Prolégomènes aux probabilités

Ce petit chapitre, en marge du programme, a pour but d'introduire les notions d'ensemble dénombrable et de sommation de suites réelles ou complexes sur de tels ensembles.

1. Parties de $\mathbb{N}$

Théorème 1. *Si $A \subset \mathbb{N}$, alors ou bien A est en bijection avec un unique* segment initial *de $\mathbb{N}$, i.e. un intervalle entier de la forme $[\![0, n-1]\!]$, ou bien A est en bijection avec $\mathbb{N}$. Dans le premier cas, on dit que A est fini et l'on appelle n son* cardinal*. Dans le second cas, on dit que A est dénombrable et l'on note $\aleph_0$ son cardinal.*

Notations pour le cardinal : $|A|$, $\mathrm{Card}(A)$, $\#A$.

Rappelons quelques dénombrements finis classiques. Pour A et B deux ensembles finis :

— $A^B = \{f : B \longrightarrow A\}$, $\#A^B = (\#B)^{\#A}$.

— $\#(A \cup B) = \#A + \#B - \#(A \cap B)$.

— Pour $\mathfrak{S}_n$ l'ensemble des permutations de I_n (bijections de I_n dans lui-même), $\#\mathfrak{S}_n = n!$.

— $\#\{A \subset B\,;\ \#A = p\} = \binom{\#B}{p}$. Par ailleurs, $\binom{n}{k} = \dfrac{n!}{k!\,(n-k)!}$ si $0 \leqslant k \leqslant n$ et 0 sinon.

— $\#\{(a_1, a_2, \ldots, a_p) \in A^p \text{ deux à deux distincts}\} = \dfrac{(\#A)!}{(\#A - p)!}$.

— Principe des tiroirs : si $X = \biguplus_{i=1}^{n} A_i$ (réunion disjointe) et $\#X > n$, il existe $i \in [\![1, n]\!]$ tel que $\#A_i \geqslant 2$.

2. Ensembles dénombrables

Définition 1. *Un ensemble est dit* dénombrable *s'il est en bijection avec $\mathbb{N}$. Il est dit* au plus dénombrable *s'il est en bijection avec une partie de $\mathbb{N}$.*

Un ensemble E est au plus dénombrable et l'on a donc $\#E \leqslant \aleph_0$ si, et seulement s'il est fini ou dénombrable.

Il est souvent difficile d'exhiber une bijection explicite entre un ensemble et $\mathbb{N}$, même si elle existe. C'est pourquoi la proposition suivante est bien utile :

Proposition 1. *Un ensemble A est au plus dénombrable si, et seulement s'il existe une application injective $A \hookrightarrow \mathbb{N}$, si, et seulement s'il existe une application surjective $\mathbb{N} \twoheadrightarrow A$.*

Il découle de la définition qu'un ensemble au plus dénombrable peut s'écrire sous la forme $\{x_0, x_1, x_2, \ldots, x_{n-1}\}$ s'il est fini et $\{x_0, x_1, x_2, \ldots, x_{n-1}, \ldots\}$ s'il est dénombrable. On parle d'écriture *en extension*. En pratique, on utilise souvent une telle énumération, notamment pour l'écriture de sommes sur un ensemble dénombrable, que l'on indicie ainsi sur $\mathbb{N}$. Un ensemble au plus dénombrable est donc un ensemble que l'on peut *énumérer*, complètement s'il est fini, avec des points de suspensions ou par une formule s'il est dénombrable. La notion d'infini *potentiel* (celui des points de suspension) est connue et théorisée depuis Aristote, et opposée à l'infini *en acte* (totalité achevée). Toutefois, la définition formelle de $\mathbb{N}$ est inconnue d'Euclide qui conçoit le nombre comme « collection d'unités » et ne l'axiomatise pas, contrairement à la géométrie. Une définition axiomatique cohérente (HP) remonte à Peano, à la fin du XIXè siècle :

i) Il existe un entier appelé *zéro* et noté 0.

ii) Tout entier admet un unique successeur.

iii) Aucun entier n'admet 0 comme successeur.

iv) Deux entiers distincts n'ont pas le même successeur.

v) Si $A \subset \mathbb{N}$ contient 0 et le successeur de chacun de ses éléments, alors $A = \mathbb{N}$ (axiome de récurrence).

