MÉTHODES MATHÉMATIQUES POUR L'INFORMATIQUE

Cours et exercices corrigés

Jacques Vélu
Professeur honoraire au
Conservatoire national des arts et métiers

5e édition

DUNOD

ISBN 978-2-10-059452-8

Table des matières

Avant-propos

Depuis sa première version, des dizaines de milliers de personnes ont utilisé *Méthodes mathématiques pour l'informatique* ; le livre est présenté ici dans sa nouvelle édition, une fois de plus revue, mise à jour et corrigée.
Primitivement destiné à accompagner les deux enseignements de Mathématiques pour l'Informatique du Conservatoire National des Arts et Métiers, ce cours a élargi son audience au fil des années et maintenant il est utilisé autant hors du CNAM que dans le CNAM.
Ses lecteurs sont de deux sortes : des débutants ou des curieux, dont c'est le premier et dernier contact avec les Mathématiques discrètes, et des auditeurs qui entreprennent un cycle d'étude plus ou moins long. Citons par exemple les étudiants de DUT, de BTS, de licence STIC (Sciences et techniques de l'information et de la communication) mention informatique et mention mathématiques appliquées, des certificats inscrits au RNCP (registre national de la certification professionnelle).
Conçu pour un public protéiforme, il vise cependant un unique objectif : *apprendre des méthodes en faisant comprendre les idées qui les ont engendrées*.
Il y a plus de quinze ans, quand le premier cours a été bâti, on pouvait justement se demander s'il existait des mathématiques de l'informatique, et quelles étaient leurs limites. Fallait-il en faire un enseignement séparé ou, comme cela se faisait jusque là, glisser quelques recettes au gré des cours d'informatique ?
Le choix de l'époque, dont la justesse ne s'est pas démentie, a été de remplacer les recettes par des méthodes qui reposent sur des théorèmes de mathématiques ; même si les plus difficiles sont plus montrés que démontrés, les théorèmes forment l'ossature du livre.
L'enseignement qui repose sur ce livre, est constitué, au CNAM, de deux cours d'une durée de 60 heures chacun (6 ECTS), répartis sur deux semestres. C'est beaucoup et c'est peu ; beaucoup quand l'objectif est avant tout de devenir informaticien, souvent uniquement praticien, mais c'est peu car le domaine est si vaste …
Le livre a été bâti pour qu'on y retrouve deux types de sujets, avec deux niveaux de difficulté. D'abord ceux qui sont inévitables et qu'on enseigne généralement au premier semestre : l'algèbre de Boole, le calcul propositionnel, les dénombrements, etc. Puis d'autres, qui demandant davantage d'efforts, et qui constituent le cours du deuxième semestre. Ceux-là ont pour thème sous-jacent les applications du calcul matriciel : on rencontre des matrices dans les codes, dans les graphes, dans les automates, partout, mais je n'en dis pas plus afin de laisser au lecteur le soin d'en faire lui-même la découverte. Leur importance interdit de traiter tout ces sujets en si peu de temps ; il faudra

donc en choisir quelques-uns et ne donner que les grandes lignes des autres, le livre venant alors en complément du cours.
Je me suis toujours efforcé de commencer par présenter les concepts de la façon la plus intuitive possible avant de procéder à leur mise en forme abstraite ; c'est pourquoi les sujets débutent souvent par une introduction très concrète qui pose les problèmes. Ensuite viennent les théorèmes qui conduisent aux méthodes pratiques permettant de résoudre mécaniquement ces problèmes.
Les chapitres finissent toujours par de nombreux exercices. Beaucoup sont faciles et seront résolus dès qu'on aura trouvé le paragraphe auquel ils se rapportent, mais d'autres, nettement plus difficiles, se cachent dans la masse ; c'est donc un exercice supplémentaire de les débusquer. Certains exercices doivent être considérés comme un moment de détente ; souvent écrits en italique, ils adoptent un style qu'on n'a pas l'habitude de trouver dans les livres de Mathématiques ; mais là aussi je laisse au lecteur le plaisir de les découvrir. À la fin du livre, on trouvera les solutions des exercices. Pour certains, le résultat seulement est donné, mais, pour beaucoup d'autres, des indications détaillées sont fournies.
Tout au long du livre j'ai posé des jalons dans l'espoir d'exciter votre curiosité. Si je vous ai donné envie de lire un livre de Mathématiques sans y être obligé mon but est atteint.
Des parties ont été récrites spécialement pour cette quatrième édition, en tenant compte des questions posées par les élèves. Autre nouveauté, pour ceux qui ont accès à internet et qui peuvent lire l'anglais, quelques URL, qui m'ont été demandées, permettront de rechercher un complément d'information ; voici, tout de suite, les trois premières :
– pour chercher des renseignements sur l'histoire des mathématiques et les biographies de mathématiciens http ://www-history.mcs.st-and.ac.uk/
– pour parcourir une gigantesque encyclopédie des mathématiques qui donne l'actualité des grands résultats http ://mathworld.wolfram.com/
– si vous rencontrez une suite de nombres entiers, par exemple 1, 9, 9, 3, 9, 9, 3, 9, 9, 1, 18, 9, 9, 9, 9, 9, 9, 9, 6, 9, 18, 6, 9, 9, 6, 9, 9, 4, 9, 9, 12, 18, 18, 3, 9, 9, 3, 9, 9, 3, 18, 18, 12, 18, 9, 5, 9, 9, 9, 9, 18, 6, 18, 18, 2, 9, 9, 9, 9, 9, 12, 5, 18, 3, 9, 9, 3, et si vous ne savez ni ce que sont ces nombres ni quels pouraient être les suivants, vous l'apprendrez en consultant :

  www.oeis.org,

  un site vraiment extraordinaire !

Après le fond, un dernier mot sur la forme. Chaque nouvelle édition est l'occasion de corriger des fautes (leur flux s'amenuise toujours plus mais semble intarissable, cela doit se démontrer !). Le livre a été ressaisi complètement, par une nouvelle équipe, avec un nouveau logiciel. Bien qu'il ait été relu de nombreuses fois je ne serai pas étonné de recevoir quelques courriers me signalant des copier-coller maladroits ; n'hésitez pas à me les signaler (infos@dunod.com), par avance merci.
Et surtout bonne lecture !

JACQUES VÉLU
Riga, le 14 février 2013

Corrigés vidéo

Rien ne remplace un professeur pour expliquer de vive voix des notions complexes. C'est la raison pour laquelle Jacques Vélu et les éditions Dunod vous proposent avec cet ouvrage cinq vidéos de corrigés d'exercices.

Pour chaque corrigé vous aurez à l'écran toutes les étapes de la solution sous forme d'animations avec les explications détaillées de l'auteur en arrière-plan audio.

Comme dans toute vidéo vous pourrez mettre sur « Pause » à tout moment si vous avez besoin de réfléchir avant de passer à la suite. Vous pourrez bien sûr aussi revenir en arrière si vous n'êtes pas sûr d'avoir bien compris.

Elles peuvent être visionnées sur tous types d'ordinateurs, de tablettes ou de smartphones connectés à Internet.

Ces vidéos portent sur les énoncés suivants :

Page 54 : Exercice 4.19 sur les dénombrements

Page 76 : Exercice 6.19 sur les ensembles ordonnés

Page 172 : Exercice 11.16 sur les fonctions booléennes et la simplification des formules

Page 259 : Exercice 16.18 sur les codes détecteurs et les codes correcteurs

Page 352 : Problème 20.17 sur les automates finis

Les exercices concernés sont repérés par le logo suivant : 

Vous avez plusieurs façons d'y accéder :

– Soit en tapant directement l'adresse suivante dans votre navigateur :

http://goo.gl/ACJzo

– Soit en cliquant les liens sur la page web du site Dunod dédiée à cet ouvrage

– Soit en saisissant cette adresse dans votre navigateur

http://www.youtube.com/DunodVideos.

Vous accèderez ainsi aux playlists de Dunod. Pour retrouver celle concernant cet ouvrage entrez le nom de la playlist : **Méthodes mathématiques pour l'informatique - Jacques Vélu Dunod**.

Chapitre **1**

La notion d'ensemble

Dans ce chapitre introductif, nous présentons les notions d'*ensemble*, d'*élément* et d'*application*, qui permettent de définir tous les objets mathématiques de façon cohérente et uniforme. Peu à peu, nous verrons que les mathématiques sont une écriture (*notations*), une langue (*ordonnancement des idées*) et une façon de penser (*interprétation des situations concrètes au moyen de certains concepts abstraits*).

