$\mathbb{N}$

Marc Lorenzi

26 septembre 2022

« Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk. »

« Dieu a créé les nombres entiers, tout le reste est l'oeuvre de l'homme. »

Leopold Kronecker (1823-1891)

1 Ensembles inductifs

1.1 Introduction

Nous allons dans cet article donner une construction ensembliste de l'ensemble $\mathbb{N}$ des entiers naturels. Comme la citation de Leopold Kronecker le suggère, nous allons quelque part devoir faire appel à une intervention divine. Effectivement, l'un des axiomes de la théorie des ensembles affirme l'existence d'un certain ensemble vérifiant une certaine propriété : *l'inductivité*. Une fois passée cette pénible étape, nous serons en mesure de tout prouver par nos propres moyens humains.

1.2 Successeur d'un ensemble

Définition 1. Pour tout ensemble x, le *successeur* de x est

$$S(x) = x \cup \{x\}$$

Par exemple,

- $S(\emptyset) = \{\emptyset\}$.
- $S(S(\emptyset)) = \{\emptyset, \{\emptyset\}\}$.
- $S(S(S(\emptyset))) = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.
- $S(S(S(S(\emptyset)))) = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$.

Remarquons que pour tous ensembles x et y,

$$y \in S(x) \iff y \in x \text{ ou } y = x$$

1.3 Ensembles inductifs

Définition 2. Un ensemble E est *inductif* si

- $\emptyset \in E$.
- Pour tout ensemble x, $x \in E \implies S(x) \in E$.

Proposition 1. *Toute intersection d'ensembles inductifs est un ensemble inductif.*

Démonstration. Soit $(A_i)_{i \in I}$ une famille d'ensembles inductifs. Posons

$$A = \bigcap_{i \in I} A_i$$

- Pour tout $i \in I$, $\emptyset \in A_i$, donc $\emptyset \in A$.
- Soit $x \in A$. Soit $i \in I$. On a $x \in A_i$ donc, comme A_i est inductif, $S(x) \in A_i$. Ainsi, $x \in A$.

□

L'un des axiomes de la théorie des ensembles de Zermelo-Fraenkel est *l'axiome de l'infini*, et c'est là que « Dieu » intervient. Il existe de nombreuses façons équivalentes d'écrire l'axiome de l'infini, mais la plus efficace pour nous est la suivante.

Axiome de l'infini. Il existe un ensemble inductif.

À partir du moment où il existe un ensemble inductif, on peut montrer qu'il en existe beaucoup. Celui qui va nous intéresser est le plus petit d'entre eux.

Proposition 2. *Il existe un unique ensemble* $\mathbb{N}$ *vérifiant*

- $\mathbb{N}$ *est inductif.*
- *Pour tout ensemble inductif* F*, on a* $\mathbb{N} \subseteq F$*.*

Démonstration. Prouvons d'abord l'unicité. Soient $\mathbb{N}$ et $\mathbb{N}'$ deux tels ensembles. Comme $\mathbb{N}$ vérifie la seconde propriété et $\mathbb{N}'$ est inductif, $\mathbb{N} \subseteq \mathbb{N}'$. De même, $\mathbb{N}' \subseteq \mathbb{N}$. Ainsi, $\mathbb{N} = \mathbb{N}'$.

Montrons maintenant l'existence. Par l'axiome de l'infini, il existe un ensemble inductif E. Soit

$$\mathcal{F} = \{X \subseteq E : X \text{ est inductif}\}$$

Posons $\mathbb{N} = \bigcap_{X \in \mathcal{F}} X$. Par la proposition 1, $\mathbb{N}$ est inductif. Soit maintenant F un ensemble inductif quelconque. $E \cap F$ est aussi inductif et est inclus dans E. De là, $\mathbb{N} \subseteq E \cap F$, et donc $\mathbb{N} \subseteq F$. □

1.4 Entiers naturels

Définition 3. L'ensemble $\mathbb{N}$ déterminé par la proposition ci-dessus est appelé l'ensemble des *entiers naturels*.

Remarquons que par l'inductivité de $\mathbb{N}$, on a pour tout $n \in \mathbb{N}$, $S(n) \in \mathbb{N}$. On dispose ainsi de l'application *successeur* $S : \mathbb{N} \longrightarrow \mathbb{N}$.

Nous noterons dorénavant $0 = \emptyset$ et $1 = S(\emptyset)$. Le lecteur hardi pourra aussi noter $2 = S(1)$. Quelques téméraires poseront $3 = S(2)$. Par l'inductivité de $\mathbb{N}$, 0, 1, 2 et 3 sont des entiers naturels. Il en existe d'autres ...

Proposition 3. *Soit $A \subseteq \mathbb{N}$. On suppose*

- $0 \in A$.
- *Pour tout $n \in \mathbb{N}$, $n \in A \implies S(n) \in A$.*

Alors, $A = \mathbb{N}$.

