique $p \neq 0$, alors $p > 1$ (puisque $p \neq 1$). Si p n'est pas premier, alors il existe $a > 1$ et $b > 1$ tels que $p = ab$. On en déduit

$$(a1)(b1) = p1 = 0$$

donc l'un des éléments est nul, par exemple $a1$, et par conséquent a est un multiple de p, ce qui est contradictoire.

1.2 Compléments sur les groupes et les anneaux ordonnés

Je donne dans cette section diverses propriétés, en rapport avec les groupes ou les anneaux ordonnés (et en particulier les anneaux totalement ordonnés), que je pourrai être amené à utiliser dans la suite (notamment dans le chapitre 5 où je construis et étudie les corps totalement ordonnés $\mathbb{Q}$ et $\mathbb{R}$).

Théorème 1.2.1

On considère un groupe ordonné $(G, +, 0)$ et $a \in G$.

- Si $a < 0$, alors pour tout entier naturel non nul n, $na < 0$.
- Si $a > 0$, alors pour tout entier naturel non nul n, $na > 0$.

Preuve

On a le résultat par une récurrence immédiate, par exemple si $a < 0$: $1a < 0$ et si n est un entier non nul tel que $na < 0$ alors

$$(n + 1)a = na + a < 0$$

Remarque 1.2.2 : Si l'ordre n'est pas total, il est possible que a et 0 ne soient pas comparables.

Théorème 1.2.3 (Corollaire)

Tout anneau non trivial totalement ordonné a pour caractéristique 0 (c'est donc en particulier le cas de tout corps totalement ordonné, et de tout anneau intègre totalement ordonné).

Preuve

Dans un anneau non trivial totalement ordonné on a $1 > 0$. On en déduit que pour tout $n \in \mathbb{N}^*$, $n1 > 0$, donc $n1 \neq 0$, et par conséquent la caractéristique de l'anneau est nulle.

Ces pages ne sont pas incluses dans l'aperçu.

Le volume 4 des
Éléments de mathématiques pour le XXI^e siècle
(ISBN : 978-2-9569666-4-7) est disponible
en version papier et numérique.
Détails sur le site *Paysages Mathématiques* :
https://paysmaths.net/boutique

Chapitre 2

Analyse combinatoire

2.1 Rappels et compléments

Nous avons vu dans les volumes précédents plusieurs principes permettant de compter le nombre d'éléments d'un ensemble fini, notamment :

1. Un principe multiplicatif : pour tous les ensembles finis $A_1, \dots, A_n$ $(n \geqslant 1)$

$$\left|\prod_{k=1}^{n} A_k\right| = \prod_{k=1}^{n} |A_k|$$

En particulier (en prenant n fois un même ensemble), pour tout ensemble fini A

$$|A^n| = |A|^n$$

Ceci est aussi le nombre de fonctions d'un ensemble à n éléments dans A, autrement dit pour tous les ensembles finis A et B

$$|B \longrightarrow A| = |A|^{|B|}$$

On en déduit aussi (via la bijection entre $\mathscr{P}(B)$ et $B \longrightarrow \{0,1\}$)

$$|\mathscr{P}(B)| = 2^{|B|}$$

2. Un principe additif : pour tous les ensembles finis deux à deux disjoints $A_1, \dots, A_n$ $(n \geqslant 1)$

$$\left|\bigcup_{k=1}^{n} A_k\right| = \sum_{k=1}^{n} |A_k|$$

On en déduit les résultats suivants :

- Pour tout sous-ensemble A d'un ensemble E

$$|E| = |A| + \left|\complement A\right|$$

ce qui donne l'expression du cardinal d'un ensemble en fonction de celui de son complémentaire :

$$|A| = |E| - \left|\complement A\right|$$

- Si les A_k forment une partition d'un ensemble E

$$|E| = \sum_{k=1}^{n} \left|A_k\right|$$

et si les A_k ont le même cardinal p

$$|E| = np$$

- Lemme des bergers : puisque les fibres non vides d'une fonction $A \xrightarrow{f} B$ (A ensemble fini) forment une partition de A (pour la relation d'équivalence $x \sim y \overset{\text{def}}{\equiv} f(x) = f(y)$)

$$|A| = \sum_{y \in B} \left| \underset{\leftarrow}{f}(\{y\}) \right|$$

  En particulier si les fibres de f ont le même cardinal non nul p (f est alors surjective car les fibres sont non vides, donc B est fini)

$$|A| = p \times |B|$$

- Pour tout sous-ensemble E de $A \times B$ (A et B ensembles finis)

$$|E| = \sum_{a \in A} |\{b \in B \,;\, (a,b) \in E\}| = \sum_{b \in B} |\{a \in A \,;\, (a,b) \in E\}|$$

Exemple 2.1.1
Prouvons que pour tout entier naturel n

$$\left| \left\{ (i,j) \in [1,n]^2 \,;\, i \leqslant j \right\} \right| = \frac{n(n+1)}{2}$$

De manière informelle, pour tout j entre 1 et n, il y a j couples (i,j) tels que $i \leqslant j$ donc le nombre de couples (i,j) tels que $i \leqslant j$ est

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

Plus formellement, en notant $E \overset{\text{def}}{\equiv} \left\{ (i,j) \in [1,n]^2 \,;\, i \leqslant j \right\}$, on a

$$|E| = \sum_{j \in [1,n]} |\{i \in [1,n] \,;\, (i,j) \in E\}| = \sum_{j \in [1,n]} |\{i \in [1,n] \,;\, i \leqslant j\}| = \sum_{j \in [1,n]} |[1,j]| = \sum_{j=1}^{n} j = \frac{n(n+1)}{2}$$

On a aussi la généralisation suivante du principe additif (formule du crible de Poincaré) : pour tous les ensembles finis $A_1, \ldots, A_n$ ($n \geqslant 1$)

$$\begin{aligned} \left| \bigcup_{k=1}^{n} A_k \right| &= \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \left| A_{i_1} \cap \cdots \cap A_{i_k} \right| \\ &= \left(\left|A_1\right| + \cdots + \left|A_n\right| \right) - \left(\left|A_1 \cap A_2\right| + \cdots + \left|A_1 \cap A_n\right| + \cdots + \left|A_{n-1} \cap A_n\right| \right) + \left(\left|A_1 \cap A_2 \cap A_3\right| + \cdots \right) \cdots \end{aligned}$$

3. Un principe de comparaison du cardinal de deux ensembles à partir d'une fonction entre les deux ; pour toute fonction $A \xrightarrow{f} B$:
   - Si f est bijective alors A est fini si et seulement si B est fini, et alors $|A| = |B|$.
   - Si f est injective et B fini, alors A est fini et $|A| \leqslant |B|$. On en déduit aussi par contraposition le principe des tiroirs : si A et B sont deux ensembles finis tels que $|A| > |B|$, alors il existe deux éléments distincts x et y de A tels que $f(x) = f(y)$.
   - Dans le cas particulier où f est l'injection canonique, donc quand $A \subseteq B$: si B est fini alors A est fini et $|A| \leqslant |B|$. De plus

$$|A| = |B| \iff A = B$$

- Si f est surjective et A fini, alors B est fini et $|A| \geqslant |B|$.
- Si A est fini alors $\mathrm{Im}(f)$ est fini et $|\mathrm{Im}(f)| \leqslant |A|$; de plus, $|\mathrm{Im}(f)| = |A|$ si et seulement si f est injective.
- Si A et B sont deux ensembles finis de même cardinal, alors

$$f \text{ est injective} \quad \equiv \quad f \text{ est surjective} \quad \equiv \quad f \text{ est bijective}$$

De plus, si A et B sont des ensembles finis tels que $|A| = |B|$ (respectivement $|A| \leqslant |B|$, $|A| \geqslant |B|$), alors il existe une bijection (respectivement une injection, une surjection) de A dans B.

2.2 *Twelvefold way*

Le *twelvefold way* (que l'on peut traduire par *voie dodécuple*[1]) est une manière de classer de façon systématique 12 situations de combinatoire (comprenant notamment les cas classiques du calcul du nombre de listes, d'arrangements, de permutations, et de combinaisons avec ou sans répétition). Ce mode d'organisation de différents problèmes de dénombrement est due à Richard P. Stanley[2], qui attribue l'idée à G.-C. Rota et l'expression *twelvefold way* à Joel Spencer. Le problème est le suivant : il s'agit de compter le nombre de façons de ranger k objets, par exemple des balles, dans n contenants, par exemple des boîtes, sachant que :

- D'une part, les balles et les boîtes peuvent être
  - soit discernables, c'est-à-dire que l'on peut attribuer une « étiquette » distincte à chacune, comme une couleur, un numéro, etc. ;
  - soit indiscernables (dans le cas contraire).

  Ce qui donne quatre situations possibles (balles et boîtes discernables, balles et boîtes indiscernables, balles discernables et boîtes indiscernables, balles indiscernables et boîtes discernables).
- D'autre part, on peut éventuellement imposer deux conditions supplémentaires sur le nombre de balles par boîte, de telle sorte que l'on obtient les trois possibilités suivantes :
  - chaque boîte doit contenir au plus une balle (ce n'est possible que si $k \leqslant n$) ;
  - chaque boîte doit contenir au moins une balle (ce n'est possible que si $k \geqslant n$) ;
  - aucune contrainte n'est imposée.

En combinant chacune des quatre premières possibilités avec chacune des trois autres, on obtient bien un total de 12 situations possibles. Voyons maintenant comment formaliser ces différents problèmes, qui seront traités en détail dans les sections qui suivent (dans un autre ordre que celui présenté ici, car certains des résultats peuvent dépendre d'autres).

Cas 1 : ranger k balles discernables dans n boîtes discernables

C'est probablement le cas dont la formalisation est la plus directe. La situation revient à associer à chaque élément d'un ensemble E de cardinal k (les k balles), un élément d'un ensemble F de cardinal n (les n boîtes). Le problème est donc de compter le nombre de fonctions de E dans F, avec éventuellement des contraintes supplémentaires. On a ainsi les trois cas suivants :

- aucune contrainte n'est imposée : on cherche le nombre de fonctions de E dans F ;
- chaque boîte doit contenir au moins une balle : on cherche le nombre de surjections de E dans F ;
- chaque boîte doit contenir au plus une balle : on cherche le nombre d'injections de E dans F.

1. Mais l'expression n'est pas usitée en français.
2. Richard P. STANLEY. *Enumerative Combinatorics*. T. 1. Cambridge University Press, 1997.

Comme le nombre de fonctions (respectivement d'injections, de surjections) d'un ensemble dans un autre ne change pas si on remplace un des ensembles par un autre de même cardinal, on peut étudier le problème, en toute généralité, en prenant n'importe quels ensembles de cardinaux respectifs k et n. Je prendrai dans la suite les ensembles $[1, k]$ et $[1, n]$. Il s'agit donc de déterminer le nombre de fonctions, le nombre d'injections, et le nombre de surjections de $[1, k]$ dans $[1, n]$. Je noterai

- $\mathcal{S}_n$ l'ensemble des permutations de $[1, n]$;
- $\mathrm{Inj}_{k,n}$ l'ensemble des injections de $[1, k]$ dans $[1, n]$;
- $\mathrm{Surj}_{k,n}$ l'ensemble des surjections de $[1, k]$ dans $[1, n]$.

Je rappelle que nous avons déjà vu dans les volumes précédents que le nombre de fonctions de $[1, k]$ dans $[1, n]$ est de n^k, qu'il n'y a des injections que si $k \leqslant n$ (on retrouve la condition associée à la situation où chaque boîte doit contenir au plus une balle), et qu'il n'y a des surjections que si $k \geqslant n$ (on retrouve la condition associée à la situation où chaque boîte doit contenir au moins une balle) ; par conséquent si $k > n$ alors le nombre d'injections est égal à 0 et si $k < n$ alors le nombre de surjections est égal à 0.

Par exemple si $k = 2$ et $n = 3$ (on range 2 balles discernables dans 3 boîtes discernables), et en notant les fonctions de $[1, 2] \longrightarrow [1, 3]$ comme des éléments de $[1, 3]^2$: les 9 fonctions possibles (3^2) sont

$$(1,1) \quad (1,2) \quad (1,3) \quad (2,1) \quad (2,2) \quad (2,3) \quad (3,1) \quad (3,2) \quad (3,3)$$

La fonction $(1, 1)$ représente la situation où les balles 1 et 2 sont dans la boîte 1, la fonction $(1, 2)$ représente la situation où la balle 1 est dans la boîte 1 et la balle 2 dans la boîte 2, etc. Et les 6 injections possibles (quand une boîte contient au plus une balle) sont

$$(1,2) \quad (1,3) \quad (2,1) \quad (2,3) \quad (3,1) \quad (3,2)$$

Dans cet exemple il ne peut pas y avoir de surjection puisque $2 < 3$, mais si on se place dans $[1, 3] \longrightarrow [1, 2]$, alors parmi les 8 situations possibles (2^3), on trouve 6 surjections (situations où chaque boîte contient au moins une balle) :

$$(1,1,2) \quad (1,2,1) \quad (1,2,2) \quad (2,1,1) \quad (2,1,2) \quad (2,2,1)$$

Notons enfin une autre façon d'interpréter ce premier cas : ranger k balles discernables dans n boîtes discernables, ou se donner une fonction de $[1, k]$ dans $[1, n]$, revient à se donner une k-liste d'éléments d'un ensemble de cardinal n (comme dans les exemples précédents). Cela revient donc à choisir, dans un ordre donné, k objets (discernables) parmi n, dans les trois cas suivants :

- avec des répétitions possibles, quand aucune contrainte n'est indiquée (on peut choisir plusieurs fois un même objet) ;
- avec des répétitions possibles, et de telle sorte qu'à la fin les n objets aient été choisis, quand la fonction doit être surjective ;
- sans répétition, quand la fonction doit être injective (on ne peut pas choisir plusieurs fois le même objet).

Par exemple si $k = 2$ et $n = 3$, et toujours avec les notations précédentes, la fonction $(1, 1)$ représente la situation où l'on a choisi deux fois consécutives l'objet 1, la fonction $(1, 2)$ représente la situation où l'on a choisi l'objet 1 puis l'objet 2, etc. Et si $k = 3$ et $n = 2$, la fonction $(1, 1, 2)$ représente la situation où l'on a choisi deux fois consécutives l'objet 1, puis l'objet 2, etc.

Cas 2 : ranger k balles indiscernables dans n boîtes discernables

Une façon de formaliser cette situation est de reprendre le principe précédent des fonctions de $[1,k]$ dans $[1,n]$, mais en considérant que les éléments de $[1,k]$ sont indiscernables. Cela revient à dire que deux fonctions $[1,k] \underset{g}{\overset{f}{\rightrightarrows}} [1,n]$ sont d'une certaine façon « égales » lorsqu'on permute les éléments de $[1,k]$, c'est-à-dire lorsqu'elles vérifient la relation d'équivalence suivante :

$$f \sim g \overset{\text{def}}{\equiv} \exists \sigma \in \mathfrak{S}_k, f = g \circ \sigma$$

Le nombre de façons de ranger k balles indiscernables dans n boîtes discernables est alors le nombre de classes d'équivalence. Et comme f est injective (respectivement surjective) si et seulement si g est injective (respectivement surjective), on peut interpréter les deux contraintes supplémentaires comme dans le cas précédent (la situation où chaque boîte contient au moins une balle est celle des classes d'équivalence des fonctions surjectives, et la situation où chaque boîte contient au plus une balle est celle des classes d'équivalence des fonctions injectives).

Par exemple si $k = 2$ et $n = 3$, les classes d'équivalence des fonctions de $[1,2] \longrightarrow [1,3]$ sont :

$$\{(1,1)\} \quad \{(2,2)\} \quad \{(3,3)\} \quad \{(1,2),(2,1)\} \quad \{(1,3),(3,1)\} \quad \{(2,3),(3,2)\}$$

Il y a donc 6 façons de ranger 2 balles indiscernables dans 3 boîtes discernables ; par exemple la classe $\{(1,1)\}$ correspond à la situation où les deux balles sont dans la boîte 1, la classe $\{(1,2),(2,1)\}$ correspond à la situation où il y a une balle dans la boîte 1 et une balle dans la boîte 2, etc. Les classes d'équivalence des fonctions injectives sont

$$\{(1,2),(2,1)\} \quad \{(1,3),(3,1)\} \quad \{(2,3),(3,2)\}$$

(il y a 3 façons de ranger 2 balles indiscernables dans 3 boîtes discernables, de telle sorte que chaque boîte contienne au plus une balle).

Ce deuxième cas revient aussi à définir une fonction f de $[1,n]$ dans $\mathbb{N}$ (qui, à chaque boîte, associe le nombre de balles qu'elle contient), de telle sorte que la somme des images soit égale à k (les balles sont toutes dans l'une des boîtes), c'est-à-dire que l'on a

$$f(1) + \cdots + f(n) = k$$

Puisque se donner une fonction de $[1,n]$ dans $\mathbb{N}$ équivaut à se donner une n-liste d'entiers, définir une telle fonction f équivaut donc aussi à donner une n-liste d'entiers $(x_1, \ldots, x_n)$ vérifiant l'équation

$$x_1 + \cdots + x_n = k$$

On a les trois cas suivants :

- aucune contrainte n'est imposée : on cherche le nombre de solutions de l'équation dans $\mathbb{N}^n$;
- chaque boîte doit contenir au moins une balle (cela n'est possible que si $k \geqslant n$) : la fonction f est à valeurs dans $\mathbb{N}^*$, autrement dit on cherche le nombre de solutions de l'équation dans $(\mathbb{N}^*)^n$;
- chaque boîte doit contenir au plus une balle (cela n'est possible que si $k \leqslant n$) : la fonction f est à valeurs dans $\{0,1\}$, autrement dit on cherche le nombre de solutions de l'équation dans $\{0,1\}^n$. Et comme se donner une fonction de $[1,n]$ dans $\{0,1\}$ équivaut à se donner une partie de $[1,n]$ (l'ensemble des éléments dont l'image est égale à 1), la situation équivaut à se donner une partie de $[1,n]$ ayant exactement k éléments.

  Par exemple si $k = 2$ et $n = 3$, les 6 solutions de l'équation

$$x_1 + x_2 + x_3 = 2$$

dans $\mathbb{N}^3$ sont

$$(0,0,2) \quad (0,1,1) \quad (0,2,0) \quad (1,0,1) \quad (1,1,0) \quad (2,0,0)$$

et les 3 solutions de l'équation dans $\{0,1\}^3$ sont

$$(0,1,1) \quad (1,0,1) \quad (1,1,0)$$

ce qui équivaut aux 3 parties à 2 éléments de $[1,3]$:

$$\{2,3\} \quad \{1,3\} \quad \{1,2\}$$

Dans cet exemple il ne peut pas y avoir de solution dans $(\mathbb{N}^*)^3$ puisque $2 < 3$, mais si $k = 3$ et $n = 2$ les deux solutions de l'équation

$$x_1 + x_2 = 3$$

dans $(\mathbb{N}^*)^2$ sont

$$(1,2) \quad (2,1)$$

Enfin, comme précédemment, il est possible d'interpréter ce deuxième cas de la façon suivante : ranger k balles indiscernables dans n boîtes discernables, ou se donner une équation de la forme

$$x_1 + \cdots + x_n = k$$

revient à choisir, sans ordre particulier, k objets (discernables) parmi n (chaque x_i représente le nombre de fois où l'objet i a été choisi), dans les trois cas suivants :

- avec des répétitions possibles, quand aucune contrainte n'est indiquée, et que l'on peut donc choisir plusieurs fois un même objet (les x_i sont des entiers quelconques) ;
- avec des répétitions possibles, et de telle sorte que les n objets soient choisis, quand les x_i sont non nuls ;
- sans répétition, quand on ne peut pas choisir plusieurs fois le même objet (les x_i appartiennent à $\{0,1\}$), ce qui revient à choisir un sous-ensemble de cardinal k de l'ensemble des objets.

Par exemple si $k = 2$ et $n = 3$, la solution $(0,0,2)$ de l'équation représente la situation où l'on a choisi deux fois l'objet 3, la solution $(0,1,1)$ représente la situation où l'on a choisi une fois l'objet 2 et une fois l'objet 3, etc.

Cas 3 : ranger k balles discernables dans n boîtes indiscernables

Comme précédemment, on peut formaliser cette situation en cherchant les classes d'équivalence de la relation d'équivalence telle que pour tout $[1,k] \underset{g}{\overset{f}{\rightrightarrows}} [1,n]$

$$f \sim g \overset{\text{def}}{\equiv} \exists \sigma \in \mathfrak{S}_n, f = \sigma \circ g$$

(on peut permuter les éléments de $[1,n]$).

Mais cela revient aussi à effectuer un recouvrement de l'ensemble $[1,k]$ (représentant les k balles) avec n ensembles deux à deux disjoints (chacun représentant une des boîtes), autrement dit on se donne une famille de sous-ensembles deux à deux disjoints de $[1,k]$ dont l'union est $[1,k]$; toutes les balles sont bien dans une boîte grâce au recouvrement, et chaque balle n'est que dans une seule boîte car les ensembles sont deux à deux disjoints. On a de plus les trois cas suivants :

- les n ensembles doivent être non vides (chaque boîte doit contenir au moins une balle, ce qui n'est possible que si $k \geqslant n$), autrement dit on effectue une partition de $[1, k]$ en n ensembles (non vides par définition d'une partition) ; et puisqu'il est équivalent de se donner une partition ou une relation d'équivalence, le nombre de partitions est aussi égal au nombre de relations d'équivalence sur $[1, k]$ ayant n classes d'équivalence. Par exemple si $k = 5$ et $n = 3$, on peut avoir la partition

  $$\{1\}, \{2, 4\}, \{3, 5\}$$

  et si $k = 3$ et $n = 2$, il y a en tout 3 partitions possibles :

  $$\{\{1\}, \{2, 3\}\} \quad \{\{2\}, \{1, 3\}\} \quad \{\{3\}, \{1, 2\}\}$$

- aucune contrainte n'est imposée (certains des n ensembles peuvent être vides, contrairement au cas précédent) ; par exemple, si $k = 5$ et $n = 3$, on peut avoir le recouvrement

  $$\varnothing, \{1, 5\}, \{2, 3, 4\}$$

  et si $k = 2$ et $n = 3$, il y a en tout deux recouvrements possibles :

  $$\{\varnothing, \varnothing, \{1, 2\}\} \quad \{\varnothing, \{1\}, \{2\}\}$$

- les n ensembles doivent avoir au plus un élément (chaque boîte doit contenir au plus une balle) ; il n'y a qu'une situation possible (si $k \leqslant n$) : la partition de $[1, k]$ en k ensembles

  $$\{1\} \quad \{2\} \quad \dots \quad \{k\}$$

  et les $(n - k)$ ensembles restants vides.

Cas 4 : ranger k balles indiscernables dans n boîtes indiscernables

Comme précédemment, on peut formaliser cette situation en cherchant les classes d'équivalence de la relation d'équivalence telle que pour tout $[1, k] \underset{g}{\overset{f}{\rightrightarrows}} [1, n]$

$$f \sim g \overset{\text{def}}{\equiv} \exists \sigma \in \mathfrak{S}_k, \exists \sigma' \in \mathfrak{S}_n, f = \sigma' \circ g \circ \sigma$$

(on peut permuter à la fois les éléments de $[1, k]$ et ceux de $[1, n]$).

Mais cela revient aussi à décomposer le nombre k en la somme de n nombres entiers (chacun de ces n entiers représentant le nombre de balles dans une boîte). On a les cas suivants :

- aucune contrainte n'est imposée ; par exemple si $k = 5$ et $n = 3$, on peut avoir la décomposition

  $$5 = 0 + 1 + 4$$

  (une boîte ne contient pas de balle, une boîte contient 1 balle et une boîte contient 4 balles), et si $k = 2$ et $n = 3$ il n'y a que deux décompositions possibles :

  $$2 = 0 + 0 + 2 = 0 + 1 + 1$$

  (une boîte contient les deux balles, ou chacune des deux balles est dans une boîte différente) ;

- chaque boîte doit contenir au moins une balle : les n nombres entiers doivent être non nuls (ce qui n'est possible que si $k \geqslant n$) ; par exemple si $k = 5$ et $n = 3$, on peut avoir la décomposition

  $$5 = 1 + 2 + 2$$

  et si $k = 3$ et $n = 2$ il n'y a qu'une décomposition possible :

  $$3 = 1 + 2$$

- chaque boîte doit contenir au plus une balle : les n nombres entiers doivent être dans l'ensemble $\{0,1\}$; il n'y a alors qu'une possibilité (si $k \leqslant n$) : k s'écrit comme la somme de k nombres 1 et de $(n-k)$ nombres 0 :

$$k = \underbrace{1+\cdots+1}_{k \text{ fois}} + \underbrace{0+\cdots+0}_{(n-k) \text{ fois}}$$

Synthèse

	Pas de contrainte sur les balles (ou choix d'objets avec répétition)	Au moins une balle (ou choix d'objets avec répétition, tous choisis)	Au plus une balle (ou choix d'objets sans répétition)
k balles discernables dans n boîtes discernables (ou choix ordonné de k objets parmi n)	$[1,k] \longrightarrow [1,n]$	$\mathrm{Surj}_{k,n}$	$\mathrm{Inj}_{k,n}$
k balles indiscernables dans n boîtes discernables (ou choix non ordonné de k objets parmi n)	Solutions dans $\mathbb{N}^n$ de $x_1+\cdots+x_n=k$	Solutions dans $(\mathbb{N}^*)^n$ de $x_1+\cdots+x_n=k$	Solutions dans $\{0,1\}^n$ de $x_1+\cdots+x_n=k$ Parties de $[1,n]$ à k éléments
		0 si $k < n$	**0 si $k > n$**

	Pas de contrainte	Au moins une balle	Au plus une balle
k balles discernables dans n boîtes indiscernables	Recouvrement de $[1,k]$ en n sous-ensembles 2 à 2 disjoints	Partition de $[1,k]$ en n sous-ensembles	$\{1\} \ldots \{k\} \underbrace{\varnothing \ldots \varnothing}_{(n-k) \text{ fois}}$
k balles indiscernables dans n boîtes indiscernables	Décomposition de k en somme de n nombres	Décomposition de k en somme de n nombres non nuls	$k = \underbrace{1+\cdots+1}_{k \text{ fois}} + \underbrace{0+\cdots+0}_{(n-k) \text{ fois}}$
		0 si $k < n$	**0 si $k > n$**

2.3 k-listes

Nous avons vu dans les rappels le principe multiplicatif : pour tous les ensembles finis $A_1, \ldots, A_k$ $(k \geqslant 1)$

$$\left| \prod_{i=1}^{k} A_i \right| = \prod_{i=1}^{k} |A_i|$$

Le cas particulier où les A_i ont le même cardinal n nous donne la première situation parmi les 12 :

Ces pages ne sont pas incluses dans l’aperçu.

Théorème 2.5.9
Pour tout nombre premier p et tout $k \in [1, p-1]$, p divise $\binom{p}{k}$.

Preuve
On a

$$k!\binom{p}{k} = p(p-1)\cdots(p-k+1)$$

donc p divise $k!\binom{p}{k}$. Pour tout $i \in [1, k]$, p et i sont premiers entre eux (car $1 \leqslant i \leqslant k \leqslant p-1$), et par conséquent p et $k!$ sont premiers entre eux. On en déduit, d'après le lemme de Gauss, que p divise $\binom{p}{k}$.

Théorème 2.5.10 (Symétrie des coefficients binomiaux)
On considère deux entiers n et k, avec $k \leqslant n$.

$$\binom{n}{k} = \binom{n}{n-k}$$

Preuve 1 (par calcul)

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

Preuve 2 (par dénombrement)
Soit $n \geqslant 1$ et $k \leqslant n$, et un ensemble E à n éléments. Notons P_k (respectivement P_{n-k}) l'ensemble des sous-ensembles à k éléments (respectivement $n-k$ éléments) de E. Les ensembles P_k et P_{n-k} sont respectivement de cardinal $\binom{n}{k}$ et $\binom{n}{n-k}$. Par ailleurs, les fonctions

$$\begin{cases} P_k \longrightarrow P_{n-k} \\ A \longmapsto \complement A \end{cases} \quad \text{et} \quad \begin{cases} P_{n-k} \longrightarrow P_k \\ A \longmapsto \complement A \end{cases}$$

(qui sont bien définies puisque le complémentaire d'un sous-ensemble à k éléments est un sous-ensemble à $n-k$ éléments, et réciproquement) sont des bijections réciproques. Les ensembles P_k et P_{n-k} ont donc le même cardinal : $\binom{n}{k} = \binom{n}{n-k}$.

Exemple 2.5.11
Dans ce qui suit, on considère que les notations $\binom{n}{k}$, ou $n-k$, impliquent implicitement la condition $n \geqslant k$.

$$\binom{n}{0} = \binom{n}{n} = 1 \qquad \binom{n}{1} = \binom{n}{n-1} = n \qquad \binom{n}{2} = \binom{n}{n-2} = \frac{n(n-1)}{2}$$

Théorème 2.5.12 (Relation de Pascal)
On considère deux entiers $1 \leqslant k \leqslant n$.

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Preuve 1 (par dénombrement)

- Si $n = k$ alors la formule est immédiate puisque

$$\binom{n-1}{k} = \binom{n-1}{n} = 0 \qquad \binom{n-1}{k-1} = \binom{n-1}{n-1} = 1 \qquad \binom{n}{k} = \binom{n}{n} = 1$$

  C'est en particulier le cas si $n = 1$ (alors $k = 1$ puisque $1 \leqslant k \leqslant n$). On suppose dans la suite que $n > k$ (donc $n \geqslant 2$).
- On choisit un élément a quelconque d'un ensemble E ayant n éléments. Le nombre de k-combinaisons de E (c'est-à-dire $\binom{n}{k}$), est égal à la somme du nombre de k-combinaisons qui contiennent a (il y en a $\binom{n-1}{k-1}$ puisqu'on doit choisir les $k-1$ éléments restants de la k-combinaison dans les $n-1$ éléments de $E \setminus \{a\}$), et du nombre de k-combinaisons qui ne contiennent pas a (il y en a $\binom{n-1}{k}$ puisqu'on doit choisir tous les k éléments de la k-combinaison dans les $n-1$ éléments de $E \setminus \{a\}$).

Preuve 2 (par calcul)

Comme précédemment, le cas $n = k$ est immédiat, et on suppose dans la suite que $n > k$ (donc $n \geqslant 2$).

$$\begin{aligned}\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!((n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!} = \frac{(n-k)(n-1)!}{k!(n-k)!} + \frac{k(n-1)!}{k!(n-k)!} \\ &= \frac{(n-1)!(n-k+k)}{k!(n-k)!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}\end{aligned}$$

On peut aussi présenter ce calcul de manière un peu différente :

$$\begin{aligned}\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)(n-2)\cdots(n-k)}{k!} + \frac{(n-1)(n-2)\cdots(n-k+1)}{(k-1)!} \\ &= \frac{(n-1)(n-2)\cdots(n-k+1)(n-k)}{k!} + \frac{k(n-1)(n-2)\cdots(n-k+1)}{k!} \\ &= \frac{(n-1)(n-2)\cdots(n-k+1)\cdot(n-k+k)}{k!} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \binom{n}{k}\end{aligned}$$

On notera que ce calcul reste valide si n est un élément d'un anneau commutatif de caractéristique nulle (où le coefficient binomial peut aussi être défini).

La relation de Pascal permet de calculer les coefficients binomiaux de manière récursive, à partir des égalités $\binom{n}{0} = \binom{n}{n} = 1$, la disposition obtenue s'appelant le triangle de Pascal :

n \ k	0	1	2	3	4	5	6	…
0	1							
1	1	1						
2	1	2	1					
3	1	3	3	1				
4	1	4	6	4	1			
5	1	5	10	10	5	1		
6	1	6	15	20	15	6	1	
…								

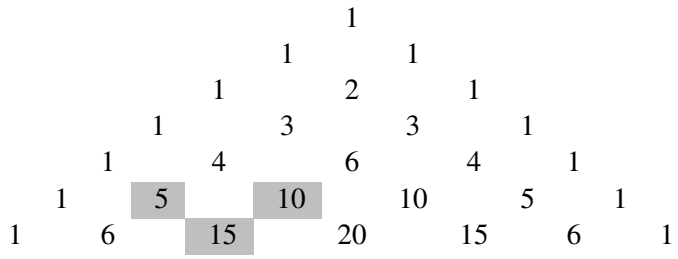
Triangle de Pascal

Si $n > k > 0$, le terme $\binom{n}{k}$ du tableau s'obtient par la somme du terme situé au-dessus, $\binom{n-1}{k}$, et du

terme précédant ce dernier sur sa ligne, $\binom{n-1}{k-1}$. Par exemple (grisé dans le tableau ci-dessus) :

$$\binom{6}{2} = \binom{5}{2} + \binom{5}{1} = 10 + 5 = 15$$

On trouve aussi la disposition suivante pour le triangle de Pascal :



Le triangle est nommé en l'honneur du mathématicien, physicien, philosophe et théologien français Blaise Pascal (1623-1662) qui l'a étudié dans son *Traité du triangle arithmétique* (écrit en 1654 et publié en 1665), mais il était connu plusieurs siècles auparavant de mathématiciens indiens, perses, et chinois. En Inde, le mathématicien Halayudha décrit le triangle au X^{e} siècle, en s'appuyant sur les travaux du mathématicien Pingala (v. 200-400 AEC[4]). En Perse et en Chine, il semble avoir été découvert vers 1100. Il est nommé triangle de Yang Hui en Chine, du nom du mathématicien Yang Hui (v. 1238-1298) qui l'a étudié dans son ouvrage Xiangjie Jiuzhang Suanfa (1261), en attribuant la paternité du triangle au mathématicien Jia Xian (v. 1010-1070). En Europe, il apparaît en 1527 dans l'ouvrage *Rechnung* de l'astronome et mathématicien allemand Petrus Apianus, ou Peter Apian (1495-1552). En Italie, le triangle est connu de nos jours sous le nom de triangle de Tartaglia, du nom du mathématicien Tartaglia (1499-1557) qui l'a étudié. Pascal, dans son traité, démontre plusieurs des propriétés du triangle (nombre de ces propriétés étaient connues mais seulement admises), en utilisant pour la première fois une version explicite de raisonnement par récurrence.

Théorème 2.5.13 (Autres relations de récurrence des coefficients binomiaux)
On considère deux entiers $1 \leqslant k \leqslant n$.

1. Par diagonale (à $n-k$ constant) :
$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$$
2. Par colonne (à k constant) :
$$\binom{n}{k} = \frac{n}{n-k}\binom{n-1}{k}$$
3. Par ligne (à n constant) :
$$\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}$$

Preuve 1 (par dénombrement)
1. Les deux nombres $\binom{n}{k} \times k$ et $n \times \binom{n-1}{k-1}$ représentent tous les deux le nombre de couples (A, a), où A est une partie de $[1, n]$ à k éléments et $a \in A$ (on peut choisir d'abord A parmi les parties à k éléments de $[1, n]$, puis a parmi les k

4. J'utilise l'abréviation AEC (avant l'ère commune), au lieu du plus classique av. J.-C. (avant Jésus-Christ), pour noter les dates correspondant aux années d'avant notre ère. Outre l'intérêt d'être culturellement neutre, et sans référence à une quelconque mythologie, cette notation est plus simple et plus esthétique.

Ces pages ne sont pas incluses dans l’aperçu.

Chapitre 3

Compléments sur les groupes

Prérequis
Les groupes et groupes quotients (notamment la section 2.7 du volume 2 et la section 4.1 du volume 3).

3.1 Ordre d'un groupe, indice d'un sous-groupe

Nous avons vu que pour tout sous-groupe H d'un groupe G, on peut notamment définir les deux relations d'équivalence suivantes sur G :

- La relation
$$a \sim_g b \overset{\text{def}}{\iff} a^{-1}b \in H$$
qui est compatible à gauche avec la loi interne, et pour laquelle la classe d'équivalence de a est aH (on l'appelle la classe à gauche de a suivant H, ou modulo H). Je noterai $(G/H)_g$ l'ensemble quotient associé.
- La relation
$$a \sim_d b \overset{\text{def}}{\iff} ab^{-1} \in H$$
qui est compatible à droite avec la loi interne, et pour laquelle la classe d'équivalence de a est Ha (on l'appelle la classe à droite de a suivant H, ou modulo H). Je noterai $(G/H)_d$ l'ensemble quotient associé.

Si H est un sous-groupe normal (ce qui est automatiquement le cas si G est un groupe commutatif), alors les classes à droite et à gauche coïncident ($aH = Ha$), et on peut munir l'ensemble quotient d'une structure de groupe, par la loi
$$aH * bH \overset{\text{def}}{\iff} abH$$

Théorème 3.1.1
Pour tout élément a d'un groupe G, et tout sous-groupe H de G

- la translation à gauche tg_a ($x \longmapsto ax$) induit une bijection de H dans aH, dont la bijection réciproque est induite par la translation à gauche $\mathrm{tg}_{a^{-1}}$;
- la translation à droite td_a ($x \longmapsto xa$) induit une bijection de H dans Ha, dont la bijection réciproque est induite par la translation à droite $\mathrm{td}_{a^{-1}}$.

On en déduit
$$|H| = |aH| = |Ha|$$

Preuve
Les fonctions

$$\mathrm{tg}_a : \begin{cases} H \longrightarrow aH \\ x \longmapsto ax \end{cases} \qquad \text{et} \qquad \mathrm{tg}_{a^{-1}} : \begin{cases} aH \longrightarrow H \\ x \longmapsto a^{-1}x \end{cases}$$

sont bien définies par définition de aH, et réciproques l'une de l'autre. Le raisonnement est semblable pour les translations à droite.