MOTS-CLÉS : ensemble - éléments - appartient - sous-ensemble - partie - inclus - contient - ensemble vide - compréhension - extension - bit - fonction - application - domaine de définition - image - suite - liste - mot binaire - injection - surjection - bijection - identité - application réciproque - application composée.

1.1 ENSEMBLES

1.1.1 Les mathématiciens préfèrent sans doute la collectivité à l'individu et le général au particulier car ce qui les intéresse le plus ce ne sont pas les propriétés propres à quelques objets isolés, mais plutôt celles que partagent *tous* les objets d'une même famille. Depuis la fin du XIX^{e} siècle, les *ensembles* sont même devenus la notion fondamentale des Mathématiques.

***Exemple* 1.1 :** Après avoir constaté sur un dessin que les médianes d'un triangle particulier semblent bien se couper en un même point, on se demande si c'est vrai pour les médianes de n'importe quel triangle car c'est une propriété d'une portée beaucoup plus générale, puisqu'elle concerne aussi les triangles qui n'ont pas encore été dessinés et même ceux qui ne le seront jamais !

***Exemple* 1.2 :** Le fait que $1023 = 2^{10} - 1$ soit divisible par 11 n'a guère retenu l'attention des mathématiciens ; par contre la découverte et la démonstration par Fermat que $2^{p-1} - 1$ est *toujours* divisible par p, quand p est un nombre premier, est un résultat fondamental de l'arithmétique.

1.1.2 On définit souvent un ***ensemble*** comme *une collection d'objets caractérisés par une propriété commune* ; il y a par exemple l'ensemble des nombres pairs, l'ensemble des nombres entiers compris entre 7 et 24, l'ensemble des droites du plan, etc. Cette façon de s'exprimer, qui peut rendre service lorsqu'on parle d'ensembles très simples est dangereuse, parce que trop vague, et laisse croire que n'importe quoi est un ensemble, ce qui conduit à des contradictions dont les plus célèbres sont sans doute le ***paradoxe de Russell*** et le ***paradoxe du barbier*** (*voir encadrés*).

Un modeste paradoxe… (d'après Russell)
Nous sommes en 2043 et à cette époque le métier de chercheur n'est plus ce qu'il était il y a cinquante ans à peine : pour avoir les moyens de faire de la recherche, il faut d'énormes crédits, pour avoir des crédits il faut les mériter et le mérite d'un chercheur se mesure au nombre de fois où ses publications sont citées. Du coup, les notes de bas de page s'allongent démesurément – on cite beaucoup ses amis, rarement ses ennemis, et il arrive parfois qu'abandonnant toute pudeur une publication aille jusqu'à se citer elle-même ! Lassé par tant de turpitude le Grand Scribe Qelbelk VIII annonce qu'il va réagir en publiant un pamphlet intitulé : Inventaire Moderne des Œuvres Modestes. Il s'agit de la liste des publications qui ne se citent pas, les seules, à ses yeux, qui soient encore dignes d'être lues. C'est alors qu'en Sardaigne le berger Anapale fait cette prophétie : « Quoi qu'il tente, notre Grand Scribe ne mènera jamais son projet à bout ! » Amis lecteurs, vous l'avez déjà deviné, je vous demande d'où vient l'inébranlable assurance d'Anapale ?
Voici ce qu'Anapale s'est dit, au frais, pendant que ses chèvres faisaient la sieste. Il y a deux sortes de publications : les modestes (celles qui ne se citent pas), et les immodestes. L'Inventaire Moderne des Œuvres Modestes (l'I.M.Œ.M. comme l'appelait déjà la presse) est-il modeste ou immodeste ? Si c'est une publication modeste, le Grand Scribe l'a fait figurer dans sa liste des publications modestes. On doit donc le trouver en parcourant l'Inventaire Moderne des Œuvres Modestes et du coup l'I.M.Œ.M se cite lui-même et il n'est pas modeste ! On a là une contradiction qui prouve que l'I.M.Œ.M. ne peut pas être une publication modeste. Alors, si l'I.M.Œ.M. n'est pas une publication modeste, c'est qu'il est immodeste et, puisqu'il est immodeste, il se cite lui-même mais, comme le Grand Scribe n'a inscrit dans son Inventaire que des publications modestes, l'I.M.Œ.M., qui y figure, doit être modeste, ce qui n'est pas possible. Nous obtenons donc une deuxième contradiction qui prouve à son tour que l'I.M.Œ.M. ne peut pas être une publication immodeste. Prévoyant ainsi que l'I.M.Œ.M. ne peut pas exister car il ne pourrait être ni modeste, ni immodeste, notre berger qui, comme tous les bergers, n'a peur que du loup, n'a pas hésité à lancer sa terrible prophétie.
Cette histoire sert à montrer qu'un ensemble ne peut pas être n'importe quelle collection d'objets regroupés au moyen d'une propriété commune. À l'habillage près, c'est le célèbre Paradoxe de Russell (1901) qui dit que si l'on pouvait construire l'ensemble de tous les ensembles qui ne sont pas un de leurs éléments, on se heurterait à une contradiction (*exercice* [1.1]).

Le paradoxe du barbier
Dans une certaine ville il y a deux sortes d'habitants : ceux qui se rasent eux-mêmes et ceux qui ne le font pas. Pour ces derniers, la ville a désigné un habitant, le barbier, chargé de tous les raser, et eux seulement. Alors, qui rase le barbier ?

À l'aube du XX^{e} siècle la découverte de ces contradictions provoqua une violente polémique qui eut le mérite de montrer qu'en Mathématiques il fallait préciser *toutes* les notions, même les plus élémentaires. On a donc été obligé de revoir la notion d'ensemble d'une façon plus restrictive et on a fini par admettre qu'une propriété commune quelconque ne permet pas toujours de définir un ensemble. Les obstacles ont été levés à ce prix et le redoutable *ensemble de tous les ensembles*, qu'on avait un moment envisagé, mais qui menaçait dangereusement les fondements des Mathématiques, s'est évanoui ...

Le but de ce cours n'étant pas d'exposer la *Théorie des Ensembles*, nous devrons nous contenter du semblant de définition qui vient d'être rappelé. En fait, le plus sage sera d'admettre : premièrement, qu'il existe des ensembles (nous allons tout de suite mentionner ceux qui servent de référence) et deuxièmement, qu'à partir d'ensembles déjà connus on peut en fabriquer d'autres au moyen de diverses constructions (les plus simples seront indiquées au fur et à mesure).

1.1.3 Pour pouvoir parler d'un ensemble il faut lui donner un nom. Si c'est un ensemble quelconque, qui n'a pas de raison d'être précisé, ou si c'est un ensemble particulier, mais dépourvu d'importance, on lui donne un nom passe-partout du type : « l'ensemble E, l'ensemble F, etc. »[1].

Les ensembles les plus importants, ceux qui servent de référence, portent des noms qui leur sont propres et sont représentés par une lettre écrite dans un alphabet spécial :

$\mathbb{B}$ est l'ensemble des ***bits***,

$\mathbb{N}$ est l'ensemble des ***entiers naturels***,

$\mathbb{Z}$ est l'ensemble des ***entiers relatifs***,

$\mathbb{R}$ est l'ensemble des ***nombres réels***, etc.

Les ensembles directement fabriqués à partir de ceux-ci sont souvent désignés par une juxtaposition de symboles qui sert à rappeler comment ils sont construits : $\mathbb{N}^2$, $\mathbb{B}^{\mathbb{N}}$, $\mathbb{R}/2\pi\mathbb{Z}$, etc. ; nous y reviendrons.

Dans ce cours, nous nous intéresserons beaucoup à l'ensemble $\mathbb{N}$ des entiers naturels (les nombres entiers positifs, zéro compris), et à des ensembles qui en sont très proches. Pour l'instant nous supposerons que $\mathbb{N}$ est bien connu, mais au § 3.4.2 nous reviendrons sur la façon de le définir.

1.2 ÉLÉMENTS

1.2.1 Les objets qui constituent un ensemble s'appellent les ***éléments*** de l'ensemble. Pour indiquer qu'un objet x est un élément d'un ensemble E on écrit $x \in E$, qui se lit : « x ***appartient à*** E » ; au contraire, pour indiquer que x n'appartient pas à E, on écrit $x \notin E$.