Démonstration. A est inductif et $\mathbb{N}$ est le plus petit ensemble inductif, donc $\mathbb{N} \subseteq A$. De plus, $A \subseteq \mathbb{N}$. □

Proposition 4. [Principe d'induction]

Soit $P(n)$ une propriété dépendant de $n \in \mathbb{N}$. On suppose

- $P(0)$.
- *Pour tout $n \in \mathbb{N}$, $P(n) \implies P(S(n))$.*

Alors, pour tout $n \in \mathbb{N}$, $P(n)$.

Démonstration. Soit $A = \{n \in \mathbb{N} : P(n)\}$. On a $0 \in A$ et pour tout $n \in \mathbb{N}$, si $n \in A$ alors $S(n) \in A$. Ainsi, $A = \mathbb{N}$. □

1.5 Un ordre sur $\mathbb{N}$

Définition 4. Pour tous $m, n \in \mathbb{N}$, on pose

$$\begin{aligned} m < n &\iff m \in n \\ m \leq n &\iff m \in n \text{ ou } m = n \end{aligned}$$

Remarquons que pour l'instant rien ne nous permet d'affirmer que $<$ et $\leq$ sont des relations différentes. Nous verrons plus bas que c'est bien le cas.

Proposition 5. *Pour tous $m, n \in \mathbb{N}$,*

$$m \leq n \iff m < S(n)$$

Démonstration. Soient $m, n \in \mathbb{N}$. On a $m \leq n$ si et seulement si $m < n$ ou $m = n$, c'est à dire $m \in n$ ou $m = n$, ou encore $m \in n \cup \{n\}$. □

Proposition 6. *La relation $<$ est transitive.*

Démonstration. Montrons par induction sur p que pour tout $p \in \mathbb{N}$, pour tous $m, n \in \mathbb{N}$, $m < n \wedge n < p \implies m < p$.

- Soient $m, n \in \mathbb{N}$. La propriété « $m < n$ et $n < 0$ » est fausse puisque $n \notin \emptyset$, donc l'implication à prouver est vraie pour $p = 0$.
- Soit $p \in \mathbb{N}$. Supposons la propriété vraie pour p. Soient $m, n \in \mathbb{N}$. Supposons $m < n$ et $n < S(p)$. On a donc $n < p$ ou $n = p$.
  Si $n < p$, on a par l'hypothèse d'induction $m < p$, c'est à dire $m \in p$. A fortiori, $m \in S(p)$, c'est à dire $m < S(p)$.
  Si $n = p$ alors, comme $m < n$, on a $m < p$. On conclut comme dans le premier cas que $m < S(p)$.

□

Proposition 7. *La relation $<$ est irréflexive. Pour tout $n \in \mathbb{N}$, $n \not< n$.*

Démonstration. Montrons par induction sur n que pour tout $n \in \mathbb{N}$, $n \not< n$.

- On a $0 \notin \emptyset$, donc $0 \not< 0$.
- Soit $n \in \mathbb{N}$. Supposons $n \not< n$. Supposons un instant que $S(n) < S(n)$. On a donc $S(n) < n$ ou $S(n) = n$.
  - Cas 1, $S(n) < n$. On a $n < S(n)$ donc, par transitivité de $<$, $n < n$, ce qui contredit l'hypothèse d'induction.
  - Cas 2, $S(n) = n$. Comme $n < S(n)$, on en déduit $n < n$ et on conclut comme dans le cas 1.

□

Corollaire 8. *Pour tous $m, n \in \mathbb{N}$,*

$$m < n \iff m \leq n \text{ et } m \neq n$$

Démonstration. Soient $m, n \in \mathbb{N}$.

Supposons $m < n$. On a alors $m < n$ ou $m = n$, donc $m \leq n$. De plus, comme $n \not< n$, on a $m \neq n$.

Le réciproque est évidente. □

Proposition 9. *La relation $<$ est asymétrique. Pour tous $m, n \in \mathbb{N}$, si $m < n$ alors $n \not< m$.*

Démonstration. Soient $m, n \in \mathbb{N}$. Supposons $m < n$ et $n < m$. Par la transitivité de $<$, on a donc $m < m$, contradiction. □

Proposition 10. *La relation $\leq$ est une relation d'ordre sur $\mathbb{N}$.*

Démonstration. Les propositions précédentes prouvent que $<$ est un ordre strict sur $\mathbb{N}$. La relation $\leq$ est donc une relation d'ordre (large). $\square$

Proposition 11. *Pour tout $n \in \mathbb{N}$, $0 \leq n$.*

Démonstration. Montrons-le par induction sur n. Tout d'abord, $0 \leq 0$. Soit $n \in \mathbb{N}$. Supposons $0 \leq n$. De $n < S(n)$ et de la transitivité de $<$, on déduit $0 < S(n)$. $\square$

Ainsi, 0 est le plus petit entier naturel.

Proposition 12. *Pour tous $m, n \in \mathbb{N}$,*

$$m < n \iff S(m) \leq n$$

Démonstration. Soient $m, n \in \mathbb{N}$. Supposons $S(m) \leq n$. Comme $m < S(m)$, la transitivité de $<$ entraîne que $m < n$.

