MARIE-CÉCILE DARRACQ • JEAN-ÉTIENNE ROMBALDI

Mathématiques pour le Capes

Algèbre et géométrie

CAPES EXTERNE
MATHÉMATIQUES

- Cours complet
- Plus de 200 exercices et problèmes
- Tous les corrigés détaillés

deboeck SUPÉRIEUR

MARIE-CÉCILE DARRACQ • JEAN-ÉTIENNE ROMBALDI

Mathématiques pour le Capes

Algèbre et géométrie

deboeck SUPÉRIEUR

Chez le même éditeur (extrait du catalogue)

Pour le Capes :

Darracq M.-C., Rombaldi J.-É., *Mathématiques pour le Capes. Probabilités* (nouveauté 2021)
Darracq M.-C., Rombaldi J.-É., *Mathématiques pour le Capes. Analyse*

Pour l'agrégation :

Dantzer J.-F., *Mathématiques pour l'agrégation. Analyse et probabilités* – 2e édition (nouveauté 2021)
Rombaldi J.-É., *Mathématiques pour l'agrégation. Algèbre et géométrie* – 2e édition (nouveauté 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 nautile © 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 : 2021/13647/106
Bibliothèque nationale, Paris : juillet 2021
ISBN : 978-2-8073-3222-5

Sommaire

Table des matières

Avant-propos

Ce cours d'algèbre s'adresse aux étudiants préparant le Capes de mathématiques. 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. C'est ce type d'exercices qu'il est utile de savoir faire avant de travailler sur des épreuves écrites du concours.

Ce deuxième volume est consacré aux notions d'algèbre habituellement enseignées en première et deux année 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. Le dernier chapitre est consacré à quelques épreuves d'algèbre et de géométrie du Capes, le niveau d'exigence pour cette épreuve ne dépassant pas le niveau de connaissance acquis en première et deuxième année d'université ou de classe préparatoire aux grandes écoles. Pour les notions de géométrie utiles dans certains problèmes de Capes, on se reportera à l'excellent livre de Dany Jacque Mercier : Cours de géométrie, préparation au CAPES et à l'agrégation. Les problèmes de Capes étant souvent trop longs pour être traités en cinq heures, à titre d'entrainement, on peut se contenter de travailler sur les deux premières parties d'un problème, la suite du problème pouvant être étudiée par la suite à titre d'approfondissement. Nous espérons que ce travail sera utile aux candidats au Capes.

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

Pour conclure, nous tenons à remercier les éditions De Boeck et en particulier Alain Luguet 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 à 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-Fränkel.

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 $a, b, c, \cdots$ pour des objets fixés ;

— les lettres minuscules $x, y, z, t, \cdots$ pour des objets inconnus à déterminer ;

— les lettres majuscules $E, F, G, H, \cdots$ pour des ensembles ;

— des lettres de l'alphabet grecques minuscules ou majuscules $\alpha, \beta, \varepsilon, \delta, \cdots$ $\Lambda, \Gamma, \Omega, \cdots$

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 vrais 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 $P \to Q$, 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 $P \to Q$ 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 $P \to Q$ 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 $P \to Q$ et $Q \to P$ sont toutes deux vraies. Dans le cas où $P \leftrightarrow Q$ est vraie on dit que P est 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	$\overline{P}$	$P \wedge Q$	$P \vee Q$	$P \to Q$	$P \leftrightarrow Q$
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

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

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 :

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

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

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

Les équivalences $\left(\overline{P \wedge Q}\right) \Leftrightarrow \left(\overline{P} \vee \overline{Q}\right)$ et $\left(\overline{P \vee Q}\right) \Leftrightarrow \left(\overline{P} \wedge \overline{Q}\right)$ 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 $\overline{H \to C}$ et on montre qu'on aboutit à une impossibilité si cette dernière assertion est vraie (pratiquement, on suppose que la conclusion est fausse avec les hypothèses et on aboutit à une absurdité). Il en résulte alors que $\overline{H \to C}$ est fausse, c'est-à-dire que $H \to C$ est vraie, soit $H \Rightarrow C$.
- On peut aussi essayer de montrer la contraposée $\overline{C} \Rightarrow \overline{H}$ puisque les implications $H \to C$ et $\overline{C} \to \overline{H}$ sont équivalentes.
- La démonstration par contre-exemple permet de montrer qu'une implication $H \to C$, où H est C sont des propriétés portant sur des variables x, est fausse. Pour ce faire on cherche une ou des valeurs de x pour lesquels $H(x)$ est vraie et $C(x)$ est fausse.

— 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 $E = \{x_1, x_2, \cdots, x_n\}$ s'il s'agit d'un ensemble fini ou $E = \{x_1, x_2, \cdots, x_n, \cdots\}$ 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 $\{n, \cdots, m\}$. 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 $\{n, n+1, \cdots, m\}$ 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 équivalent 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 :

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

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

La négation de l'assertion 1.1 est $(\exists x \in E) \mid \left(\overline{P(x)}\right)$ en utilisant le symbole $\mid$ 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 $(\forall x \in E)\ \left(\overline{P(x)}\right)$.

