COURS DE MATHÉMATIQUES PREMIÈRE ANNÉE (L1)

UNIVERSITÉ DENIS DIDEROT PARIS 7

Marc HINDRY

Tous les chapitres sont importants. Le premier chapitre est volontairement bref mais fondamental : il y aura intérêt à revenir sur les notions de langage mathématique et de raisonnement tout au long du cours, à l'occasion de démonstrations. Les chapitre 19 et 20 reposent sur une synthèse de l'algèbre (linéaire) et de l'analyse (calcul différentiel et intégral) tout en étant assez géométriques. Le chapitre 21 (fonctions de plusieurs variables) appartient en pratique plutôt à un cours de deuxième année; il a été ajouté pour les étudiants désirant anticiper un peu ou ayant besoin, par exemple en physique, d'utiliser les fonctions de plusieurs variables et dérivées partielles, dès la première année.

L'ordre des chapitres. L'ordre choisi n'est que l'un des possibles. En particulier on pourra vouloir traiter l'"analyse" (chapitres 12-20) en premier : pour cela on traitera d'abord le chapitre sur les nombres réels et complexes (ou la notion de limite est introduite très tôt), le principe de récurrence et on grapillera quelques notions sur les polynômes et l'algèbre linéaire. La séquence d'algèbre linéaire (chapitres 7-11) est très inspirée de la présentation par Mike Artin (Algebra, Prentice-Hall 1991) mais on peut choisir bien d'autres présentations. On pourra aussi par exemple préférer étudier **Z** avant **R** et **C** (du point de vue des constructions, c'est même préférable!). Le chapitre 16 sur les fonctions usuelles peut être abordé à peu près à n'importe quel moment, quitte à s'appuyer sur les notions vues en terminale.

Nous refusons le point de vue : "... cet ouvrage part de zéro, nous ne supposons rien connu...". Au contraire nous pensons qu'il faut s'appuyer sur les connaissances de terminale et sur l'intuition (notamment géométrique). Il semble parfaitement valable (et utile pédagogiquement) de parler de droites, courbes, plans, fonction exponentielle, logarithme, sinus, etc ... avant de les avoir formellement introduit dans le cours. Il semble aussi dommage de se passer complètement de la notion très intuitive d'angle sous prétexte qu'il s'agit d'une notion délicate à définir rigoureusement (ce qui est vrai).

Illustrations : Nous avons essayé d'agrémenter le cours d'applications et de motivations provenant de la physique, de la chimie, de l'économie, de l'informatique, des sciences humaines et même de la vie pratique ou récréative. En effet nos pensons que même si on peut trouver les mathématiques intéressantes et belles en soi, il est utile de savoir que beaucoup des problèmes posés ont leur origine ailleurs, que la séparation avec la physique est en grande partie arbitraire et qu'il est passionnant de chercher à savoir à quoi sont appliquées les mathématiques.

Indications historiques Il y a hélas peu d'indications historiques faute de temps, de place et de compétence mais nous pensons qu'il est souhaitable qu'un cours contienne des allusions : 1) au développement historique, par exemple du calcul différentiel 2) aux problèmes ouverts (ne serait-ce que pour mentionner leur existence) et aux problème résolus disons dans les dernières années. Les petites images (mathématiques et philathéliques) incluses à la fin de certains chapitres sont donc une invitation à une recherche historique.

Importance des démonstrations Les mathématiques ne se réduisent pas à l'exactitude et la rigueur mais quelque soit le point de vue avec lequel ont les aborde la notion de démonstration y est fondamentale. Nous nous efforçons de donner presque toutes les démonstrations. L'exception la plus notable est la construction des fonctions cosinus et sinus, pour laquelle nous utiliserons l'intuition géométrique provenant de la représentation du cercle trigonométrique ; l'intégrabilité des fonctions continues sera aussi en partie admise.

Il y a là une difficulté qui sera levée avec l'étude des fonctions analytiques (faite en seconde année).

Difficulté des chapitres Elle est inégale et bien sûr difficile à évaluer. Certains chapitres développent essentiellement des techniques de calculs (chapitres 6, 7, 10, 16, 17, 18, 19, 20), le chapitre 11 reprend du point de vue de l'algèbre linéaire des notions vues en terminales, d'autres développent des concepts (chapitres 2, 3, 4, 5, 8, 9, 12, 13, 15) et sont donc en ce sens plus difficiles ; le chapitre 14 est intermédiaire dans cette classification un peu arbitraire. Enfin le chapitre 21 n'est destiné à être appronfondi qu'en deuxième année.

Résumés En principe les énoncés importants sont donnés sous l'entête "thèorème" suivis par ordre décroissant d'importance des "propositions" et des "lemmes". Un "résumé" de chaque chapitre peut donc être obtenu en rassemblant les énoncés des théorèmes (et les définitions indispensables à la compréhension des énoncés). Nous avons seulement inclus un chapitre résumant et synthétisant les différents points de vue développés en algèbre linéaire (après le chapitre 11).

Archimède [$A\rho\chi\iota\mu\acute{\eta}\delta\eta\varsigma$] ($\sim$ 287–$\sim$ 212)

Al Khwārizmī (fin VIII^{e}, début IX^{e})

CHAPITRE 1 LE LANGAGE MATHÉMATIQUE

Ce chapitre, volontairement court, précise les modalités du raisonnement mathématique. En effet on n'écrit pas un texte mathématique comme un texte de langage courant : ce serait théoriquement possible mais totalement impraticable pour de multiples raisons (le raccourci des "formules" est notamment une aide précieuse pour l'esprit).

Une *définition* précise le sens mathématique d'un mot ; par exemple :

Définition: Un ensemble E est fini si il n'est pas en bijection avec lui-même privé d'un élement. Un ensemble est infini si il n'est pas fini.

On voit tout de suite deux difficultés avec cet exemple : d'abord il faut avoir défini "ensemble" (ce que nous ne ferons pas) et "être en bijection" (ce qu'on fera au chapitre suivant) pour que la définition ait un sens ; ensuite il n'est pas immédiat que la définition donnée coïncide avec l'idée intuitive que l'on a d'un ensemble fini (c'est en fait vrai).

Un *énoncé mathématique* (nous dirons simplement *énoncé*) est une phrase ayant un sens mathématique précis (mais qui peut être vrai ou faux) ; par exemple :

(A) 1=0

(B) Pour tout nombre réel x on a $x^2 \geq 0$

(C) $x^3 + x = 1$

sont des énoncés ; le premier est faux, le second est vrai, la véracité du troisième dépend de la valeur de la variable x. Par contre, des phrases comme "les fraises sont des fruits délicieux", "j'aime les mathématiques" sont clairement subjectives. L'affirmation : "l'amiante est un cancérogène provoquant environ trois mille décès par an en France et le campus de Jussieu est floqué à l'amiante" n'est pas un énoncé mathématique, même si l'affirmation est exacte. Nous ne chercherons pas à définir précisément la différence entre énoncé mathématique et énoncé non mathématique.

Un *théorème* est un énoncé vrai en mathématique ; il peut toujours être paraphrasé de la manière suivante : "Sous les hypothèses suivantes : .... , la chose suivante est toujours vraie :... ". Dans la pratique certaines des hypothèses sont omises car considérés comme vraies a priori : ce sont les *axiomes*. La plupart des mathématiciens sont d'accord sur un certain nombre d'axiomes (ceux qui fondent la théorie des ensembles, voir chapitre suivant) qui sont donc la plupart du temps sous-entendus.

Par exemple nous verrons au chapitre 5 que :

THÉORÈME: *Soit n un nombre entier qui n'est pas le carré d'un entier alors il n'existe pas de nombre rationnel x tel que $x^2 = n$ (en d'autres termes $\sqrt{n}$ n'est pas un nombre rationnel).*

Pour appliquer un théorème à une situation donnée, on doit d'abord vérifier que les hypothèses sont satisfaites dans la situation donnée, traduire la conclusion du théorème dans le contexte et conclure.

Par exemple : prenons $n = 2$ (puis $n = 4$) alors 2 n'est pas le carré d'un entier donc le théorème nous permet d'affirmer que $\sqrt{2}$ n'est pas un nombre rationnel. Par contre l'hypothèse n'est pas vérifiée pour $n = 4$ et le théorème ne permet pas d'affirmer que $\sqrt{4}$ n'est pas un nombre rationnel (ce qui serait d'ailleurs bien sûr faux!).

