



MARIE-CÉCILE DARRACQ • JEAN-ÉTIENNE ROMBALDI

Algèbre et géométrie pour la Licence

LICENCES 1 & 2
MATHÉMATIQUES

- Cours complet
- Près de 200 exercices
- Tous les corrigés détaillés



MARIE-CÉCILE DARRACQ • JEAN-ÉTIENNE ROMBALDI

Algèbre et géométrie pour la Licence

Des mêmes auteurs

DARRACQ M.-C., ROMBALDI J.-É., *Probabilités pour la Licence* (nouveau 2021)

DARRACQ M.-C., ROMBALDI J.-É., *Analyse pour la Licence*

DARRACQ M.-C., ROMBALDI J.-É., *Mathématiques pour le Capes. Probabilités* (nouveau 2021)

DARRACQ M.-C., ROMBALDI J.-É., *Mathématiques pour le Capes. Algèbre et géométrie* (nouveau 2021)

DARRACQ M.-C., ROMBALDI J.-É., *Mathématiques pour le Capes. Analyse*

ROMBALDI J.-É., *Mathématiques pour l'agrégation. Algèbre et géométrie – 2^e édition* (nouveau 2021)

ROMBALDI J.-É., *Exercices et problèmes corrigés pour l'agrégation de mathématiques*

ROMBALDI J.-É., *Leçons d'oral pour l'agrégation de mathématiques. Première épreuve : les exposés*

ROMBALDI J.-É., *Leçons d'oral pour l'agrégation de mathématiques. Seconde épreuve : les exercices*

Pour toute information sur notre fonds et les nouveautés dans votre domaine de spécialisation, consultez notre site web :

www.deboecksuperieur.com

En couverture : Coupe d'un nautille © AdrianHancu/Istockphoto

Maquette intérieure : Hervé Soulard/Nexeme

Mise en pages de l'auteur

Maquette de couverture : Primo&Primo

Couverture : SCM, Toulouse

Dépôt légal :

Bibliothèque royale de Belgique : 2021/13647/105

Bibliothèque nationale, Paris : juillet 2021

ISBN : 978-2-8073-3221-8

Tous droits réservés pour tous pays.

Il est interdit, sauf accord préalable et écrit de l'éditeur, de reproduire (notamment par photocopie) partiellement ou totalement le présent ouvrage, de le stocker dans une banque de données ou de le communiquer au public, sous quelque forme ou de quelque manière que ce soit.

Sommaire

Avant-propos	ix
1 Éléments de logique et de théorie des ensembles	1
2 Structure de groupe	31
3 Structures d'anneau et de corps	57
4 Division euclidienne dans \mathbb{Z}	71
5 Le corps \mathbb{C} des nombres complexes	109
6 Espaces vectoriels réels ou complexes	139
7 Espaces vectoriels réels ou complexes de dimension finie	169
8 Opérations élémentaires et déterminants	191
9 Polynômes à coefficients réels ou complexes	211
10 Réduction des endomorphismes	245
11 Formes bilinéaires et quadratiques réelles ou complexes	263
12 Espaces préhilbertiens	305
Bibliographie	337
Index	339

Table des matières

Avant-propos	ix
1 Éléments de logique et de théorie des ensembles	1
1.1 Quelques notions de logique	1
1.2 Les connecteurs logiques de base	2
1.3 Quelques méthodes de raisonnement	4
1.4 Notions de base sur les ensembles. Quantificateurs	5
1.5 Les symboles \sum et \prod	7
1.6 Les théorèmes de récurrence	8
1.7 L'algèbre des parties d'un ensemble	9
1.8 Applications. Notions d'injectivité, surjectivité et bijectivité	11
1.9 Relations d'ordre et d'équivalence	16
1.10 Exercices	18
2 Structure de groupe	31
2.1 Loi de composition interne	31
2.2 Groupes	33
2.3 Sous-groupes	35
2.4 Sous-groupe engendré par une partie	36
2.5 Groupes monogènes	37
2.6 Groupes finis. Théorème de Lagrange	39
2.7 Morphismes de groupes	40
2.8 Ordre d'un élément dans un groupe	43
2.9 Exercices	46
3 Structures d'anneau et de corps	57
3.1 Anneaux	57
3.2 Éléments inversibles dans un anneau unitaire	60
3.3 Sous-anneaux	61
3.4 Morphismes d'anneaux	62
3.5 Corps	62
3.6 Morphismes de corps	64
3.7 Exercices	64
4 Division euclidienne dans \mathbb{Z}	71
4.1 Divisibilité et congruences	71
4.2 Le théorème de division euclidienne dans \mathbb{Z}	72

4.3	Les systèmes de numération	73
4.4	Plus grand commun diviseur et plus petit commun multiple	74
4.5	L'algorithme d'Euclide	80
4.6	Equations diophantiennes $ax + by = c$	82
4.7	Equations $ax \equiv b \pmod{n}$	83
4.8	Le théorème Chinois	84
4.9	L'ensemble \mathcal{P} des nombres premiers	85
4.10	Décomposition en facteurs premiers	87
4.11	Les théorèmes de Fermat et de Wilson	89
4.12	Les anneaux $\frac{\mathbb{Z}}{n\mathbb{Z}}$ et la fonction indicatrice d'Euler	92
4.13	Exercices	97
5	Le corps \mathbb{C} des nombres complexes	109
5.1	Conditions nécessaires à la construction de \mathbb{C}	110
5.2	Construction de \mathbb{C}	110
5.3	Conjugué et module d'un nombre complexe	113
5.4	Les équations de degré 2	116
5.5	Les équations de degré 3 et 4	119
5.6	Arguments d'un nombre complexe	120
5.7	Racines n -ièmes d'un nombre complexe	125
5.8	Exercices	127
6	Espaces vectoriels réels ou complexes	139
6.1	L'espace vectoriel \mathbb{K}^n	139
6.2	Définition d'un espace vectoriel réel ou complexe	140
6.3	Sous-espaces vectoriels	142
6.4	Applications linéaires	146
6.5	Base canonique de \mathbb{K}^n et expression matricielle des applications linéaires de \mathbb{K}^n dans \mathbb{K}^m	149
6.6	Matrices réelles ou complexes	151
6.7	Systèmes d'équations linéaires	159
6.8	Sommes et sommes directes de sous-espaces vectoriels	160
6.9	Exercices	162
7	Espaces vectoriels réels ou complexes de dimension finie	169
7.1	Systèmes libres, systèmes générateurs et bases	169
7.2	Espaces vectoriels de dimension finie	172
7.3	Rang d'un système de vecteurs ou d'une application linéaire	179
7.4	Expression matricielle des applications linéaires	181
7.5	Formules de changement de base	184
7.6	Exercices	186
8	Opérations élémentaires et déterminants	191
8.1	Opérations élémentaires. Matrices de dilatation et de transvection	192
8.2	Déterminants des matrices carrées	195
8.3	Déterminant d'une famille de vecteurs	203
8.4	Déterminant d'un endomorphisme	204
8.5	Exercices	205

9	Polynômes à coefficients réels ou complexes	211
9.1	L'algèbre $\mathbb{K}[X]$ des polynômes à coefficients dans \mathbb{K}	211
9.2	Division euclidienne dans $\mathbb{K}[X]$	215
9.3	Polynômes premiers entre eux	220
9.4	Fonctions polynomiales, racines des polynômes	222
9.5	Dérivation des polynômes. Formule de Taylor	225
9.6	Polynômes irréductibles	227
9.7	Décomposition des fractions rationnelles en éléments simples	231
9.8	Polynômes d'interpolation de Lagrange	236
9.9	Exercices	238
10	Réduction des endomorphismes	245
10.1	Polynômes d'endomorphismes, polynômes annulateurs, polynôme minimal	245
10.2	Le théorème de décomposition des noyaux	246
10.3	Valeurs et vecteurs propres	248
10.4	Le théorème de Cayley-Hamilton	251
10.5	Diagonalisation	253
10.6	Endomorphismes trigonalisables	255
10.7	Exercices	257
11	Formes bilinéaires et quadratiques réelles ou complexes	263
11.1	Formes linéaires	263
11.2	Formes bilinéaires	266
11.3	Expression matricielle des formes bilinéaires (en dimension finie)	267
11.4	Formes quadratiques	269
11.5	Théorème de réduction de Gauss	271
11.6	Orthogonalité, noyau et rang	278
11.7	Signature d'une forme quadratique réelle en dimension finie	282
11.8	Quadriques dans \mathbb{R}^n ou \mathbb{C}^n	285
11.9	Exercices	289
12	Espaces préhilbertiens	305
12.1	Produit scalaire	305
12.2	Orthogonalité	307
12.3	Procédé d'orthogonalisation de Gram-Schmidt	309
12.4	Projection orthogonale sur un sous-espace de dimension finie	311
12.5	Les endomorphismes symétriques réels	317
12.6	Espaces vectoriels hermitiens	319
12.7	Réduction des matrices normales	321
12.8	Exercices	322
	Bibliographie	337
	Index	339

Avant-propos

Ce cours d'algèbre s'adresse aux étudiants de première et deuxième année d'université. C'est le deuxième volume d'une série qui en comporte 3, le premier volume étant consacré à l'analyse et le troisième à la théorie des probabilités. Il ne s'agit pas de manuels de « méthodes » où l'on sacrifie la notion de rigueur qui est l'essence même des mathématiques. Les notions étudiées le sont de façon rigoureuse en démontrant tous (ou presque) les résultats énoncés. Chaque chapitre se termine par une série d'exercices tous corrigés en détails.

Ce deuxième volume est consacré aux notions d'algèbre habituellement enseignées en première et deux années de licence (L1 et L2), à savoir l'étude de quelques notions de logique et de théorie des ensembles, des structures de groupe, d'anneaux et de corps, en se concentrant sur l'anneau des entiers relatifs, le corps des nombres complexes, l'anneau des polynômes à coefficients réels ou complexes et les principales notions d'algèbre linéaire et bilinéaire avec la réduction des endomorphismes et des formes quadratiques. On s'intéresse également à quelques notions d'arithmétique.