On dit qu'un ensemble A est une ***partie*** d'un ensemble B, ou encore que A est un ***sous-ensemble*** de B, si tout élément de A est aussi un élément de B ; on écrit alors $A \subset B$ et on lit : « A est ***inclus*** dans B », ou bien $B \supset A$ et on lit : « A ***contient*** B ». Si A n'est pas une partie de B, on écrit $A \not\subset B$.

[1] C'est ce qu'on fait quand on dit « le jour J » ou « l'heure H ».

***Exemple* 1.3 :** L'ensemble A formé des nombres entiers multiples de 6 est une partie de l'ensemble B formé des nombres entiers pairs.

Remarque : Copiant les symboles $\leqslant$ et $<$, certains auteurs écrivent $A \subseteq B$ pour dire que A est une partie quelconque de B et réservent la notation $A \subset B$ pour dire que A est inclus dans B, sans être égal à B, propriété qui s'énonce « A est ***strictement inclus*** dans B », ou encore « A est un sous-ensemble ***strict*** de B ». Cet usage ancien, que nous ne suivrons pas, a peu à peu disparu. Pour signifier que A est strictement inclus dans B, on préfère écrire $A \subsetneq B$.

1.2.2 Nous admettrons que les parties d'un ensemble E sont les éléments d'un nouvel ensemble que l'on note $\wp(E)$. C'est le premier exemple d'un procédé permettant de construire un nouvel ensemble à partir d'un ensemble donné.

Il faut remarquer que les éléments de $\wp(E)$ sont des ensembles, puisque ce sont les parties de E ; en particulier $E \in \wp(E)$. Ceci montre qu'un même objet, selon la façon dont on le regarde, peut être tantôt un ensemble, tantôt un élément. On ne doit pas s'en étonner : le *FC–Barcelone* est un élément de l'ensemble des équipes espagnoles de football, mais c'est aussi un ensemble de joueurs !

De même qu'en arithmétique on introduit le nombre 0, dans la théorie des ensembles il est utile d'introduire un ensemble appelé ***ensemble vide***, qui a la particularité de ne pas avoir d'élément[1] ; on le note $\varnothing$. Par convention chaque ensemble admet $\varnothing$ pour partie, autrement dit $\varnothing \in \wp(E)$ quel que soit l'ensemble E.

Remarque : On ne peut pas dire que l'ensemble vide soit très consistant ! Pourtant, il permet à lui seul de reconstituer tous les ensembles n'ayant qu'un nombre fini d'éléments (*voir* § 3.4.2).

1.3 SUR LES FAÇONS DE DÉFINIR UN ENSEMBLE

1.3.1 Bien évidemment, pour s'intéresser à un ensemble, il faut être capable de le définir et de le représenter. Nous allons indiquer deux façons de procéder.

Quand on veut définir un ensemble E, la façon la plus intuitive consiste à énoncer une propriété, appelons-la P, qui caractérise les éléments de E. La propriété P doit permettre de décider, lorsqu'on rencontre un objet, s'il appartient à l'ensemble ou s'il n'y appartient pas. En notant $P(x)$ le fait que l'objet x vérifie cette propriété, on convient de représenter l'ensemble E par la suite de symboles $\{x \mid P(x)\}$ qui se dit : « l'ensemble des x tels que P de x » et qui se lit : « l'ensemble des x qui vérifient la propriété P »[2]. On dit alors que P est un ***prédicat*** et que E est défini en ***compréhension***[3] au moyen du prédicat P.

---

[1] Bien sûr, la définition : *un ensemble est une collection d'objets caractérisés par une propriété commune* ne s'applique pas à cet ensemble, qui n'a pas d'élément ! C'est pourquoi on est souvent obligé de faire un cas particulier pour l'ensemble vide lorsqu'on donne des définitions basées sur l'idée naïve de collection.

[2] Dans cette formulation le choix de la lettre x n'a aucune importance et n'importe quel autre symbole qui n'est pas déjà employé ferait l'affaire ; c'est pour cela que x est qualifié de ***symbole muet***.

[3] Car le prédicat aide à *comprendre* ce que sont les éléments de E.

***Exemple* 1.4 :** De la sorte $\wp(E)$, l'ensemble des parties de l'ensemble E, peut être représenté par la suite de symboles : $\{A \mid A \subset E\}$, qui se lit : « l'ensemble des A tels que A est un sous-ensemble de E ».

Si l'on souhaite préciser que les éléments de l'ensemble à définir doivent être pris dans un ensemble F, au lieu de $\{x \mid x \in F \text{ et } P(x)\}$ on écrit $\{x \in F \mid P(x)\}$ et on lit : « l'ensemble des x appartenant à F tels que $P(x)$ ».

***Exemple* 1.5 :** $\mathbb{N}^\times = \{x \in \mathbb{N} \mid 1 \leqslant x\}$ est l'ensemble des entiers naturels supérieurs ou égaux à 1 ; c'est aussi l'ensemble des entiers naturels non nuls. Si n est un entier naturel supérieur ou égal à 1, le symbole $\mathbb{N}_n^\times = \{x \in \mathbb{N} \mid 1 \leqslant x \leqslant n\}$ désigne l'ensemble des nombres entiers compris entre 1 et n ; nous conviendrons que $\mathbb{N}_0^\times = \varnothing$.

1.3.2 Une difficulté due à la définition en compréhension des ensembles provient de ce que plusieurs prédicats peuvent conduire à la même collection d'objets. Par exemple l'ensemble vide peut être défini aussi bien par : $\{x \mid x \neq x\}$, que par : $\{x \in \mathbb{N} \mid x^2 < 0\}$. Parce que l'important dans un ensemble n'est pas le prédicat employé pour le définir, mais les éléments qui le composent, on convient de dire que deux ensembles E et F sont ***égaux*** quand ils ont les mêmes éléments et cela se note $E = F$ (en privé les mathématiciens ne se gênent pas pour dire que les deux ensembles sont les *mêmes*).

***Exemple* 1.6 :** $\{x \in \mathbb{Z} \mid x^2 = 1\} = \{x \in \mathbb{R} \mid |x| = 1\}$ car nous avons à gauche l'ensemble des entiers relatifs dont le carré vaut 1, qui a donc pour éléments +1 et -1, alors qu'à droite nous avons l'ensemble des nombres réels dont la valeur absolue est égale à 1, et dont les éléments sont à nouveau +1 et -1.

Remarque : Reconnaître si deux ensembles définis par des prédicats différents sont égaux est un problème difficile, qu'on ne sait pas traiter en général. Pour démontrer que E et F sont égaux, on procède souvent en deux temps, en démontrant d'abord que E est inclus dans F, puis que F est inclus dans E.

1.3.3 La définition d'un ensemble au moyen d'une propriété caractéristique n'est pas toujours commode, surtout quand on doit manipuler ses éléments. Il faut donc trouver une autre façon de définir les ensembles.

Il arrive qu'on ne connaisse pas du tout les éléments d'un ensemble[1] mais il se peut aussi qu'on les connaisse tous, ce qui permet, quand il n'y en a pas trop, de représenter l'ensemble par la liste de ses éléments ; on dit alors que l'ensemble est défini en ***extension***. Dans la pratique on écrit les éléments rangés dans un certain ordre, séparés par des virgules, encadrés par deux accolades. Au § 1.4.5 nous reviendrons sur la notion de liste.

Exemple* 1.7 :** L'ensemble des ***bits, noté $\mathbb{B}$ (comme ***binaire***, ou ***booléen***), a deux éléments, 0 et 1 ; on écrira donc $\mathbb{B} = \{0, 1\}$.

***Exemple* 1.8 :** L'ensemble $\{1, 2, 3, 4, 5, 6\}$ n'est autre que $\mathbb{N}_6^\times$.

[1] Il peut même arriver qu'on n'ait pas d'autre connaissance d'un ensemble que sa définition, comme dans l'exemple suivant. On définit les ***nombres parfaits*** : ce sont les entiers naturels qui sont égaux à la somme de leurs diviseurs strictement plus petits qu'eux-même (28 est parfait car 28 = 1 + 2 + 4 + 7 + 14). On peut donc définir l'ensemble des nombres qui sont à la fois *parfaits* et *impairs* mais on ne connaît pas un seul de ses éléments, on ne sait même pas s'il est vide !