Remarque 3.1.2 : On en déduit aussi que pour tout a et b

$$|Ha| = |aH| = |bH| = |Hb|$$

(le cardinal commun étant celui de H), autrement dit les classes à gauche et les classes à droite ont toutes le même cardinal $|H|$.

Théorème 3.1.3 (Indice d'un sous-groupe)
Pour tout sous-groupe H d'un groupe G, les ensembles quotients $(G/H)_g$ et $(G/H)_d$ sont équipotents, par les bijections réciproques

$$\begin{cases} (G/H)_g \longrightarrow (G/H)_d \\ xH \longmapsto Hx^{-1} \end{cases} \qquad \text{et} \qquad \begin{cases} (G/H)_d \longrightarrow (G/H)_g \\ Hx \longmapsto x^{-1}H \end{cases}$$

Si G est fini, alors $(G/H)_g$ et $(G/H)_d$ sont des ensembles finis, dont le cardinal commun s'appelle *l'indice de H dans G*. On le note $(G : H)$:

$$(G : H) \overset{\text{def}}{=\!=} \left|(G/H)_g\right| = \left|(G/H)_d\right|$$

Preuve
La fonction

$$\varphi : \begin{cases} (G/H)_g \longrightarrow (G/H)_d \\ xH \longmapsto Hx^{-1} \end{cases}$$

est bien définie, par passage au quotient, car la fonction

$$f : \begin{cases} G \longrightarrow (G/H)_d \\ x \longmapsto Hx^{-1} \end{cases}$$

est constante sur les classes d'équivalence à gauche : en effet

$$x \sim_g y \equiv x^{-1}y \in H \equiv x^{-1} \sim_d y^{-1}$$

donc si $x \sim_g y$ alors x^{-1} et y^{-1} ont la même classe à droite, autrement dit $f(x) = f(y)$. On peut définir de la même façon une fonction

$$\varphi' : \begin{cases} (G/H)_d \longrightarrow (G/H)_g \\ Hx \longmapsto x^{-1}H \end{cases}$$

et on voit que φ et φ' sont deux bijections réciproques.

Définition 3.1.4 (Ordre d'un groupe)
On dit que le groupe $(G, *, e)$ est fini lorsque G est fini, et on appelle alors *ordre* du groupe le cardinal de G.

Ces pages ne sont pas incluses dans l’aperçu.

Remarque 3.3.8 : On retrouve le fait qu'un groupe cyclique dont l'ordre n est un nombre premier est engendré par l'un quelconque de ses éléments autre que l'élément neutre (car tous les entiers k tels que $0 < k < n$ sont premiers avec n).

Théorème 3.3.9 (Corollaire)
Pour tout $n \in \mathbb{N}^*$ et tout $k \in \mathbb{Z}$, $[k]$ est un élément générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si k et n sont premiers entre eux. L'ensemble des générateurs de $\mathbb{Z}/n\mathbb{Z}$ est donc

$$\{[k]\ ;\ k \in [0, n-1] \text{ et } \mathrm{PGCD}(k, n) = 1\}$$

Preuve 1 (faisant appel au théorème précédent)
$[1]$ est un élément générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$, car pour tout $k \in \mathbb{Z}$, $k[1] = [k]$. On déduit alors du théorème précédent que $[k]$ est générateur si et seulement si k et n sont premiers entre eux.

Preuve 2 (ne faisant pas appel au théorème précédent)
$[k]$ est un élément générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si il existe $p \in \mathbb{Z}$ tel que

$$[p][k] = [pk] = p[k] = [1]$$

autrement dit si et seulement si $[k]$ est inversible dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, et on sait que cette condition équivaut à : k et n sont premiers entre eux. Ce que l'on pouvait aussi redémontrer directement : la condition

$$[pk] = [1]$$

équivaut à : il existe $p' \in \mathbb{Z}$ tel que

$$pk - 1 = p'n$$

Et d'après le théorème de Bachet-Bézout, cela équivaut à dire que k et n sont premiers entre eux.

On en déduit les équivalences suivantes :

- $[k]$ est un élément générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
- $[k]$ est un élément inversible de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.
- $[k]$ est un élément simplifiable (pour la multiplication) de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.
- k et n sont premiers entre eux.

L'ensemble des éléments générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$, l'ensemble des éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, et l'ensemble des éléments simplifiables (pour la multiplication) de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, sont donc égaux, et cet ensemble est

$$\{[k]\ ;\ (0 \leqslant k \leqslant n-1) \text{ et } \mathrm{PGCD}(k, n) = 1\}$$

D'après le théorème des restes chinois, on sait que si m et n sont premiers entre eux, les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ sont isomorphes. Il en est de même pour les groupes sous-jacents, donc en particulier si m et n sont premiers entre eux, alors $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique (puisque isomorphe au groupe cyclique $\mathbb{Z}/mn\mathbb{Z}$). Cette propriété reste valable pour n'importe quels groupes cycliques (un groupe cyclique d'ordre n étant isomorphe à $\mathbb{Z}/n\mathbb{Z}$), autrement dit si les ordres de deux groupes cycliques sont premiers entre eux, alors le produit des groupes est aussi un groupe cyclique (dont l'ordre, c'est-à-dire le cardinal, est nécessairement le produit des deux ordres). La réciproque est vraie, ce qui donne le théorème suivant :

Théorème 3.3.10 (Caractérisation des produits cycliques)
Si G et G' sont deux groupes finis d'ordre respectif n et n', alors le groupe produit $G \times G'$ est cyclique

si et seulement si G et G' sont cycliques et n et n' premiers entre eux.

Preuve

- On fait l'hypothèse que G et G' sont cycliques et que n et n' sont premiers entre eux. On peut faire appel au théorème des restes chinois comme dans la remarque précédente (G et G' sont respectivement isomorphes à $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/n'\mathbb{Z}$, donc $G \times G'$ est isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$, donc au groupe cyclique $\mathbb{Z}/nn'\mathbb{Z}$), mais on peut aussi justifier directement le résultat : on considère un générateur x de G (donc d'ordre n) et un générateur x' de G' (donc d'ordre n'). On en déduit que l'ordre de (x, x') est le PPCM de n et n', c'est-à-dire nn' (car n et n' sont premiers entre eux), et par conséquent $G \times G'$ est cyclique, engendré par (x, x').
- Réciproquement, on fait l'hypothèse que $G \times G'$ est cyclique, et on considère un élément générateur (x, x') de $G \times G'$, donc d'ordre nn'. Notons m l'ordre de x (dans G) et m' l'ordre de x' (dans G'). On en déduit $\text{PPCM}(m, m') = nn'$, donc nn' divise mm'. Or m divise n et m' divise n', donc il existe des entiers non nuls k et k' tels que

$$\begin{cases} n = km \\ n' = k'm' \end{cases}$$

On en déduit que $kk'mm'$ divise mm', donc $k = k' = 1$, et par conséquent $m = n$ et $m' = n'$, ce qui prouve que G et G' sont cycliques (engendrés respectivement par x et x'). De plus $nn' = \text{PPCM}(m, m') = \text{PPCM}(n, n')$ donc

$$nn' = \text{PGCD}(n, n') \cdot \text{PPCM}(n, n') = \text{PGCD}(n, n') \cdot nn'$$

et par conséquent $\text{PGCD}(n, n') = 1$, autrement dit n et n' sont premiers entre eux.

Théorème 3.3.11 (Corollaire)
Pour tous les entiers non nuls m et n, $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique (donc isomorphe à $\mathbb{Z}/mn\mathbb{Z}$) si et seulement si m et n sont premiers entre eux.

Théorème 3.3.12 (Sous-groupes d'un groupe monogène)
Tout sous-groupe d'un groupe monogène est monogène. Plus précisément, si G est un groupe monogène engendré par a ($G = \langle a \rangle$) :

1. Les sous-groupes de G sont les groupes monogènes $\langle a^n \rangle$, avec $n \in \mathbb{N}$.
2. Si G est un groupe monogène infini, alors ses sous-groupes $\langle a^n \rangle$, avec $n \in \mathbb{N}^*$, sont infinis et distincts.
3. Si G est un groupe cyclique d'ordre n, alors il y a autant de sous-groupes de G que de diviseurs de n. Plus précisément, pour tout diviseur d de n, le groupe cyclique $\langle a^{\frac{n}{d}} \rangle$ est le seul sous-groupe de G d'ordre d. De plus
$$\langle a^{\frac{n}{d}} \rangle = \left\{ x \in G \,;\, x^d = e \right\}$$
On en déduit que pour tout diviseur d de n, le groupe cyclique $\langle a^d \rangle$ est le seul sous-groupe de G d'ordre $\dfrac{n}{d}$, et
$$\langle a^d \rangle = \left\{ x \in G \,;\, x^{\frac{n}{d}} = e \right\}$$

Preuve

1. On considère un sous-groupe H de G et le morphisme de groupes surjectif
$$f : \begin{cases} \mathbb{Z} \longrightarrow G \\ k \longmapsto a^k \end{cases}$$

Ces pages ne sont pas incluses dans l’aperçu.

- Réciproquement, si s et s' sont du même type, on a notamment $m = p$. On considère une permutation σ qui transforme chaque cycle c_i en un des cycles de $c'_1 \cdots c'_p$ (et qui laisse fixe tout point n'appartenant à aucun des supports des cycles c_i), ce qui est possible car s et s' sont du même type (il existe une permutation φ de $[1, p]$ telle que pour tout $i \in [1, p]$, c'_i et $c_{\varphi(i)}$ sont de la même longueur). Et alors $s' = \sigma s \sigma^{-1}$, donc s et s' sont conjuguées.

Théorème 3.6.18 (Décomposition d'un cycle en transpositions)
Pour tous les éléments distincts $a_1, \dots, a_p$ de E

$$\begin{pmatrix} a_1 & a_2 & \dots & a_p \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_2 & a_3 \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_{p-1} & a_p \end{pmatrix}$$

Preuve
On démontre le résultat par récurrence sur p : on a trivialement $\begin{pmatrix} a_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \end{pmatrix}$, et si on fait l'hypothèse de récurrence au rang $p \geqslant 2$, on a

$$\begin{pmatrix} a_1 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_2 & a_3 \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_{p-1} & a_p \end{pmatrix} \circ \begin{pmatrix} a_p & a_{p+1} \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_p \end{pmatrix} \circ \begin{pmatrix} a_p & a_{p+1} \end{pmatrix}$$

et la permutation

$$\sigma \overset{\text{def}}{\equiv} \begin{pmatrix} a_1 & a_2 & \dots & a_p \end{pmatrix} \circ \begin{pmatrix} a_p & a_{p+1} \end{pmatrix}$$

est telle que

- tout $x \notin \{a_1, \dots, a_{p+1}\}$ est un point fixe ;
- pour tout $i \in [1, p-1]$, $\sigma(a_i) = a_{i+1}$;
- $\sigma(a_p) = a_{p+1}$ et $\sigma(a_{p+1}) = a_1$.

On en déduit $\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_p & a_{p+1} \end{pmatrix}$.

Puisqu'une permutation, autre que l'identité, se décompose en un produit de cycles, et qu'un cycle se décompose en produit de transpositions, on en déduit que si $n \geqslant 2$ toute permutation peut se décomposer en produit de transpositions (car c'est aussi le cas de l'identité, qui est le produit d'une transposition quelconque par elle-même), et par conséquent l'ensemble de toutes les transpositions est une partie génératrice du groupe symétrique. D'où le théorème suivant, qui donne aussi d'autres exemples classiques de parties génératrices de $\mathfrak{S}_n$ (liste non exhaustive) :

Théorème 3.6.19 (Exemples de parties génératrices de $\mathfrak{S}_n$)
On considère le groupe symétrique $\mathfrak{S}_n$, avec $n \geqslant 2$.

1. Toute permutation se décompose en un produit de transpositions, et par conséquent l'ensemble
$$\left\{ \begin{pmatrix} i & j \end{pmatrix} ;\ 1 \leqslant i < j \leqslant n \right\}$$
est une partie génératrice de $\mathfrak{S}_n$.
2. Toute permutation se décompose en un produit de transpositions de la forme $\begin{pmatrix} 1 & i \end{pmatrix}$, et par conséquent l'ensemble
$$\left\{ \begin{pmatrix} 1 & i \end{pmatrix} ;\ 1 < i \leqslant n \right\}$$
est une partie génératrice de $\mathfrak{S}_n$.
3. Toute permutation se décompose en un produit de transpositions de la forme $\begin{pmatrix} i & i+1 \end{pmatrix}$, et par conséquent l'ensemble
$$\left\{ \begin{pmatrix} i & i+1 \end{pmatrix} ;\ 1 \leqslant i \leqslant n-1 \right\}$$
est une partie génératrice de $\mathfrak{S}_n$.

4. Toute permutation se décompose en produit faisant intervenir uniquement les deux cycles $(1 \quad 2)$ et $(1 \quad 2 \quad \dots \quad n)$, et par conséquent l'ensemble

$$\{(1 \quad 2), (1 \quad 2 \quad \dots \quad n)\}$$

est une partie génératrice de $\mathcal{S}_n$.

Preuve

Dans le cas où la permutation est l'identité, on obtient une décomposition de la forme souhaitée avec $(1 \quad 2)\circ(1 \quad 2)$ (la transposition $(1 \quad 2)$ fait partie de chacun des quatre exemples de parties génératrices). Pour toute autre permutation, on utilise la décomposition d'une permutation en cycles. Il suffit alors de justifier qu'un cycle se décompose selon chacune des formes indiquées :

1. Nous avons déjà vu qu'un cycle se décompose en produit de transpositions :

$$(a_1 \quad a_2 \quad \dots \quad a_p) = (a_1 \quad a_2)\circ(a_2 \quad a_3)\circ\cdots\circ(a_{p-1} \quad a_p)$$

2. Toute transposition $(a \quad b)$, avec $a \neq 1$ et $b \neq 1$, est telle que

$$(a \quad b) = (1 \quad a)\circ(1 \quad b)\circ(1 \quad a)$$

et par conséquent toute permutation se décompose en un produit de transpositions de la forme $(1 \quad i)$.

3. Démontrons qu'une transposition $(a \quad b)$, avec $a < b$, se décompose en produit de transpositions de la forme $(i \quad i+1)$, par récurrence sur $k \overset{\text{def}}{=} b - a$:
   - Pour $k = 1$ (autrement dit $b = a + 1$), on a directement le résultat.
   - On fait l'hypothèse de récurrence au rang k ($k \geqslant 1$), et on considère a et b tels que $b = a + k + 1$. On a

$$(a \quad b) = (b-1 \quad b)\circ(a \quad b-1)\circ(b-1 \quad b)$$

   et par hypothèse de récurrence $(a \quad b-1)$ se décompose en produit de transpositions de la forme $(i \quad i+1)$.

   On en déduit que toute permutation se décompose en un produit de transpositions de la forme $(i \quad i+1)$.

4. On a

$$(i \quad i+1) = (1 \quad 2 \quad \dots \quad n)^{i-1}\circ(1 \quad 2)\circ(1 \quad 2 \quad \dots \quad n)^{1-i}$$

car, en notant $c \overset{\text{def}}{=} (1 \quad 2 \quad \dots \quad n)$, on a

- $c^{i-1}(1) = i$ par une récurrence immédiate : $c^{1-1}(1) = c^0(1) = 1$, et si $c^{i-1}(1) = i$, avec $1 \leqslant i \leqslant n-1$, alors $c^i(1) = c(c^{i-1}(1)) = c(i) = i+1$;
- et de même $c^{i-1}(2) = i + 1$.

On déduit alors du point précédent que toute permutation se décompose en un produit faisant intervenir uniquement les deux cycles $(1 \quad 2)$ et $(1 \quad 2 \quad \dots \quad n)$.

3.7 Signature, groupe alterné

Il y a unicité de la décomposition d'une permutation en produit de cycles à supports disjoints, mais pas d'une décomposition en transpositions : on peut toujours ajouter $t\circ t$ à toute décomposition (t étant une transposition quelconque), sans altérer le résultat ($\sigma\circ t\circ t = \sigma\circ \mathrm{id} = \sigma$) ; par ailleurs, on peut aussi, par exemple, avoir une décomposition ne faisant intervenir que des transpositions de la forme $(1 \quad i)$, ou que des transpositions de la forme $(i \quad i+1)$). Mais ce qui reste constant, c'est la parité du nombre de transpositions intervenant dans la décomposition. Ceci va nous permettre de classer les permutations en deux catégories : celles qui se décomposent en un nombre pair de transpositions, qu'on appelle des permutations *paires*, et celles qui se décomposent en un nombre impair de transpositions, qu'on appelle des permutations *impaires*. Il est possible de justifier ce résultat de différentes façons, notamment à l'aide de la notion d'*inversion* d'une permutation :

Définition 3.7.1 (Inversion)
Pour toute permutation σ de $\mathfrak{S}_n$, on appelle *inversion de* σ tout couple (i, j) d'éléments de $[1, n]$ tel que

$$\begin{cases} i < j \\ \sigma(i) > \sigma(j) \end{cases}$$

Théorème 3.7.2
Toute transposition a un nombre impair d'inversions.

Preuve
On considère une transposition $t \overset{\text{def}}{=} \begin{pmatrix} a & b \end{pmatrix}$ de $\mathfrak{S}_n$, avec $a < b$. Pour chercher les couples (i, j) tels que $i < j$ et qui sont des inversions, nous pouvons distinguer quatre cas :

- 1er cas : si i et j sont différents de a et b, alors
$$t(i) = i < j = t(j)$$
donc (i, j) n'est pas une inversion.
- 2e cas : si $i = b$ alors nécessairement $j \notin \{a, b\}$ (car $i < j$), donc
$$t(i) = t(b) = a < b = i < j = t(j)$$
De même si $j = a$ alors nécessairement $i \notin \{a, b\}$ (car $i < j$), donc
$$t(i) = i < j = a < b = t(a) = t(j)$$
Dans ces deux cas, (i, j) n'est pas une inversion.
- 3e cas : si $i = a$, on obtient une inversion si et seulement $b > t(j)$, ce qui équivaut à $j \in [a + 1, b]$. En effet, $j > i = a$ et
  - si $j \in [a + 1, b[$, alors $b > j = t(j)$;
  - si $j = b$, alors $b > a = t(j)$;
  - si $j > b$, alors $b < j = t(j)$.
- 4e cas : de même, si $j = b$, on obtient une inversion si et seulement si $t(i) > a$, ce qui équivaut à $i \in [a, b - 1]$. En effet, $i < j = b$ et
  - si $i \in]a, b - 1]$ alors $t(i) = i > a$;
  - si $i = a$ alors $t(i) = b > a$;
  - si $i < a$ alors $t(i) = i < a$.

On en déduit que l'ensemble des inversions est

$$\{(a, j)\,;\ a + 1 \leqslant j \leqslant b\} \cup \{(i, b)\,;\ a \leqslant i \leqslant b - 1\}$$

L'intersection de ces deux ensembles est le singleton $\{(a, b)\}$, donc le nombre des inversions est

$$(b - a) + (b - a) - 1 = 2(b - a) - 1$$

Théorème 3.7.3
On considère une permutation σ de $\mathfrak{S}_n$ et on note p le nombre de ses inversions.

1. Pour tout anneau commutatif A, et tout $(x_1, \dots, x_n) \in A^n$
$$\prod_{1 \leqslant i < j \leqslant n} (x_{\sigma(i)} - x_{\sigma(j)}) = (-1)^p \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j)$$

Ces pages ne sont pas incluses dans l’aperçu.

Chapitre 4

Compléments de théorie des nombres

Prérequis
Les nombres premiers entre eux (section 3.4 du volume 3), et les anneaux $\mathbb{Z}/n\mathbb{Z}$ (section 4.3 du volume 3).

4.1 Triplets pythagoriciens

Définition 4.1.1 (Triplet pythagoricien)
On appelle *triplet pythagoricien* tout triplet $(a, b, c) \in (\mathbb{N}^*)^3$ tel que

$$a^2 + b^2 = c^2$$

Exemple 4.1.2 (Exemples de triplets pythagoriciens)
Les triplets $(3, 4, 5)$ et $(5, 12, 13)$ sont pythagoriciens, puisque

$$3^2 + 4^2 = 25 = 5^2 \quad \text{et} \quad 5^2 + 12^2 = 169 = 13^2$$

Remarque 4.1.3 (Remarque historique) : L'expression *triplet pythagoricien* est bien évidemment une référence au théorème de Pythagore, qui dit que dans un triangle ABC rectangle en A on a $AB^2 + AC^2 = BC^2$. Les triplets pythagoriciens donnent donc les dimensions possibles de triangles rectangles dont les mesures des longueurs des côtés sont des entiers naturels. Même si ce théorème porte le nom du mathématicien et philosophe grec Pythagore (VI$^{\text{e}}$ siècle avant notre ère), il était connu avant lui, en particulier des mathématiciens babyloniens, qui étaient aussi familiers des triplets pythagoriciens (on peut trouver une liste de tels triplets sur une tablette d'argile babylonienne datant d'environ 1 800 ans avant notre ère).

Théorème 4.1.4 (Propriétés élémentaires d'un triplet pythagoricien)
1. (a, b, c) est un triplet pythagoricien si et seulement si (b, a, c) en est un.
2. Pour tout entier strictement positif k, (a, b, c) est un triplet pythagoricien si et seulement si (ka, kb, kc) en est un.

Preuve

1. Il est immédiat, d'après la définition, que l'on peut permuter les deux premières composantes d'un triplet pythagoricien.
2. Les trois égalités suivantes sont équivalentes :

$$\begin{aligned} (ka)^2 + (kb)^2 &= (kc)^2 \\ k^2(a^2 + b^2) &= k^2c^2 \\ a^2 + b^2 &= c^2 \qquad \text{puisque } k \neq 0 \end{aligned}$$

De plus, comme $k \neq 0$, a, b et c sont non nuls si et seulement si ka, kb et kc sont non nuls, donc (a, b, c) est un triplet pythagoricien si et seulement si (ka, kb, kc) en est un.

Théorème 4.1.5 (Triplet pythagoricien primitif)

1. Pour tout triplet pythagoricien (a, b, c), les trois propriétés suivantes sont équivalentes :
   - Les entiers a, b, c sont premiers entre eux deux à deux.
   - Deux entiers parmi les trois sont premiers entre eux.
   - Les entiers a, b, c sont premiers entre eux dans leur ensemble.

   On dit alors que (a, b, c) est un *triplet pythagoricien primitif*.
2. Si (a, b, c) est un triplet pythagoricien primitif, alors a ou b est pair et les autres composantes du triplet sont impaires.
3. On considère trois entiers non nuls a, b, c et leur PGCD d. Alors (a, b, c) est un triplet pythagoricien si et seulement si $\left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right)$ est un triplet pythagoricien primitif.

Preuve

1. Prouvons l'équivalence des trois propriétés par implications circulaires. Si a, b, c sont premiers entre eux deux à deux, alors a fortiori il existe deux entiers parmi les trois qui sont premiers entre eux. Et si, parmi les trois nombres, deux sont premiers entre eux, alors ils sont premiers dans leur ensemble (un diviseur des trois nombres est a fortiori un diviseur des deux qui sont premiers entre eux, donc est égal à 1). Il reste à justifier la dernière implication : faisons donc l'hypothèse que a, b, c sont premiers entre eux dans leur ensemble, et prouvons qu'ils sont premiers deux à deux. Si d est un diviseur de deux des nombres, il divise aussi le carré du troisième (si d divise a et b alors d divise $a^2 + b^2 = c^2$, si d divise a et c alors d divise $c^2 - a^2 = b^2$, et si d divise b et c alors d divise $c^2 - b^2 = a^2$). On en déduit que si $d \neq 1$, alors d admet un diviseur premier p qui divise le carré du troisième nombre, donc qui divise aussi ce troisième nombre, en contradiction avec $\mathrm{PGCD}(a, b, c) = 1$. Par conséquent $d = 1$, ce qui signifie que les trois nombres sont premiers deux à deux.
2. On considère un triplet pythagoricien primitif (a, b, c).
   - a et b ne peuvent pas être tous les deux pairs puisqu'ils sont premiers entre eux.
   - Prouvons que a et b ne peuvent pas être tous les deux impairs, en faisant l'hypothèse contraire qu'ils le sont. Il existe un entier k tel que $a = 2k + 1$ donc

$$a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$$

   et par conséquent $a^2 \equiv 1 \mod 4$. Il en est de même pour b^2, donc

$$a^2 + b^2 \equiv 2 \mod 4$$

   Mais comme $a^2 + b^2$ (autrement dit c^2) est pair, c est pair donc c^2 est un multiple de 4, et on obtient la contradiction

$$\begin{cases} c^2 = a^2 + b^2 \equiv 2 \mod 4 \\ c^2 \equiv 0 \mod 4 \end{cases}$$

   - On en déduit que a et b ne peuvent pas être tous les deux pairs, ni tous les deux impairs : l'un des deux nombres est pair et l'autre impair. Il en est de même pour leur carré, donc c^2 est impair (somme d'un nombre pair et d'un nombre impair), et par conséquent c est impair.

Ces pages ne sont pas incluses dans l’aperçu.

x	y	x^2-y^2	$2xy$	x^2+y^2	Triplet
2	1	3	4	5	(3,4,5)
3	2	5	12	13	(5,12,13)
4	3	7	24	25	(7,24,25)
4	1	15	8	17	(8,15,17)
5	4	9	40	41	(9,40,41)
5	2	21	20	29	(20,21,29)
6	5	11	60	61	(11,60,61)
6	1	35	12	37	(12,35,37)
7	6	13	84	85	(13,84,85)
7	4	33	56	65	(33,56,65)
7	2	45	28	53	(28,45,53)
8	7	15	112	113	(15,112,113)
8	5	39	80	89	(39,80,89)
8	3	55	48	73	(48,55,73)
8	1	63	16	65	(16,63,65)
9	8	17	144	145	(17,144,145)
9	4	65	72	97	(65,72,97)
9	2	77	36	85	(36,77,85)

4.2 Nombres de Mersenne

Définition 4.2.1 (Nombres de Mersenne)

1. On considère deux entiers a et n supérieurs ou égaux à 2. Si a^n-1 est un nombre premier, alors $a=2$ et n est un nombre premier. En particulier
   - Si $a>2$ alors a^n-1 n'est pas premier.
   - Si 2^n-1 est premier, alors n est premier.
2. On appelle *nombres de Mersenne* les termes de la suite $(M_n)_{n\in\mathbb{P}}$ définie par

$$M_n \overset{\text{def}}{\equiv} 2^n-1$$

Preuve

D'après la formule

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

on a ici

$$a^n-1=(a-1)\sum_{k=0}^{n-1}a^k$$

- Si $a>2$ alors $a-1$ est un diviseur de a^n-1 strictement supérieur à 1, et différent de a^n-1 (car $n>1$), donc a^n-1 n'est pas un nombre premier. Par contraposition, si a^n-1 est premier alors $a=2$.
- De la même façon, si n n'est pas un nombre premier et s'écrit $n=mp$, avec $m>1$ et $p>1$, alors d'après la même formule

$$2^n-1=2^{mp}-1=(2^m)^p-1=(2^m-1)\sum_{k=0}^{p-1}2^{km}$$

On en déduit que 2^m-1 est un diviseur de 2^n-1, strictement supérieur à 1 car $2^m>2$ (puisque $m>1$), et qui est différent de 2^n-1 car $m\neq n$. Donc 2^n-1 n'est pas un nombre premier. Par contraposition, si 2^n-1 est premier alors n est premier.

Par conséquent les seuls nombres premiers de la forme $a^n - 1$ sont les nombres $2^n - 1$, avec n nombre premier.

Remarque 4.2.2 (Origine du vocabulaire) : C'est le mathématicien français Édouard Lucas (1842-1891) qui désigne ainsi en 1883 cette classe de nombres dans le deuxième tome de ses *Récréations mathématiques*, en l'honneur de Marin Mersenne (1588-1648), érudit, théologien, et mathématicien français, qui les avait étudiés dans la *Préface générale* de ses *Cogitata physico mathematica* (1644). La dénomination « nombres de Mersenne » sera ensuite reprise en anglais par le mathématicien britannique W.W. Rouse Ball (1850-1925) dans un article de 1891 [1], puis en 1892 dans son *Mathematical Recreations and Problems of Past and Present Times* (retitré *Mathematical Recreations and Essays* dans les éditions suivantes).

Exemple 4.2.3
Les plus petits nombres de Mersenne sont

$$M_2 \overset{\text{def}}{=} 2^2 - 1 = 3 \qquad M_3 \overset{\text{def}}{=} 2^3 - 1 = 7 \qquad M_5 \overset{\text{def}}{=} 2^5 - 1 = 31 \qquad M_7 \overset{\text{def}}{=} 2^7 - 1 = 127$$

On constate que les nombres précédents sont des nombres premiers. Le suivant par contre ne l'est pas, ce qui montre que tous les nombres de Mersenne ne sont pas premiers :

$$M_{11} \overset{\text{def}}{=} 2^{11} - 1 = 2\,047 = 23 \times 89$$

Dans la suite, les nombres qui ne sont pas premiers sont indiqués par leur décomposition en facteurs premiers (quand aucune décomposition n'est indiquée c'est que le nombre est premier) :

$$\begin{aligned}
M_{13} &\overset{\text{def}}{=} 2^{13} - 1 = 8\,191 \\
M_{17} &\overset{\text{def}}{=} 2^{17} - 1 = 131\,071 \\
M_{19} &\overset{\text{def}}{=} 2^{19} - 1 = 524\,287 \\
M_{23} &\overset{\text{def}}{=} 2^{23} - 1 = 8\,388\,607 = 47 \times 178\,481 \\
M_{29} &\overset{\text{def}}{=} 2^{29} - 1 = 536\,870\,911 = 233 \times 1\,103 \times 2\,089 \\
M_{31} &\overset{\text{def}}{=} 2^{31} - 1 = 2\,147\,483\,647 \\
M_{37} &\overset{\text{def}}{=} 2^{37} - 1 = 137\,438\,953\,471 = 223 \times 616\,318\,177 \\
M_{41} &\overset{\text{def}}{=} 2^{41} - 1 = 2\,199\,023\,255\,551 = 13\,367 \times 164\,511\,353 \\
M_{43} &\overset{\text{def}}{=} 2^{43} - 1 = 8\,796\,093\,022\,207 = 431 \times 9\,719 \times 2\,099\,863 \\
M_{47} &\overset{\text{def}}{=} 2^{47} - 1 = 140\,737\,488\,355\,327 = 2\,351 \times 4\,513 \times 13\,264\,529 \\
M_{53} &\overset{\text{def}}{=} 2^{53} - 1 = 9\,007\,199\,254\,740\,991 = 6\,361 \times 69\,431 \times 20\,394\,401 \\
M_{59} &\overset{\text{def}}{=} 2^{59} - 1 = 576\,460\,752\,303\,423\,487 = 179\,951 \times 3\,203\,431\,780\,337 \\
M_{61} &\overset{\text{def}}{=} 2^{61} - 1 = 2\,305\,843\,009\,213\,693\,951 \\
&\dots
\end{aligned}$$

À la date d'achèvement de ce volume, 52 nombres de Mersenne premiers sont connus, dont le plus grand, qui est aussi le plus grand nombre premier connu, est

$$M_{136\,279\,841} \overset{\text{def}}{=} 2^{136\,279\,841} - 1$$

1. W.W. Rouse Ball. « Mersenne's numbers ». *Messenger of Mathematics* (1891).

C'est un nombre comportant 41 024 320 chiffres (en base décimale). Il a été découvert en octobre 2024 dans le cadre du programme *Great Internet Mersenne Prime Search*, ou GIMPS, un projet de calcul partagé (projet collaboratif utilisant la puissance de plusieurs ordinateurs reliés en réseau) pour chercher les nombres premiers de Mersenne[a].

a. `https://www.mersenne.org/`

4.3 Nombres de Fermat

Définition 4.3.1 (Nombres de Fermat)

1. Pour tout nombre entier $m \geqslant 1$, si $2^m + 1$ est un nombre premier, alors m est une puissance de 2.
2. On appelle *nombres de Fermat* les termes de la suite $(F_n)_{n\in\mathbb{N}}$ définie pour tout entier n par

$$F_n \overset{\text{def}}{\equiv} 2^{2^n} + 1$$

Preuve

On considère un entier $m \geqslant 1$ tel que $2^m + 1$ est un nombre premier. L'entier m étant non nul, il peut s'écrire sous la forme d'un produit d'une puissance de 2 par un nombre impair : il existe un entier p et un entier impair i tels que $m = 2^p \cdot i$. On a donc

$$2^m + 1 = 2^{2^p \cdot i} + 1 = (2^{2^p})^i + 1 = (2^{2^p} + 1) \sum_{k=0}^{i-1} (-1)^k (2^{2^p})^k$$

On en déduit que $2^{2^p} + 1$ divise le nombre premier $2^m + 1$. Comme $2^{2^p} + 1 \neq 1$ on a $2^m + 1 = 2^{2^p} + 1$, donc $2^m = 2^{2^p}$, et par conséquent $m = 2^p$ (par injectivité de la fonction $n \longmapsto 2^n$).

Exemple 4.3.2

$$F_0 \overset{\text{def}}{\equiv} 2^{2^0} + 1 = 3 \qquad F_1 \overset{\text{def}}{\equiv} 2^{2^1} + 1 = 5 \qquad F_2 \overset{\text{def}}{\equiv} 2^{2^2} + 1 = 17$$
$$F_3 \overset{\text{def}}{\equiv} 2^{2^3} + 1 = 257 \qquad F_4 \overset{\text{def}}{\equiv} 2^{2^4} + 1 = 65\,537$$

On constate que les nombres précédents sont premiers. Le mathématicien français Pierre de Fermat (1601/1608-1665) généralise le résultat et conjecture que tout nombre de la forme $2^{2^n} + 1$ est premier. Pourtant, le mathématicien suisse Leonhard Euler (1707-1783) réfute cette conjecture en montrant en 1732 que F_5 est divisible par 641. On peut en effet vérifier que

$$F_5 \overset{\text{def}}{\equiv} 2^{2^5} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417$$

Notons que l'on peut aussi justifier que 641 divise $2^{2^5} + 1$ sans avoir besoin d'effectuer la factorisation complète (c'est ce qu'a fait Euler) ; cela revient à démontrer que 2^{2^5} est congru à -1 modulo 641 : on a

$$2^{2^5} = 2^{32} = 2^4 \times 2^{28}$$

Par ailleurs

$$2^4 \equiv 16 \equiv -625 \equiv -5^4 \mod 641$$

donc

$$2^{2^5} \equiv -5^4 \times 2^{28} \equiv -(5 \times 2^7)^4 \mod 641$$

Or

$$5 \times 2^7 \equiv 640 \equiv -1 \mod 641$$

donc

$$2^{2^5} \equiv -(5 \times 2^7)^4 \equiv -1 \mod 641$$

Aujourd'hui, on conjecture plutôt que si $n \geqslant 5$, $2^{2^n} + 1$ n'est pas un nombre premier. À la date d'achèvement de ce volume, on connaît une factorisation complète des nombres de Fermat de F_5 à F_{11}, on sait que les nombres de Fermat de F_{12} jusqu'à F_{32} ne sont pas premiers[a], et le plus petit nombre de Fermat dont le statut (nombre premier ou composé) est inconnu est F_{33} (mais on connaît d'autres nombres de Fermat plus grands dont on sait qu'ils sont composés)[b].

a. Pour deux d'entre eux, F_{20} et F_{24}, on sait qu'ils sont composés mais on ne dispose d'aucun facteur, et pour les autres on dispose d'une factorisation partielle (c'est-à-dire qu'on connaît certains des facteurs premiers, mais pas tous).

b. Source : Wilfrid KELLER. *Prime factors $k \times 2^n + 1$ of Fermat numbers F_m and complete factoring status*. URL : `http://www.prothsearch.com/fermat.html` (compilation de résultats connus sur la factorisation des nombres de Fermat, effectuée par Wilfrid Keller).

Une propriété classique des nombres de Fermat est qu'ils sont deux à deux premiers entre eux. Ce résultat porte parfois le nom de *théorème de Goldbach* :

Théorème 4.3.3 (Lemme du théorème de Goldbach)
Pour tous les entiers n et k tels que $n < k$, F_n divise $F_k - 2$.

Preuve
Démontrons d'abord par récurrence sur $k \geqslant n+1$ que le reste de la division euclidienne de 2^{2^k} par F_n est 1 :

- Pour $k = n+1$, on a
$$2^{2^{n+1}} = \left(2^{2^n}\right)^2 = (F_n - 1)^2 = F_n^2 - 2F_n + 1 = F_n(F_n - 2) + 1$$
donc le reste de la division euclidienne de $2^{2^{n+1}}$ par F_n est 1.
- Faisons l'hypothèse de récurrence au rang k (avec $k \geqslant n+1$). Il existe donc un entier q tel que
$$2^{2^k} = qF_n + 1$$
On en déduit
$$2^{2^{k+1}} = \left(2^{2^k}\right)^2 = q^2F_n^2 + 2qF_n + 1 = F_n(q^2F_n + 2q) + 1$$
donc le reste de la division euclidienne de $2^{2^{k+1}}$ par F_n est 1.

On en déduit que si $k > n$, il existe un entier q tel que

$$2^{2^k} = qF_n + 1$$
$$F_k = 2^{2^k} + 1 = qF_n + 2$$

et par conséquent F_n divise $F_k - 2$.

Théorème 4.3.4 (Théorème de Goldbach)
Deux nombres de Fermat différents sont premiers entre eux.

Preuve
On considère deux nombres de Fermat distincts F_n et F_k, avec $n < k$. D'après le lemme précédent, F_n divise $F_k - 2$, donc

Ces pages ne sont pas incluses dans l’aperçu.

