Construction des entiers naturels

Tout ce qui suit est une définition et l'étude des propriétés élémentaires de l'ensemble des entiers naturels, définis dans le cadre axiomatique de la théorie des ensembles. Nous utilisons ces propriétés sans y penser, elles nous semblent évidentes... Mais peut-être méritent-t'elles parfois que l'on s'y attarde quelque peu ?

Le cadre de théorie des ensembles est ici l'axiomatique de Zermelo-Fraenkel, ainsi que l'axiome de fondation, même si celui-ci n'est pas réellement nécessaire. On pourra trouver une introduction à cette axiomatique dans le texte "Les axiomes de théorie des ensembles".

1 Définition. Propriétés

AXIOME :
Il existe un ensemble $\mathbb{N}$ (dont les éléments sont dits *entiers naturels)* vérifiant les propriétés suivantes :

(i) $\emptyset \in \mathbb{N}$

(ii) L'inclusion est un bon ordre sur $\mathbb{N}$ (*i.e.* tout sous-ensemble non vide de $\mathbb{N}$ admet un plus petit élément).

(iii) En notant $\mathbb{N}^* = \mathbb{N} \setminus \{\emptyset\}$:

$$n \in \mathbb{N}^* \iff \exists m \in \mathbb{N}, \quad n = m \cup \{m\}$$

Remarques

- $\forall n \in \mathbb{N}, \quad n \cup \{n\} \in \mathbb{N}^*$
- $\forall n \in \mathbb{N}, \quad n \in n \cup \{n\}$ et $n \subset n \cup \{n\}$

NOTATION :
$\emptyset = 0$; $0 \cup \{0\} = 1$; $1 \cup \{1\} = 2$... La relation d'ordre $\subset$ sur $\mathbb{N}$ est notée $\leq$; on définit sur $\mathbb{N}$ la relation $\prec$ par :

$$n \prec m \Longleftrightarrow [n \leq m \text{ et } n \neq m]$$

Remarque $\leq$ étant un bon ordre, c'est un ordre total sur $\mathbb{N}$.

Théorème 1.1 *La relation $\leq$ vérifie :*

$$a \leq x \leq a \cup \{a\} \quad \Rightarrow \quad [x = a \text{ ou } x = a \cup \{a\}]$$

Démonstration : Supposons $x \neq a$. $a \subset x$ et $a \neq x$ donc $\exists y \in x \setminus a$. Alors $y \in x$ donc $y \in a \cup \{a\}$; et comme $y \notin a$ on a $y \in \{a\}$ donc $y = a$ et donc $a \in x$.

D'où $\{a\} \subset x$; et comme $a \subset x$, on a bien $a \cup \{a\} \subset x$ donc $a \cup \{a\} = x$.

□

Théorème 1.2 *L'application φ de $\mathbb{N}$ dans $\mathbb{N}^*$ qui à un entier n associe l'entier $\varphi(n) = n \cup \{n\}$ est une bijection de $\mathbb{N}$ sur $\mathbb{N}^*$.*

Démonstration :

- φ est surjective d'après la définition de $\mathbb{N}^*$.
- Soient m et n deux entiers de même image par φ. On peut supposer $n \leq m$ ($\leq$ est un ordre total). $\varphi(m) = \varphi(n) \Rightarrow m \cup \{m\} = n \cup \{n\}$.
  Alors $m \leq m \cup \{m\} = n \cup \{n\}$; or $m \neq m \cup \{m\}$ (sinon on aurait $m \in m$), donc $m \neq n \cup \{n\}$. C'est-à-dire que $n \leq m \prec n \cup \{n\}$ et donc $m = n$.

□

N.B. La propriété $x \notin x$ est prise ici comme axiome, conséquence de l'axiome de fondation. Sans cet axiome, cette propriété reste toutefois vérifiée pour x un entier, et de manière plus générale pour x un ordinal (l'appartenance étant un ordre strict sur tout ordinal).

Remarque $\mathbb{N}$ est donc un ensemble *infini* (car en bijection avec une de ses parties strictes).

