1 Qu'est ce qu'un nombre ?

Nous avons vu tout au long de ce cours divers outils de mathématiques très utilisés en physique. Ces outils concernaient la manipulation des fonctions dans le but très alimentaire de résoudre des équations issue de la physique. Les fonctions elles mêmes étaient définies comme des boîtes noires transformant un *nombre* en un autre. Nous nous sommes jamais demandé ce qu'est un nombre, nous avons pris cela comme une donnée dont la signification est à priori connue.

Nous allons dans ce chapitre revenir un peu sur ce concept et voir la construction des nombres réels. Nous verrons également que ce n'est pas la seule façon de construire un ensemble complet de nombre, et d'autres ensembles qui défient notre intuition de "proche" et de "loin" sont également constructible. Ce chapitre n'a pas d'autre but que d'éveiller la curiosité du lecteur.

Le plan général que l'on va suivre est de d'abord construire les nombres entiers, ensuite les nombres rationnels. Nous munirons alors notre ensemble d'une *topologie* et construirons soit l'ensemble des nombres réels, soit celui des nombres p-adiques. "Munir un ensemble d'une topologie" est un terme pour effrayer l'étudiant. En langage profane, cela veut simplement dire que l'on va définir *les distances*, la notion *d'être proche*. La topologie habituelle que l'on définie, et à laquelle nous sommes habitués depuis notre tendre enfance nous dit par exemple que 4.3 et plus *proche* de 4.2 que 5. Tant que nous construisons l'ensemble des nombres rationnels, nous n'avons pas besoin de ce concept, celui d'*avant* et *après* nous suffira.

1.1 Les entiers naturels $\mathbb{N}$.

Dedekind, grand mathématicien de la fin du dix-neuvième siècle disait : "Dieu inventa les nombres entiers ; tous le reste est invention humaine". La construction moderne des nombres entiers est due à Peano et ses cinq principes. De façon intuitif, on peut dire que c'est le plus simple ensemble ou chaque élément (excepté le premier qu'on appelle 0) possède *un* élément *juste avant* et *un* élément *juste après*, et cela de façon non-cyclique. Bon, bien sûr, comme nous sommes en train de faire des mathématiques, nous devons définir exactement ce que ces termes veulent dire. Voilà les axiomes de Peano.

1. $0 \in \mathbb{N}$ [1]
2. Chaque nombre naturel x possède un autre élément $x' = s(x) \in \mathbb{N}$ appelé son successeur (voilà pour le *juste après*).

1. Grand débat philosophique pour savoir si il faut commencer par 0 ou par 1. Cette question n'a pas de sens tant que l'on a pas défini l'opération addition et son élément neutre. Tout ce que l'on veut ici est de définir un premier élément.

3. 0 n'est le successeur d'aucun nombre (cela nous enlève le danger des cycles).
4. Si $s(x) = s(y)$ alors $x = y$ (cela nous enlève le problème de plusieurs nombre ayant le même successeur).
5. Axiome d'induction. Soit Q une propriété telle que

— Q est valable pour 0
— Si Q est valable pour x, alors Q est valable pour $s(x)$
— Alors Q est valable pour tous les nombres entiers (cela entre autre nous enlève le problème d'avoir plusieurs "premier élément")

Nous avons insisté sur cette construction pour souligner que tout ce dont on a besoin à cette étape est le concept d'avant et d'après.

Comme nous ne voulons pas écrire un texte très rigoureux, nous allons aller un peu plus vite à partir de là. On peut commencer par donner des noms aux divers éléments. Par exemple, le successeur de 0 sera appelé un (et noté 1), le successeur de 1 deux (2) et ainsi de suite. On peut donc noter $\mathbb{N} = \{0, 1, 2, ...\}$. Ensuite, nous allons munir notre ensemble de l'opération $+$. C'est une application qui à deux nombres entiers associe un troisième, et cela en généralisant le concept de successeur : $x+0 = x$ et $x+s(y) = s(x+y)$. Par exemple, et $x + 1 = s(x)$ [2]. L'opération $+$ a bien sûr toutes les bonnes propriétés d'associativité, commutativité, etc. dont nous sommes habitué (exercices : les démontrer). Nous laissons au lecteur le soin d'en donner une définition rigoureuse.

