Chapitre préliminaire

# Théorie des ensembles

Ces préliminaires ensemblistes, indispensables à la rigueur de certaines démonstrations, seront d'emploi peu fréquent dans le livre, et n'en constituent pas l'un des objectifs.

On pourra les *omettre* en première lecture et ne s'y référer qu'en cas de besoin (ou par curiosité). Ceci est conforme à l'esprit actuel qui est de privilégier les aspects constructifs, finis, et algorithmiques ([(f), Coh, Mi, NQ, PR, PZ, ...], [(g), Ag, DLQ, LQ, MRR, ...]) ; cependant, il peut arriver qu'un contexte « bourbachique » soit plus facile à gérer pour beaucoup d'étudiant(e)s (construction de la clôture algébrique d'un corps par exemple, sans quoi la notion de racine d'un polynôme reste ambiguë). L'essentiel est de disposer des deux aspects.

La grande difficulté, au niveau d'un livre comme celui-ci, est de proposer une *construction* des objets mathématiques utilisés : en effet, il n'y a pas unicité et les mathématiciens ont été très inconstants dans l'histoire en ce qui concerne les fondements (systèmes d'axiomes de base, notions de « concepts premiers » c'est-à-dire non définis, ...). Ceci dit, il apparaît que l'on peut parler d'« unicité intellectuelle » pour les objets de base en question (les nombres, les fractions et leurs généralisations, etc.), ce qui suffit en pratique.

Nous nous contenterons d'un certain nombre d'usages, à caractère ensembliste (constituant le système dit de Zermelo [(1)]–Fraenkel [(2)]–Skolem [(3)]), qui ne doivent pas être considérés comme immuables.

---

(1) Mathématicien allemand (1871–1953), débute en analyse et physique mathématique ; dès 1902 il démontre, suite aux travaux de Cantor et à l'influence de Hilbert, que tout ensemble peut être bien ordonné (i.e., muni d'un ordre total pour lequel toute partie non vide admet un plus petit élément) : cette propriété est équivalente à l'axiome du choix. Il introduit vers 1905 une axiomatisation de la théorie des ensembles.

(2) Mathématicien allemand (1891–1965), contribue à l'axiomatisation de la théorie des ensembles (1922) à la suite de Zermelo ; il publie une biographie de Cantor (1930).

(3) Mathématicien norvégien (1887–1963), étudie les équations diophantiennes puis la théorie des modèles en logique ; il modifie le système de Zermelo–Fraenkel pour donner ce qui est en usage de nos jours.

L'étudiant(e) intéressé(e) par ces questions peut se référer aux travaux épistémologiques de Henri Lombardi [4] et à l'abondante bibliographie sur les mathématiques constructives que nous donnons en fin d'ouvrage.

Les notions classiques d'ensembles, parties d'un ensemble, complémentaires, inclusions, réunions, intersections, applications, injectivité, surjectivité, relations binaires sur un ensemble (équivalence, ordre), ... sont supposées connues (voir [(a), DNR, DV], puis plus tard [(a), Kri]).

Rappelons les notations dites ensemblistes :

$$\{x \in E,\ \ P(x)\}$$

désignant la partie de $E$ dont les éléments vérifient la propriété $P$, donc à lire : « l'ensemble des $x \in E$ tels que $P(x)$ est vraie »), et $\{x, y, \ldots\}$ (donnant la liste explicite des éléments de l'ensemble).

De ce fait, la notation $\{1, \{2\}\}$ signifie que l'ensemble considéré (un peu bizarre) est du second type, que ses éléments sont l'entier 1 et l'ensemble formé de l'unique entier 2 ; cet ensemble a donc deux éléments. Par rapport à $\mathbb{N}$ on peut dire qu'il est formé d'un élément de $\mathbb{N}$ et d'une partie de celui-ci ; ceci est légal, ainsi que $\{1, \{1\}\}$ qui a toujours *deux* éléments.

Par exemple, si $A$ et $B$ sont deux parties de $E$, on définit la différence ensembliste $A \setminus B := \{a \in A,\ \ a \notin B\}$ qui est le complémentaire, dans $A$, de $A \cap B$.