Montrons maintenant par induction sur n que pour tout $n \in \mathbb{N}$, pour tout $m \in \mathbb{N}$, $m < n \implies S(m) \leq n$.

- Soit $m \in \mathbb{N}$. L'assertion $m < 0$ est fausse, donc l'implication à montrer est vraie pour $n = 0$.
- Soit $n \in \mathbb{N}$. Supposons que pour tout $m \in \mathbb{N}$, $m < n \implies S(m) \leq n$. Soit $m \in \mathbb{N}$. Supposons $m < S(n)$. On a alors, par la proposition 5, $m \leq n$. Si $m < n$, alors par l'hypothèse d'induction, $S(m) \leq n < S(n)$. Si $m = n$ alors $S(m) = S(n) \leq S(n)$.

$\square$

Proposition 13. *Pour tous $m, n \in \mathbb{N}$, $m < n \iff S(m) < S(n)$.*

Démonstration. Soient $m, n \in \mathbb{N}$. Supposons $m < n$. On a alors $S(m) \leq n < S(n)$, d'où $S(m) < S(n)$. Supposons, inversement, que $S(m) < S(n)$. Par la proposition 12, on a $S(m) \leq n$. De là, $m < S(m) \leq n$. $\square$

Proposition 14. *La relation $\leq$ est un ordre total sur $\mathbb{N}$.*

Démonstration. Montrons par induction sur n que pour tout $n \in \mathbb{N}$, pour tout $m \in \mathbb{N}$, $m \leq n$ ou $n \leq m$.

- Soit $m \in \mathbb{N}$. Nous avons vu que $0 \leq m$.
- Soit $n \in \mathbb{N}$. Supposons que pour tout $m \in \mathbb{N}$, $m \leq n$ ou $n \leq m$. Soit $m \in \mathbb{N}$.
  - Si $m \leq n$ alors, comme $n < S(n)$ et $\leq$ est transitive, $m < S(n)$.

- Si $n < m$ alors, par la proposition 12, $S(n) \leq m$.

□

Remarque. Soit $n \in \mathbb{N}$. Pour tout $m \in \mathbb{N}$, si $m < n$ alors $m \in \mathbb{N}$ par définition de la relation $<$. L'ensemble n a-t-il d'autres éléments que des entiers naturels ? La réponse est non.

Proposition 15. *Soit $n \in \mathbb{N}$. Soit m un ensemble. On a $m \in n$ si et seulement si $m \in \mathbb{N}$ et $m < n$.*

Démonstration. Montrons par induction sur n que pour tout $n \in \mathbb{N}$, pour tout ensemble m, $m \in n \implies m \in \mathbb{N}$. Le reste de la proposition en découle facilement.

- La propriété est claire pour $n = 0$ puisque pour tout ensemble m, $m \in 0$ est faux.
- Soit $n \in \mathbb{N}$. Supposons que pour tout ensemble m, $m \in n \implies m \in \mathbb{N}$. Soit m un ensemble. Supposons que $m \in S(n)$. On a donc $m \in n$ ou $m = n$. Si $m \in n$ alors, par l'hypothèse d'induction, $m \in \mathbb{N}$. Si $m = n$ alors $m \in \mathbb{N}$.

□

Pour tout entier $n \in \mathbb{N}$, on a donc

$$n = \{m \in \mathbb{N} : m \in n\} = \{m \in \mathbb{N} : m < n\}$$

Si nous adoptons une notation de type « intervalle » et que pour tous entiers a et b, nous notons

$$[\![a, b]\!] = \{m \in \mathbb{N} : a \leq m \leq b\}$$

avec des notations analogues pour les intervalles ouverts, nous avons donc pour tout $n \in \mathbb{N}$,

$$n = [\![0, n[\![$$

1.6 La fonction S

Nous sommes maintenant en mesure de préciser quelques propriétés de la fonction successeur $S : \mathbb{N} \longrightarrow \mathbb{N}$.

Proposition 16. *S est injective.*

Démonstration. Soient $m, n \in \mathbb{N}$. Supposons $m \neq n$. L'ordre $<$ étant total, on a $m < n$ ou $n < m$. Si $m < n$, alors $S(m) < S(n)$ et donc $S(m) \neq S(n)$. De même si $n < m$. □

Proposition 17. $S(\mathbb{N}) = \mathbb{N} \setminus \{0\}$.

Démonstration. Soit $n \in \mathbb{N}$. Supposons que $S(n) = 0$. On a alors $n < 0$, contradiction. Ainsi, $0 \notin S(\mathbb{N})$. Montrons par induction sur n que pour tout $n \in \mathbb{N}$, si $n \neq 0$ alors il existe $m \in \mathbb{N}$ tel que $n = S(m)$.