- Injectivité (unicité d'un antécédent par f d'un élément de $[1, n]$) : pour tout $m \in [1, n]$, si $(d, k) \in E$ et $m = f(d, k) = \frac{n}{d}k$, alors
$$\mathrm{PGCD}(n, m) = \mathrm{PGCD}\Big(\frac{n}{d}d, \frac{n}{d}k\Big) = \frac{n}{d}$$
(car d et k sont premiers entre eux), d'où l'unicité de d et k, qui sont nécessairement tels que
$$d = \frac{n}{\mathrm{PGCD}(n, m)} \qquad \text{et} \qquad k = \frac{m}{\mathrm{PGCD}(n, m)}$$

On en déduit que f est bijective, donc $|E| = n$.

4.6 Somme des diviseurs, nombres parfaits

Un autre exemple de fonction multiplicative est donné par la somme des diviseurs :

Théorème 4.6.1 (Somme des diviseurs)
Pour tout entier naturel non nul n, on note $\sigma(n)$ la somme de ses diviseurs :
$$\sigma(n) \overset{\text{def}}{\equiv} \sum_{d|n} d$$

1. Si p est un nombre premier et n un entier
$$\sigma(p^n) = \sum_{k=0}^{n} p^k = \frac{p^{n+1} - 1}{p - 1}$$
en particulier
$$\sigma(1) = 1 \qquad \text{et} \qquad \sigma(p) = p + 1$$
2. σ est une fonction multiplicative.

Preuve
1. Le seul diviseur de 1 est 1 donc
$$\sigma(p^0) = \sigma(1) = 1 = \sum_{k=0}^{0} p^k$$
et si $n > 0$ les diviseurs de p^n sont tous les p^k avec $k \leqslant n$, donc
$$\sigma(p^n) = \sum_{k=0}^{n} p^k = \frac{p^{n+1} - 1}{p - 1}$$
2. On considère deux entiers non nuls premiers entre eux n et p, et l'ensemble D_n (respectivement D_p, D_{np}) des diviseurs de n (respectivement p, np). Prouvons que les fonctions
$$f : \begin{cases} D_n \times D_p \longrightarrow D_{np} \\ (x, y) \longmapsto xy \end{cases} \qquad g : \begin{cases} D_{np} \longrightarrow D_n \times D_p \\ x \longmapsto (\mathrm{PGCD}(x, n), \mathrm{PGCD}(x, p)) \end{cases}$$
sont bijectives et réciproques l'une de l'autre. La fonction f est bien définie puisque si x divise n et y divise p alors xy divise np, et la fonction g est bien définie par définition du PGCD.
   - Si $(x, y) \in D_n \times D_p$ alors, comme n et p sont premiers entre eux, on en déduit que y et n sont premiers entre eux, ainsi que x et p, donc
   $$\mathrm{PGCD}(xy, n) = \mathrm{PGCD}(x, n) = x \qquad \text{et} \qquad \mathrm{PGCD}(xy, p) = \mathrm{PGCD}(y, p) = y$$
   Par conséquent
   $$(g \circ f)(x, y) = (\mathrm{PGCD}(xy, n), \mathrm{PGCD}(xy, p)) = (x, y)$$

- On considère un diviseur x de np. Puisque n et p sont premiers entre eux, PGCD(x,n) et PGCD(x,p) aussi donc

$$(\text{PGCD}(x,n))(\text{PGCD}(x,p)) = \text{PPCM}(\text{PGCD}(x,n),\text{PGCD}(x,p)) = \text{PGCD}(x,\text{PPCM}(n,p)) = \text{PGCD}(x,np) = x$$

Par conséquent $(f\circ g)(x) = (\text{PGCD}(x,n))(\text{PGCD}(x,p)) = x$.

On a par définition

$$\sigma(np) = \sum_{d\in D_{np}} d$$

On utilise alors la bijection entre D_{np} et $D_n \times D_p$ pour effectuer le changement d'indice $D_n \times D_p \xrightarrow{f} D_{np}$:

$$\sigma(np) = \sum_{d\in D_{np}} d = \sum_{(x,y)\in D_n\times D_p} xy = \left(\sum_{x\in D_n} x\right)\left(\sum_{y\in D_p} y\right) = \sigma(n)\sigma(p)$$

On en déduit que pour tous les entiers $a_1,\dots,a_m$ premiers entre eux deux à deux,

$$\sigma(a_1\cdots a_m) = \sigma(a_1)\cdots\sigma(a_m)$$

et l'expression de $\sigma(n)$ ($n>1$) à partir de la décomposition de n en facteurs premiers :

Théorème 4.6.2 (Corollaire)
Pour tout entier $n>1$ dont la décomposition en facteurs premiers est $n=\prod_{k=1}^{m} p_k^{\alpha_k}$, on a

$$\sigma(n) = \prod_{k=1}^{m} \frac{p_k^{\alpha_k+1}-1}{p_k-1}$$

L'étude de la somme des diviseurs nous amène au concept de *nombre parfait* :

Définition 4.6.3 (Nombre parfait)
On appelle *nombre parfait* tout entier naturel non nul n dont la somme des diviseurs est égale à $2n$, autrement dit tout entier naturel non nul égal à la somme de ses diviseurs stricts (c'est-à-dire les diviseurs différents de n).

Preuve (de l'équivalence)
Puisque n fait partie des diviseurs de n, la somme des diviseurs stricts de n est $\sigma(n)-n$ et on a bien

$$\sigma(n)-n = n \iff \sigma(n) = 2n$$

Exemple 4.6.4
Les plus petits nombres parfaits sont

$$\begin{aligned} 6 &= 1+2+3\\ 28 &= 1+2+4+7+14\\ 496 &= 1+2+4+8+16+31+62+124+248 \end{aligned}$$

Ces pages ne sont pas incluses dans l’aperçu.

Chapitre 5

Extension de la notion de nombre

Prérequis
Les compléments sur les anneaux du chapitre 1.

5.1 Corps des fractions d'un anneau intègre

Prérequis
Les lois quotients (section 2.13 du volume 2).

Une limitation des anneaux est l'impossibilité d'obtenir un symétrique de certains éléments (si l'anneau n'est pas un anneau à division). On peut se demander s'il est possible, d'une certaine manière, « d'agrandir » un anneau pour pallier ce problème. Dans le cas d'un anneau intègre, on peut le faire facilement : nous allons voir comment il est possible de construire, à partir d'un tel anneau A, un corps qui prolonge les lois $+$ et $\times$ de A, qu'on appelle le corps des fractions de A. C'est ce principe qui sera utilisé pour construire le corps $\mathbb{Q}$ des rationnels à partir de l'anneau $\mathbb{Z}$ des entiers relatifs, ou encore pour construire le corps des fractions rationnelles $A(X)$ à partir de l'anneau des polynômes $A[X]$. Le principe est de définir sur $A \times A^*$ une relation d'équivalence correspondant au produit en croix classique

$$\frac{x}{y} = \frac{x'}{y'} \iff xy' = yx'$$

Théorème 5.1.1 (Corps des fractions d'un anneau intègre)

1. On considère un anneau intègre A, et sur $A \times A^*$ la relation d'équivalence
$$(x, y) \sim (x', y') \overset{\text{def}}{\equiv} xy' = yx'$$
On note $\mathrm{Frac}(A)$ l'ensemble quotient $A \times A^*/\sim$, et $\dfrac{x}{y}$ la classe de (x, y).
2. On définit sur $\mathrm{Frac}(A)$ l'addition et la multiplication suivantes :
$$\frac{x}{y} + \frac{z}{t} \overset{\text{def}}{\equiv} \frac{xt + yz}{yt} \qquad \frac{x}{y} \times \frac{z}{t} \overset{\text{def}}{\equiv} \frac{xz}{yt}$$
3. $\left(\mathrm{Frac}(A), +, \times, \dfrac{0}{1}, \dfrac{1}{1}\right)$ est un corps, que l'on l'appelle le *corps des fractions* de A. De plus pour tout $(x, y) \in A \times A^*$

- Pour tout k non nul dans A

$$\frac{kx}{ky} = \frac{x}{y} \qquad \text{(en particulier } \frac{-x}{-y} = \frac{x}{y}\text{)}$$

- L'opposé de $\frac{x}{y}$ est $\frac{-x}{y}$.
- Si $\frac{x}{y}$ est non nul, son inverse est $\frac{y}{x}$.

4. La fonction

$$i : \begin{cases} A \longrightarrow \mathrm{Frac}(A) \\ x \longmapsto \frac{x}{1} \end{cases}$$

est un morphisme d'anneaux injectif, qu'on appelle l'*injection canonique* de A dans $\mathrm{Frac}(A)$.

Preuve

- La relation

$$(x, y) \sim (x', y') \overset{\text{def}}{\equiv} xy' = yx'$$

est bien une relation d'équivalence sur $A \times A^*$, car elle est réflexive ($xy = yx$, car l'anneau A est intègre, donc commutatif par définition), symétrique (si $xy' = yx'$, alors $x'y = yx' = xy' = y'x$, toujours par commutativité), et transitive : si $xy' = yx'$ et $x'y'' = y'x''$, alors

— soit $x' = 0$, et alors $xy' = y'x'' = 0$ donc $x = x'' = 0$ (car A est intègre et $y' \neq 0$ par définition de A^*), et par conséquent $xy'' = 0 = yx''$.

— soit $x' \neq 0$, et alors comme $(xy')(x'y'') = (yx')(y'x'')$, on en déduit, en simplifiant par les termes non nuls x' et y' (A étant un anneau intègre), $xy'' = yx''$.

- On peut munir l'ensemble quotient $\mathrm{Frac}(A)$ de l'addition et la multiplication indiquées, car les deux opérations

$$\oplus : ((x, y), (z, t)) \longmapsto (xt + yz, yt) \qquad \text{et} \qquad \otimes : ((x, y), (z, t)) \longmapsto (xz, yt)$$

sont compatibles avec la relation d'équivalence : en effet, si $(x, y) \sim (x', y')$ et $(z, t) \sim (z', t')$, autrement dit si $xy' = yx'$ et $zt' = tz'$, alors

$$(xt + yz, yt) \sim (x't' + y'z', y't')$$

car

$$(xt + yz)y't' = xty't' + yzy't' = (xy')(tt') + (zt')(yy') = (yx')(tt') + (tz')(yy') = (yt)(x't') + (yt)(y'z') = (yt)(x't' + y'z')$$

et

$$(xz, yt) \sim (x'z', y't')$$

car

$$(xz)(y't') = (xy')(zt') = (yx')(tz') = (yt)(x'z')$$

- L'opération $\times$ est commutative (respectivement associative) car $\otimes$ l'est : en effet, $\otimes$ est la loi produit classique sur $A \times A^*$ (induite par la multiplication de A), et par conséquent nous savons déjà que cette opération est commutative et associative, mais on peut aussi le redémontrer : elle est commutative car

$$(x, y) \otimes (z, t) = (xz, yt) = (zx, ty) = (z, t) \otimes (x, y)$$

et associative car

$$(x, y) \otimes ((z, t) \otimes (u, v)) = (x, y) \otimes (zu, tv) = (x(zu), y(tv)) = ((xz)u, (yt)v) = ((x, y) \otimes (z, t)) \otimes (u, v)$$

De plus, $(1, 1)$ est élément neutre pour $\otimes$, donc $\frac{1}{1}$ est élément neutre pour $\times$.

- L'opération $+$ est commutative, car $\oplus$ l'est :

$$(x, y) \oplus (z, t) = (xt + yz, yt) = (zy + tx, ty) = (z, t) \oplus (x, y)$$

L'opération $+$ est associative, car $\oplus$ l'est :

$$(x, y) \oplus ((z, t) \oplus (u, v)) = (x, y) \oplus (zv + tu, tv) = (xtv + yzv + ytu, ytv) = ((xt + yz)v + ytu, ytv)$$

Ces pages ne sont pas incluses dans l’aperçu.

- On note que 0 est un élément de $\mathrm{Frac}(A)_+$ (donc aussi de $-\mathrm{Frac}(A)_+$). Réciproquement, si $\frac{p}{q} \in \mathrm{Frac}(A)_+ \cap -\mathrm{Frac}(A)_+$, alors d'une part $pq \geqslant 0$, et d'autre part $-\frac{p}{q} \in \mathrm{Frac}(A)_+$ donc $-pq \geqslant 0$ et par conséquent $pq \leqslant 0$. On en déduit $pq = 0$, donc $p = 0$ et $\frac{p}{q} = 0$.

Par conséquent la relation

$$x \leqslant y \overset{\text{def}}{\Longleftrightarrow} y - x \in \mathrm{Frac}(A)_+$$

est une relation d'ordre sur $\mathrm{Frac}(A)$ compatible avec l'addition, telle que

$$\mathrm{Frac}(A)_+ = \{x \in \mathrm{Frac}(A)\ ;\ x \geqslant 0\}$$

Par ailleurs, l'ordre est total puisque

$$\mathrm{Frac}(A) = \mathrm{Frac}(A)_+ \cup -\mathrm{Frac}(A)_+$$

En effet, si $\frac{p}{q} \in \mathrm{Frac}(A)$, alors $pq \geqslant 0$ (donc $\frac{p}{q} \in \mathrm{Frac}(A)_+$) ou $pq \leqslant 0$ (donc $-\frac{p}{q} \in \mathrm{Frac}(A)_+$). Pour démontrer que $\mathrm{Frac}(A)$ muni de $\leqslant$ est un corps ordonné, il reste à justifier la compatibilité avec la multiplication par les éléments positifs : si $\frac{a}{b}$ et $\frac{c}{d}$ sont des éléments de $\mathrm{Frac}(A)_+$, alors $\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$ aussi car $acbd = (ab)(cd) \geqslant 0$.

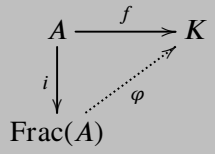
5. Vérifions enfin que la relation d'ordre précédente est la seule possible qui prolonge celle de A et qui fasse de $\mathrm{Frac}(A)$ un corps totalement ordonné. On suppose donc que $\mathrm{Frac}(A)$, muni d'une relation d'ordre $\leqslant$, est un corps totalement ordonné, et que la relation $\leqslant$ prolonge l'ordre $\leqslant_A$. Pour tout $(p, q) \in A \times A_+^*$, $\frac{p}{q} \cdot q = p$. Donc, d'après la règle des signes, $\frac{p}{q} \geqslant 0$ si et seulement si $p \geqslant 0$. On en déduit que l'ensemble des éléments positifs est

$$\left\{ x \in \mathrm{Frac}(A)\ ;\ \exists (p, q) \in A_+ \times A_+^*, x = \frac{p}{q} \right\}$$

Théorème 5.1.5 (Propriété universelle du corps des fractions)
Soit A un anneau intègre, $\mathrm{Frac}(A)$ son corps des fractions et $A \xrightarrow{i} \mathrm{Frac}(A)$ l'injection canonique. Pour tout corps K et tout morphisme d'anneaux injectif $A \xrightarrow{f} K$, il existe un unique morphisme de corps $\mathrm{Frac}(A) \xrightarrow{\varphi} K$ tel que

$$f = \varphi \circ i$$

ce qui peut se représenter par le diagramme commutatif suivant (où les flèches représentent des morphismes d'anneaux) :



Preuve

- Commençons par l'unicité : un morphisme φ répondant à la question est nécessairement tel que pour tout $(x, y) \in A \times A^*$

$$\varphi\left(\frac{x}{y}\right) = \varphi\left(\frac{x}{1} \cdot \frac{1}{y}\right) = \varphi\left(\frac{x}{1}\right)\varphi\left(\frac{1}{y}\right) = \varphi\left(\frac{x}{1}\right)\left(\varphi\left(\frac{y}{1}\right)\right)^{-1} = \varphi(i(x))(\varphi(i(y)))^{-1} = f(x)(f(y))^{-1}$$

- L'existence de φ est donnée par le théorème de factorisation pour les fonctions : on considère la fonction

$$g : \begin{cases} A \times A^* \longrightarrow K \\ (x, y) \longmapsto f(x)(f(y))^{-1} \end{cases}$$

Elle est bien définie car f est injective : si $y \neq 0$ alors $f(y) \neq 0$ donc $f(y)$ est un élément inversible de K. Vérifions que la fonction g est constante sur les classes d'équivalence : si $xy' = x'y$, alors

$$f(x)f(y') = f(xy') = f(x'y) = f(x')f(y)$$

donc

$$f(x)f(y)^{-1} = f(x')f(y')^{-1}$$

On en déduit qu'il existe une fonction $\mathrm{Frac}(A) \xrightarrow{\varphi} K$ telle que pour tout $(x, y) \in A \times A^*$

$$\varphi\left(\frac{x}{y}\right) = g(x, y) = f(x)(f(y))^{-1}$$

donc $f = \varphi \circ i$, car pour tout $x \in A$

$$\varphi(i(x)) = \varphi\left(\frac{x}{1}\right) = f(x)f(1)^{-1} = f(x)$$

- Vérifions enfin que φ est un morphisme d'anneaux : $\varphi\left(\frac{1}{1}\right) = f(1) = 1$, et pour tout (x, y) et (x', y') dans $A \times A^*$

$$\begin{aligned}\varphi\left(\frac{x}{y} + \frac{x'}{y'}\right) &= \varphi\left(\frac{xy' + x'y}{yy'}\right)\\ &= f(xy' + x'y)(f(yy'))^{-1} = f(x)f(y')f(y)^{-1}f(y')^{-1} + f(x')f(y)f(y)^{-1}f(y')^{-1} = f(x)f(y)^{-1} + f(x')f(y')^{-1}\\ &= \varphi\left(\frac{x}{y}\right) + \varphi\left(\frac{x'}{y'}\right)\end{aligned}$$

et

$$\varphi\left(\frac{x}{y} \times \frac{x'}{y'}\right) = \varphi\left(\frac{xx'}{yy'}\right) = f(xx')f(yy')^{-1} = f(x)f(y)^{-1}f(x')f(y')^{-1} = \varphi\left(\frac{x}{y}\right) \cdot \varphi\left(\frac{x'}{y'}\right)$$

Remarque 5.1.6 : Il s'agit d'une *propriété universelle* au sens de la théorie des catégories (voir le volume 3). Je rappelle que ce genre de propriétés permet d'obtenir des caractérisations, à un isomorphisme près, de certains objets mathématiques. D'une certaine manière, elles capturent « l'essence mathématique » des objets en question, indépendamment de la façon dont ces objets ont pu être construits.

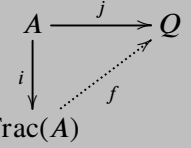
Remarque 5.1.7 : Cette propriété universelle signifie que le corps des fractions de A est le « plus petit » corps « contenant » A, dans le sens suivant : si K est un corps contenant un sous-anneau isomorphe à A (l'image de la fonction f du théorème précédent), alors K contient un sous-corps isomorphe à $\mathrm{Frac}(A)$ (l'image de la fonction φ du théorème précédent).

Il y a unicité du corps des fractions, dans la mesure où il n'existe qu'un corps (à un isomorphisme près) qui vérifie la propriété universelle précédente :

Théorème 5.1.8 (Unicité du corps des fractions)
On considère un anneau intègre A, un corps Q et un morphisme d'anneaux injectif $A \xrightarrow{j} Q$ vérifiant la propriété universelle du corps des fractions de A, autrement dit tel que pour tout corps K et tout morphisme d'anneaux injectif $A \xrightarrow{\varphi} K$, il existe un unique morphisme de corps $Q \xrightarrow{\overline{\varphi}} K$ tel que $\varphi = \overline{\varphi} \circ j$. Alors il existe un unique isomorphisme de corps $\mathrm{Frac}(A) \xrightarrow{f} Q$ tel que

$$j = f \circ i$$

ce qui peut se représenter par le diagramme commutatif suivant (où les flèches représentent des morphismes d'anneaux) :



Preuve
C'est le principe habituel des propriétés universelles. Puisque $A \xrightarrow{i} \mathrm{Frac}(A)$ vérifie la propriété universelle et que $A \xrightarrow{j} Q$ est un morphisme d'anneaux injectif, il existe un morphisme de corps $\mathrm{Frac}(A) \xrightarrow{f} Q$ tel que $j = f \circ i$. De même, puisque $A \xrightarrow{j} Q$ vérifie la propriété universelle et que $A \xrightarrow{i} \mathrm{Frac}(A)$ est un morphisme d'anneaux injectif, il existe un morphisme de corps $Q \xrightarrow{g} \mathrm{Frac}(A)$ tel que $i = g \circ j$. On en déduit $g \circ f \circ i = g \circ j = i$, donc $g \circ f$ est un morphisme de corps de $\mathrm{Frac}(A)$ dans $\mathrm{Frac}(A)$ tel que $(g \circ f) \circ i = i$. Puisque l'identité est aussi un tel morphisme, on déduit encore de la propriété universelle, par unicité, que $g \circ f = \mathrm{id}_{\mathrm{Frac}(A)}$. De même $f \circ g = \mathrm{id}_Q$, et par conséquent f et g sont deux bijections réciproques, donc deux isomorphismes.

Théorème 5.1.9 (Corollaire)
Tout corps est isomorphe à son corps des fractions.

Preuve
Tout corps K, muni de son identité, vérifie la propriété universelle du corps des fractions. En effet, pour tout corps K' et tout morphisme d'anneaux (nécessairement injectif) $K \xrightarrow{f} K'$, il existe un unique morphisme de corps $K \xrightarrow{\varphi} K'$ tel que $f = \varphi \circ \mathrm{id} = \varphi$. On en déduit que K est isomorphe à son corps des fractions.

Remarque 5.1.10 : Ainsi, il n'y a pas d'intérêt à étudier le corps des fractions d'un corps, puisqu'on retrouve le même corps (à un isomorphisme près). Par exemple si n est un nombre premier, le corps des fractions de $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

5.2 Corps $\mathbb{Q}$ des nombres rationnels

Définition 5.2.1 (Corps des nombres rationnels)
On note $\mathbb{Q}$ le corps des fractions de l'anneau intègre $\mathbb{Z}$, autrement dit $\mathbb{Q}$ est l'ensemble quotient sur $\mathbb{Z} \times \mathbb{Z}^*$ de la relation d'équivalence

$$(x, y) \sim (x', y') \overset{\text{def}}{\Leftrightarrow} xy' = yx'$$

muni de l'addition et la multiplication suivantes :

$$\frac{x}{y} + \frac{z}{t} \overset{\text{def}}{=} \frac{xt + yz}{yt} \qquad \frac{x}{y} \times \frac{z}{t} \overset{\text{def}}{=} \frac{xz}{yt}$$

où $\dfrac{x}{y}$ représente la classe d'équivalence de (x, y). De plus, on identifie $\mathbb{Z}$ et son image par l'injection canonique, et l'addition et la multiplication sur $\mathbb{Q}$ prolongent les opérations équivalentes sur $\mathbb{Z}$.

Remarque 5.2.2 (Origine des notations) : Le groupe Bourbaki [1] serait à l'origine de la notation Q, initiale de *Quotient*. On la trouve dans le premier chapitre d'*Algèbre* des *Éléments de mathématique*, paru en 1942. On lit parfois que c'est Peano [2] qui aurait désigné ainsi cet ensemble, comme initiale de *quoziente* (quotient) : c'est faux ! Dans *Arithmetices principia, nova methodo exposita* [Les principes de l'arithmétique, nouvelle méthode d'exposition] (1889) [3], Peano utilise la lettre $\boldsymbol{R}$ pour désigner les nombres rationnels positifs, et la

1. Nicolas Bourbaki est le pseudonyme collectif d'un groupe de mathématiciens francophones, formé en 1935.
2. Giuseppe Peano (1858-1932), mathématicien italien.
3. Et aussi, par exemple, dans son *Formulario di Matematica* [Formulaire de mathématiques] (1894).

lettre *Q* pour désigner les nombres réels positifs, qu'il appelle aussi des quantités (*quantitas*). Cette erreur est apparue un temps sur les pages Wikipédia (anglophone et francophone) des nombres rationnels, mais a été corrigée[4].

Théorème 5.2.3
$\mathbb{Q}$ est en bijection avec $\mathbb{N}$.

Preuve
La fonction

$$\begin{cases} \mathbb{Z} \times \mathbb{Z}^* \longrightarrow \mathbb{Q} \\ (a, b) \longmapsto \dfrac{a}{b} \end{cases}$$

est surjective, et $\mathbb{Z} \times \mathbb{Z}^*$ est en bijection avec $\mathbb{N}$, donc $\mathbb{Q}$ est dénombrable. De plus, $\mathbb{Q}$ est infini, car la fonction

$$\begin{cases} \mathbb{N} \longrightarrow \mathbb{Q} \\ x \longmapsto x \end{cases}$$

est une injection. Donc $\mathbb{Q}$ est en bijection avec $\mathbb{N}$.

Théorème 5.2.4 (Forme irréductible)
1. Pour tout $x \in \mathbb{Q}$, il existe un couple $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $x = \dfrac{p}{q}$.
2. Pour tout $x \in \mathbb{Q}^*$, il existe un unique couple $(a, b) \in \mathbb{Z}^* \times \mathbb{N}^*$ tel que

$$\begin{cases} x = \dfrac{a}{b} \\ \mathrm{PGCD}(a, b) = 1 \end{cases}$$

On dit que $\dfrac{a}{b}$ est la *forme irréductible* de x. De plus les autres représentants de x sont les éléments de la forme $\dfrac{ka}{kb}$, avec k entier relatif non nul.

Preuve
- Nous avons déjà vu le premier point, qui est vrai pour tout corps des fractions d'un anneau intègre totalement ordonné. On en déduit que tout $x \in \mathbb{Q}^*$ peut s'écrire sous la forme $x = \dfrac{p}{q}$, avec $p \in \mathbb{Z}^*$ et $q \in \mathbb{N}^*$. On note d le PGCD de p et q. Il existe $a \in \mathbb{Z}^*$ et $b \in \mathbb{N}^*$ tels que $p = da$ et $q = db$, avec a et b premiers entre eux. Et

$$x = \frac{p}{q} = \frac{da}{db} = \frac{a}{b}$$

- Si $\dfrac{a'}{b'}$ est un autre représentant de x, on a $\dfrac{a'}{b'} = \dfrac{a}{b}$, donc $a'b = ab'$. On en déduit que a divise $a'b$. Or a et b sont premiers entre eux, donc d'après le lemme de Gauss, a divise a'. Il existe donc $k \in \mathbb{Z}$ tel que $a' = ka$, et par conséquent

$$ab' = a'b = kab$$

  donc $b' = kb$, et on en déduit

$$x = \frac{a'}{b'} = \frac{ka}{kb}$$

- Vérifions enfin l'unicité de la forme irréductible : si ka et kb sont premiers entre eux et $kb \in \mathbb{N}^*$ (donc $k \in \mathbb{N}^*$), alors

$$1 = \mathrm{PGCD}(ka, kb) = k\,\mathrm{PGCD}(a, b) = k$$

4. Assez récemment pour la page Wikipédia francophone, qui est encore un peu confuse, au moment où j'écris ces lignes, en donnant les deux origines et en indiquant une source (visiblement peu fiable…) pour l'attribution incorrecte à Peano.

Ces pages ne sont pas incluses dans l’aperçu.

$x_0 < x_1$, et pour tout $n \geqslant 1$,

$$x_{n+1} \in I \setminus \{x_0, \dots, x_n\} \subseteq I \setminus \{x_0, \dots, x_{n-1}\}$$

donc

$$x_n = \min(I \setminus \{x_0, \dots, x_{n-1}) \leqslant x_{n+1}$$

et $x_{n+1} \neq x_n$ donc $x_n < x_{n+1}$.

Théorème 5.5.11
Toute suite à valeurs dans un ensemble totalement ordonné admet une suite extraite monotone.

Preuve
On considère une suite $(x_n)_{n\in\mathbb{N}}$, et l'ensemble

$$A \overset{\text{def}}{\equiv} \left\{n \in \mathbb{N}\,;\ \forall k > n, x_k < x_n\right\}$$

Démontrons que selon que A est un ensemble fini ou infini, on peut extraire de $(x_n)_{n\in\mathbb{N}}$ une suite croissante ou décroissante :

- On fait l'hypothèse que A est infini. D'après le théorème précédent, il existe une suite strictement croissante d'éléments de A, autrement dit une fonction strictement croissante φ de $\mathbb{N}$ dans A, et la suite extraite $(x_{\varphi_n})_{n\in\mathbb{N}}$ est strictement décroissante, car pour tout $n \in \mathbb{N}$, $\varphi_n \in A$ donc $x_{\varphi_{n+1}} < x_{\varphi_n}$.
- On fait l'hypothèse que A est fini. Il existe alors un entier p qui majore strictement A, et on peut définir une suite strictement croissante $(\varphi_n)_{n\in\mathbb{N}}$ d'entiers qui n'appartiennent pas à A (d'où l'on déduira une suite extraite $(x_{\varphi_n})_{n\in\mathbb{N}}$ de $(x_n)_{n\in\mathbb{N}}$ croissante), de la façon suivante :
  - On choisit $\varphi_0 \overset{\text{def}}{\equiv} p$.
  - Puisque $\varphi_0 \notin A$, il existe $k > \varphi_0$ tel que $x_k \geqslant x_{\varphi_0}$. On peut alors choisir un tel k pour φ_1, et ainsi de suite.

  Pour éviter de *choisir* k (en faisant appel à l'axiome du choix), on peut aussi prendre le plus petit des entiers k possibles. On définit ainsi par récurrence la suite

$$\begin{cases} \varphi_0 \overset{\text{def}}{\equiv} p \\ \varphi_{n+1} \overset{\text{def}}{\equiv} \min\left\{k > \varphi_n\,;\ x_k \geqslant x_{\varphi_n}\right\} \end{cases}$$

  Par construction, la suite $(\varphi_n)_{n\in\mathbb{N}}$ est une suite strictement croissante d'entiers qui n'appartiennent pas à A, telle que la suite $(x_{\varphi_n})_{n\in\mathbb{N}}$ est croissante (pour tout entier n, $x_{\varphi_n} \leqslant x_{\varphi_{n+1}}$).

5.6 Suites convergentes dans un corps archimédien

Prérequis
Les sections sur les anneaux et corps des volumes 1 et 2.

Dans cette section, on se place dans un corps $\mathbb{K}$ archimédien (donc en particulier totalement ordonné). Nous savons par exemple que pour tout $a \in \mathbb{K}$ tel que $a > 0$ et tout $n \in \mathbb{N}^*$, $na > 0$ (en particulier na est non nul, donc inversible), et que l'ordre est dense : pour tout a et b dans $\mathbb{K}$ tels que $a < b$, il existe $c \in \mathbb{K}$ tel que $a < c < b$.

Définition 5.6.1 (Suite convergente, suite divergente)
On considère une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}$, et un élément a de $\mathbb{K}$.

1. On dit que la suite *converge* vers a, ou que la suite a pour *limite* a, lorsque

$$\forall \epsilon \in]0, +\infty[_{\mathbb{K}}, \exists p \in \mathbb{N}, \forall n \in [p, +\infty[_{\mathbb{N}}, \left|x_n - a\right| \leqslant \epsilon$$

ce que l'on peut aussi écrire plus simplement

$$\forall \epsilon > 0, \exists p \in \mathbb{N}, \forall n \geqslant p, \left|x_n - a\right| \leqslant \epsilon$$

Lorsqu'une suite est *convergente*, sa limite a est unique. On la note

$$\lim_{n \longrightarrow +\infty} x_n \qquad \text{ou} \qquad \lim_n x_n \qquad \text{ou juste} \qquad \lim x_n$$

2. On dit que la suite est *divergente* lorsqu'elle n'est pas convergente.

Preuve
Vérifions que si une suite est convergente, alors sa limite est unique. On fait l'hypothèse que la suite $(x_n)_{n\in\mathbb{N}}$ converge vers a et b. On en déduit que pour tout $\epsilon > 0$, il existe des entiers p et q tels que

$$\begin{cases} n \geqslant p \implies \left|x_n - a\right| \leqslant \epsilon \\ n \geqslant q \implies \left|x_n - b\right| \leqslant \epsilon \end{cases}$$

Donc pour tout $n \geqslant \max(p, q)$

$$|a - b| = \left|a - x_n + x_n - b\right| \leqslant \left|a - x_n\right| + \left|x_n - b\right| \leqslant \epsilon + \epsilon = 2\epsilon$$

On en déduit $a - b = 0$ (donc $a = b$), car si $a - b \neq 0$, alors il existe $\epsilon > 0$ tel que $\epsilon < \dfrac{|a-b|}{2}$, en contradiction avec l'inégalité ci-dessus.

Remarque 5.6.2 : Dans le cas d'une suite définie à partir d'un certain rang, de la forme $(x_n)_{n\geqslant n_0}$, la définition précédente s'adapte en ne considérant que les valeurs de n pour lesquelles elle est définie : la suite converge vers a lorsque

$$\forall \epsilon > 0, \exists p \geqslant n_0, \forall n \geqslant p, \left|x_n - a\right| \leqslant \epsilon$$

Remarque 5.6.3 : Toute suite $(x_n)_{n\in\mathbb{N}}$ constante, égale à a, est trivialement une suite convergente (vers a) puisque dans ce cas, pour tout $\epsilon > 0$ et tout entier n

$$\left|x_n - a\right| = 0 < \epsilon$$

Remarque 5.6.4 : Pour toute suite $(x_n)_{n\in\mathbb{N}}$

$$\lim_n x_n = 0 \quad \equiv \quad \lim_n (-x_n) = 0 \quad \equiv \quad \lim_n \left|x_n\right| = 0$$

car la définition de la convergence de $(x_n)_{n\in\mathbb{N}}$ vers 0 est

$$\forall \epsilon > 0, \exists p \in \mathbb{N}, \forall n \geqslant p, \left|x_n\right| \leqslant \epsilon$$

et pour tout $n \in \mathbb{N}$

$$\left|\left|x_n\right|\right| = \left|-x_n\right| = \left|x_n\right|$$

Remarque 5.6.5 : Toujours par définition de la convergence, $(x_n)_{n\in\mathbb{N}}$ converge vers a si et seulement si la suite $(x_n - a)_{n\in\mathbb{N}}$ converge vers 0.

Remarque 5.6.6 : Si deux suites $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ sont égales à partir d'un certain rang, alors

- $(x_n)_{n\in\mathbb{N}}$ converge vers a si et seulement si $(y_n)_{n\in\mathbb{N}}$ converge vers a.
- La suite $(x_n - y_n)$ converge vers 0.

En effet :

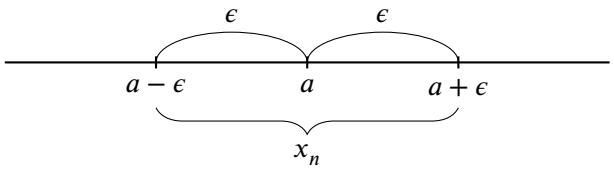
- Si $(x_n)_{n\in\mathbb{N}}$ converge vers a, alors pour tout $\epsilon > 0$, il existe $p \in \mathbb{N}$ tel que si $n \geqslant p$ alors $\left|x_n - a\right| \leqslant \epsilon$. Comme par ailleurs il existe $q \in \mathbb{N}$ tel que si $n \geqslant q$ alors $x_n = y_n$, on en déduit que si $n \geqslant \max(p, q)$
$$\left|y_n - a\right| = \left|x_n - a\right| \leqslant \epsilon$$
ce qui prouve que $(y_n)_{n\in\mathbb{N}}$ converge vers a.
- En appliquant ce qui précède à la suite $(x_n - y_n)_{n\in\mathbb{N}}$ (égale à 0 à partir d'un certain rang) et la suite constante égale à 0 (qui converge donc vers 0), on en déduit que $(x_n - y_n)_{n\in\mathbb{N}}$ converge aussi vers 0.

Remarque 5.6.7 : Je rappelle que pour tout x et y on a les équivalences suivantes

$$|x - y| \leqslant \epsilon \qquad \equiv \qquad y - \epsilon \leqslant x \leqslant y + \epsilon \qquad \equiv \qquad x - \epsilon \leqslant y \leqslant x + \epsilon$$

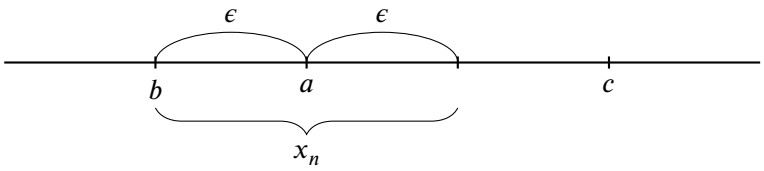
($|x - y|$ représente la « distance » entre x et y). Ainsi, la définition de la convergence vers a équivaut à

$$\forall \epsilon > 0, \exists p \in \mathbb{N}, \forall n \geqslant p, a - \epsilon \leqslant x_n \leqslant a + \epsilon$$



On en déduit que si $(x_n)_{n\in\mathbb{N}}$ converge vers a et si b et c sont des éléments de $\mathbb{K}$ tels que $b < a < c$, alors il existe $p \in \mathbb{N}$ tel que pour tout $n \geqslant p$, $x_n \in [b, c]$. En effet, en prenant $\epsilon \overset{\text{def}}{\equiv} \min(a - b, c - a) > 0$, on en déduit l'existence de $p \in \mathbb{N}$ tel que pour tout $n \geqslant p$

$$b \leqslant a - \epsilon \leqslant x_n \leqslant a + \epsilon \leqslant c$$



On peut aussi avoir des inégalités strictes en prenant ϵ' tel que $0 < \epsilon' < \epsilon$, par exemple $\epsilon' \overset{\text{def}}{\equiv} \dfrac{\epsilon}{2}$: il existe $p' \in \mathbb{N}$ tel que pour tout $n \geqslant p'$

$$b < a - \epsilon' \leqslant x_n \leqslant a + \epsilon' < c$$

donc $x_n \in]b, c[$.