Les ensembles (au plus) dénombrables vérifient des propriétés de stabilité :

- tout sous-ensemble d'un ensemble au plus dénombrable est au plus dénombrable ;
- une réunion au plus dénombrable d'ensembles au plus dénombrables est au plus dénombrable ;
- une réunion au plus dénombrable d'ensembles dénombrables est dénombrable ;
- un produit d'ensemble non vides est fini si, et seulement si, tous les ensembles du produit sont finis ;
- un produit fini d'ensembles dénombrables est dénombrable ;

Parmi les ensembles courants :

- $\mathbb{N}$, ensemble des entiers naturels, $\mathbb{Z}$, ensemble des entiers relatifs, $\mathbb{D}$, ensemble des nombres décimaux, $\mathbb{Q}$, ensemble des nombres rationnels, $\mathbb{N}^k$, pour tout entier non nul k, $\mathbb{Q}[X]$, l'ensemble des polynômes à coefficients rationnels, sont dénombrables.
- $\mathcal{P}(\mathbb{N})$, l'ensemble des parties de $\mathbb{N}$, $\{0,1\}^{\mathbb{N}}$ l'ensemble des suites binaires, $\mathbb{R}$ et tout intervalle de longueur non nulle de $\mathbb{R}$, $\mathbb{R}^{\mathbb{N}}$, l'ensemble des suites réelles, $\mathcal{C}\big([0,1],\mathbb{R}\big)$, l'ensemble des fonctions continues définies sur $[0,1]$, sont infinis non dénombrables.

La première preuve de non dénombrabilité est due à Cantor et porte le nom d'*argument diagonal*. Voici comment l'on montre par cet argument que $\{0,1\}^{\mathbb{N}}$ est non dénombrable.

Soit une application $\phi\colon \mathbb{N} \to \{0,1\}^{\mathbb{N}}$; on note $\phi(n) = (\omega_{i,n})_{i\geqslant 0}$. On pose, pour tout $n \in \mathbb{N}$, $\tau_n = 1 - \omega_{n,n}$. Alors, par construction, $\{0,1\}^{\mathbb{N}} \ni (\tau_n)_{n\geqslant 0} \neq \phi(k)$ pour tout entier k, puisque leurs élément d'indice k diffèrent. Donc ϕ n'est pas surjective. Il n'existe donc pas de bijection de $\mathbb{N}$ sur $\{0,1\}^{\mathbb{N}}$.

3. Extension aux ensembles généraux (HP)

Il existe une théorie des cardinaux infinis (on parle de nombres *transfinis*), qu'il n'est pas question de développer ici. Toutefois, on peut jeter quelques idées de base.

Définition 2. *Deux ensembles sont dits* équipotents *ou de même cardinal s'il existe une bijection de l'un sur l'autre.*

La relation d'équipotence est une relation d'équivalence.

Intuitivement, un ensemble F est « plus gros » qu'un ensemble E si F contient une « copie » de E, donc s'il existe une application injective de E dans F, ce qui permet d'identifier bijectivement E à son image dans F. Intuitivement toujours (définition 2), deux ensembles ont même *cardinal* (sans préciser le sens donné à ce terme) s'ils sont en bijection. Contrairement au cas des ensembles finis, un ensemble infini peut être en bijection avec l'une de ses parties strictes : ainsi, $n \mapsto 2n$ définit une bijection entre $\mathbb{N}$ et l'ensemble des nombres pairs. De même, la fonction arctangente définit une bijection de $\mathbb{R}$ sur l'intervalle borné $]-\pi/2, \pi/2[$. On obtient même ainsi une caractérisation des ensembles infinis : un ensemble est infini si, et seulement s'il est en bijection avec l'une de ses parties strictes.