Les élèves en classes préparatoires aux grandes écoles pourront aussi tirer profit de cet ouvrage.

Ces livres seront également utiles aux candidats au Capes. Une deuxième version de ce volume d'algèbre avec un dernier chapitre consacré à quelques épreuves choisies de ce concours sera également publiée à destination de ces candidats, le niveau d'exigence pour ces épreuves ne dépassant pas le niveau L1-L2. Nous espérons que ce travail leur sera utile.

Pour conclure, nous tenons à remercier les éditions De Boeck et en particulier Alain Luguët pour la confiance qu'ils nous accordent en publiant ce travail.

Chapitre 1

Éléments de logique et de théorie des ensembles

Pour les exemples et exercices traités dans ce chapitre les ensembles usuels de nombres entiers, rationnels réels et complexes sont supposés connus, au moins de manière intuitive comme cela se passe au Lycée.

1.1 Quelques notions de logique

Nous allons préciser à un premier niveau quelques notions mathématiques qui sont relativement intuitives mais nécessitent quand même des définitions rigoureuses. L'idée étant de préciser schématiquement comment se présente une théorie mathématique ainsi que la notion essentielle de démonstration.

La première notion est celle d'assertion. De manière intuitive, une assertion est un énoncé mathématique aussi rigoureux que possible qui ne peut prendre que deux valeurs de vérité à savoir « vrai » ou « faux » mais jamais entre les deux comme dans le langage courant.

Une assertion qui est toujours vraie est une tautologie.

Par exemple les énoncés suivants sont des assertions : $2 < 15$ (elle est vraie), $\sqrt{2}$ est un nombre rationnel (elle est fausse), $\cos(n\pi) = (-1)^n$ (vraie), ...

Deux assertions sont dites logiquement équivalentes, ou plus simplement équivalentes, si elles sont toutes deux vraies ou toutes deux fausses.

Il y a ensuite les énoncés qui se démontrent. Pour ce faire, on se donne des règles précises (que nous verrons par la pratique) qui permettent de construire de nouvelles assertions à partir d'assertions données.

Il ne faut pas croire que dans une théorie donnée toute assertion P soit obligatoirement démontrable. En 1931 Kurt Gödel a démontré qu'il y a des assertions non démontrables (on dit aussi qu'elles sont indécidables) : il n'est pas possible de démontrer que P est vraie ni que P est fausse.

À la base de toute théorie mathématique, on dispose d'un petit nombre d'assertions qui sont supposés vraies *a priori* (c'est-à-dire avant toute expérience) et que l'on nomme axiomes ou postulats. Ces axiomes sont élaborés par abstraction à partir de l'intuition et ne sont pas déduits d'autres relations.

Par exemple, la géométrie euclidienne est basée sur une quinzaine d'axiomes. L'un de ces axiomes est le postulat numéro 15 qui affirme que par un point donné passe une et une seule droite parallèle à une droite donnée.

Une autre exemple important est donné par la construction de l'ensemble noté \mathbb{N} des entiers naturels. Cette construction peut se faire en utilisant les axiomes de Peano suivants :

- 0 est un entier naturel ;
- tout entier naturel n a un unique successeur noté $n + 1$;
- deux entiers naturels ayant même successeur sont égaux ;
- une partie P de \mathbb{N} qui contient 0 et telle que si n est dans P alors le successeur de n y est aussi, est égale à \mathbb{N} (axiome de récurrence).

Nous reviendrons au paragraphe 1.6 sur l'ensemble \mathbb{N} en partant sur une autre base.

La théorie des ensemble est basée sur le système d'axiomes de Zermelo-Fränkël.

La notion de définition nous permet de décrire un objet ou une situation précise à l'aide du langage courant.

Les énoncés qui se démontrent sont classés en fonction de leur importance dans une théorie comme suit :

- un théorème est une assertion vraie déduite d'autres assertions, il s'agit en général d'un résultat important à retenir ;
- un lemme est un résultat préliminaire utilisé pour démontrer un théorème ;
- un corollaire est une conséquence importante d'un théorème ;
- une proposition est de manière générale un résultat auquel on peut attribuer la valeur vraie ou fausse sans ambiguïté.

Pour rédiger un énoncé mathématique, on utilise le langage courant et les objets manipulés sont représentés en général par des lettres de l'alphabet latin ou grec. Usuellement, on utilise :

- les lettres minuscules a, b, c, \dots pour des objets fixés ;
- les lettres minuscules x, y, z, t, \dots pour des objets inconnus à déterminer ;
- les lettres majuscules E, F, G, H, \dots pour des ensembles ;
- des lettres de l'alphabet grecques minuscules ou majuscules $\alpha, \beta, \varepsilon, \delta, \dots \Lambda, \Gamma, \Omega, \dots$

1.2 Les connecteurs logiques de base

L'élaboration de nouvelles assertions à partir d'autres se fait en utilisant les connecteurs logiques de négation, de conjonction, de disjonction, d'implication et d'équivalence définis comme suit, où P et Q désignent des assertions.

- La négation de P , notée $\neg P$, ou non P ou \overline{P} , est l'assertion qui est vraie si P est fausse et fausse si P est vraie. Par exemple la négation de l'assertion : « x est strictement positif » est « x est négatif ou nul ». En théorie des ensembles on admet qu'il n'existe pas d'assertion P telle que P et \overline{P} soient toutes deux vraies. On dit que cette théorie est non contradictoire.

- La conjonction de P et Q , notée $P \wedge Q$ (lire P et Q), est l'assertion qui est vraie uniquement si P et Q sont toutes deux vraies (et donc fausse dans les trois autres cas). Par exemple $P \wedge \overline{P}$ est toujours faux (on se place dans des théories non contradictoires).
- La disjonction de P et Q , notée $P \vee Q$ (lire P ou Q), est l'assertion qui est vraie uniquement si l'une des deux assertions P ou Q est vraie (donc fausse si P et Q sont toutes deux fausses). Par exemple $P \vee \overline{P}$ est toujours vraie (c'est une tautologie). Il faut remarquer que le « ou » pour « ou bien » est inclusif, c'est-à-dire que P et Q peuvent être toutes deux vraies dans le cas où $P \vee Q$ est vraie. On peut aussi introduire le « ou exclusif », noté W , qui est vrai uniquement lorsque l'une des deux assertions, mais pas les deux simultanément, est vraie.
- L'implication, notée $P \rightarrow Q$, est l'assertion qui est fausse uniquement si P est vraie et Q fausse (donc vraie dans les trois autres cas). On peut remarquer que si P est fausse, alors $P \rightarrow Q$ est vraie indépendamment de la valeur de vérité de Q . L'implication est à la base du raisonnement mathématique. En partant d'une assertion P (ou de plusieurs), une démonstration aboutit à un résultat Q . Si cette démonstration est faite sans erreur, alors $P \rightarrow Q$ est vraie et on notera $P \Rightarrow Q$ (ce qui signifie que si P est vraie, alors Q est vraie). Dans ce cas, on dit que P est une condition suffisante et Q une condition nécessaire. On peut remarquer que l'implication est transitive, c'est-à-dire que si P implique Q et Q implique R , alors P implique R .
- L'équivalence de P et Q , notée $P \leftrightarrow Q$, est l'assertion qui est vraie uniquement si $P \rightarrow Q$ et $Q \rightarrow P$ sont toutes deux vraies. Dans le cas où $P \leftrightarrow Q$ est vraie on dit que P et Q sont équivalentes et on note $P \Leftrightarrow Q$ (ce qui signifie que P et Q sont, soit toutes deux vraies, soit toutes deux fausses). Dans ce cas, on dit que Q est une condition nécessaire et suffisante de P .

On peut résumer ce qui précède, en utilisant la table de vérité suivante :

P	Q	\overline{P}	$P \wedge Q$	$P \vee Q$	$P \rightarrow Q$	$P \leftrightarrow Q$
V	V	F	V	V	V	V
V	F	F	F	V	F	F
F	V	V	F	V	V	F
F	F	V	F	F	V	V

Les tables de vérité peuvent être utilisées pour faire certaines démonstrations. Deux assertions qui ont même table de vérité sont équivalentes. Avec le théorème qui suit, on résume quelques règles de calcul.

Théorème 1.1.

Soient P, Q, R des propositions. On a les équivalences :

1. *commutativité :*

$$(P \wedge Q) \Leftrightarrow (Q \wedge P) \text{ et } (P \vee Q) \Leftrightarrow (Q \vee P)$$

2. associativité

$$(P \wedge (Q \wedge R)) \Leftrightarrow ((P \wedge Q) \wedge R) \text{ et } (P \vee (Q \vee R)) \Leftrightarrow ((P \vee Q) \vee R)$$

3. distributivité :

$$(P \wedge (Q \vee R)) \Leftrightarrow ((P \wedge Q) \vee (P \wedge R))$$

$$(P \vee (Q \wedge R)) \Leftrightarrow ((P \vee Q) \wedge (P \vee R))$$

4. négations :

$$(\overline{\overline{P}}) \Leftrightarrow (P), (\overline{P \wedge Q}) \Leftrightarrow (\overline{P} \vee \overline{Q}), (\overline{P \vee Q}) \Leftrightarrow (\overline{P} \wedge \overline{Q})$$

$$(P \rightarrow Q) \Leftrightarrow (\overline{Q} \rightarrow \overline{P}), (P \rightarrow Q) \Leftrightarrow (\overline{P} \vee Q), (\overline{P \rightarrow Q}) \Leftrightarrow (P \wedge \overline{Q})$$

Preuve. On utilise les tables de vérité (exercice laissé au lecteur). \square

Les équivalences $(\overline{P \wedge Q}) \Leftrightarrow (\overline{P} \vee \overline{Q})$ et $(\overline{P \vee Q}) \Leftrightarrow (\overline{P} \wedge \overline{Q})$ sont appelées lois de Morgan.