Remarque : En changeant l'ordre des éléments dans une liste, on pourrait penser qu'on obtient un nouvel ensemble, mais l'ancien et le nouvel ensemble sont égaux, puisqu'ils ont les mêmes éléments. Par conséquent, quand on définit un ensemble en extension, l'ordre dans lequel on fait la liste de ses éléments n'a pas d'importance ; par exemple $\{1, 0\}$ représente $\mathbb{B}$ autant que $\{0, 1\}$.

Bien évidemment la définition en extension s'applique mal à l'ensemble vide qui n'a pas d'élément[1] ou à l'ensemble $\mathbb{N}$ qui en a trop, bien qu'on écrive souvent :

$$\begin{aligned} \mathbb{N} &= \{0, 1, 2, 3, \ldots\} \\ \mathbb{N}^\times &= \{1, 2, 3, \ldots\} \\ \mathbb{Z} &= \{\ldots, -2, -1, 0, 1, 2, \ldots\} \end{aligned}$$

1.3.4 Pour définir un ensemble en extension, on doit pouvoir représenter ses éléments. Au § 1.4.6 nous définirons $\mathbb{B}^n$, un exemple fondamental d'ensemble dont les éléments sont représentés par des symboles.
Si l'informaticien cherche à représenter les éléments d'un ensemble par des symboles, en général des 0 et des 1, c'est parce que ses machines sont bien adaptées à la manipulation de ces objets. À côté de cela le mathématicien utilise très souvent des figures géométriques pour communiquer ses idées. Dans la suite du cours, nous aurons plusieurs occasions de le vérifier, avec les diagrammes cartésiens, les diagrammes sagittaux, les diagrammes de Hasse, de Venn, de Karnaugh, etc.

1.4 FONCTIONS ET APPLICATIONS

1.4.1 Les fonctions sont le moyen par lequel les ensembles *communiquent* entre eux. Rappelons brièvement qu'on appelle ***fonction*** d'un ensemble A vers un ensemble B toute loi qui permet d'associer à *chaque* élément x, d'une certaine partie de A, un *unique* élément y de B ; pour l'instant ce semblant de définition nous suffit mais nous serons plus précis au § 5.1.3. On dit que A est l'ensemble de ***départ***, ou la ***source***, et que B est l'ensemble d'***arrivée***, ou le ***but***. Le sous-ensemble de A formé des éléments x auxquels est associé un élément de B s'appelle le ***domaine de définition*** de la fonction. La suite de symboles $f : A \to B$ se lit : « f est une fonction de A vers B ».

***Exemple* 1.9 :** On range certains objets d'une collection dans les tiroirs d'un meuble préalablement vide. En associant à chaque objet le tiroir qui le contient, on définit une fonction qui va de l'ensemble des objets vers l'ensemble des tiroirs ; son image est l'ensemble des tiroirs qui ne sont pas vides ; son domaine de définition est l'ensemble des objets rangés.

***Exemple* 1.10 :** L'action qui consiste à associer à chaque nombre entier son carré définit une fonction de $\mathbb{N}$ vers $\mathbb{N}$.

***Exemple* 1.11 :** Actuellement le numéro d'immatriculation d'une voiture est formé d'une suite de chiffres et de lettres qui se succèdent de la façon suivante : 2 lettres, puis 3 chiffres, puis 2 lettres. En termes mathématiques l'immatriculation des voitures définit une fonction qui va de l'ensemble A des voitures nouvellement imatriculées vers un ensemble B dont les éléments sont les suites de chiffres et de lettres construites selon cette règle.

[1] On peut quand même le représenter par la ***liste vide*** : $\{\}$.

Retenons de l'exemple 1.11 qu'associer un numéro de code (ou un numéro d'immatriculation) à chaque élément d'un ensemble A c'est construire une fonction qui va de A vers l'ensemble B des numéros de code possibles.

1.4.2 Si une fonction s'appelle f, l'élément associé à x par f s'appelle l'***image*** de x et généralement on le note $f(x)$. Les images des divers éléments de A forment un sous-ensemble de B qu'on appelle l'***image*** de f et qu'on note $f(A)$. Par convention, si A est l'ensemble vide, l'image de f est vide, autrement dit : $f(\varnothing) = \varnothing$. D'une façon générale, quand C est une partie de A, on note $f(C)$ l'ensemble des images des éléments de C.

Les mathématiciens ont l'habitude de faire une distinction entre la notion de fonction et celle plus restrictive d'application. Une ***application*** d'un ensemble A vers un ensemble B est une fonction dont le domaine de définition est A tout entier. ; autrement dit, une application est une fonction ***partout définie***[1].

Nous admettrons que les fonctions d'un ensemble A vers un ensemble B forment un ensemble, de même que les applications de A vers B ; pour des raisons qui apparaîtront avec le théorème 4.2, on note B^A l'ensemble des applications de A vers B.

1.4.3 Une même fonction peut être définie de plusieurs façons mais, comme ce qui compte dans les fonctions c'est avant tout leurs valeurs, on dit que deux fonctions f et g sont ***égales*** quand $f(x) = g(x)$ quel que soit x ; on écrit alors $f = g$.

La méthode pour définir et représenter une fonction d'un ensemble A vers un ensemble B dépend beaucoup de la nature de A et de B. Une fonction entre deux ensembles de nombres, $\mathbb{N}$ ou $\mathbb{R}$ par exemple, est souvent définie au moyen d'une ***formule*** qui indique des calculs à effectuer.

> ***Exemple* 1.12 :** La formule $f(x) = (6 + e^x)x^{-3}$ définit une fonction de $\mathbb{R}$ vers $\mathbb{R}$ ayant pour domaine de définition $\mathbb{R}$ privé de 0.

Cependant, les fonctions entre deux ensembles de nombres ne sont pas toujours définies par des formules, certaines sont même uniquement définies par leur ***courbe représentative***. Ainsi, lorsqu'on mesure une grandeur physique en continu, appelons-la G, on obtient une courbe qui montre comment G évolue au cours du temps. Cela définit une fonction $f : \mathbb{R} \to \mathbb{R}$ telle que $G = f(t)$, qui n'est pas nécessairement représentable par une formule[2].

> ***Exemple* 1.13 :** La courbe de la figure 1.1 représente l'évolution de la pression atmosphérique d'un lieu au cours du temps. La fonction correspondante n'est pas définie par une formule, on la connaît seulement par cette courbe.

1.4.4 L'informatique manipule des symboles qui ne représentent pas toujours des nombres, donc les fonctions de l'informaticien ne sont pas toujours définies par des formules.

Au chapitre 5, nous verrons que définir une fonction revient à définir un certain ensemble, le *graphe* de la fonction, et que le problème de la définition des fonctions est un cas particulier de celui de la définition des ensembles.

Lorsque l'ensemble A est défini en extension, on peut toujours représenter une application $f : A \to B$ par sa ***table de valeurs***. Il s'agit d'un tableau qui montre côte à côte x et $f(x)$ pour tous les éléments x de A.

[1] En informatique, comme le mot application a plusieurs sens, on préfère dire ***fonction totale*** et appeler ***fonction partielle*** une fonction qui n'est pas partout définie.

[2] La tâche du physicien consiste à découvrir s'il en existe une et laquelle.

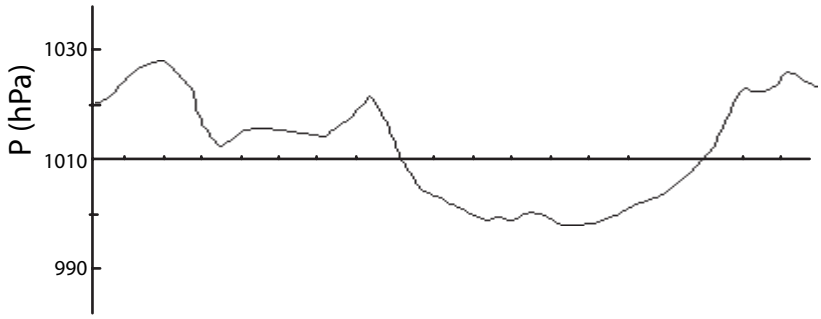

Figure 1.1

***Exemple* 1.14 :** Si $A = \{André, Bernard, Charles, Denise, Édith, Françoise\}$ et B est l'ensemble des jours de l'année, on définit une application $f : A \to B$ en associant à chaque élément de A le jour de son anniversaire. La figure 1.2 représente la table de valeurs de f.

x	$f(x)$
André	15 avril
Bernard	2 février
Charles	8 mai
Denise	30 octobre
Édith	19 décembre
Françoise	21 août

Figure 1.2

1.4.5 À présent voici un type d'application qui va jouer un rôle très important. Soit $n \geqslant 1$, un entier naturel. Construire une application de $\mathbb{N}_n^\times$ vers un ensemble E, c'est associer à chaque entier compris entre 1 et n un élément de E ; une telle application s'appelle une ***suite finie*** d'éléments de E, ***de longueur n***.

