La construction des nombres

Arthur Touati

8 décembre 2018

Table des matières

Introduction

Nous utilisons les nombres depuis plusieurs millénaires, mais leur construction n'a été réalisé que dans la deuxième moitié du 19ème siècle. C'est le lot de beaucoup de concepts mathématiques : dans un premier temps on les découvre et on les utilise conformément à l'intuition que l'on a d'eux sans nécessairement se poser la question fondamentale de leur définition, et dans un deuxième temps on cherche à les définir à travers des constructions abstraites qui permettent deux choses :

— appuyer notre usage des mathématiques sur des définitions parfois abstraites mais solides, qui ne laissent pas de place à l'interprétation et au doute quant à la nature des objets.
— conforter notre intuition première, qui est à la source de tout objet mathématique.

Dans son livre *Les Origines de la Géométrie*, le philosophe Michel Serres écrit :

> La mathématique n'a donc pas été une fois, et ceci à tout jamais, en situation d'origine. L'édification d'un langage nouveau pour une nouvelle communication parfaite, la constitution de nouvelles idéalités, la prise en charge de la totalité de l'édifice amènent le savant, au moment des grandes entreprises systématiques, à reprendre l'intégralité du chemin parcouru.

Il reprend plus loin :

> On n'en finirait pas de redire combien de fois la question est repassée sur la droite réelle, sur le zéro, sur les nombres entiers, sur l'égalité, sur la diagonale ou sur le cercle, et combien de fois la réponse à la question reconstruisit les fondations en sous-oeuvre, non seulement pour les axiomes de départ, mais dans la constitution même des idéalités en question.

Dans ce cours nous allons expliquer comment les mathématiciens du 19ème siècle ont défini les nombres (entiers, rationnels et réels) et comment ils ont, pour citer Serres, repris l'intégralité du chemin parcouru, au moins sur cette question.

1 Les relations d'équivalence

La construction des nombres passent par la notion de relation d'équivalence et d'ensemble quotient. L'intérêt de cette notion dépasse largement le cadre de ce cours, on la retrouve dans tous les domaines des mathématiques sans exception. L'idée générale est la suivante : si je me donne un ensemble quelconque, je veux pouvoir établir une règle qui me dit si deux éléments sont "proches" ou "équivalents" (au mathématicien de choisir sa notion d'équivalence en fonction de ses besoins) ; l'ensemble quotient est l'ensemble obtenu en identifiant les éléments équivalents.

De manière plus abstraite, on propose les définitions suivantes :

Définition 1. Une relation binaire R sur un ensemble E est une partie G de $E \times E$, qu'on appelle le graphe de la relation.
Si $(x, y) \in G$, on note xRy et on dit que x est en relation avec y.

Définition 2. Une relation d'équivalence R sur un ensemble E est une relation binaire qui est :

— réflexive : $\forall x \in E, xRx$.
— symétrique : $\forall x, y \in E, xRy \Longrightarrow yRx$.
— transitive : $\forall x, y, z \in E, xRy$ et $yRz \Longrightarrow xRz$.

Exemple 1. Voici quelques exemples de relations d'équivalence simples :

1. Si E est un ensemble, la relation d'égalité est une relation d'équivalence, quel est son graphe ?
2. Si on suppose l'ensemble $\mathbb{Z}$ connu, et si $n \in \mathbb{Z}$, la relation définie par $aRb \iff n|(a-b)$ est une relation d'équivalence appelée la congruence.
3. Dans une salle de classe, on peut définir la relation sur l'ensemble des élèves "être assis sur la même rangée".

Définition 3. Si E est un ensemble muni d'une relation d'équivalence R, pour $x \in E$ on appelle la classe de x l'ensemble $[x] = \{y \in E \mid yRx\}$.

Proposition 1. Si E est un ensemble muni d'une relation d'équivalence R, on a les propriétés suivantes :

— $\forall x, y \in E, xRy \Longrightarrow [x] = [y]$.
— $\forall x, y \in E, \text{non}(xRy) \Longrightarrow [x] \cap [y] = \emptyset$.