1.3 Quelques méthodes de raisonnement

En général l'énoncé d'une proposition à démontrer est formé d'une ou plusieurs hypothèses qui constituent l'assertion H et d'une ou plusieurs conclusions qui constituent l'assertion C . Il s'agit donc de montrer l'implication $H \Rightarrow C$. Si de plus, on peut montrer que $C \Rightarrow H$, on dira alors que la réciproque de la proposition est vraie. Les idées de base que l'on peut utiliser sont les suivantes.

- Une assertion peut toujours être remplacée par n'importe quelle assertion qui lui est équivalente.
- On peut effectuer une démonstration directe, c'est-à-dire de déduire logiquement C de H .
- L'implication étant transitive, on peut essayer de montrer que $C \Rightarrow C'$ sachant par ailleurs que $C' \Rightarrow H$.
- Dans le cas où une démonstration directe semble difficile, on peut essayer une démonstration par l'absurde qui consiste à étudier l'assertion $H \wedge \overline{C}$ équivalente à $\overline{H \rightarrow C}$ et on montre qu'on aboutit à une impossibilité si cette dernière assertion est vraie (pratiquement, on suppose que la conclusion est fautive avec les hypothèses et on aboutit à une absurdité). Il en résulte alors que $\overline{H \rightarrow C}$ est fautive, c'est-à-dire que $H \rightarrow C$ est vraie, soit $H \Rightarrow C$.
- On peut aussi essayer de montrer la contraposée $\overline{C} \Rightarrow \overline{H}$ puisque les implications $H \rightarrow C$ et $\overline{C} \rightarrow \overline{H}$ sont équivalentes.
- La démonstration par contre-exemple permet de montrer qu'une implication $H \rightarrow C$, où H et C sont des propriétés portant sur des variables x , est fautive. Pour ce faire on cherche une ou des valeurs de x pour lesquels $H(x)$ est vraie et $C(x)$ est fautive.

- La démonstration par récurrence permet de montrer qu'une propriété portant sur des entiers naturels est toujours vraie. Cette méthode de démonstration est décrite au paragraphe 1.6, où elle apparaît comme un théorème basé sur le fait que l'ensemble des entiers naturels est bien ordonné. Si on accepte l'axiome de Péano, le principe de récurrence en est une conséquence immédiate.

1.4 Notions de base sur les ensembles. Quantificateurs

Nous nous contenterons d'une définition intuitive de la notion d'ensemble.

Un ensemble est une collection d'objets possédant des propriétés communes, ces objets sont les éléments de l'ensemble. On admet l'existence d'un ensemble qui ne contient aucun élément. Cet ensemble est noté \emptyset et on dit que c'est l'ensemble vide.

On utilisera les notations suivantes, pour les ensembles de nombres usuels :

- \mathbb{N} est l'ensemble des entiers naturels ;
- \mathbb{Z} est l'ensemble des entiers relatifs ;
- \mathbb{Q} est l'ensemble des nombres rationnels
- \mathbb{R} est l'ensemble des nombres réels ;
- \mathbb{C} est l'ensemble des nombres complexes.

Nous serons souvent amenés à décrire un ensemble en précisant les propriétés que doivent vérifier tous ses éléments, ce que nous noterons de la façon suivante :

$$E = \{\text{description des propriétés des éléments de } E\}$$

(on dit que l'ensemble E est défini en compréhension).

Cette notion d'ensemble défini en compréhension peut conduire à des paradoxes liés au problème de « l'ensemble de tous les ensembles », mais à un premier niveau, on se contente de ce point de vue intuitif. Une étude approfondie de la théorie des ensembles peut mener assez loin. Le lecteur intéressé peut consulter le volume de Bourbaki sur les ensembles, ou tout autre ouvrage spécialisé.

On peut aussi décrire un ensemble en donnant la liste finie ou infinie de tous ces éléments, quand cela est possible, ce qui se note $E = \{x_1, x_2, \dots, x_n\}$ s'il s'agit d'un ensemble fini ou $E = \{x_1, x_2, \dots, x_n, \dots\}$ s'il s'agit d'un ensemble infini pour lequel on peut numéroter les éléments (un tel ensemble est dit dénombrable). On dit alors que l'ensemble E est défini en extension.

Un singleton est un ensemble qui ne contient qu'un élément, soit $E = \{a\}$.

Si n, m sont deux entiers relatifs, l'ensemble des entiers relatifs compris entre n et m sera noté $\{n, \dots, m\}$. Dans le cas où $m < n$, il ne peut y avoir d'entiers entre n et m et cet ensemble est tout simplement l'ensemble vide. Dans le cas où $n = m$, cet ensemble est le singleton $\{n\}$. Pour $n < m$, on notera aussi $\{n, n+1, \dots, m\}$ cet ensemble.

Si E est un ensemble, on notera alors $a \in E$ pour signifier que a est un élément de E , ce qui se lit « a appartient à E ». La négation de cette assertion est « a n'appartient pas à E » et se notera $a \notin E$.

Pour signifier qu'un ensemble F est contenu dans un ensemble E , ce qui signifie que tout élément de F est dans E , nous noterons $F \subset E$ qui se lit « F est contenu dans E ». On peut écrire de manière équivalente que $E \supset F$ pour dire que E contient F . La négation de cette assertion est notée $F \not\subset E$.

Deux ensembles E et F sont égaux si, et seulement si, ils ont les mêmes éléments, ce qui se traduit par $E \subset F$ et $F \subset E$.

On admet que si E est un ensemble, il existe un ensemble dont tous les éléments sont formés de tous les sous-ensembles (ou parties) de E . On note $\mathcal{P}(E)$ cet ensemble et on dit que c'est l'ensemble des parties de E . Ainsi $F \subset E$ est équivalent à $F \in \mathcal{P}(E)$. L'ensemble vide et E sont des éléments de $\mathcal{P}(E)$.

Par exemple pour $E = \{1, 2, 3\}$, on a :

$$\mathcal{P}(E) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Pour décrire des ensembles, ou faire des raisonnements, nous utiliseront les deux quantificateurs suivants.

- Le quantificateur universel « quel que soit » ou « pour tout » noté \forall utilisé pour signifier que tout élément x d'un ensemble E vérifie une propriété $P(x)$, la syntaxe étant :

$$(\forall x \in E) (P(x)) \tag{1.1}$$

- Le quantificateur existentiel « il existe » noté \exists pour signifier qu'il existe au moins un élément x de E vérifiant la propriété $P(x)$, la syntaxe étant :

$$(\exists x \in E) | (P(x)) \tag{1.2}$$

Pour signifier qu'il existe un et un seul x dans E vérifiant la propriété $P(x)$, on utilisera la syntaxe $(\exists! x \in E) | (P(x))$.

La négation de l'assertion 1.1 est $(\exists x \in E) | (\overline{P(x)})$ en utilisant le symbole $|$ qui se lit « tel que » utilisé pour traduire le fait que x est tel que la propriété $\overline{P(x)}$ est vérifiée et la négation de 1.2 est $(\forall x \in E) (\overline{P(x)})$.

Nous verrons qu'il n'est pas toujours facile de traduire la négation d'une assertion en utilisant les quantificateurs. Par exemple pour traduire le fait qu'une suite $(u_n)_{n \in \mathbb{N}}$ de nombres réels est convergente vers un réel ℓ nous écrivons :

$$(\exists \ell \in \mathbb{R}) | (\forall \varepsilon > 0, \exists n_0 \in \mathbb{N} | \forall n \geq n_0, |u_n - \ell| < \varepsilon)$$

ce qui signifie qu'il existe un réel ℓ tel que quel que soit la précision $\varepsilon > 0$ que l'on choisisse l'écart entre u_n et ℓ (soit $|u_n - \ell|$) est inférieur à ε à partir d'un certain rang n_0 . La négation de cette assertion s'écrit :

$$(\forall \ell \in \mathbb{R}), (\exists \varepsilon > 0, \forall n_0 \in \mathbb{N}, \exists n \geq n_0 | |u_n - \ell| \geq \varepsilon)$$

En utilisant les quantificateurs, il faudra faire attention à l'ordre d'apparition de ces derniers. Par exemple les assertions suivantes, où f est une fonction à valeurs réelles définie sur un ensemble E :

$$\forall x \in E, \exists M > 0 | f(x) < M$$

$$\exists M > 0 \mid \forall x \in E, f(x) < M$$

ne sont pas équivalentes. La première assertion signifie que pour tout élément x de E il existe un réel $M > 0$ qui dépend à priori de x (il faudrait donc le noter $M(x)$) tel que $f(x) < M$ (par exemple $M(x) = f(x) + 1$ convient), alors que la seconde signifie qu'il existe un réel $M > 0$, indépendant de x dans E , tel que $f(x) < M$, ce qui n'est pas la même chose.

1.5 Les symboles \sum et \prod

Si n est un entier naturel non nul et x_1, x_2, \dots, x_n des entiers, rationnels, réels ou complexes, on notera :

$$\sum_{k=1}^n x_k = x_1 + x_2 + \dots + x_n \text{ et } \prod_{k=1}^n x_k = x_1 \cdot x_2 \cdot \dots \cdot x_n$$

la somme et le produit des x_k . Dans une telle somme ou produit l'indice est muet, ce qui signifie que $\sum_{k=1}^n x_k = \sum_{i=1}^n x_i$ et $\prod_{k=1}^n x_k = \prod_{i=1}^n x_i$.

La manipulation d'un produit de réels strictement positifs se ramène à une somme en utilisant la fonction logarithme $\ln \left(\prod_{k=1}^n x_k \right) = \sum_{k=1}^n \ln(x_k)$.

On peut également effectuer des changements d'indice. Par exemple, en posant $i = k + 1$, on a $\sum_{k=1}^n x_k = \sum_{i=2}^{n+1} x_{i-1} = \sum_{k=2}^{n+1} x_{k-1}$.