Remarque 5.6.8 : Dans la définition de la convergence, on obtient une formule équivalente en remplaçant n'importe quelle inégalité ($\leqslant$ ou $\geqslant$) par l'inégalité stricte associée. Autrement dit $(x_n)_{n\in\mathbb{N}}$ converge vers a si et seulement si les formules équivalentes suivantes sont vérifiées

$$\begin{aligned}
&(1) \quad \forall \epsilon > 0, \exists p \in \mathbb{N}, \forall n \geqslant p, \left|x_n - a\right| \leqslant \epsilon \\
&(2) \quad \forall \epsilon > 0, \exists p \in \mathbb{N}, \forall n \geqslant p, \left|x_n - a\right| < \epsilon \\
&(3) \quad \forall \epsilon > 0, \exists p \in \mathbb{N}, \forall n > p, \left|x_n - a\right| \leqslant \epsilon \\
&(4) \quad \forall \epsilon > 0, \exists p \in \mathbb{N}, \forall n > p, \left|x_n - a\right| < \epsilon
\end{aligned}$$

Nous avons déjà vu l'équivalence entre les « $\leqslant \epsilon$ » et les « $< \epsilon$ » (remarque 5.4.13, p. 139), ce qui donne l'équivalence entre (1) et (2) et entre (3) et (4). En ce qui concerne les autres équivalences, notons d'abord qu'une inégalité stricte implique l'inégalité large associée : on en déduit que si une propriété est vérifiée pour tout $n \geqslant p$, alors elle est a fortiori aussi vérifiée pour tout $n > p$ (donc (1) $\Longrightarrow$ (3) et (2) $\Longrightarrow$ (4)). Réciproquement, s'il existe un entier p tel qu'une propriété est vérifiée si $n > p$, alors cette propriété est vérifiée si $n \geqslant p + 1$ (donc (3) $\Longrightarrow$ (1) et (4) $\Longrightarrow$ (2)).

Ces pages ne sont pas incluses dans l’aperçu.

On considère deux entiers m et n tels que $m \geqslant n \geqslant \varphi_k$. On a

$$k \leqslant \varphi_k \leqslant n \leqslant m \leqslant \varphi_m$$

donc

$$x_{\varphi_k} \leqslant x_n \leqslant x_m \leqslant x_{\varphi_m}$$

et par conséquent

$$\left|x_m - x_n\right| = x_m - x_n \leqslant x_{\varphi_m} - x_{\varphi_k} = \left|x_{\varphi_m} - x_{\varphi_k}\right| \leqslant \epsilon$$

On en déduit que la suite $(x_n)_{n\in\mathbb{N}}$ est de Cauchy.

- Si la suite $(x_n)_{n\in\mathbb{N}}$ est décroissante et minorée, alors la suite $(-x_n)_{n\in\mathbb{N}}$ est croissante et majorée, donc est de Cauchy, et par conséquent $(x_n)_{n\in\mathbb{N}}$ est aussi une suite de Cauchy.

5.8 Corps $\mathbb{R}$ des nombres réels (introduction)

Prérequis
Les corps archimédiens (section 5.4).

Nous avons maintenant les outils nécessaires pour définir et construire le corps $\mathbb{R}$ des réels. Nous avons vu que le corps $\mathbb{Q}$ possède notamment deux limitations : certains rationnels positifs ne sont pas le carré d'un autre rationnel (ce qui ne serait pas le cas si $\mathbb{Q}$ possédait la propriété de la borne supérieure), et il peut exister des suites de Cauchy qui ne convergent pas (ce qui ne serait pas le cas, par définition, si $\mathbb{Q}$ était complet). Dans n'importe quel corps archimédien, ces deux propriétés (propriété de la borne supérieure et complétude) sont en fait équivalentes. Plus généralement, le théorème suivant donne une série de propriétés équivalentes d'un corps totalement ordonné, qui seront même des propriétés caractéristiques de $\mathbb{R}$, dans le sens où il n'existe qu'un corps totalement ordonné (à un isomorphisme près) vérifiant ces propriétés.

Théorème 5.8.1 (Caractérisations du corps des réels)
Pour tout corps totalement ordonné K, les propriétés suivantes sont équivalentes :

1. K vérifie la propriété dite *de la limite monotone*, qui peut s'exprimer par les deux propriétés équivalentes suivantes :
   - Toute suite croissante majorée converge.
   - Toute suite décroissante minorée converge.
2. K vérifie la propriété dite *de la borne supérieure*, qui peut s'exprimer par les deux propriétés équivalentes suivantes :
   - Toute partie non vide majorée possède une borne supérieure.
   - Toute partie non vide minorée possède une borne inférieure.
3. K est archimédien et complet (toute suite de Cauchy converge).
4. K vérifie le théorème dit *de Bolzano-Weierstrass* : de toute suite bornée on peut extraire une suite convergente.
5. K est archimédien, et vérifie le théorème dit *des suites adjacentes* : si $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont deux suites de K telles que

$$\begin{cases} (a_n)_{n\in\mathbb{N}} \text{ est croissante} \\ (b_n)_{n\in\mathbb{N}} \text{ est décroissante} \end{cases} \qquad \text{et} \qquad \lim_{n\to+\infty} (b_n - a_n) = 0$$

(on dit de telles suites qu'elles sont *adjacentes*) alors $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont deux suites convergentes, de même limite. De plus, pour tous les entiers n et p, cette limite c est telle que

$$a_n \leqslant c \leqslant b_p$$

6. K est archimédien, et vérifie le théorème dit des *segments emboîtés* : si $\left(\left[a_n, b_n\right]\right)_{n\in\mathbb{N}}$ est
   - une suite décroissante de segments non vides, c'est-à-dire que pour tout entier n
   $$\left[a_{n+1}, b_{n+1}\right] \subseteq \left[a_n, b_n\right]$$
   (on dit aussi de tels segments qu'ils sont emboîtés)
   - telle que la suite $(b_n - a_n)_{n\in\mathbb{N}}$ converge vers 0

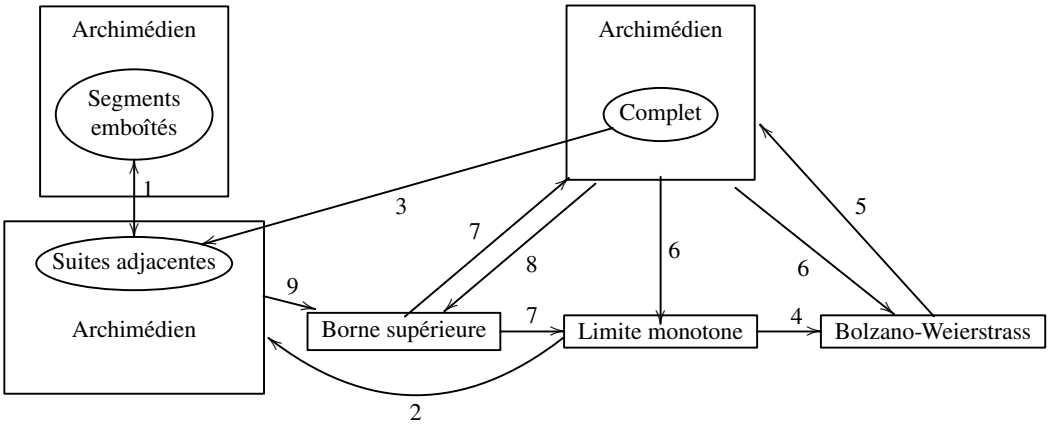
   alors il existe $c \in K$ tel que
   $$\bigcap_{n\in\mathbb{N}} \left[a_n, b_n\right] = \{c\}$$

Preuve

Commençons par deux équivalences simples :

- L'équivalence des deux formulations de la propriété de la limite monotone se déduit du fait que la suite $(x_n)_{n\in\mathbb{N}}$ converge si et seulement si $(-x_n)_{n\in\mathbb{N}}$ converge. En effet, la suite $(x_n)_{n\in\mathbb{N}}$ est croissante si et seulement si $(-x_n)_{n\in\mathbb{N}}$ est décroissante (car $x_{n+1} \geqslant x_n$ si et seulement si $-x_{n+1} \leqslant -x_n$), et elle est majorée par un élément a si et seulement si la suite $(-x_n)_{n\in\mathbb{N}}$ est minorée par $-a$ (car $x_n \leqslant a$ si et seulement si $-a \leqslant -x_n$). On en déduit que si toute suite décroissante minorée converge, alors toute suite $(x_n)_{n\in\mathbb{N}}$ croissante et majorée est telle que $(-x_n)_{n\in\mathbb{N}}$ est décroissante et minorée, donc converge, et par conséquent la suite $(x_n)_{n\in\mathbb{N}}$ converge. Et réciproquement, de la même manière, si toute suite croissante majorée converge alors toute suite décroissante minorée converge.
- Nous avons déjà vu l'équivalence des deux formulations de la propriété de la borne supérieure (définition 1.11.32 du volume 2). Cela est vrai dans n'importe quel ensemble ordonné. Mais on peut aussi démontrer ce résultat en utilisant les propriétés de l'opposé, comme dans le point précédent : on considère une partie A de K, et la partie $-A \overset{\text{def}}{=} \{-x\ ;\ x \in A\}$. Alors A est non vide (respectivement majorée) si et seulement si $-A$ est non vide (respectivement minorée), et elle possède une borne supérieure si et seulement si $-A$ possède une borne inférieure.

Dans la suite, je démontre une liste d'implications qui sont plus que suffisantes pour justifier l'équivalence de toutes les propriétés (on pourrait ne garder qu'une série d'implications circulaires en supprimant ce qui est superflu). Cela correspond au schéma suivant (les numéros renvoient à ce qui suit) :



1. Vérifions l'équivalence du théorème des suites adjacentes et du théorème des segments emboîtés.
   - Notons d'abord que si $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont deux suites adjacentes convergentes, de même limite c, alors pour tous les entiers n et p
   $$a_n \leqslant c \leqslant b_p$$
   (puisque $(a_n)_{n\in\mathbb{N}}$ est croissante de limite c, et $(b_n)_{n\in\mathbb{N}}$ décroissante de limite c).

- Notons aussi qu'il est équivalent de se donner deux suites adjacentes ou une suite de segments emboîtés dont la longueur tend vers 0. En effet, si $(\left[a_n, b_n\right])_{n\in\mathbb{N}}$ est une suite de segments emboîtés, alors pour tout entier n

$$a_n \leqslant a_{n+1} \leqslant b_{n+1} \leqslant b_n$$

donc la suite $(a_n)_{n\in\mathbb{N}}$ est croissante, la suite $(b_n)_{n\in\mathbb{N}}$ est décroissante, et si de plus $(b_n - a_n)_{n\in\mathbb{N}}$ converge vers 0 alors ces suites sont adjacentes. Réciproquement, si les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$, respectivement croissante et décroissante, sont des suites adjacentes, alors $(\left[a_n, b_n\right])_{n\in\mathbb{N}}$ est une suite de segments emboîtés. En effet, s'il existe deux entiers n et p tels que $a_n > b_p$ alors pour tout $k \geqslant \max(n, p)$

$$a_k \geqslant a_n > b_p \geqslant b_k$$

en contradiction avec le fait que $(a_n - b_n)_{n\in\mathbb{N}}$ converge vers 0. On en déduit que pour tout entier n et p, $a_n \leqslant b_p$. En particulier, pour tout n et tout $p \geqslant n$

$$a_n \leqslant a_p \leqslant b_p \leqslant b_n$$

- On fait l'hypothèse que K vérifie le théorème des suites adjacentes. Avec les notations précédentes, $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont convergentes vers une même limite c, donc pour tout $n \in \mathbb{N}$

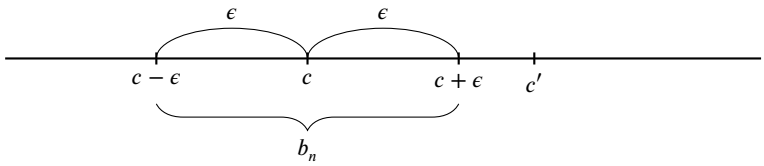
$$a_n \leqslant c \leqslant b_n$$

et par conséquent

$$c \in \bigcap_{n\in\mathbb{N}} \left[a_n, b_n\right]$$

S'il existe dans cette intersection un autre élément $c' \neq c$, on peut par exemple supposer $c' > c$ (le raisonnement est semblable si $c' < c$), et on considère ϵ tel que $0 < \epsilon < c' - c$. D'après la convergence de $(b_n)_{n\in\mathbb{N}}$ vers c, il existe $n \in \mathbb{N}$ tel que $\left|b_n - c\right| \leqslant \epsilon$, donc

$$b_n \leqslant c + \epsilon < c'$$



en contradiction avec $c' \in \left[a_n, b_n\right]$. On en déduit

$$\bigcap_{n\in\mathbb{N}} \left[a_n, b_n\right] = \{c\}$$

- On fait l'hypothèse que K vérifie le théorème des segments emboîtés, et on reprend les notations précédentes. Il existe donc $c \in K$ tel que

$$\bigcap_{n\in\mathbb{N}} \left[a_n, b_n\right] = \{c\}$$

Démontrons que la suite $(a_n)_{n\in\mathbb{N}}$ converge vers c (le raisonnement est semblable pour démontrer que $(b_n)_{n\in\mathbb{N}}$ converge vers c). On considère $\epsilon > 0$. Il existe un entier p tel que $c - \epsilon \notin \left[a_p, b_p\right]$, donc

$$c - \epsilon < a_p \leqslant c \leqslant b_p$$

On en déduit que pour tout $n \geqslant p$

$$c - \epsilon < a_p \leqslant a_n \leqslant c$$

et par conséquent $(a_n)_{n\in\mathbb{N}}$ converge vers c.

2. Supposons que K vérifie la propriété de la limite monotone, et vérifions qu'il est archimédien et qu'il vérifie le théorème des suites adjacentes :
   - K est archimédien, car si $\mathbb{N}$ était majoré la suite $(n)_{n\in\mathbb{N}}$ serait croissante et majorée, donc convergente, et par conséquent ce serait une suite de Cauchy, ce qui est absurde (l'écart entre deux termes consécutifs est $n + 1 - n = 1$).
   - On considère des suites adjacentes $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$, respectivement croissante et décroissante. Alors $(a_n)_{n\in\mathbb{N}}$ est majorée (par tous les termes de $(b_n)_{n\in\mathbb{N}}$), et $(b_n)_{n\in\mathbb{N}}$ est minorée (par tous les termes de $(a_n)_{n\in\mathbb{N}}$). On en déduit que ces deux suites sont convergentes, et comme $(b_n - a_n)_{n\in\mathbb{N}}$ a pour limite 0, ces suites ont une même limite.
3. Supposons que K est complet, et prouvons qu'il vérifie le théorème des suites adjacentes. On considère deux suites adjacentes $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$, respectivement croissante et décroissante. Justifions que ces suites sont de Cauchy (elles

Ces pages ne sont pas incluses dans l’aperçu.

- y majore Q_x, puisque par définition de x, si $q < x$ alors q ne majore pas $\{q \in \mathbb{Q}\,;\ q < y\}$, autrement dit il existe $q' \in \mathbb{Q}$ tel que
$$q < q' < y$$
- Si m est un élément de R' tel que $m < y$, alors il existe des rationnels q et q' tels que
$$m < q < q' < y$$
avec $q' \leqslant x$ (car $q' < y$), donc $q < x$ et par conséquent m ne majore pas Q_x.

Les propriétés indiquées dans le théorème 5.8.1 correspondent à celles que l'on attend de l'ensemble des nombres réels $\mathbb{R}$. Pour le définir, le plus simple est d'introduire un axiome d'existence d'un corps archimédien complet. Le théorème précédent montre alors que ce corps est unique, à un isomorphisme près. Mais pour justifier son existence de façon plus satisfaisante, sans faire appel à un nouvel axiome, il est préférable de construire un tel corps. Les deux façons les plus classiques de le faire [14] s'appuient sur le corps $\mathbb{Q}$. Ce sont

1. La construction par les coupures de Dedekind, imaginée par le mathématicien allemand Richard Dedekind (1831-1916) en 1858 et publiée en 1872 [15].
2. La construction par les suites de Cauchy, imaginée par le mathématicien allemand Georg Cantor (1845-1918) [16].

Ces deux constructions seront détaillées dans les sections qui suivent. On obtient dans le premier cas un corps totalement ordonné vérifiant la propriété de la borne supérieure, dans le deuxième un corps totalement ordonné archimédien et complet. D'après le théorème précédent, ces constructions sont donc équivalentes, dans le sens où les corps obtenus sont isomorphes. Dans tous les cas, on notera $\mathbb{R}$ le corps obtenu, et ses éléments seront nommés *nombres réels*. En résumé, $\mathbb{R}$ est un corps totalement ordonné archimédien et complet, qui vérifie la propriété de *la borne supérieure*, la propriété de *la limite monotone*, le théorème de *Bolzano-Weierstrass*, le *théorème des suites adjacentes*, et le *théorème des segments emboîtés*. De plus, tout corps archimédien est isomorphe à un sous-corps de $\mathbb{R}$.

Remarque 5.8.10 : Pour tout corps archimédien K, il existe un unique morphisme de corps croissant de $\mathbb{Q}$ dans K, et un unique morphisme de corps croissant de K dans $\mathbb{R}$. On peut traduire ces propriétés en disant que dans la catégorie des corps archimédiens (les flèches étant les morphismes de corps croissants), $\mathbb{Q}$ est un objet initial et $\mathbb{R}$ un objet terminal.

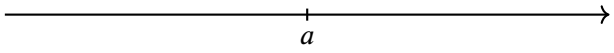
Remarque 5.8.11 : L'habitude que l'on a de manipuler des nombres décimaux depuis notre plus jeune âge peut donner l'illusion qu'une construction naturelle des réels peut se faire à partir de leur développement décimal illimité. C'est une approche possible, mais plus complexe que les deux autres envisagées ; pas d'un point de vue théorique, mais d'un point de vue technique : il suffit pour s'en convaincre de réfléchir à comment définir l'addition et la multiplication à partir du développement décimal illimité de réels, et penser qu'à partir de là il faut encore démontrer les différentes propriétés de ces opérations…

14. Il en existe d'autres.
15. R. Dedekind. *Stetigkeit und irrationale Zahlen* [Continuité et nombres irrationnels] (1872).
16. G. Cantor. « Über die Ausdehnung eines Satzes aus der Theorie der trigonometrischen Reihen [Sur l'extension d'un théorème de la théorie des séries trigonométriques] ». *Mathematische Annalen* 5 (1872).

5.9 Construction de $\mathbb{R}$ par les coupures de Dedekind

Si l'on se représente l'ensemble des rationnels sur une droite, on constate que tout rationnel a coupe la droite en deux (les rationnels x tels que $x < a$ et ceux tels que $x > a$), ce qui permet de faire une partition de $\mathbb{Q}$ en deux ensembles (il y a deux possibilités) :

$$\{x \in \mathbb{Q}\ ;\ x < a\}, \{x \in \mathbb{Q}\ ;\ x \geqslant a\} \qquad \text{ou} \qquad \{x \in \mathbb{Q}\ ;\ x \leqslant a\}, \{x \in \mathbb{Q}\ ;\ x > a\}$$



Ces partitions, de la forme (A, B), sont telles que tout élément de A est strictement inférieur à tout élément de B. Si l'on suppose connus les nombres réels, on constate qu'un réel irrationnel, par exemple $\sqrt{2}$, partage de la même façon la droite en deux ensembles de rationnels (les rationnels x tel que $x < \sqrt{2}$ et ceux tels que $x > \sqrt{2}$). Mais cette partition peut s'exprimer uniquement à partir de $\mathbb{Q}$, sans faire appel à l'ensemble $\mathbb{R}$ des réels que l'on veut construire : elle est formée de l'ensemble des rationnels positifs x tels que $x^2 > 2$, et de son complémentaire.

L'idée de Dedekind est alors de *définir* les réels par ces partitions de $\mathbb{Q}$ de la forme (A, B), où tout élément de A est strictement inférieur à tout élément de B, et qu'il appelle des *coupures*. Quand A a un plus grand élément (ou B un plus petit élément) a, la coupure correspond au rationnel a, et sinon elle correspond à un irrationnel.

De nos jours, on impose généralement une condition supplémentaire pour éviter la double représentation d'un rationnel, en supposant que A ne peut pas avoir de plus grand élément. Par ailleurs, comme chacun des ensembles A et B détermine l'autre, il est équivalent de définir une coupure uniquement par la première composante A (j'adopterai ce point de vue), ce qui donne les définitions suivantes :

Définition 5.9.1 (Coupure de Dedekind, version symétrique)
On appelle *coupure de Dedekind* de $\mathbb{Q}$ tout couple (A, B) formant une partition de $\mathbb{Q}$, tel que tout élément de A soit strictement inférieur à tout élément de B, et tel que A n'admette pas de plus grand élément. Autrement dit, A et B sont des sous-ensembles de $\mathbb{Q}$ tels que

$$\begin{cases} A \neq \varnothing \\ B \neq \varnothing \\ A \cup B = \mathbb{Q} \end{cases} \qquad \text{et} \qquad \begin{cases} \forall a \in A, \forall b \in B, a < b \\ \forall a \in A, \exists x \in A, x > a \end{cases}$$

Définition 5.9.2 (Coupure de Dedekind, version non symétrique)
On appelle *coupure de Dedekind* de $\mathbb{Q}$ tout segment initial strict non vide A de $\mathbb{Q}$ n'ayant pas de plus grand élément, autrement dit tout sous-ensemble A de $\mathbb{Q}$ tel que

$$\begin{cases} A \neq \varnothing \\ A \neq \mathbb{Q} \end{cases} \qquad \text{et} \qquad \begin{cases} \forall x\ a \in \mathbb{Q}, \begin{cases} x \leqslant a \\ a \in A \end{cases} \implies x \in A \\ \forall a \in A, \exists x \in A, x > a \end{cases}$$

Preuve (de l'équivalence des définitions)
- Une partition (A, B) vérifiant la version symétrique de la définition est telle que A vérifie la version non symétrique : $A \neq \mathbb{Q}$ car $A = \complement B$ et $B \neq \varnothing$. Et pour tout x et a dans $\mathbb{Q}$ tels que $a \in A$, si $x \notin A$, autrement dit si $x \in B$, alors $x > a$,

donc par contraposition si $x \leqslant a$ alors $x \in A$.

- Une partie de A vérifiant la version non symétrique de la définition est telle que $(A, \complement A)$ vérifie la version symétrique : $A \cup \complement A = \mathbb{Q}$ par définition du complémentaire et $\complement A \neq \varnothing$ car $A \neq \mathbb{Q}$, et pour tout $a \in A$ et $b \in \mathbb{Q}$, si $b \leqslant a$ alors $b \in A$, donc par contraposition si $b \in \complement A$ alors $a < b$.

Remarque 5.9.3 : D'après l'équivalence des deux définitions, toute coupure A est telle que tout élément de A est strictement inférieur à tout élément du complémentaire de A, et pour tout $x \in \mathbb{Q}$, on a les équivalences suivantes :

- $x \notin A$.
- x majore strictement A (pour tout $a \in A$, $a < x$).
- x majore A (pour tout $a \in A$, $a \leqslant x$).

En effet : si $x \notin A$ alors x majore strictement A d'après ce qui précède, si x majore strictement A alors a fortiori x majore A, et si x majore A alors $x \notin A$, car sinon x serait le plus grand élément de A, en contradiction avec la définition d'une coupure.

Exemple 5.9.4 (Exemples de coupure)

1. Pour tout $a \in \mathbb{Q}$, l'intervalle $]-\infty, a[_{\mathbb{Q}}$ est une coupure : nous avons déjà vu dans le volume 2 que ce type d'intervalle est un segment initial strict non vide (ce qui est immédiat : il est non vide car il contient $a - 1$, il est différent de $\mathbb{Q}$ car il ne contient pas a, et si $x < a$ et $y \leqslant x$ alors $y < a$), qui n'a pas de plus grand élément car si x est un rationnel tel que $x < a$, il existe un rationnel y tel que $x < y < a$.
2. L'ensemble $A \overset{\text{def}}{=} \left\{x \in \mathbb{Q} \,;\, x < 0 \text{ ou } x^2 < 2\right\}$ est une coupure :
   - Il est non vide (par exemple $0 \in A$), et différent de $\mathbb{Q}$ (par exemple $2 \notin A$ car $2^2 \geqslant 2$).
   - Si $a \in A$ et $x \leqslant a$, alors soit $x < 0$ donc $x \in A$, soit $x \geqslant 0$ et alors $x^2 \leqslant a^2 < 2$ donc $x \in A$.
   - A n'a pas de plus grand élément, car sinon ce serait aussi le plus grand élément de $\left\{x \in \mathbb{Q} \,;\, x^2 < 2\right\}$, donc a fortiori la borne supérieure de cet ensemble, et nous avons vu que c'est impossible (un tel élément devrait avoir pour carré le nombre 2).

L'exemple précédent illustre les deux types de coupures possibles. En effet, pour toute coupure A :

- Soit A admet une borne supérieure (dans $\mathbb{Q}$). C'est le cas de la coupure $]-\infty, a[_{\mathbb{Q}}$, qui admet a comme borne supérieure, et qui représentera l'élément a de $\mathbb{R}$, nombre rationnel. Toutes les coupures ayant une borne supérieure a sont de cette forme. En effet :

  — Puisque a est un majorant de A c'est un majorant strict, donc tout $x \in A$ est tel que $x < a$, autrement dit $A \subseteq]-\infty, a[$.

  — Réciproquement, puisque a est la borne supérieure de A, pour tout élément $x < a$ il existe $y \in A$ tel que $x < y$, donc $x \in A$. On en déduit $]-\infty, a[\subseteq A$.

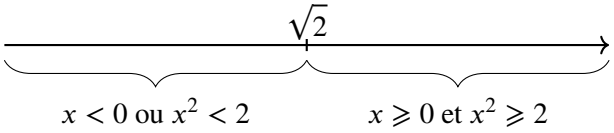
  On notera que dans ce cas, la borne supérieure de A est aussi le plus petit élément de son complémentaire.

- Soit A n'admet pas de borne supérieure. C'est le cas de $\left\{x \in \mathbb{Q} \,;\, x < 0 \text{ ou } x^2 < 2\right\}$. Dans cette situation, le complémentaire de A n'a pas de borne inférieure, car si $\complement A$ admet une borne inférieure a, alors a est la borne supérieure de A :

  — a est un majorant de A car $a \notin A$: en effet, si $a \in A$ alors il existe $x \in A$ tel que $x > a$ (car A n'a pas de plus grand élément), donc il existe $y \notin A$ tel que $y < x$ (car a est la borne inférieure de $\complement A$), ce qui est impossible.

— a est la borne supérieure de A, car si $x < a$ alors $x \in A$ (car a minore $\complement A$), donc il existe $y \in A$ tel que $y > x$ (car A n'a pas de plus grand élément).

Cette seconde situation correspond d'une certaine manière à un « trou » dans l'ensemble des rationnels, qui sera comblé par un nombre réel irrationnel. Ainsi, la coupure de l'exemple ci-dessus représentera l'élément $\sqrt{2}$ de $\mathbb{R}$, nombre irrationnel.



D'où le théorème suivant :

Théorème 5.9.5
- Si une coupure A admet une borne supérieure a, alors $A =]-\infty, a[$.
- Une coupure A n'a pas de borne supérieure si et seulement si $\complement A$ n'a pas de borne inférieure.

Une dernière propriété avant de définir $\mathbb{R}$: pour toute coupure A et tout rationnel strictement positif ϵ, on peut toujours trouver un élément de A et un majorant de A (autrement dit un rationnel qui n'appartient pas à A) de telle sorte que l'écart entre ces deux nombres soit égal à ϵ :

Théorème 5.9.6
Pour toute coupure A et tout $\epsilon \in \mathbb{Q}_+^*$, il existe $a \in A$ et $b \notin A$ tel que

$$b - a = \epsilon$$

Preuve
On considère $x \in A$ et $y \notin A$ (on a donc $y > x$). Puisque $\mathbb{Q}$ est archimédien, il existe un entier n tel que $x + n\epsilon > y$, et par conséquent tel que $x + n\epsilon \notin A$. On peut donc définir

$$m \stackrel{\text{def}}{\equiv} \min\{n \in \mathbb{N} \,;\, x + n\epsilon \notin A\}$$

De plus $m \neq 0$ car $x \in A$. On en déduit

$$\begin{cases} x + m\epsilon \notin A \\ x + (m-1)\epsilon \in A \end{cases}$$

et

$$(x + m\epsilon) - (x + (m-1)\epsilon) = \epsilon$$

Théorème 5.9.7 (Corollaire)
Pour toute coupure A et tout $\epsilon \in \mathbb{Q}_+^*$, il existe $a \in a$ et $b \notin A$ tel que

$$0 < b - a < \epsilon$$

Preuve
Il suffit d'appliquer le théorème précédent en prenant n'importe quel rationnel strictement positif et strictement inférieur à ϵ, par exemple $\frac{\epsilon}{2}$.

Ces pages ne sont pas incluses dans l’aperçu.

Remarque 5.11.23 : Si x et y sont deux réels strictement positifs et a et b deux rationnels tels que $x^a = y^b$, alors $x = y^{\frac{b}{a}}$, car

$$x = x^1 = (x^a)^{\frac{1}{a}} = (y^b)^{\frac{1}{a}} = y^{\frac{b}{a}}$$

Théorème 5.11.24 (Corollaire)
Pour tous les réels $x \geqslant 0$ et $y \geqslant 0$

$$\sqrt{xy} = \sqrt{x}\sqrt{y}$$

Pour tout réel $x > 0$ et tout rationnel b

$$\frac{1}{\sqrt{x}} = \sqrt{\frac{1}{x}}$$
$$(\sqrt{x})^b = \sqrt{x^b}$$

Preuve
On a

$$\sqrt{xy} = (xy)^{\frac{1}{2}} = x^{\frac{1}{2}} y^{\frac{1}{2}} = \sqrt{x}\sqrt{y}$$
$$\frac{1}{\sqrt{x}} = (\sqrt{x})^{-1} = (x^{\frac{1}{2}})^{-1} = (x^{-1})^{\frac{1}{2}} = \sqrt{x^{-1}} = \sqrt{\frac{1}{x}}$$
$$(\sqrt{x})^b = (x^{\frac{1}{2}})^b = x^{\frac{b}{2}} = (x^b)^{\frac{1}{2}} = \sqrt{x^b}$$

Théorème 5.11.25 (Valeurs approchées par défaut et par excès)
On considère un entier $b > 1$, un réel x, et pour tout entier n les nombres

$$x_n \overset{\text{def}}{\equiv} \frac{\lfloor b^n x \rfloor}{b^n} \qquad \text{et} \qquad y_n \overset{\text{def}}{\equiv} x_n + \frac{1}{b^n}$$

- Pour tout entier n

$$x_n \leqslant x < y_n \qquad \text{et} \qquad \begin{cases} x - x_n < b^{-n} \\ y_n - x \leqslant b^{-n} \end{cases}$$

  On dit que x_n est la *valeur approchée* de x à b^{-n} *par défaut*, et y_n la *valeur approchée* de x à b^{-n} *par excès*.
- Les suites $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ sont adjacentes, de limite commune x.

Preuve
On a

$$\lfloor b^n x \rfloor \leqslant b^n x < \lfloor b^n x \rfloor + 1$$
$$\frac{\lfloor b^n x \rfloor}{b^n} \leqslant x < \frac{\lfloor b^n x \rfloor}{b^n} + \frac{1}{b^n}$$
$$x_n \leqslant x < y_n$$

donc

$$x - x_n < y_n - x_n = b^{-n} \qquad \text{et} \qquad y_n - x \leqslant y_n - x_n = b^{-n}$$

Par ailleurs,

$$\lfloor b^n x \rfloor \leqslant b^n x$$

$$b\lfloor b^n x\rfloor \leqslant b^{n+1}x$$

Or $b\lfloor b^n x\rfloor \in \mathbb{Z}$, donc

$$b\lfloor b^n x\rfloor \leqslant \lfloor b^{n+1}x\rfloor$$
$$x_n = \frac{\lfloor b^n x\rfloor}{b^n} \leqslant \frac{\lfloor b^{n+1}x\rfloor}{b^{n+1}} = x_{n+1}$$

et par conséquent la suite $(x_n)_{n\in\mathbb{N}}$ est croissante. De même

$$b^n x < \lfloor b^n x\rfloor + 1$$
$$b^{n+1}x < b\lfloor b^n x\rfloor + b$$

Or $b\lfloor b^n x\rfloor + b \in \mathbb{Z}$, donc

$$\lfloor b^{n+1}x\rfloor + 1 \leqslant b\lfloor b^n x\rfloor + b$$
$$y_{n+1} = \frac{\lfloor b^{n+1}x\rfloor}{b^{n+1}} + \frac{1}{b^{n+1}} \leqslant \frac{\lfloor b^n x\rfloor}{b^n} + \frac{1}{b^n} = y_n$$

et par conséquent la suite $(y_n)_{n\in\mathbb{N}}$ est décroissante. Enfin,

$$y_n - x_n = \frac{1}{b^n}$$

donc la suite $(y_n - x_n)_{n\in\mathbb{N}}$ converge vers 0 (car $b > 1$). On en déduit que ces deux suites sont adjacentes, et que leur limite est x.

Théorème 5.11.26 (Développement d'un nombre réel en base *b*)
On considère un entier $b > 1$, un réel x, la suite $(x_n)_{n\in\mathbb{N}}$ des valeurs approchées de x à b^{-n} près par défaut, autrement dit

$$x_n \overset{\text{def}}{\equiv} \frac{\lfloor b^n x\rfloor}{b^n}$$

et la suite $(a_n)_{n\in\mathbb{N}}$ d'entiers relatifs définie par

$$\begin{cases} a_0 \overset{\text{def}}{\equiv} \lfloor x\rfloor \\ a_{n+1} \overset{\text{def}}{\equiv} \lfloor b^{n+1}x\rfloor - b\lfloor b^n x\rfloor \end{cases}$$

que l'on appelle le *développement de x en base b* (ou le *développement décimal* quand $b = 10$).

1. Pour tout $n \in \mathbb{N}$
$$x_n = \sum_{k=0}^{n} \frac{a_k}{b^k} = a_0 + \frac{a_1}{b} + \cdots + \frac{a_n}{b^n}$$
2. Les suites $\left(\sum_{k=0}^{n} \frac{a_k}{b^k}\right)_{n\geqslant 0}$ et $\left(\sum_{k=1}^{n} \frac{a_k}{b^k}\right)_{n\geqslant 1}$ sont convergentes, et
$$x = \lim_{n\longrightarrow+\infty} \sum_{k=0}^{n} \frac{a_k}{b^k} = a_0 + \lim_{n\longrightarrow+\infty} \sum_{k=1}^{n} \frac{a_k}{b^k}$$
3. On considère l'ensemble E des suites $(\alpha_n)_{n\in\mathbb{N}}$ d'entiers relatifs tels que
   - Pour tout $n > 0$
   $$0 \leqslant \alpha_n < b$$

- Pour tout $n > 0$, il existe $k \geqslant n$ tel que $\alpha_k \neq b-1$.

Alors $(a_n)_{n\in\mathbb{N}} \in E$, et la fonction

$$\begin{cases} \mathbb{R} \longrightarrow E \\ x \longmapsto (a_n)_{n\in\mathbb{N}} \end{cases}$$

est une bijection.

Preuve

1. On a $a_0 = x_0 = \lfloor x \rfloor$, et pour tout entier $k > 0$

$$\frac{a_k}{b^k} = \frac{\lfloor b^k x \rfloor}{b^k} - \frac{\lfloor b^{k-1} x \rfloor}{b^{k-1}} = x_k - x_{k-1}$$

donc

$$\sum_{k=0}^{n} \frac{a_k}{b^k} = x_0 + \sum_{k=1}^{n} (x_k - x_{k-1}) = x_0 + x_n - x_0 = x_n$$

2. D'après le théorème précédent), $(x_n)_{n\in\mathbb{N}}$ converge vers x ; de plus

$$x_n = \sum_{k=0}^{n} \frac{a_k}{b^k} = a_0 + \sum_{k=1}^{n} \frac{a_k}{b^k}$$

donc $\left(\sum_{k=1}^{n} \frac{a_k}{b^k} \right)_{n\geqslant 1}$ converge aussi (vers $x - a_0$), et

$$x = \lim_{n\longrightarrow+\infty} x_n = \lim_{n\longrightarrow+\infty} \sum_{k=0}^{n} \frac{a_k}{b^k} = a_0 + \lim_{n\longrightarrow+\infty} \sum_{k=1}^{n} \frac{a_k}{b^k}$$

3. Prouvons que la suite $(a_n)_{n\in\mathbb{N}}$ appartient à l'ensemble E :

- C'est une suite d'entiers relatifs par construction, et on a vu dans la preuve du théorème précédent que l'on a les inégalités suivantes, pour tout $n \in \mathbb{N}$

$$\begin{cases} b\lfloor b^n x \rfloor \leqslant \lfloor b^{n+1} x \rfloor \\ \lfloor b^{n+1} x \rfloor + 1 \leqslant b\lfloor b^n x \rfloor + b \end{cases}$$

autrement dit

$$0 \leqslant a_{n+1} = \lfloor b^{n+1} x \rfloor - b\lfloor b^n x \rfloor \leqslant b - 1 < b$$

- Vérifions la seconde condition, par l'absurde, en faisant l'hypothèse contraire qu'il existe un entier p tel que pour tout $k \geqslant p+1$, $a_k = b-1$. Pour tout $n \geqslant p+1$

$$x_n - x_p = \sum_{k=0}^{n} \frac{a_k}{b^k} - \sum_{k=0}^{p} \frac{a_k}{b^k} = \sum_{k=p+1}^{n} \frac{a_k}{b^k} = \sum_{k=p+1}^{n} \frac{b-1}{b^k} = \sum_{k=p+1}^{n} \left(\frac{1}{b^{k-1}} - \frac{1}{b^k} \right) = \frac{1}{b^p} - \frac{1}{b^n}$$

donc la suite $(y_n)_{n\in\mathbb{N}}$ des valeurs approchées de x à b^{-n} par excès, est telle que pour tout $n \geqslant p+1$

$$y_n = x_n + \frac{1}{b^n} = x_p + \frac{1}{b^p} = y_p$$

On en déduit que la suite $(y_n)_{n\in\mathbb{N}}$ converge vers y_p (elle est constante à partir d'un certain rang). Or on sait qu'elle converge vers x, donc $x = y_p$, en contradiction avec le fait que pour tout $n \in \mathbb{N}$, $x < y_n$.