On peut *représenter* une suite finie de longueur n en écrivant de gauche à droite les images de 1, de 2, …, de n, séparées par des virgules et encadrées par des accolades ; on obtient alors une ***liste de n*** éléments de E.

L'élément associé à l'entier k s'appelle le k^{e} ***terme*** de la suite ; si la suite s'appelle σ, cet élément est souvent noté σ_k au lieu de $\sigma(k)$.

***Exemple* 1.15 :** La liste $\left\{\pi\,,\sqrt{2}\,,\pi\,,\frac{5}{7}\right\}$ représente une suite σ de nombres réels de longueur 4 pour qui : $\sigma_1 = \pi$, $\sigma_2 = \sqrt{2}$, $\sigma_3 = \pi$, $\sigma_4 = \frac{5}{7}$.

Puisque B^A désigne l'ensemble des applications d'un ensemble A vers un ensemble B, l'ensemble des suites d'éléments de E de longueur n devrait être noté $E^{\mathbb{N}_n^\times}$ mais on verra, au § 2.3.2, pourquoi on a le droit d'utiliser la notation plus simple E^n.

1.4.6 Dans le cas particulier où $E = \mathbb{B}$, au lieu d'appeler un élément de $\mathbb{B}^n$ une *suite finie de bits de longueur n*, on l'appelle une ***suite binaire de longueur n***.

Les ensembles $\mathbb{B}^n$ reviendront à de multiples occasions dans les prochains chapitres.

Pour représenter les suites binaires de longueur n, on simplifie les notations à l'extrême, en supprimant virgules et accolades ; on obtient alors des expressions qu'on appelle[1] les ***mots binaires de longueur n***.

***Exemple* 1.16 :** Le mot binaire 00101110010101101101010 représente de façon simplifiée la suite binaire de longueur 23 :

$$\{0,0,1,0,1,1,1,0,0,1,0,1,0,1,1,0,1,1,0,1,0,1,0\}$$

Remarque : Au chapitre 19, on inventera un mot binaire de longueur nulle. Bien évidemment on ne peut pas le représenter en écrivant ses bits puisqu'il n'en a pas ! On se contente de lui donner un nom, le ***mot sans lettre***, et on le note ε. Par convention, $\mathbb{B}^0$ désigne l'ensemble réduit à ε, le seul mot binaire de longueur nulle.

1.4.7 Par analogie avec ce qui précède, une application de $\mathbb{N}$ vers E s'appelle une ***suite infinie*** d'éléments de E. Puisqu'on ne peut pas définir en extension les suites infinies, il faut employer d'autres procédés. Quand c'est possible, on représente une suite σ au moyen d'une formule permettant de calculer σ_k à partir de k. On dit alors que σ_k est le ***terme général*** de la suite σ et que la suite est *définie par son terme général*.

***Exemple* 1.17 :** La formule : $\sigma_k = \sqrt{1+k}$ définit une suite par son terme général.

Mais une telle formule n'existe pas toujours ou n'est pas forcément connue.

***Exemple* 1.18 :** Il semble qu'on ne connaisse pas de formule permettant de prédire la valeur du n^{e} chiffre après la virgule du développement décimal de π.

On peut définir certaines suites au moyen d'une ***formule de récurrence***. En gros il s'agit d'une formule permettant de calculer le k^e terme de la suite à partir de k et des termes précédents. Une telle suite s'appelle une ***suite récurrente***.

***Exemple* 1.19 :** Les égalités $\sigma_0 = 1$ et $\sigma_k = k - \sigma_{k-1}$ définissent une suite récurrente dont les premiers termes sont : $\sigma_0 = 1$, $\sigma_1 = 0$, $\sigma_2 = 2$, $\sigma_3 = 1$, $\sigma_4 = 3$, $\sigma_5 = 2$, $\sigma_6 = 4$, etc.

1.5 DIVERSES PROPRIÉTÉS DES APPLICATIONS

1.5.1 Une application d'un ensemble A vers un ensemble B qui ne prend jamais deux fois la même valeur s'appelle une ***injection*** ; on dit aussi que l'application est ***injective***.

Plus précisément, l'application f est injective si l'égalité $f(x) = f(y)$ est possible seulement quand $x = y$. On peut aussi dire que f est injective si l'équation $f(x) = b$, où x est inconnu et b un élément quelconque de B, possède 0 ou 1 solution selon la valeur de b, mais jamais plus.

Pour qu'une codification permette d'identifier des objets sans ambiguïté il faut que l'application définissant le codage soit injective[2].

[1] Pour des raisons qui apparaîtront au chapitre 19.

[2] Pour pouvoir donner des contraventions sans aller au devant des pires difficultés il faut que l'application de l'exemple 1.11 soit injective !

***Exemple* 1.20 :** Reprenons l'exemple 1.9 où des objets sont rangés dans des tiroirs et où l'on associe à chaque objet le tiroir qui le contient. Dire que cette application est injective signifie simplement qu'il n'y a jamais plus d'un objet dans un tiroir.

***Exemple* 1.21 :** L'application qui associe à chaque être humain sa date de naissance n'est pas injective (qu'on pense aux jumeaux !).

***Exemple* 1.22 :** Une suite injective est une suite dont tous les termes sont différents.

Exemple* 1.23 :** Soit A un sous-ensemble d'un ensemble B. L'application $f : A \to B$ définie par $f(x) = x$ pour tout x dans A s'appelle l'injection canonique*** de A dans B. Comme son nom l'indique elle est injective !

1.5.2 Une application de A vers B qui prend pour valeurs tous les éléments de B s'appelle une ***surjection***, on dit aussi une application ***surjective***. En d'autres termes, $f : A \to B$ est surjective si son image est B ou encore si, pour tout y de B, il existe au moins un élément x de A tel que $y = f(x)$.
On peut encore dire que l'application f est surjective si l'équation $f(x) = b$, où x est inconnu et b un élément de B, possède toujours au moins une solution, quel que soit b.

***Exemple* 1.24 :** L'application de l'exemple 1.9 est surjective quand il n'y a pas de tiroir vide.

***Exemple* 1.25 :** L'application de $\mathbb{R}$ vers $\mathbb{R}$ qui associe à chaque nombre réel son carré n'est pas surjective car son image ne contient pas les nombres réels strictement négatifs.

***Exemple* 1.26 :** Soient $A = \{0, 7, 14, 21, 28, 35, 42, 49, 56, \ldots\}$, l'ensemble des nombres entiers multiples de 7 et B l'ensemble des chiffres $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. L'application f, qui associe à tout élément de A son chiffre des unités (en base 10), est surjective car son image est B tout entier, puisque :

$$0 = f(70) \qquad 1 = f(21) \qquad 2 = f(42) \qquad 3 = f(63) \qquad 4 = f(14)$$
$$5 = f(35) \qquad 6 = f(56) \qquad 7 = f(77) \qquad 8 = f(28) \qquad 9 = f(49)$$

***Exemple* 1.27 :** Si l'on reprend l'exemple précédent, en remplaçant A par l'ensemble des multiples de 5, on obtient une nouvelle application f qui n'est pas surjective car son image n'est plus que l'ensemble à deux éléments $\{0, 5\}$.

***Exemple* 1.28 :** Soit $f : A \to B$. Notons C son image et définissons $g : A \to C$ par $g(x) = f(x)$ quel que soit x dans A[1]. Alors g est surjective.

1.5.3 Une application $f : A \to B$ qui est à la fois injective et surjective s'appelle une ***bijection***, on dit aussi que l'application est ***bijective*** et on dit également que f met les ensembles A et B en bijection.

Exemple* 1.29 :** Si A est un ensemble quelconque, l'application de A vers A qui associe x à x est bijective ; on l'appelle l'identité*** de A et on la note Id_A.

***Exemple* 1.30 :** L'application qui associe à chaque entier naturel son double met en bijection $\mathbb{N}$ avec l'ensemble des nombres pairs positifs.

***Exemple* 1.31 :** L'application qui associe à chaque nombre réel strictement positif son *logarithme* est une bijection entre $\mathbb{R}^+$, l'ensemble des réels strictement positifs, et $\mathbb{R}$.

