Nombre de nombres et nombres

Cours TalENS n°1

Matthieu Boyer

Table des matières

1 Quelques Définitions Utiles

Définition 1.0.1. *On appelle ensemble une collection d'objets. On l'écrit entre accolades.*

Exemple 1.0.1. *Quelques exemples d'ensembles :*

- $\{4, 19, 30173116, 19.2459, \pi\}$
- $\{a, b, "lepetitchatestmort", "uuuuuuu"\}$
- $\{(0,0), (42,0), (31.41, 59.2)\}$
- $\{\{0\}, \{"a"\}, \{19, 8\}\}$
- $\{31, "n", \{19, "b"\}, (51, 17)\}$

Les ensembles ci-dessus sont écrits par énumération, mais on peut aussi les écrire par description :

Définition 1.0.2. *On note :* $\mathbb{N}$ *l'ensemble des nombres entiers et alors* $2\mathbb{N} = \{2n \mid n \in \mathbb{N}\}$ *est l'ensemble des nombres pairs.*

Définition 1.0.3. *Pour une fonction* $f : A \to B$*, on note* $f(A) = \{f(x) \mid x \in A\}$ *et* $f^{-1}(C) = \{x \in A \mid f(x) \in C\}$ *si* C *est inclus dans* B*.*

Exemple 1.0.2. $\left\{x \in \mathbb{R} \mid P(x) = x^3 + 2x^2 - \frac{1}{5}x + 3 = 0\right\} = P^{-1}(\{0\}) = P^{-1}(0)$

2 La Taille d'un Ensemble

2.1 Bijections et Cardinaux

Définition 2.1.1. *Une application* $f : A \to B$ *est dite* bijective *si elle permet une correspondance un à un entre* A *et* B*. Deux ensembles ont même* cardinal *noté* $|A|$ *s'ils sont en bijection.*

Exemple 2.1.1. *On a une bijection entre* $[\![0, 3]\!]$ *et* $[\![1, 4]\!]$*.*

Définition 2.1.2. *Le cardinal d'un ensemble est une quantité invariante par bijection, i.e. si* F *et* G *sont en bijection ils ont même cardinal. On notera* $|[\![1, n]\!]| = n$*.*

Remarque 2.1.0.1. *Le cardinal représente le nombre d'éléments pour un ensemble fini, donc deux ensembles avec le même nombre d'éléments sont en bijection.*

Et pour un ensemble infini alors ?
On ne peut pas mesurer directement le nombre d'éléments, seulement le comparer à d'autres

Définition 2.1.3.
- *Une application $f : A \to B$ est dite* surjective *si elle prend toute les valeurs dans B, donc si $|A| \geq |B|$*
- *Une application $f : A \to B$ est dite* injective *si deux éléments de A ont toujours une image distincte, donc si $|A| \leq |B|$*

Remarque 2.1.0.2. *Ces définitions sont valables aussi pour des ensembles infinis, et ont un sens dès qu'on dessine des patates. Maintenant, on peut partir mesurer l'infini.*

2.2 Dénombrabilité

Proposition 2.2.1. *$\mathbb{N}$ est infini, et c'est le plus petit ensemble infini, en terme de cardinal. Autrement dit, si $|A| \leq |\mathbb{N}|$, soit il y a égalité, soit A est fini. On dit que $\mathbb{N}$ est infini dénombrable.*

Remarque 2.2.0.1. *Que dire de $p : n \in \mathbb{N} \mapsto 2n$ et $i : n \in \mathbb{N} \mapsto 2n + 1$?*
Elles sont bijectives. Donc il y a 'autant' de nombres pairs que de nombre impairs (logique) que de nombres entiers...