Il reste à vérifier que la fonction

$$f : \begin{cases} \mathbb{R} \longrightarrow E \\ x \longmapsto (a_n)_{n\in\mathbb{N}} \end{cases}$$

est une bijection. C'est déjà une injection d'après un des points précédents, car si $f(x) = f(y) = (a_n)_{n\in\mathbb{N}}$ alors

$$x = \lim_{n\longrightarrow+\infty} \sum_{k=0}^{n} \frac{a_k}{b^k} = y$$

Ces pages ne sont pas incluses dans l’aperçu.

les éléments de $A \cup \{-\infty, +\infty\}$, c'est-à-dire que je noterai par exemple

$$\begin{cases}]a, +\infty] \overset{\text{def}}{=\!=} \{x \in A \cup \{-\infty, +\infty\} \ ; \ a < x \leqslant +\infty\} = \{x \in A \cup \{-\infty, +\infty\} \ ; \ x > a\} \\ ]a, +\infty[\overset{\text{def}}{=\!=} \{x \in A \cup \{-\infty, +\infty\} \ ; \ a < x < +\infty\} = \{x \in A \ ; \ x > a\} =]a, +\infty[_A \end{cases}$$

Si $a \in A$ alors ces deux intervalles sont différents car $+\infty$ appartient au premier mais pas au second.

5.13 Corps $\mathbb{C}$ des nombres complexes

D'après les propriétés des anneaux totalement ordonnés, le carré d'un nombre réel est toujours positif, ce qui conduit à certaines « limitations » de $\mathbb{R}$: par exemple, si $a < 0$, l'équation d'inconnue x

$$x^2 = a$$

n'a pas de solution. Supposons que l'on veuille « agrandir » $\mathbb{R}$ pour pallier ces limitations. Notons d'abord qu'il suffit pour cela de disposer d'un élément dont le carré est égal à -1, notons-le i [18] : dans ce cas tout nombre réel strictement négatif est de la forme $-b$, avec $b > 0$, et on a

$$(\mathrm{i}\sqrt{b})^2 = \mathrm{i}^2 \times (\sqrt{b})^2 = -1 \times b = -b$$

Mais au-delà de la possibilité de résoudre certaines équations insolubles dans $\mathbb{R}$, l'ajout de ces nouveaux nombres apporte des techniques supplémentaires pour résoudre des équations dont les solutions sont des nombres réels. C'est ce que découvre le mathématicien italien Rafael (ou Raphaël) Bombelli (1526-1572), dont les travaux marquent le début de l'étude des nombres complexes :

Il étudie la méthode de résolution des équations du troisième degré du mathématicien italien Tartaglia (1499/1500-1557), reprise par le mathématicien, philosophe, médecin et inventeur italien Girolamo Cardano (Jérôme Cardan en français) (1501-1576). Dans celle-ci, on est amené à rechercher la racine cubique d'expressions de la forme $a + \sqrt{b}$. C'est le cas où $b < 0$ qui est problématique, et qui conduit Bombelli à donner un nouveau nom à ce genre de racine carrée : il les nomme *piu di meno* (plus de moins), probablement l'abréviation de *piu radice di meno* (plus racine de moins), lorsqu'elles sont additionnées, et *meno di meno* (moins de moins), lorsqu'elles sont soustraites. Autrement dit il écrit

- *plus de moins* pour $+\mathrm{i}$;
- *moins de moins* pour $-\mathrm{i}$.

Et il donne des règles de calcul, qui reviennent à considérer ce que j'ai supposé plus haut, à savoir que i est un nombre tel que $\mathrm{i}^2 = -1$, suivant les règles de calcul usuelles dans un anneau (notamment la règle des signes). L'équation qu'il cherche à résoudre est

$$x^3 = 15x + 4$$

Les formules de résolution de Tartaglia/Cardan donnent comme solution

$$\sqrt[3]{u} + \sqrt[3]{v}$$

où u et v sont définis par

$$\begin{cases} u \overset{\text{def}}{=\!=} 2 + \sqrt{-121} \\ v \overset{\text{def}}{=\!=} 2 - \sqrt{-121} \end{cases}$$

soit, avec la notation suggérée plus haut

$$\begin{cases} u \overset{\text{def}}{=\!=} 2 + i\sqrt{121} = 2 + 11\mathrm{i} \\ v \overset{\text{def}}{=\!=} 2 - i\sqrt{121} = 2 - 11\mathrm{i} \end{cases}$$

18. Inutile de choisir un autre symbole, en faisant semblant de ne pas savoir que c'est ainsi qu'on le désigne !

Bombelli a aussi découvert une méthode pour calculer les racines cubiques de tels nombres ; il trouve ainsi que $2 + i$ est la racine cubique de $2 + 11\mathrm{i}$, ce que l'on peut vérifier :

$$(2 + \mathrm{i})^3 = 2^3 + 3 \times 4 \times \mathrm{i} + 3 \times 2 \times \mathrm{i}^2 + \mathrm{i}^3 = 8 + 12\mathrm{i} - 6 - \mathrm{i} = 2 + 11\mathrm{i}$$

et de même

$$(2 - \mathrm{i})^3 = 2 - 11\mathrm{i}$$

Il en déduit la solution

$$\sqrt[3]{u} + \sqrt[3]{v} = (2 + \mathrm{i}) + (2 - \mathrm{i}) = 4$$

et on peut en effet vérifier que 4 est bien une solution de l'équation (on peut trouver les autres solutions en factorisant par $x - 4$, et en se ramenant à une équation du second degré [19]). Ce qui est intéressant, c'est que l'on a pu ici obtenir une solution dans $\mathbb{R}$ par l'intermédiaire de nombres qui ne sont pas des nombres réels.

Revenons à une formalisation de ce nouvel ensemble de nombres : supposons que l'on veuille inclure $\mathbb{R}$ dans un corps, ou plus généralement un anneau commutatif A, dans lequel se trouve un élément i tel que $i^2 = -1$. Alors l'ensemble

$$\left\{a + ib\,;\ (a, b) \in \mathbb{R}^2\right\}$$

que je noterai C, est un sous-anneau de A, car

- il contient le neutre multiplicatif $(1 = 1 + \mathrm{i} \times 0)$;
- il est stable pour l'opposé :

$$-(a + \mathrm{i}b) = -a - \mathrm{i}b = (-a) + \mathrm{i}(-b)$$

- il est stable par addition :

$$(a + \mathrm{i}b) + (a' + \mathrm{i}b') = (a + a') + \mathrm{i}(b + b')$$

- il est stable par multiplication :

$$(a + \mathrm{i}b) \times (a' + \mathrm{i}b') = aa' + a(\mathrm{i}b') + (\mathrm{i}b)a' + (\mathrm{i}b)(\mathrm{i}b') = aa' - bb' + \mathrm{i}(ab' + ba')$$

Par ailleurs la fonction

$$f : \begin{cases} \mathbb{R}^2 \longrightarrow C \\ (x, y) \longmapsto x + \mathrm{i}y \end{cases}$$

qui est surjective par construction, est aussi injective car si $x + \mathrm{i}y = x' + \mathrm{i}y'$, alors $\mathrm{i}(y - y') = x' - x$. Si $y \neq y'$ alors $\mathrm{i} = \dfrac{x' - x}{y - y'}$, donc

$$\left(\frac{x' - x}{y - y'}\right)^2 = \mathrm{i}^2 = -1$$

ce qui est impossible (puisque le carré d'un nombre réel est positif). On en déduit $y = y'$, et par conséquent $x = x'$. De plus

$$f(a, b) + f(a', b') = f(a + a', b + b')$$

et

$$f(a, b) \times f(a', b') = f(aa' - bb', ab' + ba')$$

On voit alors que si $\mathbb{R}^2$ est muni de la « bonne » structure (suggérée par ce qui précède), il est isomorphe à l'anneau C (via la fonction f).

Ce qui amène la définition suivante :

19. Voir l'exemple 7.4.8, p. 308.

Définition 5.13.1 (Ensemble des nombres complexes)
On note $\mathbb{C}$ l'ensemble $\mathbb{R}^2$ muni de l'addition

$$(x, y) + (x', y') \stackrel{\text{def}}{\equiv} (x + x', y + y')$$

et de la multiplication

$$(x, y) \times (x', y') \stackrel{\text{def}}{\equiv} (xx' - yy', xy' + yx')$$

Ses éléments s'appellent des nombres *complexes*.

Théorème 5.13.2
$(\mathbb{C}, +, \times)$ est un corps, dont l'élément neutre additif est $(0, 0)$ et l'élément neutre multiplicatif est $(1, 0)$.

Preuve

- Comme l'addition est la loi produit de $(\mathbb{R}, +) \times (\mathbb{R}, +)$, on sait qu'elle est commutative et associative (puisque l'addition sur $\mathbb{R}$ l'est), que l'élément neutre est $(0, 0)$ (puisque 0 est l'élément neutre additif de $\mathbb{R}$), et que l'opposé de (x, y) est $(-x, -y)$.
- La commutativité de la multiplication est immédiate, car l'expression de $(x, y) \times (x', y')$ est invariante quand on permute x avec x' et y avec y' (par commutativité des opérations sur $\mathbb{R}$) :

$$(x, y) \times (x', y') = (xx' - yy', xy' + yx') = (x', y') \times (x, y)$$

- $(1, 0)$ est l'élément neutre de la multiplication :

$$(x, y) \times (1, 0) = (x \times 1 - y \times 0, x \times 0 + y \times 1) = (x, y)$$

  Par ailleurs, les deux éléments neutres sont distincts : $(0, 0) \neq (1, 0)$.
- Associativité de la multiplication : on a d'une part

$$\begin{aligned}(x, y) \times ((x', y') \times (x'', y'')) &= (x, y) \times (x'x'' - y'y'', x'y'' + y'x'') \\ &= (x(x'x'' - y'y'') - y(x'y'' + y'x''), x(x'y'' + y'x'') + y(x'x'' - y'y'')) \\ &= (xx'x'' - xy'y'' - x'yy'' - x''yy', xx'y'' + xx''y' + x'x''y - yy'y'')\end{aligned}$$

  et d'autre part

$$\begin{aligned}((x, y) \times (x', y')) \times (x'', y'') &= (xx' - yy', xy' + yx') \times (x'', y'') \\ &= ((xx' - yy')x'' - (xy' + yx')y'', (xx' - yy')y'' + (xy' + yx')x'') \\ &= (xx'x'' - x''yy' - xy'y'' - x'yy'', xx'y'' - yy'y'' + xx''y' + x'x''y)\end{aligned}$$

  et ces deux expressions sont égales.
- Distributivité de la multiplication sur l'addition : on a d'une part

$$\begin{aligned}(x, y) \times ((x', y') + (x'', y'')) &= (x, y) \times (x' + x'', y' + y'') \\ &= (x(x' + x'') - y(y' + y''), x(y' + y'') + y(x' + x'')) \\ &= (xx' + xx'' - yy' - yy'', xy' + xy'' + x'y + x''y)\end{aligned}$$

  et d'autre part

$$\begin{aligned}(x, y) \times (x', y') + (x, y) \times (x'', y'') &= (xx' - yy', xy' + yx') + (xx'' - yy'', xy'' + yx'') \\ &= (xx' - yy' + xx'' - yy'', xy' + x'y + xy'' + x''y)\end{aligned}$$

  et ces deux expressions sont égales.
- Inverse d'un élément non nul : on considère un élément non nul (x, y), autrement dit tel que $(x, y) \neq (0, 0)$. On en déduit $x^2 + y^2 \neq 0$, ce qui permet de définir les deux réels

$$x' \stackrel{\text{def}}{\equiv} \frac{x}{x^2 + y^2} \qquad y' \stackrel{\text{def}}{\equiv} -\frac{y}{x^2 + y^2}$$

Ces pages ne sont pas incluses dans l’aperçu.

Chapitre 6

Algèbre linéaire

6.1 Modules et espaces vectoriels

Dans tout ce chapitre, $\mathbb{A}$ (respectivement $\mathbb{K}$) désigne un anneau (respectivement un corps) quelconque. Parfois, l'anneau $\mathbb{A}$ pourra avoir des propriétés supplémentaires (commutatif, intègre…) ; cela sera alors précisé. Bien entendu, puisqu'un corps est un anneau particulier, tous les théorèmes restent valables si on remplace $\mathbb{A}$ par $\mathbb{K}$.

Définition 6.1.1 (Module, espace vectoriel)

1. On appelle *module* sur $\mathbb{A}$, ou $\mathbb{A}$-*module*, tout groupe $(E, +)$ muni d'une loi de composition externe (que l'on appelle *multiplication par un scalaire*, ou *multiplication scalaire*)

$$\begin{cases} \mathbb{A} \times E \longrightarrow E \\ (a, x) \longmapsto a \cdot x \end{cases}$$

vérifiant les propriétés suivantes :

- La loi $\cdot$ est distributive à gauche sur l'addition de E : pour tout a dans $\mathbb{A}$ et tout x, y dans E

$$a \cdot (x + y) = a \cdot x + a \cdot y$$

- La loi $\cdot$ est distributive à droite sur l'addition de $\mathbb{A}$: pour tout a et b dans $\mathbb{A}$ et tout x dans E

$$(a + b) \cdot x = a \cdot x + b \cdot x$$

- « Associativité mixte » : pour tout a et b dans $\mathbb{A}$ et tout x dans E

$$(ab) \cdot x = a \cdot (b \cdot x)$$

- L'élément neutre multiplicatif de $\mathbb{A}$ est neutre (à gauche) pour $\cdot$: pour tout x dans E

$$1 \cdot x = x$$

2. On appelle *espace vectoriel* tout module sur un corps.

Remarque 6.1.2 (Notations) : Comme d'habitude :

1. Je pourrai noter uniquement E un tel module, ou détailler plus ou moins la structure, selon le contexte, en

notant par exemple $(E, +, -, 0, \cdot)$ ou $(E, +, \cdot)$.

2. Je pourrai aussi noter directement $a \cdot x$ par simple juxtaposition des deux variables (ax). Dans le cas où a est un élément inversible, je pourrai noter $\dfrac{x}{a}$ pour $\dfrac{1}{a} \cdot x$ (c'est-à-dire $a^{-1} \cdot x$).
3. Il y a une légère ambiguïté sur le symbole $+$, mais qui n'est pas très grave dans la mesure où l'on sait à quels éléments il s'applique : par exemple, comme a et b sont des éléments de $\mathbb{A}$, le symbole $+$ de « $a + b$ » représente l'addition dans l'anneau $\mathbb{A}$; et comme $a \cdot x$ et $b \cdot x$ sont des éléments de E, le symbole $+$ de « $a \cdot x + b \cdot x$ » représente l'addition dans le groupe E.

Remarque 6.1.3 (Vocabulaire) : Les éléments de l'anneau $\mathbb{A}$ s'appellent des *scalaires*, et les éléments d'un espace vectoriel s'appellent des *vecteurs* (les éléments d'un module quelconque n'ont pas de nom particulier).

Remarque 6.1.4 : Si B est un sous-anneau de $\mathbb{A}$, alors tout $\mathbb{A}$-module est aussi un B-module (il suffit de restreindre la multiplication scalaire aux éléments de B).

Remarque 6.1.5 : Il arrive qu'on appelle *module à gauche* la structure que je viens de décrire, par opposition à un *module à droite*, que l'on peut définir de la façon symétrique suivante, avec une opération externe

$$\begin{cases} E \times \mathbb{A} \longrightarrow E \\ (x, a) \longmapsto x * a \end{cases}$$

vérifiant les quatre propriétés

$$(x + y) * a = x * a + y * a \qquad x * (a + b) = x * a + x * b \qquad x * (ab) = (x * a) * b \qquad x * 1 = x$$

Cela équivaut aussi à définir l'opération externe

$$\begin{cases} \mathbb{A} \times E \longrightarrow E \\ (a, x) \longmapsto a \cdot x \overset{\text{def}}{=\!=} x * a \end{cases}$$

vérifiant *presque* la définition d'un module à gauche, car on a

$$\begin{aligned} a \cdot (x + y) = (x + y) * a = x * a + y * a = a \cdot x + a \cdot y \\ (a + b) \cdot x = x * (a + b) = x * a + x * b = a \cdot x + b \cdot x \\ 1 \cdot x = x * 1 = x \end{aligned}$$

la seule différence avec un module à gauche étant « l'associativité mixte » qui s'exprime alors ainsi

$$(ab) \cdot x = x * (ab) = (x * a) * b = b \cdot (a \cdot x)$$

Si l'anneau est commutatif on a

$$(ab) \cdot x = (ba) \cdot x = a \cdot (b \cdot x)$$

et on obtient un module à gauche ; il y a alors équivalence entre module à droite et module à gauche. Mais même si l'anneau n'est pas commutatif, on peut se ramener à un module à gauche en prenant l'anneau obtenu en permutant les termes de la multiplication, c'est-à-dire en définissant la multiplication

$$a \times b \overset{\text{def}}{=\!=} ba$$

(ba étant la multiplication de b par a dans l'anneau initial).

Remarque 6.1.6 : Je donnerai des exemples de modules un peu plus loin, après avoir précisé quelques éléments simples, mais importants, de leur structure.

On ajoute parfois dans la définition d'un module la commutativité du groupe $(E, +)$, mais c'est inutile car c'est une conséquence des autres propriétés :

Théorème 6.1.7 (Commutativité du groupe sous-jacent d'un module)
Si $(E, +, \cdot)$ est un $\mathbb{A}$-module, alors le groupe $(E, +)$ est commutatif.

Preuve
Pour tout x et y dans E on a d'une part, par distributivité à droite,

$$(1+1)\cdot(x+y) = 1\cdot(x+y) + 1\cdot(x+y) = x+y+x+y$$

et d'autre part, par distributivité à gauche,

$$(1+1)\cdot(x+y) = (1+1)\cdot x + (1+1)\cdot y = 1\cdot x + 1\cdot x + 1\cdot y + 1\cdot y = x+x+y+y$$

On en déduit

$$x+y+x+y = x+x+y+y$$

$(E, +)$ étant un groupe, on peut simplifier à gauche par x et à droite par y, ce qui donne

$$y+x = x+y$$

Théorème 6.1.8
On considère un $\mathbb{A}$-module E.

1. Pour tout $a \in \mathbb{A}$, la fonction
$$\begin{cases} E \longrightarrow E \\ x \longmapsto a\cdot x \end{cases}$$
est un endomorphisme du groupe E, que l'on appelle *homothétie* de rapport a.
2. Pour tout $x \in E$, la fonction
$$\begin{cases} \mathbb{A} \longrightarrow E \\ a \longmapsto a\cdot x \end{cases}$$
est un morphisme (de groupes) de $(\mathbb{A}, +)$ dans $(E, +)$.

Preuve
La distributivité à gauche prouve que pour tout $a \in \mathbb{A}$, la fonction $x \longmapsto a\cdot x$ est un endomorphisme de E, car pour tout x et y dans E

$$a\cdot(x+y) = a\cdot x + a\cdot y$$

et la distributivité à droite prouve que pour tout $x \in E$, la fonction $a \longmapsto a\cdot x$ est un morphisme de $\mathbb{A}$ dans E, car pour tout a et b dans $\mathbb{A}$

$$(a+b)\cdot x = a\cdot x + b\cdot x$$

Théorème 6.1.9 (Corollaire)
On considère un $\mathbb{A}$-module E. Pour tout $a \in \mathbb{A}$ et $x \in E$

$$a\cdot 0 = 0$$
$$0\cdot x = 0$$
$$-(a\cdot x) = (-a)\cdot x = a\cdot(-x)$$

En particulier

$$(-1)\cdot x = -x$$

Ces pages ne sont pas incluses dans l’aperçu.

Définition 6.3.1 (Fonction linéaire)

1. On considère deux $\mathbb{A}$-modules E et F. On appelle *fonction linéaire*, ou *morphisme de $\mathbb{A}$-modules*, tout morphisme entre les structures $(E,+,\cdot)$ et $(F,+,\cdot)$, autrement dit toute fonction $E \xrightarrow{f} F$ vérifiant les deux propriétés équivalentes suivantes :
   - Pour tout x et y dans E
   $$f(x+y) = f(x) + f(y)$$
   et pour tout a dans $\mathbb{A}$ et tout x dans E
   $$f(a \cdot x) = a \cdot f(x)$$
   - Pour tout a et b dans $\mathbb{A}$, et pour tout x et y dans E
   $$f(a \cdot x + b \cdot y) = a \cdot f(x) + b \cdot f(y)$$
2. On appelle *forme linéaire* toute fonction linéaire d'un $\mathbb{A}$-module E dans le $\mathbb{A}$-module $\mathbb{A}$.
3. On appelle
   - *endomorphisme* (de module) toute fonction linéaire d'un module dans lui-même ;
   - *isomorphisme* (de modules) toute fonction linéaire bijective ;
   - *automorphisme* (de module) tout isomorphisme d'un module dans lui-même.

Preuve (de l'équivalence des définitions)
Si f est un morphisme de $(E,+,\cdot)$ dans $(F,+,\cdot)$ alors
$$f(a \cdot x + b \cdot y) = f(a \cdot x) + f(b \cdot y) = a \cdot f(x) + b \cdot f(y)$$
Réciproquement, si cette propriété est vérifiée, alors en prenant $a \overset{\text{def}}{=} 1$ et $b \overset{\text{def}}{=} 1$, on a pour tout x et y de E
$$f(x+y) = f(1 \cdot x + 1 \cdot y) = 1 \cdot f(x) + 1 \cdot f(y) = f(x) + f(y)$$
et en prenant $b \overset{\text{def}}{=} 0$ et y quelconque, on a pour tout $a \in \mathbb{A}$ et $x \in E$
$$f(a \cdot x) = f(a \cdot x + 0 \cdot y) = a \cdot f(x) + 0 \cdot f(y) = a \cdot f(x)$$

Définition 6.3.2 (Fonction bilinéaire)
On considère trois $\mathbb{A}$-modules E, F, G. On dit qu'une fonction $E \times F \xrightarrow{f} G$ est *bilinéaire* lorsqu'elle est linéaire en chacune de ses variables, c'est-à-dire lorsque

- pour tout $x \in E$, la fonction $y \longmapsto f(x,y)$ est linéaire ;
- pour tout $y \in F$, la fonction $x \longmapsto f(x,y)$ est linéaire.

Autrement dit : pour tout x et x' dans E et tout y et y' dans F
$$f(x, y+y') = f(x,y) + f(x,y')$$
$$f(x+x', y) = f(x,y) + f(x',y)$$
et pour tout a dans $\mathbb{A}$
$$f(x, a \cdot y) = f(a \cdot x, y) = a \cdot f(x,y)$$

Remarque 6.3.3 (Vocabulaire) : Comme en algèbre il est fréquent de nommer *application* ce que je nomme

fonction (mais il n'y a en fait aucune différence entre les deux concepts !), on utilise en général l'expression *application linéaire*. Celle-ci est par ailleurs aussi parfois réservée au cas d'un morphisme entre espaces vectoriels uniquement. Il y a certes de grosses différences entre les propriétés d'un espace vectoriel, et celles d'un module sur un anneau quelconque, mais comme il n'y a aucune différence entre la définition d'un morphisme entre deux modules ou entre deux espaces vectoriels, je ne vois pas d'intérêt à ne pas employer le même terme (c'est comme si on donnait un nom différent à des morphismes de groupes, selon que ces groupes sont commutatifs ou pas).

Remarque 6.3.4 : Comme dans le cas général d'un morphisme entre deux structures, si f est un isomorphisme (respectivement automorphisme), alors f^{-1} est une fonction linéaire, donc f^{-1} est aussi un isomorphisme (respectivement automorphisme).

Remarque 6.3.5 : Une fonction linéaire $E \xrightarrow{f} F$ étant aussi par définition un morphisme de groupes, on a en particulier $f(0) = 0$, et pour tout x dans E, $f(-x) = -f(x)$, et plus généralement pour tout entier relatif n

$$f(nx) = nf(x)$$

De plus, le noyau de f est toujours défini par

$$\mathrm{Ker}(f) \overset{\text{def}}{\equiv} \{x \in E\,;\ f(x) = 0\}$$

et f est injective si et seulement si $\mathrm{Ker}(f) = \{0\}$.

Exemple 6.3.6 (Exemples de fonctions linéaires)

1. Pour tous les $\mathbb{A}$-modules E et F, la fonction constante

$$\begin{cases} E \longrightarrow F \\ x \longmapsto 0 \end{cases}$$

   est (trivialement) linéaire. C'est la seule fonction constante linéaire, puisque l'image de 0 par une fonction linéaire est égale à 0.

2. Pour tout $\mathbb{A}$-module E, la fonction identité

$$\begin{cases} E \longrightarrow E \\ x \longmapsto x \end{cases}$$

   est (trivialement) linéaire.

3. Pour tout module E sur un anneau commutatif $\mathbb{A}$ (donc notamment pour tout espace vectoriel), et pour toute liste $(a_1, \dots, a_n)$ de scalaires, la fonction

$$f : \begin{cases} E^n \longrightarrow E \\ (x_1, \dots, x_n) \longmapsto \displaystyle\sum_{i=1}^{n} a_i \cdot x_i \end{cases}$$

   est linéaire : on a

$$f((x_1, \dots, x_n) + (y_1, \dots, y_n)) = f(x_1 + y_1, \dots, x_n + y_n) = \sum_{i=1}^{n} a_i(x_i + y_i) = \sum_{i=1}^{n} a_i x_i + \sum_{i=1}^{n} a_i y_i$$

Ces pages ne sont pas incluses dans l’aperçu.

Chapitre 7

Séries formelles et polynômes

Prérequis
L'algèbre linéaire du chapitre 6, et en particulier la notion de famille libre et de base (section 6.4).

Dans tout ce chapitre, $\mathbb{A}$ désigne un anneau commutatif et $\mathbb{K}$ un corps.

7.1 Algèbres des séries formelles et des polynômes

Nous avons vu que pour toute $\mathbb{A}$-algèbre E (notamment l'algèbre $\mathbb{A}$), le module $E^{\mathbb{N}}$, muni de la multiplication produit, est une algèbre. Une autre opération, nommée *produit de Cauchy*[1], permet de munir $E^{\mathbb{N}}$ d'une structure d'algèbre :

Théorème 7.1.1 (Produit de Cauchy)
Pour toute $\mathbb{A}$-algèbre E, le $\mathbb{A}$-module $E^{\mathbb{N}}$, muni de la multiplication suivante, nommée *produit de Cauchy*,

$$(u_n)_{n\in\mathbb{N}} * (v_n)_{n\in\mathbb{N}} \overset{\text{def}}{\equiv} \left(\sum_{k=0}^{n} u_k v_{n-k}\right)_{n\in\mathbb{N}} = \left(\sum_{i+j=n} u_i v_j\right)_{n\in\mathbb{N}}$$

est une $\mathbb{A}$-algèbre dont l'élément neutre multiplicatif est la suite $(1, 0, 0, \dots)$, commutative si E est une algèbre commutative.

Preuve

- On a par changement de variable, pour tout $n \in \mathbb{N}$

$$\sum_{k=0}^{n} u_k v_{n-k} = \sum_{i+j=n} u_i v_j$$

grâce à la bijection

$$\begin{cases} [0,n] \longrightarrow \left\{(i,j) \in [0,n]^2 \,;\, i+j=n\right\} \\ k \longmapsto (k, n-k) \end{cases}$$

- La suite $(v_n)_{n\in\mathbb{N}} \overset{\text{def}}{\equiv} (1, 0, \dots)$ est élément neutre pour la multiplication car pour tout $n \in \mathbb{N}$

$$\sum_{k=0}^{n} u_k v_{n-k} = \sum_{k=0}^{n} v_k u_{n-k} = u_n$$

1. Du nom du mathématicien français Augustin-Louis Cauchy (1789-1857).

($v_{n-k} = 1$ si et seulement si $k = n$, et $v_{n-k} = 0$ sinon, $v_k = 1$ si et seulement si $k = 0$, et $v_k = 0$ sinon).

- Vérifions l'associativité de la multiplication :
  On considère trois suites $(u_n)_{n\in\mathbb{N}}$, $(v_n)_{n\in\mathbb{N}}$, $(w_n)_{n\in\mathbb{N}}$. Notons $(x_n)_{n\in\mathbb{N}} \overset{\text{def}}{\equiv} (v_n)_{n\in\mathbb{N}} * (w_n)_{n\in\mathbb{N}}$. Pour tout $n \in \mathbb{N}$
  $$x_n = \sum_{j+k=n} v_j w_k$$
  donc le terme de rang n de la suite $(u_n)_{n\in\mathbb{N}} * ((v_n)_{n\in\mathbb{N}} * (w_n)_{n\in\mathbb{N}})$ est
  $$\sum_{i+l=n} u_i x_l = \sum_{i+l=n} u_i \sum_{j+k=l} v_j w_k = \sum_{i+l=n} \sum_{j+k=l} u_i v_j w_k = \sum_{i+j+k=n} u_i v_j w_k$$
  car on a une partition de $\left\{(i,j,k) \in [0,n]^3 \ ; \ i+j+k = n\right\}$ par la famille $(P_{(i,l)})_{(i,l)\in I}$, avec
  $$I \overset{\text{def}}{\equiv} \left\{(i,l) \in [0,n]^2 \ ; \ i+l = n\right\} \qquad \text{et} \qquad P_{(i,l)} \overset{\text{def}}{\equiv} \left\{(i,j,k) \in [0,n]^3 \ ; \ j+k = l\right\}$$
  De même, en notant $(y_n)_{n\in\mathbb{N}} \overset{\text{def}}{\equiv} (u_n)_{n\in\mathbb{N}} * (v_n)_{n\in\mathbb{N}}$, on a pour tout $n \in \mathbb{N}$
  $$y_n = \sum_{i+j=n} u_i v_j$$
  donc le terme de rang n de la suite $((u_n)_{n\in\mathbb{N}} * (v_n)_{n\in\mathbb{N}}) * (w_n)_{n\in\mathbb{N}}$ est
  $$\sum_{l+k=n} y_l w_k = \sum_{l+k=n} \left(\sum_{i+j=l} u_i v_j \right) w_k = \sum_{l+k=n} \sum_{i+j=l} u_i v_j w_k = \sum_{i+j+k=n} u_i v_j w_k$$
  On en déduit
  $$(u_n)_{n\in\mathbb{N}} * ((v_n)_{n\in\mathbb{N}} * (w_n)_{n\in\mathbb{N}}) = ((u_n)_{n\in\mathbb{N}} * (v_n)_{n\in\mathbb{N}}) * (w_n)_{n\in\mathbb{N}}$$
- Vérifions la distributivité de la multiplication sur l'addition : le terme de rang n de $(u_n)_{n\in\mathbb{N}} * ((v_n)_{n\in\mathbb{N}} + (w_n)_{n\in\mathbb{N}})$ est
  $$\sum_{k=0}^{n} u_k (v_{n-k} + w_{n-k}) = \sum_{k=0}^{n} u_k v_{n-k} + \sum_{k=0}^{n} u_k w_{n-k}$$
  donc
  $$(u_n)_{n\in\mathbb{N}} * ((v_n)_{n\in\mathbb{N}} + (w_n)_{n\in\mathbb{N}}) = ((u_n)_{n\in\mathbb{N}} * (v_n)_{n\in\mathbb{N}}) + ((u_n)_{n\in\mathbb{N}} * (w_n)_{n\in\mathbb{N}})$$
  et de même, le terme de rang n de $((v_n)_{n\in\mathbb{N}} + (w_n)_{n\in\mathbb{N}}) * (u_n)_{n\in\mathbb{N}}$ est
  $$\sum_{k=0}^{n} (v_k + w_k) u_{n-k} = \sum_{k=0}^{n} v_k u_{n-k} + \sum_{k=0}^{n} w_k u_{n-k}$$
  donc
  $$((v_n)_{n\in\mathbb{N}} + (w_n)_{n\in\mathbb{N}}) * (u_n)_{n\in\mathbb{N}} = ((v_n)_{n\in\mathbb{N}} * (u_n)_{n\in\mathbb{N}}) + ((w_n)_{n\in\mathbb{N}} * (u_n)_{n\in\mathbb{N}})$$
- On en déduit que $(E^{\mathbb{N}}, +, *)$ est un anneau. Si de plus E est une algèbre commutative, alors le produit de Cauchy est commutatif, car pour tout $n \in \mathbb{N}$
  $$\sum_{k=0}^{n} u_k v_{n-k} = \sum_{k=0}^{n} u_{n-k} v_k = \sum_{k=0}^{n} v_k u_{n-k}$$
- Enfin, pour tout $a \in \mathbb{A}$ les suites
  $$a \cdot ((u_n)_{n\in\mathbb{N}} * (v_n)_{n\in\mathbb{N}}) \qquad (a \cdot (u_n)_{n\in\mathbb{N}}) * (v_n)_{n\in\mathbb{N}} \qquad (u_n)_{n\in\mathbb{N}} * (a \cdot (v_n)_{n\in\mathbb{N}})$$
  ont le même terme de rang n, car
  $$\sum_{k=0}^{n} a \cdot (u_k v_{n-k}) = \sum_{k=0}^{n} (a \cdot u_k) v_{n-k} = \sum_{k=0}^{n} u_k (a \cdot v_{n-k})$$
  donc elles sont égales.

On déduit de tout ce qui précède que $E^{\mathbb{N}}$ est une $\mathbb{A}$-algèbre (commutative si E est une algèbre commutative).

Ces pages ne sont pas incluses dans l’aperçu.

7.2 Évaluation des polynômes

Dans toute cette section, E représente une $\mathbb{A}$-algèbre.

Définition 7.2.1 (Évaluation d'un polynôme)
Pour tout $x \in E$ et tout polynôme $P \overset{\text{def}}{=} \sum_{n\geqslant 0} a_n X^n$ de $\mathbb{A}[X]$, on appelle *évaluation* de P en x, ce que l'on note $P(x)$, l'élément de E suivant :

$$P(x) \overset{\text{def}}{=} \sum_{n\geqslant 0} a_n x^n$$

Remarque 7.2.2 : L'expression de $P(x)$ est bien définie : la somme est à support fini, et elle se calcule à partir de l'élément x de E et de la suite de scalaires $(a_n)_{n\in\mathbb{N}}$ de l'anneau $\mathbb{A}$, les opérations étant celles de l'algèbre E (addition, multiplication, multiplication scalaire). Notons aussi que pour tout $x \in E$, on a $x^0 = 1_E$, et qu'on a donc notamment $P(0) = a_0 1_E$.

Exemple 7.2.3
Quatre cas particuliers sont particulièrement importants :

- Celui où E est l'anneau $\mathbb{A}$ lui-même.
- Celui où E est l'algèbre $\mathbb{A}[X]$. Dans ce cas $\mathbb{A}$ est un sous-anneau de E.
- Celui où E est l'algèbre $\mathscr{M}_n(\mathbb{A})$ des matrices carrées sur $\mathbb{A}$ ($n \in \mathbb{N}^*$). Dans ce cas l'élément neutre multiplicatif est la matrice I_n.
- Celui où E est l'algèbre des endomorphismes d'un $\mathbb{A}$-module. Dans ce cas l'élément neutre multiplicatif est l'identité de E.

Par exemple avec

$$P \overset{\text{def}}{=} X^2 + 3X + 1 \in \mathbb{Z}[X]$$

- Dans $\mathbb{Z}$, on a par exemple
$$P(2) = 2^2 + 3 \times 2 + 1 = 11$$
- Dans $\mathbb{Z}[X]$, on a par exemple
$$P(X+1) = (X+1)^2 + 3(X+1) + 1 = X^2 + 2X + 1 + 3X + 3 + 1 = X^2 + 5X + 5$$
- Dans $\mathscr{M}_2(\mathbb{Z})$, on a par exemple
$$P\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 + 3\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 3 & 3 \\ 0 & 3 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 5 \\ 0 & 5 \end{pmatrix}$$
- Dans $\mathscr{L}(\mathbb{Z})$, on a par exemple, avec $f \overset{\text{def}}{=} x \longmapsto 2x$,
$$P(f) = f^2 + 3f + \mathrm{id}$$
donc pour tout $x \in \mathbb{Z}$
$$P(f)(x) = f(f(x)) + 3f(x) + x = 4x + 6x + x = 11x$$

Théorème 7.2.4
Pour tout $x \in E$ et pour tous les polynômes P et Q

$$(P+Q)(x) = P(x) + Q(x)$$
$$(PQ)(x) = P(x)Q(x)$$

et pour tout $\lambda \in \mathbb{A}$

$$(\lambda P)(x) = \lambda P(x)$$

Preuve
On considère $x \in E$ et deux polynômes P et Q, avec

$$P = \sum_{n\geqslant 0} a_n X^n \qquad Q = \sum_{n\geqslant 0} b_n X^n$$

On a

$$(P+Q)(x) = \sum_{n\geqslant 0}(a_n + b_n)x^n = \sum_{n\geqslant 0} a_n x^n + \sum_{n\geqslant 0} b_n x^n = P(x) + Q(x)$$

et

$$P(x)Q(x) = \left(\sum_{n\geqslant 0} a_n x^n\right)\left(\sum_{n\geqslant 0} b_n x^n\right) = \sum_{n\geqslant 0}\sum_{k=0}^{n}(a_k x^k)(b_{n-k}x^{n-k}) = \sum_{n\geqslant 0}\sum_{k=0}^{n} a_k b_{n-k} x^n = \sum_{n\geqslant 0}\left(\sum_{k=0}^{n} a_k b_{n-k}\right)x^n = PQ(x)$$

(formules sur les sommes de la section 4.8 du volume 2). Enfin

$$(\lambda P)(x) = \sum_{n\geqslant 0} \lambda a_n x^n = \lambda \sum_{n\geqslant 0} a_n x^n = \lambda P(x)$$

Théorème 7.2.5 (Corollaire)
Pour tout $x \in E$, la fonction

$$\begin{cases} \mathbb{A}[X] \longrightarrow E \\ P \longmapsto P(x) \end{cases}$$

est l'unique morphisme d'algèbres $\mathbb{A}[X] \xrightarrow{\varphi} E$ tel que $\varphi(X) = x$.