[1] D'une façon concrète, g c'est comme f, à ceci près qu'on remplace B, trop grand, par C.

***Exemple* 1.32 :** Soit $f : A \to B$. Si f est injective, l'application g définie dans l'exemple 1.28 est bijective.

***Exemple* 1.33 :** La représentation des mois du calendrier par leur numéro (*fig.* 1.3) est une bijection entre l'ensemble des mois et $\mathbb{N}_{12}^{\times}$.

janvier	→	1	1	→	*janvier*
février	→	2	2	→	*février*
mars	→	3	3	→	*mars*
avril	→	4	4	→	*avril*
mai	→	5	5	→	*mai*
juin	→	6	6	→	*juin*
juillet	→	7	7	→	*juillet*
août	→	8	8	→	*août*
septembre	→	9	9	→	*septembre*
octobre	→	10	10	→	*octobre*
novembre	→	11	11	→	*novembre*
décembre	→	12	12	→	*décembre*

Figure 1.3

Souvent, on utilise une bijection $f : A \to B$ pour représenter les éléments d'un ensenble A par ceux d'un ensemble B ; c'est le cas de l'exemple 1.33 où les mois sont représentés par leur numéro.
Comme le montre l'exemple 1.33, une bijection qui va d'un ensemble A vers un ensemble B met en correspondance un à un les éléments de A avec ceux de B ; en retour elle permet d'associer à chaque élément de B un élément de A.
Plus précisément, soit f une bijection de A vers B (*fig.* 1.4). Alors, quel que soit l'élément y de B, il existe x dans A tel que $y = f(x)$ car f est surjective ; cet x est unique car f est injective. L'application de B vers A qui associe x à y s'appelle l'***application réciproque*** de f et on la note f^{-1}. Bien évidemment, f^{-1} aussi est bijective, et f est son application réciproque. Dans l'exemple 1.33 l'élément $f^{-1}(9)$ n'est autre que *septembre*.

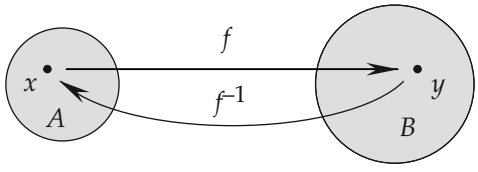

Figure 1.4

1.5.4 Soient $f : A \to B$ et $g : B \to C$ deux applications. Si l'on associe à tout élément x de A l'élément z de C obtenu en calculant d'abord $y = f(x)$, puis $z = g(y)$, on construit une application de A vers C, qu'on appelle l'***application composée*** de f par g et qu'on note[1] $g \circ f$ pour rappeler que $z = g(f(x))$.

[1] On prononce « g rond f ».

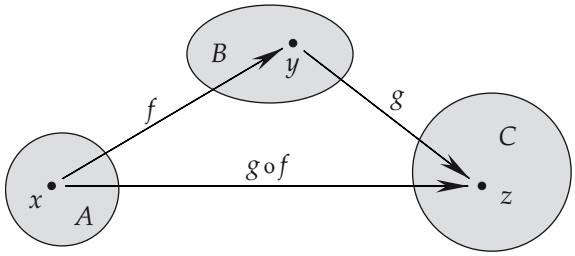

Figure 1.5

Nous avons les résultats suivants dont la démonstration est laissée en exercice.

***Théorème* 1.1**

1. Si f et g sont *injectives*, il en est de même de $g \circ f$.
2. Si f et g sont *surjectives*, il en est de même de $g \circ f$.
3. Si f et g sont *bijectives*, il en est de même de $g \circ f$ et $f^{-1} \circ g^{-1}$ est son application réciproque.

1.6 EXERCICES SUR LE CHAPITRE 1

[1.1] On suppose que l'ensemble de tous les ensembles qui ne sont pas éléments d'eux-mêmes existe et on l'appelle X ; autrement dit, $X = \{x \mid x \notin x\}$.

1. A-t-on $X \in X$? A-t-on $X \notin X$?
2. Quel est le lien avec le paradoxe de Russell ?

[1.2] Montrer que $\wp(A) \subset \wp(B)$ quand $A \subset B$.

[1.3] Est-ce que $\{a\} \in \{a, b, c\}$? Former la liste des parties de $\{a, b, c\}$.

[1.4] On rappelle que les éléments de $\mathbb{B}$ sont 0 et 1.

1. A-t-on $\mathbb{B} \in \mathbb{B}$?
2. Quels sont les éléments de $\wp(\mathbb{B})$?
3. Quels sont les éléments de $\wp\big(\wp(\mathbb{B})\big)$?

[1.5] Quels sont les éléments de $\wp(\varnothing)$? Quels sont ceux de $\wp\big(\wp(\varnothing)\big)$?

[1.6] Si E est un ensemble quelconque, concrètement qu'est-ce qu'un élément de $\wp\big(\wp(E)\big)$?

[1.7] Dans chacun des cas suivants déterminer si les ensembles A et B sont égaux.

1. $A = \{x \in \mathbb{R} \mid x > 0\}$ $\quad B = \{x \in \mathbb{R} \mid x \geqslant |x|\}$
2. $A = \{x \in \mathbb{R} \mid x > 0\}$ $\quad B = \{x \in \mathbb{R} \mid x \leqslant |x|\}$
3. $A = \mathbb{Z}$ $\quad B = \{x \in \mathbb{Z} \mid x^2 - x \text{ pair}\}$
4. $A = \{x \in \mathbb{N}_{20}^{\times} \mid x \text{ impair, non divisible par } 3\}$ $\quad B = \{x \in \mathbb{N}_{20}^{\times} \mid 24 \text{ divise } x^2 - 1\}$
5. $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
   $B = \{\text{l'ensemble des chiffres du développement décimal de } \frac{333630696667}{3000300030003}\}$

[1.8] Définir les ensembles suivants en compréhension :

1. $A = \{1, 2, 4, 8, 16, 32, 64\}$
2. $B = \{1, 2, 7, 14\}$
3. $C = \{4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20\}$

[1.9] Définir les ensembles suivants en extension :

1. $A = \{x \in \mathbb{R} \mid x(x+5) = 14\}$
2. $B = \{x \in \mathbb{N} \mid x(2x+3) = 14\}$
3. $C = \{x \in \mathbb{N}_{25}^{\times} \mid x$ est la somme des carrés de deux entiers naturels $\}$
4. $D = \{x \in \mathbb{N}_{10}^{\times} \mid x^4 - 1$ est divisible par $5\}$

[1.10] Interpréter chacune des situations suivantes au moyen d'une fonction. Pour cela on définira deux ensembles A et B ainsi qu'une fonction $f : A \to B$.

1. Le résultat d'une course de tiercé.
2. Le registre d'un hôtel qui possède 55 chambres.
3. Le numéro d'INSEE.
4. La parité d'un entier naturel.
5. Un emploi du temps.
6. Un livre.
7. La table des matières d'un livre.

[1.11] Si A n'est pas vide, pourquoi $\varnothing^A$ est-il vide ?
Que pourrait-on dire si A était vide ? (★ voir le § 4.3.4 ★)

[1.12] Que peut-on dire de B^A quand B est un *singleton*[1] ?

[1.13] Soient A et B deux ensembles, avec $A \neq \varnothing$. Construire une injection de B dans B^A.

[1.14] Soient E un ensemble quelconque et $f : E \to \wp(E)$.

1. Démontrer que f ne peut pas être surjective. (★ si E est un ensemble fini, on peut raisonner sur le nombre d'éléments, sinon on associe à f la partie X de E, qui peut être vide, formée des éléments x de E tels que $x \notin f(x)$ et on montre qu'il n'existe pas d'élément y de E tel que $f(y) = X$ ★)
2. Quel est le lien avec le paradoxe du barbier ?

[1.15] Soit $f : A \to B$. Montrer qu'il existe toujours un ensemble C, ainsi qu'une surjection $g : A \to C$ et une injection $h : C \to B$ tels que $f = h \circ g$. (★ penser aux exemples 1.23 et 1.28 ★)

[1.16] Si $f : A \to B$ est bijective, démontrer qu'il en est de même pour f^{-1} et déterminer son application réciproque.

[1] Un *singleton* est un ensemble réduit à un seul élément.

[1.17] Dans chaque cas dire si l'application $f : A \to B$ est injective, surjective, ou bijective. Quand elle est bijective déterminer l'application réciproque.