Définition 2.2.1. *On note $\mathbb{Z}$ l'ensemble des nombres relatifs (entiers, négatifs compris). On note $\mathbb{N}^2$ l'ensemble des couples de nombre entiers, i.e. l'ensemble des points du plan situés à une abscisse entière et une ordonnée entière. On note $\mathbb{Q}$ l'ensemble des fractions de nombres entiers, appelé l'ensemble des nombres* rationnels *(qui viennent d'un ration/d'une division). $\mathbb{Q}$ est en bijection avec $\mathbb{N}$, donc est dénombrable. On note $\mathcal{P}$ l'ensemble des nombres premiers. Il est infini et inclus dans $\mathbb{N}$, il est donc en bijection avec $\mathbb{N}$ et est donc dénombrable.*

Proposition 2.2.2.
- *L'application*

$$r : n \in \mathbb{N} \mapsto \begin{cases} n/2 & \text{si } n \text{ est pair} \\ -\frac{n+1}{2} & \text{sinon} \end{cases}$$

  est bijective. Il y a donc autant de nombre relatifs que de nombres positifs.
- *L'application $\psi : (p, q) \mapsto 2^p(2q + 1)$ est bijective. Il y a donc autant de couples d'entiers que d'entiers.*

Remarque 2.2.0.2. *Plus généralement, on montre qu'une union finie d'ensemble dénombrables est dénombrables, qu'une intersection quelconque d'ensembles dénombrables est au plus dénombrable (finie ou dénombrable). Un produit fini d'ensemble dénombrable est dénombrable. Un produit dénombrable d'ensemble finis, comme une union dénombrable d'ensemble finis est au plus dénombrable.*

2.3 Indénombrabilité

Théorème 2.3.1. *L'ensemble des parties de $\mathbb{N}$ n'est pas dénombrable, et $\mathbb{R}$ non plus.*

Démonstration. On ne démontre ici que la partie sur $\mathbb{R}$:
Supposons qu'on a une bijection de $\mathbb{N}$ dans $\mathbb{R}$. Cela revient à numéroter les nombres réels entre 0 et 1, car $[0, 1]$ et $\mathbb{R}$ sont en bijection.
On a donc une liste :

$$\begin{array}{ll} 0 & 0.189280493920472\ldots \\ 0 & 0.892019759218405\ldots \\ 0 & 0.249200000000000\ldots \\ 0 & 0.361846238100291\ldots \\ \vdots & \vdots \end{array}$$

En prenant le premier chiffre après la virgule du premier nombre, puis le second chiffre du second nombre puis ainsi de suite et en leur ajoutant tous 1, on crée un nombre qui diffère de chacun des nombres de la liste d'au moins un chiffre. Donc on ne peut pas avoir de bijection... ■

Remarque 2.3.1.1. *En fait, on a montré qu'il n'y avait pas de surjection de* $\mathbb{N}$ *dans* $\mathbb{R}$.

Remarque 2.3.1.2. *On a utilisé une méthode appelée* Procédé Diagonal de Cantor. *On montre de même que jamais* A *et* $\mathcal{P}(A)$ *ne sont en bijection, c'est le théorème de Cantor.*

Définition 2.3.1. *On note* $\aleph_0 = |\mathbb{N}| = |\mathbb{Q}| < |\mathbb{R}| = \aleph_1$. *On appelle ces nombres les premiers et seconds cardinaux infinis et on dit que* $\mathbb{R}$ *est indénombrable. Il existe des cardinaux infinis encore plus grand. En fait, il en existe une infinité, en considérant* $P(P(P(\dots P(P(\mathbb{R})))))$ *autant de fois qu'on veut.*

Si $\mathbb{Q}$ contient les nombres rationnels, $\mathbb{R} \setminus \mathbb{Q}$ est l'ensemble des nombres irrationnels.

3 Nombres dans $\mathbb{R}$

3.1 Nombres Irrationels

Définition 3.1.1. *Un nombre irrationnel est un nombre dont le développement décimal est apériodique et infini (dénombrable !). De manière équivalente, ce sont des nombres qui ne s'écrivent pas sous la forme* $\frac{p}{q}$ *avec* $pgcd(p,q) = 1$.