Tant que nous y sommes, nous pouvons également définir l'opération $\times$ (multiplication) comme une autre application qui a chaque deux nombres entiers associe un troisième : $x \times 0 = 0$; $x \times s(y) = x \times y + x$. Bien sûr, c'est la multiplication habituelle et on aurait été plus claire si on avait noté $x \times (y + 1) = x \times y + x$. Par exemple, $x \times 1 = x$.

Enfin, ça ne mange pas de pain de définir rigoureusement les relations de comparaison $<$ et $>$, à nouveau en suivant la piste des successeurs.

Nous suggérons au lecteur de faire ces constructions en détails et de façon rigoureuse, c'est un exercice très intéressant.

Nous disposons donc maintenant d'un ensemble $\mathbb{N}$, muni des deux opérations $+$ et $\times$. En langage chique, nous dirrions que $(\mathbb{N}, +, \times)$ est un anneau commutatif.

1.2 Les ensembles $\mathbb{Z}$ et $\mathbb{Q}$.

A partir de là, nous allons commencer à élargir notre ensemble N.

D'abord, nous pouvons définir l'opération soustraction $-$ comme "l'inverse" de l'addition : si $x - y = z$ alors c'est que $y + z = x$ (exercice : donner une définition rigoureuse de la soustraction). Mais cela nous pose un problème. $\mathbb{N}$ est fermé pour l'addition, c'est à dire que l'addition de n'importe quel deux nombres est encore dans $\mathbb{N}$. Cela est loin d'être le cas pour la soustraction. Il suffit d'examiner $0 - 1$: si $0 - 1 = z \in \mathbb{N}$, alors $z + 1 = 0$, ce qui contredit violemment un des axiomes de Peano. Qu'à cela ne tienne : nous allons définir un ensemble $\mathbb{Z}$ qui contient $\mathbb{N}$ et qui est fermé pour la soustraction, $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$.

2. Notez comment l'operation $+1$ devient alors le synonyme de l'opération "successeur".

Nous pouvons également définir l'opération de division /comme "l'inverse" de la multiplication : si $x/y = z$ alors c'est que $x = yz$. Le même problème se pose : en général, pour un couple quelconque, x/y n'a pas de sens dans $\mathbb{N}$ ou $\mathbb{Z}$. A nouveau, on peut "agrandir" notre ensemble et définir l'ensemble des nombres rationnels $\mathbb{Q}$ qui est fermé pour l'opération de division. Notez que nous avons pas vraiment définit comment on agrandit nos ensembles, cela alourdirait trop ce texte [3].

L'ensemble $\mathbb{Q}$ est très riche. Concrètement les humains n'en sortent jamais pour faire leurs calculs. Le trait principal de cet ensemble est qu'entre n'importe quel deux nombres rationnels, on peut en trouver d'autres. Ceci dit, comme le lecteur le sait, l'ensemble $\mathbb{Q}$ reste dénombrable, et même s'il est fermé pour la division, il n'est pas *algébriquement* fermé. Par cela nous voulons dire que les racines de tous les polynômes (de coefficients entiers) ne se trouvent pas dans $\mathbb{Q}$. Par exemple, il est trivial de montrer que la racine de $x^2 - 2 = 0$ (qui représente l'hypoténuse d'un triangle rectangle de coté unité) n'est pas rationnelle.

Il suffit de suivre la même démarche et construire l'ensemble des nombre algébrique $\mathbb{A}$, la fermeture algébrique de $\mathbb{Q}$, et qui contient tous ces nombres du genre $\sqrt{2+\sqrt{3}+\sqrt[17]{253}}$. A t'on épuisé tous les nombres ou existe t'il des nombres non-algébriques qu'on appelle *transcendants* ? Est ce que par exemple, le périmètre d'un cercle de diamètre unité π, ou le nombre e sont algébriques ? La réponse à ces questions n'est venu qu'à la fin du dix-neuvième siècle.