On peut ajouter ou multiplier de telles sommes (ou produits). Par exemple, on a :

$$\begin{aligned} \sum_{k=1}^n x_k + \sum_{k=1}^n y_k &= \sum_{k=1}^n (x_k + y_k), \quad \lambda \sum_{k=1}^n x_k = \sum_{k=1}^n \lambda x_k \\ \left(\sum_{k=1}^n x_k \right) \left(\sum_{k=1}^m y_k \right) &= \left(\sum_{j=1}^n x_j \right) \left(\sum_{k=1}^m y_k \right) = \sum_{\substack{1 \leq j \leq n \\ 1 \leq k \leq m}} x_j y_k \end{aligned}$$

Pour vérifier ce dernier résultat, on écrit que :

$$\begin{aligned} S &= \left(\sum_{k=1}^n x_k \right) \left(\sum_{k=1}^m y_k \right) = (x_1 + x_2 + \dots + x_n) \left(\sum_{k=1}^m y_k \right) \\ &= x_1 \sum_{k=1}^m y_k + \dots + x_n \sum_{k=1}^m y_k = \sum_{j=1}^n x_j \left(\sum_{k=1}^m y_k \right) \\ &= \sum_{j=1}^n \left(\sum_{k=1}^m x_j y_k \right) = \sum_{\substack{1 \leq j \leq n \\ 1 \leq k \leq m}} x_j y_k \end{aligned}$$

1.6 Les théorèmes de récurrence

On désigne par \mathbb{N} l'ensemble des entiers naturels, soit $\mathbb{N} = \{0, 1, 2, \dots, n, \dots\}$. La construction de cet ensemble avec les opérations usuelles d'addition et de multiplication est admise. On note \mathbb{N}^* l'ensemble \mathbb{N} privé de 0.

Notre point de départ est l'axiome du bon ordre suivant : toute partie non vide de \mathbb{N} admet un plus petit élément, ce qui signifie que si A est une partie non vide de \mathbb{N} , il existe alors un entier $m \in \mathbb{N}$ tel que $m \leq n$ pour tout $n \in A$. De cet axiome du bon ordre, on déduit les deux théorèmes fondamentaux qui suivent. Le premier résultat est souvent appelé théorème de récurrence faible et le second théorème de récurrence forte.

Théorème 1.2.

Soient $n_0 \in \mathbb{N}$ et $\mathcal{P}(n)$ une propriété portant sur les entiers $n \geq n_0$. La propriété $\mathcal{P}(n)$ est vraie pour tout entier $n \geq n_0$ si, et seulement si :

- (i) $\mathcal{P}(n_0)$ est vraie ;
- (ii) pour tout $n \geq n_0$ si $\mathcal{P}(n)$ est vrai alors $\mathcal{P}(n+1)$ est vraie.

Preuve. La condition nécessaire est évidente. En supposant les conditions (i) et (ii) vérifiées, on note A l'ensemble des entiers $n \geq n_0$ pour lesquels $\mathcal{P}(n)$ est faux. Si A est non vide, il admet alors un plus petit élément $n > n_0$ (puisque $\mathcal{P}(n_0)$ est vraie). Mais alors $\mathcal{P}(n-1)$ est vraie ce qui implique, d'après (ii), que $\mathcal{P}(n)$ est vraie, soit une contradiction. En définitive A est vide et la propriété est vraie pour tout entier $n \geq n_0$. \square

Théorème 1.3.

Soient $n_0 \in \mathbb{N}$ et $\mathcal{P}(n)$ une propriété portant sur les entiers $n \geq n_0$. La propriété $\mathcal{P}(n)$ est vraie pour tout entier $n \geq n_0$ si, et seulement si :

- (i) $\mathcal{P}(n_0)$ est vraie ;
- (ii) pour tout $n \geq n_0$ si $\mathcal{P}(k)$ est vrai pour tout entier k compris entre n_0 et n , alors $\mathcal{P}(n+1)$ est vraie.

Preuve. La condition nécessaire est évidente. En supposant les conditions (i) et (ii) vérifiées, on note A l'ensemble des entiers $n \geq n_0$ pour lesquels $\mathcal{P}(n)$ est faux. Si A est non vide, il admet alors un plus petit élément $n > n_0$ et $\mathcal{P}(k)$ est vraie pour tout k compris entre n_0 et $n-1$, ce qui implique que $\mathcal{P}(n)$ est vraie, soit une contradiction. En définitive A est vide et la propriété est vraie pour tout entier $n \geq n_0$. \square

Le théorème de récurrence nous permet de définir la fonction factorielle sur l'ensemble des entiers naturels de la façon suivante :

$$\begin{cases} 0! = 1 \\ \forall n \in \mathbb{N}, (n+1)! = (n+1)n! \end{cases}$$

De manière plus générale, c'est le théorème de récurrence qui nous assure de l'existence et de l'unicité d'une suite (réelle ou complexe) définie par :

$$\begin{cases} u_0 \text{ est donné} \\ \forall n \in \mathbb{N}, u_{n+1} = f(u_n) \end{cases}$$

où f est une fonction définie sur un ensemble I et à valeurs dans le même ensemble I . Une telle suite est dite définie par une relation de récurrence (d'ordre 1). Une telle suite peut aussi se définir en donnant les premières valeurs u_0, u_1, \dots, u_p et une relation $u_{n+1} = f(u_n, \dots, u_{n-(p-1)})$ pour $n \geq p-1$. Une telle suite est dite définie par une relation de récurrence d'ordre p .

1.7 L'algèbre des parties d'un ensemble

Nous allons définir sur l'ensemble $\mathcal{P}(E)$ des parties d'un ensemble E des opérations qui vont traduire les idées intuitives de partie complémentaire, d'intersection et de réunion.

L'ensemble E étant donné et A, B, C, \dots désignant des parties de E (donc des éléments de $\mathcal{P}(E)$), on définit les ensembles suivant.

- le complémentaire de A dans E est l'ensemble noté $C_E A$, ou $E \setminus A$ (lire E moins A) ou \overline{A} des éléments de E qui ne sont pas dans A , ce qui peut se traduire par :

$$(x \in \overline{A}) \Leftrightarrow ((x \in E) \wedge (x \notin A))$$

ou encore par $\overline{A} = \{x \in E \mid x \notin A\}$.

- L'intersection de A et B , notée $A \cap B$, est l'ensemble des éléments de E qui sont dans A et dans B , soit :

$$(x \in A \cap B) \Leftrightarrow ((x \in A) \wedge (x \in B))$$

ou encore $A \cap B = \{x \in E \mid x \in A \text{ et } x \in B\}$. Si $A \cap B = \emptyset$, on dit alors que A et B sont disjointes. Par exemple A et \overline{A} sont disjointes.

- La réunion de A et B , notée $A \cup B$, est l'ensemble des éléments de E qui sont soit dans A , soit dans B (éventuellement dans A et B) soit :

$$(x \in A \cup B) \Leftrightarrow ((x \in A) \vee (x \in B))$$

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

- La différence de A et B , notée $A \setminus B$, est l'ensemble des éléments de E qui sont dans A et qui ne sont pas dans B , soit :

$$(x \in A \setminus B) \Leftrightarrow ((x \in A) \wedge (x \notin B))$$

ou encore $A \setminus B = \{x \in A \mid x \notin B\}$. Ainsi $\overline{\overline{A}} = A$.

- La différence symétrique de A et B , notée $A \Delta B$, est l'ensemble des éléments de E qui sont soit dans A et pas dans B soit dans B et pas dans A (c'est-à-dire dans A ou exclusif dans B), soit :

$$(x \in A \Delta B) \Leftrightarrow ((x \in A) \wedge (x \notin B)) \vee ((x \in B) \wedge (x \notin A))$$

Par exemple, on a $A \Delta \emptyset = A$, $A \Delta E = \overline{A}$.

Ces opérateurs de complémentarité, intersection, réunion et différence symétrique sont décrits à l'aide des connecteurs logiques non de négation, \wedge de conjonction, \vee de disjonction et Δ de disjonction exclusive.

Avec le théorème qui suit, on résume les résultats essentiels relatifs à ces opérateurs ensemblistes.

Théorème 1.4.

Soient E un ensemble et A, B, C, \dots des sous-ensembles de E . On a :

1. commutativité : $A \cap B = B \cap A$, $A \cup B = B \cup A$, $A \Delta B = B \Delta A$;
2. associativité :

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

$$A \Delta (B \Delta C) = (A \Delta B) \Delta C$$

3. distributivité :

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \quad A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$$

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

4. différence symétrique : $A \Delta A = \emptyset$, $A \Delta B = (A \setminus B) \cup (B \setminus A)$,
 $A \Delta B = (A \cap \overline{B}) \cup (B \cap \overline{A})$, $A \Delta B = (A \cup B) \setminus (A \cap B)$;
5. négations : $\overline{\overline{A}} = A$, $(A \subset B) \Leftrightarrow (\overline{B} \subset \overline{A})$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$,
 $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Preuve. L laissée au lecteur. □

On notera l'analogie entre ce théorème et le théorème 1.1 sur les règles de calculs avec les connecteurs logiques.

La propriété d'associativité de l'intersection et de la réunion nous permet d'écrire $A \cap B \cap C$ et $A \cup B \cup C$ l'intersection et la réunion de trois ensembles sans se soucier de parenthèses. De manière plus générale, grâce à cette associativité, on peut définir l'intersection ou la réunion de n sous-ensembles A_1, A_2, \dots, A_n de E par :

$$(x \in A_1 \cap A_2 \cap \dots \cap A_n) \Leftrightarrow ((x \in A_1) \wedge (x \in A_2) \wedge \dots \wedge (x \in A_n))$$

et :

$$(x \in A_1 \cup A_2 \cup \dots \cup A_n) \Leftrightarrow ((x \in A_1) \vee (x \in A_2) \vee \dots \vee (x \in A_n))$$

De façon condensée, on écrira $(A_k)_{1 \leq k \leq n}$ une telle famille de sous ensembles de E , $\bigcap_{k=1}^n A_k = A_1 \cap A_2 \cap \dots \cap A_n$ l'intersection et $\bigcup_{k=1}^n A_k = A_1 \cup A_2 \cup \dots \cup A_n$ la réunion.