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 écrirons :

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

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 :

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

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 :

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

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

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 $x_1, x_2, \cdots, x_n$ des entiers, rationnels, réels ou complexes, on notera :

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

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 :

$$\sum_{k=1}^{n} x_k + \sum_{k=1}^{n} y_k = \sum_{k=1}^{n} (x_k + y_k),\ \lambda \sum_{k=1}^{n} x_k = \sum_{k=1}^{n} \lambda x_k$$

$$\left(\sum_{k=1}^{n} x_k\right)\left(\sum_{k=1}^{m} y_k\right) = \left(\sum_{j=1}^{n} x_j\right)\left(\sum_{k=1}^{m} y_k\right) = \sum_{\substack{1 \leq j \leq n \\ 1 \leq k \leq m}} x_j y_k$$

Pour vérifier ce dernier résultat, on écrit que :

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

1.6 Les théorèmes de récurrence

On désigne par $\mathbb{N}$ l'ensemble des entiers naturels, soit $\mathbb{N} = \{0, 1, 2, \cdots, n, \cdots\}$. 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 $n \geq n_0$. □

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 $n \geq n_0$. □

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 $u_0, u_1, \cdots, u_p$ et une relation $u_{n+1} = f\left(u_n, \cdots, u_{n-(p-1)}\right)$ 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 $A, B, C, \cdots$ 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 :

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

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 $\overline{A} = E \setminus A$.

— 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 W 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 $A, B, C, \cdots$ 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 :*

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

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

3. *distributivité :*

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

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

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

Preuve. 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 $A_1, A_2, \cdots, A_n$ de E par :

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

et :

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

De façon condensée, on écrira $(A_k)_{1 \leq k \leq n}$ une telle famille de sous ensembles de E, $\bigcap_{k=1}^{n} A_k = A_1 \cap A_2 \cap \cdots \cap A_n$ l'intersection et $\bigcup_{k=1}^{n} A_k = A_1 \cup A_2 \cup \cdots \cup A_n$ 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 $E_1 \times E_2 \times \cdots \times E_n$ de n ensembles comme l'ensemble des listes (ordonnées) $(x_1, x_2, \cdots, x_n)$ formées d'un élément x_1 de E_1 suivi d'un élément x_2 de E_2, $\cdots$, suivi d'un élément x_n de E_n. On notera de façon condensé $\prod_{k=1}^{n} E_k = E_1 \times \cdots \times E_n$.

Là encore, on a $(x_1, x_2, \cdots, x_n) = (x'_1, x'_2, \cdots, x'_n)$ 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 $E \times E \times \cdots \times E$ (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 :

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

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

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

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. $f^{-1}\left(\overline{C}\right) = \overline{f^{-1}(C)}$

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 $x_1 = x_2$. □

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 ou 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 $f_1 \circ f_2 \circ \cdots \circ f_n$ 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 on deux images distinctes dans F, soit :*

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

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 y 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 y a un unique antécédent par f, encore équivalent à dire que pour 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 :

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

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 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 $f^{\zeta\xi\Diamond\boxtimes}(f)$), mais nous préfèrons 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 $z = g \circ f(x_1)$ 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 $\left(f^{-1} \circ g^{-1}\right) \circ g \circ f = f^{-1} \circ Id_F \circ f = f^{-1} \circ f = Id_E$, 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 $x\mathcal{R}y$;*
- *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 $x\mathcal{R}y$;*
- *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 $x \in E$:

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

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 :

$$\begin{array}{rccc} \pi : & E & \to & E/\mathcal{R} \\ & x & \mapsto & \overline{x} \end{array}$$

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 $C = \overline{x}$, donc $E \subset \bigcup_{C \in E/\mathcal{R}} C$ et on a l'égalité. Soient C et C' deux clases

d'équivalence distinctes. Si $C \cap C' \neq \emptyset$, il existe alors $x \in C \cap C'$ avec $C = \overline{y}$ et $C' = \overline{z}$ 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 $E = \bigcup_{C \in E/\mathcal{R}} C$. □

1.10 Exercices

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

Solution. Ces deux assertions ont même table de vérité.

P	Q	$\overline{P}$	$\overline{P} \vee Q$	$P \to Q$
V	V	F	V	V
V	F	F	F	F
F	V	V	V	V
F	F	V	V	V

,

P	Q	$P \wedge \overline{Q}$	$\overline{P \to Q}$
V	V	F	F
V	F	V	V
F	V	F	F
F	F	F	F

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

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

P	Q	$P \to Q$	$Q \to P$	$P \vee (P \to Q)$	$P \to (Q \to P)$	$((P \to Q) \to P) \to P$
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 $R = \left(\overline{P} \wedge Q\right) \vee \left(\overline{P} \wedge \overline{Q}\right) \vee (P \wedge Q)$.*

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

P	Q	$\overline{P} \wedge Q$	$\overline{P} \wedge \overline{Q}$	$\left(\overline{P} \wedge Q\right) \vee \left(\overline{P} \wedge \overline{Q}\right)$	$P \wedge Q$	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 $P \to Q$, ce qui signifie que R est équivalent à $P \to Q$.