- C'est clair pour $n = 0$.
- Soit $n \in \mathbb{N}$. Supposons la propriété vérifiée pour n. Supposons $S(n) \neq 0$ (ce qui est un pléonasme). Il existe alors $m \in \mathbb{N}$ tel que $S(n) = S(m)$, à savoir $m = n$.

□

Remarque. Tout entier naturel non nul est ainsi le successeur d'un unique entier naturel.

2 Induction et récursion

2.1 Le principe d'induction forte

Le principe d'induction a été dans ce qui précède un outil essentiel pour montrer certaines propriétés des entiers naturels. Parfois, ce principe se révèle trop faible. Énonçons donc un résultat plus puissant, le *principe d'induction forte*.

Proposition 18. [Principe d'induction forte]

Soit $P(n)$ une propriété dépendant de $n \in \mathbb{N}$. On suppose que pour tout $n \in \mathbb{N}$,

$$(\forall m \in \mathbb{N}, m < n \implies P(m)) \implies P(n)$$

Alors, pour tout $n \in \mathbb{N}$, $P(n)$.

Démonstration. Considérons la propriété

$$Q(n) = \forall m \in \mathbb{N}, m < n \implies P(m)$$

On a clairement $Q(0)$. Soit $n \in \mathbb{N}$. Supposons $Q(n)$. Soit $m \in \mathbb{N}$. Supposons $m < S(n)$. Si $m < n$ alors, par l'hypothèse d'induction, on a $P(m)$. Si $m = n$ alors, par l'hypothèse du théorème, on a $P(m)$. Ainsi, on a $Q(S(n))$.

Par le principe d'induction, on a ainsi pour tout $n \in \mathbb{N}$, $Q(n)$. De là, pour tout $n \in \mathbb{N}$, on a $Q(S(n))$, c'est à dire pour tout $m < S(n)$, $P(m)$. En particulier, on a $P(n)$. □

2.2 Parties non vides de $\mathbb{N}$

Proposition 19. *Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.*

Démonstration. Soit $A \subseteq \mathbb{N}$. Supposons que A n'a pas de plus petit élément. Considérons $B = \mathbb{N} \setminus A$. Montrons par induction forte sur n que pour tout $n \in \mathbb{N}$, $n \in B$.

Soit $n \in \mathbb{N}$. Supposons que pour tout $m < n$, $m \in B$. Supposons un instant que $n \in A$. Pour tout $m \in A$, $m \notin B$ et donc, par l'hypothèse d'induction, $n \leq m$. Mais alors n est le plus petit élément de A, contradiction. Donc, $n \in B$.

Par le principe d'induction forte, $B = \mathbb{N}$ et donc $A = \emptyset$. □

Proposition 20. *Toute partie non vide et majorée de $\mathbb{N}$ possède un plus grand élément.*

Démonstration. Soit A une partie de $\mathbb{N}$ non vide et majorée. Soit B l'ensemble des majorants de A. B est une partie non vide de $\mathbb{N}$, donc B possède un plus petit élément b.

- Cas 1, $b = 0$. L'ensemble A est majoré par 0. Comme A est non vide, $A = \{0\}$ et ainsi $\max A = 0$.
- Cas 1, $b \neq 0$. Il existe donc $c \in \mathbb{N}$ tel que $b = S(c)$. Comme $c < S(c) = b$ on en déduit, par minimalité de b, que c ne majore pas A. Il existe donc $a \in A$ tel que
$$c < a \leq b$$
et donc aussi
$$b = S(c) \leq a \leq b$$
Par l'antisymétrie de $\leq$, il en résulte que $a = b$. Ainsi, $a \in A$ et a majore A, donc $a = \max A$.

□

2.3 Le théorème de récursion

Ce paragraphe est difficile. Le lecteur pourra sans difficulté admettre la preuve du théorème de récursion donné ci-dessous.

Les deux principes d'induction permettent de *démontrer* des propriétés. Le théorème de récursion permet quant à lui de *définir* des fonctions.

Soit A un ensemble non vide. Notons
$$\mathcal{S}(A) = \bigcup_{n \in \mathbb{N}} A^n$$
L'ensemble $\mathcal{S}(A)$ est donc l'ensemble des *suites finies* d'éléments de A.

Proposition 21. [Théorème de récursion]
Soit $\varphi : \mathcal{S}(A) \longrightarrow A$. Il existe une unique fonction $f : \mathbb{N} \longrightarrow A$ vérifiant
$$\forall n \in \mathbb{N}, f(n) = \varphi\left(f|_n\right)$$

2.3.1 Unicité

Soient $f, g : \mathbb{N} \longrightarrow A$. Supposons que f et g conviennent. Montrons par induction forte sur n que pour tout $n \in \mathbb{N}$, $f(n) = g(n)$.

Soit $n \in \mathbb{N}$. Supposons que pour tout entier $k < n$, $f(k) = g(k)$. On a donc $f|_n = g|_n$. De là,

$$f(n) = \varphi(f|_n) = \varphi(g|_n) = g(n)$$

La preuve de l'existence est plus délicate.