1.3 Un peu de topologie.

Nous n'avons pas encore introduit le concept de distance entre deux nombres. La distance entre deux nombres est une application qui prend deux nombres en entrée et produit un nombre en sortie. On peut la définir sur n'importe quel corps k [4] [5] (dont par exemple le corps des rationnels). Nous demandons à cette application d'avoir un minimum de propriétés : Pour tous $a, b, c \in k$,

1. $d(a, b) \geq 0$ et $d(a, b) = 0$ si et seulement si $a = b$.
2. $d(a, b) = d(b, a)$.
3. $d(a, b) \leq d(a, c) + d(b, c)$ (l'inégalité du triangle).

Ce n'est pas beaucoup demander, mais à partir du moment où nous disposons d'une métrique, nous pouvons faire une quantité phénoménale de choses. Essentiellement, c'est

3. Voyons rapidement la construction des rationnels. Considérons l'ensemble $A = \mathbb{N} \times \mathbb{N}$, c'est à dire l'ensemble de toutes les pairs (x, y) où x et y sont des entiers naturels. Nous définissons une relation d'équivalence $(x, y) = (x', y')$ si $xy' = x'y$. Nous définissons l'opération $+$dans A par $(a, b) + (c, d) = (ad + bc, bd)$ et l'opération $\times$ par $(a, b) \times (c, d) = (ac, bd)$. L'ensemble A partitionné par la relation d'équivalence ci-dessus et muni des deux opérations $+$ et $\times$ peut être identifié au corps des rationnels $\mathbb{Q}$. Un exercice intéressant serait de suivre les mêmes lignes pour construire les entiers relatifs à partir des entiers naturels.

4. Rappelons qu'un corps est un ensemble, muni des deux opérations $+$ et $\times$ et fermé vis à vis d'elles.

5. Bien sûr, pour définir une norme, nous n'avons pas nécessairement besoin d'un corps. Nous avons vu dès le début de ce livre comment en définir une pour l'espace vectoriel des fonctions de carré sommable.

l'étape où l'on passe de l'algèbre à l'analyse, où on peut commencer à définir le concept de *continu*, de la convergence des suites, ...

Un concept étroitement lié à la notion de distance est celle de *la valeur absolue.* Supposons que nous disposons d'une valeur absolue sur un corps k avec les propriétés suivantes :

p1 : $|a| = 0$ ssi $a = 0$.

p2 : $|ab| = |a||b|$

p3 : $|a + b| \leq |a| + |b|$

alors nous pouvons facilement définir la distance entre deux éléments par $d(a, b) = |a-b|$. Nous laissons au lecteur le soin de démontrer cela. L'exemple usuel de la valeur absolue sur $\mathbb{Q}$ est $|x| = x$ si $x \geq 0$ et $-x$ sinon. Bien sûr, ce n'est pas la seule valeur absolue possible, nous en verrons des exemples plus bas.

Comme nous l'avons dit, dès que nous disposons d'une distance, nous pouvons définir la convergence des suites. Nous disons que la suite $a_n$converge vers la limite a si tous les éléments de la suite, à partir d'un certain N sont aussi *proche* de la limite que nous le souhaitons. Dans l'ensemble $\mathbb{Q}$, nous écrirons par exemple que a est la limite de a_n si pour tout $\epsilon \in \mathbb{Q}$, nous pouvons trouver N tel que si $n > N$ alors $d(a, a_n) < \epsilon$.

Un des problèmes de cette définition de la convergence est que pour savoir si une suite converge, nous devons connaître à l'avance sa limite ! Le grand Cauchy a trouvé comment y remédier : une suite converge si la distance entre deux éléments quelconques converge vers zéro au delà d'un certain N : si pour tout $\epsilon \in \mathbb{Q}$, nous pouvons trouver N tel que si $n, m > N$ alors $d(a_m, a_n) < \epsilon$ alors la suite est convergente.