Preuve
- Le fait que cette fonction est un morphisme d'algèbres est une conséquence du théorème précédent. Il reste juste à justifier que l'image du polynôme constant égal à 1 (élément neutre de la multiplication dans $\mathbb{A}[X]$) est égale à 1_E (élément neutre de la multiplication dans E) : c'est immédiat, car si $P = 1$ alors pour tout $x \in E$, $P(x) = 1 \cdot 1_E = 1_E$.
- De plus, cette fonction est l'unique morphisme d'algèbres $\mathbb{A}[X] \xrightarrow{\varphi} E$ tel que $\varphi(X) = x$ car, d'une part on a $X(x) = x$, et d'autre part tout morphisme d'algèbres $\mathbb{A}[X] \xrightarrow{\varphi} E$ vérifiant $\varphi(X) = x$ est tel que pour tout polynôme $P \overset{\text{def}}{\equiv} \sum_{n\geqslant 0} a_n X^n$

$$\varphi(P) = \sum_{n\geqslant 0} a_n \varphi(X)^n = \sum_{n\geqslant 0} a_n x^n = P(x)$$

Remarque 7.2.6 : En particulier, pour tout $x \in \mathbb{A}$, la fonction

$$\begin{cases} \mathbb{A}[X] \longrightarrow \mathbb{A} \\ P \longmapsto P(x) \end{cases}$$

est un morphisme d'algèbres.

Ces pages ne sont pas incluses dans l’aperçu.

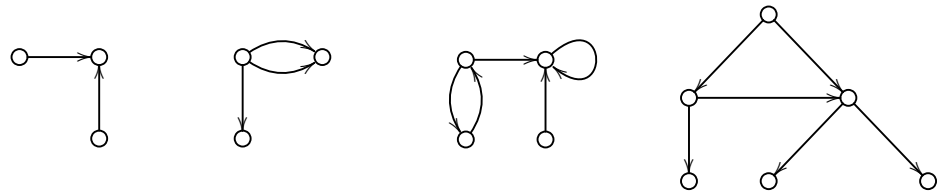
Chapitre 8

Introduction à la théorie des graphes

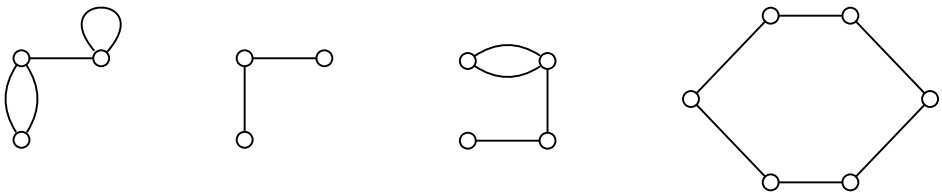
8.1 Présentation informelle et exemples

Un graphe est un objet mathématique représenté par ce qu'on appelle un *diagramme sagittal*, qui est un ensemble de points, que l'on appelle des *sommets*, reliés par des *flèches*, que l'on appelle des *arcs*, ou par de simples traits (non orientés), que l'on appelle des *arêtes*. Dans le premier cas, on dit du graphe qu'il est *orienté*, et dans le second qu'il est *non orienté*. Il peut aussi y avoir parfois plusieurs arêtes (respectivement arcs) entre deux sommets, ainsi que des arêtes (respectivement arcs) d'un sommet à lui-même (c'est ce qu'on appelle une *boucle*).

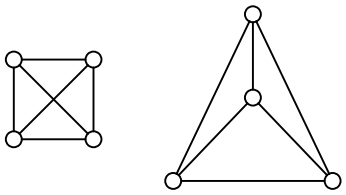
Exemple 8.1.1 (Exemples de graphes orientés)



Exemple 8.1.2 (Exemples de graphes non orientés)



Remarque 8.1.3 : Un même graphe peut avoir des représentations différentes. Par exemple les deux diagrammes suivants représentent le même graphe (non orienté), dans lequel chacun des quatre sommets est relié aux trois autres :



Les graphes peuvent notamment servir à résoudre des problèmes issus de domaines divers, dont voici quelques exemples (simples) classiques :

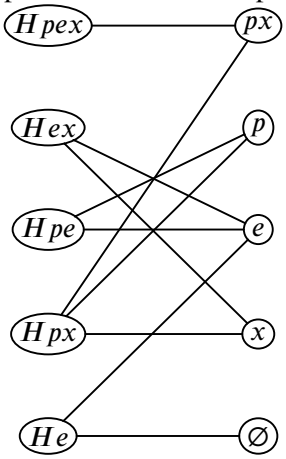
Exemple 8.1.4 (Problème du loup, de la chèvre, et des choux)
Ce problème, qui a connu de nombreuses variantes et reprises, se trouve dans *Propositiones ad acuendos juvenes* [*Problèmes pour aiguiser la jeunesse*], un recueil médiéval de 56 problèmes (53 dans certaines éditions), attribué au poète, érudit et théologien anglais Alcuin (v.735-804) ; c'est l'un des plus anciens textes de mathématiques récréatives connus. Dans ce problème, un homme doit faire traverser une rivière à un loup, une chèvre, et une botte de choux. Sa barque ne lui permettant de transporter qu'un élément à la fois, il doit faire plusieurs voyages, mais avec la condition suivante : il ne peut laisser sans surveillance le loup avec la chèvre, ni la chèvre avec les choux. Un graphe permet ici de visualiser et trouver simplement la solution. Notons

$$H \overset{\text{def}}{\equiv} \text{l'homme} \qquad p \overset{\text{def}}{\equiv} \text{le loup} \qquad e \overset{\text{def}}{\equiv} \text{la chèvre} \qquad x \overset{\text{def}}{\equiv} \text{les choux}$$

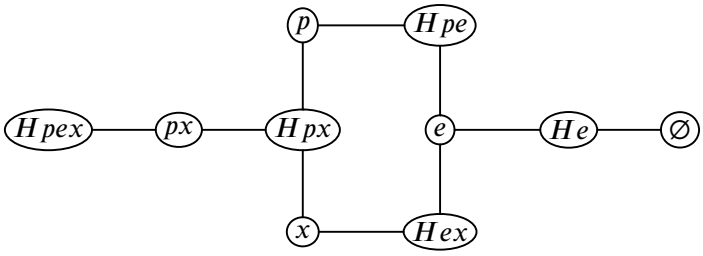
On peut faire la liste de toutes les configurations possibles donnant la position des différents acteurs sur les deux rives (sans tenir compte des déplacements pour l'instant) ; étant donné les contraintes, il n'y en a que 10 :

Rive 1	Hpex	Hex	Hpe	Hpx	He	px	p	e	x	∅
Rive 2	∅	p	x	e	px	He	Hex	Hpx	Hpe	Hpex

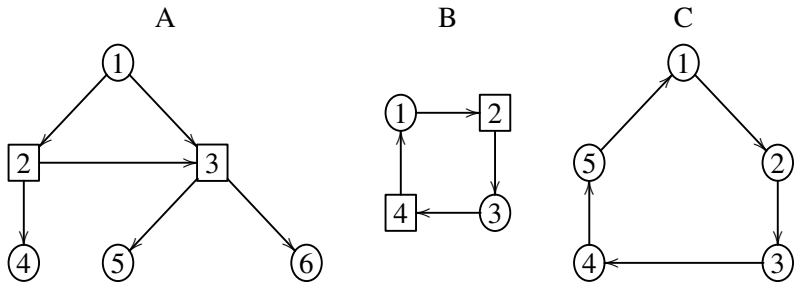
Comme chaque rive est complémentaire l'une de l'autre, on peut caractériser chaque situation uniquement à l'aide de la configuration de la rive 1. L'objectif est de passer de « Hpex » (situation initiale) à « ∅ » (situation finale souhaitée). On peut alors faire un graphe dont les sommets sont ces configurations, et dont les arêtes relient les configurations qui peuvent s'obtenir l'une à partir de l'autre ; on constate en effet que la situation est symétrique, et qu'il est inutile d'orienter le graphe. On constate aussi que les différentes traversées de la rivière font alterner une configuration où l'homme se situe sur la rive 1, à une configuration où il se situe sur la rive 2 ; autrement dit le graphe relie toujours un point « avec H » à un point « sans H » :



En représentant différemment ce graphe, on obtient de façon évidente les deux solutions permettant de résoudre ce problème en un minimum de trajets :



Ces pages ne sont pas incluses dans l’aperçu.



Le graphe A a pour noyau $\{1, 4, 5, 6\}$, le graphe cyclique B a pour noyaux $\{1, 3\}$ et $\{2, 4\}$, et le graphe cyclique C n'a pas de noyau.

Théorème 8.5.6
Un graphe orienté sans cycle possède un unique noyau.

Preuve
On démontre ce résultat par récurrence sur l'ordre du graphe, autrement dit sur le nombre n de ses sommets.

- Si $n = 1$, un graphe sans cycle consiste en un sommet isolé a, qui n'a donc pas de successeur et l'unique noyau est alors (trivialement) $N \stackrel{\text{def}}{=} \{a\}$.
- On fait l'hypothèse de récurrence pour tout $k \leqslant n$, et on considère un graphe G orienté sans cycle d'ordre $n+1$. Comme il n'y a pas de cycle, on sait que G a au moins un puits a, qui doit nécessairement appartenir au noyau (s'il existe). On considère le sous-graphe G' de G obtenu en supprimant a et tous ses prédécesseurs. Le graphe G' est d'ordre inférieur ou égal à n, et n'a pas de cycle (un cycle de G' serait aussi un cycle de G). On déduit de l'hypothèse de récurrence que G' admet un unique noyau N'. Alors $N' \cup \{a\}$ est l'unique noyau de G. En effet :

— Si $x \in N' \cup \{a\}$, alors soit $x = a$ et n'a pas de successeur, soit $x \in N'$, donc si y est un successeur de x, alors $y \neq a$ (car les prédécesseurs de a ne sont pas dans G'), et $y \notin N'$ (car N' est un noyau de G'), donc $y \notin N' \cup \{a\}$.

— On fait l'hypothèse que $x \notin N' \cup \{a\}$, autrement dit $x \notin N'$ et $x \neq a$. Si x est un prédécesseur de a alors x a un successeur dans $N' \cup \{a\}$, et sinon $x \in G'$, et par conséquent x a un successeur dans N', donc dans $N' \cup \{a\}$.

On en déduit que $N' \cup \{a\}$ est un noyau de G. Et il y a unicité, car un noyau N de G contient a, ne contient pas les prédécesseurs de a, et $N \setminus \{a\}$ est l'unique noyau de G' (raisonnement semblable à celui ci-dessus).

Remarque 8.5.7 : La démonstration du théorème donne une méthode algorithmique pour trouver le noyau d'un graphe orienté sans cycle :

- Les puits (les sommets sans successeur) sont dans le noyau, et leurs prédécesseurs ne sont pas dans le noyau.
- Retirer tous ces sommets (et les arêtes associées), et reproduire l'opération dans le sous-graphe obtenu.
- Continuer jusqu'à avoir traité tous les sommets.

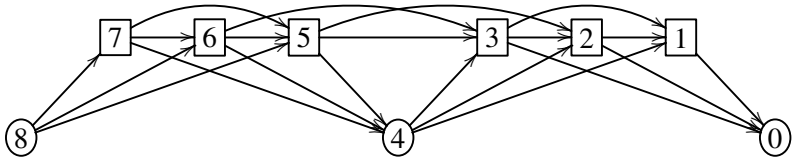
Le noyau peut notamment servir à trouver des stratégies gagnantes à certains jeux. Considérons en effet un jeu de réflexion (donc sans hasard), dans lequel deux joueurs jouent à tour de rôle, et à information complète (c'est-à-dire que les joueurs connaissent à tout moment la situation complète du jeu et l'évolution de cette situation selon les coups joués). Chaque position du jeu peut être modélisée par un sommet d'un graphe orienté, deux sommets étant reliés par un arc s'il existe un coup permettant de passer de l'une à l'autre des positions. Ainsi, à chaque tour de jeu, un joueur se situe sur l'un des sommets et joue un coup plaçant son adversaire sur un autre sommet. On suppose de plus que le jeu s'arrête quand un joueur ne peut plus jouer (c'est-à-dire quand il se situe sur un sommet sans successeur), avec deux variantes : dans une telle position, un joueur peut-être perdant (variante dite *directe*), ou gagnant (variante dite *inverse*). On suppose de plus que le jeu interdit de passer deux fois par une même position, et par conséquent le graphe n'a pas de cycle

et admet donc un noyau. Dans la variante directe, un joueur a une stratégie gagnante s'il peut placer son adversaire dans le noyau (il y a donc une stratégie gagnante pour le premier joueur si la position de départ n'est pas dans le noyau, et une stratégie gagnante pour le deuxième joueur si la position de départ est dans le noyau). En effet, le noyau contient les positions finales perdantes, celles où le joueur ne peut plus jouer (les sommets sans successeur) ; si un joueur est dans le noyau, n'importe lequel de ses coups fait sortir du noyau, ce qui place son adversaire en dehors du noyau ; et un joueur qui n'est pas dans le noyau dispose toujours d'un coup qui place son adversaire dans le noyau. Dans le cas de la variante inverse, on peut toujours se ramener à la situation précédente, en ajoutant un sommet supplémentaire et un arc entre chaque puits du graphe et ce nouveau sommet. Le noyau du nouveau graphe correspond aux positions perdantes, car il amène à l'unique puits du nouveau graphe (le nouveau sommet sans successeur que l'on a ajouté), dont les prédécesseurs sont les positions gagnantes (qui correspondent aux puits du graphe initial).

Exemple 8.5.8 (Jeu de Nim)
On reprend l'exemple du jeu de Nim. Dans la version directe, les deux joueurs prennent de 1 à p allumettes d'un tas qui en contient n, et la personne qui ne peut plus jouer perd. On peut représenter cette situation par un graphe (sans cycle) dont les sommets sont les entiers de 0 à n. L'ensemble des successeurs d'un sommet x est

$$\{y \in \mathbb{N} \,;\; x - p \leqslant y \leqslant x - 1\}$$

Par exemple, si $p \stackrel{\text{def}}{=} 3$, on peut représenter ainsi la partie finale du graphe :



Le noyau est l'ensemble des multiples de $p+1$, c'est-à-dire $N = \{k(p+1) \,;\; k \in \mathbb{N}\}$. On peut le trouver en appliquant l'algorithme proposé un peu plus haut : le seul puits du graphe est 0 (qui est donc dans le noyau), et ses prédécesseurs (1 à p) ne le sont pas. On retire ces sommets et on recommence : le puits est maintenant $p+1$ (qui est dans le noyau), et ses prédécesseurs ($p+2$ à $2p+1$) ne le sont pas, le puits suivant est $2(p+1)$, et ainsi de suite. On peut aussi vérifier par le calcul que N est bien le noyau :

- Un successeur y de $k(p+1)$ est tel que

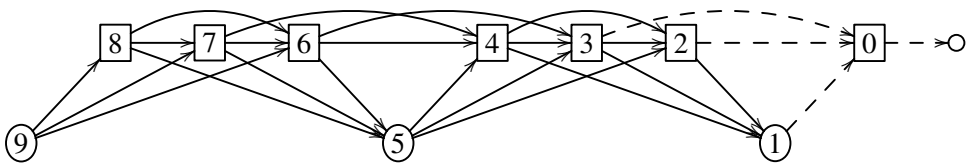
$$(k-1)(p+1) = k(p+1) - (p+1) < k(p+1) - p \leqslant y \leqslant k(p+1) - 1 < k(p+1)$$

  donc $y \notin N$.
- Si $x \notin N$, alors en effectuant la division euclidienne de x par $p+1$, on obtient

$$x = q(p+1) + r$$

  avec $0 < r < p+1$, donc $q(p+1)$ est un successeur de x, avec $q(p+1) \in N$.

La stratégie gagnante consiste à retirer un nombre d'allumettes tel qu'après avoir joué, le nombre restant d'allumettes soit un multiple de $p+1$. Si n est un multiple de $p+1$, alors le deuxième joueur a une stratégie gagnante, sinon le premier joueur a une stratégie gagnante. Dans la version inverse du jeu de Nim, on a par exemple, avec $p \stackrel{\text{def}}{=} 3$



Ces pages ne sont pas incluses dans l’aperçu.

Chapitre 9

Structures topologiques

9.1 Espaces topologiques

La topologie est une notion mathématique permettant de formaliser le concept de *proximité*, et en particulier de définir les notions de limites, de continuité, de convergence de suites, etc. Ce concept de proximité va se traduire, sur un ensemble E quelconque, par ce qu'on appelle des *voisinages*, qui eux-mêmes peuvent s'exprimer à l'aide de sous-ensembles particuliers de E, que l'on appelle des *ouverts*, ou de manière équivalente par les complémentaires de ces sous-ensembles, que l'on appelle des *fermés*.

Définition 9.1.1 (Topologie, espace topologique, ouvert)

1. On appelle *topologie* sur un ensemble E, tout ensemble $\mathcal{T}$ de sous-ensembles de E (autrement dit $\mathcal{T} \subseteq \mathcal{P}(E)$), que l'on appelle des *ouverts*, vérifiant les propriétés suivantes :
   - E et $\emptyset$ appartiennent à $\mathcal{T}$.
   - Toute réunion d'ouverts est un ouvert, c'est-à-dire que si $(O_i)_{i\in I}$ est une famille d'éléments de $\mathcal{T}$, alors $\bigcup_{i\in I} O_i \in \mathcal{T}$.
   - L'intersection de deux ouverts est un ouvert, c'est-à-dire que si O et O' sont des éléments de $\mathcal{T}$, alors $O \cap O' \in \mathcal{T}$.
2. On appelle *espace topologique* tout ensemble muni d'une topologie.
3. On dit que $(E, \mathcal{T})$ est un *espace séparé*, ou *espace de Hausdorff*, lorsque pour tous points distincts a et b de E, il existe deux ouverts disjoints A et B tels que $a \in A$ et $b \in B$ (donc en particulier $a \notin B$ et $b \notin A$).
4. Si $\mathcal{T}$ et $\mathcal{T}'$ sont deux topologies sur E, on dit que $\mathcal{T}'$ est *plus fine* que $\mathcal{T}$, ou que $\mathcal{T}$ est *plus grossière* que $\mathcal{T}'$, lorsque les ouverts de $\mathcal{T}$ sont aussi des ouverts de $\mathcal{T}'$, autrement dit lorsque $\mathcal{T} \subseteq \mathcal{T}'$.

Remarque 9.1.2 (Vocabulaire) : Attention au vocabulaire, qui est peut-être un peu contre-intuitif : $\mathcal{T}'$ est *plus fine* que $\mathcal{T}$ quand elle est plus grande pour la relation d'inclusion ($\mathcal{T}' \supseteq \mathcal{T}$). $\mathcal{T}'$ est plus fine que $\mathcal{T}$ quand elle a, d'une certaine façon, « plus d'ouverts » (tous les ouverts de $\mathcal{T}$ sont des ouverts de $\mathcal{T}'$).

Remarque 9.1.3 : Par une récurrence immédiate, toute intersection *finie* d'ouverts est un ouvert, c'est-à-dire que si $O_1, \dots, O_n$ sont des éléments de $\mathcal{T}$, alors $O_1 \cap \cdots \cap O_n \in \mathcal{T}$. En effet, c'est vrai si $n = 1$, et si on fait l'hypothèse de récurrence au rang n, alors $O_1 \cap \cdots \cap O_n \in \mathcal{T}$, donc $(O_1 \cap \cdots \cap O_n) \cap O_{n+1} \in \mathcal{T}$ (intersection de deux ouverts). On notera que cette propriété reste valable si $n = 0$, l'intersection d'une famille vide étant égale à E, qui est un ouvert par définition.

Définition 9.1.4 (Fermé)
On appelle *fermé* de l'espace topologique $(E, \mathscr{T})$ tout sous-ensemble de E dont le complémentaire est un ouvert (F est fermé lorsque $\complement_E F \in \mathscr{T}$). On en déduit par dualité[a] les propriétés suivantes :

- E et $\varnothing$ sont des fermés.
- Toute intersection de fermés est un fermé, c'est-à-dire que si $(F_i)_{i\in I}$ est une famille de fermés, alors $\bigcap_{i\in I} F_i$ est fermé.
- Toute réunion finie de fermés est un fermé, c'est-à-dire que si $F_1, \dots, F_n$ sont des fermés, alors $\bigcup_{i=1}^{n} F_i$ est fermé.

a. $\complement\varnothing = E$, $\complement E = \varnothing$, le complémentaire d'une union est une intersection, le complémentaire d'une intersection est une union.

Remarque 9.1.5 : L'ensemble des fermés d'une topologie $\mathscr{T}$ est donc l'ensemble de tous les complémentaires des ouverts, c'est-à-dire l'ensemble $\left\{\complement O\ ;\ O \in \mathscr{T}\right\}$.

Remarque 9.1.6 (Vocabulaire) : Les termes *ouvert* et *fermé* sont à la fois des noms et des adjectifs : on peut dire d'un sous-ensemble de E qu'il est *ouvert* (respectivement *fermé*), ou que c'est *un ouvert* (respectivement *un fermé*).

Remarque 9.1.7 : Une topologie $\mathscr{T}'$ est plus fine qu'une topologie $\mathscr{T}$ si et seulement si tout fermé de $\mathscr{T}$ est un fermé de $\mathscr{T}'$.

Remarque 9.1.8 (Vocabulaire) : Si la topologie $\mathscr{T}$ sur E est implicite, je pourrai juste désigner par E l'espace topologique $(E, \mathscr{T})$, et parler par exemple d'ouverts et de fermés de E, plutôt que d'ouverts et de fermés de la topologie $\mathscr{T}$.

Remarque 9.1.9 : Si F est un fermé et O un ouvert, alors $F \setminus O$ est un fermé puisque son complémentaire est l'ouvert

$$\complement(F \setminus O) = \complement(F \cap (\complement O)) = \complement F \cup O$$

(réunion de deux ouverts).

Exemple 9.1.10 (Exemples de topologies)

1. $\{\varnothing, E\}$ est une topologie sur E (les seuls ouverts sont E et $\varnothing$), que l'on appelle *topologie grossière*, ou *topologie triviale*. C'est la topologie la moins fine possible sur E (autrement dit la plus grossière), puisque par définition toute topologie $\mathscr{T}$ est telle que $\{\varnothing, E\} \subseteq \mathscr{T}$. Par ailleurs si l'ensemble E a au moins deux éléments, muni de cette topologie ce n'est pas un espace séparé, car le seul ouvert auquel appartiennent les éléments de E est E.
2. $\mathscr{P}(E)$ est une topologie sur E (toute partie de E est un ouvert), que l'on appelle *topologie discrète*. C'est la topologie la plus fine possible sur E, puisque par définition toute topologie $\mathscr{T}$ est telle que $\mathscr{T} \subseteq \mathscr{P}(E)$. Par ailleurs
   - E muni de cette topologie est un espace séparé, car si $a \neq b$ alors $\{a\}$ et $\{b\}$ sont des ouverts disjoints.
   - Les singletons sont des ouverts, et la réciproque est vraie : si tous les singletons d'un espace topologique sont des ouverts, alors la topologie est la topologie discrète, autrement dit toute partie

A de E est un ouvert, car $A = \bigcup_{x\in A} \{x\}$.

- On en déduit que si un espace topologique E séparé est fini, alors la topologie est la topologie discrète. En effet, pour tout élément x de E et tout élément y de E distinct de x, il existe un ouvert O_y tel que $x \in O_y$ et $y \notin O_y$. Puisque E est fini, $\bigcap_{y\in E\setminus\{x\}} O_y$ est un ouvert dont le seul élément est x. Par conséquent $\{x\}$ est un ouvert donc la topologie est discrète.

3. La réunion de l'ensemble vide et des parties cofinies d'un ensemble E (c'est-à-dire les parties dont le complémentaire est un ensemble fini) est une topologie, dite *cofinie*. Elle peut être décrite plus simplement par ses fermés, qui sont E et les parties finies de E. Dans le cas où E est un ensemble fini, toutes les parties sont des ouverts et cette topologie coïncide avec la topologie discrète.

Remarque 9.1.11 : Une partie de E peut être à la fois ouverte et fermée (c'est toujours le cas de E et $\varnothing$, quelle que soit la topologie, et dans la topologie discrète c'est le cas de toutes les parties), et elle peut n'être ni ouverte ni fermée (dans la topologie grossière, une partie autre que E et $\varnothing$ n'est ni ouverte ni fermée).

Remarque 9.1.12 : Dans le cas d'un ensemble à un seul élément (un singleton $\{a\}$), la seule topologie possible est à la fois la topologie grossière et la topologie discrète, car dans ce cas $\mathcal{P}(\{a\}) = \{\varnothing, \{a\}\}$. De même pour l'ensemble vide, puisque dans ce cas $\mathcal{P}(\varnothing) = \{\varnothing\}$.

Théorème 9.1.13
Si $(F, \mathcal{T})$ est un espace topologique, alors pour toute fonction $E \xrightarrow{f} F$, l'ensemble des images réciproques par f des ouverts de F, c'est-à-dire $\left\{ \underset{\leftarrow}{f}(O)\ ;\ O \in \mathcal{T} \right\}$, est une topologie sur E, dont les fermés sont les images réciproques des fermés de F.

Preuve
On a $\underset{\leftarrow}{f}(\varnothing) = \varnothing$, $\underset{\leftarrow}{f}(F) = E$, pour toutes parties O et O' de F, $\underset{\leftarrow}{f}(O) \cap \underset{\leftarrow}{f}(O') = \underset{\leftarrow}{f}(O \cap O')$, et pour toute famille $(O_i)_{i\in I}$ de parties de F, $\bigcup_{i\in I} \underset{\leftarrow}{f}(O_i) = \underset{\leftarrow}{f}\left(\bigcup_{i\in I} O_i\right)$. Et les fermés de E sont les images réciproques des fermés de F car pour toute partie O de F, $\complement_E \underset{\leftarrow}{f}(O) = \underset{\leftarrow}{f}(\complement_F O)$.

Nous verrons d'autres exemples de topologies dans les prochaines sections (notamment les cas des espaces métriques et des espaces vectoriels normés, qui sont les espaces topologiques usuels les plus simples), après avoir étudié un principe permettant de décrire de façon simple une topologie, à partir de ce qu'on appelle une base de topologie. Mais pour l'instant nous continuons l'étude des espaces topologiques avec une notion importante, celle de *voisinage* :

Définition 9.1.14 (Voisinage)
On considère un espace topologique $(E, \mathcal{T})$ et $x \in E$. On appelle *voisinage* de x toute partie V de E dans laquelle est inclus un ouvert contenant x, autrement dit telle qu'il existe un ouvert O tel que $x \in O \subseteq V$.

Remarque 9.1.15 : Si A est une partie de E incluant un voisinage de x, alors A est aussi un voisinage de x.

Ces pages ne sont pas incluses dans l’aperçu.

9.4 Espaces métriques et espaces vectoriels normés

Un autre cas particulier très important d'espace topologique est celui des *espaces métriques*[1], qui sont des ensembles sur lesquels on peut définir une notion de distance (à partir de laquelle on pourra construire une topologie). Et parmi les espaces métriques on distingue aussi le cas des *espaces vectoriels normés*, qui sont des $\mathbb{R}$-espaces vectoriels ou des $\mathbb{C}$-espaces vectoriels sur lesquels on peut définir une notion de « taille » des vecteurs, qu'on appelle une *norme*, et qui induit une distance. Dans la suite de ce chapitre, $\mathbb{K}$ désignera soit le corps $\mathbb{R}$, soit le corps $\mathbb{C}$. Dans ce cadre, la notation $|x|$ pourra représenter soit la valeur absolue (si $x \in \mathbb{R}$), soit le module (si $x \in \mathbb{C}$), et je pourrai la désigner dans les deux cas par l'expression *module* (puisque de toute façon, la valeur absolue du réel x est égale au module du complexe x).

Définition 9.4.1 (Distance, espace métrique)
On appelle *distance*, sur un ensemble E, toute fonction $E \times E \xrightarrow{d} \mathbb{R}_+$ vérifiant les trois propriétés suivantes :

1. Symétrie : pour tout $x\ y \in E$
$$d(x,y) = d(y,x)$$
2. Séparation : pour tout $x\ y \in E$
$$d(x,y) = 0 \iff x = y$$
3. Inégalité triangulaire : pour tout $x\ y\ z \in E$
$$d(x,z) \leqslant d(x,y) + d(y,z)$$

On appelle *espace métrique* tout ensemble muni d'une distance.

Remarque 9.4.2 : Une distance pourrait être définie, de manière équivalente, comme une fonction à valeurs dans $\mathbb{R}$, car les trois axiomes de la définition impliquent qu'elle est à valeurs positives : pour tout x et y dans E
$$0 = d(x,x) \leqslant d(x,y) + d(y,x) = 2d(x,y)$$

Remarque 9.4.3 : Si A est une partie d'un espace métrique (E,d), la restriction de d à $A\times A$ est une distance sur A, que l'on appelle *distance induite*.

Remarque 9.4.4 : Je noterai le plus souvent « d » une distance, je pourrai noter uniquement E pour désigner un espace métrique (E,d), et je pourrai aussi parfois utiliser le même symbole d pour noter des distances différentes (s'il n'y a pas d'ambiguïté). Par exemple, si $E \xrightarrow{f} F$ est une fonction entre deux espaces métriques, alors pour tout $x\ y \in E$, $d(x,y)$ représente la distance dans E entre x et y, et $d(f(x),f(y))$ représente la distance dans F entre $f(x)$ et $f(y)$. Ces deux symboles « d » ne représentent pas la même fonction, mais le contexte impose une interprétation.

Remarque 9.4.5 : L'inégalité triangulaire peut se généraliser à plus de 3 points. Par exemple, pour tout $x\ y\ z\ t \in E$
$$d(x,t) \leqslant d(x,y) + d(y,t) \leqslant d(x,y) + d(y,z) + d(z,t)$$
et par une récurrence immédiate, pour tous les points $x_1, \dots, x_n$ de E
$$d(x_1,x_n) \leqslant \sum_{i=1}^{n-1} d(x_i,x_{i+1})$$

1. La plupart des exemples usuels les plus simples sont de cette forme.

Remarque 9.4.6 : On déduit de la symétrie et de l'inégalité triangulaire ce qu'on appelle la *deuxième inégalité triangulaire* : pour tout $x\ y\ z \in E$

$$|d(z,x) - d(z,y)| \leqslant d(x,y)$$

En effet, d'après l'inégalité triangulaire

$$d(z,x) - d(z,y) \leqslant d(y,x) \qquad \text{et} \qquad d(z,y) - d(z,x) \leqslant d(x,y) = d(y,x)$$

donc

$$|d(z,x) - d(z,y)| = \max(d(z,x) - d(z,y), d(z,y) - d(z,x)) \leqslant d(x,y)$$

Définition 9.4.7 (Norme, espace vectoriel normé)

1. On appelle *norme* sur un $\mathbb{K}$-espace vectoriel E toute fonction $E \xrightarrow{N} \mathbb{R}_+$ vérifiant les propriétés suivantes :
   - Pour tout $x \in E$
   $$N(x) = 0 \iff x = 0$$
   - Pour tout $x \in E$ et tout $\lambda \in \mathbb{K}$
   $$N(\lambda x) = |\lambda| N(x)$$
   - Inégalité triangulaire : pour tout $x\ y \in E$
   $$N(x+y) \leqslant N(x) + N(y)$$

   On note souvent
   $$\|x\| \overset{\text{def}}{=} N(x)$$
2. On appelle *espace vectoriel normé* tout $\mathbb{K}$-espace vectoriel muni d'une norme.
3. On appelle *algèbre normée* toute $\mathbb{K}$-algèbre E munie d'une norme telle que pour tout $x\ y \in E$
   $$\|x \times y\| \leqslant \|x\| \|y\|$$

Remarque 9.4.8 : Je pourrai noter indifféremment N ou $\|\|$ une norme et, comme pour les distances, noter aussi de la même façon des normes d'espaces vectoriels normés différents.

Remarque 9.4.9 : On a notamment pour tout $x \in E$

$$\|-x\| = |-1| \|x\| = \|x\|$$

Remarque 9.4.10 : Dans une algèbre normée on a par récurrence, pour tout $n \geqslant 1$, $\|x^n\| \leqslant \|x\|^n$, puisque $\left\|x^1\right\| \leqslant \|x\|^1$, et si $\|x^n\| \leqslant \|x\|^n$ alors

$$\left\|x^{n+1}\right\| = \|x^n \times x\| \leqslant \|x^n\| \|x\| \leqslant \|x\|^n \|x\| = \|x\|^{n+1}$$

Remarque 9.4.11 : Si $x \neq 0$ alors $\dfrac{x}{\|x\|}$ est de norme 1, car

$$\left\|\frac{x}{\|x\|}\right\| = \left\|\frac{1}{\|x\|} x\right\| = \left|\frac{1}{\|x\|}\right| \|x\| = \frac{\|x\|}{\|x\|} = 1$$

Ces pages ne sont pas incluses dans l’aperçu.

9.8 Intérieur, adhérence

Pour toute partie A d'un espace topologique E :

- L'ensemble des ouverts inclus dans A est non vide (il contient $\varnothing$), et la réunion de tous ces ouverts, qui est la borne supérieure de cet ensemble (pour la relation d'inclusion), en est le plus grand élément (puisque les ouverts sont stables par réunion, cette réunion est un ouvert inclus dans A).
- De même, l'ensemble de tous les fermés incluant A est non vide (il contient E), et l'intersection de tous ces fermés, qui est la borne inférieure de cet ensemble (pour la relation d'inclusion), en est le plus petit élément (puisque les fermés sont stables par intersection, cette intersection est un fermé incluant A).

D'où les définitions suivantes :

Définition 9.8.1 (Intérieur, adhérence, frontière)
On considère une partie A d'un espace topologique.

1. On appelle *intérieur* de A, ce que l'on note $\mathring{A}$, l'union de tous les ouverts inclus dans A, autrement dit le plus grand ouvert inclus dans A. On dit qu'un point x est *intérieur* à A lorsque $x \in \mathring{A}$.
2. On appelle *adhérence* de A, ce que l'on note $\overline{A}$, l'intersection de tous les fermés incluant A, autrement dit le plus petit fermé incluant A. On dit qu'un point x est *adhérent* à A lorsque $x \in \overline{A}$.
3. On appelle *frontière* de A, ce que l'on note $\mathrm{Fr}(A)$, le complémentaire de l'intérieur de A dans son adhérence, autrement dit $\overline{A} \setminus \mathring{A}$.

Remarque 9.8.2 : Par définition, $\mathring{A}$ est un ouvert et $\overline{A}$ un fermé tels que $\mathring{A} \subseteq A \subseteq \overline{A}$. De plus A est un ouvert si et seulement si $A = \mathring{A}$ (si $A = \mathring{A}$ alors A est un ouvert, et si A est un ouvert alors c'est le plus grand ouvert inclus dans A), et A est un fermé si et seulement si $A = \overline{A}$ (si $A = \overline{A}$ alors A est un fermé, et si A est un fermé alors c'est le plus petit des fermés incluant A). On en déduit aussi que $\mathring{\mathring{A}} = \mathring{A}$ (car $\mathring{A}$ est un ouvert), et $\overline{\overline{A}} = \overline{A}$ (car $\overline{A}$ est un fermé).

Remarque 9.8.3 : $A = \mathrm{Fr}(A)$ si et seulement si A est un fermé d'intérieur vide : en effet, si A est un fermé d'intérieur vide, alors $A = \overline{A} \setminus \varnothing = \overline{A} \setminus \mathring{A}$, et réciproquement si $A = \overline{A} \setminus \mathring{A}$, alors pour tout $x \in A$ on a $x \notin \mathring{A}$, donc $\mathring{A} = \varnothing$ (car $\mathring{A} \subseteq A$), et par conséquent $A = \overline{A}$ donc A est fermé.

Remarque 9.8.4 : Les fonctions $X \longmapsto \mathring{X}$ et $X \longmapsto \overline{X}$ sont croissantes (pour l'inclusion), autrement dit si $A \subseteq B$ alors $\mathring{A} \subseteq \mathring{B}$ et $\overline{A} \subseteq \overline{B}$. En effet, si $A \subseteq B$ alors $\mathring{A} \subseteq A \subseteq B \subseteq \overline{B}$. On en déduit que $\mathring{A}$ est un ouvert inclus dans B donc $\mathring{A} \subseteq \mathring{B}$, et que $\overline{B}$ est un fermé incluant A donc $\overline{A} \subseteq \overline{B}$.