Exercice 1.4. *On dit qu'une théorie est non contradictoire si $P \wedge \overline{P}$ est faux pour toute proposition P. Montrer que si dans une théorie une propriété P est contradictoire, c'est-à-dire si $P \wedge \overline{P}$ est vraie, alors $Q \wedge \overline{Q}$ 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 $\overline{Q}$ aussi et $Q \wedge \overline{Q}$ est vraie. On vérifie tout d'abord que $R = \overline{P} \to (P \to Q)$ est une tautologie avec la table de vérité :

P	Q	$\overline{P}$	$P \to Q$	$\overline{P} \to (P \to Q)$
V	V	F	V	V
V	F	F	F	V
F	V	V	V	V
F	F	V	V	V

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

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

Solution. Supposons que $\sqrt{2} = \dfrac{p}{q}$ 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 $\dfrac{\ln(2)}{\ln(3)} = \dfrac{p}{q}$ 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 $\sqrt{n} = \dfrac{p}{q}$ 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 :

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

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

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

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

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

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

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 :*

$$U_n = \sum_{k=1}^{n} k = \frac{n\,(n+1)}{2},\ V_n = \sum_{k=1}^{n} k^2 = \frac{n\,(n+1)\,(2n+1)}{6},$$
$$W_n = \sum_{k=1}^{n} k^3 = \left(\frac{n\,(n+1)}{2}\right)^2 = U_n^2$$

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

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

$$V_{n+1} = \frac{n\,(n+1)\,(2n+1)}{6} + (n+1)^2 = \frac{(n+1)\left(2n^2+7n+6\right)}{6}$$
$$= \frac{(n+1)\,(n+2)\,(2n+3)}{6}$$

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

On a aussi $U_n = 1+2+\cdots+(n-1)+n = n+(n-1)+\cdots+2+1$ 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 $U_n = \dfrac{n\,(n+1)}{2}$. 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 $V_n = \dfrac{n\,(n+1)\,(2n+1)}{6}$.

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

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

$$\begin{aligned} b^{n+2} - a^{n+2} &= \left(b^{n+1} - a^{n+1}\right) b + b a^{n+1} - a^{n+2} \\ &= (b-a) \sum_{k=0}^{n} a^k b^{n+1-k} + (b-a)\, a^{n+1} \\ &= (b-a) \left(b^{n+1} + a b^n + \cdots + a^{n-1} b^2 + a^n b\right) + (b-a)\, a^{n+1} \\ &= (b-a) \sum_{k=0}^{n+1} a^k b^{n+1-k} \end{aligned}$$

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 $(a+b)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$, où $\displaystyle\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$ 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 :

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

Exercice 1.13. *Soit $x_1,\cdots,x_n$ 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 $D = \text{ppcm}\,(1, 3, \cdots, 2p-1)$ 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. $C = \left(\overline{A} \cap B\right) \cup \left(\overline{A} \cap \overline{B}\right) \cup (A \cap B)\,,\ \overline{C}$.
2. $D = \overline{\overline{\overline{A \cap \overline{B}} \cap \left(\overline{A} \cap B\right)} \cup (A \cap B)} \cap (A \cap B)$

Solution.

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

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

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

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

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

2. En posant :

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

on a :

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

avec $\left(A \cup \overline{B}\right) \cup \left(\overline{A} \cup \overline{B}\right) = E$, donc $D = E$.

Exercice 1.16. *Soient $A_1, \cdots, A_p$ des ensembles deux à deux distincts. Montrer que l'un de ces ensembles ne contient aucun des autres.*

Solution. On raisonne par l'absurde, c'est-à-dire qu'on suppose que chacun des ensembles A_k contient un ensemble A_j différent de A_k. Donc A_1 contient un ensemble $A_{j_1} \neq A_1$, soit $A_{j_1} \subsetneqq A_1$, A_{j_1} contient un ensemble $A_{j_2} \neq A_{j_1}$, soit $A_{j_2} \subsetneqq A_{j_1}$, et on peut continuer indéfiniment, ce qui est impossible puisque la famille d'ensembles est finie.

Exercice 1.17. *Que dire de 2 ensembles A, B tels que $A \cap B = A \cup B$?*

Solution. On a toujours $A \cap B \subset A \cup B$. Si de plus $A \cup B \subset A \cap B$, on a alors :

$$A \subset A \cup B \subset A \cap B \subset B \text{ et } B \subset A \cup B \subset A \cap B \subset A$$

ce qui donne $A = B$.

Exercice 1.18. *Soient A, B, C trois ensembles. Montrer que :*

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

Solution. On a $(A \cup B) \cap (B \cup C) = B \cup (A \cap C)$ et en notant $D = (A \cup B) \cap (B \cup C) \cap (C \cup A)$, on a :

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

Ou alors on part de $x \in D$ et on montre que $x \in E = (A \cap B) \cup (B \cap C) \cup (C \cap A)$, puis partant de $x \in E$, on montre que $x \in D$.

Exercice 1.19. *Soient E un ensemble et une application $f : \mathcal{P}(E) \to \mathbb{R}$ telle que pour toutes parties disjointes de E on ait :*

$$f(A \cup B) = f(A) + f(B)$$

Montrer que $f(\emptyset) = 0$, puis que pour toutes parties A, B de E, on a :

$$f(A \cup B) + f(A \cap B) = f(A) + f(B)$$

Pour E fini, la fonction f qui associe à une partie A de E son cardinal (c'est-à-dire le nombre de ses éléments) vérifie l'équation fonctionnelle de cet exercice.