Cela nous pose un nouveau problème : la limite d'une suite dans un corps k n'a aucune raison d'appartenir au même corps. Mais nous pouvons continuer notre procédure d'enrichissement et considérer un ensemble qui contient *et* le corps k *et* toutes les limites de toutes les suites convergentes. Nous verrons ci-dessous deux exemples de fermeture topologique de l'ensemble $\mathbb{Q}$: l'ensemble des nombres réels et l'ensemble des nombres $p-$adiques.

1.4 L'ensemble des nombres réels.

Munissons nous de la valeur absolue usuelle, et la distance (la métrique) qui en découle. Et considérons les suites convergentes dans $\mathbb{Q}$. Il est évident que beaucoup (vraiment beaucoup) de ces suites n'ont pas leurs limites dans $\mathbb{Q}$.

Exemple 1. Le nombre $1/e$, défini comme la limite de $\sum_{n=0}(-1)^n/n!$ n'est pas un nombre rationnel. Pour voir cela supposons qu'il l'est et ecrivons le comme p/q. Nous décomposons la série en une somme jusqu'au terme q et le reste :

$$\frac{p}{q} = \sum_{n=0}^{q}(-1)^n/n! + R_q$$

Comme nous avons affaire à une série alternative convergente, le reste est plus petit que le dernier terme : $|R_q| < 1/q!$. Multiplions maintenant les deux cotés par $q!$. Nous avons à gauche un entier, et à droite un entier *plus* un terme plus petit que l'unité. Le coté droit n'est donc pas un entier naturel. Notre hypothèse de rationnalité de $1/e$ est donc fausse.

Nous définissons l'ensemble des nombres réel $\mathbb{R}$ comme un ensemble qui contient l'ensemble $\mathbb{Q}$ et les limites de toutes les suites convergentes dans $\mathbb{Q}$ au sens de Cauchy. Les opérations $+$ et $\times$ se généralisent aisement par continuité. Par exemple,pour $a, b \in \mathbb{R}$, (mais pas nécessairement rationnel) $a + b = \lim(a_n + b_n)$ où a_n et b_n sont des suites dans $\mathbb{Q}$ convergeant vers a et b.

Nous pouvons pousser un ouf de soulagement, nous sommes au bout de notre chemin (à part peut-être une extension triviale à $\mathbb{C}$). Mais est ce que c'était vraiment la peine de faire tout ce parcours ? Est ce que l'ensemble $\mathbb{R}$ est vraiment plus riche que l'ensemble des nombres algébriques ? La réponse est évidement oui, mais elle est loin d'être évidente. Jusqu'à presque la fin du dix-neuvième siècle, la réponse à cette question n'était pas connue. On a pu démontrer à cette époque avec peine que les nombre e et π ne sont pas algébriques, c'est à dire que nous ne pouvons pas trouver un polynôme de coefficients entiers dont une des racines soit un de ces nombres. Mais combien y avait il de ces nombres transcendants ? très peu, beaucoup ? La réponse, un coup de maître, est venu de Greg Cantor : les nombres algébriques forment une minorité négligeable comparée aux nombres réels. Cette démonstration a provoqué beaucoup de débats furieux à l'époque, puisque Cantor ne construisait pas *un seul* nombre transcendant. Sa démonstration se fait en deux étapes très simples : (i) les nombres algébriques sont dénombrables ; (ii) les nombres réels ne sont pas dénombrable. Voyons cela de plus près.

1.4.1 Les nombres algébriques sont dénombrables.

Comme nous l'avons dit, les nombres algébriques comprennent les racines de tous les polynômes. Les nombres rationnels sont évidement des nombres algébriques, puisque p/q est solution de l'équation $px - q = 0$.