On vérifie facilement que $E \setminus \bigcap_{k=1}^n A_k = \bigcup_{k=1}^n (E \setminus A_k)$, $E \setminus \bigcup_{k=1}^n A_k = \bigcap_{k=1}^n (E \setminus A_k)$ et

que pour tout entier j compris entre 1 et n , on a $\bigcap_{k=1}^n A_k \subset A_j \subset \bigcup_{k=1}^n A_k$.

Définition 1.1. On dit qu'une famille $(A_k)_{1 \leq k \leq n}$ de parties d'un ensemble E forme une partition de E , si les A_k sont deux à deux disjoints, c'est-à-dire que $A_k \cap A_j = \emptyset$ pour $1 \leq k \neq j \leq n$ et de réunion égale à E , soit

$$\bigcup_{k=1}^n A_k = E.$$

Dans le cas où (A_1, A_2) forme une partition de E , on a nécessairement $A_2 = \overline{A_1}$. La notion de produit cartésien de deux ensembles sera très souvent utilisée. Elle correspond à l'idée de couples et se généralise pour aboutir à la notion de liste.

Définition 1.2. Étant donné deux ensembles E et F , on appelle produit cartésien de E par F l'ensemble $E \times F$ des couples (x, y) formés d'un élément x de E et d'un élément y de F .

Il est à noter que les couples sont ordonnés, c'est-à-dire que $(x, y) = (y, x)$ $E \times F$ si, et seulement si, $x = y$. De manière plus générale, on a $(x, y) = (x', y')$ dans $E \times F$ si, et seulement si, $x = x'$ et $y = y'$.

Dans le cas où $F = E$, on note E^2 pour $E \times E$.

On peut itérer le procédé et définir le produit cartésien $E_1 \times E_2 \times \dots \times E_n$ de n ensembles comme l'ensemble des listes (ordonnées) (x_1, x_2, \dots, x_n) formées d'un élément x_1 de E_1 suivi d'un élément x_2 de E_2 , \dots , suivi d'un élément x_n de E_n .

On notera de façon condensé $\prod_{k=1}^n E_k = E_1 \times \dots \times E_n$.

Là encore, on a $(x_1, x_2, \dots, x_n) = (x'_1, x'_2, \dots, x'_n)$ dans $E \times F$ si, et seulement si, $x_k = x'_k$ pour tout k compris entre 1 et n .

Dans le cas où tous les E_k sont égaux à un même ensemble E , on notera E^n pour $E \times E \times \dots \times E$ (n fois).

1.8 Applications. Notions d'injectivité, surjectivité et bijectivité

Les notations E, F, G désignent des ensembles.

Définition 1.3. On appelle application, ou fonction, de E dans F (ou de E vers F) toute partie Γ du produit cartésien $E \times F$ telle que :

$$\forall x \in E, \exists ! y \in F \mid (x, y) \in \Gamma$$

En notant f une application de E dans F (c'est en réalité le triplet (E, F, Γ) avec la propriété énoncée ci-dessus), on note pour tout $x \in E$, $f(x)$ l'unique élément de F tel que $(x, f(x)) \in \Gamma$ et on dit que $f(x)$ est l'image de x par f et x est un antécédent de y par f . Un antécédent de y par f n'est pas unique a priori. On dit aussi que E est l'ensemble de départ (ou l'ensemble de définition), F l'ensemble d'arrivée et Γ le graphe de l'application f .

Deux applications f et g sont égales si, et seulement si, elles ont même ensemble de départ E , même ensemble d'arrivée F et même graphe Γ , c'est-à-dire que :

$$\forall x \in E, g(x) = f(x)$$

On a tout simplement précisé l'idée d'un procédé qui associe à tout élément de E un unique élément de F . On note :

$$\begin{array}{lcl} f : & E & \rightarrow & F \\ & x & \mapsto & f(x) \end{array}$$

une telle application (ou fonction). On utilisera aussi les notation $f : E \rightarrow F$ ou $f : x \mapsto f(x)$.

Nous ne faisons pas la distinction ici entre fonction et application. Usuellement, on distingue ces notions en disant qu'une fonction de E dans F toute partie Γ du produit cartésien $E \times F$ telle que pour tout élément x de E , il existe au plus un élément y de F tel que $(x, y) \in \Gamma$. Le sous-ensemble D de E pour lequel il existe un unique élément y de F tel que $(x, y) \in \Gamma$ est appelé l'ensemble de définition de la fonction. Une application est donc une fonction pour laquelle tout élément de l'ensemble de départ E a une image dans F .

On note $\mathcal{F}(E, F)$ ou F^E l'ensemble de toutes les applications de E dans F (la deuxième notation sera justifiée plus loin).

L'application qui associe à tout x d'un ensemble E le même x est l'application identique notée Id_E , où Id si l'ensemble E est fixé.

Si f est une fonction de E dans F et D un sous-ensemble non vide de E , on définit une application g de D dans F en posant :

$$\forall x \in D, g(x) = f(x)$$

et on dit que g est la restriction de f à D , ce qui se note $g = f|_D$.

Définition 1.4. Soit f une application de E dans F . Pour toute partie A de E , l'image de A par f est le sous ensemble de F noté $f(A)$ et défini par $f(A) = \{f(x) \mid x \in A\}$. Pour toute partie B de F , l'image réciproque de B par f est le sous ensemble de E noté $f^{-1}(B)$ et défini par $f^{-1}(B) = \{x \in E \mid f(x) \in B\}$.

On a donc, pour tout $y \in F$:

$$(y \in f(A)) \Leftrightarrow (\exists x \in A \mid y = f(x))$$

et pour tout $x \in E$:

$$(x \in f^{-1}(B)) \Leftrightarrow (f(x) \in B)$$

L'ensemble $f(E)$ est appelé l'image de f .

Exemple 1.1 On a $f(\emptyset) = \emptyset$, $f(\{x\}) = \{f(x)\}$ pour tout $x \in E$, $f^{-1}(\emptyset) = \emptyset$ et $f^{-1}(F) = E$.

Pour tout $y \in F$, $f^{-1}\{y\}$ est l'ensemble des $x \in E$ tels que $f(x) = y$ et cet ensemble peut être vide ou formé de un ou plusieurs éléments. En fait $f^{-1}\{y\}$ est l'ensemble des solutions dans E de l'équation $f(x) = y$, où y est donné dans F et x l'inconnue dans E . Cette équation peut avoir 0 ou plusieurs solutions.

On vérifie facilement le résultat suivant.

Théorème 1.5.

Soit f une application de E dans F . Pour toutes parties A, B de E et C, D de F , on a :

1. $A \subset B \Rightarrow f(A) \subset f(B)$
2. $f(A \cup B) = f(A) \cup f(B)$
3. $f(A \cap B) \subset f(A) \cap f(B)$
4. $C \subset D \Rightarrow f^{-1}(C) \subset f^{-1}(D)$
5. $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$
6. $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$
7. $f^{-1}(\overline{C}) = \overline{f^{-1}(C)}$

Preuve. Vérification immédiate. Par exemple, pour le point **2**, on peut écrire que y est dans $f(A \cup B)$ si, et seulement si, il existe x dans $A \cup B$ tel que $y = f(x)$, ce qui implique que $y \in f(A)$ dans le cas où $x \in A$ ou $y \in f(B)$ dans le cas où $x \in B$, soit $y \in f(A) \cup f(B)$ dans tous les cas. Réciproquement si $y \in f(A) \cup f(B)$, il est dans $f(A)$ ou $f(B)$ et s'écrit donc $y = f(x)$ avec x dans A ou B , ce qui signifie que $y \in f(A \cup B)$. On a donc les inclusions $f(A \cup B) \subset f(A) \cup f(B)$ et $f(A) \cup f(B) \subset f(A \cup B)$, c'est-à-dire l'égalité souhaitée.

Pour le point **3**, on a seulement une inclusion. Dire que $y \in f(A \cap B)$ équivaut à dire qu'il existe $x \in A \cap B$ tel que $y = f(x)$ et $y \in f(A) \cap f(B)$. Réciproquement, si $y \in f(A) \cap f(B)$, il existe $x_1 \in A$ et $x_2 \in B$ tels que $y = f(x_1) = f(x_2)$ et, a priori, il n'y a aucune raison pour que $x_1 = x_2$. \square

On dispose d'une opération importante sur les fonctions, c'est la composition des fonctions qui permet de construire de nouvelles fonctions à partir de fonctions données.

Définition 1.5. Soient f une application de E dans F et g une application de F dans G . La composée de f par g est la fonction de E dans G notée $g \circ f$ et définie par :

$$\forall x \in E, g \circ f(x) = g(f(x))$$

Ce qui peut se schématiser par :

$$\begin{array}{ccccc} E & \xrightarrow{f} & F & \xrightarrow{g} & G \\ x & \mapsto & f(x) & \mapsto & g(f(x)) \end{array}$$

On remarquera que $f \circ g$ n'est pas définie *a priori* (dans la situation de la définition).

Dans le cas où f est définie de E dans F et g de F dans E , on peut définir les applications $f \circ g$ (de F dans F) et $g \circ f$ (de E dans E) et il n'y a aucune raison pour que ces applications soient égales, même dans le cas où $F = E$.

Dans le cas où $E = F$, on dit que les applications f et g (définies de E dans E) commutent, si $f \circ g = g \circ f$.

On vérifie facilement que la loi de composition est associative, c'est-à-dire que $f \circ (g \circ h) = (f \circ g) \circ h$, quand toutes ces composées ont un sens. Cette propriété d'associativité permet de définir la composée de n applications $f_1 \circ f_2 \circ \dots \circ f_n$ sans se soucier de parenthèses.