Les *connecteurs logiques* permettent de fabriquer de nouveaux énoncés à partir d'autres ; nous utiliserons exclusivement les connecteurs suivants :

non : non(A) est vrai si et seulement si (A) est faux

ou : (A) *ou* (B) est vrai si et seulement si (A) est vrai ou (B) est vrai.

et : (A) *et* (B) est vrai si et seulement si (A) est vrai et (B) est vrai.

implique (en symbole $\Rightarrow$) : (A) *implique* (B) est vrai si et seulement si chaque fois que (A) est vrai alors (B) est aussi vrai.

équivaut (en symbole $\Leftrightarrow$) : (A) équivaut (B) est vrai si (A) est vrai chaque fois que (B) est vrai et réciproquement.

Une *démonstration logique* (nous dirons ensuite simplement une démonstration) est un énoncé, comportant éventuellement comme variable d'autres énoncés de sorte qu'il soit vrai quel que soit les énoncés variables. Voici des exemples de démonstration :

Si $(A) \Rightarrow (B)$ et $(B) \Rightarrow (C)$ alors $(A) \Rightarrow (C)$

$non(non(A))$ équivaut à (A)

Si $(A) \Rightarrow (B)$ et $non(B)$ alors $non(A)$.

Si (A) *ou* (B) et $non(B)$ alors (A).

Bien entendu, les démonstrations "intéressantes" en mathématiques sont plus longues et sont composées de chaînes d'implications élémentaires comme celles qui précèdent. Une manière simple (mais fastidieuse) de vérifier ce type d'énoncé est faire un tableau avec les diverses possibilités : chaque énoncé est vrai ou faux (V ou F). Par exemple, pour le premier énoncé il y a huit possibilités :

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

On constate bien que chaque fois que $A \Rightarrow B$ et $B \Rightarrow C$ sont simultanément vrais alors $A \Rightarrow C$ est vrai aussi.

Exemples de raisonnements parmi les plus utilisés :

Raisonnement cas par cas :
Schéma : si (A) *ou* (B), $(A) \Rightarrow (C)$ et $(B) \Rightarrow (C)$, alors C

Raisonnement par contraposée :
Schéma : si $(A) \Rightarrow (B)$, alors $non(B) \Rightarrow non(A)$

Raisonnement par l'absurde :
Schéma : si $(B) \Rightarrow (A)$ *et* $non(A)$, alors $non(B)$.

On voit qu'il n'y a aucune difficulté fondamentale avec les raisonnements logiques, la seule difficulté est parfois d'arriver à enchaîner les déductions. A titre d'exercice on vérifiera les déductions suivantes :

$non((A)\ ou\ (B)) \Leftrightarrow (non(A)\ et\ non(B))$

$non((A)\ et\ (B)) \Leftrightarrow (non(A)\ ou\ non(B))$

$non(A)\ ou\ (B) \Leftrightarrow (A \Rightarrow B)$

$(A\ et\ B)\ ou\ (C) \Leftrightarrow (A\ ou\ C)\ et\ (B\ ou\ C)$

Les *quantificateurs* permettent de transformer un énoncé contenant une variable en un énoncé "absolu" : nous utiliserons exclusivement deux quantificateurs :
il existe (en symbole $\exists$)
pour tout (en symbole $\forall$)

Exemple : considérons les énoncés suivants contenant la variable $x \in \mathbf{R}$.

$$A(x)\ : x^2 - 1 = 0$$
$$B(x)\ : x^2 + x = x(x+1)$$
$$C(x)\ : x + 1 = x$$

L'affirmation ($\forall x \in \mathbf{R}\ non(C(x))$) tout comme ($\exists x \in \mathbf{R}\ A(x)$) est vraie. Par contre il est faux que : $\forall x \in \mathbf{R}\ A(x)$

La négation de $\forall x\ A(x)$ est $\exists x\ non(A(x))$. La négation de $\exists x\ A(x)$ est $\forall x\ non(A(x))$. Par exemple la négation de :

$$(A)\ :\ \ \forall x \in \mathbf{R},\ \forall \epsilon \in \mathbf{R}_+^*,\ \exists \delta \in \mathbf{R}_+^*,\ \forall y \in \mathbf{R},\ |x-y| \leq \delta \Rightarrow |f(x) - f(y)| \leq \epsilon$$

est :

$$non(A)\ :\ \ \exists x \in \mathbf{R},\ \exists \epsilon \in \mathbf{R}_+^*,\ \forall \delta \in \mathbf{R}_+^*,\ \exists y \in \mathbf{R},\ |x-y| \leq \delta \text{ et } |f(x) - f(y)| > \epsilon$$

Remarque : l'énoncé (A) écrit que la fonction f est continue en tout point alors que $non(A)$ écrit qu'il existe un point où f n'est pas continue (voir chapitre 13).

Commentaires : la nécessité de la formalisation du raisonnement mathématique et de la notion d'ensemble a accompagné historiquement l'apparition de *paradoxes* au tournant de ce siècle. Ceux-ci sont essentiellement de deux types : paradoxes sémantiques et paradoxes logiques.

Un exemple de paradoxe sémantique est le suivant : on choisit un dictionnaire de langue française et on considère l'ensemble S des nombres entiers que l'on peut définir à l'aide de moins de vingt mots de ce dictionnaire. Comme le nombre de mots est fini et le nombre de phrase de moins de vingt mots est fini, l'ensemble S est fini ; il existe donc "Le plus petit nombre entier que l'on ne peut pas définir en moins de vingt mots". Mais nous venons de le définir en moins de vingt mots!

Un exemple de paradoxe logique (dû à Russel) est le suivant : considérons l'ensemble S formé de tous les éléments qui ne s'appartiennent pas à eux-mêmes ; en symboles :

$$S := \{x \mid x \notin x\}$$

Cet ensemble à l'air inoffensif mais si on pense que $S \in S$ alors on en déduit $S \notin S$ et inversement!

La méthode pour éliminer les paradoxes du premier type est de se restreindre au langage purement mathématique (ou plus précisément de séparer langage et métalangage, nous ne précisons pas cette notion) : on se borne à travailler avec des notions qui peuvent s'écrire en langage symbolique (idéalement on pourrait penser à écrire tout en langage symbolique, mais on s'aperçoit vite que pour des raisons de longueur, c'est impraticable).

La méthode pour éliminer les paradoxes du type "Russel" est de restreindre la notion d'ensemble ; en particulier on déclare qu'on ne peut pas former un ensemble seulement à partir d'un énoncé avec variables. Ainsi $S := \{x \mid A(x)\}$ ne définit pas nécessairement un ensemble ; par contre, si T est un ensemble alors $S := \{x \in T \mid A(x)\}$ définit encore un (sous-)ensemble.

Terminons ce premier chapitre par une description lapidaire de l'usage et de la place des mathématiques au sein des autres sciences.

Un des paradigmes des sciences peut être succintement décrit par le diagramme suivant :

$$\begin{array}{ccc} \text{observation} & \longrightarrow & \text{modélisation} \\ \downarrow & & \downarrow \quad \text{Math.} \\ \text{expérience} & \longrightarrow & \text{prédiction} \end{array}$$

Concernant les *applications* des notions de ce cours en sciences indiquons par une flèche quelques unes des plus marquantes :

- Algèbre et Arithmétique $\rightarrow$ informatique;
- Théorie des groupes $\rightarrow$ chimie;
- Calcul différentiel et intégral $\rightarrow$ physique;
- Equations différentielles $\rightarrow$ physique, biologie, économie;

Exercice : (logique, inégalités, ...)

Sachant que les statistiques disponibles (code 163 de l'INSERM) indiquent 902 décès pour l'année 1994 par mésothéliome de la plèvre (cancer mortel, causé par l'inhalation de fibres d'amiante), discuter la compatibilité des déclarations suivantes du professeur Brochard, chercheur à l'INSERM, membre du Comité Permanent Amiante (C.P.A) :

(a) "Le mésothéliome est un cancer rare, moins de 200 cas par an [en France]" (C.P.A, l'amiante et la santé, page 13, 1994). (b) "Au moins 150 mésothéliomes dus à l'amiante [par an en France]" (déclaration sur TF1, fin 1994). (c) "On aurait en fait 440 mésothéliomes par an en France" (rapport destiné au ministère du travail, novembre 1994)

"Environ 600 mésothéliomes pleuraux en 1992, en France" (conférence internationale sur le mésothéliome à Créteil, 1995)(*)

Indications : on pourra utiliser les tables de vérité et aussi le fait que le C.P.A a été créé et financé par les industriels de l'amiante et géré par l'agence de communnication et lobbying "Communications Economiques et Sociales" (C.E.S. 10 Avenue de Messine, 75008 Paris).

(*) Post-Scriptum (1996) Le rapport INSERM sur "*les effets sur la santé de l'amiante*" conclut qu'il y a *au minimum* 750 décès par an en France dus aux mésothéliomes causés par l'amiante.