Théorème 2. *Soient E et F deux ensembles.*
1. *Il existe une application injective de E dans F si, et seulement s'il existe une application surjective de F sur E.*
2. *Il existe une application injective de E dans F ou il existe une application injective de F dans E.*
3. Théorème de Cantor-Bernstein. *S'il existe une application injective de E dans F et une application injective de F dans E, alors il existe une bijection entre E et F.*

Il existe une infinité d'infinis distincts, comme on peut le déduire de la proposition suivante.

Proposition 2. *Un ensemble E n'est jamais en bijection avec l'ensemble $\mathcal{P}(E)$ de ses parties.*

Il existe toutefois un « plus petit infini », celui de $\mathbb{N}$ et un ensemble E est infini si, et seulement s'il existe une injection de $\mathbb{N}$ dans E.

4. Convergence commutative

On s'intéresse dans la deuxième partie de ce chapitre à des compléments sur les séries. Soient I un ensemble dénombrable et $(u_i)_{i\in I}$ une famille réelle ou complexe indiciée par I. D'après ce qui précède, il existe une bijection $\varphi\colon \mathbb{N} \xrightarrow{\sim} I$ et l'on peut considérer la série $\sum u_{\varphi(n)}$. Pour donner un sens à la somme d'une telle série, il faut que la somme obtenue ne dépende pas de φ, ce qui revient à montrer que la somme de la série est indépendante de φ. Le problème est que c'est faux en général... Dans la suite, on note $\mathfrak{S}_{\mathbb{N}}$ l'ensemble des bijections de $\mathbb{N}$ sur $\mathbb{N}$, appelées aussi *permutations de* $\mathbb{N}$.

Exemple 1 (Réarrangement de Laurent)**.** On sait que la série $\sum \dfrac{(-1)^n}{n+1}$ est semi-convergente et que $\displaystyle\sum_{n=0}^{\infty} \frac{(-1)^n}{n+1} = \ln 2$. Alors,

$$1 - \frac{1}{2} - \frac{1}{4} + \frac{1}{3} - \frac{1}{6} - \frac{1}{8} + \frac{1}{5} - \frac{1}{10} - \frac{1}{12} + \cdots = \frac{\ln 2}{2}.$$

Pour le montrer, on réécrit la somme partielle

$$\begin{aligned}\sum_{k=0}^{n} \left(\frac{1}{2n+1} - \frac{1}{4n+2} - \frac{1}{4n+4}\right) &= \sum_{k=0}^{n} \frac{1}{2n+1} - \frac{1}{2}\sum_{k=0}^{n}\left(\frac{1}{2n+1} - \frac{1}{2n+2}\right)\\ &= \frac{1}{2}\sum_{k=0}^{n}\left(\frac{1}{2n+1} - \frac{1}{2n+2}\right) = \sum_{k=0}^{4n+2} \frac{(-1)^k}{k+1}.\end{aligned}$$

Proposition 3. *Soit $(u_n)_n$ une suite (réelle, complexe, à valeurs dans un e.v.n...) Alors, la propriété « $\lim u_n = \ell$ »est invariante par permutation en ce sens que si $\lim u_n = \ell$, alors, pour toute permutation $\sigma \in \mathfrak{S}_{\mathbb{N}}$, on a $\lim u_{\sigma(n)} = \ell$.*

Ce résultat, peut-être un peu étonnant de prime abord, se justifie par le fait que l'on peut réécrire la définition de la limite d'une suite sous la forme suivante :

$$\lim u_n = \ell \iff \forall \varepsilon > 0\colon \#\big\{n \in \mathbb{N}\,;\ |u_n - \ell| \geqslant \varepsilon\big\} < \aleph_0.$$

Il a pour conséquence que la divergence grossière d'une série est elle aussi invariante par permutation : si $\neg(\lim u_n = 0)$, *i.e.* si la série $\sum u_n$ diverge grossièrement, alors, pour toute permutation $\sigma \in \mathfrak{S}(\mathbb{N})$, $\sum u_{\sigma(n)}$ diverge grossièrement.