2.3.2 Une remarque sur la notion de fonction

Dans la suite de notre démonstration, nous assimilerons une fonction f à son graphe. Ainsi, une fonction est un ensemble de couples. Le lecteur intrigué par l'idée d'effectuer une réunion de fonctions n'a donc plus de raison de s'inquiéter. Bien sûr, une réunion de fonction n'a aucune raison d'être elle-même une fonction, sauf que dans le domaine qui nous intéresse ce sera justement le cas.

2.3.3 Calculs

Définition 5. Soit $n \in \mathbb{N}$. Soit $g : n \longrightarrow A$. Nous dirons que g est un *calcul* en n étapes à partir de φ si pour tout entier $k < n$, $g(k) = \varphi(g|_k)$.

Nous noterons $\mathcal{C}(g, n, \varphi)$ lorsque g est un calcul en n étapes à partir de φ. Notons

$$T = \{g : \exists n \in \mathbb{N}, \mathcal{C}(g, n, \varphi)\}$$

Notons également

$$f = \bigcup_{g \in T} g$$

2.3.4 f est une fonction

Lemme 22. *f est une fonction.*

Démonstration. Soient (x, y) et (x, y') deux éléments de f. Il existe $n, n' \in \mathbb{N}$ et deux fonctions $g : n \longrightarrow A$ et $g' : n' \longrightarrow A$ éléments de T tels que $y = g(x)$ et $y' = g'(x)$. Prenons par exemple $n \leq n'$. Par une preuve analogue à celle de l'unicité de f, on montre alors que pour tout entier $k < n$, $g(k) = g'(k)$. En particulier, $g(x) = g'(x)$ et donc $y = y'$. □

2.3.5 L'ensemble de départ de f

Lemme 23. *L'ensemble de départ de f est $\mathbb{N}$.*

Démonstration. Cet ensemble de départ est clairement inclus dans $\mathbb{N}$. Inversement, montrons par induction sur n que pour tout $n \in \mathbb{N}$ il existe un calcul en n étapes à partir de φ.

- Il existe évidemment un calcul en 0 étape à partir de φ, qui est l'unique fonction $\emptyset \longrightarrow A$.
- Soit $n \in \mathbb{N}$. Supposons qu'il existe un calcul g en n étapes à partir de φ. Soit $g' : S(n) \longrightarrow A$ définie par $g'(k) = g(k)$ si $k < n$ et $g'(n) = \varphi(g|_n)$. Alors, g' est un calcul en $S(n)$ étapes à partir de φ.

□

2.3.6 La fin de la preuve

Il ne reste plus qu'une étape pour terminer la preuve du théorème de récursion.

Proposition 24. *La fonction f répond à la question.*

Démonstration. Soit $x \in \mathbb{N}$. Soit $g \in T$ un calcul en n étapes à partir de φ, où $x < n$. On a

$$f(x) = g(x) = \varphi(g|_x) = \varphi(f|_x)$$

□

2.4 Récursion faible

Le théorème de récursion est très général. Il admet un certain nombre de corollaires, plus simples à utiliser. Citons-en un, qui nous sera suffisant dans la suite de l'article.

Proposition 25. [Théorème de récursion faible]

Soit A un ensemble non vide. Soit $a \in A$. Soit $\varphi : A \longrightarrow A$. Il existe une unique fonction $f : \mathbb{N} \longrightarrow A$ telle que

- $f(0) = a$.
- *Pour tout $n \in \mathbb{N}$, $f(S(n)) = \varphi(f(n))$.*

Démonstration. L'unicité se montre facilement par induction sur n.

Pour montrer l'existence, considérons la fonction $\Phi : \mathcal{S}(A) \longrightarrow A$ définie comme suit.

- $\Phi(\emptyset) = a$.

- Pour tout $n \in \mathbb{N}$ et tout $g \in A^{S(n)}$,

$$\Phi(g) = \varphi(g(n))$$

Par le théorème de récursion, il existe une unique fonction $f : \mathbb{N} \longrightarrow A$ telle que pour tout $n \in \mathbb{N}$, $f(n) = \Phi(f|_n)$.

On a alors

- $f(0) = \Phi(f|_0) = \Phi(\emptyset) = a$.
- Pour tout $n \in \mathbb{N}$,

$$f(S(n)) = \Phi(f|_{S(n)}) = \varphi(f|_{S(n)}(n)) = \varphi(f(n))$$

□

Nous allons dans les sections suivantes voir comment le théorème de récursion permet de définir une addition et une multiplication dans $\mathbb{N}$. Nous prouverons ensuite les principales propriétés de ces deux opérations.

Commençons par utiliser le théorème de récursion pour prouver une propriété d'unicité de l'ensemble ordonné $(\mathbb{N}, \leq)$.

2.5 L'« unicité » de $\mathbb{N}$

Proposition 26. *Soit $(\mathcal{N}, \preceq)$ un ensemble non vide totalement ordonné. On suppose que*

(1) $\mathcal{N}$ n'a pas de plus grand élément.
(2) Toute partie non vide de $\mathcal{N}$ a un plus petit élément.
(3) Toute partie non vide et majorée de $\mathcal{N}$ a un plus grand élément.