CHAPITRE 2 ENSEMBLES ET APPLICATIONS.

Georg Cantor, le fondateur de la théorie des ensembles définissait un ensemble comme "un groupement d'objets déterminés et bien distincts, de notre perception ou de notre entendement, et que l'on appelle les éléments de l'ensemble". Nous considèrerons la notion d'ensemble comme intuitive en gardant néanmoins en mémoire le fait qu'on ne peut pas considérer "n'importe quoi" comme un ensemble si l'on veut éviter les contradictions. Nous allons donc juste définir les opérations usuelles sur les ensembles (sous-ensembles, complémentaires, intersections, unions, produits, ensemble des parties) puis nous abordons les deux points cruciaux : la notion de fonction (ou application) qui est fondamentale dans toutes les mathématiques et le concept d'infini avec l'exemple fondamental : l'ensemble des entiers naturels, noté **N**, *est infini.*

2.1 ENSEMBLES

Dans la pratique il y a deux façons de construire ou décrire des ensembles : en donnant la liste de ses éléments, par exemple $E := \{0, 1, 2, 3, 5, 7, 8\}$ est un ensemble, ou bien en décrivant une caractérisation des éléments, par exemple nous admettrons que $\mathbf{N} := \{n \mid n \text{ est un entier naturel}\}$ est un ensemble. Parmi les ensembles les plus importants nous étudierons outre $\mathbf{N}$ déjà cité, l'ensemble des nombres entiers relatifs, noté $\mathbf{Z}$, l'ensemble des nombres rationnels, noté $\mathbf{Q}$, l'ensemble des nombres réels, noté $\mathbf{R}$ et l'ensemble des nombres complexes, noté $\mathbf{C}$.

Ensemble vide : il s'agit de l'ensemble ne contenant aucun élément ; on le note $\emptyset$; on peut aussi le définir comme $\emptyset := \{x \mid x \neq x\}$

Relations entre éléments et ensembles :

Un ensemble E est donc une collection d'objets qu'on appelle éléments ; pour chaque élément x on écrit $x \in E$ (lire "x appartient à E"). Si l'élément x n'est pas dans l'ensemble E on écrira $x \notin E$ (lire "x n'appartient pas à E").

Par exemple il est clair que $4 \in \mathbf{N}$ et $4 \notin \emptyset$. Quelque soit l'élément x on a toujours $x \notin \emptyset$.

On dit qu'un ensemble E est *inclus* dans un autre ensemble F (ce qu'on note $E \subset F$), si tous les éléments de E sont aussi dans F ; en d'autres termes si $x \in E \Rightarrow x \in F$. Deux ensembles sont égaux si ils ont les mêmes éléments ; en particulier :

$$E \subset F \; et \; F \subset E \Leftrightarrow E = F$$

Par exemple $\emptyset \subset \mathbf{N}$ mais les ensembles ne sont pas égaux (donc $non(\mathbf{N} \subset \emptyset)$ ou encore $\mathbf{N} \not\subset \emptyset$).

Opérations sur les ensembles :

Sous-ensemble : si E est un ensemble et $A(x)$ un énoncé avec une variable x dans E, on peut fabriquer l'ensemble :

$$\{x \in E \mid A(x)\}$$

Par exemple l'ensemble des nombres entiers pairs est décrit par :

$$\mathcal{P} := \{x \in \mathbf{N} \mid \exists y \in \mathbf{N}, \; x = 2y\}$$

Complémentaire : Soit F un sous-ensemble de E ; on définit le complémentaire de F dans E que l'on note $\complement_E F$ (ou simplement $\complement F$ si E est sous-entendu) comme l'ensemble des éléments de E qui n'appartiennent pas à F :

$$\complement_E F := \{x \in E \mid x \notin F\}$$

Si F n'est plus nécessairement un sous-ensemble de E on emploiera la notation : $E \setminus F$ pour désigner $\{x \in E \mid x \notin F\}$.

Par exemple le complémentaire de $\mathcal{P}$ dans $\mathbf{N}$ est l'ensemble des nombres impairs :

$$\complement_{\mathbf{N}} \mathcal{P} = \mathcal{I} := \{x \in \mathbf{N} \mid \exists y \in \mathbf{N},\ x = 2y + 1\}$$

Intersection : si E et F sont deux ensembles on peut former un ensemble appelé leur intersection notée $E \cap F$ et définie par :

$$E \cap F := \{x \in E \mid x \in F\} = \{x \in F \mid x \in E\} = \{x \mid x \in E \text{ et } x \in F\}$$

Par exemple, si $E = \{0, 1, 2, 3, 5, 7, 8\}$ et $\mathcal{P}$ désigne l'ensemble des entiers pairs, alors $E \cap \mathcal{P} = \{0, 2, 8\}$.

Union : si E et F sont deux ensembles on peut former un ensemble appelé leur union et notée $E \cup F$ et définie par :

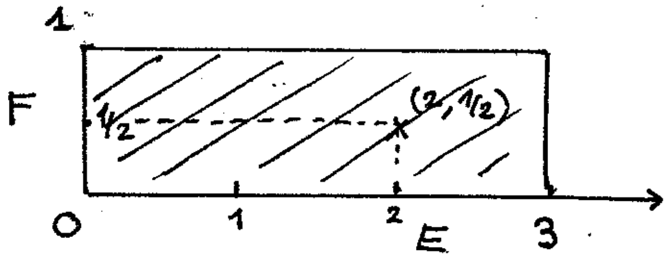
$$E \cup F := \{x \mid x \in E \text{ ou } x \in F\}$$

Par exemple si $E := \{0, 1, 2, 3, 5, 7, 8\}$ et $F := \{0, 1, 2, 4, 8, 16, 32\}$ alors $E \cup F = \{0, 1, 2, 3, 4, 5, 7, 8, 16, 32\}$

Produit : Si $x \in E$ et $y \in F$ on peut fabriquer un nouvel élément appelé *couple* et noté (x, y), caractérisé par le fait que $(x, y) = (z, t)$ si et seulement si $x = z$ et $y = t$. L'ensemble de ces couples s'appelle le produit (cartésien) de E et F et se note :

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

Pour se représenter un produit cartésien on aura avantage à avoir en tête l'exemple suivant : soit $E := [0, 3]$ (l'intervalle des nombres réels compris entre 0 et 3) et $F := [0, 1]$ alors $E \times F$ est le rectangle de la figure suivante



Un autre exemple familier est celui du plan que l'on peut représenter comme le produit $\mathbf{R} \times \mathbf{R}$.

Ensemble des parties : Soit E un ensemble, on peut former un nouvel ensemble dont les éléments sont les sous-ensembles de E et que l'on note $\mathcal{P}(E)$:

$$\mathcal{P}(E) := \{F \mid F \subset E\}$$

Par exemple $\mathcal{P}(\emptyset) = \{\emptyset\}$ (ensemble avec un élément) mais on a aussi $\mathcal{P}(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$ (ensemble avec quatre éléments)

Remarque : on notera que l'on n'a pas donné de démonstration pour l'existence de l'union, du produit etc. En fait il faut comprendre ces énoncés comme des *axiomes* i.e. des énoncés élémentaires que l'on admet être vrais et à partir desquels on va démontrer toutes les autres affirmations. Le caractère extrêmement intuitif (on a envie de dire "évident" de ces axiomes fait qu'ils sont admis par presque tout le monde).

Calculs sur les ensembles : il est très important de savoir calculer et raisonner sur les ensembles ; il faut aussi remarquer que le calcul sur les ensembles est entièrement analogue au calcul sur les propositions ; en effet l'union correspond au connecteur *ou*, l'intersection correspond au connecteur *et* et la relation d'inclusion correspond à l'implication, prendre le complémentaire correspond au connecteur *non* : si les éléments x de A sont caractérisés par la propriété $P(x)$ et ceux de B par la propriété $Q(x)$ alors :

Les éléments x de $A \cup B$ sont caractérisés par la propriété $P(x)$ *ou* $Q(x)$.

Les éléments x de $A \cap B$ sont caractérisés par la propriété $P(x)$ *et* $Q(x)$.

La relation $A \subset B$ équivaut à l'implication $\forall x,\ P(x) \Rightarrow Q(x)$.

Les éléments x de $\complement_E A$ sont caractérisés, parmi les éléments de E par la propriété $non(A(x))$.