Exemple 2. On reprends les relations d'équivalences de l'exemple précédent, décrire dans les trois les cas les classes d'équivalence :

1. Egalité sur un ensemble quelconque.
2. Congruence sur $\mathbb{Z}$.
3. "Etre assis sur la même rangée" sur l'ensemble des élèves d'une salle de classe.

Exercice 1. Soit E un ensemble, on note $F = E^E$ et $\text{Bij}(E)$ le sous-ensemble de F des applications bijectives. On définit sur F une relation d'équivalence par

$$f \sim g \iff \exists \phi \in \text{Bij}(E),\ f = \phi \circ g \circ \phi^{-1}.$$

Montrer que c'est bien une relation d'équivalence sur F et donner la classe d'équivalence de Id_E.

Théorème 1. Si E est un ensemble muni d'une relation d'équivalence, alors les classes d'équivalence forment une partition de E.

Définition 4. Si E est un ensemble muni d'une relation d'équivalence R, on appelle ensembl quotient de E par la relation R, et on note $E/_R$ l'ensemble $\{[x] \mid x \in E\} \subset \mathcal{P}(E)$.

Exemple 3. On reprends les relations d'équivalences de l'exemple précédent, décrire dans les trois les cas l'ensemble quotient :

1. Egalité sur un ensemble quelconque.
2. Congruence sur $\mathbb{Z}$.
3. "Etre assis sur la même rangée" sur l'ensemble des élèves d'une salle de classe.

2 Les entiers relatifs

On suppose dans cette partie que l'ensemble $\mathbb{N}$ est définit et que ses propriétés sont connues (en particuliers l'addition, la multiplication et la relation d'ordre).

Pourquoi a-t-on besoin d'un ensemble de nombres plus gros que $\mathbb{N}$? Le principal problème de $\mathbb{N}$ est l'absence d'inverse pour l'addition : c'est-à-dire qu'il n'existe pas de solution dans $\mathbb{N}$ à l'équation

$$x + n = 0,$$

où x est l'inconnue et $n \in \mathbb{N}^*$.

On ne peut pas naïvement rajouter les éléments -1,-2 (et tous les autres), car le symbole "-" n'existe pas si notre horizon mathématique s'arrête à $\mathbb{N}$.

L'idée est la suivante : si on veut définir le nombre -1, on le voit comme la différence entre 0 et 1. On rencontre deux problèmes :

— -1 est aussi la différence entre 1 et 2, ou entre 100 et 101, nous avons donc plusieurs paires de nombres qu'on cherche à identifier à -1, d'où l'irrésistible envie de quotienter...
— on parle ici de différence entre deux entiers mais cette différence n'est pas définie, et c'est justement ce que l'on souhaite faire !

On procède comme suit.

Définition 5. On définit sur $\mathbb{N}^2$ la relation binaire suivante :

$$(a, b)R_1(c, d) \iff a + d = b + c.$$

Proposition 2. La relation précédente est une relation d'équivalence sur $\mathbb{N}^2$.

Définition 6. On définit l'ensemble des nombres entiers relatifs :

$$\mathbb{Z} = \mathbb{N}^2/_{R_1}.$$

Cette définition est claire et ne laisse place à aucun paradoxe mais elle ne correspond pas à notre intuition des entiers relatifs, qui sous cette forme, sont des ensembles de couples de nombres entiers naturels...

Nous allons commencer par donner un peu de structure à notre nouvel ensemble.

Théorème 2. On définit sur $\mathbb{Z}$ la loi $+_{\mathbb{Z}}$ par :

$$[(a,b)] +_{\mathbb{Z}} [(c,d)] = [(a +_{\mathbb{N}} c, b +_{\mathbb{N}} d)].$$

Cette opération ne dépend pas du choix du représentant dans la classe d'équivalence, elle est commutative et associative d'élément neutre $[(0,0)]$. L'inverse d'un élément $[(a,b)]$ de $\mathbb{Z}$ pour cette loi est donné par $[(b,a)]$.

Les propriétés prouvées dans le théorème font de $(\mathbb{Z}, +_{\mathbb{Z}})$ un groupe commutatif.