Considérons maintenant un polynôme à coefficient entier du genre $a_0 + a_1x + ... + a_nx^n (a_n \neq 0)$. Nous appellerons *hauteur* de ce polynôme le nombre $H = n - 1 + |a_0| + |a_1| + ...|a_n|$. Il existe un seul polynôme de hauteur 1 : x. Pour $H = 2$, nous avons les polynômes suivants : x^2 ; $x \pm 1$. Pour $H = 3$, x^3 ; $\pm 2x^2$; $x^2 \pm x$; $x^2 \pm 1$; $2x \pm 1$; $x \pm 2$ et ainsi de suite. Le fait intéressant est que le nombre de racines de tous les polynômes d'une hauteur H est finie (Combien y en a t il au plus ?). Nous pouvons donc ranger les nombres algébriques de façon suivante : On prend d'abord toutes les racines associées à la hauteur 1, et on les range dans l'ordre croissant, en éliminant les doublons. On prend ensuite toutes les racines associées à $H = 2$, on les ranges dans l'ordre croissant en éliminant les doublons et on continu le procédé pour $H = 3$, $H = 4$,... Cela nous donne par $\mathbb{A} = \{0 ; -1, 1 ; -2, -1/2, 1/2, 2 ; ...\}$ et il n'est pas difficile de voir que nous avons ainsi une procédure pour dénombrer les nombres algébriques !

1.4.2 Les nombres réels ne sont pas dénombrables.

Supposons que nous avons réussi à dénombrer tous les nombres réel entre 0 et 1. Nous les listons dans l'ordre croissant en utilisant leur représentation décimale :

$$\begin{aligned} r_0 &= 0.a_{00}a_{01}a_{02}... \\ r_1 &= 0.a_{10}a_{11}a_{12}... \\ r_2 &= 0.a_{20}a_{21}a_{22}... \\ &... \end{aligned}$$

Soit maintenant le chiffre r construit à partir des décimaux diagonaux : $r = 0.a_{00}a_{11}a_{22}...$ et construisons un nombre r' à partir de r en changeant chacun des décimaux de r d'une façon quelconque. Il est alors facile de voir que r' ne peut pas être dans la liste ci-dessus ! (Exercice : le démontrer).

1.4.3 Au delà des nombres réels : les hyper-réels.

Si on voulait donner une image de nos nombres, les rationnels seraient des points isolés dans un espace et les réels rempliraient le vide qu'il y a entre. Peut on encore inventer des nombres qui se mettraient *entre* les nombres réels ? Avant le dix-neuvième siècle, les mathématiciens avaient l'habitude de manipuler ce genre de nombres qu'ils appelaient des *infiniment petits*. Ces nombres cependant provoquaient pas mal de contradictions et ont été vite chassés du monde. Dans les années 1960, Abraham Robinson à réussi de les réintroduire de façon rigoureuse par une méthode pas trop loin de ce que nous avons vu pour la construction des nombres réels. Un infiniment petit est par exemple un nombre ϵ tel que $0 < \epsilon < 1/n$ quelque soit $n \in \mathbb{N}$. Dans l'ensemble des nombres hyper-réel, chaque réel classique est entouré d'un nuage de nombre à distance infiniment petit.

Concrètement, l'introduction de ces nombres n'apporte pas de nouvelles méthodes et nous ne développerons pas ce concept plus ici. Nous suggérons au lecteur intéressé de se diriger vers des livres plus spécialisés sur ces nombres et l'analyse non-standard.

1.5 Les nombres $p-$adiques.

Nous allons voir dans cette section des nombres étranges, très différents de ce que nous connaissions jusque là. La notion de *proche* et de *loin* est complètement dissociée de la notion d'avant et après, contrairement à la distance usuelle que nous avons utilisée pour construire $\mathbb{R}$ à partir de $\mathbb{Q}$. Il existe d'autres valeurs absolues, et la topologie qu'elles définissent est radicalement différente. Rappelons que la valeur absolue doit avoir les trois propriétés mentionnées à la section 1.3. Si la valeur absolue a en plus la propriété suivante :

p4 : $|x + y| \leq \max\{|x|, |y|\}$

nous l'appelons *non-archimédienne*. Notons que la propriété 4 implique la propriété 3, puisque $\max\{|x|, |y|\} \leq |x| + |y|$.

