Nombres naturels

Roland Christophe

4 avril 2014

Table des matières

1 L'ensemble des naturels

1.1 Introduction

Le concept de «nombre» existe depuis la nuit des temps. C'est un concept fondamental en mathématique, c'est pourquoi Gauss disait : *La mathématique est la reine des sciences et la théorie des nombres est la reine des mathématiques.*

Un type de nombre en particuliers se distingue des autres : *les nombres naturels.* On désigne sous ce terme les nombres entiers positifs : 0, 1, 2, 3, ... sont des nombres naturels. L'ensemble des nombres naturels est noté par la lettre $\mathbb{N}$.

Les pythagoriciens attribuait à ces nombres un statut spécial. Pour eux, seuls les nombres naturels étaient vraiment «naturels», et le résultat d'une mesure ne pouvait être qu'un nombre naturel, ou un rapport entre deux nombres naturels (une fraction entière). Pourtant, un jour, les pythagoriciens démontrèrent qu'un nombre ayant une signification géométrique claire (dans le sens que l'on peut facilement construire géométriquement un segment dont la longueur est ce nombre) ne pouvait pas se mettre sous la forme d'une fraction entière. Ce nombre est la racine carré de deux.

La découverte de ce nombre jeta un trouble chez les disciples de Pythagore : cela contredisait leur philosophie ! Il est d'ailleurs intéressant que ces nombres (qui ne peuvent pas s'écrire sous la forme d'une fraction entière) ont été baptisés «irrationnels». Le trouble fut tel qu'il fut décidé que cette découverte devait rester secrète. Ainsi on raconte même qu'un pythagoricien, Hippase de Métaponte, fut jeté à la mer et mourra noyé pour avoir osé divulgué ce secret. Proclus, un historien du cinquième siècle raconte :

«On dit que les gens qui ont divulgué les nombres irrationnels ont péri dans un naufrage jusqu'au dernier, car l'inexprimable, l'informe, doit être absolument tenu secret ; ceux qui l'ont divulgué et ont touché à cette image de la vie ont instantanément péri et doivent rester éternellement ballottés par les vagues.»

Cette histoire illustre bien l'étrange attraction qu'exerce l'ensemble des naturels. Leurs importance n'est pas seulement philosophique : les naturels ont une place de choix dans les mathématiques, par exemple, c'est à partir de cet ensemble que nous allons définir le raisonnement par récurrence, technique de démonstration très puissante.

Nous avons déjà introduit le concept de nombre naturel en terme d'ensemble. On arrivait à construire à partir de l'axiome de l'infini un ensemble qui contenait des nombres entiers avec des propriétés étranges comme $1 \in 2$ car on avait considéré les nombres comme des ensembles. On avait dit alors que l'on pouvait prouver qu'il existe un ensemble qui ne contient que des nombres puisqu'on n'était pas sûr que c'était le cas de l'ensemble ω. Ce ce que nous allons faire maintenant.

1.2 Définir l'ensemble des naturels

Nous avons montré dans le cadre de la théorie des ensembles, que l'on pouvait construire un ensemble qui contient les éléments $0, 1, 2, 3, \ldots$ plus éventuellement d'autres éléments. Il suffit donc, pour définir l'ensemble des nombres naturels, de considérer l'ensemble de ces ensembles, et de dire que l'ensemble des naturels est «le plus petit» de ces ensembles. On élimine ainsi les éléments «parasites». La manière formelle dont on procède est décrite dans les modes «normal» et «difficile».

On sait tout d'abord qu'il existe au moins un ensemble, que nous notons ω, qui a comme propriété :

$$\emptyset \in \omega \wedge \forall X (X \in \omega \Rightarrow X \cup \{X\} \in \omega)$$

D'autre ensembles que ω ont peut-être aussi cette propriété. On va noter cette propriété P :

$$P(E) \Leftrightarrow (\emptyset \in E \wedge \forall X (X \in E \Rightarrow X \cup \{X\} \in E))$$

Il existe donc certainement plusieurs ensembles vérifiant cette propriété. Parmi eux se trouve l'ensemble de nombres que l'on cherche à définir, plus d'autre qui sont des sur-ensembles de cet ensemble car ils ont des éléments en plus. L'ensemble de nombres est donc «le plus petit» de ces ensembles. On va le noter $\mathbb{N}$.