1.	$A = \mathbb{R}$	$B = \mathbb{R}$	$f(x) = x + 7$
2.	$A = \mathbb{R}$	$B = \mathbb{R}$	$f(x) = x^2 + 2x - 3$
3.	$A = \{x \in \mathbb{R} \mid 9 \geqslant x \geqslant 4\}$	$B = \{x \in \mathbb{R} \mid 96 \geqslant x \geqslant 21\}$	$f(x) = x^2 + 2x - 3$
4.	$A = \mathbb{R}$	$B = \mathbb{R}$	$f(x) = 3x - 2\lvert x\rvert$
5.	$A = \mathbb{R}$	$B = \mathbb{R}$	$f(x) = \mathrm{e}^x + 1$
6.	$A = \mathbb{N}$	$B = \mathbb{N}$	$f(x) = x(x + 1)$

[1.18] Soit $f : \mathbb{Z} \to \mathbb{Z}$ définie par $f(n) = n + (-1)^n$.

1. Montrer que n et $f(n)$ sont toujours de parité différente.
2. Montrer que f est bijective.
3. Calculer $f(f(n))$. En déduire une expression de f^{-1} et résoudre l'équation :

$$347 = n + (-1)^n$$

dans laquelle n désigne un entier inconnu.

[1.19] Montrer qu'il existe une bijection entre $\mathbb{N}$ et $\mathbb{Z}$, l'ensemble des entiers relatifs. (★ essayer de la représenter par une formule ★)

[1.20] Soient A, B et C trois ensembles et $f : A \to B$. On suppose $B \subset C$ et on définit $F : A \to C$ en posant $F(x) = f(x)$ pour tout x dans A.

1. Montrer que l'application de B^A vers C^A qui associe F à f est injective.
2. À quelle condition est-elle surjective ?

[1.21] Soient A, B, C trois ensembles et $f : A \to B$. On suppose $C \subset A$ et on définit $F : C \to B$ en posant $F(x) = f(x)$ pour tout x dans C (on dit que F est la ***restriction*** de f à C).

1. Montrer que l'application de B^A vers B^C qui associe F à f est surjective.
2. À quelle condition est-elle injective ?

[1.22] On considère les deux applications f et g de $\mathbb{N}_9^\times$ vers lui-même définies par leurs tables des valeurs :

x	1	2	3	4	5	6	7	8	9
$f(x)$	6	4	7	8	9	3	5	1	2

x	1	2	3	4	5	6	7	8	9
$g(x)$	1	2	7	4	5	6	3	8	9

1. Représenter de la même façon les applications : $g \circ g$, $g \circ f$, $f \circ f$, $f \circ g$.
2. Montrer que f est bijective. Représenter de la même façon son application réciproque.

[1.23] Soient A, B, C, D des ensembles et $f : A \to B$, $g : B \to C$, $h : C \to D$ trois applications. Démontrer que $h \circ (g \circ f) = (h \circ g) \circ f$ (on note $h \circ g \circ f$ cette application).

[1.24] Si E est un ensemble, on appelle ***identité*** de E, et on note Id_E, l'application de E vers E définie par : $\mathrm{Id}_E(x) = x$ quel que soit x dans E.

1. Est-elle injective ? surjective ? bijective ?

À présent soit $f : A \to B$ une application entre deux ensembles non vides A et B.

2. Montrer que l'application f est injective si et seulement si il existe une application $g : B \to A$ telle que $g \circ f = \mathrm{Id}_A$.
3. Montrer que f est surjective si et seulement si il existe $h : B \to A$ telle que $f \circ h = \mathrm{Id}_B$.
4. Quand elles existent les applications g et h sont-elles uniques ?
5. Si f est bijective montrer qu'on a nécessairement $g = h$.

[1.25] Soit $f : A \to A$. On note : $f_0 = \mathrm{Id}_A$, $f_1 = f$, $f_2 = f \circ f$, $f_3 = f \circ f \circ f$ et plus généralement si n est un entier $\geqslant 1$ on pose : $f_{n+1} = f_n \circ f$, ce qui donne :

$$f_n = \underbrace{f \circ f \circ \cdots \circ f \circ f}_{n \text{ fois}}$$

1. Montrer que : $f_{m+n} = f_m \circ f_n$.
2. Si A est un ensemble fini, montrer qu'il existe toujours deux entiers m et n différents tels que $f_m = f_n$.
3. En déduire qu'il existe un plus petit n à partir duquel les applications f_n se répètent périodiquement. Dans le cas où f est une bijection que peut-on dire de plus ?

[1.26] Soient A et B des ensembles non vides, $f : A \to B$ et $g : B \to C$.

1. On suppose $g \circ f$ injective ; montrer que f est injective. Est-ce que g est obligatoirement injective ?
2. On suppose $g \circ f$ surjective ; montrer que g est surjective. Est-ce que f est obligatoirement surjective ?
3. Si f et g sont bijectives démontrer que $g \circ f$ est bijective. Quelle est son application réciproque ?
4. On suppose $g \circ f$ bijective. Que peut-on dire de f et de g ? Est-ce que f et g sont bijectives ?

[1.27] S'il existe une bijection entre A et B et une bijection entre A et C démontrer qu'il existe une bijection entre B et C.

[1.28] *Première partie :* Soit $f : A \to B$. On définit $F : \wp(A) \to \wp(B)$ de la façon suivante. Si $C \subset A$ on note $F(C)$ le sous-ensemble de B ayant pour éléments les images par f des éléments de C et on convient que $F(\varnothing) = \varnothing$.

1. Quelle est l'image par F du singleton $\{x\}$?
2. Montrer que F est injective si f l'est (★ on montrera que si A_1 et A_2 sont deux parties de A telles que $F(A_1) = F(A_2)$, alors $A_1 = A_2$ ★). La réciproque est-elle vraie ?
3. Montrer que F est surjective si f l'est. La réciproque est-elle vraie ?
4. L'application de B^A vers $\wp(B)^{\wp(A)}$ qui associe F à f est-elle injective, surjective, bijective ?

Deuxième partie : On définit une nouvelle application $G : \wp(B) \to \wp(A)$ de la façon suivante : si $D \subset B$ on note $G(D)$ le sous-ensemble de A ayant pour éléments les éléments de A dont l'image par f est dans D (éventuellement $G(D)$ est vide) et on convient que $G(\varnothing) = \varnothing$.

5. L'application G est-elle toujours injective ?

Maintenant on suppose f surjective.

6. Que peut-on dire de $F \circ G$?
7. L'application G est-elle injective ?
8. L'application G est-elle surjective ?

Chapitre **2**

Constructions d'ensembles

Ici, nous verrons comment on peut construire des ensembles compliqués à partir d'ensembles plus simples. La notion de produit d'ensembles permet de donner une interprétation mathématique à de nombreuses situations concrètes. D'une certaine façon, elle est le point de départ de l'étude des bases de données.

MOTS-CLÉS : produit - diagramme cartésien - couple - triplet - n-uple - fonction de plusieurs variables - famille d'ensembles - puissances d'un ensemble - paire d'éléments - réunion - union - intersection - ensembles disjoints - somme disjointe.

2.1 PRODUIT D'ENSEMBLES

2.1.1 À partir de deux ensembles A et B, on peut toujours construire un nouvel ensemble qu'on appelle le ***produit*** de A par B ; on le note $A \times B$ et ses éléments sont les ***couples*** (a, b) formés en prenant de toutes les façons possibles un élément a dans A et un élément b dans B.

***Exemple* 2.1 :** Avec $A = \{Z, T\}$ et $B = \{1, 2, 3\}$, les éléments de $A \times B$ sont les 6 couples :

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

alors que les éléments de $B \times A$ sont :

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

Cet exemple montre comment former la liste des éléments de $A \times B$ quand A et B sont définis en extension. La méthode est générale, le produit de deux ensembles définis en extension peut toujours être défini en extension.

Lorsqu'on fait l'inventaire des couples, on a parfois intérêt à ne pas les disposer à la suite, l'un derrière l'autre. Souvent, il vaut mieux les ranger de façon que deux couples *qui se ressemblent* se retrouvent l'un à côté de l'autre. Pour cela, on représente $A \times B$ au moyen de son ***diagramme cartésien***. Il s'agit d'un rectangle découpé en cases qui correspondent chacune à un couple (*fig. 2.1*). Chaque ligne du rectangle correspond à un élément de A car on y trouve tous les couples ayant cet élément pour première composante, et chaque colonne correspond à un élément de B car on y trouve tous les couples ayant cet élément pour deuxième composante.