Proposition 3.1.1. $\sqrt{2}, e, \pi$ *sont irrationnels.*

Lemme 3.1.1. *Un nombre est pair si et seulement si son carré est pair.*

Démonstration. Si $n = 2k$, $n^2 = 4k^2 = 2 \times 2k^2$ est pair. Si $n = 2k+1$, $n^2 = 4k^2 + 4k + 1 = 2 \times (2k^2 + 2k) + 1$ est impair. ■

Des Irrationalités Promises.

- Irrationalité de $\sqrt{2}$: Si $\sqrt{2} = \frac{p}{q}$ avec $p \wedge q = 1$. Alors, $2 = \frac{p^2}{q^2}$ Donc p^2 est pair et donc p est pair et donc q est impair. Or, avec $p = 2r$, on trouve que $q^2 = 2r^2$ est pair et donc que q est pair.
- Preuve de Niven de l'Irrationalité de π : On introduit $f(x) = \frac{x^n(a-bx)^n}{n!}$ si on écrit $\pi = a/b$. On introduit ensuite

$$F(x) = f(x) - f^{''}(x) + f^4(x) - \ldots + (-1)^n f^{(2n)}(x)$$

. On remarque d'abord que $F(0) + F(\pi)$ est entier. Ensuite, on montre que

$$\int_0^\pi f(x) \sin x \, \mathrm{d}x = F(0) + F(\pi)$$

Enfin, pour $0 < x < \pi$, on a : $0 < f(x) \sin x < \frac{(\pi a)^n}{n!}$. Donc quand n est suffisamment grand, on aboutit à une contradiction.

- Preuve de l'Irrationalité de e : On utilise la définition de e par une série convergente, et la formule de Taylor avec reste intégral.

■

Corollaire 3.1.1.1 (Théorème de Lambert)**.** *La tangente d'un nombre rationnel est irrationnelle.*

3.1.1 Nombre de Nombres Irrationnels

Théorème 3.1.2. *Il y a infiniment plus de nombres irrationels que de nombres rationnels. Autrement dit, si on prend un nombre réel 'au hasard', il sera irrationnel.*

Démonstration. En effet, sinon, on pourrait écrire $\mathbb{R}$ comme l'union de deux ensembles dénombrables $\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$, et on montre qu'alors $\mathbb{R}$ est dénombrable, en choissant à tour de rôle dans le premier ensemble ou dans le second. ■

Toutefois, on peut toujours approcher un nombre irrationnel par une suite de nombre rationnels : c'est le développement décimal :

Théorème 3.1.3. *Pour* $u \in \mathbb{R}$, *la suite de terme général* $u_n = \frac{\lfloor 10^n u \rfloor}{10^n}$ *converge vers* u. *On dit que* $\mathbb{Q}$ *est dense dans* $\mathbb{R}$

Démonstration. On a : $|u_n - u| \leq \frac{1}{10^n} \to 0$ par construction. ■

3.2 Quelques autres types de Nombres

Nous ne démontrerons rien sur ces nombres, il s'agit plus de présentation culturelles.

Définition 3.2.1 (Nombres Normaux)**.** *Les Nombres Normaux, sont des nombres dont les décimales sont équiréparties. C'est à dire, qu'en moyenne, chacun des chiffres de* 0 *à* b *apparaît autant de fois dans leur développement en base* b *:*

$$\lim_{n\to\infty} \frac{b_n}{n} = \frac{1}{b}$$

Presque tout nombre réel est un nombre normal.

Il existe des liens entre ces nombres et la théorie des langages formels [1], puisque ces nombres sont « facilement »représentés en base dix.