Puisque $\mathbb{N}$ est «le plus petit» de ces ensembles, si on a un élément $n \in \mathbb{N}$, alors n est aussi élément de tous les ensembles qui vérifient la propriété P. De même, si n est élément de tous les ensembles qui vérifient la propriété P, alors $n \in \mathbb{N}$ puisque $\mathbb{N}$ vérifie la propriété P. On tiens donc un critère pour savoir quels éléments parmi les éléments de ω sont éléments de $\mathbb{N}$ et on le définit en compréhension :

$$\mathbb{N} = \{n \in \omega | \forall E, P(E) \Rightarrow n \in E\}$$

On a donc l'ensemble :

$$\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$$

On dit que c'est l'ensemble des *nombres naturels*.

1.3 Notion de successeur

Définition 1. *On a vu que si $n \in \mathbb{N}$, alors $n \cup \{n\} \in \mathbb{N}$. On va dire que $n \cup \{n\}$ est le* successeur *de n, et on va le noter $s(n)$. On a donc $s(n) = n \cup \{n\}$ et il est facile de voir que s est une fonction de $\mathbb{N}$ vers $\mathbb{N}$.*

Nous avons vu en théorie des ensemble, que l'on peut définir la notion de successeur dans l'ensemble des naturels (voir l'axiome de l'infini). Ainsi, à chaque nombre $x \in \mathbb{N}$, on peut associer «l'élément suivant» que l'on note $s(x)$.

On a donc tout simplement : $s(0) = 1$, $s(1) = 2$, ...

2 Relation d'ordre

Si nous avons deux nombres $a, b \in \mathbb{N}$, alors on peut dire que l'un est «plus petit» que l'autre, et on note si a est plus petit que b, $a < b$. On peut facilement définir cette notion de manière formelle avec ce qui a été vu précédemment, on a tout simplement :

$$\forall a, b \in \mathbb{N}, a < b \Leftrightarrow a \in b$$

Et si $a < b$, on peut écrire aussi $b > a$.

En plus de la notion de «plus petit que» on définit «plus petit ou égal à» et si a est plus petit ou égal à b, on note : $a \leqslant b$ ou $a \leq b$. On le définit comme ceci :

$$\forall a, b \in \mathbb{N}, a \leqslant b \Leftrightarrow (a \in b \vee a = b)$$

On va dire que nous définissons ainsi une *relation d'ordre* sur $\mathbb{N}$ car on introduit l'idée d'«ordre» entre les éléments.

Il reste à définir ce qu'est vraiment une relation d'ordre de manière générale, car on rencontrera ce type de relation dans d'autres ensembles que dans $\mathbb{N}$. On va voir qu'en fait «$\leqslant$» est une relation d'ordre et que «$<$» est une relation d'ordre strict.

2.1 Définition

Sans surprise, on va définir la relation d'ordre comme une relation binaire.

Définition 2. *On dit que la relation binaire R est une relation d'ordre sur un ensemble E, si elle est réflexive, antisymétrique et transitive (si x et y sont en relation, on écrit xRy) :*

1. réflexive *: $\forall x \in E, xRx$,*
2. antisymétrique *: $\forall (x, y) \in E^2, (xRy) \wedge (yRx) \Rightarrow x = y$,*
3. transitive *: $\forall (x, y, z) \in E^3, (xRy) \wedge (yRz) \Rightarrow xRz$.*

On peut facilement se rendre compte que «$\leqslant$» est une relation d'ordre.