Nous pouvons aussi définir la multiplication :

Théorème 3. On définit sur $\mathbb{Z}$ la loi $\times_{\mathbb{Z}}$ par :

$$[(a,b)] \times_{\mathbb{Z}} [(c,d)] = [(a \times_{\mathbb{N}} c +_{\mathbb{N}} b \times_{\mathbb{N}} d, a \times_{\mathbb{N}} d +_{\mathbb{N}} b \times_{\mathbb{N}} c)].$$

Cette opération ne dépend pas du choix du représentant dans les classes d'équivalence, elle est commutative et associative d'élément neutre $[(1,0)]$.

Les propriétés prouvées dans le théorème (en ajoutant le fait que $\times_{\mathbb{Z}}$ est distributive sur $+_{\mathbb{Z}}$) font de $(\mathbb{Z}, +_{\mathbb{Z}}, \times_{\mathbb{Z}})$ un anneau commutatif. A partir de maintenant on omettra l'indice $\mathbb{Z}$, en gardant bien en tête que ces lois ne sont formellement pas les mêmes que celles de $\mathbb{N}$.

Avant de passer aux rationnels, prouvons qu'avec cette définition des entiers relatifs, on retrouve bien le fait que $\mathbb{Z}$ est composé de deux copies de $\mathbb{N}$ avec un symbole "-" sur l'une des deux.

Théorème 4. Soit $[(a,b)] \in \mathbb{Z}$, on est dans une des trois situations suivantes :
- si $a = b$, alors $[(a,b)] = [(0,0)]$.
- si $a > b$, alors $[(a,b)] = [(d,0)]$ où $a = b + d$.
- si $a < b$, alors $[(a,b)] = [(0,d)]$ où $a + d = b$.

Pour se simplifier la vie, on va donc écrire d au lieu de $[(d,0)]$ et $-d$ au lieu de $[(0,d)]$ (car $[(0,d)]$ est bien l'opposé pour la loi $+$ dans $\mathbb{Z}$ de $[(d,0)]$), on a bien définit le symbole "-" ! Avec cette convention et l'identification naturelle entre $\mathbb{N}$ et $\{[(d,0)] \mid d \in \mathbb{N}\}$, on retrouve bien la forme attendue de $\mathbb{Z}$:

$$\mathbb{Z} = \mathbb{N} \cup \{-d \mid d \in \mathbb{N}^*\}.$$

Avec ce cadre très formel, on peut démontrer un vieux résultat du collège : "moins par moins ça fait plus" !

Proposition 3. Si $a, b \in \mathbb{N}$, on a les égalités

$$\begin{aligned} [(a,0)] \times [(b,0)] &= [(ab,0)] \\ [(a,0)] \times [(0,b)] &= [(0,ab)] \\ [(0,a)] \times [(0,b)] &= [(ab,0)]. \end{aligned}$$

Avec nos conventions précédentes, l'égalité $[(0,1)] \times [(0,1)] = [(1,0)]$ se réécrit $(-1) \times (-1) = 1$! Dans la suite, on notera $\mathbb{Z}^*$ l'ensemble $\mathbb{Z}$ privé de $[(0,0)]$.

Toute la théorie de l'arithmétique peut se déduire de ces définitions, dans la suite nous les supposerons démontrées.

3 Les nombres rationnels

La construction des nombres rationnels à partir de $\mathbb{Z}$ est très similaire à la construction de $\mathbb{Z}$ à partir de $\mathbb{N}$.

Le problème de $\mathbb{Z}$ est qu'il n'y pas d'inverse pour la multiplication (sauf pour 1 et -1), c'est-à-dire que si $n \in \mathbb{Z}\backslash\{-1, 1\}$, l'équation

$$x \times n = 1$$

n'a pas de solutions dans $\mathbb{Z}$.

Nous voulons rajouter à $\mathbb{Z}$ des quantités telles que $\frac{1}{2}$ ou $-\frac{2}{3}$, mais comme ci-dessus nous ne pouvons pas les rajouter naïvement. Nous singeons donc la démarche suivie pour définir $\mathbb{Z}$:

Définition 7. On définit sur $\mathbb{Z} \times \mathbb{Z}^*$ la relation binaire suivante :

$$(a, b)R_2(c, d) \iff ad = bc.$$

Proposition 4. La relation précédente est une relation d'équivalence sur $\mathbb{Z} \times \mathbb{Z}^*$.

