Entiers Naturels.

par Alain Prouté
Université Denis Diderot — Paris 7

Table des matières

1 Les fondements.

1.1 Définition des entiers naturels.

DÉFINITION. *On appelle "système d'entiers naturels", un triplet* $(\mathbf{N}, 0, s)$ *tel que :*
- $\mathbf{N}$ *est un ensemble,*
- 0 *est un élément de* $\mathbf{N}$ *(appelé "zéro"),*
- s *est une application de* $\mathbf{N}$ *vers* $\mathbf{N}$ *(appelée "successeur"),*
- *Pour tout ensemble* X*, tout élément* a *de* X*, et toute application* $h : X \longrightarrow X$*, il existe une unique application* $\varphi : \mathbf{N} \longrightarrow X$*, telle que (pour tout* $n \in \mathbf{N}$*) :*

$$\begin{aligned} \varphi(0) &= a, \\ \varphi(s(n)) &= h(\varphi(n)) \end{aligned}$$

(principe de récursion simple).

Le principe de récursion simple permet de définir des applications par récurrence. La formule $\varphi(0) = a$ impose l'image de 0, l'autre formule impose l'image de $s(n)$ dès que l'image de n est connue. Remarquer que $\varphi(n)$ n'est rien d'autre que le résultat de l'itération n fois de la fonction h sur l'élément a, ce qu'on note en général $h^n(a)$.

Comme on va le voir, ce principe entraine tous les autres principes de récurrence, y compris la forme la plus classique, à savoir le troisième axiome de Peano.

LEMME. *Soient* $(\mathbf{N}, 0, s)$ *et* $(\mathbf{N}', 0', s')$ *deux systèmes d'entiers naturels. Alors il existe une unique bijection* $\varphi : \mathbf{N} \longrightarrow \mathbf{N}'$, *telle que* $\varphi(0) = 0'$, *et* $\forall_{n\in\mathbf{N}}\ \varphi(s(n)) = s'(\varphi(n))$.

C'est une application immédiate du principe de récursion simple (Appliquer deux fois la partie "existence" pour construire φ et sa réciproque φ^{-1}, et deux fois la partie "unicité" pour démontrer que φ^{-1} est bien l'inverse de φ). □

Autrement-dit, deux systèmes d'entiers naturels sont équivalents (isomorphes). Nous postulons maintenant qu'il en existe au moins un. Désormais, on notera $(\mathbf{N}, 0, s)$ un système d'entiers naturels choisi une fois pour toutes, et $\mathbf{N}$ sera appelé l'*ensemble des entiers naturels*.

On notera que la partie unicité du principe de récursion simple, implique que l'application identique $\mathrm{id} : \mathbf{N} \longrightarrow \mathbf{N}$ est caractérisée par (où $n \in \mathbf{N}$) :

$$\begin{aligned} \mathrm{id}(0) &= 0, \\ \mathrm{id}(s(n)) &= s(\mathrm{id}(n)). \end{aligned}$$

1.2 Récursion Primitive.

Du principe de récursion simple, on peut déduire la variante suivante :

THÉORÈME. *(Principe de récursion primitive) Soit* X *un ensemble,* a *un élément de* X, *et* $g : \mathbf{N}\times X \longrightarrow X$ *une application. Alors il existe une unique application* $\varphi : \mathbf{N} \longrightarrow X$, *telle que (pour tout* $n \in \mathbf{N}$*) :*

$$\begin{aligned} \varphi(0) &= a, \\ \varphi(s(n)) &= g(n, \varphi(n)). \end{aligned}$$