## 1. Axiome du choix

L'un des axiomes de la théorie des ensembles est l'axiome du choix qui concerne l'ensemble des parties (noté $\mathcal{P}(E)$) d'un ensemble $E$ :

« *pour tout ensemble $E$, il existe une application :*

$$f : \mathcal{P}(E)\setminus\{\emptyset\} \longrightarrow E,$$

*qui à tout $A \in \mathcal{P}(E)$, $A \neq \emptyset$, associe un élément de $E$ appartenant à $A$ (i.e., $f(A) \in A$)* ».

Ceci signifie que l'on peut « choisir », dans toute partie $A$ non vide de $E$, un élément $a$ unique de $A$ (élément distingué de $A$, que l'on note $f(A)$).
Cette application $f$ est nécessairement surjective : pour le prouver, appliquer l'hypothèse $f(A) \in A$ à $A = \{x\},\ \ x \in E$ arbitraire.

(4) `http://hlombardi.free.fr/`, [(g), Lom2]

Par nature, $f$ n'est pas unique (sauf si $E$ possède au plus un élément), mais seule l'existence d'une application $f$ au moins est affirmée.

Si $E = \emptyset$, alors $\mathcal{P}(E) = \{\emptyset\}$ (le seul élément de $\mathcal{P}(\emptyset)$ est la partie vide $\emptyset$ ici égale à la partie pleine $E$), auquel cas $\mathcal{P}(\emptyset)\setminus\{\emptyset\} = \emptyset$ et $f$ est l'application vide (qui ne fait rien : c'est par exemple la restriction de n'importe quelle application à la partie vide de l'ensemble de définition).

Cet axiome est l'un des piliers de la théorie des ensembles car il permet de « faire exister » une grande variété d'objets mathématiques dans le cas où les ensembles manipulés sont *infinis*. Indiquons qu'il faut un axiome pour avoir l'existence d'au moins un ensemble infini (par définition, un ensemble $E$ est dit fini si *toute* injection de $E$ dans $E$ est surjective).

## 2. Théorème de Zorn

L'axiome du choix admet des énoncés équivalents qui sont alors des théorèmes. Le plus important en pratique est celui de Zorn [5] dont l'énoncé suppose les rappels suivants sur les relations d'ordre [6].

**2.1. Définitions**. — (i) *Soit $E$ un ensemble non vide ordonné ; $E$ est dit inductif si toute partie non vide de $E$ totalement ordonnée (appelée aussi chaîne) admet un majorant dans $E$, i.e., un élément de $E$ plus grand, au sens large (c'est-à-dire avec égalité possible), que tous les éléments de la chaîne.*

(ii) *Un élément $a$ d'un ensemble non vide ordonné $E$ est dit maximal s'il n'existe pas d'élément de $E$ strictement plus grand que $a$.*

Si $A$ est une partie non vide de $E$, on parlera d'élément maximal $a$ de $A$ s'il n'existe pas d'élément de $A$ strictement plus grand que $a$ (il peut y en avoir dans $E\setminus A$).

Rappelons qu'un élément $\mu$ de $A$ est dit maximum dans $A$ si l'on a $\mu \geq a$ pour tout $a \in A$ ; ceci suppose que $\mu$ est comparable à tous les éléments de $A$ et est le plus grand élément ; $\mu$ est aussi maximal dans $A$, mais la réciproque est fausse : un élément maximal est (le) maximum si et seulement si il est

[5] Mathématicien allemand (1906–1993), travaux en théorie des ensembles, algèbre (algèbres de Cayley), et analyse.

[6] Une relation d'ordre sur $E$ satisfait aux axiomes suivants : $x \leq x$, $x \leq y$ **et** $y \leq x$ implique $x = y$, $x \leq y$ **et** $y \leq z$ implique $x \leq z$, pour tout $x, y, z \in E$. Attention, deux éléments distincts ne sont pas toujours comparables (ordre non total) ; dans le cas contraire (ordre total), quels que soient $x$ et $y$, on a $x \leq y$ **ou** $y \leq x$.

comparable à tous les autres (ce qui le rend unique). Si $A$ est une chaîne (par exemple une partie non vide quelconque d'un ensemble totalement ordonné), maximal dans $A$ est équivalent à maximum dans $A$, mais attention, en général une chaîne n'a pas d'élément maximal ($\mathbb{N}$, $[0,1[$ par exemple).