Définition 8. On définit l'ensemble des nombres rationnels :

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/_{R_2}.$$

Avec cette définition on peut démontrer la proposition suivante, qui nous sera utile plus tard :

Proposition 5. Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, on a :

$$[(a, b)] = [(0, 1)] \iff a = 0.$$

On peut du coup définir l'ensemble $\mathbb{Q}^* = \mathbb{Q}\backslash\{[(0, 1)]\}$

Comme précédemment, nous allons munir $\mathbb{Q}$ d'une structure algébrique, cette fois de corps commutatif.

Théorème 5. On définit sur $\mathbb{Q}$ la loi $+_{\mathbb{Q}}$ par :

$$[(a, b)] +_{\mathbb{Q}} [(c, d)] = [(ad + bc, bd)].$$

Cette opération ne dépend pas du choix du représentant dans la classe d'équivalence, elle est commutative et associative d'élément neutre $[(0, 1)]$. L'inverse d'un élément $[(a, b)]$ de $\mathbb{Q}$ pour cette loi est donné par $[(-a, b)]$.

Théorème 6. On définit sur $\mathbb{Q}$ la loi $\times_{\mathbb{Q}}$ par :

$$[(a, b)] \times_{\mathbb{Q}} [(c, d)] = [(ac, bd)].$$

Cette opération ne dépend pas du choix du représentant dans la classe d'équivalence, elle est commutative et associative d'élément neutre $[(1, 1)]$. L'inverse d'un élément $[(a, b)] \in \mathbb{Q}^*$ pour cette loi est donné par $[(b, a)]$.

On peut aussi montrer que la loi de multiplication est distributive sur l'addition. Ce résultat ainsi que les deux théorèmes précédents font de $(\mathbb{Q}, +_{\mathbb{Q}}, \times_{\mathbb{Q}})$ un corps commutatif.

Comme dernier résultat sur les nombres rationnels, nous pouvons démontrer la proposition suivante, qui correspond au fait bien connu suivant : toute fraction peut se mettre sous une forme irréductible.

Proposition 6. Soit $[(a,b)]$ un rationnel non-nul, alors il existe un unique couple $(p,q) \in \mathbb{Z}^* \times \mathbb{Z}_+^*$ tels que

$$[(a,b)] = [(p,q)] \text{ et } PGCD(p,q) = 1.$$

4 Les nombres réels

Nous allons maintenant nous atteler à la difficile tâche de construire l'ensemble $\mathbb{R}$. Comme ci-dessus, nous allons nous demander pourquoi nous avons besoin de $\mathbb{R}$, quels problèmes nous pose l'ensemble $\mathbb{Q}$? Nous adoptons comme ci-dessus le point de vue "équation" : dans $\mathbb{Q}$ il n'y a pas de solutions à l'équation $x^2 = 2$. Mais ici il ne s'agit ici pas d'un manque de structure algébrique (comme dans le cas de $\mathbb{N}$ ou $\mathbb{Z}$) mais d'un manque de structure topologique...

4.1 Les suites rationnelles

Définition 9. Une suite rationnelle est une application $u : \mathbb{N} \longrightarrow \mathbb{Q}$.

On oublie le point de vue fonctionnel pour garder celui d'une liste de rationnels ordonnés. Au lieu de u, on note $(u_n)_{n\in\mathbb{N}}$ la suite, et au lieu de $u(n)$, on note u_n le n-ième terme.

On peut définir la somme et le produit de deux suites rationnelles en s'appuyant sur la somme et le produit dans $\mathbb{Q}$:

Proposition 7. Soit $u = (u_n)_{n\in\mathbb{N}}$ et $v = (v_n)_{n\in\mathbb{N}}$ deux suites rationnelles, on définit alors

$$\begin{aligned} u + v &= (u_n + v_n)_{n\in\mathbb{N}} \\ u \times v &= (u_n \times v_n)_{n\in\mathbb{N}}. \end{aligned}$$

Ces deux lois font de l'ensemble des suites rationnelles un anneau commutatif. La structure de corps de $\mathbb{Q}$ ne passe pas aux suites rationnelles : une suite est inversible pour $\times$ si et seulement si tous ses termes sont non-nuls, alors qu'elle est non-nulle si au moins un de ses termes est non-nul.