Ainsi le calcul sur les ensembles peut toujours se ramener au calcul propositionnel ; voici une liste (non exhaustive) de formules où $A, B, C, \ldots$ sont des ensembles :

Formulaire

$A \cap B = B \cap A$ et $A \cup B = B \cup A$ (commutativité)
$A \cap (B \cap C) = (A \cap B) \cap C$ et $A \cup (B \cup C) = (A \cup B) \cup C$ (associativité)
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ et $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (distributivité)
$\complement_E(\complement_E A) = A$
$(A \subset B) \Rightarrow (\complement_E B \subset \complement_E A)$
$\complement_E(A \cup B) = \complement_E A \cap \complement_E B$ et $\complement_E(A \cap B) = \complement_E A \cup \complement_E B$ (loi de Morgan)
$A \times (B \cap C) = (A \times B) \cap (A \times C)$ et $A \times (B \cup C) = (A \times B) \cup (A \times C)$
$(A \subset B)$ *et* $(C \subset D) \Rightarrow A \times C \subset B \times D$

Démonstration: Démontrons la première formule de distributivité :

$x \in A \cap (B \cup C) \Leftrightarrow x \in A$ *et* $(x \in B$ *ou* $x \in C) \Leftrightarrow (x \in A$ *et* $x \in B)$*ou*$(x \in A$ *et* $x \in C) \Leftrightarrow x \in (A \cap B) \cup (A \cap C)$.

La loi de Morgan se démontre de manière similaire :

$$x \in \complement(A \cup B) \Leftrightarrow non(x \in A \text{ ou } x \in B) \Leftrightarrow non(x \in A) \text{ et } non(x \in B) \Leftrightarrow x \in \complement A \cap \complement B$$

Les autre démonstrations sont similaires et laissées en exercice. □

2.2 APPLICATIONS

Définition: Une *application* (ou *fonction*) définie sur X et à valeurs dans Y est une loi qui, à tout élément de X fait correspondre un unique élément de Y. Si on note f cette application, l'élément associé à x par f est noté $f(x)$. L'ensemble X s'appelle l'*ensemble de départ*, l'ensemble Y s'appelle l'*ensemble d'arrivée* de f. On note souvent une fonction $f : X \to Y$ ou, si les ensembles X et Y sont sous-entendus $x \mapsto f(x)$. L'élément $f(x) = y$ s'appelle l'*image* de x par f et x s'appelle un *antécédent* de y par f.

Remarque : une fonction peut être définie par son *graphe*, un sous-ensemble $\Gamma \subset X \times Y$ qui possède la propriété suivante : $\forall x \in X,\ \exists y \in Y,\ (x,y) \in \Gamma$ et de plus $(x,y) \in \Gamma$ et $(x,y') \in \Gamma \Rightarrow y = y'$. Le graphe d'une fonction f est l'ensemble des couples $(x, f(x))$ pour $x \in X$.

Remarque : une phrase usuelle comme "la fonction $\cos(x)$" comporte une ambigüité qui devient transparente si on augmente la phrase en "la fonction $\cos(x)$ est une bijection" qui est manifestement fausse si on parle d'une fonction de $\mathbf{R}$ dans $\mathbf{R}$ et néanmoins vraie si l'on parle d'une fonction de $[0, \pi]$ vers $[-1, +1]$ (voir le chapitre 16).

Remarque : on ne fait pas de distinction entre fonction et application.

Exemples :

L'association $x \mapsto x^2 + 1$ définit une application de $\mathbf{R}$ dans $\mathbf{R}$.

L'association $x \mapsto \sqrt{x}$ définit une application de $\mathbf{N}$ dans $\mathbf{R}$ (mais pas de $\mathbf{N}$ dans $\mathbf{N}$).

L'association $x \mapsto \frac{1}{x^2-1}$ définit une application de $\mathbf{R} \setminus \{+1, -1\}$ dans $\mathbf{R}$.

La loi qui associe à un point du plan Π son symétrique par rapport à un point donné O, définit une application de Π dans Π.

L'association $F \mapsto \complement_E F$ définit une application de $\mathcal{P}(E)$ dans $\mathcal{P}(E)$.

L'application qui à tout élément $x \in X$ associe x s'appelle l'*application identique* et se note id_X.

Si f est une application de X dans Y et si X' est un sous-ensemble de X, on peut définir f' la *restriction* de f à X' par : $\forall x \in X',\ f'(x) := f(x)$.

Composition : Si $f : X \to Y$ et $g : Y \to Z$ sont deux applications, on peut définir la *composée* de f et g par $(g \circ f)(x) = g(f(x))$. Une propriété importante de la composition des applications est l'associativité :

PROPOSITION: *La composition des applications est associative. C'est-à-dire que si $h : X \to Y$, $g : Y \to Z$ et $f : Z \to W$ sont trois applications, alors $(f \circ g) \circ h = f \circ (g \circ h)$ (que l'on note donc simplement $f \circ g \circ h$).*

Démonstration: En effet $\forall x \in X$, $(f \circ (g \circ h)(x) = f((g \circ h)(x)) = f(g(h(x)))$ et $((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$ sont bien égaux. □

Exemples : Si f est donnée par $x \mapsto \frac{1}{x^2-1}$ de $\mathbf{R} \setminus \{+1, -1\}$ dans $\mathbf{R}$ et g est donnée par $x \mapsto x^2 + 1$ de $\mathbf{R}$ dans $\mathbf{R}$; alors $g \circ f$ est une application de $\mathbf{R} \setminus \{+1, -1\}$ dans $\mathbf{R}$ décrite par $g \circ f(x) = (\frac{1}{x^2-1})^2 + 1$.

Si f est la symétrie du plan Π par rapport au point O, alors $f \circ f = id_\Pi$.

Il est souvent intéressant de décomposer une application (par exemple pour calculer sa dérivée) ; par exemple l'application définie par $f(x) := \left(e^{\cos(x)} + 1\right)^3$ se décompose en $f = g \circ h \circ k$ où $k(x) = \cos(x)$, $h(x) = e^x$ et $g(x) = (x+1)^3$.

Il est naturel, disposant d'une fonction f d'étudier les équations du type : $f(x) = f(y)$ ou encore $y = f(x)$. Cela conduit à la notion d'application injective ou surjective.

Définition: Une application $f : X \to Y$ est *injective* si (pour tout $x, y \in X$) l'égalité $f(x) = f(y)$ entraîne $x = y$. En d'autres termes tout élément de Y a au plus un antécédent ou encore est l'image d'au plus un élément de X.

Exemple : les fonctions $x \mapsto x+2$ (de $\mathbf{R}$ dans $\mathbf{R}$) et $x \mapsto \log(x)$ (de $\mathbf{R}_+^*$ dans $\mathbf{R}$) sont injectives mais les fonctions $x \mapsto x^2$ et $x \mapsto \sin(x)$ de $\mathbf{R}$ dans $\mathbf{R}$ ne sont pas injectives.

Définition: Une application $f : X \to Y$ est *surjective* si, pour tout $y \in Y$ il existe $x \in X$ tel que $y = f(x)$. En d'autres termes tout élément de Y a au moins un antécédent.

Exemple : La fonction f définie par $f(x) = x + 2$ de $\mathbf{R}$ dans $\mathbf{R}$ est surjective. La fonction définie par $g(x) = x^2$ de $\mathbf{R}$ dans $\mathbf{R}$ n'est pas surjective. Par contre la "même" fonction considérée de $\mathbf{R}$ dans $\mathbf{R}_+$ est surjective. On voit donc qu'il faut bien préciser ensemble de départ et d'arrivée pour parler de surjectivité et d'injectivité.

Remarque : considérons les "mêmes" fonctions mais sur des ensembles différents. Les fonctions $x \mapsto x^2$ restreinte à $\mathbf{R}_+$ et $x \mapsto \sin(x)$ à l'intervalle $[-\frac{\pi}{2}, \frac{\pi}{2}]$ sont injectives. La fonction $x \mapsto x^2$ considérée de $\mathbf{R}$ dans $\mathbf{R}_+$ est surjective. On voit donc qu'il faut bien préciser ensemble de départ et d'arrivée pour parler de surjectivité et d'injectivité.

Définition: Une application $f : X \to Y$ est *bijective* si elle est à la fois injective et surjective. En d'autres termes tout élément de Y a exactement un antécédent.

Exemple : La fonction f de $\mathbf{R}$ dans $\mathbf{R}$ donnée par $x \mapsto x + 2$ est une bijection ; de même la fonction $x \mapsto \log(x)$ est une bijection de $\mathbf{R}_+^*$ dans $\mathbf{R}$.

Lorsque $f : X \to Y$ est une bijection, on peut définir une application de Y dans X par la loi qui à y associe l'unique élément x tel que $y = f(x)$ (le fait que f soit bijective garantit exactement l'existence et l'unicité d'un tel x).