Si f est une application de E dans E , on peut définir la suite de ses itérées par la relation de récurrence suivante :

$$\begin{cases} f^1 = f \\ \forall n \in \mathbb{N}^*, f^{n+1} = f^n \circ f \end{cases}$$

On convient que $f^0 = Id_E$. On vérifie facilement que $f^p \circ f^q = f^q \circ f^p = f^{p+q}$ pour tous entiers naturels p, q .

Les notions suivantes d'injectivité et de surjectivité sont aussi très importantes.

Définition 1.6. Soient E, F deux ensembles et f une application de E dans F . On dit que f est :

1. *injective* (ou que c'est une injection) si deux éléments distincts de E ont deux images distinctes dans F , soit :

$$x_1 \neq x_2 \text{ dans } E \Rightarrow f(x_1) \neq f(x_2) \text{ dans } F \quad (1.3)$$

2. *surjective* (ou que c'est une surjection) si tout élément de F a au moins un antécédent dans E , soit :

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

3. *bijective* (ou que c'est une bijection) si elle est à la fois injective ou surjective.

Une injection peut aussi se caractériser en disant que tout élément de F a au plus un antécédent par f , encore équivalent à dire que pour tout $y \in F$ l'équation $y = f(x)$ a au plus une solution x dans E , ce qui revient à dire que si x_1 et x_2 sont deux éléments de E tels que $f(x_1) = f(x_2)$, alors $x_1 = x_2$ (contraposée de (1.3)).

Une surjection peut se caractériser en disant que pour tout $y \in F$ l'équation $y = f(x)$ a au moins une solution x dans E , encore équivalent à dire que $f(E) = F$.

Si f est une surjection de E dans F , on dit parfois que f est une surjection de E sur (pour surjection) F .

Une bijection peut se caractériser en disant que tout élément de F a un unique antécédent par f , encore équivalent à dire que pour tout $y \in F$ l'équation $y = f(x)$ a une et une seule solution x dans E , ce qui permet de définir l'application réciproque de f , notée f^{-1} , de F dans E par :

$$(y \in F \text{ et } x = f^{-1}(y)) \Leftrightarrow (x \in E \text{ et } y = f(x))$$

Cette application f^{-1} est une bijection de F dans E . L'application $f \circ f^{-1}$ est alors l'application identité $y \mapsto y$ de F dans F et l'application $f^{-1} \circ f$ est l'application identité $x \mapsto x$ de E dans E , ce qui se note $f \circ f^{-1} = Id_F$ et $f^{-1} \circ f = Id_E$.

Définition 1.7. On appelle permutation d'un ensemble E toute bijection de E dans lui-même.

On note en général $\mathfrak{S}(E)$ l'ensemble des permutations de E .

Exemple 1.2 L'application $x \mapsto x^2$ est surjective de \mathbb{R} dans \mathbb{R}^+ , mais non injective. Elle est bijective de \mathbb{R}^+ dans \mathbb{R}^+ .

Dans le cas où f est une application de E dans F , on a noté pour toute partie B de F , $f^{-1}(B)$ l'image réciproque de B par f , sans aucune hypothèse de bijectivité pour f . Dans le cas où f est bijective, $f^{-1}(B)$ est aussi l'image directe de B par f^{-1} , mais dans le cas général, il faut bien prendre garde, malgré la notation, que f n'a aucune raison d'être bijective. Il faudrait en réalité utiliser un autre symbole que f^{-1} (par exemple $f^*(B)$, $f^{(-1)}(B)$, ou $f^{\zeta\zeta\boxtimes}(f)$), mais nous préférons utiliser la notation $f^{-1}(B)$ rencontrée le plus souvent. Si l'on sait de quoi l'on parle il n'y a pas de véritable problème, il s'agit seulement d'une notation.

On vérifie facilement le résultat suivant.

Théorème 1.6.

Soient E, F, G des ensembles, f une application de E dans F et g une application de F dans G .

1. Si f et g sont injectives, alors $g \circ f$ est injective (la composée de deux injections est une injection).
2. Si f et g sont surjectives, alors $g \circ f$ est surjective (la composée de deux surjections est une surjection).
3. Si f et g sont bijectives, alors $g \circ f$ est bijective (la composée de deux injections est une bijection) et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Preuve.

1. Supposons f et g injectives. Si $g \circ f(x_1) = g \circ f(x_2)$, alors $g(f(x_1)) = g(f(x_2))$, donc $f(x_1) = f(x_2)$ puisque g est injective et $x_1 = x_2$ puisque f est injective.
2. Supposons f et g surjectives. Pour tout $z \in G$, il existe $y \in F$ tel que $z = g(y)$ puisque g est surjective et $y \in F$ s'écrit $y = f(x)$ avec $x \in E$ puisque f est surjective. On a donc $z = g \circ f(x)$ avec $x \in E$. L'application $g \circ f$ est donc surjective. De manière plus compacte, on peut écrire que :

$$(g \circ f)(E) = g(f(E)) = g(F) = G.$$

3. Les deux premiers points nous disent que $g \circ f$ est bijective si f et g le sont. Puis avec $(f^{-1} \circ g^{-1}) \circ g \circ f = f^{-1} \circ Id_F \circ f = f^{-1} \circ f = Id_E$, on déduit que $f^{-1} \circ g^{-1}$ est l'inverse de $g \circ f$.

□

Le résultat qui suit peut parfois être utile pour montrer l'injectivité, la surjectivité ou la bijectivité d'une application.

Théorème 1.7.

Soient E, F deux ensembles et f une application de E dans F .

1. *S'il existe une application g de F dans E telle que $g \circ f = Id_E$, alors f est injective.*
2. *S'il existe une application h de F dans E telle que $f \circ h = Id_F$, alors f est surjective.*
3. *S'il existe deux applications g et h de F dans E telles que $g \circ f = Id_E$ et $f \circ h = Id_F$, alors f est bijective et $g = h = f^{-1}$.*

Preuve.

1. Si x, x' dans E sont tels que $f(x) = f(x')$, alors $x = g \circ f(x) = g \circ f(x') = x'$ et f est injective.
2. Pour tout $y \in F$, on a $y = (f \circ h)(y) = f(h(y))$ avec $x = h(y) \in E$, donc f est surjective.
3. Les deux premiers points nous disent que f est bijective et de $g \circ f = Id_E$, on déduit que $f^{-1} = (g \circ f) \circ f^{-1} = g$. De même $h = g^{-1}$.

□

1.9 Relations d'ordre et d'équivalence

On se donne un ensemble non vide E et une propriété \mathcal{P} sur les éléments (x, y) de E^2 . On dit que x et y dans E sont en relation, ce que l'on notera $x\mathcal{R}y$, si le couple (x, y) vérifie la propriété \mathcal{P} . On dit que \mathcal{R} est une relation sur E .

Définition 1.8. *On dit que \mathcal{R} est une relation d'ordre sur E , si elle vérifie les propriétés suivantes :*

- *réflexivité : pour tout $x \in E$, on a $x\mathcal{R}x$;*
- *anti-symétrie : si x, y dans E sont tels que $x\mathcal{R}y$ et $y\mathcal{R}x$, on a alors $x = y$;*
- *transitivité : si x, y, z dans E sont tels que $x\mathcal{R}y$ et $y\mathcal{R}z$, on a alors $x\mathcal{R}z$.*

Définition 1.9. *Un ensemble E muni d'une relation d'ordre est dit ordonné.*

Définition 1.10. *Si \mathcal{R} est une relation d'ordre sur E telle que deux éléments quelconques de E sont comparables, c'est-à-dire que pour tous x, y*

dans E , on a $x\mathcal{R}y$ ou $y\mathcal{R}x$, on dit alors que l'ensemble E est totalement ordonné ou que \mathcal{R} est une relation d'ordre total sur E .

Exemples 1.1

1. Les ensembles \mathbb{N} , \mathbb{Z} , \mathbb{Q} et \mathbb{R} sont totalement ordonnés par la relation \leq .
2. La relation de divisibilité est une relation d'ordre total sur $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$, mais ce n'est pas une relation d'ordre sur $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$.
3. La relation d'inclusion \subset est une relation d'ordre sur l'ensemble $\mathcal{P}(E)$ des parties de E .

Définition 1.11. On dit que \mathcal{R} est une relation d'équivalence sur E , si elle vérifie les propriétés suivantes :

- réflexivité : pour tout $x \in E$, on a $x\mathcal{R}x$;
- symétrie : si x, y dans E sont tels que $x\mathcal{R}y$, on a alors $y\mathcal{R}x$;
- transitivité : si x, y, z dans E sont tels que $x\mathcal{R}y$ et $y\mathcal{R}z$, on a alors $x\mathcal{R}z$.

Exemple 1.3 Soient E, F deux ensembles et φ une application de E dans F . La relation \mathcal{R} définie sur E par $x\mathcal{R}y$ si, et seulement si, on a $\varphi(x) = \varphi(y)$ est une relation d'équivalence. Pour $F = E$ et $\varphi = Id$, on a la relation d'égalité.

Si \mathcal{R} est une relation d'équivalence sur E , on note pour tout $x \in E$:

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

un tel ensemble est non vide car il contient x (propriété de symétrie) et on dit que c'est la classe d'équivalence de x . L'ensemble de toutes ces classes d'équivalence est appelé l'ensemble quotient de E par \mathcal{R} et noté E/\mathcal{R} .

Il est facile de vérifier que l'application :

$$\begin{aligned} \pi : E &\rightarrow E/\mathcal{R} \\ x &\mapsto \bar{x} \end{aligned}$$

est surjective. On dit que c'est la surjection canonique de E sur E/\mathcal{R} .

Théorème 1.8.

Si \mathcal{R} est une relation d'équivalence sur E , ses classes d'équivalence forment alors une partition de E , c'est-à-dire que $E = \bigcup_{C \in E/\mathcal{R}} C$.