Définition 3. *Soit $(u_n)_{n\geqslant 0}$ une suite réelle. On dit que la série $\sum u_n$ est commutativement convergente si, pour toute permutation $\sigma \in \mathfrak{S}(\mathbb{N})$, la série $\sum u_{\sigma(n)}$ est convergente et que $S_\sigma = \displaystyle\sum_{n=0}^{\infty} u_{\sigma(n)}$ ne dépend pas de σ.*

Théorème 3. *Soit $(u_n)_{n\geqslant 0}$ une suite réelle ou complexe.*
1. *La série $\sum u_n$ est commutativement convergente si, et seulement si, elle est absolument convergente.*
2. *De plus, si $\sum u_n$ est semi-convergente, i.e. convergente, mais pas absolument convergente, alors, pour tout $\ell \in \overline{\mathbb{R}} = [-\infty, +\infty]$, il existe une permutation $\sigma \in \mathfrak{S}(\mathbb{N})$ telle que $\displaystyle\lim_{N\to\infty} \sum_{n=0}^{N} u_{\sigma(n)} = \ell$. Il existe aussi $\sigma \in \mathfrak{S}_n$ telle que $N \longmapsto \displaystyle\sum_{n=0}^{N} u_{\sigma(n)}$ n'ait pas de limite.*

La deuxième partie du théorème est amusante, mais anecdotique. Ce qu'il faut retenir, c'est que toute série absolument convergente est commutativement convergente. Du coup, on peut maintenant poser une définition.

Théorème et définition 1. *Soient I un ensemble dénombrable et $(u_i)_{i\in I}$ une famille réelle ou complexe indiciée par I. Soit $\varphi\colon \mathbb{N} \xrightarrow{\sim} I$ une bijection. Si la série $\sum u_{\varphi(n)}$ est absolument convergente, on dit que la famille $\sum u_i$ est* sommable *et l'on note $S = \displaystyle\sum_{n=0}^{\infty} u_{\varphi(n)}$. L'hypothèse de convergence absolue ne dépend pas de φ et la somme S non plus. Si $(u_i)_{i\in I} \in \mathbb{R}_+^I$ et si la famille $\sum u_i$ n'est pas sommable, on peut affecter à la somme la valeur $+\infty$.*

Pour faire simple, si une famille est sommable, on peut se permettre de la manipuler comme une somme finie. C'est ce qu'illustre le théorème ci-dessous.

Théorème 4. *Soient I et J des ensembles dénombrables.*
1. Sommes doubles (théorème de Fubini-Tonelli). *La famille $(u_{i,j})_{(i,j)\in I\times J}$ est sommable si, et seulement si, les familles $(u_{i,j})_{j\in J}$ et $i\mapsto \sum_{j\in J}|u_{i,j}|$ sont sommables et l'on a alors*

$$\sum_{i\in I}^{\infty}\sum_{j\in J}^{\infty}u_{i,j}=\sum_{j\in J}^{\infty}\sum_{i\in I}^{\infty}u_{i,j}=\sum_{(i,j)\in I\times J}u_{i,j}.$$

En particulier, si $(u_i)_{i\in I}$ et $(v_j)_{j\in J}$ sont sommables, alors $(u_iv_j)_{(i,j)\in I\times J}$ est sommable et $\sum_{(i,j)\in I\times J}u_iv_j=\sum_{i\in I}u_i\times\sum_{j\in J}v_j$.
2. Sommation par paquets. *Si $(u_i)_{i\in I}$ est sommable et si $I=\biguplus_{j\in J}K_j$, alors $(u_m)_{m\in K_j}$ est sommable pour tout $j\in J$; pour $S_j=\sum_{m\in K_j}u_m$, la famille $(S_j)_{j\in J}$ est sommable et $\sum_{j\in J}\sum_{m\in K_j}u_m=\sum_{i\in I}u_i$.*

Le deuxième item se déduit du premier. Si I et J sont finis, le théorème résulte de l'associativité et la commutativité de l'addition dans $\mathbb{K}$. Si l'un des deux ensembles est fini et l'autre, dénombrable, il se réduit à la linéarité de la limite.