La définition suivante est très importante et peut être transposée telle quelle dans beaucoup d'autres cadres que $\mathbb{Q}$.

Définition 10. On dit qu'une suite rationnelle $u = (u_n)_{n\in\mathbb{N}}$ converge vers un rationnel ℓ lorsque

$$\forall \varepsilon \in \mathbb{Q}_+^*, \exists N \in \mathbb{N}, \forall n \geq N, |u_n - \ell| \leq \varepsilon.$$

Au cours du 19ème siècle les mathématiciens ont cherché une définition équivalente de la convergence ne faisant pas intervenir la limite de la suite. Le mathématicien français Auguste Cauchy proposa la définition suivante qui est restée comme celle des suites de Cauchy :

Définition 11. Une suite rationnelle $u = (u_n)_{n\in\mathbb{N}}$ est dite de Cauchy lorsque

$$\forall \varepsilon \in \mathbb{Q}_+^*, \exists N \in \mathbb{N}, \forall n, m \geq N, |u_n - u_m| \leq \varepsilon.$$

On définit l'ensemble $\mathcal{C}$ comme l'ensemble des suites de Cauchy rationnelles.

Nos deux définitions se ressemblent et la question est la suivante : une suite convergente est-elle de Cauchy et une suite de Cauchy est-elle convergente ? Dans un monde idéal, si les termes d'une suite se rapprochent à l'infini (être de Cauchy), on aimerait qu'ils se rapprochent d'une valeur donnée, qui correspondrait alors à la limite de la suite au sens des suites convergentes. Mais justement, les rationnels ne sont pas un monde idéal...

Proposition 8. Toute suite rationnelle convergente est de Cauchy.

On définit la suite de rationnelle suivante (qui correspond à la méthode de Héron, que les grecs utilisaient pour extraire des racines carrées) : $u_0 = 1$ et pour $n \in \mathbb{N}$ on pose :

$$u_{n+1} = \frac{1}{2}\left(u_n + \frac{2}{u_n}\right).$$

Proposition 9. La suite $(u_n)_{n\in\mathbb{N}}$ est une suite rationnelle de Cauchy mais qui ne converge pas.

Cet exemple nous permet de faire le lien avec ce que l'on a dit au début de cette section : il n'existe pas de rationnel x tel que $x^2 = 2$, et si la suite précédente convergeait, sa limite vérifierait $x^2 = 2$. Les lacunes de l'ensemble des rationnels ne sont donc pas algébriques (alors que la formulation "pas de solution à $x^2 = 2$" le sous-entend) mais topologiques : certaines suites de Cauchy rationnelles ne convergent pas dans $\mathbb{Q}$. Au lieu de rajouter les solutions des équations comme on l'a fait pour $\mathbb{Z}$ et $\mathbb{Q}$, nous allons rajouter les limites des suites de Cauchy, nous allons combler les vides présents dans $\mathbb{Q}$.

Avant de définir l'ensemble des réels, démontrons une petite propriété qui nous sera utile plus tard.

Proposition 10. Toute suite de Cauchy est bornée, c'est-à-dire :

$$\forall u \in \mathcal{C}, \exists M \in \mathbb{Q}_+, \forall n \in \mathbb{N}, |u_n| \leq M.$$

4.2 L'ensemble $\mathbb{R}$ et ses propriétés

De la même manière que nous avons identifié le nombre -1 avec le couple $(0, 1)$, nous allons identifier le nombre $\sqrt{2}$ avec la suite $(u_n)_{n\in\mathbb{N}}$ précédente. Mais là encore il va nous falloir quotienter : en effet si on considère la suite $v_n = u_n + \frac{1}{n}$, cette suite est de Cauchy mais ne converge pas et si elle convergeait sa limite vérifierait encore $x^2 = 2$, on veut donc pouvoir dire que les suites $(v_n)_{n\in\mathbb{N}}$ et $(u_n)_{n\in\mathbb{N}}$ sont équivalentes.