Preuve. Toute classe d'équivalence est dans E , donc $\bigcup_{C \in E/\mathcal{R}} C \subset E$ et tout $x \in E$ appartient à $C = \bar{x}$, donc $E \subset \bigcup_{C \in E/\mathcal{R}} C$ et on a l'égalité. Soient C et C' deux classes

d'équivalence distinctes. Si $C \cap C' \neq \emptyset$, il existe alors $x \in C \cap C'$ avec $C = \bar{y}$ et $C' = \bar{z}$ pour deux éléments y et z de E , ce qui implique que $x\mathcal{R}y$ et $x\mathcal{R}z$ et donc que $y\mathcal{R}z$ par symétrie et transitivité, mais cela implique que $C = C'$, ce qui n'est pas. En conclusion, on a la partition $E = \bigcup_{C \in E/\mathcal{R}} C$. \square

1.10 Exercices

Exercice 1.1. Montrer que les assertions $P \rightarrow Q$ et $\bar{P} \vee Q$ sont équivalentes, ainsi que les assertions $\bar{P} \rightarrow \bar{Q}$ et $P \wedge \bar{Q}$.

Solution. Ces deux assertions ont même table de vérité.

P	Q	\bar{P}	$\bar{P} \vee Q$	$P \rightarrow Q$
V	V	F	V	V
V	F	F	F	F
F	V	V	V	V
F	F	V	V	V

,

P	Q	$P \wedge \bar{Q}$	$\bar{P} \rightarrow \bar{Q}$
V	V	F	F
V	F	V	V
F	V	F	F
F	F	F	F

Exercice 1.2. Montrer que les assertions $P \leftrightarrow P$, $(P \wedge Q) \rightarrow P$, $P \rightarrow (P \vee Q)$, $P \vee (P \rightarrow Q)$, $P \rightarrow (Q \rightarrow P)$ et $((P \rightarrow Q) \rightarrow P) \rightarrow P$ sont des tautologies (i. e. toujours vraies).

Solution. Pour $P \leftrightarrow P$, $(P \wedge Q) \rightarrow P$, $P \rightarrow (P \vee Q)$, c'est évident et pour les autres, on utilise la table de vérité :

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

Exercice 1.3. Simplifier l'expression $R = (\bar{P} \wedge Q) \vee (\bar{P} \wedge \bar{Q}) \vee (P \wedge Q)$.

Solution. En utilisant les tables de vérité, on a :

P	Q	$\bar{P} \wedge Q$	$\bar{P} \wedge \bar{Q}$	$(\bar{P} \wedge Q) \vee (\bar{P} \wedge \bar{Q})$	$P \wedge Q$	R
V	V	F	F	F	V	V
V	F	F	F	F	F	F
F	V	V	F	V	F	V
F	F	F	V	V	F	V

Donc R a la même table de vérité que $P \rightarrow Q$, ce qui signifie que R est équivalent à $P \rightarrow Q$.

Exercice 1.4. On dit qu'une théorie est non contradictoire si $P \wedge \bar{P}$ est faux pour toute proposition P . Montrer que si dans une théorie une propriété P est contradictoire, c'est-à-dire si $P \wedge \bar{P}$ est vraie, alors $Q \wedge \bar{Q}$ est vraie pour toute propriété Q .

Solution. Nous allons montrer que s'il existe un énoncé contradictoire P , alors tout énoncé Q est vrai, donc \bar{Q} aussi et $Q \wedge \bar{Q}$ est vraie. On vérifie tout d'abord que $R = \bar{P} \rightarrow (P \rightarrow Q)$ est une tautologie avec la table de vérité :

P	Q	\bar{P}	$P \rightarrow Q$	$\bar{P} \rightarrow (P \rightarrow Q)$
V	V	F	V	V
V	F	F	F	V
F	V	V	V	V
F	F	V	V	V

Comme R et \bar{P} sont vraies, $P \rightarrow Q$ est vraie et Q est vraie puisque P est vraie.

Exercice 1.5. En raisonnant par l'absurde, montrer que $\sqrt{2}$ et $\frac{\ln(2)}{\ln(3)}$ sont irrationnels.

Solution. Supposons que $\sqrt{2} = \frac{p}{q}$ avec p, q entiers naturels non nuls premiers entre eux. On a alors $p^2 = 2q^2$ qui entraîne que p est pair, soit $p = 2p'$ et $q^2 = 2p'^2$ entraîne q pair, ce qui contredit p et q premiers entre eux. Supposons que l'on ait $\frac{\ln(2)}{\ln(3)} = \frac{p}{q}$ avec p, q entiers naturels non nuls premiers entre eux. On a alors $\ln(2^q) = \ln(3^p)$ et $2^p = 3^q$, ce qui est impossible puisque 2^p est un entier pair et 3^q est un entier impair.

Exercice 1.6. Soit n un entier naturel non carré, c'est-à-dire ne s'écrivant pas sous la forme $n = p^2$ avec p entier. En raisonnant par l'absurde et en utilisant le théorème de Bézout, montrer que \sqrt{n} est irrationnel.

Solution. Si n est non carré, on a alors $n \geq 2$. Supposons que $\sqrt{n} = \frac{p}{q}$ avec p, q premiers entre eux dans \mathbb{N}^* . Le théorème de Bézout nous dit qu'il existe un couple (u, v) d'entiers relatifs tels que $up + vq = 1$. On a alors :

$$1 = (up + vq)^2 = u^2p^2 + 2uvpq + v^2q^2$$

avec $u^2p^2 = u^2nq^2$. L'égalité précédente s'écrit alors $qr = 1$ avec $r = u^2nq + 2uvp + v^2q$ dans \mathbb{Z} , ce qui implique que $q = 1$ et $\sqrt{n} = p$, en contradiction avec n non carré.

Exercice 1.7. Montrer que $P_n = \prod_{k=1}^n \left(1 + \frac{1}{k}\right)^k = \frac{(n+1)^n}{n!}$ pour tout $n \in \mathbb{N}^*$.

Solution. Il revient au même de calculer $S_n = \ln(P_n)$. On a :

$$\begin{aligned} S_n &= \ln \left(\prod_{k=1}^n \left(\frac{k+1}{k} \right)^k \right) = \sum_{k=1}^n (k \ln(k+1) - k \ln(k)) \\ &= \sum_{k=1}^n k \ln(k+1) - \sum_{k=1}^n k \ln(k) \end{aligned}$$

et le changement d'indice $j = k + 1$ dans la première somme donne :

$$\begin{aligned} S_n &= \sum_{j=2}^{n+1} (j-1) \ln(j) - \sum_{k=1}^n k \ln(k) = \sum_{j=2}^{n+1} j \ln(j) - \sum_{j=2}^{n+1} \ln(j) - \sum_{k=1}^n k \ln(k) \\ &= \sum_{k=2}^{n+1} k \ln(k) - \sum_{k=2}^{n+1} \ln(k) - \sum_{k=1}^n k \ln(k) = (n+1) \ln(n+1) - \sum_{k=2}^{n+1} \ln(k) \end{aligned}$$

(on a utilisé le fait que l'indice est muet dans une somme). On a donc en définitive :

$$\begin{aligned} S_n &= \ln(P_n) = \ln \left((n+1)^{n+1} \right) - \sum_{k=2}^{n+1} \ln(k) \\ &= \ln \left((n+1)^{n+1} \right) - \ln \left(\prod_{k=2}^n k \right) = \ln \left((n+1)^{n+1} \right) - \ln(n!) = \ln \left(\frac{(n+1)^{n+1}}{n!} \right) \end{aligned}$$

et $P_n = \frac{(n+1)^n}{n!}$.

Exercice 1.8. Montrer que si φ est une fonction strictement croissante de \mathbb{N} dans \mathbb{N} , on a alors $\varphi(n) \geq n$ pour tout n .

Solution. Comme φ est une fonction de \mathbb{N} dans \mathbb{N} , $\varphi(0)$ est un entier naturel et donc $\varphi(0) \geq 0$. Supposant le résultat acquis pour $n \geq 0$, sachant que φ est strictement croissante, on a $\varphi(n+1) > \varphi(n) \geq n$, donc $\varphi(n+1) > n$, ce qui équivaut à $\varphi(n+1) \geq n+1$ puisque $\varphi(n+1)$ est un entier.

Exercice 1.9. Montrer par récurrence que pour tout entier naturel non nul n , on a :

$$U_n = \sum_{k=1}^n k = \frac{n(n+1)}{2}, \quad V_n = \sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6},$$

$$W_n = \sum_{k=1}^n k^3 = \left(\frac{n(n+1)}{2}\right)^2 = U_n^2$$

Solution. Pour $n = 1$ c'est clair. En supposant les résultats acquis pour $n \geq 1$, on a :

$$U_{n+1} = \frac{n(n+1)}{2} + n + 1 = \frac{n^2 + 3n + 2}{2} = \frac{(n+1)(n+2)}{2}$$

$$V_{n+1} = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \frac{(n+1)(2n^2 + 7n + 6)}{6}$$

$$= \frac{(n+1)(n+2)(2n+3)}{6}$$

$$W_{n+1} = \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 = \left(\frac{(n+1)(n+2)}{2}\right)^2$$

On a aussi $U_n = 1 + 2 + \dots + (n-1) + n = n + (n-1) + \dots + 2 + 1$ et en additionnant terme à terme on obtient $2U_n = n(n+1)$. Le calcul de U_n peut aussi se faire en passant par V_{n+1} et en utilisant l'identité $(k+1)^2 = k^2 + 2k + 1$. Précisément, en effectuant le changement d'indice $k = j + 1$, on a :

$$V_{n+1} = \sum_{k=1}^{n+1} k^2 = \sum_{j=0}^n (j+1)^2 = \sum_{j=0}^n j^2 + 2 \sum_{j=0}^n j + \sum_{j=0}^n 1$$

soit $V_{n+1} = V_n + 2U_n + n + 1$ et :

$$2U_n = V_{n+1} - V_n - (n+1) = (n+1)^2 - (n+1) = n(n+1)$$

ce qui donne bien $U_n = \frac{n(n+1)}{2}$. De même, le calcul de V_n peut aussi se faire en passant par W_{n+1} et en utilisant l'identité $(k+1)^3 = k^3 + 3k^2 + 3k + 1$. Précisément, en effectuant le changement d'indice $k = j + 1$, on a :

$$W_{n+1} = \sum_{k=1}^{n+1} k^3 = \sum_{j=0}^n (j+1)^3 = \sum_{j=0}^n j^3 + 3 \sum_{j=0}^n j^2 + 3 \sum_{j=0}^n j + \sum_{j=0}^n 1$$

soit $W_{n+1} = W_n + 3V_n + 3U_n + n + 1$ et :

$$3V_n = W_{n+1} - W_n - 3U_n - (n+1) = (n+1)^3 - 3 \frac{n(n+1)}{2} - (n+1)$$

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

ce qui donne bien $V_n = \frac{n(n+1)(2n+1)}{6}$.