**2.2. Théorème** (de Zorn). — *Tout ensemble non vide inductif admet au moins un élément maximal.*

Ce résultat est admis (la preuve est purement « ensembliste » et n'apporte rien de plus), mais on peut le comprendre intuitivement :

Soit $E \neq \emptyset$ inductif ; on part d'une chaîne $C$ de $E$ (ceci existe toujours puisque $\{a\},\ a \in E$, est une chaîne) ; cette chaîne est finie ou non, mais on essaye de la prolonger en une chaîne $C \cup \{c\}$, $c \in E \backslash C$ majorant $C$, et ainsi de suite tant que c'est possible ; la difficulté logique est ici, car il faudra peut-être rajouter des éléments une infinité de fois [(7)] pour arriver à une chaîne $\mathbf{C}$ non prolongeable (i.e., telle que pour tout $x \notin \mathbf{C}$, $x$ ne majore pas $\mathbf{C}$).

Par hypothèse d'inductivité, il existe $m \in E$ majorant pour $\mathbf{C}$, mais $m \in \mathbf{C}$ sinon $\mathbf{C}$ serait prolongeable en $\mathbf{C} \cup \{m\}$ ; donc $m$ est un maximum *pour* $\mathbf{C}$ et donc un élément maximal pour $E$ (en général non maximum pour $E$).

Un exemple concret est donné en 2.4, 2.5.

**2.3. Applications**. — On en verra dans ce livre, mais on peut déjà donner un type de cas très fréquent.

On suppose que $E$ est contenu dans $\mathcal{P}(X)$ (pour un certain ensemble $X$), l'ordre sur $E$ étant la restriction à $E$ de la relation d'inclusion ($\subseteq$) définie sur $\mathcal{P}(X)$ ; on suppose en outre que pour tout sous-ensemble (fini ou non) totalement ordonné de $E$, la réunion des éléments de cet ensemble est encore dans $E$ (autrement dit, $E$ contient les réunions des éléments de ses chaînes).

Alors dans ces conditions $E$ est inductif (donc admet un élément maximal) : en effet, soit une chaîne d'éléments de $E$, alors leur réunion (qui est dans $E$ par hypothèse) est un majorant dans $E$ des éléments de cette chaîne.

**2.4.** *Exemple.* — Nous allons détailler la preuve de l'existence des bases dans les espaces vectoriels car elle illustre tous les principes logiques précédents, tout en ne reposant que sur des définitions simples d'algèbre linéaire de premier cycle ([(a), Al, Gob1, PL, ...]).

(7) Infinité non nécessairement dénombrable, c'est-à-dire non assimilable à une construction par récurrence classique, mais associée directement à l'axiome du choix.

Plus précisément, on va montrer que d'un système de générateurs on peut extraire une base.

Soit $X$ une partie génératrice d'un espace vectoriel $V$ sur le corps $K$ (par exemple l'espace tout entier convient !) ; vérifions que l'ensemble $E$ des parties $K$-libres [8] $L$ de $X$ satisfait aux conditions précédentes (on a $E \neq \emptyset$ car $\emptyset \in E$) : soit $\mathcal{L}$ une chaîne d'éléments de $E$ ; on a donc à vérifier que

$$\mathbf{L} := \bigcup_{L \in \mathcal{L}} L \in E \ ;$$

si l'on a une relation de la forme $\sum_{i=1}^{n} a_i x_i = 0$, $x_i \in \mathbf{L}$, $a_i \in K$, appelons $L_i \in \mathcal{L}$ un élément de la chaîne qui contient $x_i$ ; comme les $x_i$ sont en nombre *fini*, il existe $i_0 \in \{1, \ldots, n\}$ tel que $L_i \subseteq L_{i_0}$ pour tout $i \in \{1, \ldots, n\}$ [9]. Autrement dit, la combinaison linéaire ci-dessus est relative à $L_{i_0}$ qui est libre, d'où $a_i = 0$ pour $i = 1, \ldots, n$. Donc $\mathbf{L}$ est libre, i.e., $\mathbf{L} \in E$ qui est bien inductif.