2 Récurrence

Théorème 2.1 (principe de récurrence) *Soit* $\mathrm{A} \subset \mathbb{N}$ *tel que :*

- $0 \in \mathrm{A}$
- $\forall n \in \mathbb{N}, \quad n \in \mathrm{A} \quad \Rightarrow \quad \varphi(n) \in \mathrm{A}$

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

Démonstration : Supposons $\mathrm{A} \neq \mathbb{N}$ et notons n le plus petit élément de $\mathbb{N} \backslash \mathrm{A}$ (qui existe puisque $\leq$ est un bon ordre). Alors $n \in \mathbb{N}^*$ (car $0 \in \mathrm{A}$) ; et d'autre part $\varphi^{-1}(n) \in \mathrm{A}$ (car $\varphi^{-1}(n) \prec n$). Donc $n = \varphi(\varphi^{-1}(n)) \in \mathrm{A}$, ce qui contredit la définition de n.

□

Remarque (Principe de récurrence finie)

Soit $b \in \mathbb{N}$ et $\mathrm{B} = \{n \in \mathbb{N} \,|\, n \leq b\}$. Soit $\mathrm{A} \subset \mathrm{B}$ tel que :

- $0 \in \mathrm{A}$
- $\forall n \in \mathrm{B} \backslash \{b\}, \quad n \in \mathrm{A} \quad \Rightarrow \quad \varphi(n) \in \mathrm{A}$

Alors $\mathrm{A} = \mathrm{B}$.

(démonstration identique à la précédente, en remplaçant $\mathbb{N}$ par B).

Le principe de la démonstration par récurrence est donc le suivant. Pour prouver une propriété $\mathfrak{P}_n$ (propriété dépendant de n) pour tout $n \in \mathbb{N}$, il suffit de prouver que :

- $\mathfrak{P}_0$ est vraie.
- $\forall n \in \mathbb{N}, \quad \mathfrak{P}_n \Rightarrow \mathfrak{P}_{\varphi(n)}$

On applique ensuite le principe de récurrence à l'ensemble $\mathrm{A} = \{n \in \mathbb{N} \,|\, \mathfrak{P}_n\}$.

Théorème 2.2 *Pour tout entier n, on a :*

$$n = \{m \in \mathbb{N} \,|\, m \prec n\}$$

Démonstration :

Par récurrence. La propriété $\mathfrak{P}_n$ est ici $\quad [n = \{m \in \mathbb{N} \,|\, m \prec n\}]$.

1) $\mathfrak{P}_0$ est ici $\quad 0 = \{m \in \mathbb{N} \,|\, m \prec 0\}$. Comme $0 = \emptyset$, aucun entier m ne peut vérifier $m \prec 0$ (c'est-à-dire $m \subset \emptyset$ et $m \neq \emptyset$). Donc $\mathfrak{P}_0$ est vraie.

2) Par hypothèse de récurrence, $n = \{m \in \mathbb{N} \,|\, m \prec n\}$. Montrons que $\varphi(n) = \{m \in \mathbb{N} \,|\, m \prec \varphi(n)\}$, c'est-à-dire que $n \cup \{n\} = \{m \in \mathbb{N} \,|\, m \prec \varphi(n)\}$.

a) Soit $m \in n \cup \{n\}$. Alors $m \in n$ ou $m \in \{n\}$, c'est-à-dire $m = n$.
Si $m \in n$, alors $m \prec n$ (par hypothèse de récurrence) ; donc $m \prec \varphi(n)$ (car $n \prec \varphi(n)$).
Si $m = n$, alors $m \prec \varphi(n)$.

b) Soit $m \prec \varphi(n) = n \cup \{n\}$. Alors $m \leq n$ (sinon $n \prec m \prec \varphi(n)$, ce qui est impossible). Si $m \prec n$, alors par hypothèse de récurrence $m \in n$ donc $m \in n \cup \{n\}$. Sinon $m = n$, donc $m \in n \cup \{n\}$.

□

Remarque $\qquad m \in n \quad \Leftrightarrow \quad m \prec n \quad \Leftrightarrow \quad m \leq \varphi^{-1}(n)$

(sinon $\varphi^{-1}(n) \prec m \prec \varphi(\varphi^{-1}(n))$, ce qui est impossible).