Alors, $(\mathcal{N}, \preceq)$ et $(\mathbb{N}, \leq)$ sont isomorphes.

Démonstration. Pour tout $x \in \mathcal{N}$, notons

$$x^+ = \{y \in \mathcal{N} : x \prec y\}$$

Par (1), l'ensemble x^+ est non vide. Par (2), cet ensemble possède un plus petit élément. Notons-le $\varphi(x)$. On dispose ainsi de la fonction $\varphi : \mathcal{N} \longrightarrow \mathcal{N}$.

Notons également $\omega = \min \mathcal{N}$. Ce minimum existe par (2).

Par le théorème de récursion, il existe une unique fonction $f : \mathbb{N} \longrightarrow \mathcal{N}$ telle que $f(0) = \omega$ et pour tout $n \in \mathbb{N}$, $f(S(n)) = \varphi(f(n))$.

Clairement, on a pour tout $n \in \mathbb{N}$, $f(n) \prec f(S(n))$. On en déduit facilement par induction sur n que pour tous $m, n \in \mathbb{N}$,

$$m < n \implies f(m) \prec f(n)$$

Ainsi, f est strictement croissante. La croissance stricte implique l'injectivité. Il reste à montrer que f est surjective. Supposons le contraire. L'ensemble

$$B = \mathcal{N} \setminus f(\mathbb{N})$$

est donc une partie non vide de $\mathcal{N}$. Soit $b = \min B$. Considérons l'ensemble

$$C = \{x \in \mathcal{N} : x \prec b\}$$

On n'a pas $b = \omega$ puisque $f(0) = \omega \in f(\mathbb{N})$. De là, $C \neq \emptyset$. De plus, C est majoré par b donc, par (3), C a un plus grand élément. Notons-le c. On a $c \in C$, donc $c \notin B$. Ainsi, il existe $n \in \mathbb{N}$ tel que $c = f(n)$.

Soit $x \in \mathcal{N}$. Supposons $c \prec x$. On ne peut pas avoir $x \prec b$, sinon $x \in C$ ce qui contredit la maximalité de c. Comme $\preceq$ est un ordre total, on a donc $b \preceq x$. De plus, $c \prec b$, donc b est le plus petit élément de $\mathcal{N}$ strictement supérieur à c. Ainsi,

$$b = \varphi(c) = \varphi(f(n)) = f(n+1)$$

ce qui contredit le fait que $b \notin f(\mathbb{N})$. La fonction f est donc surjective. □

Le plus dur est fait. Nous voici donc en possession d'un ensemble $\mathbb{N}$ totalement ordonné, vérifiant de merveilleuses propriétés. Le théorème de récursion va nous permettre de définir sur $\mathbb{N}$ une addition et une multiplication. Nous montrerons que ces deux opérations vérifient les propriétés que l'on en attend.

3 L'addition dans $\mathbb{N}$

3.1 La définition

Définition 6. Soit $m \in \mathbb{N}$. On définit par récursion sur n l'entier $m + n$ en posant

- $m + 0 = m$.
- Pour tout $n \in \mathbb{N}$, $m + S(n) = S(m + n)$.

Remarque. Pour être précis, nous avons, pour tout $m \in \mathbb{N}$, défini par récursion une fonction « $m+$ ». En fait, on a appliqué le théorème de récursion faible à la fonction $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ définie par $\varphi(x) = S(x)$ et à la valeur initiale $a = m$.

3.2 Associativité

Proposition 27. *Pour tous entiers naturels m, n, p, $(m + n) + p = m + (n + p)$.*

Démonstration. Montrons par induction sur p que pour tout $p \in \mathbb{N}$, pour tous $m, n \in \mathbb{N}$, $(m + n) + p = m + (n + p)$.

- Soient $m, n \in \mathbb{N}$. On a

$$(m + n) + 0 = m + n = m + (n + 0)$$

- Soit $p \in \mathbb{N}$. Supposons que pour tous $m, n \in \mathbb{N}$, $(m+n)+p = m+(n+p)$. Soient $m, n \in \mathbb{N}$. On a

$$\begin{aligned}(m+n)+S(p) &= S((m+n)+p)\\ &= S(m+(n+p))\\ &= m+S(n+p)\\ &= m+(n+S(p))\end{aligned}$$

□

3.3 Commutativité

Lemme 28. *Pour tout $n \in \mathbb{N}$, $0+n=n$.*

Démonstration. Montrons la propriété par induction sur n. On a $0+0=0$. Soit $n \in \mathbb{N}$. Supposons que $0+n=n$. On a alors

$$0+S(n) = S(0+n) = S(n)$$

□

Posons $1 = S(0)$.