On définit aussi la notion de relation d'ordre strict : une relation d'ordre strict est une relation binaire *irréflexive* et transitive. On dit qu'une relation est irréflexive si aucun élément n'est en relation avec lui-même :

$$\forall x \in E, \neg(xRx)$$

On peut facilement se rendre compte que «$<$» est une relation d'ordre strict.

2.2 Ordre totale et partiel

Définition 3. *Si R est une relation d'ordre sur l'ensemble E et qu'elle vérifie :*

$$\forall (x, y) \in E^2, (xRy) \vee (yRx)$$

alors on dit que c'est une relation d'ordre totale. *On dit aussi que E est totalement ordonné ou que (E, R) est un ordre totale.*

3 Principe de récurrence

Nous allons voir maintenant que la structure de l'ensemble $\mathbb{N}$ permet une nouvelle technique de démonstration : la démonstration par récurrence.

3.1 Idée générale du principe de récurrence

Supposons que nous devions démontrer une formule qui dépend uniquement d'un nombre naturel n, c'est à dire une propriété vraie pour tout $n \in \mathbb{N}$. Si cette propriété est P, on a que $P(n)$ est vrai quel que soit n. Le problème est de savoir comment démontrer que $P(n)$ est toujours vrai.

En effet, on peut écrire une démonstration pour démontrer que $P(0)$ est vrai. Puis faire la même chose pour $P(1)$, puis pour $P(2)$, ... mais on n'aura jamais fini la démonstration. Face à ce problème, on peut tenter de prouver $P(n)$ sans faire d'hypothèse sur n c'est à dire que l'on démontre directement $P(n)$ mais ce n'est pas toujours possible ni toujours facile.

Il est cependant parfois possible de démontrer que si pour un certain n $P(n)$ est vrai, alors $P(s(n))$ est vrai aussi. L'idée est donc de montrer d'abord que $P(0)$ est vrai. On suppose alors que $P(n)$ est vrai pour un certain n ce que l'on appelle l'*hypothèse de récurrence*. Ensuite on démontre que $P(s(n))$ est vrai avec cette hypothèse.

Cette démarche est suffisante pour prouver $P(n)$ pour tout $n \in \mathbb{N}$. En effet, on sait que $P(0)$ est vrai (car on le démontre au préalable). Puisqu'on montre ensuite que si $P(n)$ est vrai, alors $P(s(n))$ est vrai aussi, cela veut dire que $P(1)$ est vrai car $P(0)$ est vrai. De la même manière, cela prouve que $P(2)$ est vrai puisque $P(1)$ est vrai, et donc $P(3)$ et ainsi de suite. On a donc démontré $P(n)$ pour tout n.

3.2 Écriture formelle du principe

Dans une démonstration par récurrence on démontre $P(0)$ et on démontre $\forall n \in \mathbb{N}, P(n) \Rightarrow P(s(n))$. Remarquez qu'on devrait écrire formellement : $\forall n, (n \in \mathbb{N} \wedge P(n) \Rightarrow P(s(n)))$ mais on ne le fait pas pour rendre l'écriture de la formule plus facile à lire. Désormais on va accepter ce léger abus de notation.

Le principe de récurrence nous dit donc que si ces deux choses sont prouvées, alors on a montré $\forall n \in \mathbb{N}, P(n)$. On a donc :

$$(P(0) \wedge \forall n \in \mathbb{N}, P(n) \Rightarrow P(s(n))) \Rightarrow (\forall n \in \mathbb{N}, P(n))$$

3.3 Démonstration

Il reste à démontrer cette formule. On suppose donc que $P(0)$ et $\forall n \in \mathbb{N}, P(n) \Rightarrow P(s(n))$ sont vrais et on démontre $\forall n \in \mathbb{N}, P(n)$. On va le faire par l'absurde. Supposons qu'il existe $n \in \mathbb{N}$ tel que $P(n)$ soit faux. On considère le plus petit n tel que $P(n)$ soit faux, et on le note m. $m \neq 0$ car on sait que $P(0)$ est vrai. m est donc le successeur d'un entier p. p est donc plus petit que m et donc $P(p)$ est vrai. On a donc par hypothèse que $P(s(p)) = P(m)$ est vrai et on a une contradiction.