Montrons qu'un élément maximal de $E$ est une $K$-base de l'espace : soit $B \subseteq X$ une telle partie $K$-libre maximale. Il reste à prouver que $B$ est génératrice, autrement dit que tout $x$ de l'espace est combinaison linéaire (finie) d'éléments de $B$. Pour cela il suffit que tout $x \in X$ ait cette propriété. Soit donc $x \in X$. Si $x \in B$, $x = 1\,.\,x$ est une telle combinaison ; sinon, $B \cup \{x\} \subseteq X$ étant strictement plus grande que $B$, elle n'est pas dans $E$ (i.e., elle est non-libre) : il existe $m \in \mathbb{N}$, des $b_j \in B$ et $\lambda_j, \lambda \in K$ *non tous nuls*, tels que :

$$\sum_{j=1}^{m} \lambda_j b_j + \lambda x = 0.$$

Alors $\lambda \neq 0$ car sinon, $B$ étant libre, $\sum_{j=1}^{m} \lambda_j b_j = 0$ implique $\lambda_j = 0$ pour tout $j$, ce qui est contraire à l'hypothèse sur les coefficients $\lambda_j, \lambda$ ; $K$ étant un corps, $\lambda \neq 0$ équivaut à $\lambda$ inversible, ce qui permet d'écrire $x = \sum_{j=1}^{m} (-\lambda^{-1}\lambda_j)\, b_j$ (si $K$ était par exemple remplacé par $\mathbb{Z}$, la preuve échouerait à ce stade final). Donc $B$ est bien génératrice.

**2.5. Remarque**. — Noter que si $X$ est « dénombrable » :

$$X =: \{x_1, \ldots, x_n, \ldots\},$$

[8] Rappelons que $L \subseteq X$ ($L$ non nécessairement finie) est dite libre si quels que soient $x_1, \ldots, x_n$ distincts dans $L$, $n$ arbitraire, la relation $a_1 x_1 + \cdots + a_n x_n = 0$, $a_i \in K$, implique $a_i = 0$ pour $i = 1, \ldots, n$.

[9] Ceci est général : un nombre fini $m$ de « maillons » d'une chaîne forme une chaîne qui a un plus grand élément comme on peut le voir par induction sur $m$ : le cas $m = 1$ est trivial et le cas $m + 1$ s'obtient en fixant $m$ maillons $x_1, \ldots, x_m$, en posant $x := \max\{x_1, \ldots, x_m\}$ qui existe par hypothèse de récurrence, puis en notant que $x$ et $x_{m+1}$, faisant partie de la chaîne, sont comparables ; le plus grand des deux est la solution (tout ceci est évident en faisant un dessin).

l'existence d'une partie libre maximale dans $X$ s'obtient par une récurrence. Posons $B_0 := \emptyset$ et supposons avoir défini jusqu'au rang $n \geq 0$, $B_n$, libre formée d'éléments de $\{x_1, \ldots, x_n\}$. Passons au rang $n+1$ : si $x_{n+1}$ est combinaison linéaire d'éléments de $B_n$, on pose $B_{n+1} := B_n$ sinon $B_{n+1} := B_n \cup \{x_{n+1}\}$, auquel cas $B_{n+1}$ est libre (on suppose le contraire et on place ici le raisonnement avec les $b_j$, $\lambda_j$, $\lambda$, avec $x := x_{n+1}$). [10]

Une fois cette construction terminée, on pose :

$$B := \bigcup_{i \in \mathbb{N}} B_i \subseteq X \ ;$$

la partie $B$ est alors libre (tout se ramène à un $B_{i_0}$ assez grand) et maximale dans $E$ par construction : pour ceci, il suffit de voir que si $x_\ell \in X \backslash B$, $B \cup \{x_\ell\}$, qui majore strictement $B$, n'est pas dans $E$ (i.e., est non-libre) ; or $x_\ell$ est combinaison linéaire d'éléments de $B_{\ell-1}$ sinon on aurait posé $B_\ell := B_{\ell-1} \cup \{x_\ell\}$ qui implique $x_\ell \in B$ ; donc $B \cup \{x_\ell\}$ est non-libre. La partie $B$ construite est donc bien maximale.