Solution. On a $f(\emptyset) = f(\emptyset \cup \emptyset) = f(\emptyset) + f(\emptyset)$ dans $\mathbb{R}$, donc $f(\emptyset) = 0$. Avec les partitions $A \cup B = A \cup (B \setminus A)$ et $B = (A \cap B) \cup (B \setminus A)$, on a :

$$\begin{cases} f(A \cup B) = f(A) + f(B \setminus A) \\ f(B) = f(A \cap B) + f(B \setminus A) \end{cases}$$

et par soustraction $f(A \cup B) - f(B) = f(A) - f(A \cap B)$, ce qui donne le résultat.

Exercice 1.20. *Montrer qu'une application f strictement monotone de $\mathbb{R}$ dans $\mathbb{R}$ est injective.*

Solution. Supposons que f soit strictement croissante (au besoin on remplace f par $-f$). Si $x \neq y$, on a nécessairement $x > y$ ou $y > x$ et donc $f(x) > f(y)$ ou $f(x) < f(y)$, soit $f(x) \neq f(y)$ dans tous les cas.

Exercice 1.21. *Soit m un entier naturel. Montrer que s'il existe un entier naturel n et une injection φ de $E_n = \{1, \cdots, n\}$ dans $E_m = \{1, \cdots, m\}$, on a alors nécessairement $n \leq m$.*

Solution. On procède par récurrence sur $m \geq 0$. Si $m = 0$, on a alors $E_m = \emptyset$ et $E_n = \emptyset$ (en effet, si $E_n \neq \emptyset$, l'ensemble $f(E_n)$ est alors non vide et contenu dans l'ensemble vide, ce qui est impossible), donc $n = 0$. Supposons le résultat acquis pour $m \geq 0$. Soit φ une injection de E_n dans E_{m+1}. Si $n = 0$, on a bien $n \leq m+1$. Si $n \geq 1$, on distingue alors deux cas de figure :

- soit $\varphi(n) = m + 1$ et dans ce cas φ induit une bijection de E_{n-1} dans E_m (la restriction de φ à E_{n-1}) et $n - 1 \leq m$, soit $n \leq m + 1$;
- soit $\varphi(n) \neq m + 1$ et dans ce cas, en désignant par ψ l'application de E_{m+1} dans lui même définie par $\psi(\varphi(n)) = m + 1$, $\psi(m + 1) = \varphi(n)$ et $\psi(k) = k$ pour $k \in E_{m+1} \setminus \{\varphi(n), m + 1\}$, l'application $\psi \circ \varphi$ est injective de E_n dans E_{m+1} (composée de deux injections puisque φ est injective et ψ bijective) avec $\psi \circ \varphi(n) = m + 1$, ce qui nous ramène au cas précédent.

Exercice 1.22. *Soient n, m deux entiers naturels. Montrer que s'il existe une bijection φ de $E_n = \{1, \cdots, n\}$ sur $E_m = \{1, \cdots, m\}$, on a alors nécessairement $n = m$.*

Solution. On a $n \leq m$ puisque φ est une injection de E_n dans E_m et $m \leq n$ puisque φ^{-1} est une injection de E_m dans E_n, ce qui donne $n = m$.

Exercice 1.23. *Soient E, F deux ensembles et f une bijection de E sur F. Montrer que si g [resp. h] est une application de F sur E telle que $g \circ f = Id_E$ [resp. $f \circ h = Id_F$], alors g [resp. h] est bijective et $g = f^{-1}$ [resp. $h = f^{-1}$].*

Solution. Résulte de $g = (g \circ f) \circ f^{-1} = Id_E \circ f^{-1} = f^{-1}$ et $h = f^{-1} \circ (f \circ h) = f^{-1} \circ Id_F = f^{-1}$.

Exercice 1.24. *Soient E, F, G des ensembles, f une application de E dans F et g une application de F dans G. Montrer que :*

1. *si $g \circ f$ est injective, alors f est injective ;*
2. *si $g \circ f$ est surjective, alors g est surjective ;*
3. *si $g \circ f$ est surjective et g injective, alors f est surjective ;*
4. *Si $g \circ f$ est injective et f surjective, alors g est injective.*

Solution.

1. Si x, x' dans E sont tels que $f(x) = f(x')$, alors $g \circ f(x) = g \circ f(x')$ et $x = x'$ puisque $g \circ f$ est injective. L'application f est donc injective.
2. Pour tout z dans G, il existe x dans E tel que $z = g \circ f(x)$ puisque $g \circ f$ est surjective et en notant $y = f(x)$, on a $y \in F$ et $z = g(y)$, ce qui prouve que g est surjective.
3. Soit $y \in F$. Comme $g \circ f$ est surjective, il existe $x \in E$ tel que $z = g(y) = (g \circ f)(x) = g(f(x))$ et $y = f(x)$ si on suppose de plus que g est injective. En conséquence, f est surjective.
4. Soient y, y' dans F tels que $g(y) = g(y')$. Comme f est surjective, il existe x, x' dans E tels que $y = f(x)$ et $y' = f(x')$, ce qui donne $g \circ f(x) = g \circ f(x')$ et $x = x'$ puisque $g \circ f$ est injective, donc $y = y'$.