4 L'addition

4.1 Définition

Tout le monde connaît ce qu'est l'addition de deux nombres naturels depuis l'école primaire. On va essayer donc d'aller plus loin et de définir cette notion de manière formelle. On va donc définir l'addition comme une fonction.

Imaginons que nous voulons additionner deux nombres a et b. On va dire que b est l'argument de la fonction «addition», c'est à dire que la fonction s'applique sur b et non sur a. En fait pour chaque a différents, on a une fonction différente.

C'est à dire que pour tout $a \in \mathbb{N}$, on a une fonction f_a de $\mathbb{N}$ vers $\mathbb{N}$, que nous devons définir uniquement à partir des seules notions que nous avons déjà définies dans $\mathbb{N}$, on va donc définir cette notion à partie de la notion de successeur.

On définit donc l'addition comme ceci :

$$\begin{cases} f_a(0) = a \\ \forall n \in \mathbb{N}, f_a(s(n)) = s(f_a(n)) \end{cases}$$

Et on note : $f_a(n) = a + n$. Les deux propriétés qui définissent l'addition peuvent donc s'écrire :

$$a + 0 = a$$

et :

$$\forall n \in \mathbb{N}, a + s(n) = s(a + n)$$

Ces deux seuls propriétés suffisent à définir l'addition.

On remarque que l'on peut facilement démontrer quelque chose d'intuitif : $\forall n \in \mathbb{N}, s(n) = n + 1$. On sait que :

$$\forall n \in \mathbb{N}, a + s(n) = s(a + n)$$

donc pour $n = 0$ on a :

$$a + s(0) = s(a + 0)$$

donc :

$$a + 1 = s(a)$$

On peut donc aussi réécrire la deuxième propriété comme ceci : $a + (n + 1) = (a + n) + 1$.

On va maintenant énoncer une série de propriétés de l'addition.

Théorème 1. *L'addition est* associative*, c'est à dire que :*

$$\forall a, b, c \in \mathbb{N}, (a + b) + c = a + (b + c)$$

On faire cette démonstration par récurrence sur c. On doit donc tout d'abord prouver que c'est vrai pour $c = 0$:

$$(a + b) + 0 = a + (b + 0) \Rightarrow a + b = a + b$$

ce qui est vrai car on sait que $a+0 = a$. Il reste à montrer que si on a : $(a+b)+c = a+(b+c)$ pour un certain c, alors on a : $(a+b)+(c+1) = a+[b+(c+1)]$.

On a :

$$\begin{aligned}(a+b)+(c+1) &= [(a+b)+c]+1\\ &= [a+(b+c)]+1\\ &= a+[(b+c)+1]\\ &= a+[b+(c+1)]\end{aligned}$$

On utilise la propriété : $a+(n+1) = (a+n)+1$ à la première, troisième et quatrième ligne. On utilise l'hypothèse de récurrence à la deuxième ligne.

Théorème 2. *L'addition admet un* élément neutre*, qui n'est autre que zéro :*

$$\forall a \in \mathbb{N}, a+0 = 0+a = a$$

On sait déjà que $a+0 = a$, il reste à montrer que $0+a = a$. On va le faire par récurrence.

On a déjà que $0+0 = 0$. On a comme hypothèse de récurrence : $0+a = a$ et on doit montrer : $0+(a+1) = a+1$.

$$0+(a+1) = (0+a)+1 = a+1$$

Théorème 3. *L'addition est* commutative*, c'est à dire que :*

$$\forall a, b \in \mathbb{N}, a+b = b+a$$

Pour démontrer cela, on doit démontrer au préalable que $a+1 = 1+a$. On va le faire par récurrence. On a pour $a = 0$: $0+1 = 1+0$ ce qui est vrai car 0 est l'élément neutre.