Le théorème de Zorn peut donc être vu comme une extrapolation logique de la notion de récurrence lorsque celle-ci n'a pas de sens (revoir les commentaires qui suivent l'énoncé du théorème de Zorn).

Rappelons à cette occasion que les bases sont vues en général comme des « familles » [11] d'éléments : on distingue par exemple

$$((1,0),(0,1)) \ \text{ de } \ ((0,1),(1,0)),$$

qui sont deux bases indexées ; on parle alors de familles ou parties, libres et/ou génératrices, selon le contexte. En outre, on a le piège suivant : comme famille, $((1,0),(1,0),(0,1))$ n'est pas libre, mais l'ensemble $\{(0,1),(1,0)\}$ de ses éléments est une partie libre.

## 3. Produit cartésien d'ensembles

Faisons quelques rappels sur la notion, *a priori* connue, de produit cartésien de $n \geq 1$ ensembles $X_1, \ldots, X_n$ (non nécessairement distincts), noté :

$$X_1 \times \cdots \times X_n, \text{ ou encore } \prod_{i=1}^{n} X_i,$$

et dont les éléments sont les $n$-uples $(x_1, \ldots, x_n)$, avec la condition $x_i \in X_i$ pour tout $i \in \{1, \ldots, n\}$, notés plus simplement $(x_i)_{i \in I}$ (avec $I = \{1, \ldots, n\}$).

[10] Pour chaque $i \in \mathbb{N}$, $B_i$ a au plus $i$ éléments, et $B_i = \emptyset$ voudrait dire que $x_1 = \cdots = x_i = 0$.
[11] Voir les rappels du § 3 ci-après sur la notion de famille.

On a par définition $(x_i)_{i\in I} = (y_i)_{i\in I}$ dans $\prod_{i=1}^{n} X_i$, si et seulement si $x_i = y_i$ pour tout $i \in \{1, \ldots, n\}$. Le produit est vide si et seulement si l'un des $X_i$ au moins est vide. L'ensemble d'indices utilisé est ici l'ensemble $I = \{1, \ldots, n\}$ qui est fini. On peut définir le produit cartésien $\prod_{i\in I} X_i$ pour un ensemble d'indices $I$ quelconque fini ou non (chaque $X_i$ étant un ensemble dépendant de $i \in I$, ces ensembles n'étant pas nécessairement distincts) : ses éléments sont notés $(x_i)_{i\in I}$ et sont appelés des *familles* (le mot $n$-uple n'étant plus utilisable si $I$ n'a plus un nombre fini d'éléments).

Tout repose donc, logiquement, sur la *définition* de familles d'éléments d'ensembles $X_i$, donnés pour $i \in I$ $\big(\prod_{i\in I} X_i$ étant alors, *par définition*, l'ensemble de ces familles$\big)$. Ceci incluera la définition de $n$-uple qui n'est pas plus définie pour l'instant !

On peut donner une définition rigoureuse de famille $(x_i)_{i\in I}$, $x_i \in X_i$ pour tout $i \in I$, pour $I$ non vide, de la façon suivante : d'un point de vue ensembliste, une famille $(x_i)_{i\in I}$ est le *graphe* d'une application $f$ de $I$ dans un ensemble $X$ contenant tous les ensembles $X_i$ (leur réunion par exemple) qui à $i \in I$ associe $f(i) = x_i$, avec la condition $x_i \in X_i$.

Mais le graphe d'une application $f : I \longrightarrow X$ est l'ensemble des *couples* $(i, f(i))$, $i \in I$ : on a alors l'impression d'un cercle vicieux puisque la définition générale de produit cartésien utilise le produit particulier :

$$I \times X \ ;$$

cette impression est fondée, et il faut pouvoir définir, de façon directe et indépendante, le produit de deux ensembles $A$ et $B$ *donnés dans cet ordre* (notion plus précise).