Définition: On appelle *bijection réciproque* d'une bijection f et on note f^{-1} l'application caractérisée par : $x = f^{-1}(y) \Leftrightarrow y = f(x)$. Il est clair que f^{-1} est aussi une bijection.

Exemple : la bijection réciproque de $x \mapsto x+2$ est donnée par $x \mapsto x-2$. La bijection réciproque de $x \mapsto \log(x)$ de $\mathbf{R}_+^*$ dans $\mathbf{R}$ est la fonction $x \mapsto \exp(x)$ de $\mathbf{R}$ dans $\mathbf{R}_+^*$. La symétrie par rapport à un point du plan est sa propre bijection réciproque.

Définition: Soit $f : E \to F$ une application.

i) Si A est une partie de E on appelle *image directe* de A par f et on note $f(A)$ l'ensemble :

$$f(A) := \{y \in F \mid \exists x \in A,\ f(x) = y\}$$

ii) Si B est une partie de F on appelle *image réciproque* de B par f et on note $f^{-1}(B)$ l'ensemble :

$$f^{-1}(B) := \{x \in E \mid f(x) \in B\}$$

Remarques : On prendra bien garde à ne pas confondre l'application $f^{-1} : \mathcal{P}(F) \to \mathcal{P}(E)$ ainsi définie (qui existe pour toute fonction f) avec la bijection réciproque $f^{-1} : F \to E$ (qui n'existe que si f est bijective).

On pourra vérifier en exercice que :
(i) f est surjective si et seulement si $F = f(E)$
(ii) f est injective si et seulement si $f : E \to f(E)$ est une injection.

PROPOSITION: *Soit $f : E \to F$ une application, on a les formules suivantes*
(i) Pour toutes parties A, B de E

$$f(A \cup B) = f(A) \cup f(B) \quad , \quad A \subset B \Rightarrow f(A) \subset f(B) \ \text{ et } \ f(A \cap B) \subset f(A) \cap f(B)$$

(les deux derniers ensembles sont, en général, distincts).
(ii) Pour toutes parties A, B de F, on a $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$, $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$, $A \subset B \Rightarrow f^{-1}(A) \subset f^{-1}(B)$ et également $f^{-1}(\complement_F A) = \complement_E f^{-1}(A)$

Démonstration: Supposons $y \in f(A \cup B)$ c'est-à-dire $y = f(x)$ avec $x \in A \cup B$ soit encore $x \in A$ ou $x \in B$; alors $y = f(x) \in f(A)$ ou $y = f(x) \in f(B)$ donc $y = f(x) \in f(A) \cup f(B)$; ainsi $f(A \cup B) \subset f(A) \cup f(B)$. Si maintenant $y \in f(A) \cup f(B)$ alors $y = f(x')$ avec $x' \in A$ ou bien $y = f(x'')$ avec $x'' \in B$ donc il existe $x \in A \cup B$ (égal à x' ou x'') tel que $y = f(x)$ donc $y \in f(A \cup B)$ et $f(A) \cup f(B) \subset f(A) \cup f(B)$ et finalement l'égalité des deux ensembles.

Supposons $y \in f(A \cap B)$, alors $y = f(x)$ avec $x \in A \cap B$ donc $x \in A$ et $y = f(x) \in f(A)$ mais aussi $x \in B$ donc $y = f(x) \in f(B)$; on peut conclure $y \in f(A) \cap f(B)$ et $f(A \cap B) \subset f(A) \cap f(B)$. L'exemple suivant montre qu'on n'a pas en général égalité : prenons $E := \{a, b\}$, $F := \{c\}$, $f(a) = f(b) = c$, $A := \{a\}$ et $B := \{b\}$. Alors $\emptyset = f(A \cap B) \neq f(A) \cap f(B) = \{c\}$.

Pour changer un peu raisonnons par équivalence : $x \in f^{-1}(A \cup B)$ équivaut à $f(x) \in A \cup B$, qui équivaut à $f(x) \in A$ ou $f(x) \in B$, qui équivaut à $x \in f^{-1}(A)$ ou $x \in f^{-1}(B)$, qui équivaut à $x \in f^{-1}(A) \cup f^{-1}(B)$. Ainsi on a bien $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

On fait de même avec l'intersection ; enfin $x \in f^{-1}(\complement_F A)$ équivaut à $f(x) \in \complement_F A$, qui équivaut à $f(x) \notin A$ ou encore $non(f(x) \in A)$, qui équivaut à $non(x \in f^{-1}(A))$ équivaut à $x \in \complement_E f^{-1}(A)$; d'où l'égalité $f^{-1}(\complement_F A) = \complement_E f^{-1}(A)$. □

2.3 RELATION D'ORDRE ET D'EQUIVALENCE

Une relation sur un ensemble E est un énoncé $\mathcal{R}(x, y)$ (ou $x\mathcal{R}y$) à deux variables : si $\mathcal{R}(x, y)$ est vrai on dira que x est relié à y par la relation $\mathcal{R}$. Les deux exemples les plus importants sont les relations d'ordre et d'équivalence. Une relation d'ordre établit une règle de comparaison entre tous ou certains des éléments : par exemple dans un dictionnaire les mots sont classés suivant une certaine loi, on peut classer les habitants d'un pays par ordre croissant d'âge. Une relation d'équivalence regroupe les éléments d'un ensemble par des propriétés mutuellement exclusives. Par exemple on peut regrouper ensemble les mots commençant par la même lettre, on peut séparer les habitants d'un pays d'après leur sexe, leur année de naissance etc...

2.3.1 Relation d'ordre.

Définition: Une *relation d'ordre* sur un ensemble E est une relation $\mathcal{R}$ telle que :

(i) (Réflexivité) Pour tout $x \in E$ on a $x \mathcal{R} x$.
(ii) (Transitivité) Si $x \mathcal{R} y$ et $y \mathcal{R} z$ alors $x \mathcal{R} z$
(iii) (Antisymétrie) Si $x \mathcal{R} y$ et $y \mathcal{R} x$ alors $x = y$.

Remarques : ces propriétés correspondent aux propriétés de la relation "être plus petit que, ou égal". En fait en mathématique la phrase "être plus petit que" doit presque toujours s'interpréter comme "être plus petit ou égal à". Si l'on veut ajouter que les éléments sont distincts on dira "être *strictement* plus petit".

Exemples : Les ensembles $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ sont tous munis d'une relation d'ordre $\leq$ que l'on peut décrire par : $x \leq y$ si et seulement si $y - x$ est positif (ou nul). Si $x \leq y$ et $x \neq y$ on écrit $x < y$. La notion d'ordre permet de caractériser les intervalles :

Définition: Soit E l'un des ensembles $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$ ou $\mathbf{R}$. Un *intervalle* est un sous-ensemble I tel que, si $x, y \in I$ et $x \leq z \leq y$ alors $z \in I$.

Par contre l'ensemble $\mathbf{C}$ n'a pas de relation d'ordre naturelle et la notion d'intervalle n'y a pas de sens ; on peut néanmoins définir par exemple un ordre lexicographique ainsi (rappelons que tout nombre complexe s'écrit de manière unique $x + iy$ avec x, y réels) :

décrètons que $x + iy \mathcal{R} x' + iy'$ si et seulement si $x < x'$ ou $x = x'$ et $y \leq y'$ (comme pour classer les mots dans un dictionnaire, on compare d'abord les premières lettres et, si elles sont égales on compare les secondes lettres et ainsi de suite).

La relation d'inclusion est aussi une relation d'ordre ; en effet on a bien $F \subset F$ pour tout ensemble F ; si $E \subset F$ et $F \subset G$ alors $E \subset G$ et enfin si $E \subset F$ et $F \subset E$ alors $E = F$.

Il y a une différence importante entre les premiers exemples et ce dernier : dans les premiers cas deux éléments sont toujours comparables ; parmi deux éléments l'un est plus petit que l'autre. Par contre deux ensembles ne sont pas nécessairement comparables : si $E := \{0, 1, 2, 3\}$ et $F := \{0, 1, 4\}$ alors on a $E \not\subset F$ et $F \not\subset E$. Ceci suggère la définition suivante: un ordre $\mathcal{R}$ sur un ensemble E est dit *total* (ou encore l'ensemble E *totalement ordonné*) si deux éléments sont toujours comparables i.e. si :

$$\forall x, y \in E, \ x \mathcal{R} y \text{ ou } y \mathcal{R} x$$

Par exemple : la relation sur l'ensemble $\mathbf{N}$ définie par $x \mid y$ si et seulement si x *divise* y (ou encore y est un multiple entier de x) est une relation d'ordre (vérification laissée en exercice) mais ce n'est pas un ordre total ; en effet 5 ne divise pas 6 et 6 ne divise pas 5.