Définition 3.2.2. *On appelle nombre univers tout nombre qui contient toute suite finie de chiffre.*

Proposition 3.2.1. *Le nombre* 12345678910111213141516171819202 1 . . . *(constante de Champernowne) est un nombre univers. Depuis l'invention du CD-Rom, on sait que chaque nombre univers contient l'entièreté des livres, films, musiques jamais écrits.*

Proposition 3.2.2. *Presque tout réel est un nombre univers, ce qui fait que si on prend un réel au hasard, il sera un nombre univers.*

4 Algébricité

4.1 Polynômes et Equation Polynomiales

Définition 4.1.1. *Une équation Polynomiale est une équation de la forme :* $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$ *où les* a_i *sont des nombres appartenant à un corps* [2] $\mathbb{K}$*. Elle est dite de degré* n *sur* $\mathbb{K}$*.*
On dit que $P = a_n X + \ldots + a_0$ *est un polynôme (formel) sur* $\mathbb{K}[X]$*, appelé anneaux*[3] *des polynômes sur* $\mathbb{K}$*. On dit que* n *est le degré* $\deg(P)$ *du polynôme.*
On appelle solution tout x *vérifiant l'équation.*

Proposition 4.1.1. *Dans le cas* $n = 2$*, on a :* $ax^2 + bx + c$ *et on connaît les solutions :* $x_{+,-} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

Théorème 4.1.1. *Une équation de degré* n *admet au plus* n *solutions. Toutes ne sont pas dans* $\mathbb{K}$*.*

Démonstration. Si λ est une solution de $P(x) = 0$ où P est un polynôme de degré n sur $\mathbb{K}$, P peut s'écrire $(X - \lambda)Q(x) = 0$ et le degré d'un produit de polynôme étant la somme des degrés, $\deg Q = n - 1$. On conclut par récurrence. ■

Définition 4.1.2. *On appelle nombre algébrique sur* $\mathbb{K}$ *tout nombre* x *tel qu'il existe une équation sur* $\mathbb{K}$ *dont il est solution :*

$$\mathcal{A}(\mathbb{K}) = \{x \mid \exists\ P \in E[X], P(x) = 0\}$$

Un nombre non algébrique est dit transcendant.

Proposition 4.1.2. π *et* e *sont transcendants.*

Démonstration. Ces preuves sont largement hors de portée. ■

Proposition 4.1.3. *Tous les nombres algébriques ne sont pas dans* $\mathbb{K}$*, mais tout nombre* a *de* $\mathbb{K}$ *est algébrique.*

1. Voir plus tard. . .
2. On ne définit pas vraiment les corps ici, comprendre $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$
3. On ne définit pas non plus cette notion ici.

Démonstration.
- a est solution de $x - a = 0$.
- Pour $\mathbb{K} = \mathbb{Q}$, $\sqrt{2} \notin \mathbb{Q}$ est solution de $X^2 - 2 = 0$.

■

Dans la suite, on dira qu'un nombre est algébrique s'il est algébrique sur $\mathbb{Q}$.
On cherche l'ensemble des nombres algébriques. On sait que ce n'est pas $\mathbb{R}$ car il y a des nombres dans $\mathbb{R}$ qui ne sont pas algébriques, et que $x^2 = -1$ n'a pas de solution sur $\mathbb{R}$.

Définition 4.1.3. *La cloture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ est le plus petit ensemble contenant $\mathbb{Q}$ et tel que toute équation de degré au moins 1 sur $\overline{\mathbb{Q}}$ admet au moins une solution sur $\overline{\mathbb{Q}}$. C'est équivalent au fait que toutes les solutions d'une équation de degré au moins 1 sur $\overline{\mathbb{Q}}$ sont dans $\overline{\mathbb{Q}}$, ce qui se montre par récurrence sur le degré.*

Trouver la cloture algébrique d'un ensemble n'est pas un problème très compliqué en théorie. On peut s'en rendre compte en regardant $\mathbb{Q}[\sqrt{2}] = \left\{a + \sqrt{2}b \mid (a,b) \in \mathbb{Q}^2\right\}$: il suffit de rajouter toutes les solutions aux équations sur $\mathbb{Q}$. Toutefois, en pratique, cela génère des ensembles abstraits et sans forme simple.