Exercice 1.25. *Soient m un entier naturel non nul et E un ensemble non vide. Montrer que s'il existe une surjection φ de $E_m = \{1, \cdots, m\}$ sur E, on peut alors construire une injection de E dans E_m. Pour $E = E_n = \{1, \cdots, n\}$, on a alors nécessairement $n \leq m$.*

Solution. Comme φ est surjective de E_m sur E, on a $\varphi^{-1}\{x\} \neq \emptyset$ pour tout $x \in E$ et chacun de ces sous-ensembles de E_m a un plus petit élément $j_x = \min \varphi^{-1}\{x\} \in E_m$, ce qui permet de définir l'application ψ de E dans E_m par $\psi(x) = j_x$. On a alors $\varphi \circ \psi(x) = \varphi(j_x) = x$ pour tout $x \in E$, c'est-à-dire que $\varphi \circ \psi = Id_E$ et l'application ψ est injective.

Exercice 1.26. *Soient E un ensemble et f une application de E dans E. Montrer que f est injective si, et seulement si, $f(A \cap B) = f(A) \cap f(B)$ pour toutes partie A et B de E.*

Solution. On a toujours $f(A \cap B) \subset f(A) \cap f(B)$ pour toutes partie A et B de E, que f soit injective ou pas. En effet un élément y de $f(A \cap B)$ s'écrit $y = f(x)$ avec $x \in A \cap B$ et donc $y \in f(A) \cap f(B)$. Réciproquement si $y \in f(A) \cap f(B)$, il existe $x \in A$ et $x' \in B$ tels que $y = f(x) = f(x')$ et dans le cas où f est injective, on a nécessairement $x = x' \in A \cap B$, donc $y \in f(A \cap B)$. On a donc $f(A \cap B) = f(A) \cap f(B)$ pour toutes partie A et B de E, si f est injective. Réciproquement supposons que $f(A \cap B) = f(A) \cap f(B)$ pour toutes partie A et B de E. Si f n'est pas injective, il existe $x \neq x'$ dans E tels que $f(x) = f(x')$ et :

$$\emptyset = f(\emptyset) = f(\{x\} \cap \{x'\}) = f(\{x\}) \cap f(\{x\}) = f(\{x\}) = \{f(x)\}$$

ce qui est impossible. Donc f est injective.

Exercice 1.27. *Soient E un ensemble et f une application de E dans E. Montrer que f est bijective si, et seulement si, $f\left(\overline{A}\right) = \overline{f(A)}$ pour toute partie A de E.*

Solution. Supposons f bijective. Un élément y de E est dans $f\left(\overline{A}\right)$ si, et seulement si, il s'écrit $y = f(x)$ où x est uniquement déterminé dans $\overline{A}$, ce qui implique $y \notin f(A)$ (sinon $y = f(x') = f(x)$ avec $x' \in A$ et $x = x' \in A$, ce qui contredit $x \in \overline{A}$). On a donc $f\left(\overline{A}\right) \subset \overline{f(A)}$. Si $y \notin f(A)$, il s'écrit $y = f(x)$ (f est bijective) et $x \notin A$, donc $y \in f\left(\overline{A}\right)$ .On a donc $\overline{f(A)} \subset f\left(\overline{A}\right)$ et $f\left(\overline{A}\right) = \overline{f(A)}$. Supposons que $f\left(\overline{A}\right) = \overline{f(A)}$ pour toute partie A de E. En particulier, on a $f(E) = f\left(\overline{\emptyset}\right) = \overline{f(\emptyset)} = \overline{\emptyset} = E$ et f est surjective. Si $x \neq x'$ dans E, en remarquant que $x' \in \overline{\{x\}}$, on a $f(x') \in f\left(\overline{\{x\}}\right) = \overline{\{f(x)\}}$ et $f(x) \neq f(x')$. Donc f est injective.

Exercice 1.28. *Soient E, F, G, H des ensembles, f une application de E dans F, g une application de F dans G et h une application de G dans H. Montrer que si $g \circ f$ et $h \circ g$ sont bijectives, alors f, g et h sont bijectives.*

Solution. Si $g \circ f$ est bijective, elle est alors surjective et il en est de même de g (exercice 1.24). Si $h \circ g$ est bijective, elle est alors injective et il en est de même de g (exercice 1.24). Donc g est bijective. Il en résulte que $f = g^{-1} \circ (g \circ f)$ et $h = (h \circ g) \circ g^{-1}$ sont bijectives comme composées.

Exercice 1.29. *On désigne par f l'application définie sur $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ par $f(n, m) = 2^n 3^m$. Montrer que f est injective. Il résulte que $\mathbb{N}^2$ est en*

bijection avec le sous ensemble $f\left(\mathbb{N}^2\right)$ de $\mathbb{N}$. Ce résultat se traduit en disant que $\mathbb{N}^2$ est dénombrable.

Solution. L'égalité $f(n,m) = f(n',m')$ avec (n,m) et (n',m') dans $\mathbb{N}^2$ équivaut à $2^n 3^m = 2^{n'} 3^{m'}$ et l'unicité de la décomposition en facteurs premiers d'un entier naturel non nul nous dit que $(n,m) = (n',m')$. L'application f est donc injective de $\mathbb{N}^2$ dans $\mathbb{N}$ et bijective de $\mathbb{N}^2$ dans $f\left(\mathbb{N}^2\right) \subset \mathbb{N}$.