Lemme 29. *Pour tout $n \in \mathbb{N}$, $S(n) = n+1 = 1+n$.*

Démonstration. Soit $n \in \mathbb{N}$ On a

$$n+1 = n+S(0) = S(n+0) = S(n)$$

Montrons par induction sur n que pour tout $n \in \mathbb{N}$, $S(n) = 1+n$. On a $S(0) = 1 = 1+0$. Soit $n \in \mathbb{N}$. Supposons que $S(n) = 1+n$. On a alors

$$\begin{aligned}S(S(n)) &= S(1+n)\\ &= 1+S(n)\end{aligned}$$

□

Proposition 30. *Pour tous entiers m et n, $m+n = n+m$.*

Démonstration. Montrons par induction sur n que pour tout $n \in \mathbb{N}$, pour tout $m \in \mathbb{N}$, $m+n = n+m$.

- Soit $m \in \mathbb{N}$. On a $m+0 = m$ et, par le lemme ci-dessus, $0+m = m$. Ainsi, $m+0 = 0+m$.

- Soit $n \in \mathbb{N}$. Supposons que pour tout $m \in \mathbb{N}$, $m+n = n+m$. On a alors

$$\begin{aligned} m + S(n) &= S(m+n) \\ &= S(n+m) \\ &= n + S(m) \\ &= n + (m+1) \\ &= n + (1+m) \\ &= (n+1) + m \\ &= S(n) + m \end{aligned}$$

□

3.4 Compatibilité avec l'ordre

Proposition 31. *Pour tous entiers m, n, p,*

$$m < n \iff m + p < n + p$$

Démonstration. Montrons l'implication directe par induction sur p.

- Le résultat est évident si $p = 0$.
- Soit $p \in \mathbb{N}$. Supposons que pour tous $m, n \in \mathbb{N}$, $m < n \implies m+p < n+p$. Soient $m, n \in \mathbb{N}$. Supposons $m < n$. On a $m + p < n + p$ et donc $S(m + p) < S(n + p)$, c'est à dire $m + S(p) < n + S(p)$.

Pour l'implication réciproque, soient $m, n, p \in \mathbb{N}$. Si $m > n$ alors, par l'implication directe, $n + p < m + p$ et donc $m + p \not< n + p$. Si $m = n$ alors $m + p = n + p$ et donc $m + p \not< n + p$. Ainsi, si $m + p < n + p$, alors $m < n$. □

Corollaire 32. *Pour tous entiers m, n, p,*

$$m + p = n + p \implies m = n$$

Démonstration. Supposons $m \neq n$. Si $m < n$ alors $m + p < n + p$ et donc $m + p \neq n + p$. De même si $m > n$. □

3.5 Soustraction

Proposition 33. *Pour tous entiers m et n, on a $m \leq n$ si et seulement si il existe $p \in \mathbb{N}$ tel que $n = m + p$.*

Démonstration. Soient $m, n, p \in \mathbb{N}$. Supposons que $n = m + p$. On a $0 \leq p$ donc $m + 0 \leq m + p$, c'est à dire $m \leq n$.

Montrons la réciproque par induction sur n.

- Soit $n \in \mathbb{N}$. Supposons que pour tout $m \in \mathbb{N}$, si $m \leq n$ alors il existe $p \in \mathbb{N}$ tel que $n = m + p$. Soit $m \in \mathbb{N}$. Supposons $m \leq S(n)$, c'est à dire $m < n$. Par l'hypothèse d'induction, il existe $p \in \mathbb{N}$ tel que $n = m + p$. De là,
$$S(n) = S(m + p) = m + S(p)$$

□

4 La multiplication dans $\mathbb{N}$

4.1 La définition

Définition 7. Soit $m \in \mathbb{N}$. On définit par récursion sur n l'entier $m \times n$ en posant

- $m \times 0 = 0$.
- Pour tout $n \in \mathbb{N}$, $m \times S(n) = m \times n + m$.

Remarque. Nous avons ici défini par récursion, pour tout $m \in \mathbb{N}$, une fonction « $m\times$ ». Pour cela, on a appliqué le théorème de récursion faible à la fonction $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ définie par $\varphi(x) = x + m$ et à la valeur initiale $a = 0$.

4.2 Produits par 0 et 1

Proposition 34. *Pour tout $n \in \mathbb{N}$, $n \times 0 = 0 \times n = 0$.*

Démonstration. L'égalité $n\times 0 = 0$ résulte de la définition de la multiplication. Montrons par induction sur n que pour tout $n \in \mathbb{N}$, $0 \times n = 0$.

- On a $0 \times 0 = 0$.
- Soit $n \in \mathbb{N}$. Supposons $0 \times n = 0$. On a alors
$$0 \times S(n) = 0 \times n + 0 = 0 + 0 = 0$$

□

Proposition 35. *Pour tout $n \in \mathbb{N}$, $n \times 1 = 1 \times n = 1$.*

Démonstration. Soit $n \in \mathbb{N}$. On a
$$n \times 1 = n \times S(0) = n \times 0 + n = 0 + n = n$$
Montrons par induction sur n que pour tout $n \in \mathbb{N}$, $1 \times n = n$.