Théorème 9.8.5
Pour toute partie A d'un espace topologique

$$\complement\overline{A} = \overset{\circ}{\overline{\complement A}} \qquad \complement\mathring{A} = \overline{\complement A}$$

et

$$\mathrm{Fr}(A) = \overline{A} \cap \overline{\complement A} = \mathrm{Fr}(\complement A)$$

Preuve

- Puisque $\overline{A}$ est un fermé tel que $A \subseteq \overline{A}$, $\complement\overline{A}$ est un ouvert tel que $\complement\overline{A} \subseteq \complement A$, donc $\complement\overline{A} \subseteq \overset{\circ}{\overline{\complement A}}$. Réciproquement, puisque $\overset{\circ}{\overline{\complement A}}$

est un ouvert tel que $\overset{\circ}{\complement A} \subseteq \complement A$, $\complement\overset{\circ}{\complement A}$ est un fermé tel que $A \subseteq \complement\overset{\circ}{\complement A}$, et par conséquent $\overline{A} \subseteq \complement\overset{\circ}{\complement A}$, donc $\overset{\circ}{\complement A} \subseteq \complement\overline{A}$.

- En appliquant ce qui précède à $\complement A$, on obtient $\complement\overline{\complement A} = \overset{\circ}{\complement\complement A} = \mathring{A}$, donc $\complement\mathring{A} = \overline{\complement A}$.
- La frontière de A est l'ensemble des points qui sont à la fois adhérents à A et à son complémentaire, car

$$\mathrm{Fr}(A) = \overline{A} \setminus \mathring{A} = \overline{A} \cap \complement\mathring{A} = \overline{A} \cap \overline{\complement A} = \mathrm{Fr}(\complement A)$$

Exemple 9.8.6
Justifions que pour tout réel a

$$\overset{\circ}{]-\infty, a]} =]-\infty, a[\qquad \overset{\circ}{[a, +\infty[} =]a, +\infty[\qquad \overline{]-\infty, a[} =]-\infty, a] \qquad \overline{]a, +\infty[} = [a, +\infty[$$

- $]-\infty, a[$ est un ouvert inclus dans $]-\infty, a]$.
- Si O est un ouvert inclus dans $]-\infty, a]$ alors $a \notin O$, car sinon il existerait un réel $r > 0$ tel que $]a - r, a + r[\subseteq O$, d'où $O \cap]a, +\infty[\neq \emptyset$, en contradiction avec $O \subseteq]-\infty, a]$. Donc $O \subseteq]-\infty, a[$.

Par conséquent $\overset{\circ}{]-\infty, a]} =]-\infty, a[$. On en déduit

$$\overline{]a, +\infty[} = \overline{\complement]-\infty, a]} = \complement\overset{\circ}{]-\infty, a]} = \complement]-\infty, a[= [a, +\infty[$$

On justifie de même les deux autres égalités.

Théorème 9.8.7 (Caractérisation de l'intérieur et de l'adhérence par les voisinages)
On considère une partie A d'un espace topologique E, et $x \in E$.

1. $x \in \mathring{A}$ si et seulement si A est un voisinage de x, autrement dit si et seulement si il existe un ouvert O tel que $x \in O \subseteq A$.
2. $x \in \overline{A}$ si et seulement si les propriétés équivalentes suivantes sont vérifiées :
   - Pour tout voisinage V de x, $V \cap A \neq \emptyset$.
   - Pour tout voisinage V d'une base de voisinages de x, $V \cap A \neq \emptyset$.
   - Pour tout ouvert O contenant x, $O \cap A \neq \emptyset$.

Preuve
1. Si $x \in \mathring{A}$, alors $\mathring{A}$ est un ouvert tel que $x \in \mathring{A} \subseteq A$, ce qui signifie, par définition, que A est un voisinage de x. Réciproquement, s'il existe un ouvert O tel que $x \in O \subseteq A$, alors cet ouvert O est inclus dans $\mathring{A}$ par définition, donc $x \in \mathring{A}$.
2. Vérifions d'abord l'équivalence des trois propriétés :
   - Si pour tout voisinage V de x, $V \cap A \neq \emptyset$, c'est a fortiori le cas pour un voisinage d'une base de voisinages. Réciproquement, si cette propriété est vérifiée pour les voisinages d'une base de voisinages $\mathscr{V}$ de x, et si V est un voisinage quelconque de x, il existe $V' \in \mathscr{V}$ tel que $V' \subseteq V$. Et comme $V' \cap A \neq \emptyset$, on en déduit $V \cap A \neq \emptyset$.
   - Si pour tout voisinage V de x, $V \cap A \neq \emptyset$, alors comme tout ouvert O contenant x est un voisinage de x on a $O \cap A \neq \emptyset$, et réciproquement si pour tout ouvert O contenant x, $O \cap A \neq \emptyset$, alors pour tout voisinage V de x, il existe un ouvert O tel que $x \in O \subseteq V$, donc $\emptyset \neq O \cap A \subseteq V \cap A$.

   Enfin, $x \in \overline{A}$ si et seulement si $x \notin \complement\overline{A} = \overset{\circ}{\complement A}$, ce qui équivaut à dire, d'après le point précédent, que pour tout ouvert O contenant x, $O \not\subseteq \complement A$, autrement dit $O \cap A \neq \emptyset$ (car $O \subseteq \complement A \iff O \cap A = \emptyset$).

Ces pages ne sont pas incluses dans l’aperçu.

$\mathbb{Z}$ sont des parties non connexes de $\mathbb{R}$.

Théorème 9.19.4
Si A est une partie connexe d'un espace topologique E et B une partie de E telle que $A \subseteq B \subseteq \overline{A}$, alors B est connexe.

Preuve
On considère une partie C de B non vide qui est à la fois ouverte et fermée ; on veut prouver que $C = B$.

- Il existe un ouvert O et un fermé F de E tels que $C = O \cap B = F \cap B$. Comme $A \subseteq B$

$$C \cap A = O \cap A = F \cap A$$

  On en déduit que $C \cap A$ est un ouvert et un fermé de A, donc $C \cap A = \varnothing$ ou $C \cap A = A$.
- Par ailleurs, $O \cap \overline{A} \neq \varnothing$ car $C = O \cap B \subseteq O \cap \overline{A}$ et $C \neq \varnothing$. O étant un voisinage d'un point de $\overline{A}$, il rencontre A : on a $C \cap A = O \cap A \neq \varnothing$, donc $C \cap A = A$, et par conséquent $A \subseteq C$.

On en déduit $A \subseteq C \subseteq B \subseteq \overline{A}$, donc l'adhérence $\overline{C}$ de C dans E est telle que $\overline{C} = \overline{A}$. Et comme la partie C est fermée dans B, elle est égale à son adhérence dans B donc $C = \overline{C} \cap B = \overline{A} \cap B = B$.

En prenant pour B l'espace E, on obtient :

Théorème 9.19.5 (Corollaire)
Un espace topologique qui contient une partie connexe dense est connexe.

Théorème 9.19.6
Les parties connexes de $\mathbb{R}$ sont les intervalles.

Preuve

- Prouvons que toute partie connexe de $\mathbb{R}$ est un intervalle, ce qui équivaut, par contraposition, à prouver que si une partie A de $\mathbb{R}$ n'est pas un intervalle, alors A n'est pas connexe. A n'étant pas un intervalle, il existe x et y dans A tels que $[x, y] \not\subseteq A$ (car les intervalles sont les parties *convexes* de $\mathbb{R}$). Il existe donc un réel $z \notin A$ tel que $x < z < y$ ($z \neq x$ et $z \neq y$ car x et y sont des éléments de A). On en déduit que $]-\infty, z[$ et $]z, +\infty[$ sont deux ouverts disjoints qui rencontrent A, tels que $A \subseteq]-\infty, z[\cup]z, +\infty[$, et par conséquent A n'est pas connexe.
- Prouvons que tout intervalle ouvert de $\mathbb{R}$ est connexe. On considère un tel intervalle non vide (le cas vide étant trivial) $]a, b[$, avec $a < b$ et a et b dans $\overline{\mathbb{R}}$ (donc a peut être égal à $-\infty$ et b peut être égal à $+\infty$), et une partie A de cet intervalle qui est ouverte, fermée, et non vide. On veut démontrer que $]a, b[\subseteq A$ (d'où $A =]a, b[$). On considère $x \in A$ et

$$B \stackrel{\text{def}}{\equiv} \{y \in]a, b[\ ; \ y \geqslant x \text{ et } [x, y] \subseteq A\}$$

  Comme $B \neq \varnothing$ (car $x \in B$), cet ensemble admet une borne supérieure $c \in \mathbb{R} \cup \{+\infty\}$.
  — On fait l'hypothèse que $c < b$ (donc $c \in \mathbb{R}$). Comme c appartient à l'adhérence de B (dans $]a, b[$), incluse dans celle de A, et que A est un fermé dans $]a, b[$, on a $c \in A$. Et comme A est un ouvert de $]a, b[$, qui est ouvert dans $\mathbb{R}$, A est un ouvert de $\mathbb{R}$, donc il existe $\epsilon > 0$ tel que $]c - \epsilon, c + \epsilon[\subseteq A$. De plus il existe $z > c - \epsilon$ tel que $z \in B$ (car $c - \epsilon$ ne majore pas B), donc $z \geqslant x$ et $[x, z] \subseteq A$. On en déduit $[x, c + \epsilon[\subseteq A$, donc $[x, c + \epsilon] \subseteq A$ (car A est un fermé), et par conséquent $c + \epsilon \in B$, en contradiction avec le fait que c est un majorant de B.
  — Donc b est la borne supérieure de B, et par conséquent si $x \leqslant z < b$ alors il existe $y > z$ tel que $[x, y] \subseteq A$, donc $[x, b[\subseteq A$.
  — On démontre de la même manière que $]a, x] \subseteq A$, et on en déduit que $]a, b[\subseteq A$, donc $]a, b[$ est connexe.
- Prouvons enfin que tout intervalle I de $\mathbb{R}$ est connexe : $\mathring{I}$ est un intervalle ouvert, donc connexe d'après ce qui précède, tel que $\mathring{I} \subseteq I \subseteq \overline{I} = \overline{\mathring{I}}$. On déduit alors du théorème 9.19.4 que I est connexe.

Théorème 9.19.7
Si E est un connexe, F un espace topologique et $E \xrightarrow{f} F$ une fonction continue, alors $\mathrm{Im}(f)$ est connexe.

Preuve
Si deux ouverts U et V de F recouvrent $\mathrm{Im}(f)$ et sont tels que $(\mathrm{Im}(f) \cap U) \cap (\mathrm{Im}(f) \cap V) = \emptyset$, alors $\underset{\leftarrow}{f}(U)$ et $\underset{\leftarrow}{f}(V)$ sont des ouverts (car f est continue), disjoints (sinon $\mathrm{Im}(f) \cap U \cap V$ serait non vide), qui recouvrent E car

$$E = \underset{\leftarrow}{f}(\mathrm{Im}(f)) \subseteq \underset{\leftarrow}{f}(U \cup V) = \underset{\leftarrow}{f}(U) \cup \underset{\leftarrow}{f}(V)$$

Comme E est connexe, l'un des deux ouverts est vide, par exemple $\underset{\leftarrow}{f}(U)$, donc $\mathrm{Im}(f) \cap U = \emptyset$, et par conséquent $\mathrm{Im}(f)$ est connexe.

Remarque 9.19.8 : En particulier, un espace homéomorphe à un espace connexe est connexe.

Théorème 9.19.9 (Corollaire 1)
Si I est un intervalle de $\mathbb{R}$ et $I \xrightarrow{f} \mathbb{R}$ une fonction continue, alors $\mathrm{Im}(f)$ est un intervalle de $\mathbb{R}$.

Preuve
Un intervalle I de $\mathbb{R}$ est un connexe et par conséquent son image par f est un connexe de $\mathbb{R}$, donc un intervalle.

Théorème 9.19.10 (Corollaire 2 : théorème des valeurs intermédiaires)
On considère deux réels $a < b$ et une fonction continue $[a, b] \xrightarrow{f} \mathbb{R}$. Pour tout réel y compris entre $f(a)$ et $f(b)$, autrement dit tel que

$$\min(f(a), f(b)) \leqslant y \leqslant \max(f(a), f(b))$$

il existe $x \in [a, b]$ tel que $f(x) = y$.

Preuve 1 (corollaire du théorème précédent)
Notons $m \overset{\text{def}}{\equiv} \min(f(a), f(b))$ et $M \overset{\text{def}}{\equiv} \max(f(a), f(b))$. D'après le théorème précédent $\mathrm{Im}(f)$ est un intervalle, qui contient $f(a)$ et $f(b)$, donc $[m, M] \subseteq \mathrm{Im}(f)$, ce qui signifie que pour tout $y \in [m, M]$, il existe $x \in [a, b]$ tel que $f(x) = y$.

Preuve 2 (ne faisant pas appel au théorème précédent)
On considère par exemple $f(a) \leqslant y \leqslant f(b)$ (le raisonnement est semblable si $f(b) \leqslant f(a)$). Le résultat étant immédiat si $y = f(a)$ ou $y = f(b)$, on suppose dans la suite

$$f(a) < y < f(b)$$

On note

$$A \overset{\text{def}}{\equiv} \{x \in [a, b] \,;\; f(x) \leqslant y\}$$

Cet ensemble est non vide (car $a \in A$) et majoré (par b), donc il admet une borne supérieure c dans $\mathbb{R}$. Prouvons que c est un élément de $[a, b]$ tel que $f(c) = y$.

- Puisque c est la borne supérieure de A, il existe une suite $(u_n)_{n\in\mathbb{N}}$ d'éléments de A qui converge vers c. Puisque f est continue, $(f(u_n))_{n\in\mathbb{N}}$ converge vers $f(c)$, et comme on a pour tout entier n, $f(u_n) \leqslant y$, on en déduit $f(c) \leqslant y$.
- Par ailleurs $a \leqslant c$ (car $a \in A$), $c \leqslant b$ (car b majore A), et $c \neq b$ car $f(b) > y$ et $f(c) \leqslant y$, donc $c \in [a, b[$.
- Puisque c est la borne supérieure de A, il existe une suite $(v_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{R} \setminus A$ qui converge vers c ; et comme $c < b$, on peut prendre tous les termes de cette suite dans $]c, b[$ (voir le théorème 5.6.39, p. 157). Pour tout entier n, $v_n \in]c, b[\subseteq [a, b]$ et $v_n \notin A$, donc $f(v_n) > y$. Puisque f est continue, $f(v_n)$ converge vers $f(c)$, et par conséquent $f(c) \geqslant y$, donc $f(c) = y$.

Ces pages ne sont pas incluses dans l’aperçu.

Chapitre 10

Fonctions à valeurs réelles

Nous allons appliquer dans ce chapitre plusieurs notions vues dans le chapitre 9 (notamment celle de limite), au cas particulier de fonctions définies sur une partie de $\mathbb{R}$, généralement un intervalle (ou une réunion d'intervalles). Les intervalles de $\mathbb{R}$ sont en effet des parties ayant de « bonnes » propriétés d'un point de vue topologique : je rappelle que les intervalles sont les *convexes* et les *connexes* de $\mathbb{R}$, que les intervalles ouverts (ou les intervalles ouverts bornés, donc de la forme $]a, b[$) forment une base de la topologie, et que les intervalles fermés bornés, donc de la forme $[a, b]$, sont des compacts.

L'intervalle I de définition d'une fonction sera parfois supposé être d'intérieur non vide, ce qui équivaut à dire que I n'est ni vide, ni un singleton [1], de telle sorte que tout point a de I est alors un point d'accumulation, c'est-à-dire un point adhérent à $I \setminus \{a\}$ (voir l'exemple 9.8.28, p. 392). Cela permet de donner un sens à la limite en a de fonctions de domaine $I \setminus \{a\}$, nécessaire à la définition de la dérivabilité en a, point de départ de ce chapitre.

Je précise aussi que je ne traiterai pas toujours en détail les notions abordées dans ce chapitre et le suivant (suites et séries de fonctions) [2], certaines d'entre elles ne me servant pour l'instant qu'à disposer des outils nécessaires pour terminer l'étude du corps des nombres complexes (forme polaire, et théorème fondamental de l'algèbre). [3]

10.1 Dérivabilité

Définition 10.1.1 (Dérivabilité, nombre dérivé)
On considère un intervalle I de $\mathbb{R}$ d'intérieur non vide, un $\mathbb{K}$-espace vectoriel normé E, et une fonction $I \xrightarrow{f} E$. On dit que f est *dérivable* en un point a de I, lorsqu'il existe un élément b de E vérifiant les propriétés équivalentes suivantes :

- la fonction

$$\tau : \begin{cases} I \setminus \{a\} \longrightarrow E \\ x \longmapsto \dfrac{1}{x-a} \cdot (f(x) - f(a)) \end{cases}$$

  a pour limite b en a.

1. Il est à noter que si I est un intervalle ouvert et si $a \in I$, alors I est automatiquement d'intérieur non vide puisque $\mathring{I} = I$.
2. Ce seul volume n'est pas suffisant pour cela.
3. Cette remarque est d'ailleurs valable pour d'autres chapitres de cette série d'ouvrages, la nécessité de disposer de certains théorèmes pouvant m'amener à étudier partiellement certaines notions (mais qui seront complétées dans les volumes suivants).

- la fonction

$$\rho : \begin{cases} J \longrightarrow E \\ h \longmapsto \dfrac{1}{h} \cdot (f(h+a) - f(a)) \end{cases}$$

a pour limite b en 0, où J est l'image directe de $I \setminus \{a\}$ par la translation additive

$$t_{-a} : \begin{cases} \mathbb{R} \longrightarrow \mathbb{R} \\ x \longmapsto x - a \end{cases}$$

- il existe une fonction $I \xrightarrow{\varphi} E$ continue en a, telle que $\varphi(a) = 0$ et

$$f(x) = f(a) + (x-a) \cdot b + (x-a) \cdot \varphi(x)$$

On dit alors que b est le *nombre dérivé* de f en a, et on le note

$$f'(a) \qquad \text{ou} \qquad \frac{\mathrm{d}f}{\mathrm{d}x}(a)$$

On dit que f est *dérivable* lorsqu'elle est dérivable en tout point de I, et on appelle fonction *dérivée* la fonction

$$f' : \begin{cases} I \longrightarrow E \\ a \longmapsto f'(a) \end{cases}$$

Preuve

- Vérifions d'abord l'équivalence des deux premières propriétés, qui est une conséquence du fait que les translations additives sont des homéomorphismes, et du théorème de composition des limites. On a $\tau = \rho \circ t_{-a}$ et $\rho = \tau \circ t_a$, donc si τ a pour limite b en a alors, comme t_a a pour limite a en 0, ρ a pour limite b en 0. De même, si ρ a pour limite b en 0 alors, comme t_{-a} a pour limite 0 en a, τ a pour limite b en a.
- On fait l'hypothèse que $\lim\limits_{x \longrightarrow a} \tau(x) = b$, et on note

$$\varphi : \begin{cases} I \longrightarrow E \\ x \longmapsto \begin{cases} \dfrac{1}{x-a} \cdot (f(x) - f(a)) - b = \tau(x) - b & \text{si } x \neq a \\ 0 & \text{si } x = a \end{cases} \end{cases}$$

Pour tout $x \neq a$

$$(x-a) \cdot \varphi(x) = f(x) - f(a) - (x-a) \cdot b$$

donc

$$f(x) = f(a) + (x-a) \cdot b + (x-a) \cdot \varphi(x)$$

et cette égalité reste vraie si $x = a$. De plus, la fonction φ est telle que $\varphi(a) = 0$, et comme par hypothèse $\lim\limits_{x \longrightarrow a} \tau(x) = b$, on en déduit $\lim\limits_{x \longrightarrow a, x \neq a} \varphi(x) = b - b = 0 = \varphi(a)$, donc φ est continue en a.

- Réciproquement, on fait l'hypothèse qu'il existe une fonction $I \xrightarrow{\varphi} E$ vérifiant les conditions de l'énoncé. Pour tout $x \in I$

$$f(x) - f(a) = (x-a) \cdot b + (x-a) \cdot \varphi(x)$$

donc la fonction

$$\tau : \begin{cases} I \setminus \{a\} \longrightarrow E \\ x \longmapsto \dfrac{1}{x-a} \cdot (f(x) - f(a)) \end{cases}$$

est telle que pour tout $x \neq a$, $\tau(x) = b + \varphi(x)$ donc $\lim\limits_{x \longrightarrow a} \tau(x) = b + 0 = b$ (car $\lim\limits_{x \longrightarrow a} \varphi(x) = \varphi(a) = 0$ puisque φ est continue en a).

Remarque 10.1.2 : Quand E est l'espace vectoriel normé $\mathbb{R}$, la multiplication scalaire est la multiplication dans $\mathbb{R}$, donc dans ce cas, pour tout $x \neq a$

$$\tau(x) = \frac{f(x) - f(a)}{x - a}$$

Si V est un voisinage de a dans $\mathbb{R}$, alors f a pour dérivée b en a si et seulement si $f|_{I \cap V}$ a pour dérivée b en a, car $(I \cap V) \setminus \{a\} = (I \setminus \{a\}) \cap V$, et

$$\lim_{x \longrightarrow a} \tau(x) = b \quad \Longleftrightarrow \quad \lim_{x \longrightarrow a} \tau|_{(I \setminus \{a\}) \cap V}(x) = b$$

En particulier, si J est un intervalle ouvert tel que $a \in J \subseteq I$, alors f est dérivable en a si et seulement si $f|_J$ est dérivable en a, et alors $f'(a) = f|'_J(a)$. Cela permet de justifier la définition suivante :

Définition 10.1.3
On considère un ouvert O de $\mathbb{R}$, un $\mathbb{K}$-espace vectoriel normé E, et une fonction $O \xrightarrow{f} E$.

1. Pour tout $a \in O$, on dit que f est *dérivable en a* lorsque pour tout intervalle ouvert I tel que $a \in I \subseteq O$, $f|_I$ est dérivable en a. On note alors $f'(a) \overset{\text{def}}{\equiv} f|'_I(a)$.
2. On dit que f est *dérivable* lorsqu'elle est dérivable en tout point de O, et on appelle fonction *dérivée* la fonction
$$f' : \begin{cases} O \longrightarrow E \\ a \longmapsto f'(a) \end{cases}$$

Remarque 10.1.4 : La dérivabilité de f en a et le nombre dérivé ne dépendent pas de l'intervalle I : si I et J sont deux intervalles ouverts tels que $a \in I \subseteq O$ et $a \in J \subseteq O$, alors $I \cap J$ est un intervalle ouvert tel que $a \in I \cap J \subseteq O$, et il y a équivalence entre la dérivabilité en a de $f|_{I \cap J}$, celle de $f|_I$, et celle de $f|_J$.

Théorème 10.1.5
Si une fonction est dérivable (respectivement dérivable en a), alors elle est continue (respectivement continue en a).

Preuve
C'est une conséquence de la troisième caractérisation de la définition de la dérivabilité, puisqu'une fonction dérivable en un point a est la somme de fonctions continues en a, donc est continue en a.

La réciproque de ce théorème est fausse : une fonction peut être continue sans être dérivable (voir exemple ci-dessous).

Exemple 10.1.6
1. Si f est une fonction constante, le nombre dérivé en tout point a est égal à 0, puisque pour tout

$x \neq a$

$$\frac{1}{x-a} \cdot (f(x) - f(a)) = 0$$

2. Si f est l'injection canonique de I dans $\mathbb{R}$ (c'est-à-dire $f(x) = x$ pour tout $x \in I$), alors le nombre dérivé en tout point est égal à 1 puisque pour tout $x \neq a$

$$\frac{f(x) - f(a)}{x-a} = \frac{x-a}{x-a} = 1$$

3. De même la fonction $x \longmapsto -x$, de I dans $\mathbb{R}$, a pour nombre dérivé en tout point -1, car

$$\frac{-x-(-a)}{x-a} = -1$$

4. La fonction valeur absolue

$$f : \begin{cases} \mathbb{R} \longrightarrow \mathbb{R} \\ x \longmapsto |x| \end{cases}$$

- est dérivable en tout point $a \neq 0$, car on peut trouver un intervalle ouvert I tel que $a \in I$ et tel que $f|_I$ est soit la fonction $x \longmapsto x$ (quand $a > 0$), soit la fonction $x \longmapsto -x$ (quand $x < 0$), qui sont dérivables ;
- est continue en 0, mais n'est pas dérivable en 0 : pour tout $x \neq 0$

$$\tau(x) = \frac{f(x) - f(0)}{x-0} = \frac{|x|}{x} = \begin{cases} 1 \text{ si } x > 0 \\ -1 \text{ si } x < 0 \end{cases}$$

f ne peut pas avoir de dérivée en 0, car l'image directe par τ d'un voisinage de 0 contient -1 et 1, et pour tout réel b on peut toujours trouver un intervalle ouvert contenant b, mais ne contenant pas 1, ou ne contenant pas -1.

5. La fonction

$$f : \begin{cases} \mathbb{R}_+ \longrightarrow \mathbb{R} \\ x \longmapsto \sqrt{x} \end{cases}$$

n'est pas dérivable en 0, car pour tout $x > 0$

$$\frac{f(x) - f(0)}{x-0} = \frac{\sqrt{x}}{x} = \frac{1}{\sqrt{x}}$$

qui n'a pas de limite quand x tend vers 0. Et cette fonction est dérivable en tout point $a > 0$, car

$$\frac{\sqrt{x} - \sqrt{a}}{x-a} = \frac{(\sqrt{x} - \sqrt{a})(\sqrt{x} + \sqrt{a})}{(x-a)(\sqrt{x} + \sqrt{a})} = \frac{x-a}{(x-a)(\sqrt{x} + \sqrt{a})} = \frac{1}{\sqrt{x} + \sqrt{a}}$$

qui a pour limite $\dfrac{1}{2\sqrt{a}}$ quand x tend vers a.

Ces pages ne sont pas incluses dans l’aperçu.

Chapitre 11

Séries

11.1 Séries à valeurs dans un espace vectoriel normé

Prérequis
La manipulation des sommes finies (section 4.8 du volume 2).

Définition 11.1.1 (Série, somme partielle)
On considère une suite $(u_n)_{n\in\mathbb{N}}$ d'un espace vectoriel. On appelle *série* de terme général u_n la suite $(U_n)_{n\in\mathbb{N}}$ définie pour tout entier n par

$$U_n \overset{\text{def}}{\equiv} \sum_{k=0}^{n} u_k \overset{\text{def}}{\equiv} u_0 + u_1 + \cdots + u_n$$

On la note

$$\left(\sum u_n\right)_{n\in\mathbb{N}} \quad \text{ou} \quad \sum_{n\geqslant 0} u_n \quad \text{ou} \quad \sum u_n$$

De plus, U_n s'appelle la *somme partielle* d'ordre n (ou de rang n) de la série.

Remarque 11.1.2 (Notations) : Comme je l'ai fait ici, je noterai généralement une somme partielle avec la lettre majuscule correspondant à la notation du terme général : par exemple A_n pour la somme partielle d'ordre n de la série de terme général $(a_n)_{n\in\mathbb{N}}$, etc. Ce n'est pas une norme, mais un usage courant. Une autre notation usuelle pour la somme partielle est d'utiliser la lettre S (comme *somme*).

Définition 11.1.3 (Somme d'une série)
On considère une suite $(u_n)_{n\in\mathbb{N}}$ d'un espace vectoriel normé.

1. On dit que la série $\displaystyle\sum_{n\geqslant 0} u_n$ *converge* lorsque la suite des sommes partielles, autrement dit la suite $\left(\displaystyle\sum_{k=0}^{n} u_k\right)_{n\in\mathbb{N}}$, converge.

2. On appelle *somme* d'une série convergente $\sum_{n\geqslant 0} u_n$, ce que l'on note $\sum_{k=0}^{+\infty} u_k$, la limite de la suite des sommes partielles, autrement dit

$$\sum_{k=0}^{+\infty} u_k = \lim_{n\longrightarrow+\infty} U_n = \lim_{n\longrightarrow+\infty} \sum_{k=0}^{n} u_k = \lim_{n\longrightarrow+\infty} (u_0 + u_1 + \cdots + u_n)$$

Remarque 11.1.4 : Dans le cas d'une suite $(u_n)_{n\geqslant p}$, la somme partielle U_n est définie, pour tout $n \geqslant p$, par

$$U_n \overset{\text{def}}{\equiv} \sum_{k=p}^{n} u_k \overset{\text{def}}{\equiv} u_p + u_{p+1} + \cdots + u_n$$

On note alors $\sum_{n\geqslant p} u_n$ une telle série, et $\sum_{n=p}^{+\infty} u_n$ sa somme (quand elle converge).

Le terme général u_n d'une série et la somme partielle U_n sont telles que $u_0 = U_0$, et pour tout entier n

$$u_{n+1} = U_{n+1} - U_n$$

On en déduit une condition nécessaire simple de convergence d'une série :

Théorème 11.1.5
Si la série $\sum_{n\geqslant 0} u_n$ converge, alors la suite $(u_n)_{n\in\mathbb{N}}$ converge vers 0 (donc par contraposition, si la suite $(u_n)_{n\in\mathbb{N}}$ ne converge pas vers 0, alors la série $\sum_{n\geqslant 0} u_n$ diverge).

Preuve
Si la série $\sum_{n\geqslant 0} u_n$ converge, alors les suites $(U_n)_{n\in\mathbb{N}}$ et $(U_{n+1})_{n\in\mathbb{N}}$ convergent vers la même limite, donc la suite $(u_n)_{n\in\mathbb{N}}$ converge vers 0, puisque pour tout entier n, $u_{n+1} = U_{n+1} - U_n$.

Exemple 11.1.6
1. Pour tout $a \in \mathbb{R}$ tel que $|a| < 1$, la série $\sum_{n\geqslant 0} a^n$ converge, et

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

(exemple 5.6.22, p. 153).
2. Pour tout $a \in \mathbb{R}$ tel que $|a| \geqslant 1$, la série $\sum_{n\geqslant 0} a^n$ diverge, car la suite $(a^n)_{n\in\mathbb{N}}$ ne converge pas vers 0.

Ces pages ne sont pas incluses dans l’aperçu.

Théorème 11.5.6 (Corollaire 1)
Pour tout élément a d'une algèbre de Banach, $\exp(a)$ est inversible, et

$$(\exp(a))^{-1} = \exp(-a)$$

Preuve
Puisque a et $-a$ commutent, on déduit du théorème précédent

$$\exp(a) \times \exp(-a) = \exp(-a) \times \exp(a) = \exp(a - a) = \exp(0) = 1$$

Remarque 11.5.7 : On notera en particulier que $\exp(a)$ n'est jamais nul.

Théorème 11.5.8 (Corollaire 2)
Dans une algèbre de Banach commutative E, la fonction exponentielle est un morphisme de groupes de $(E, +)$ dans $(E^\times, \times)$ (c'est-à-dire du groupe additif dans le groupe multiplicatif des éléments inversibles de l'anneau E).

Preuve
C'est une conséquence immédiate des deux théorèmes précédents, puisque la fonction exponentielle est à valeurs dans le groupe des éléments inversibles de E, et que c'est un morphisme (de $+$ vers $\times$).

Théorème 11.5.9 (Corollaire 3)
Pour tout élément a d'une algèbre de Banach et tout entier relatif n

$$\exp(na) = (\exp(a))^n$$

Preuve
Le cas où n est un entier naturel se démontre par récurrence : $\exp(0) = 1 = (\exp(a))^0$, et si $\exp(na) = (\exp(a))^n$, alors

$$\exp(na + a) = \exp(na) \times \exp(a) = (\exp(a))^n \times \exp(a) = (\exp(a))^{n+1}$$

(car a et na commutent). Et si $n < 0$ alors $-n \in \mathbb{N}$ donc $\exp(-na) = (\exp(a))^{-n}$, et par conséquent

$$\exp(na) = (\exp(-na))^{-1} = (\exp(a)^{-n})^{-1} = \exp(a)^n$$

Les propriétés que l'on vient de voir rappelant celles des puissances, on utilise aussi la notation suivante pour la fonction exponentielle :

Définition 11.5.10 (Notation de la fonction exponentielle)
Pour tout élément a d'une algèbre de Banach, on note

$$\mathrm{e}^a \stackrel{\text{def}}{=\!=} \exp(a)$$

Remarque 11.5.11 : On a donc

- $\mathrm{e}^0 = 1$;
- pour tout a, e^a est non nul, inversible tel que $(\mathrm{e}^a)^{-1} = \mathrm{e}^{-a}$, et pour tout entier relatif n, $\mathrm{e}^{na} = (\mathrm{e}^a)^n$;

- pour tout a et b qui commutent, $\mathrm{e}^{a+b} = \mathrm{e}^a \times \mathrm{e}^b = \mathrm{e}^b \times \mathrm{e}^a$.

11.6 Exponentielle complexe, exponentielle réelle

Prérequis
Les nombres complexes (section 5.13).

Voyons quelques propriétés de l'exponentielle complexe et de l'exponentielle réelle, qui seront utilisées dans le prochain chapitre.

Théorème 11.6.1
Pour tout $x \in \mathbb{C}$

$$\overline{\mathrm{e}^x} = \mathrm{e}^{\overline{x}}$$

Preuve
On a

$$\overline{\mathrm{e}^x} = \overline{\sum_{n=0}^{+\infty} \frac{x^n}{n!}} = \overline{\lim_{n\longrightarrow+\infty} \sum_{k=0}^{n} \frac{x^k}{k!}} = \lim_{n\longrightarrow+\infty} \overline{\sum_{k=0}^{n} \frac{x^k}{k!}} = \lim_{n\longrightarrow+\infty} \sum_{k=0}^{n} \frac{\overline{x}^k}{k!} = \sum_{n=0}^{+\infty} \frac{\overline{x}^n}{n!} = \mathrm{e}^{\overline{x}}$$

($\overline{\lim_{n\longrightarrow+\infty} \sum_{k=0}^{n} \frac{x^k}{k!}} = \lim_{n\longrightarrow+\infty} \overline{\sum_{k=0}^{n} \frac{x^k}{k!}}$ car la fonction $x \longmapsto \overline{x}$ est continue).

Remarque 11.6.2 : En particulier, pour tout $x \in \mathbb{R}$, $\overline{\mathrm{e}^{\mathrm{i}x}} = \mathrm{e}^{-\mathrm{i}x}$.

Théorème 11.6.3
Pour tout $k \in \mathbb{C}$, la fonction

$$f : \begin{cases} \mathbb{R} \longrightarrow \mathbb{C} \\ x \longmapsto \mathrm{e}^{kx} \end{cases}$$

est dérivable, et pour tout $x \in \mathbb{R}$

$$f'(x) = kf(x) = k\mathrm{e}^{kx}$$

Preuve
Si $k = 0$ alors le résultat est immédiat puisque la fonction f est alors constante et sa dérivée nulle. On suppose dans la suite que $k \neq 0$. On considère $a \in \mathbb{R}$, et on veut démontrer que la limite de

$$\frac{f(x+a) - f(a)}{x} - kf(a) = \frac{f(x+a) - f(a) - kxf(a)}{x}$$

quand x tend vers 0 ($x \neq 0$), est égale à 0. On a

$$\begin{cases} f(x+a) = 1 + kx + ka + \sum_{n=2}^{+\infty} \frac{(kx+ka)^n}{n!} \\ f(a) = 1 + ka + \sum_{n=2}^{+\infty} \frac{(ka)^n}{n!} \\ kxf(a) = kx + \sum_{n=1}^{+\infty} kx\frac{(ka)^n}{n!} = kx + \sum_{n=2}^{+\infty} kx\frac{(ka)^{n-1}}{(n-1)!} = kx + \sum_{n=2}^{+\infty} \frac{nkx(ka)^{n-1}}{n!} \end{cases}$$

Ces pages ne sont pas incluses dans l’aperçu.

Chapitre 12

Compléments sur les corps $\mathbb{R}$ et $\mathbb{C}$

Prérequis
Les nombres complexes (section 5.13), les séries (chapitre 11) et notamment la fonction exponentielle (sections 11.5 et 11.6).