***Exemple* 2.2 :** Pour les ensembles A et B de l'exemple 2.1, la figure 2.1 représente le diagramme cartésien de $A \times B$ et la figure 2.2 celui de $B \times A$.

$(Z,1)$	$(Z,2)$	$(Z,3)$
$(T,1)$	$(T,2)$	$(T,3)$

Figure 2.1

$(1,Z)$	$(1,T)$
$(2,Z)$	$(2,T)$
$(3,Z)$	$(2,T)$

Figure 2.2

Souvent on se contente d'indiquer autour du rectangle les éléments de A et de B qui correspondent aux lignes et aux colonnes (*fig. 2.3 et 2.4*), ce qui évite d'écrire le nom des couples dans les cases ; c'est d'ailleurs la méthode employée avec les coordonnées cartésiennes, d'où le mot *cartésien*.

	1	2	3
Z			
T			

Figure 2.3

	Z	T
1		
2		
3		

Figure 2.4

Remarque : L'ordre dans lequel on range les éléments de A et de B détermine la position des couples dans le diagramme, si l'on change cet ordre, le diagramme n'est plus le même.

2.1.2 La notion de produit s'étend à un nombre quelconque d'ensembles. En effet, on peut construire le produit $E_1 \times E_2 \times \cdots \times E_n$ de n ensembles $E_1, E_2, \ldots, E_n$. Les éléments $(e_1, e_2, \ldots, e_n)$ de ce produit s'appellent des ***n-uples***[1]. Ils sont obtenus en prenant de toutes les façons possibles un élément e_1 dans E_1, qui sera la ***première composante*** du n-uple, un élément e_2 dans E_2, qui sera la ***deuxième composante***, et ainsi de suite, jusqu'à e_n, sa n^e composante.

Quand $u_1 = v_1$, $u_2 = v_2$, … , $u_n = v_n$ les deux n-uples $u = (u_1, u_2, \ldots, u_n)$ et $v = (v_1, v_2, \ldots, v_n)$ sont *égaux* ; on écrit $u = v$. Par conséquent, écrire l'égalité de deux n-uples est une façon abrégée d'écrire n égalités.

D'un point de vue concret, construire un n-uple c'est choisir un premier objet dans un premier ensemble, un deuxième objet dans un deuxième ensemble, etc., jusqu'au

[1] À la place de 2-uple et 3-uple on préfère dire ***couple*** et ***triplet***.

n^e objet dans le n^e ensemble. C'est une situation très commune et, sans le savoir, on rencontre beaucoup de n-uples dans la vie de tous les jours !

***Exemple* 2.3 :** La figure 2.5 représente la carte proposée, aujourd'hui, au restaurant du CNAM ; composer son menu consiste à choisir une entrée, un plat principal, un légume et un dessert. Si l'on note $\mathcal{E}$ l'ensemble des entrées, $\mathcal{P}$ l'ensemble des plats principaux, $\mathcal{L}$ l'ensemble des légumes, et $\mathcal{D}$ l'ensemble des desserts, chaque menu, par exemple (Carottes râpées, Poisson frit, Épinards, Pomme), est un élément de $\mathcal{E} \times \mathcal{P} \times \mathcal{L} \times \mathcal{D}$.

Figure 2.5

2.1.3 On peut se demander si la multiplication des ensembles a des propriétés analogues à celle des nombres.

Dans l'exemple 2.1 chaque élément de $A \times B$ est constitué d'une lettre et d'un chiffre, tandis que chaque élément de $B \times A$ est constitué d'un chiffre et d'une lettre, ce qui n'est pas la même chose. D'une façon générale, quand les ensembles A et B ne sont pas égaux, les deux produits $A \times B$ et $B \times A$ ne le sont pas non plus ; le produit des ensembles n'est donc pas *commutatif*. Cependant les deux produits se ressemblent beaucoup et il est toujours possible de les mettre en correspondance bijective, la bijection la plus naturelle, qu'on appelle la ***bijection canonique*** de $A \times B$ vers $B \times A$, étant celle qui associe le couple (b, a) au couple (a, b).

Après la commutativité on peut s'intéresser à l'*associativité* du produit en se demandant, quand trois ensembles A, B et C sont donnés, si les produits $A \times B \times C$ et $(A \times B) \times C$ sont toujours égaux. Il est clair que cela n'arrive jamais, car un élément

de $A \times B \times C$ est un triplet, alors qu'un élément de $(A \times B) \times C$ est un couple, dont la première composante est elle-même un couple, ce qui, formellement, n'est pas pareil. Toutefois il existe toujours des bijections entre $A \times B \times C$ et $(A \times B) \times C$, la plus naturelle étant celle qui associe le couple $\big((a,b),c\big)$ au triplet (a,b,c) ; on l'appelle la ***bijection canonique*** de $A \times B \times C$ vers $(A \times B) \times C$.

2.1.4 Considérons trois ensembles A, B et C. Une fonction $f : B \times C \to A$ associe au couple (b,c) un élément a de A ; pour simplifier, on le note $f(b,c)$ au lieu de $f\big((b,c)\big)$. Lorsque b et c varient, a varie lui aussi, et on dit que f est une ***fonction de 2 variables***.

D'une façon générale, si A et $E_1, E_2, \ldots, E_n$ sont des ensembles, un élément f de $A^{E_1 \times E_2 \times \ldots \times E_n}$ s'appelle une ***fonction de n variables***. L'élément de A associé par f au n-uple $(e_1, e_2, \ldots, e_n)$ est noté $f(e_1, e_2, \ldots, e_n)$ au lieu de $f\big((e_1, e_2, \ldots, e_n)\big)$.

2.2 PRODUIT D'UNE FAMILLE D'ENSEMBLES

2.2.1 Jusqu'ici nous n'avions qu'un nombre fini d'ensembles, mais on peut aussi construire des produits infinis ; voici quelques indications sur la marche à suivre.

Considérons un ensemble I appelé ensemble des ***indices.*** En associant à chaque élément i de I un ensemble E_i on obtient ce qu'on appelle une ***famille*** d'ensembles indexée par I ; on note $(E_i)_{i \in I}$ cette famille.

À partir de $(E_i)_{i \in I}$ on peut fabriquer un nouvel ensemble qu'on appelle le ***produit*** de la famille. On le note $\prod_{i \in I} E_i$; ses éléments sont la généralisation des n-uples, ils sont formés de composantes ; il y en a une pour chaque valeur de l'indice i, choisie dans l'ensemble E_i correspondant.

> ***Exemple* 2.4 :**
> En associant à chaque entier naturel $n \geqslant 1$ l'ensemble $\mathbb{B}^n$ des mots binaires de longueur n on construit une famille d'ensembles indexée par $\mathbb{N}^\times$. Le produit de cette famille a pour éléments les suites infinies constituées d'un mot de longueur 1, un mot de longueur 2, etc., par exemple : (1, 01, 110, 1101, 00111, ...).

La notion de produit d'une famille d'ensembles généralise celle de produit de n ensembles. En effet, si $I = \mathbb{N}_n^\times$, une famille indexée par I c'est n ensembles $E_1, \ldots, E_n$ et le produit de la famille est bien le produit de ces n ensembles. Elle sert aussi à construire le produit de plusieurs ensembles qui n'ont pas été numérotés mais qui sont indexés au moyen d'un ensemble particulier d'indices.

> ***Exemple* 2.5 :** Dans un jeu de 52 cartes examinons en quoi consiste la donnée d'un cœur, d'un pique, d'un trèfle ou d'un carreau. Prenons comme ensemble d'indices $\{\heartsuit, \spadesuit, \clubsuit, \diamondsuit\}$ et associons à chaque indice l'ensemble des cartes de la couleur correspondante[1]. Alors se donner une carte de chaque couleur c'est se donner un élément du produit des ensembles de la famille.

Enfin, quand $I = \mathbb{N}^\times$, comme dans l'exemple 2.4, ou plus généralement quand I est infini, la notion de produit d'une famille d'ensembles permet de construire le produit d'une infinité d'ensembles.

---

[1] Dans les jeux de cartes, contrairement à ce qu'on pourrait penser, le mot *couleur* ne désigne pas *rouge* ou *noir*, mais ***cœur***, ***pique***, ***trèfle*** ou ***carreau***.