Exercice 1.30. *Soient E un ensemble et A une partie de E. On définit une relation $\mathcal{R}$ sur $\mathcal{P}(E)$ par :*

$$(X \mathcal{R} Y) \Leftrightarrow (X \cup A = Y \cup A)$$

1. *Montrer que $\mathcal{R}$ est une relation d'équivalence.*
2. *Donner la classe d'équivalence de $X \in \mathcal{P}(E)$.*

Solution.

1. La relation est clairement réflexive, symétrique, transitive.
2. Soit $X \in \mathcal{P}(E)$. on a :

$$\left(Y \in \overline{X}\right) \Leftrightarrow (X \cup A = Y \cup A)$$

Pour tout $x \in Y \setminus A$, on a $x \in Y \cup A = X \cup A$ avec $x \notin A$, donc $x \in X \setminus A$. De même on montre que si $x \in X \setminus A$ alors $x \in Y \setminus A$. Ainsi $Y \setminus A = X \setminus A$. De plus $Y = (Y \setminus A) \cup (Y \cap A)$ donc $Y = (X \setminus A) \cup B$ avec $B \in \mathcal{P}(A)$. Inversement soit $Y = (X \setminus A) \cup B$ avec $B \in \mathcal{P}(A)$. On a :

$$Y \cup A = (X \setminus A) \cup A = X \cup A$$

Ainsi $\overline{X} = \{(X \setminus A) \cup B \mid B \in \mathcal{P}(A)\}$.

Exercice 1.31. *Soient $(X, \leq)$ et $(Y, \leq)$ deux ensembles ordonnés (on note abusivement les deux ordres de la même manière). On définit sur $X \times Y$ la relation $\mathcal{R}$ par :*

$$(x,y)\,\mathcal{R}\,(x',y') \Leftrightarrow (x < x') \text{ ou } (x = x' \text{ et } y \leq y')$$

Montrer que $\mathcal{R}$ est une relation d'ordre et qu'il est total si, et seulement si, X et Y sont totalement ordonnés.

Solution. $\mathcal{R}$ est clairement réflexive, antisymétrique et transitive. Pour l'ordre total, considérons deux couples (x,y) et (x',y'). Comme X et Y sont d'ordre total, il y a plusieurs cas :

— si $x < x'$, alors $(x,y)\,\mathcal{R}\,(x',y')$;

— si $x > x'$, alors $(x', y')\,\mathcal{R}\,(x, y)$;
— si $x = x'$ et $y < y'$, alors $(x, y)\,\mathcal{R}\,(x', y')$;
— si $x = x'$ et $y > y'$, alors $(x', y')\,\mathcal{R}\,(x, y)$;
— si $x = x'$ et $y = y'$, alors $(x', y') = (x, y)$ (et donc $(x, y)\,\mathcal{R}\,(x', y')$ et $(x', y')\,\mathcal{R}\,(x, y)$).

Tous les couples étant comparables on a une relation d'ordre total. Réciproquement, on vérifie que si $\mathcal{R}$ est total, il en est alors de même des ordres sur X et Y.

Chapitre 2

Structure de groupe

2.1 Loi de composition interne

Définition 2.1. *On appelle loi de composition interne sur un ensemble non vide G toute application φ définie sur $G \times G$ et à valeurs dans G.*

Si φ est loi de composition interne sur G, on notera souvent $a \star b = \varphi(a, b)$ pour tous a, b dans G. Il sera parfois commode de noter une telle loi sous la forme additive $(a, b) \mapsto a + b$ ou sous la forme multiplicative $(a, b) \mapsto a \cdot b$ ou plus simplement $(a, b) \mapsto ab$. On note $(G, \star)$ l'ensemble G muni de la loi de composition interne $\star$.

Exemples 2.1

1. *L'addition et la multiplication usuelles sont des lois de composition interne sur* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *et* $\mathbb{C}$.
2. *Si E est un ensemble non vide et $\mathcal{P}(E)$ l'ensemble de toutes les parties de E, les applications :*

$$(A, B) \mapsto A \cap B,\ (A, B) \mapsto A \cup B,\ (A, B) \mapsto A \triangle B = (A \cup B) \setminus (A \cap B)$$

   sont des lois de composition interne sur $\mathcal{P}(E)$.
3. *Si E est un ensemble non vide et $\mathcal{F}(E)$ l'ensemble de toutes les applications de E dans E, alors l'application de composition $(f, g) \mapsto f \circ g$ est une loi de composition interne sur $\mathcal{F}(E)$.*

Définition 2.2. *Soit G un ensemble non vide muni d'une loi de composition interne $(a, b) \mapsto a \star b$. On dit que :*

1. *cette loi est associative si $(a \star b) \star c = a \star (b \star c)$ pour tous a, b, c dans G ;*
2. *cette loi est commutative si $a \star b = b \star a$ pour tous a, b dans G ;*
3. *e est un élément neutre pour cette loi si $a \star e = e \star a = a$ pour tout $a \in G$;*

4. un élément a de G est dit régulier (ou simplifiable) si :

$$\forall\,(b,c)\in G^2,\ \begin{cases} a\star b=a\star c\Rightarrow b=c\\ b\star a=c\star a\Rightarrow b=c\end{cases}$$

Dire qu'un élément $a\in G$ est régulier à gauche [resp. à droite] signifie que l'application $g\mapsto a\star g$ [resp. $g\mapsto g\star a$] est injective.