Un Théorème dû à Kedlaya fait état d'un lien entre la clôture algébrique d'un espace de fonctions, i.e. les solutions à des équations à coefficients fonctionels, et les développements numériques en base q. Mais ce théorème qui se base sur la théorie des séries de Laurent et celle des langages formels (voir plus tard...) est hors de notre portée.

5 Extensions

5.1 Tous Ensembles Alors ?

Définition 5.1.1. *Un groupe est un ensemble muni d'une loi interne, associative, unifère, inversible. C'est à dire une application $\cdot : G \times G \to G$ qui vérifie :*
- *Pour tous a, b, c dans G, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$*
- *Il existe $e \in G$ tel que $e \cdot x = x$ pour tout $x \in G$*
- *Pour tout x, il existe y tel que $xy = e$.*

Ici le groupe est noté multiplicativement, mais on aurait pû choisir d'adopter une convention additive, c'est à dire pour une loi $+$.

Définition 5.1.2. *Un espace vectoriel réel*[4] *sur $\mathbb{R}$ est un groupe E, noté additivement, stable par multiplication par un réel, i.e. si $x \in E$, $\lambda \in \mathbb{R}$ alors $\lambda x \in E$.*
Deux espaces vectoriels sont dit isomorphes s'ils sont en bijection par une application linéaire f, i.e. qui préserve la somme.

Définition 5.1.3. *Les groupes (resp. les espaces vectoriels) reposent parfois (resp. toujours) sur une famille d'éléments qui les engendre, i.e. un ensemble $\{g_1, \ldots, g_n\}$ tel que si $g \in G$, $g = g_1^{t_1} g_2^{t_2} \ldots g_n^{t_n}$ pour certains t_i.*
On appelle un tel ensemble une famille génératrice. Une famille génératrice de cardinal minimal est appelée une base.
On appelle Indice d'un groupe le cardinal d'une base de ce groupe (elles ont toutes le même). C'est une nouvelle notion de taille d'ensemble qui est invariante par la notion d'isomorphisme, une notion de bijection remaniée.

Dans le cadre d'un espace vectoriel E sur $\mathbb{R}$, le cardinal d'une base est appelé *dimension* de l'espace et noté $\dim E$. Lorsqu'il est fini, E est de cardinal indénombrable égal à $\aleph_1$. Toutefois, on peut montrer que E est en bijection avec $\mathbb{R}^{\dim E}$, et donc, lorsqu'il est infini, selon sa valeur, E va devenir plus ou moins grand.

4. On peut les définir sur tout corps

Proposition 5.1.1.
- *Si* $\dim E = \aleph_0$, *E est en bijection avec* $\mathbb{R}^{\mathbb{N}}$ *l'ensemble des suites à valeurs réelles.*
- *Lorsque* $\dim E = \aleph_1$, *E est en bijection avec* $\mathbb{R}^{\mathbb{R}}$ *l'ensemble des fonctions réelles.*

Remarque 5.1.0.1. *En réalité, il s'agit plus que d'une bijection, puisqu'il s'agit d'un isomorphisme, mais cela importe peu.*

5.2 Encore plus de Nombres

Définition 5.2.1. *Un nombre de Liouville est un nombre vérifiant :*

$$\forall n \in \mathbb{N}, \exists\ q_n > 1, p_n, 0 < \left| x - \frac{p_n}{q_n} \right| <= \frac{1}{q_n^n}$$

Remarque 5.2.0.1. *Ce sont des nombres facilement approchés par des nombres rationnels.*

Théorème 5.2.1. *Tout nombre de Liouville est transcendant (voir plus haut), mais que à presque tout nombre réel est transcendant sans être de Liouville.*