Si $f : X \to Y$ est une application entre deux ensembles ordonnés par les relations $\leq$ il est naturel de se demander si f préserve l'ordre :

Définition: Une application f est *croissante* si pour tout x, y dans l'ensemble de départ de f, la relation $x \leq y$ entraîne $f(x) \leq f(y)$. Si $x \leq y$ entraîne $f(y) \leq f(x)$ on dit que f est *décroissante* (ou renverse l'ordre). On dit que f est *monotone* si elle est croissante ou décroissante.

Exemples : Les fonctions de $\mathbf{R}$ dans $\mathbf{R}$ donnée par $x \mapsto 2x - 3$ ou $x \mapsto \exp(x)$ sont croissantes, l'application donnée par $x \mapsto -4x + 1$ est décroissante, l'application donnée par $x \mapsto \sin(x)$ n'est pas monotone (sur $\mathbf{R}$).

Soit $f : E \to F$ une fonction, alors les applications $A \mapsto f(A)$ (de $\mathcal{P}(E)$ dans $\mathcal{P}(F)$) et $B \mapsto f^{-1}(B)$ (de $\mathcal{P}(F)$ dans $\mathcal{P}(E)$) sont toutes deux croissantes (si $\mathcal{P}(E)$ et $\mathcal{P}(F)$ sont ordonnés par l'inclusion).

L'importance pratique des fonctions croissantes (ou décroissantes) est qu'elles permettent de transformer des inégalités ; par exemple :

$$\frac{x-y}{3} \leq z^2 \Rightarrow \exp(\frac{x-y}{3}) \leq \exp(z^2) \Rightarrow -4\exp(\frac{x-y}{3}) + 1 \geq -4\exp x(z^2) + 1$$

Nous verrons que la méthode la plus puissante pour voir si une fonction (de $\mathbf{R}$ dans $\mathbf{R}$) est monotone est le calcul différentiel. En effet nous *démontrerons* au chapitre 14 qu'une fonction dérivable sur un intervalle est monotone si et seulement si sa dérivée est de signe constant (résultat admis en terminale).

2.3.2 Plus grand élément, borne supérieure.

Une des traductions les plus fréquentes d'un problème est la recherche d'un minimum ou d'un maximum : si l'on veut placer son argent on cherchera naturellement à le placer de manière à obtenir un rendement maximum ; pour se déplacer d'un point à un autre on cherche le chemin le plus court ; ayant construit (ou dessiné) un pont il est important de connaître le poids maximal qu'il peut supporter ; de nombreux problèmes en physique (ou chimie) peuvent se formuler ainsi : par exemple un rayon lumineux se réfléchit ou se réfracte en suivant un chemin minimal (principe de Fermat) ; un solide posé sur un plan horizontal restera en équilibre seulement si son centre de gravité est situé dans une position minimale.

Définition: Soit $(E, \leq)$ un ensemble ordonné, un élément y de E est le *plus grand élément* de E si tous les autres éléments sont plus petits, c'est-à-dire si $\forall x \in E, x \leq y$.

Remarque : il y a bien sûr une définition analogue du *plus petit élément.*

Exemples : Le plus petit élément de $\mathbf{N}$ est 0 mais $\mathbf{N}$ n'a pas de plus grand élément. Considérons la relation d'inclusion sur l'ensemble $\mathcal{P}(E)$; ce n'est pas un ensemble totalement ordonné mais il a un plus petit élément : l'ensemble vide $\emptyset$ et un plus grand élément : l'ensemble E.

Considérons maintenant un sous-ensemble F d'un ensemble ordonné E ; il est souvent intéressant de connaître un élément de E qui est plus grand que tous les éléments de F ; on peut aussi chercher un tel élément le plus petit possible. C'est le but des définitions suivantes :

Définition: Soit $F \subset E$ un sous-ensemble d'un ensemble ordonné, un élément M de E est un *majorant* de F si pour tout x dans F on a $x \leq M$. Le plus petit des majorants de F (s'il existe) s'appelle la *borne supérieure* de F (dans E).

On peut bien sûr définir de la même façon un *minorant* et la *borne inférieure* comme le plus grand des minorants.

Exemples : Soit $\mathbf{N} \subset \mathbf{R}$, tout nombre réel négatif est un minorant de $\mathbf{N}$ et sa borne inférieure est donc 0 (qui est aussi le plus petit élément de $\mathbf{N}$).

Soit $E := [0,1[\subset \mathbf{R}$ l'intervalle des nombres réels positifs et strictement plus petits que 1. Il est clair que 0 est la borne inférieure de E (et son plus petit élément) et que 1 est sa borne supérieure bien que E n'ait pas de plus grand élément.

Soit $F := \{x \in \mathbf{Q} \mid x < \sqrt{2}\}$ considéré comme sous-ensemble de $\mathbf{Q}$, alors F admet des majorants (par exemple 2 ou $\frac{3}{2}$) mais pas de borne supérieure. En effet, si elle existait, la borne supérieure m de F vérifierait $m^2 \leq 2$ et $2 \leq m^2$ donc $m^2 = 2$, mais ceci est impossible (voir par exemple le chapitre 5). Bien sûr le même ensemble F, considéré comme sous-ensemble de $\mathbf{R}$ admet $\sqrt{2}$ comme borne supérieure.

Une caractérisation commode de la borne supérieure d'un ensemble de réels est la suivante :

PROPOSITION: *Un réel M est la borne supérieure d'un ensemble $E \subset \mathbf{R}$ si et seulement si :*

(i) $\forall x \in E,\ x \leq M$

(ii) $\forall \varepsilon > 0,\ \exists x \in E,\ M - \varepsilon \leq x$

Démonstration: En effet la première propriété dit que M est un majorant et la seconde que c'est le plus petit des majorants : si m est un majorant de E on voit que $\forall \varepsilon > 0,\ M - \varepsilon \leq m$ et donc $M \leq m$. □

En fait nous verrons qu'une propriété très importante de $\mathbf{R}$ est que tout sous-ensemble (non vide) majoré admet une borne supérieure ; cette dernière propriété est fausse dans l'ensemble $\mathbf{Q}$..

2.3.3 Relation d'équivalence.

Définition: Une *relation d'équivalence* sur un ensemble E est une relation $\mathcal{R}$ telle que :

(i) (Réflexivité) Pour tout $x \in E$ on a $x \,\mathcal{R}\, x$.

(ii) (Transitivité) Si $x \,\mathcal{R}\, y$ et $y \,\mathcal{R}\, z$ alors $x \,\mathcal{R}\, z$

(iii) (Symétrie) Si $x \,\mathcal{R}\, y$ entraîne $y \,\mathcal{R}\, x$.

Exemples : Sur l'ensemble $\mathbf{N}$ la relation $x \,\mathcal{R}\, y$ si $x - y$ est pair définit une relation d'équivalence.

Définition: La *classe d'équivalence* d'un élément x est l'ensemble des éléments qui lui sont reliés par $\mathcal{R}$:

$$C(x) := \{y \in E \mid x \,\mathcal{R}\, y\}$$

Remarque : Les classes d'équivalence forment une partition de E, i.e. on peut écrire E comme union disjointe de classes d'équivalence. En effet si $x, x' \in E$ ou bien $C(x) \cap C(x') = \emptyset$ ou bien $C(x) = C(x')$ (si $y \in C(x) \cap C(x')$ alors $y\mathcal{R}x$ et $y\mathcal{R}x'$ entraîne $x\mathcal{R}x'$).

Définition: L'ensemble des classes d'équivalence de E pour la relation $\mathcal{R}$ s'appelle l'*ensemble quotient* de E par $\mathcal{R}$ et se note $E/\mathcal{R}$.

Commentaire : il s'agit d'une notion délicate qui permet de nombreuses constructions : l'ensemble $\mathbf{Z}$ est construit à partir de $\mathbf{N}$ comme le quotient de $\mathbf{N} \times \mathbf{N}$ par la relation d'équivalence $(x,y)\mathcal{R}(x',y') \Leftrightarrow x+y' = x'+y$ et l'ensemble $\mathbf{Q}$ est construit à partir de $\mathbf{Z}$ comme le quotient de $\mathbf{Z}\times(\mathbf{Z}\setminus\{0\})$ par la relation d'équivalence $(x,y)\mathcal{R}(x',y') \Leftrightarrow xy' = x'y$.