On note $\qquad n = \left\{0, 1, \cdots, \varphi^{-1}(n)\right\}$

3 Addition dans $\mathbb{N}$

Pour tout $a \in \mathbb{N}$ on définit la fonction f_a, de $\mathbb{N}$ dans $\mathbb{N}$, de la façon suivante :

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

NOTATION :

On note $f_a(n) = a + n$. On a ainsi défini une addition sur $\mathbb{N}$. Les deux propriétés définissant f_a se traduisent par :

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

Remarque Pour $n = 0$ dans cette égalité, on obtient $a + 1 = \varphi(a)$ donc :

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

Propriétés de l'addition :

a) Associativité :

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

Démonstration : Par récurrence sur c.

$c = 0$: $\qquad (a + b) + 0 = a + b = a + (b + 0)$

On suppose $\qquad (a + b) + c = a + (b + c)$

Alors $\quad (a + b) + (c + 1) = [(a + b) + c] + 1 = [a + (b + c)] + 1$
$\qquad = a + [(b + c) + 1] = a + [b + (c + 1)]$

b) 0 est élément noutre.

Démonstration : Il suffit de montrer $\forall a \in \mathbb{N}, \quad 0 + a = a$ (on a déjà vu $\forall a \in \mathbb{N}, \quad a + 0 = a$). Par récurrence sur a.

$a = 0$: $\qquad 0 + 0 = 0$

On suppose $0 + a = a$. Alors $0 + (a + 1) = (0 + a) + 1 = a + 1$.

c) Commutativité :

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

Démonstration : Par récurrence sur b.

$b = 0$: $\qquad a + 0 = a = 0 + a$

On suppose $a + b = b + a$.
Alors $a + (b + 1) = (a + b) + 1 = (b + a) + 1 = b + (a + 1)$.
Montrons par récurrence sur a que $a + 1 = 1 + a$:

$a = 0$: $\qquad 0 + 1 = 1 = 1 + 0$

Si $a + 1 = 1 + a$, alors $(a + 1) + 1 = (1 + a) + 1 = 1 + (a + 1)$.
On peut alors conclure : $b + (a + 1) = b + (1 + a) = (b + 1) + a$, et la commutativité a été établie par récurrence.

d) Régularité de tout élément de $\mathbb{N}$:

$$\forall a, b, c \in \mathbb{N}, \quad [a + b = a + c \Rightarrow b = c]$$

Démonstration : Par récurrence sur a.

$a = 0$: $\qquad 0 + b = 0 + c \Rightarrow b = c$ car $0 + b = b$ et $0 + c = c$.

On suppose $\qquad [a + b = a + c \Rightarrow b = c]$

Soient a, b et c tels que $(a+1)+b = (a+1)+c$. Alors $a+(1+b) = a+(1+c)$ donc $1 + b = 1 + c$.

Il vient $\qquad \varphi^{-1}(1 + b) = \varphi^{-1}(1 + c)$ soit $b = c$

4 Addition et relation $\leq$

Théorème 4.1 *Pour tous entiers a et n, on a :*

$$a + n \geq a$$

Démonstration : Par récurrence sur n. Le résultat est vrai pour $n = 0$: on a l'égalité. Soit donc $n \in \mathbb{N}$, on suppose $a + n \geq a$.

Alors $a + (n + 1) = (a + n) + 1 = \varphi(a + n) \succ a + n \geq a$, et l'on conclue par récurrence.

□

Théorème 4.2 *Soient a et b deux entiers. Alors on a l'équivalence :*

$$a \leq b \quad \Longleftrightarrow \quad [\exists c \in \mathbb{N}, \quad b = a + c]$$

Démonstration : Par double implication.