Définition 12. On définit la relation binaire suivante sur l'ensemble $\mathcal{C}$:

$$uR_3v \iff u - v \text{ converge vers } 0.$$

Proposition 11. La relation précédente est une relation d'équivalence sur $\mathcal{C}$.

Définition 13. On définit l'ensemble des réels comme suit :

$$\mathbb{R} = \mathcal{C}/R_3.$$

Le plus difficile est encore devant nous : faire correspondre cette définition abstraite avec notre intuition des nombres réels, et expliquer en quoi cette définition augmente notre compréhension de $\mathbb{R}$.

Dans la suite nous utiliserons les notations suivantes : la classe d'un élément $u \in \mathbb{C}$ sera notée $\overline{u}$, qui est donc un nombre réel. De plus, on note $\mathbb{R}^* = \mathbb{R} \backslash \{\overline{(0)_{n\in\mathbb{N}}}\}$.

4.2.1 Structure algébrique de $\mathbb{R}$

Nous allons commencer par donner une structure algébrique à $\mathbb{R}$: tout comme $\mathbb{Q}$, c'est un corps commutatif.

Théorème 7. On définit sur $\mathbb{R}$ la loi $+_{\mathbb{R}}$ par :

$$\overline{u} +_{\mathbb{R}} \overline{v} = \overline{u + v}.$$

Cette opération ne dépend pas du choix du représentant, elle est commutative et associative, d'élément neutre $\overline{(0)_{n\in\mathbb{N}}}$. L'inverse d'un réel $\overline{u}$ est donné par $\overline{-u}$.

Théorème 8. On définit sur $\mathbb{R}$ la loi $\times_{\mathbb{R}}$ par :

$$\overline{u} \times_{\mathbb{R}} \overline{v} = \overline{u \times v}.$$

Cette opération ne dépend pas du choix du représentant, elle est commutative et associative, d'élément neutre $\overline{(1)_{n\in\mathbb{N}}}$, distributive sur l'addition de $\mathbb{R}$. De plus, tout réel non-nul est inversible.

Le bilan de ces deux théorèmes est que $(\mathbb{R}, +_{\mathbb{R}}, \times_{\mathbb{R}})$ est un corps commutatif.

4.2.2 Relation d'ordre sur $\mathbb{R}$

On peut définir la relation d'ordre usuelle sur $\mathbb{Q}$, en s'appuyant sur celle que l'on a déjà sur $\mathbb{Q}$.

Définition 14. Un réel α est positif si $\alpha = \overline{(0)}$ ou si

$$\exists u \in \alpha, \exists a \in \mathbb{Q}_+^*, \exists N \in \mathbb{N}, \forall n \geq N, u_n \geq a.$$

L'ensemble des réels positifs est noté $\mathbb{R}_+$ et l'ensemble des réels strictement positifs est noté $\mathbb{R}_+^* = \mathbb{R}_+ \backslash \{\overline{(0)}\}$.

On peut définir de la même manière les ensembles $\mathbb{R}_-$ et $\mathbb{R}_-^*$, et on peut démontrer le résultat suivant :

Proposition 12. On a $\mathbb{R}_+ \cap \mathbb{R}_- = \{\overline{(0)}\}$.

Définition 15. On définit une relation binaire sur $\mathbb{R}$ par :

$$\alpha \leq \beta \iff \beta - \alpha \in \mathbb{R}_+.$$

Théorème 9. La relation $\leq$ est une relation d'ordre sur $\mathbb{R}$, c'est-à-dire :
- réflexivité : $\forall \alpha \in \mathbb{R}, \alpha \leq \alpha$.
- anti-symétrie : $\forall \alpha, \beta \in \mathbb{R}, (\alpha \leq \beta \text{ et } \beta \leq \alpha) \Longrightarrow \alpha = \beta$.
- transitivité : $\forall \alpha, \beta, \gamma \in \mathbb{R}, (\alpha \leq \beta \text{ et } \beta \leq \gamma) \Longrightarrow \alpha \leq \gamma$.