12.1 Fonctions trigonométriques

Définition 12.1.1 (Cosinus et sinus)
1. Pour tout $x \in \mathbb{C}$, on note

$$\cos(x) \stackrel{\text{def}}{=} \frac{e^{ix} + e^{-ix}}{2} \qquad \text{et} \qquad \sin(x) \stackrel{\text{def}}{=} \frac{e^{ix} - e^{-ix}}{2i}$$

2. On appelle respectivement fonction *cosinus* et fonction *sinus* les fonctions

$$\cos : \begin{cases} \mathbb{C} \longrightarrow \mathbb{C} \\ x \longmapsto \cos(x) \end{cases} \qquad \text{et} \qquad \sin : \begin{cases} \mathbb{C} \longrightarrow \mathbb{C} \\ x \longmapsto \sin(x) \end{cases}$$

3. Pour tout entier non nul n, on note

$$\cos^n(x) \stackrel{\text{def}}{=} (\cos(x))^n \qquad \text{et} \qquad \sin^n(x) \stackrel{\text{def}}{=} (\sin(x))^n$$

Remarque 12.1.2 (Notations) : On note aussi les fonctions cosinus et sinus sans les parenthèses autour de la variable :

$$\cos x \stackrel{\text{def}}{=} \cos(x) \qquad \sin x \stackrel{\text{def}}{=} \sin(x) \qquad \cos^n x \stackrel{\text{def}}{=} \cos^n(x) \qquad \sin^n x \stackrel{\text{def}}{=} \sin^n(x)$$

Remarque 12.1.3 : On a en particulier

$$\cos 0 = \frac{e^0 + e^0}{2} = 1 \qquad \text{et} \qquad \sin 0 = \frac{e^0 - e^0}{2i} = 0$$

De plus, la fonction cosinus est paire, car pour tout $x \in \mathbb{C}$

$$\cos(-x) = \frac{e^{-ix} + e^{ix}}{2} = \cos x$$

et la fonction sinus est impaire, car pour tout $x \in \mathbb{C}$

$$\sin(-x) = \frac{e^{-ix} - e^{ix}}{2i} = -\sin x$$

Théorème 12.1.4

1. Pour tout $x \in \mathbb{C}$
   - On a
   $$\cos^2 x + \sin^2 x = 1$$
   - Formule d'Euler :
   $$e^{ix} = \cos x + i \sin x$$
   - Formule de Moivre : pour tout $n \in \mathbb{Z}$
   $$(\cos x + i \sin x)^n = \cos(nx) + i \sin(nx)$$
2. Si $x \in \mathbb{R}$ alors l'expression de e^{ix} ci-dessus représente sa forme algébrique, autrement dit
   $$\cos x = \mathfrak{R}(e^{ix}) \in \mathbb{R} \qquad \text{et} \qquad \sin x = \mathfrak{I}(e^{ix}) \in \mathbb{R}$$
   De plus
   $$\cos x \in [-1, 1] \qquad \sin x \in [-1, 1] \qquad \left|e^{ix}\right| = 1$$
   Les fonctions complexes cos et sin induisent donc les deux fonctions réelles
   $$\mathbb{R} \xrightarrow{\cos} [-1, 1] \qquad \text{et} \qquad \mathbb{R} \xrightarrow{\sin} [-1, 1]$$

Preuve

1. On a
   $$\cos x + i \sin x = \frac{e^{ix} + e^{-ix}}{2} + i\frac{e^{ix} - e^{-ix}}{2i} = \frac{2e^{ix}}{2} = e^{ix}$$
   On en déduit que pour tout $n \in \mathbb{Z}$
   $$(\cos x + i \sin x)^n = (e^{ix})^n = e^{nix} = \cos(nx) + i \sin(nx)$$
   De plus, $(e^{ix})^2 = e^{2ix}$, $(e^{-ix})^2 = e^{-2ix}$, et $e^{ix}e^{-ix} = e^{ix-ix} = e^0 = 1$, donc
   $$\cos^2 x + \sin^2 x = \left(\frac{e^{ix} + e^{-ix}}{2}\right)^2 + \left(\frac{e^{ix} - e^{-ix}}{2i}\right)^2 = \frac{e^{2ix} + e^{-2ix} + 2}{4} + \frac{e^{2ix} + e^{-2ix} - 2}{-4} = \frac{e^{2ix} + e^{-2ix} + 2 - e^{2ix} - e^{-2ix} + 2}{4} = 1$$
2. Si $x \in \mathbb{R}$ alors
   $$\begin{cases} \cos x = \dfrac{e^{ix} + e^{-ix}}{2} = \dfrac{e^{ix} + \overline{e^{ix}}}{2} = \mathfrak{R}(e^{ix}) \in \mathbb{R} \\ \sin x = \dfrac{e^{ix} - e^{-ix}}{2i} = \dfrac{e^{ix} - \overline{e^{ix}}}{2i} = \mathfrak{I}(e^{ix}) \in \mathbb{R} \end{cases}$$
   On en déduit $\left|e^{ix}\right|^2 = \cos^2 x + \sin^2 x = 1$ donc $\left|e^{ix}\right| = 1$; on pouvait aussi calculer directement
   $$\left|e^{ix}\right|^2 = e^{ix}\overline{e^{ix}} = e^{ix}e^{-ix} = e^{ix-ix} = e^0 = 1$$
   On déduit aussi de la formule
   $$\cos^2 x + \sin^2 x = 1$$
   que $\cos^2 x \leqslant 1$ et $\sin^2 x \leqslant 1$, donc $\cos x \in [-1, 1]$ et $\sin x \in [-1, 1]$.

Ces pages ne sont pas incluses dans l’aperçu.

Chapitre 13

Arithmétique des anneaux

Prérequis
La divisibilité dans les anneaux (notamment la section 2.4 du volume 3), les idéaux et anneaux quotients (sections 2.9 du volume 2 et 4.2 du volume 3), et les polynômes (chapitre 7).

Nous allons voir quelques propriétés arithmétiques des anneaux, en rapport avec la notion de divisibilité, qui généralisent des propriétés de $\mathbb{Z}$ (nombres premiers, PGCD et PPCM…). Dans tout ce chapitre, $\mathbb{A}$ représente un anneau commutatif, $\mathbb{A}^\times$ l'ensemble de ses éléments inversibles, et $\mathbb{K}$ un corps.

Quelques petites remarques avant de commencer : je rappelle que deux éléments a et b d'un anneau sont dits *associés* lorsque a divise b et b divise a (ce qui équivaut à dire que a et b ont les mêmes diviseurs et les mêmes multiples), et que dans un anneau intègre cela équivaut aussi à dire que chacun de ces deux éléments est le produit de l'autre par un élément inversible. Par ailleurs, la relation « a et b sont associés » est une relation d'équivalence (que l'on soit dans un anneau intègre ou pas).

1 divise tout élément a de $\mathbb{A}$ (puisque $a = a \cdot 1$) et a divise 1 si et seulement si a est inversible, car par définition ces deux notions signifient qu'il existe $b \in \mathbb{A}$ tel que $a \cdot b = 1$. Cette propriété s'étend aussi aux éléments inversibles autres que 1, c'est-à-dire que si u est inversible, alors u divise tout élément a (car $a = u \cdot (u^{-1} \cdot a)$), et a divise u si et seulement si a est inversible : en effet si a est inversible alors a divise u d'après ce qui précède, et si a divise u alors il existe b tel que $u = ab$ donc $1 = uu^{-1} = a(bu^{-1})$, ce qui signifie que a est inversible. Par conséquent les éléments inversibles sont dans une même classe d'équivalence (si u est inversible, alors a et u sont associés si et seulement si a est inversible).

Enfin, les propriétés arithmétiques étudiées dans ce chapitre seront souvent liées à la notion d'idéal. Je rappelle qu'un idéal de $\mathbb{A}$ est un sous-groupe additif I stable par multiplication par un élément quelconque de $\mathbb{A}$ (autrement dit si $a \in \mathbb{A}$ et $x \in I$ alors $ax \in I$). Un sous-groupe additif est un sous-ensemble non vide stable pour l'addition et l'opposé, mais comme la stabilité pour la multiplication implique la stabilité pour l'opposé (car $-x = (-1) \times x$), on en déduit qu'un sous-ensemble non vide I de $\mathbb{A}$ est un idéal si et seulement si pour tout $x\ y \in I$, $x + y \in I$, et pour tout $a \in \mathbb{A}$ et tout $x \in I$, $ax \in I$.

13.1 Compléments sur les idéaux

Nous avons vu dans le volume 2 que les seuls idéaux d'un corps $\mathbb{K}$ sont $\{0\}$ et $\mathbb{K}$ (car un idéal qui contient un élément non nul, donc inversible, contient aussi 1 donc est égal à $\mathbb{K}$). La réciproque est vraie, ce qui donne le théorème suivant :

Théorème 13.1.1
Si $\mathbb{A}$ est non trivial, alors $\mathbb{A}$ est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et $\mathbb{A}$.

Preuve
Si $\mathbb{A}$ est un corps, alors ses seuls idéaux sont $\{0\}$ et $\mathbb{A}$. Réciproquement, on fait l'hypothèse que les seuls idéaux de $\mathbb{A}$ sont $\{0\}$ et $\mathbb{A}$, et on considère un élément non nul a de $\mathbb{A}$, et l'idéal engendré par a, c'est-à-dire $a\mathbb{A}$. Puisque $a \neq 0$ et $a \in a\mathbb{A}$, $a\mathbb{A} \neq \{0\}$ donc $a\mathbb{A} = \mathbb{A}$. On en déduit $1 \in a\mathbb{A}$, donc il existe $b \in \mathbb{A}$ tel que $ab = 1$, ce qui signifie que a est inversible, et par conséquent $\mathbb{A}$ est un corps (puisque $\mathbb{A}$ est aussi commutatif et non trivial par hypothèse).

Remarque 13.1.2 : Nous avons aussi vu dans le volume 2 que le fait qu'il n'y a que deux idéaux dans un corps a la conséquence suivante : tout morphisme de corps est injectif. Je redonne l'argument ici, dans un cadre un tout petit peu plus général : si $\mathbb{A}$ est un anneau non trivial et si $\mathbb{K} \xrightarrow{f} \mathbb{A}$ est un morphisme d'anneaux, alors f est injectif (et par conséquent $\mathrm{Im}(f)$ est un sous-anneau de $\mathbb{A}$ qui est un corps isomorphe à $\mathbb{K}$). En effet le noyau de f est un idéal de $\mathbb{K}$, qui ne peut pas être $\mathbb{K}$ lui-même car 1 n'est pas dans le noyau ($f(1) = 1 \neq 0$), donc $\ker(f) = \{0\}$ et par conséquent f est injective.

Théorème 13.1.3
On considère un idéal I de $\mathbb{A}$, et $x \in \mathbb{A}$. Alors les trois propriétés suivantes sont équivalentes :

$$[x] \text{ est inversible dans } \mathbb{A}/I \qquad x\mathbb{A} + I = \mathbb{A} \qquad 1 \in x\mathbb{A} + I$$

Preuve
Notons d'abord que $x\mathbb{A} + I$ est un idéal (c'est l'idéal engendré par $\{x\} \cup I$). Par conséquent

$$x\mathbb{A} + I = \mathbb{A} \iff 1 \in x\mathbb{A} + I$$

$[x]$ est inversible si et seulement si il existe $y \in \mathbb{A}$ tel que $[xy] = [x][y] = [1]$, ce qui équivaut à : il existe $i \in I$ tel que $1 = xy + i$. Donc $[x]$ est inversible si et seulement si il existe $y \in \mathbb{A}$ et $i \in I$ tels que $1 = xy + i$, autrement dit $[x]$ est inversible si et seulement si $1 \in x\mathbb{A} + I$.

Théorème 13.1.4
On considère un idéal I de $\mathbb{A}$, et la projection canonique $\mathbb{A} \xrightarrow{\mathrm{pr}} \mathbb{A}/I$. Alors $\underset{\rightarrow}{\mathrm{pr}}$ induit une bijection entre les idéaux de $\mathbb{A}$ incluant I et les idéaux de $\mathbb{A}/I$, dont la bijection réciproque est induite par $\underset{\leftarrow}{\mathrm{pr}}$.

Preuve
Notons

$$\begin{cases} \mathcal{I}_{\mathbb{A}} \text{ l'ensemble des idéaux de } \mathbb{A} \text{ incluant } I \\ \mathcal{I}_{\mathbb{A}/I} \text{ l'ensemble des idéaux de } \mathbb{A}/I \end{cases}$$

- Si J est un idéal de $\mathbb{A}$, alors $\underset{\rightarrow}{\mathrm{pr}}(J)$ est un idéal de $\mathbb{A}/I$, car l'image d'un idéal par le morphisme d'anneaux pr est un idéal de l'image de pr, égale à $\mathbb{A}/I$ puisque pr est surjectif.
- Si K est un idéal de $\mathbb{A}/I$, alors l'image réciproque de K par pr est un idéal de $\mathbb{A}$ incluant le noyau de pr (car l'idéal K contient l'élément neutre de $\mathbb{A}/I$), autrement dit $\underset{\leftarrow}{\mathrm{pr}}(K)$ est un idéal de $\mathbb{A}$ incluant I.

On peut donc définir les fonctions

$$f : \begin{cases} \mathcal{I}_{\mathbb{A}} \longrightarrow \mathcal{I}_{\mathbb{A}/I} \\ J \longmapsto \underset{\rightarrow}{\mathrm{pr}}(J) \end{cases} \qquad \text{et} \qquad g : \begin{cases} \mathcal{I}_{\mathbb{A}/I} \longrightarrow \mathcal{I}_{\mathbb{A}} \\ K \longmapsto \underset{\leftarrow}{\mathrm{pr}}(K) \end{cases}$$

De plus, comme pr est surjective, pour toute partie K de $\mathbb{A}/I$, $\underset{\rightarrow}{\mathrm{pr}}(\underset{\leftarrow}{\mathrm{pr}}(K)) = K$, donc $f \circ g = \mathrm{id}$ et par conséquent f est surjective. Prouvons que f est injective : on considère deux idéaux J et J' de $\mathbb{A}$ incluant I tels que $\underset{\rightarrow}{\mathrm{pr}}(J) = \underset{\rightarrow}{\mathrm{pr}}(J')$. Pour tout $x \in J$, comme $\mathrm{pr}(x) \in \underset{\rightarrow}{\mathrm{pr}}(J) = \underset{\rightarrow}{\mathrm{pr}}(J')$, il existe $x' \in J'$ tel que $\mathrm{pr}(x) = \mathrm{pr}(x')$, et par conséquent $x - x' \in I \subseteq J'$, donc $x \in J'$. On en déduit $J \subseteq J'$, et de même $J' \subseteq J$, donc $J = J'$. Par conséquent f est injective, et on en déduit que f est bijective et que $f^{-1} = g$.

Théorème 13.1.5
Si $A \xrightarrow{f} B$ est un morphisme d'anneaux surjectif et $a \in A$, alors l'image directe par f de l'idéal principal engendré par a est l'idéal principal engendré par $f(a)$, autrement dit $\underset{\rightarrow}{f}(aA) = f(a)B$.

Preuve

$$\underset{\rightarrow}{f}(aA) = \{f(ax)\,;\, x \in A\} = \{f(a)f(x)\,;\, x \in A\} = \{f(a)b\,;\, b \in B\} = f(a)B$$

Théorème 13.1.6 (Corollaire)
Si tous les idéaux de $\mathbb{A}$ sont principaux et si I est un idéal de $\mathbb{A}$, alors tous les idéaux de $\mathbb{A}/I$ sont principaux.

Preuve
Un idéal J de $\mathbb{A}/I$ est l'image par $\underset{\rightarrow}{\mathrm{pr}}$ d'un idéal de $\mathbb{A}$ incluant I. Comme tous les idéaux de $\mathbb{A}$ sont principaux, il s'agit d'un idéal de la forme $a\mathbb{A}$ (avec $a \in \mathbb{A}$). Donc, d'après le théorème précédent, J est l'idéal principal engendré par $\mathrm{pr}(a)$.

13.2 Anneaux principaux, anneaux euclidiens

Définition 13.2.1 (Anneau principal)
On appelle *anneau principal* tout anneau intègre dont tous les idéaux sont principaux.

Exemple 13.2.2 (Exemples d'anneaux principaux)
Les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ sont principaux.

Remarque 13.2.3 : Attention, si $\mathbb{A}$ est un anneau principal et si I est un idéal de $\mathbb{A}$, alors $\mathbb{A}/I$ peut ne pas être un anneau principal : nous avons vu que si tous les idéaux de $\mathbb{A}$ sont principaux, alors tous les idéaux de $\mathbb{A}/I$ sont principaux ; mais $\mathbb{A}/I$ n'est pas nécessairement un anneau principal car il peut ne pas être intègre. Par exemple, les idéaux des $\mathbb{Z}/n\mathbb{Z}$ sont principaux (car tous les idéaux de $\mathbb{Z}$ sont principaux), mais si n n'est pas un nombre premier alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas un anneau principal, car ce n'est pas un anneau intègre.

Ces pages ne sont pas incluses dans l’aperçu.

Liste des symboles

$\bigcup \mathscr{E}$ ou $\bigcup_{A\in\mathscr{E}} A$	Réunion de l'ensemble $\mathscr{E}$
$\bigcup_{i\in I} A_i$	Réunion de la famille $(A_i)_{i\in I}$
$A \cup B$	Réunion des ensembles A et B
$\bigcap \mathscr{E}$ ou $\bigcap_{A\in\mathscr{E}} A$	Intersection de l'ensemble $\mathscr{E}$
$\bigcap_{i\in I} A_i$	Intersection de la famille $(A_i)_{i\in I}$
$A \cap B$	Intersection des ensembles A et B
$A \setminus B$	Différence des ensembles A et B
$\complement_E A$	Complémentaire de l'ensemble A dans E
$A \Delta B$	Différence symétrique des ensembles A et B
$\mathscr{P}(E)$	Ensemble des sous-ensembles (ou parties) de l'ensemble E
$A \times B$	Produit cartésien des ensembles A et B
$\prod_{i\in I} A_i$	Produit de la famille $(A_i)_{i\in I}$
$A \sqcup B$	Somme (ou union) disjointe des ensembles A et B
$E/\sim$	Ensemble quotient de E par la relation d'équivalence $\sim$
$[x]$	Classe de x pour une relation d'équivalence donnée
$a \in A$	L'élément a appartient à l'ensemble A
$\subseteq$	Symbole d'inclusion entre ensembles
$\subset$	Symbole d'inclusion stricte entre ensembles
$\varnothing$	Ensemble vide
$\mathbb{N}$	Ensemble des entiers naturels
$\mathbb{N}^*$	Ensemble des entiers naturels différents de 0
$\mathbb{P}$	Ensemble des nombres premiers
$\mathbb{Z}$	Ensemble des entiers relatifs
$\aleph_0$	Cardinal de $\mathbb{N}$ (plus petit cardinal transfini)

$\mathbb{Q}$	Corps des nombres rationnels, page 128
$\mathbb{R}$	Corps des nombres réels, page 168
$\mathbb{C}$	Corps des nombres complexes, page 214
$\mathbb{U}$	Groupe des complexes de module 1 (cercle unité), page 227
$\mathbb{Z}$[i]	Anneau des entiers de Gauss, page 220
$\mathbb{A}[\![X]\!]$	$\mathbb{A}$-algèbre des séries formelles, page 287
$\mathbb{A}[X]$	$\mathbb{A}$-algèbre des polynômes, page 287
$\deg(P)$	Degré du polynôme P, page 290
$\mathrm{val}(P)$	Valuation du polynôme P, page 290
A^*	Ensemble des éléments non nuls de l'anneau A
$A^\times$	Ensemble des éléments inversibles de l'anneau A (pour la multiplication)
$H \trianglelefteq G$	H est un sous-groupe normal de G
$\mathrm{SGr}(G)$	Ensemble des sous-groupes de G
$Z(G)$	Centre du groupe G (ensemble des éléments qui commutent avec tous les autres)
$\mathrm{supp}(\sigma)$	Support de la permutation σ, page 74
$\mathrm{fix}(\sigma)$	Ensemble des points fixes de la permutation σ, page 74
$\mathcal{O}(x)$	Orbite de x, page 80
$\mathrm{End}(E)$	Ensemble des endomorphismes du groupe E
$\mathrm{Aut}(G)$	Groupe des automorphismes du groupe G (isomorphismes de G dans lui-même)
$\mathrm{Int}(G)$	Groupe des automorphismes intérieurs du groupe G (automorphismes de la forme $x \longmapsto axa^{-1}$)
$\mathscr{L}(E,F)$	Ensemble des fonctions linéaires de E dans F, page 257
$\mathscr{L}(E)$	Ensemble des endomorphismes du module E, page 257
$\mathrm{Ker}(f)$	Noyau du morphisme de groupes f (ensemble des éléments dont l'image est l'élément neutre)
$\mathcal{S}_E$	Groupe symétrique de E (groupe des permutations de E), page 69
$\mathcal{S}_n$	Groupe symétrique de l'ensemble $[1,n]$, page 69
$\langle A \rangle$	Sous-groupe engendré par A, page 59
$\langle A \rangle$	Sous-module engendré par A, page 245
$\langle A \rangle$ ou $\mathrm{Vect}(A)$	Sous-espace vectoriel engendré par A, page 245
$\langle P \rangle$	Idéal principal engendré par le polynôme P, page 306
$\|x\|$	Norme du vecteur x, page 357
$\mathrm{BO}(a,r)$	Boule ouverte de centre a et de rayon r, page 365
$\mathrm{BF}(a,r)$	Boule fermée de centre a et de rayon r, page 365
$\mathrm{S}(a,r)$	Sphère de centre a et de rayon r, page 365

$\mathring{A}$	Intérieur d'une partie A d'un espace topologique, page 384
$\overline{A}$	Adhérence d'une partie A d'un espace topologique, page 384
$\mathrm{Fr}(A)$	Frontière d'une partie A d'un espace topologique, page 384
$a \mid b$	a divise b
$\sum_{k=p}^{n} a_k$	Somme : $a_p + a_{p+1} + \cdots + a_{n-1} + a_n$
$\prod_{k=p}^{n} a_k$	Produit : $a_p \times a_{p+1} \times \cdots \times a_{n-1} \times a_n$
$\lfloor x \rfloor$	Partie entière de x, page 140
x^+	Partie positive du réel x, page 494
x^-	Partie négative du réel x, page 494
$\mathfrak{R}(z)$	Partie réelle du complexe z, page 219
$\mathfrak{I}(z)$	Partie imaginaire du complexe z, page 219
$\lvert z \rvert$	Module du complexe z, page 224
$\overline{z}$	Conjugué du complexe z, page 222
$=$	Égalité logique entre deux objets identiques, page 5
$\overset{\text{def}}{=}$	Égalité par définition, page 5
$\equiv$	Équivalence logique (sémantique ou syntaxique), page 5
id_A	Fonction identité de l'ensemble A ($x \longmapsto x$)
$f : A \longrightarrow B$ ou $A \xrightarrow{f} B$	f est une fonction de A dans B, page 6
$(a_i)_{i \in I}$	Famille indexée par I (fonction $i \longmapsto a_i$), page 6
χ_A	Fonction indicatrice de l'ensemble $A : x \longmapsto \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{sinon} \end{cases}$
$f \circ g$	Composée de la fonction g par la fonction f : $f \circ g(x) = f(g(x))$
$f\vert_A$	Restriction de la fonction f à un sous-ensemble A de son domaine
$A \longrightarrow B$ ou B^A	Ensemble des fonctions de A dans B, page 6
$\mathrm{Inj}_{k,n}$	Ensemble des injections de $[1, k]$ dans $[1, n]$, page 20
$\mathrm{Surj}_{k,n}$	Ensemble des surjections de $[1, k]$ dans $[1, n]$, page 20
$\mathrm{Inj}(A, B)$	Ensemble des injections de A dans B
$\mathrm{Surj}(A, B)$	Ensemble des surjections de A dans B
$\mathrm{Bij}(A, B)$	Ensemble des bijections de A dans B
$A \simeq B$	Les ensembles A et B sont en bijection, page 7
$A \simeq B$ ou $(A, \dots) \simeq (B, \dots)$	Les structures $(A, \dots)$ et $(B, \dots)$ sont isomorphes, page 7
$\mathrm{dom}(f)$	Domaine de la fonction f

$\mathrm{cod}(f)$	Codomaine (ensemble d'arrivée) de la fonction f
$\mathrm{Im}(f)$	Image de la fonction f, page 7
$\underset{\rightarrow}{f}(A)$	Image directe de l'ensemble A par la fonction f, page 6
$\underset{\leftarrow}{f}(A)$	Image réciproque de l'ensemble A par la fonction f, page 6
$\binom{n}{k}$	Coefficient binomial : nombre de k-combinaisons (sans répétition) d'un ensemble de cardinal n, page 33
Γ_n^k	Nombre de k-combinaisons avec répétition d'un ensemble de cardinal n, page 44
A_n^k	Nombre de k-arrangements d'éléments d'un ensemble de cardinal n, page 27
$\neg$	Connecteur logique pour la négation
« et », « $\wedge$ »	Connecteur logique pour la conjonction (*et*)
« ou », « $\vee$ »	Connecteur logique pour la disjonction (*ou*)
$\Longrightarrow$	Connecteur logique pour l'implication
$\Longleftrightarrow$	Connecteur logique pour l'équivalence
$\Gamma \vdash \mathscr{F}$	$\mathscr{F}$ est une conséquence syntaxique de Γ, Γ prouve $\mathscr{F}$
$\mathscr{F}(t/x)$	Formule $\mathscr{F}$ dans laquelle le terme t remplace la variable x
$\forall x$	Quantificateur universel : quel que soit x…
$\exists x$	Quantificateur existentiel : il existe x…
$\exists ! x$	Il existe un unique x tel que…
$[a,b]_A,]-\infty,b]_A, \ldots$	Intervalles de l'ensemble ordonné A, page 6
$a \wedge b$ ou $\min(a,b)$	Minimum de a et b
$a \vee b$ ou $\max(a,b)$	Maximum de a et b
ZF	Théorie des ensembles de Zermelo-Fraenkel
ZFC	Théorie des ensembles de Zermelo-Fraenkel avec axiome du choix

Index des notions

Accumulation (point d'), 391
Action
    (de groupe), 76
    par conjugaison, 81
Addition dans $\mathbb{R}$, 183
Adhérence, 384
    (valeur d'), 432
Algèbre, 274
    de Banach, 437
    des polynômes, 287
    des séries formelles, 287
Alternée (série), 482
Anneau
    à division, 7
    archimédien, 136
    des nombres décimaux, 130
    euclidien, 532
    factoriel, 553
    principal, 531
Application linéaire, 251
Arbre (théorie des graphes), 333
Arc (d'un graphe), 316
Archimédien, 136
Arête (d'un graphe), 316
Argument (d'un nombre complexe), 521
Arrangement avec répétition, 25

Banach
    (algèbre de), 437
    (espace de), 437
Base
    (d'un module ou d'un espace vectoriel), 260
    (d'une topologie), 349
    canonique, 262
    d'ouverts, 349
    de topologie, 351
    de voisinages, 350
Bilinéaire (fonction), 250
Biparti (graphe), 326
Bornée
    (fonction), 368
    (partie), 368
Boucle (d'un graphe), 316
Boule
    fermée, 365
    ouverte, 365

Caractéristique (d'un anneau), 10
Cauchy (suite de), 158, 435
Cercle unité, 227
Chemin
    (théorie des graphes), 329
    élémentaire (théorie des graphes), 329
    eulérien, 340
    hamiltonien, 342
    simple (théorie des graphes), 329
Classe de conjugaison, 81
Coefficient
    binomial, 32
    dominant (d'un polynôme), 291
Coefficients d'un polynôme, 290
Coloration (d'un graphe), 343
Combinaison
    avec répétition, 44
    linéaire, 242
    sans répétition, 32
Compacité locale, 451
Compact, 442
Complet
    (corps), 162
    (espace métrique), 437
    (graphe), 324
Complexes (nombres), 216
Composantes connexes (d'un graphe), 331
Composition (de polynômes), 302
Conjugué, 222

Conjugués (éléments), 81
Connexe
(espace), 457
(graphe), 330
Continuité
(en un point), 394
(globale), 398
uniforme, 401
Convergence
absolue, 491
d'une suite, 146, 424
normale, 502
simple, 430
simple (d'une série de fonctions), 501
uniforme, 431
uniforme (d'une série de fonctions), 501
Convergent, 146, 424
Convexe, 196
Corps
complet, 162
des fractions d'un anneau intègre, 121
des nombres complexes, 216
des nombres rationnels, 128
des nombres réels, 181, 192
gauche, 7
premier, 133
Cosinus, 511
Coupure de Dedekind, 178
Critère de Cauchy pour les séries, 491
Curryfication, 6
Cycle, 83
(théorie des graphes), 329
eulérien, 340
hamiltonien, 342
Cyclique (graphe), 325

Dedekind (coupure de), 178
Degré
(d'un polynôme), 290
(d'un sommet d'un graphe), 326
Dense (sous-ensemble), 12
Densité (topologie), 419
Dérivabilité, 463
Dérivée
à droite, 467
à gauche, 467
Développement
d'un réel en base *b*, 208
décimal, 208
Diamètre
(d'un graphe), 337
(dans un espace métrique), 367
Dimension
(d'un espace vectoriel), 273
finie (espace vectoriel), 270
Discriminant, 202
Distance, 356
(théorie des graphes), 337
Distances
équivalentes, 372
topologiquement équivalentes, 375
Divergence
d'une suite, 146, 424
Divergent, 146, 424
Division euclidienne
(dans un anneau euclidien), 532
des polynômes, 304
Droite réelle achevée, 213
Décimaux, 130

Élément
de torsion, 237
irréductible (dans un anneau), 538
premier (dans un anneau), 535
réductible (dans un anneau), 538
Ensemble
des nombres complexes, 216
des nombres réels, 181, 192
Entiers de Gauss, 220
Équivalence
(de distances), 372
(de normes), 372
Espace
à base dénombrable de voisinages, 377
connexe, 457
de Banach, 437
localement compact, 451
métrique, 356
métrique complet, 437
précompact, 445
topologique, 345
vectoriel, 229
vectoriel de dimension finie, 270
vectoriel normé, 357
Étiquette (théorie des graphes), 321
Euclidien (anneau), 532
Évaluation (d'un pôlynôme), 299
Exponentielle, 503

Exposant
(d'un groupe), 64
rationnel, 204
réel, 510
Extremum local, 472

Factoriel (anneau), 553
Famille
génératrice, 260
libre, 260
liée, 260
sommable, 487, 492
Fermat (nombres de), 107
Fermé, 346
Fonction
additive, 109
arithmétique, 109
bilinéaire, 250
bornée, 368
cosinus, 511
dérivable, 463
exponentielle, 503
impaire, 478
linéaire, 250
lipschitzienne, 401
multiplicative, 109
paire, 478
polynôme, 301
sinus, 511
Forme
algébrique, 219
exponentielle, 521
irréductible (d'un rationnel), 129
polaire, 521
trigonométrique, 521
Formule du binôme de Newton, 38
Frontière, 384

Gauss (entiers de), 220
Génératrice (famille), 260
Graphe
biparti, 326
complet, 324
connexe, 330
cyclique, 325
eulérien, 340
hamiltonien, 342
k-régulier, 328
non orienté, 316
orienté, 316
simple, 317
symétrique, 319
Groupe
alterné, 94
archimédien, 136
cyclique, 64
de Klein, 96
linéaire, 258
monogène, 64
symétrique, 69

Homéomorphisme, 400
Homothétie, 231

Idéal
maximal, 536
premier, 535
Imaginaire
(partie), 219
pur, 219
Indicatrice d'Euler, 111
Indice (d'un sous-groupe), 56
Inégalité
de Bernoulli, 15
de Cauchy-Schwarz, 16
des accroissements finis, 475
des accroissements finis généralisée, 476
Intérieur, 384
Inversion, 90
Irrationnel (nombre), 200
Irréductible (élément), 538
Isolé (point), 391
Isométrie, 364
Isomorphisme (de graphes), 320

k-arrangement, 27
k-combinaison, 32

Libre (famille), 260
Liée (famille), 260
Limite, 393
Linéaire
(combinaison), 242
(fonction), 250
Lipschitzienne (fonction), 401
Liste des 9 plus petits nombres parfaits, 119
Logarithme, 509

Matrice, 239

colonne, 239
d'une fonction linéaire, 278
de changement de base, 283
de passage, 283
diagonale, 239
ligne, 239
scalaire, 239
symétrique, 242
transposée, 241
triangulaire, 239
Maximal (idéal), 536
Maximum local, 472
Mersenne (nombres de), 105
Métrique (espace), 356
Métrisable (topologie), 372
Minimum local, 472
Module
(d'un nombre complexe), 224
(structure algébrique), 229
de torsion, sans torsion, 237
Monôme, 290
Multiplication
dans $\mathbb{R}$, 185
de matrices, 280

Népérien (logarithme), 509
Nombre
π, 514
chromatique, 343
dérivé, 463
i, 217
irrationnel, 200
parfait, 117
Nombres
de Fermat, 107
de Mersenne, 105
de Stirling de seconde espèce, 47
Normale (convergence), 502
Norme, 357
Normes équivalentes, 372
Noyau (théorie des graphes), 334

Orbite, 80
Ordre
(d'un élément), 61
(d'un graphe), 317
(d'un groupe), 56
Ouvert, 345
élémentaire, 377

p-graphe, 317
Parcours
en largeur (théorie des graphes), 337
en profondeur (théorie des graphes), 338
Parfait (nombre), 117
Parité (d'une fonction), 478
Partie
bornée, 368
entière, 140
imaginaire, 219
négative (d'un réel), 494
positive (d'un réel), 494
réelle, 219
Période (d'une fonction), 422
PGCD (dans un anneau), 544
Pi, 514
Point
d'accumulation, 391
isolé, 391
Polynôme, 287
(fonction), 301
constant, 290
scindé, 527
unitaire, 291
PPCM (dans un anneau), 544
Précompacité, 445
Premier
(élément), 535
(idéal), 535
Premiers entre eux (éléments), 545
Principal (anneau), 531
Produit de Cauchy, 285
Prolongement par continuité, 412
Propriété
de la borne supérieure, 168
de la limite monotone, 168
Puits (théorie des graphes), 327
Pythagoricien (triplet), 101

Racine
(d'un polynôme), 307
carrée, 197
cubique, 197
n-ième d'un complexe, 522
Rationnels, 128
Recouvrement, 442
Rectangle (topologie), 377
Réductible (élément), 538
Réelle (partie), 219

Réels (nombres), 181, 192
Règle
de Cauchy, 486
de d'Alembert, 485
Relation
d'ordre dans $\mathbb{R}$, 181
de Bézout, 547
Reste (d'une série), 481

Scalaire, 230
Scindé (polynôme), 527
Série, 479
absolument convergente, 491
alternée, 482
de fonctions uniformément de Cauchy, 501
formelle, 287
Signature, 91
Simple
(convergence), 430
(graphe), 317
Sinus, 511
Sommable (famille), 487, 492
Somme partielle, 479
Sommet
(d'un graphe), 316
isolé (théorie des graphes), 327
pendant (théorie des graphes), 327
Source (théorie des graphes), 327
Sous-algèbre, 274
Sous-corps premier, 133
Sous-espace vectoriel engendré, 245
Sous-graphe, 323
engendré, 324
Sous-groupes d'un groupe quotient, 99
Sous-module, 243
engendré, 245
Sphère, 365
Stabilisateur, 79
Stathme euclidien, 532
Stirling (nombres de), 47
Suite
convergente, 146, 424
de Cauchy, 158, 435
de fonctions uniformément de Cauchy, 438
divergente, 146, 424
exhaustive de parties finies, 489
Support (d'une permutation), 74
Symétrique (graphe), 319

Taille (d'un graphe), 317
Théorème
d'Euclide-Euler, 118
d'Euler, 113
de Bézout, 547
de Cayley, 71
de d'Alembert-Gauss, 525
de Fermat (petit), 114
de Goldbach, 108
de Heine, 449
de Krull, 537
de la base incomplète, 271
de Lagrange, 57
de Mertens, 499
de Riesz, 456
de Rolle, 473
de Wilson, 98
des accroissements finis, 474
des gendarmes, 154
des segments emboîtés, 169
des suites adjacentes, 168
fondamental de l'algèbre, 525
Topologie, 345
(base de), 351
engendrée, 351
induite, 380
métrisable, 372
trace, 380
Torsion
(élément de), 237
(module de, module sans), 237
Trace (topologie), 380
Transposée (d'une matrice), 241
Transposition, 71, 241
Triangle
de Pascal, 35
de Stirling, 49
Triplet Pythagoricien, 101
primitif, 102

Uniforme
(continuité), 401
(convergence), 431
Unitaire (polynôme), 291

Valeur
approchée, 207
d'adhérence, 432
Valuation (d'un polynôme ou d'une série formelle), 290

Vecteur, 230

Vectoriel (espace), 229

Voisinage, 347

Zéro (d'une fonction), 307

Index des noms propres

ADLEMAN, Leonard, 115
AL-HAYTHAM, 118
ANASTÁCIO DA CUNHA, José, 159
APIANUS, Petrus, 36
ARGAND, Jean-Robert, 527

BACHET DE MÉZIRIAC, Claude-Gaspard, 547
BARROW, Isaac, 16
BERNOULLI, Jakob (Jacques), 15
BÉZOUT, Étienne, 547
BOLZANO, Bernard, 159
BOUNIAKOVSKI, Viktor, 16
BOURBAKI, Nicolas, 128

CANTOR, Georg, 173, 177, 450
CARDAN, Jérôme, 214
CARMICHAEL, Robert Daniel, 114
CAUCHY, Augustin-Louis, 16, 159, 285, 498

DEDEKIND, Richard, 177
DESCARTES, René, 119, 220, 527
DIRICHLET, Peter Gustav Lejeune, 450

EUCLIDE, 118
EULER, Leonhard, 33, 107, 112, 118, 315

FERMAT, Pierre de, 107
FRÉCHET, Maurice, 159

GAUSS, Carl Friedrich, 112, 141, 220, 527

HALAYUDHA, 36
HEINE, Eduard, 450
HODGES, Wilfrid, 538
HUI, Yang, 36

IVERSON, Kenneth Eugene, 141

KRULL, Wolfgang, 537

LAGRANGE, Joseph-Louis, 57, 311
LEGENDRE, Adrien-Marie, 141
LEURECHON, Jean, 119
LUCAS, Édouard, 106

MERSENNE, Marin, 106, 119
MERTENS, Franz, 499
MYDORGE, Claude, 120

NEWTON, Isaac, 39
NIELSEN, Niels, 48

PASCAL, Blaise, 36
PEANO, Giuseppe, 128
PINGALA, 36
PYTHAGORE, 101

RIESZ, Frigyes, 456
RIVEST, Ronald, 115

SCHWARZ, Hermann Amandus, 16
SHAMIR, Adi, 115
SHIJIE, Zhu, 42
SLUSE, René-François de, 16
STIRLING, James, 48
SYLVESTER, James Joseph, 112

TARTAGLIA, 36, 214

VAN ETTEN, H., 119
VANDERMONDE, Alexandre-Théophile, 41
VON ETTINGSHAUSEN, Andreas, 33

WEIERSTRASS, Karl, 173

XIAN, Jia, 36