– $\boxed{\Rightarrow}$ Par récurrence finie, on montre que pour b un entier fixé,

$$\forall a \in \{0, 1, \ldots, b\}\,, \exists c \in \mathbb{N}, \quad b = a + c$$

Pour $a = 0$, on a bien $b = 0 + b$. Supposons le résultat établi pour $a \prec b$. Soit donc c un entier tel que $b = a + c$.
$c \in \mathbb{N}^*$; soit donc $d = \varphi^{-1}(c)$. Alors $c = d + 1$, donc :

$$b = a + (d + 1) = a + (1 + d) = (a + 1) + d$$

– $\boxed{\Leftarrow}$ Sachant que $b = a + c$ ($c \in \mathbb{N}$), supposons que $a \succ b$.
D'après ce qui précède, il existe un entier $d \in \mathbb{N}^*$ tel que $a = b + d$.

On obtient $$b = (b + d) + c = b + (d + c)$$

Donc, comme b est régulier, $d + c = 0$. Or $d + c \geq d$ (théorème 4.1), donc $d + c \succ 0$, et l'on obtient une contradiction.

□

Remarque Si $a \leq b$, l'entier c tel que $b = a + c$ est unique. En effet, l'égalité $a + c = a + c_1$ implique $c = c_1$, puisque a est régulier. Cet entier est appelé différence de a et b, et est noté $b - a$.

Théorème 4.3 *L'addition et la relation d'ordre $\leq$ sont compatibles :*

$$[\, a \leq b \text{ et } c \leq d \,] \quad \Rightarrow \quad a + c \leq b + d$$

Démonstration : Soient a, b, c et d quatre entiers tels que $[\, a \leq b$ et $c \leq d\,]$. Il existe des entiers a_1 et c_1 tels que $b = a + a_1$ et $d = c + c_1$. Mais alors, $b + d = (a + c) + (a_1 + c_1)$

et donc $$b + d \geq a + c$$ □

5 Multiplication dans $\mathbb{N}$

Pour tout $a \in \mathbb{N}$; on définit une fonction g_a de $\mathbb{N}$ dans $\mathbb{N}$ par :

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

NOTATION :

On note $a \times n = g_a(n)$ (on note encore $a \cdot n$ ou an) ; on définit ainsi une multiplication sur $\mathbb{N}$. Les deux propriétés ci-dessus se traduisent par :

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

Remarque $a \times 1 = a \times 0 + a$ donc $a \times 1 = a$

Propriétés de la multiplication :

a) Distributivité sur l'addition :

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

Démonstration : Par récurrence sur c.

$c = 0$: $\qquad a(b+0) = ab = ab + a.0$

On suppose $a(b+c) = ab + ac$. Alors :

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

La distributivité à droite découle alors de la commutativité, que nous allons montrer plus loin.

b) Associativité :

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

Démonstration : Par récurrence sur c.

$c = 0$: $\qquad (ab) \cdot 0 = 0 = a(b \cdot 0)$

On suppose $(ab)c = a(bc)$. Alors :

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

c) 1 est élément neutre.

Démonstration : Il suffit de montrer, par récurrence sur a, que pour tout entier a, on a $1 \times a = a$.

$a = 0$: $\qquad 1 \times 0 = 0$

On suppose $1 \times a = a$. Alors $1 \times (a+1) = 1 \times a + 1 \times 1 = a + 1$.

d) 0 est un élément absorbant.

Démonstration : Par récurrence sur a, montrons que $\forall a \in \mathbb{N}, \quad 0 \times a = 0$.

$a = 0$: $\qquad 0 \times 0 = 0$

On suppose $0 \times a = 0$. Alors $0 \times (a+1) = 0 \times a + 0 \times 1 = 0 + 0 = 0$.

e) Commutativité :

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

Démonstration : Par récurrence sur b.

$b = 0$: $\qquad a \times 0 = 0 = 0 \times a$

On suppose donc $ab = ba$. Alors $a(b+1) = ab + a = ba + a = b(a+1)$.

f) $\forall a, b \in \mathbb{N}, \quad ab = 0 \iff [a = 0 \text{ ou } b = 0]$

Démonstration : Comme 0 est absorbant, seul reste à démontre le sens $ab = 0 \quad \Rightarrow \quad [a = 0 \text{ ou } b = 0]$.

Supposons $ab = 0$ et $a \geq 1$. Montrons que $b = 0$.