Exercice 1.10. Montrer que pour tout entier naturel n et tous nombres complexes a et b on a $b^{n+1} - a^{n+1} = (b - a) \sum_{k=0}^n a^k b^{n-k}$. En particulier, pour $a \neq 1$ et $b = 1$, on a $\sum_{k=0}^n a^k = \frac{a^{n+1} - 1}{a - 1}$.

Solution. Pour $n = 0$, c'est évident. En supposant le résultat acquis au rang $n \geq 0$, on a :

$$\begin{aligned} b^{n+2} - a^{n+2} &= (b^{n+1} - a^{n+1})b + ba^{n+1} - a^{n+2} \\ &= (b - a) \sum_{k=0}^n a^k b^{n+1-k} + (b - a)a^{n+1} \\ &= (b - a)(b^{n+1} + ab^n + \dots + a^{n-1}b^2 + a^n b) + (b - a)a^{n+1} \\ &= (b - a) \sum_{k=0}^{n+1} a^k b^{n+1-k} \end{aligned}$$

Le résultat est donc vrai pour tout $n \geq 0$.

Exercice 1.11. Montrer que pour tout entier naturel n et tous nombres complexes a et b on a $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$, où $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ pour k compris entre 0 et n avec la convention $0! = 1$ (formule du binôme de Newton).

Solution. Pour $n = 0$ et $n = 1$, c'est évident. En supposant le résultat acquis au rang $n \geq 1$, on a :

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

et tenant compte de $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ (triangle de Pascal), cela s'écrit :

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

Le résultat est donc vrai pour tout $n \geq 0$.

Exercice 1.12. Montrer par récurrence, que pour tout entier naturel non nul n et tout nombre complexe λ différent de 1, on a :

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

Solution. Pour $n = 1$, c'est clair. Si c'est vrai pour $n \geq 1$, alors :

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

Exercice 1.13. Soit x_1, \dots, x_n des réels dans $[0, 1]$. Montrer par récurrence que $\prod_{k=1}^n (1 - x_k) \geq 1 - \sum_{k=1}^n x_k$.

Solution. Notons $u_n = \prod_{k=1}^n (1 - x_k)$ et $v_n = 1 - \sum_{k=1}^n x_k$. Pour $n = 1$, on a $u_1 = v_1$. Supposant le résultat acquis au rang $n \geq 1$ et tenant compte de $1 - x_{n+1} \geq 0$, on a :

$$\begin{aligned} u_{n+1} &= u_n (1 - x_{n+1}) \geq \left(1 - \sum_{k=1}^n x_k\right) (1 - x_{n+1}) \\ &\geq 1 - \sum_{k=1}^n x_k - x_{n+1} + x_{n+1} \sum_{k=1}^n x_k \geq 1 - \sum_{k=1}^{n+1} x_k = v_{n+1} \end{aligned}$$

puisque tous les x_k sont positifs.

Exercice 1.14. Pour tout entier naturel n supérieur ou égal à 2, on note

$$H_n = \sum_{k=1}^n \frac{1}{k}.$$

1. Soit p un entier naturel non nul. Montrer que $H_{2p} = \frac{1}{2}H_p + \frac{a}{2b+1}$ où a, b sont des entiers naturels avec a non nul.

2. Montrer par récurrence que pour tout entier naturel non nul H_n est le quotient d'un entier impair par un entier pair et qu'en conséquence ce n'est pas un entier.

Solution.

1. On a $H_{2p} = \sum_{k=1}^p \frac{1}{2k} + \sum_{k=0}^{p-1} \frac{1}{2k+1} = \frac{1}{2}H_p + \frac{N}{D}$ avec $D = \text{ppcm}(1, 3, \dots, 2p-1)$ qui est impair et N entier naturel non nul.

2. On a $H_2 = \frac{3}{2} \notin \mathbb{N}$. Supposons le résultat acquis au rang $n \geq 2$. Si $n = 2p$, on a alors :

$$H_{n+1} = H_n + \frac{1}{2p+1} = \frac{2a+1}{2b} + \frac{1}{2p+1} = \frac{(2a+1)(2p+1) + 2b}{2b(2p+1)} = \frac{2a'+1}{2b'}$$

avec $a' = a + b + p + 2ap$ et $b' = b(2p+1)$. Si $n = 2p+1$, on a alors :

$$\begin{aligned} H_{n+1} &= H_{2(p+1)} = \frac{c}{2d+1} + \frac{1}{2}H_{p+1} \\ &= \frac{c}{2d+1} + \frac{1}{2} \frac{2a+1}{2b} = \frac{4bc + (2d+1)(2a+1)}{4b(2d+1)} = \frac{2a'+1}{2b'} \end{aligned}$$

avec $a' = a + d + 2ad + 2bc$ et $b' = 2b(2d+1)$. Dans tous les cas, H_n est le quotient d'un entier impair par un entier pair et en conséquence, ce n'est pas un entier.

Exercice 1.15. Simplifier les expressions suivantes, où A et B sont des sous-ensembles d'un ensemble E :

1. $C = (\overline{A \cap B}) \cup (\overline{A \cap \overline{B}}) \cup (A \cap B), \overline{C}.$

2. $D = \overline{\overline{\overline{\overline{A \cap \overline{B}} \cap (\overline{A \cap B}) \cup (A \cap B)} \cap (A \cap B)}}$

Solution.

1. Avec la distributivité de \cap sur \cup , on a :

$$\overline{A} = \overline{A \cap E} = \overline{A \cap (B \cup \overline{B})} = (\overline{A \cap B}) \cup (\overline{A \cap \overline{B}})$$

(on a mis \overline{A} en facteur) et avec la distributivité de \cup sur \cap , on a :

$$C = \overline{A} \cup (A \cap B) = (\overline{A} \cup A) \cap (\overline{A} \cup B) = E \cap (\overline{A} \cup B) = \overline{A} \cup B$$

$$\overline{C} = A \cap \overline{B}.$$

2. En posant :

$$X = A \cap \overline{B}, Y = \overline{X} \cap (\overline{A \cap B}), Z = \overline{Y} \cup (A \cap B), T = \overline{Z} \cap (A \cap B)$$

Algèbre et géométrie pour la Licence

Parfaitement adapté à la diversité des parcours scientifiques universitaires, ce manuel couvre l'ensemble des programmes d'algèbre et de géométrie enseignés en première et en deuxième années de licence mathématiques.

Il ne s'agit pas d'un manuel de « méthodes » où l'on sacrifie la notion de rigueur qui est l'essence même des mathématiques. Les notions étudiées ici le sont de façon rigoureuse en démontrant tous les résultats énoncés. Les 12 chapitres sont consacrés à l'étude de quelques notions de logique et de théorie des ensembles, des structures de groupe, d'anneaux et de corps, en se concentrant sur l'anneau des entiers relatifs, le corps des nombres complexes, l'anneau des polynômes à coefficients réels ou complexes, les principales notions d'algèbre linéaire et bilinéaire avec la réduction des endomorphismes et des formes quadratiques ainsi qu'à quelques notions d'arithmétique. Bibliographie sélective et index viennent compléter l'ensemble.

1. Éléments de logique et de théorie des ensembles
 2. Structure de groupe
 3. Structures d'anneau et de corps
 4. Division euclidienne dans \mathbb{Z}
 5. Le corps \mathbb{C} des nombres complexes
 6. Espaces vectoriels réels ou complexes
 7. Espaces vectoriels réels ou complexes de dimension finie
 8. Opérations élémentaires et déterminants
 9. Polynômes à coefficients réels ou complexes
 10. Réduction des endomorphismes
 11. Formes bilinéaires et quadratiques réelles ou complexes
 12. Espaces préhilbertiens
- Bibliographie – Index

LES PLUS

- Cours rédigé avec démonstration systématique des résultats énoncés
- Chaque théorème est suivi d'une série d'applications
- Tous les exercices sont intégralement corrigés

Docteur en mathématiques, professeur agrégé à l'université Grenoble-Alpes, **Marie-Cécile Darracq** enseigne les mathématiques en Licence. Membre du jury du Capes externe de 2006 à 2009, puis de l'agrégation interne depuis 2010, elle est directrice des études du Département Sciences Drôme-Ardèche de l'université Grenoble-Alpes.

Agrégé de mathématiques, **Jean-Étienne Rombaldi** a enseigné à l'université Grenoble-Alpes, institut Fourier. Membre du jury du CAPES externe et de l'agrégation interne de mathématiques pendant plusieurs années, il a été responsable de la préparation à l'agrégation interne de l'université de Grenoble et préparateur à l'agrégation interne et externe de cette même université ainsi que pour le CNED.

ISBN : 978-2-8073-3221-8



9 782807 332218

deboeck **B**
SUPÉRIEUR

www.deboecksuperieur.com