Si $\star$ est une loi de composition interne associative sur G, on écrira $a\star b\star c$ pour $(a\star b)\star c$ ou $a\star(b\star c)$. De manière plus générale, toujours dans le cas d'une loi associative, on peut effectuer les opérations $a_1\star a_2\star\cdots\star a_n$ où les a_j sont des éléments de G, ce que l'on notera $\prod_{j=1}^{n}a_j$ dans le cas d'une loi multiplicative ou $\sum_{j=1}^{n}a_j$ dans le cas d'une loi additive. Ce produit (ou cette somme) est donc défini par $a_1\in G$ et supposant $\prod_{j=1}^{n-1}a_j$ construit pour $n\geq 2$, on a $\prod_{j=1}^{n}a_j=\prod_{j=1}^{n-1}a_j\star a_n$, le parenthésage étant sans importance du fait de l'associativité.

Pour $n=0$, il sera commode de noter $\prod_{j=1}^{n}a_j=1$ (ou $\sum_{j=1}^{n}a_j=0$ dans le cas d'une loi additive), où 1 [resp. 0 pour une loi additive] est l'élément neutre.

Dans le cas où tous les a_j sont égaux à un même élément a, ce produit est noté a^n et on dit que c'est la puissance n-ième de a. On retiendra que ces éléments de G sont donc définis par la relation de récurrence $a^0=1$ et $a^{n+1}=a^n\star a$ pour tout $n\in\mathbb{N}$. Dans le cas où la loi est notée additivement, on note plutôt na au lieu de a^n. On vérifie facilement que $a^n\star a^m=a^m\star a^n=a^{n+m}$ [resp. $(na)+(ma)=(ma)+(na)=(n+m)\,a$ pour une loi additive] pour tous n,m dans $\mathbb{N}^*$ (voir le théorème 2.9).

Exemples 2.2

1. *Les opérations usuelles d'addition et de multiplication sont commutatives et associatives sur $G=\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. 0 est un élément neutre pour l'addition et 1 est un élément neutre pour la multiplication pour chacun de ces ensembles. Tous les éléments de G sont simplifiables pour l'addition et tous les éléments de $G^*=G\setminus\{0\}$ sont simplifiables pour la multiplication.*
2. *Si E est un ensemble non vide, les opérations $\cap$ et $\cup$ sont commutatives et associatives sur $\mathcal{P}(E)$. L'ensemble vide $\emptyset$ est un élément neutre pour $\cup$ et E est un élément neutre pour l'intersection $\cap$.*
3. *Si E est un ensemble non vide la composition des applications est associative et non commutative dans $\mathcal{F}(E)$. L'identité est un élément neutre pour cette loi.*

Théorème 2.1.

Soit $(G,\star)$ un ensemble non vide muni d'une loi de composition interne. Si G admet un élément neutre, alors ce dernier est unique.

Preuve. Soient e, e' deux éléments neutres. On a alors $e = e \star e'$ puisque e' est neutre et $e' = e \star e'$ puisque e est neutre, ce qui implique $e = e'$. □

Définition 2.3. *Soit $(G, \star)$ un ensemble non vide muni d'une loi de composition interne et admettant un élément neutre e. On dit qu'un élément a de G est inversible s'il existe un élément a' dans G tel que $a \star a' = a' \star a = e$. On dit alors que a' est un inverse (ou un symétrique) de a dans G.*

Théorème 2.2.

Soit $(G, \star)$ un ensemble non vide muni d'une loi de composition interne associative et admettant un élément neutre e. Si $a \in G$ admet un inverse dans G, alors ce dernier est unique.

Preuve. Supposons que $a \in G$ admette deux inverses a' et a''. On a alors :

$$a' \star a \star a'' = (a' \star a) \star a'' = e \star a'' = a''$$

puisque la loi est associative et a' est inverse de a et :

$$a' \star a \star a'' = a' \star (a \star a'') = a' \star e = a'$$

puisque a'' est inverse de a, ce qui implique $a' = a''$. □

Pour une loi non associative, l'unicité du symétrique n'est pas assurée. Par exemple dans l'ensemble $G = \{0, -1, 1\}$ muni de la loi définie par la table :

$\star$	0	-1	1
0	0	-1	1
-1	-1	0	0
1	1	0	0

0 est neutre et $1 \star 1 = 1 \star (-1) = 0$.

En cas d'existence, on notera a^{-1} un inverse de a dans $(G, \star)$, la loi $\star$ étant associative. Dans le cas d'une loi de composition interne notée de façon additive, on notera plutôt $-a$ un inverse de a et on l'appellera opposé.

Exemples 2.3

1. *Dans $(\mathbb{N}, +)$ seul 0 a un opposé et dans $(\mathbb{N}, \cdot)$ seul 1 a un inverse.*
2. *Dans $(\mathbb{Z}, +)$ tout élément admet un opposé et dans $(\mathbb{Z}, \cdot)$ les seuls éléments inversibles sont 1 et -1.*

2.2 Groupes

Définition 2.4. *Un groupe est un ensemble non vide G muni d'une loi de composition interne $\star$ possédant les propriétés suivantes :*

- *la loi $\star$ est associative ;*
- *il existe un élément neutre e pour la loi $\star$;*
- *tout élément de G admet un symétrique.*

Si de plus la loi $\star$ est commutative, on dit que le groupe G est commutatif ou abélien.