Si $b \geq 1$, alors b s'écrit $b = 1 + c$ $(c \in \mathbb{N})$ et $ab = a(1+c) = a + ac$ donc $ab \geq a \geq 1$, ce qui est une contradiction. Donc $b = 0$.

g) Tout entier non nul est régulier pour la multiplication :

$$\forall a \in \mathbb{N}^*, \forall b, c \in \mathbb{N}, \quad [ab = ac \quad \Rightarrow \quad b = c]$$

Démonstration : Par symétrie, on peut suppoer $b \geq c$. Alors $b = c + d$ $(d \in \mathbb{N})$.

Donc $\qquad ac = ab = a(c+d) = ac + ad$

Et comme tout élément est régulier pour l'addition, $ad = 0$. D'après le point précédent, on a donc $a = 0$ ou bien $d = 0$. Comme par hypothèse $a \in \mathbb{N}^*$, on a $d = 0$, c'est-à-dire $b = c$.

h) $\leq$ et $\times$ sont compatibles :

$$[a \leq b \text{ et } c \leq d] \quad \Rightarrow \quad ac \leq bd$$

Démonstration : Soient donc a, b, c et d tels que $a \leq b$ et $c \leq d$. Il existe deux entiers a_1 et c_1 tels que $b = a + a_1$ et $d = c + c_1$. Alors :

$$\begin{aligned} bd &= (a + a_1)(c + c_1) \\ &= a(c + c_1) + a_1(c + c_1) \\ &= ac + (ac_1 + a_1c + a_1c_1) \end{aligned}$$

donc $$ac \leq bd$$

6 Division euclidienne dans $\mathbb{N}$

Lemme 6.1 (d'Archimède) *Soient a et b entiers avec b non nul. Alors*

$$\exists k \in \mathbb{N}, \quad a \prec bk$$

Démonstration : Il suffit de prendre $k = a + 1$.

On a : $$(a + 1)\, b = ab + b \succ ab \geq a$$ □

Théorème 6.2 (division euclidienne dans $\mathbb{N}$) *Soient a et b entiers avec b non nul. Alors*

$$\exists!(q, r) \in \mathbb{N} \times \mathbb{N}, \quad \begin{cases} a = bq + r \\ r \prec b \end{cases}$$

Démonstration :

– Existence du couple (q, r).
Soit $\mathrm{E} = \{p \in \mathbb{N} \,|\, a \prec pb\}$. D'après le lemme d'Archimède, $\mathrm{E} \neq \emptyset$. Soit donc $x = \min \mathrm{E}$ son plus petit élément.
$x \neq 0$ (puisque $a \geq 0$), donc $x \geq 1$.
Si $q = x - 1$, on a alors $a \prec xb = (q + 1)b$ et $q \notin \mathrm{E}$, d'où l'encadrement $qb \leq a \prec (q + 1)b = qb + b$.
Soit $r = a - bq$. On obtient $a = bq + r \prec bq + b$ donc $r \prec b$

– Unicité du couple (q, r).
Soit $a = bq + r = bq_1 + r_1$ avec $r \prec b$ et $r_1 \prec b$.
Supposons par exemple $r_1 \geq r$. Néccessairement $q_1 \leq q$.
Soit s tel que $r_1 = r + s$ et t tel que $q = q_1 + t$. On a $s \prec b$ (car $r_1 \prec b$).
Il vient en remplaçant :

$$b(q_1 + t) + r = bq_1 + r + s \text{ donc } bt = s$$

Si $t \geq 1$, alors $bt \geq b$ donc $s \geq b$, ce qui est absurde. Donc $t = 0$ et donc $s = 0$. On obtient donc $q = q_1$ et $r = r_1$.

□

Définition L'application ainsi définie, de $\mathbb{N} \times \mathbb{N}^*$ dans $\mathbb{N} \times \mathbb{N}$, qui au couple (a, b) associe le couple (q, r) s'appelle l'opération de *division euclidienne* dans $\mathbb{N}$. q est le *quotient* et r est le *reste* dans la division euclidienne de a par b.