L'astuce que l'on trouve dans Bourbaki consiste à poser :

$$A \times B := \big\{\ \{\{a\}, \{a, b\}\},\ \ a \in A,\ b \in B\ \big\}\ ;$$

les éléments $x \in A \times B$ (i.e., les couples) sont donc des ensembles formés d'un ensemble à un élément, $\{a\}$, et d'un ensemble à un ou deux éléments, $\{a, b\}$. Si on a :

$$x = \{\{a\}, \{a, b\}\},\ y = \{\{a'\}, \{a', b'\}\},\ a, a' \in A,\ b, b' \in B,$$

l'égalité $x = y$ implique déjà (égalité de deux ensembles) :

$$\{a\} = \{a'\} \text{ ou } \{a\} = \{a', b'\}\ ;$$

si $a' \neq b'$, la seule possibilité est $\{a\} = \{a'\}$, d'où $a = a'$ et $\{a, b\} = \{a', b'\}$ qui conduit à $b = b'$. Si par extraordinaire, $\{a\} = \{a', b'\}$, on a forcément $a' = b'$

et on est encore conduit à $a = a'$, puis $b = b'$. Dans ce cadre on a en général $A \times B \neq B \times A$, les rôles de $A$ et $B$ n'étant pas symétriques (on va y revenir). Par exemple, les notations $\mathbb{R} \times \{0\}$ et $\{0\} \times \mathbb{R}$ figurent les deux « axes » bien connus en géométrie du plan.

On constate que l'idée intuitive de couple $(a, b)$ est bien restituée par ce simple artifice de théorie des ensembles que l'on s'empressera d'oublier. Bien que cette notion de couple ne présente aucun (?) problème conceptuel, on convient de la remplacer par le concept premier de « paire ordonnée » , ce qui introduit une nuance : une paire est formée d'un *premier* élément d'un *premier* ensemble donné et d'un *second* élément d'un *second* ensemble (ici, premier et second sont à prendre au sens du langage courant et non d'une relation d'ordre ; pour bien comprendre, dire par exemple qu'une paire formée d'un élément de $A$ et d'un élément de $B$ est la donnée de $x_\alpha \in X_\alpha := B$ et de $x_a \in X_a := A$, où $\alpha$ et $a$ sont des objets distincts non identifiés) ; autrement dit, on décrète que le cas $n = 2$ de la notion de famille est un concept premier.

On a alors $X_a \times X_\alpha = X_\alpha \times X_a$ au niveau des ensembles de paires (un ensemble $I$, même sous-entendu, est *indispensable* à la notion de paire). Au niveau des paires ordonnées ou couples, formés d'un élément de $A$ et d'un élément de $B$, leur ensemble est noté $A \times B$ qui signifie $X_a = A$, $X_\alpha = B$ *donnés dans cet ordre*, la paire $(x_u)_{u \in \{a,\alpha\}}$ donnant lieu au seul couple $(x_a, x_\alpha)$.

Autrement dit, l'écriture non indexée $A \times B$ de Bourbaki (utilisée constamment) est *conventionnelle* (car alors $B \times A$, qui signifie $X_\alpha = B$, $X_a = A$ donnés dans cet ordre, n'est plus $A \times B$, le couple associé à la paire précédente étant $(x_\alpha, x_a)$) ; en contrepartie, elle est ambiguë sur une planète où l'on écrit de droite à gauche et/ou de bas en haut ... Ceci ne change rien à la pratique qui mélange les deux aspects et a plutôt tendance à utiliser les ensembles facteurs (et les composantes correspondantes) dans un certain ordre, naturel ou non.

On peut tout de même s'interroger sur la difficulté qu'il y a à formaliser certaines notions basiques ...

**3.1. Remarque**. — Revenons aux familles. Comme vu ci-dessus, la définition montre que l'ensemble $I$ n'est pas ordonné (le graphe est défini dès que l'on sait quel élément correspond à tel indice $i_0 \in I$ pris au hasard ; on peut parler d'*indexation ou numérotation*, ce qui n'a rien à voir avec la notion d'ordre mais avec celle d'application) ; la confusion vient du fait qu'il est difficile d'écrire, par exemple, l'ensemble $I = \{1, \ldots, n\}$, sans utiliser son ordre naturel ! Mieux, la notation ensembliste $I = \{1, \ldots, n\}$ pose problème quant à sa *définition* :