Donc, l'hypothèse de récurrence étant $a+1 = 1+a$, on montre $(a+1)+1 = 1+(a+1)$:

$$(a+1)+1 = (1+a)+1 = 1+(a+1)$$

On peut montrer maintenant $a+b = b+a$ par récurrence sur b. On doit donc montrer sous l'hypothèse $a+b = b+a$ que $a+(b+1) = (b+1)+a$:

$$\begin{aligned}a+(b+1) &= (a+b)+1\\ &= (b+a)+1\\ &= b+(a+1)\\ &= b+(1+a)\\ &= (b+1)+a\end{aligned}$$

5 La multiplication

On utilise le même type de définition que pour l'addition.

5.1 Définition

Pour tout $a \in \mathbb{N}$ on a une fonction g_a de $\mathbb{N}$ vers $\mathbb{N}$ définie par :

$$\begin{cases} g_a(0) = 0 \\ \forall n \in \mathbb{N}, g_a(n+1) = g_a(n) + a \end{cases}$$

Et on note : $g_a(n) = a \cdot n$ ou encore an ou plus rarement $a \times n$. Les deux propriétés qui définissent la multiplication peuvent donc s'écrire :

$$a \cdot 0 = 0$$

$$\forall n \in \mathbb{N}, a \cdot (n+1) = a \cdot n + a$$

Théorème 4. *Distributivité par rapport à l'addition :*

$$\forall a, b, c \in \mathbb{N}, a(b+c) = ab + ac$$

Démonstration par récurrence sur c. On a pour $c = 0$:

$$a(b+0) = ab = ab + a \cdot 0$$

On démontre donc que $a[b+(c+1)] = ab + a(c+1)$ sous l'hypothèse que $a(b+c) = ab + ac$:

$$\begin{aligned} a[b+(c+1)] &= a[(b+c)+1] \\ &= a(b+c) + a \\ &= (ab+ac) + a \\ &= ab + (ac+a) \\ &= ab + a(c+1) \end{aligned}$$

Théorème 5. *Associativité*

$$\forall a, b, c, \in \mathbb{N}, (ab)c = a(bc)$$

Démonstration par récurrence sur c. Pour $c = 0$:

$$(ab) \cdot 0 = 0 = a(b \cdot 0)$$

Et donc sous l'hypothèse que $(ab)c = a(bc)$:

$$\begin{aligned} (ab)(c+1) &= (ab)c + ab \\ &= a(bc) + ab \\ &= a(bc+b) \\ &= a[b(c+1)] \end{aligned}$$

Théorème 6. *Élément neutre :*

$$\forall a \in \mathbb{N}, a \cdot 1 = a = 1 \cdot a$$

On peut déjà prouver facilement que $a \cdot 1 = a$ avec la propriété $a(n+1) = an + a$ pour $n = 0$: $a \cdot 1 = a(0+1) = a \cdot 0 + a = a$. Il reste à montrer que $1 \cdot a = a$ et sans surprise par récurrence. Pour $a = 0$ on a bien $1 \cdot 0 = 0$.

On suppose donc $1 \cdot a = a$ et on a $1 \cdot (a+1) = 1 \cdot a + 1 \cdot 1 = a + 1$.

Théorème 7. *Élément absorbant :*

$$\forall a \in \mathbb{N}, a \cdot 0 = 0 = 0 \cdot a$$

On sait déjà que $a \cdot 0 = 0$, il reste à montrer que $0 \cdot a = 0$. On le fait par récurrence. Pour $a = 0$ on a bien $0 \cdot 0 = 0$.

On suppose donc $0 \cdot a = 0$, on a :

$$0 \cdot (a+1) = 0 \cdot a + 0 \cdot 1 = 0 + 0 = 0$$

Théorème 8. *Commutativité :*

$$\forall a, b \in \mathbb{N}, ab = ba$$

Par récurrence sur b. Pour $b = 0$ on a bien $a \cdot 0 = 0 \cdot a = 0$. On suppose donc $ab = ba$:

$$a(b+1) = ab + a = ba + a = (b+1)a$$