- On a $1 \times 0 = 0$.
- Soit $n \in \mathbb{N}$. Supposons $1 \times n = n$. On a alors
$$1 \times S(n) = 1 \times n + 1 = n + 1 = S(n)$$

□

4.3 Distributivité

Proposition 36. *Pour tous $m, n, p \in \mathbb{N}$, $m \times (n + p) = m \times n + m \times p$.*

Démonstration. Montrons le résultat par induction sur p.

- Soient $m, n \in \mathbb{N}$. On a

$$m \times (n + 0) = m \times n = m \times n + m \times 0$$

- Soit $p \in \mathbb{N}$. Supposons que pour tous $m, n \in \mathbb{N}$, $m \times (n+p) = m \times n + m \times p$. On a alors

$$\begin{aligned} m \times (n + S(p)) &= m \times S(n + p) \\ &= m \times (n + p) + m \\ &= m \times n + m \times p + m \\ &= m \times n + m \times S(p) \end{aligned}$$

□

Proposition 37. *Pour tous $m, n, p \in \mathbb{N}$, $(n + p) \times m = n \times m + p \times m$.*

Démonstration. Montrons le résultat par induction sur m.

- Soient $n, p \in \mathbb{N}$. On a

$$(n + p) \times 0 = 0 = 0 + 0 = n \times 0 + p \times 0$$

- Soit $m \in \mathbb{N}$. Supposons que pour tous $n, p \in \mathbb{N}$, $(n+p) \times m = n \times m + p \times m$. On a alors

$$\begin{aligned} (n + p) \times S(m) &= (n + p) \times m + n + p \\ &= n \times m + p \times m + n + p \\ &= n \times m + n + p \times m + p \\ &= n \times S(m) + p \times S(m) \end{aligned}$$

□

4.4 Associativité

Proposition 38. *Pour tous $m, n, p \in \mathbb{N}$, $(m \times n) \times p = m \times (n \times p)$.*

Démonstration. Montrons le résultat par induction sur p.

- Soient $m, n \in \mathbb{N}$. On a

$$(m \times n) \times 0 = 0 = m \times 0 = m \times (n \times 0)$$

- Soit $p \in \mathbb{N}$. Supposons que pour tous $m, n \in \mathbb{N}$, $(m \times n) \times p = m \times (n \times p)$. On a alors

$$\begin{aligned}(m \times n) \times S(p) &= (m \times n) \times p + m \times n \\ &= m \times (n \times p) + m \times n \\ &= m \times (n \times p + n) \\ &= m \times (n \times S(p))\end{aligned}$$

□

4.5 Commutativité

Proposition 39. *Pour tous $m, n \in \mathbb{N}$, $m \times n = n \times m$.*

Démonstration. Montrons le résultat par induction sur n.

- Soit $m \in \mathbb{N}$. On a $m \times 0 = 0 \times m = 0$.
- Soit $n \in \mathbb{N}$. Supposons que pour tout $m \in \mathbb{N}$, $m \times n = n \times m$. Soit $m \in \mathbb{N}$. On a alors

$$\begin{aligned}m \times S(n) &= m \times n + m \\ &= n \times m + 1 \times m \\ &= (n + 1) \times m \\ &= S(n) \times m\end{aligned}$$

□

4.6 Compatibilité avec l'ordre

Proposition 40. *Pour tous $m, n, p \in \mathbb{N}$ tels que $p \geq 1$,*

$$m < n \iff m \times p < n \times p$$

Démonstration. Montrons l'implication directe par induction sur p.

- C'est évident pour $p = 1$.
- Soit $p \geq 1$. Supposons que pour tous $m, n \in \mathbb{N}$, $m < n \implies m \times p < n \times p$. Soient $m, n \in \mathbb{N}$. Supposons $m < n$. On a alors

$$\begin{aligned}m \times S(p) &= m \times p + m \\ &< n \times p + n \\ &= n \times S(p)\end{aligned}$$

La réciproque résulte de l'implication directe. Soient $m, n, p \in \mathbb{N}$. Supposons $p \geq 1$ et $m \times p < n \times p$. On ne peut pas avoir $m \geq n$ sinon, par l'implication directe, $m \times p \geq n \times p$. On a donc $m < n$. $\square$

Corollaire 41. *Pour tous entiers m, n, p tels que $p \geq 1$,*

$$m \times p = n \times p \implies m = n$$

Démonstration. Soient $m, n \in \mathbb{N}$. Soit $p \geq 1$. Supposons $m \neq n$. Par exemple, $m < n$. On a alors $m \times p < n \times p$ et donc $m \times p \neq n \times p$. $\square$

Et voilà. Comme disent certains cours de maths, $\mathbb{N} = \{0, 1, 2, \ldots\}$ est un ensemble muni de deux opérations $+$ et $\times$, ainsi que d'une relation d'ordre $\leq$ vérifiant des propriétés connues de tous.