Le seul exemple d'ensemble quotient que nous approfondirons est le suivant : Soit n un entier ≥ 1, considérons la relation d'équivalence suivante sur $\mathbf{Z}$:

$$x\mathcal{R}_n y \Leftrightarrow n \text{ divise } x-y$$

Cette relation s'appelle *relation de congruence modulo* n et se note souvent (Cf chapitre 5) $x \equiv y \mod n$. L'ensemble quotient est un ensemble à n éléments : les classes de $0,1,\ldots,n-1$ et se note d'habitude $\mathbf{Z}/n\mathbf{Z}$.

2.4 CARDINAUX ET ENTIERS NATURELS

La notion de cardinal est probablement la première notion mathématique abstraite : il y a quelque chose de commun à trois carottes et trois étoiles, c'est le nombre de ces objets. L'idée de nombre entier est en fait issue de cette intuition. Avec les notions introduites précédemment on voit que deux ensembles ont même cardinal si on peut les mettre en bijection. Ainsi un nombre entier –un cardinal– apparaît comme une classe d'équivalence d'ensembles. Ces définitions qui peuvent paraître pédantes (et le sont) quand on parle de cardinaux finis deviennent indispensables pour aborder les cardinaux infinis, c'est-à-dire pour parler du "nombre" d'éléments d'un ensemble infini.

2.4.1 Ensembles et cardinaux finis

Définition: Deux ensembles ont même *cardinal* si il existe une bijection entre les deux ensembles. On dit aussi qu'ils sont *équipotents*.

Il s'agit bien de la traduction mathématique de "avoir le même nombre d'éléments" ; mais cette intuition correspond en fait au cas des ensembles finis et pour les ensembles infinis, la définition mathématique est la seule qui permette de raisonner.

Cardinaux finis : un entier naturel est le cardinal d'un ensemble fini. Par exemple $\mathrm{card}(\emptyset) = 0$, $\mathrm{card}(\{\emptyset\}) = 1$, $\mathrm{card}(\{\emptyset,\{\emptyset\}\}) = 2$ etc... De manière plus parlante, si a,b,c,d sont des éléments distincts $\mathrm{card}\{a\} = 1$, $\mathrm{card}\{a,b\} = 2$ et $\mathrm{card}\{a,b,c,d\} = 4$.

Un ensemble est donc fini et de cardinal n si et seulement si il est en bijection avec l'ensemble $\{0,1,\ldots,n-1\}$.

Une propriété très importante des ensembles finis (qui en fait les caractérise) est la suivante :

THÉORÈME: *Soient E et F des ensembles finis de même cardinal ; soit f une application de E dans F alors les propriétés suivantes sont équivalentes :*
(i) L'application f est bijective.
(ii) L'application f est injective.
(iii) L'application f est surjective.

Démonstration: Appelons n le cardinal de E. Pour que f soit surjective il faut et il suffit que $f(E)$ ait n éléments, mais $\mathrm{card}(f(E)) \leq \mathrm{card}(E)$ avec égalité si et seulement si

f est injective. On conclut que (ii) équivaut à (iii) ; par ailleurs (i) équivaut par définition à (ii) *et* (iii) d'où le théorème. $\square$

Remarque : On voit en particulier que si $x \in E$ et E est fini alors $E \setminus \{x\}$ n'est pas en bijection avec E. Ceci est une caractérisation des ensembles finis.

Une autre application simple des ensembles finis est le *principe des tiroirs* ; "si on range $n+1$ chaussettes dans n tiroirs, l'un (au moins) des tiroirs contiendra deux chaussettes" (on laisse la preuve en exercice).

Il est naturel, sachant qu'une ensemble est fini de chercher à déterminer son cardinal (un entier naturel). On appelle combinatoire cette partie des mathématiques. Voici quelques résultats utiles.

THÉORÈME: *Soient E et F des ensembles finis de cardinaux m et n respectivement, alors :*

(i) $\mathrm{card}(E) + \mathrm{card}(F) = \mathrm{card}(E \cap F) + \mathrm{card}(E \cup F)$

(ii) $\mathrm{card}(E \times F) = mn$

(iii) Soit $\mathcal{F}(E,F)$ l'ensemble des applications de E vers F alors card$(\mathcal{F}(E,F)) = n^m$. En particulier $\mathrm{card}(\mathcal{P}(E)) = 2^m$.

(iv) Le nombre d'injection de E dans F est 0 si $m > n$ et $n(n-1)(n-2)\dots(n-m+1)$ si $m \leq n$.

(v) L'ensemble des bijections de F vers F a pour cardinal $n! = n(n-1)(n-2)\dots 2.1$

Démonstration: (i) Commençons par observer que dans le cas plus facile où $E \cap F = \emptyset$, la formule est évidente ; en effet si $X = A \cup B$ avec $A \cap B = \emptyset$ alors $\mathrm{card}(X) = \mathrm{card}(A) + \mathrm{card}(B)$. Revenons au cas général et posons $E' := E \setminus (E \cap F)$, alors $E \cup F$ est union disjointe de F et E' donc $\mathrm{card}(E \cup F) = \mathrm{card}(F) + \mathrm{card}(E')$. Mais E est union disjointe de E' et $E \cap F$ donc on a aussi : $\mathrm{card}(E) = \mathrm{card}(E') + \mathrm{card}(E \cap F)$ et on tire de ces deux égalités la formule : $\mathrm{card}(E) + \mathrm{card}(F) = \mathrm{card}(E \cap F) + \mathrm{card}(E \cup F)$

(ii) On peut écrire $E \times F = \cup_{x \in E}\{x\} \times F$; or ces ensembles sont disjoints donc on a $\mathrm{card}(E \times F) = \sum_{x \in E} \mathrm{card}(\{x\} \times F)$. Mais F est en bijection avec chacun des ensembles $\{x\} \times F$ par l'application $y \mapsto (x,y)$ donc $\mathrm{card}(\{x\} \times F) = n$ et $\mathrm{card}(E \times F) = \sum_{x \in E} n = mn$.

(iii) Pour construire une fonction de $E = \{a_1, a_2, \dots, a_m\}$ vers F il faut choisir $f(a_1)$ (il y a n choix possibles), $f(a_2)$ (il y a n choix possibles),... etc. Il y a donc $n \times n \dots n = n^m$ fonctions de E vers F.

Soit A un sous-ensemble de E, on lui associe la fonction $f_A : E \to \{0,1\}$ définie par $f_A(x) = 1$ si $x \in A$ et $f_A(x) = 0$ si $x \notin A$ (la fonction f_A s'appelle la *fonction caractéristique* de A). On obtient ainsi une bijection entre $\mathcal{P}(E)$ et $\mathcal{F}(E, \{0,1\})$ (la bijection réciproque est donnée par $f \mapsto \{x \in E \mid f(x) = 1\}$). On conclut que $\mathrm{card}(\mathcal{P}(E)) = \mathrm{card}(\{0,1\})^m = 2^m$.

(iv) Tout d'abord, il est clair que si $\mathrm{card}(E) > \mathrm{card}(F)$ il n'existe aucune injection de E dans F. Si maintenant $E = \{a_1, a_2, \dots, a_m\}$ et $m \leq n$, pour construire une application injective de E dans F on doit choisir $f(a_1) \in F$ (il y a n choix possibles) puis $f(a_2) \in F \setminus \{f(a_1)\}$ (il y a $n-1$ choix possibles) puis $f(a_3) \in F \setminus \{f(a_1), f(a_2)\}$ (il y a $n-2$ choix possibles) et ainsi de suite. On obtient donc bien en tout $n(n-1)(n-2)\dots(n-m+1)$ injections.

(v) Si $E = F$ est fini on sait qu'une fonction de E dans F est bijective si et seulement si elle est injective donc d'après le résultat précédent il y a $n(n-1)(n-2)\dots(n-n+1) = n!$ bijections. □

Introduisons maintenant une notation très utile en combinatoire :

Définition: Soit F un ensemble de cardinal n et soit $0 \leq p \leq n$, le nombre de parties de F ayant p éléments se note C_n^p ou $\binom{n}{p}$.

THÉORÈME: *On a les formules suivantes :*

(i) $C_n^p = \frac{n(n-1)(n-2)\dots(n-p+1)}{p!} = \frac{n!}{p!(n-p)!}$

(ii) $C_n^p = C_n^{n-p}$

(iii) $C_n^p = C_{n-1}^p + C_{n-1}^{p-1}$

Démonstration: (i) Un sous-ensemble à p éléments de F est donné à permutation près de ses éléments (il y a $p!$ permutations d'après le théorème précédent) par une injection de $\{0, 1, 2, \dots, p\}$ dans F ; il y a $n(n-1)(n-2)\dots(n-p+1)$ injections et donc $\frac{n(n-1)(n-2)\dots(n-p+1)}{p!}$ parties à p éléments.