Cette relation d'ordre est totale, c'est-à-dire que pour tout $\alpha, \beta \in \mathbb{R}$, on a $\alpha \leq \beta$ ou $\beta \leq \alpha$.

Grâce à cette structure d'ensemble ordonné, on peut définir la valeur absolue sur $\mathbb{R}$:

Définition 16. Si $\alpha \in \mathbb{R}$, on définit sa valeur absolue par $|\alpha| = \max(\alpha, -\alpha)$.

Cette définition a bien un sens : comme l'ordre est total, la famille $(\alpha, -\alpha)$ possède bien un plus grand élément.

On peut montrer le résultat suivant, qui montre que la valeur absolue sur $\mathbb{Q}$ et celle sur $\mathbb{R}$ sont "cohérentes" :

Proposition 13. Soit $\alpha \in \mathbb{R}$ et $u \in \alpha$, alors $|u| = (|u_n|)_{n\in\mathbb{N}} \in |\alpha|$.

On pourrait aussi démontrer les propriétés usuelles de la valeur absolue, par exemple l'inégalité triangulaire etc.

4.2.3 Topologie de $\mathbb{R}$

Dans cette partie, nous allons démontrer les propriétés topologiques de $\mathbb{R}$, qui seront les plus éclairantes quant à la nécessité même de définir les réels : en effet du point de vue algébrique on ne gagne rien ($\mathbb{Q}$ était déjà un corps commutatif)... Comme nous l'avons un peu expliqué plus haut, nous avons "donné aux suites de Cauchy rationnelles non-convergentes des limites abstraites", il reste à le prouver !

Nous allons avoir besoin de considérer $\mathbb{Q}$ comme un sous-ensemble de $\mathbb{R}$, ce qui pour l'instant n'est pas si évident que ça ! On considère l'application suivante :

$$\varphi : h \in \mathbb{Q} \longmapsto \overline{(h)} \in \mathbb{R}.$$

On peut montrer aisément que φ est un isomorphisme de corps compatible avec la relation d'ordre, ce qui concrètement nous permet d'identifier $\mathbb{Q}$ avec le sous-ensemble $\varphi(\mathbb{Q})$ de $\mathbb{R}$, et d'effectuer les opérations algébriques ou de manipuler la valeur absolue dans $\mathbb{Q}$ comme dans $\mathbb{R}$.

Le premier résultat de cette partie concerne la densité de $\mathbb{Q}$ dans $\mathbb{R}$ (en disant ça on fait un abus de notation, on devrait plutôt dire que $\varphi(\mathbb{Q})$ est dense dans $\mathbb{R}$) :

Proposition 14. Pour tous réels α, β tels que $\alpha < \beta$, on a $\mathbb{Q} \cap]a, b[\neq \emptyset$.

Dans les cours de mathématiques de prépa, on présente la densité de $\mathbb{Q}$ dans $\mathbb{R}$ comme un résultat en soi, mais ce n'est en fait qu'une conséquence directe de la définition de $\mathbb{R}$!

La proposition suivante nous permet (enfin) de comprendre ce que l'on voulait dire en disant : nous avons "donné aux suites de Cauchy rationnelles non-convergentes des limites abstraites".

Proposition 15. Soit $u = (u_n)_{n\in\mathbb{N}}$ une suite de Cauchy rationnelle et $\alpha = \overline{u} \in \mathbb{R}$. Considérée dans $\mathbb{R}$, la suite $(u_n)_{n\in\mathbb{N}}$ converge vers α.

En mathématiques, l'opération ensembliste que nous avons réalisé pour définir $\mathbb{R}$ par rapport à $\mathbb{Q}$ s'appelle la complétion, on dit que $\mathbb{R}$ est le complété de $\mathbb{Q}$. La présence dans $\mathbb{Q}$ de suite de Cauchy non-convergentes est vu comme de "l'incomplétude", il "manque" les limites de ces suites. Pour faire simple, i y avait des trous dans $\mathbb{Q}$, que nous avons bouchés. Il reste à montrer qu'il n'y pas de trous dans $\mathbb{R}$. C'est l'objet du théorème suivant :

Théorème 10. L'ensemble $\mathbb{R}$ est complet, c'est-à-dire que toute suite de Cauchy dans $\mathbb{R}$ converge vers un réel.