Commençons par les nombres entiers. Donnons nous un nombre premier p. N'importe quel entier n peut s'écrire de façon unique sous la forme

$$n = p^{v_p(n)} n'$$

où $p \nmid n'$ (p ne divise pas n'). Par exemple, si nous avons choisi le nombre premier 5, nous avons

$$\begin{aligned} 2 &= 5^0 2 \\ 5 &= 5^1 1 \\ 6 &= 5^0 6 \\ 150 &= 5^2 6 \end{aligned}$$

et nous avons donc $v_5(2) = v_5(6) = 0$; $v_5(5) = 1$; $v_5(150) = 2$. $v_p(n)$ est appelé la valuation $p-$adique du nombre n, et désigne la multiplicité du facteur premier p pour former le nombre n. Par convention, $v_p(0) = \infty$: on peut diviser 0 par p ; le résultat étant 0, on peut encore multiplier 0 par p et cela peut continuer infiniment.

On peut étendre de façon évidente la valuation $p-$adique aux nombres rationnels : $v_p(a/b) = v_p(a) - v_p(b)$

Et ce n'est pas difficile de voir que

1. $v_p(xy) = v_p(x) + v_p(y)$
2. $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$

Si l'on compare les propriétés de v_p à une valeur absolue, nous voyons que v_p agit un peu comme un logarithme. Nous pouvons donc définir la valeur absolue $p-$adique d'un nombre x par

$$|x|_p = p^{-v_p(x)}$$

et pour revenir à l'exemple des nombres précédents, $|2|_5 = |6|_5 = 1$; $|5|_5 = |10|_5 = 1/5$; $|150|_5 = 1/25$. En utilisant notre convention, nous avons en plus $|0|_5 = 0$.

Nous devons remarquer plusieurs chose à ce niveau : (i) la valeur absolue $p-$adique d'un nombre est inférieure ou égale à 1 ; (ii) plus un nombre est divisible par p, plus sa valeur absolue est proche de 0. Nous laissons au lecteur le soin de démontrer que cette valeur absolue en est vraiment une, et qu'en plus, elle est non archimédienne. Nous pouvons en plus démontrer que si $x \neq y$, alors $|x + y|_p = \max\{|x|_p, |y_p|\}$.

Super, nous disposons d'une valeur absolue sur $\mathbb{Q}$, nous pouvons donc définir une distance : $d(x, y) = |x - y|_p$. Par exemple, pour la distance 5-adique, $d(5, 6) = 1$; $d(5, 10) = 1/5$; $d(5, 30) = 1/125$. Notons que cette métrique a la propriété suivante : $d(x, y) \leq \max\{d(x, z), d(y, z)\} \forall x, y, z \in \mathbb{Q}$. Cette inégalité est appelé l'inégalité ultramétrique.

Notons combien cette distance est différente de la distance habituelle. Prenons par exemple trois points quelconques mais distinct x, y, z. Alors deux des distances sont égales ! Ceci découle du fait que $(x - y) + (y - z) = (x - z)$. Si $|x - y| \neq |y - z|$, alors $|x - z|$ est égale au plus grand d'entre eux.

Comme nous disposons d'une distance, nous pouvons définir les suites et leur convergences, et fermer $\mathbb{Q}$ pour obtenir l'ensemble $\mathbb{Q}_p$. Nous pouvons développer l'analyse exactement comme nous avons fait avec les nombres réels, définir les fonctions, leurs dérivées et intégrales, ... Nous ne développons pas plus cela ici, notons simplement quelques faits inhabituels de ces ensembles :

— Pour qu'une suite a_n converge, il suffit que $|a_{n+1} - a_n| \to 0$ (c'est beaucoup plus simple que le critère de Cauchy).
— Pour que la série $\sum a_n$ converge, il suffit que $|a_n|_p \to 0$
— Si un point appartient à une boule (ouverte ou fermée), il en est le centre,
— ...