Démontrons maintenant les deux propriétés (ii) et (iii). On peut bien sûr démontrer ces formules en utilisant la formule $C_n^p = \frac{n!}{p!(n-p)!}$ (vérifiez-le à titre d'exercice) mais nous trouvons plus instructive une démonstration en termes d'ensembles à partir de la définition des C_n^p.

(ii) Soit E un ensemble de cardinal n. L'application $A \mapsto \complement_E A$ définit une bijection entre l'ensemble des parties de E à p éléments et l'ensemble des parties de E à $n-p$ éléments, d'où la formule (ii).

(iii) Soit E un ensemble de cardinal n et soit $x \in E$. L'ensemble des parties de E à p éléments se répartit en deux sous-ensembles disjoints : l'ensemble des parties à p éléments de E contenant l'élément x et l'ensemble des parties à p éléments de E ne contenant pas l'élément x. Le premier est en bijection avec l'ensemble des parties à $p-1$ éléments de $E \setminus \{x\}$ qui a pour cardinal C_{n-1}^{p-1}, et le second est en bijection avec l'ensemble des parties à p éléments de $E \setminus \{x\}$ qui a pour cardinal C_{n-1}^p, d'où le résultat cherché. □

Remarque : Si l'on écrit dans un tableau les coefficients C_n^p (où n sera le numéro de la ligne et p le numéro de la colonne), les propriétés (i) et (ii) se traduisent par la symétrie de chaque ligne et en observant que chaque coefficient est la somme de deux coefficients de la ligne précédente : celui situé juste au-dessus et son prédécesseur. Ces remarques permettent d'ailleurs de calculer très facilement les premiers coefficients. Ce tableau s'appelle le *triangle de Pascal* (bien qu'il ait été connu par exemple des mathématiciens arabes avant sa redécouverte par Pascal).

Les coefficients C_n^p pour $0 \leq p \leq n \leq 7$:

$$\begin{array}{cccccccc}
1 &&&&&&& \\
1 & 1 &&&&&& \\
1 & 2 & 1 &&&&& \\
1 & 3 & 3 & 1 &&&& \\
1 & 4 & 6 & 4 & 1 &&& \\
1 & 5 & 10 & 10 & 5 & 1 && \\
1 & 6 & 15 & 20 & 15 & 6 & 1 & \\
1 & 7 & 21 & 35 & 35 & 21 & 7 & 1
\end{array}$$

2.4.2 Ensembles infinis, **N** et principe de récurrence.

Nous ne donnerons pas de construction de l'ensemble **N** *bien que celle-ci puisse se faire dans le cadre de la théorie des ensembles. Il faut pour cela introduire l'axiome d'existence d'un ensemble infini. Quelque soit la présentation, l'ensemble des entiers naturels est le premier ensemble infini qu'on rencontre. Il peut être caractérisé par l'existence d'un élément initial (zéro) et pour chaque élément* n *d'un successeur* $n+1$ *(distinct de* $0, 1, \ldots, n$*) et pour chaque élément différent de zéro d'un prédécesseur ainsi que par le principe de récurrence.*

Nous supposons connu donc l'ensemble :

$$\mathbf{N} := \{0, 1, 2, 3, 4, 5, \ldots\}$$

Il est muni d'une loi d'addition et de multiplication et d'un ordre ; une loi moins évidente qui le caractérise essentiellement est la suivante :

THÉORÈME: *(principe de récurrence) Soit* S *un sous-ensemble de* **N** *contenant* 0 *et tel que :*

$$\forall n \in \mathbf{N},\ n \in S \Rightarrow (n+1) \in S$$

alors $S = \mathbf{N}$.

L'utilité du théorème est de permettre de vérifier une propriété $\mathcal{P}(n)$ pour tout entier naturel n en montrant que $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ et en vérifiant $\mathcal{P}(0)$.

Exemple : Démontrons que

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

Pour cela appelons $\mathcal{P}(n)$ cette formule et $S := \{n \in \mathbf{N} \mid \mathcal{P}(n)\}$. On voit tout de suite que $\mathcal{P}(0)$ est vrai car $0 = 0$; supposons donc $\mathcal{P}(n)$ vrai et démontrons donc $\mathcal{P}(n+1)$ *à partir de* $\mathcal{P}(n)$: $\sum_{i=0}^{n+1} i = \sum_{i=0}^{n} i + (n+1)$ qui d'après $\mathcal{P}(n)$ vaut $\frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}$ soit donc : $\sum_{i=0}^{n+1} i = \frac{(n+1)(n+2)}{2}$ ce qui est bien $\mathcal{P}(n+1)$. Le théorème permet de conclure que $S = \mathbf{N}$ ce qui signifie bien que pour tout entier n la formule $\mathcal{P}(n)$ est vraie.

Exercice : démontrer de la même manière les formules suivantes :

$$\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{i=0}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$$

Pouvez-vous trouver (et prouver) une formule semblable pour $\sum_{i=0}^{n} i^4$?

THÉORÈME: *L'ensemble* $\mathbf{N}$ *est infini.*

Démonstration: Le contraire serait surprenant, mais donnons néanmoins la démonstration complète. Considérons l'ensemble $\mathbf{N}^* := \mathbf{N} \setminus \{0\}$ et l'application de $\mathbf{N}$ vers $\mathbf{N}^*$ définie par $n \mapsto n+1$. C'est une bijection (vérification facile) mais nous avons vu qu'un ensemble fini ne peut pas être en bijection avec "lui-même moins un élément" donc $\mathbf{N}$ est bien infini. $\square$

La théorie des ensembles permet de construire à partir de $\mathbf{N}$ les ensembles $\mathbf{Q}$, $\mathbf{R}$ et $\mathbf{C}$. Nous ne développerons pas ces constructions mais signalons qu'il y a beaucoup plus de nombres réels que de nombres entiers ou rationnels et en particulier qu'il existe "plusieurs infinis".

Définition: Un ensemble X est *dénombrable* s'il existe une injection de X dans $\mathbf{N}$. Il revient au même de dire que X est en bijection avec un sous-ensemble de $\mathbf{N}$.

THÉORÈME: (Cantor) *L'ensemble* $\mathbf{Q}$ *est dénombrable. L'ensemble* $\mathbf{R}$ *n'est pas dénombrable.*

Démonstration: Si $\mathbf{R}$ était dénombrable, l'intervalle $[0,1]$ le serait également. On pourrait donc écrire $[0,1] = \{x_1, x_2, \ldots, x_n, \ldots\}$. Notons $x_n = 0, a_1^{(n)} a_2^{(n)} \ldots a_m^{(n)} \ldots$ le développement décimal de x_n. Pour chaque $n \geq 1$, on peut choisir un chiffre b_n tel que $b_n \neq a_n^{(n)}$ et fabriquer le nombre réel $x := 0, b_1 b_2 \ldots b_m \ldots$. On voit alors immédiatement que, pour tout n, on a $x \neq x_n$, ce qui contredit l'hypothèse initiale. $\square$

Un peu d'histoire :

Le théorème de Cantor affirme donc qu'il y a "beaucoup plus" de nombres réels que de nombres rationnels, en d'autre termes il n'existe pas de bijection entre $\mathbf{Q}$ *et* $\mathbf{R}$. *Introduisons une définition : un nombre réel est dit algébrique s'il est racine d'un polynôme à coefficients dans* $\mathbf{Q}$ *(ainsi* $1+\sqrt{5}$, $\sqrt[3]{4+\sqrt[5]{2}}$ *sont des nombres algébriques) ; il est dit transcendant s'il n'est pas algébrique. L'existence de nombres transcendants n'est pas évidente et historiquement ils ont été découverts dans l'ordre suivant :*

Liouville montre en 1844 qu'il existe des nombres transcendants ; par exemple les nombres du type $0,10\ldots010\ldots010\ldots$ *où, à chaque fois, la suite de zéros est beaucoup plus longue que la précédente, sont transcendants.*

Hermite prouve en 1873 que le nombre e (base du logarithme népérien) est transcendant. Il est très difficile de démontrer qu'un nombre donné est transcendant et c'est le premier nombre "naturel" pour lequel cela a été démontré.

Cantor établit en 1874 que "presque tous" les nombres sont transcendants. En effet l'ensemble des nombres algébriques a le même cardinal que $\mathbf{Q}$ *(ou* $\mathbf{N}$*).*

Lindemann montre en 1882, en adaptant la méthode de Hermite, que π *est transcendant. Ce résultat achève de démontrer l'impossibilité de la quadrature du cercle.*

Pascal Blaise (1623–1662)