5 Pour aller plus loin...

5.1 Une autre construction de $\mathbb{R}$

Nous avons construit l'ensemble $\mathbb{R}$ en utilisant les suites de Cauchy rationnelles, cette construction est assez technique mais assez intuitive, et on obtient comme propriété fondamentale de $\mathbb{R}$ sa complétude.

Une autre construction est possible : elle passe par les coupures de Dedekind. Pour faire simple, il s'agit de définir un réel comme la borne supérieure d'un ensemble majoré de rationnels. Cette méthode rend compliqué l'obtention de la structure algébrique de $\mathbb{R}$ et sa complétude, mais par contre elle permet d'accéder rapidement à ce qu'on appelle la propriété de la borne supérieure :

Théorème 11. L'ensemble $\mathbb{R}$ vérifie la propriété de la borne supérieure, c'est-à-dire que toute partie non-vide bornée de $\mathbb{R}$ admet une borne supérieure (un majorant, qui est plus petit que tout autre majorant).

On pourrait bien évidemment prouver ce théorème à partir de notre définition de $\mathbb{R}$, mais ça serait assez laborieux.

Ces deux constructions sont cohérentes, dans le sens où les ensembles obtenus sont isomorphes :

Théorème 12. Soit K un corps totalement ordonné. Les propriétés suivantes sont équivalentes :
- K est isomorphe à $\mathbb{R}$.
- K est archimédien et complet.
- K vérifie la propriété de la borne supérieure.

5.2 Les nombres complexes

En passant de $\mathbb{N}$ à $\mathbb{R}$ on a gagné énormément de structure (algébrique et topologique), mais ce n'est pas encore parfait ! Le problème principal de $\mathbb{R}$ est qu'il n'y a pas de solution réelle à l'équation $x^2 = -1$, L'ensemble $\mathbb{C}$ comble ce manque ! C'est un sur-corps de $\mathbb{R}$ qui hérite de toutes les propriétés topologiques de $\mathbb{R}$ et qui est en plus algébriquement clos : toute équation algébrique (à coefficients dans $\mathbb{C}$) a des solutions dans $\mathbb{C}$.

Il y a plusieurs façons de définir $\mathbb{C}$. La plus simple étant la suivante :

Définition 17. L'ensemble $\mathbb{C}$ est $\mathbb{R}^2$ munit des deux lois suivantes :
- une loi d'addition : $(a, b) + (c, d) = (a + c, b + d)$.
- une loi de multiplication : $(a, b) \times (c, d) = (ac - bd, ad + bc)$.

Nous ne le ferons pas ici, mais avec cette définition on peut démontrer toutes les propriétés usuelles des nombres complexes (équivalence entre forme algébrique et forme trigonométrique, point de vue géométrique etc.).

5.3 Une question de taille

Comme je l'ai fais dans un exposé Parismath précédent, on peut définir la notion de "cardinal" pour les ensembles infinis, je rappelle les résultats importants sous une forme concise :

$$\mathbb{N} \approx \mathbb{Z} \approx \mathbb{Q} < \mathbb{R} \approx \mathbb{C},$$

où $E \approx F$ veut dire que les ensembles sont en bijection et $E < F$ qu'il existe une injection de E dans F mais pas de F dans E.

Il est intéressant de remarquer qu'en terme de structure algébrique, les trois premiers ensembles sont tous très différents, on passe d'un monoïde à un anneau puis à un corps, mais en terme de cardinalité ils sont totalement équivalents !

Entre $\mathbb{Q}$ et $\mathbb{R}$, il n'y a pas de différence algébrique (tous deux sont des corps), mais on gagne une propriété topologique (la complétude), qui explique pourquoi leurs cardinalités sont très différentes différentes.

Entre $\mathbb{R}$ et $\mathbb{C}$, on change de structure algébrique : on passe d'un corps à un corps algébriquement clos. Mais on ne change pas la cardinalité...