En général, s'il n'y pas de confusion possible, on dira tout simplement que G est un groupe et on notera ab ou $a+b$ le résultat de l'opération $a \star b$. Pour un groupe multiplicatif $(G,\cdot)$, on notera 1 l'élément neutre, a^{-1} le symétrique d'un élément a de G et pour un groupe additif $(G,+)$, on notera 0 l'élément neutre, $-a$ le symétrique qu'on appelle opposé.

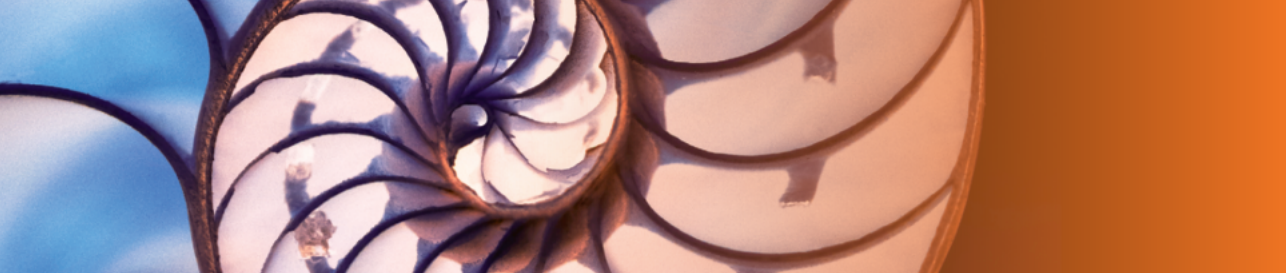
Exemples 2.4

1. *Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de l'addition usuelle sont des groupes abéliens.*
2. *L'ensemble $\mathbb{N}$ muni de l'addition usuelle n'est pas un groupe du fait qu'un élément non nul de $\mathbb{N}$ n'a pas d'opposé dans $\mathbb{N}$ (l'équation $a+x=0$ avec $a \neq 0$ dans $\mathbb{N}$ n'a pas de solution dans $\mathbb{N}$).*
3. *Les ensembles $\mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$ munis de la multiplication usuelle sont des groupes abéliens.*
4. *L'ensemble $\mathbb{Z}^*$ muni de la multiplication usuelle n'est pas un groupe du fait qu'un élément de $\mathbb{Z}\setminus\{-1,0,1\}$ n'a pas d'inverse dans $\mathbb{Z}$ (l'équation $ax=1$ avec $a \in \mathbb{Z}\setminus\{-1,0,1\}$ n'a pas de solution dans $\mathbb{Z}$).*
5. *Si E est un ensemble non vide, l'ensemble $\mathcal{P}(E)$ est alors un groupe pour l'opération de différence symétrique : $(A,B) \mapsto A \triangle B = (A \cup B) \setminus (A \cap B)$.*
6. *Si E est un ensemble non vide, l'ensemble des bijections de E dans lui même muni de la composition des applications est un groupe (en général non abélien). Ce groupe est le groupe des permutations de E, il est noté $S(E)$ ou $\mathfrak{S}(E)$.*
7. *Si $H_1, \cdots, H_n$ sont des groupes multiplicatifs, alors le produit direct $\prod_{k=1}^{n} H_k$ muni de la loi $((a_1,\cdots,a_n),(b_1,\cdots,b_n)) \mapsto (a_1b_1,\cdots,a_nb_n)$ est un groupe et ce groupe est commutatif si, et seulement si, tous les H_i le sont.*

Théorème 2.3.

Dans un groupe $(G,\star)$ tout élément est simplifiable.

Preuve. Soient a,b,c dans G. Si $a \star b = a \star c$, on a alors $a^{-1} \star a \star b = a^{-1} \star a \star c$, soit $b=c$. De même si $b \star a = c \star a$, alors $b \star a \star a^{-1} = c \star a \star a^{-1}$, soit $b=c$. □



Mathématiques pour le Capes.
Algèbre et géométrie

Ce cours d'algèbre et de géométrie s'adresse aux candidats préparant spécifiquement le Capes externe de mathématiques.

Les notions étudiées ici le sont de façon rigoureuse en démontrant tous les résultats énoncés. Chaque chapitre se termine par une série d'exercices tous corrigés en détails qu'il faut maîtriser avant de travailler sur des épreuves écrites du concours.

Les 12 premiers 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. Le dernier chapitre rassemble une sélection de six problèmes d'algèbre et de géométrie issus des épreuves du Capes. Bibliographie sélective et index viennent compléter l'ensemble.

LES PLUS

- **Cours rédigé avec démonstration systématique des résultats énoncés**
- **Chaque théorème est suivi d'une série d'applications**
- **200 exercices et 6 problèmes 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 : 978-2-8073-3222-5

9 782807 332225

deboeck SUPÉRIEUR

www.deboecksuperieur.com

Conception graphique : Primo&Primo®