En effet, considérons l'élément $(0, a)$ de $\mathbf{N} \times X$, et l'application $h : \mathbf{N} \times X \longrightarrow \mathbf{N} \times X$, définie par (pour $n \in \mathbf{N}$ et $x \in X$) :

$$h(n, x) = (s(n), g(n, x)).$$

En appliquant le principe de récursion simple, on voit qu'il existe une unique application $f : \mathbf{N} \longrightarrow \mathbf{N}\times X$, telle que, pour tout n de $\mathbf{N}$:

$$\begin{aligned} f(0) &= (0, a), \\ f(s(n)) &= h(f(n)) \end{aligned}$$

En posant $f(n) = (\psi(n), \varphi(n))$, on voit que :

$$\begin{aligned} \psi(0) &= 0, \\ \psi(s(n)) &= s(\psi(n)). \end{aligned}$$

Il en résulte que ψ est l'application identique de $\mathbf{N}$. On a donc :

$$\begin{aligned} \varphi(0) &= a, \\ \varphi(s(n)) &= g(n, \varphi(n)), \end{aligned}$$

ce qui démontre la partie "existence" du théorème. Si on a une application φ' telle que :

$$\begin{aligned} \varphi'(0) &= a, \\ \varphi'(s(n)) &= g(n, \varphi'(n)), \end{aligned}$$

on peut poser $f'(n) = (n, \varphi'(n))$, et on voit que :

$$\begin{aligned} f'(0) &= (0, a), \\ f'(s(n)) &= h(f'(n)). \end{aligned}$$

Ceci implique que $f = f'$, donc que $\varphi = \varphi'$. □

Le principe de récursion primitive permet de construire de nombreuses applications de source $\mathbf{N}$, par exemple, l'application "prédécesseur" $p : \mathbf{N} \longrightarrow \mathbf{N}$ définie par :

$$\begin{array}{rcl} p(0) & = & 0, \\ p(s(n)) & = & n. \end{array}$$

Le principe de récursion primitive existe aussi dans une variante "à paramètre". C'est utile, car on a souvent à définir des fonction dont l'ensemble de départ est non pas $\mathbf{N}$ mais un produit cartésien $\mathbf{N} \times X$.

THÉORÈME. *(Principe de récursion primitive) Soient X et A des ensembles, $a : X \longrightarrow A$ une application, et $g : \mathbf{N} \times A \times X \longrightarrow A$ une application. Alors il existe une unique application $\varphi : \mathbf{N} \times X \longrightarrow A$, telle que (pour tout $n \in \mathbf{N}$ et tout $x \in X$) :*

$$\begin{array}{rcl} \varphi(0, x) & = & a(x), \\ \varphi(s(n), x) & = & g(n, \varphi(n, x), x). \end{array}$$

Pour construire l'application $\varphi : \mathbf{N} \times X \longrightarrow A$, nous allons d'abord construire une application $\psi : \mathbf{N} \longrightarrow A^X$ (où A^X est l'ensemble des fonctions de X vers A)[1].

Pour construire ψ, nous définissons :

$$h : \mathbf{N} \times A^X \longrightarrow A^X \qquad \text{par} \qquad h(n, f) = x \mapsto g(n, f(x), x)$$

Le premier principe de récursion primitive (sans paramètre), nous donne donc une unique fonction $\psi : \mathbf{N} \longrightarrow A^X$, telle que :

$$\begin{array}{rcl} \psi(0) & = & a \\ \psi(s(n)) & = & h(n, \psi(n)) \end{array}$$

Définissons maintenant φ par $\varphi(n, x) = \psi(n)(x)$. On a $\varphi(0, x) = \psi(0)(x) = a(x)$, et

$$\begin{array}{rcl} \varphi(s(n), x) & = & \psi(s(n))(x) \\ & = & h(n, \psi(n))(x) \\ & = & g(n, \psi(n)(x), x) \\ & = & g(n, \varphi(n, x), x) \end{array}$$

On a donc montré l'existence de φ. Son unicité résulte du fait qu'on peut réciproquement définir ψ à partir de φ, en posant $\psi(n) = x \mapsto \varphi(n, x)$, et montrer par un calcul analogue au précédent que la fonctionn ψ ainsi obtenue est l'unique fonction donnée par le premier principe de récursion primitive. Les détails sont laissés au lecteur.

1.3 Les Axiomes de Peano.

THÉORÈME. *(Axiomes de Peano) On a :*

- $\forall_{n \in \mathbf{N}}\ 0 \neq s(n)$,
- $\forall_{n \in \mathbf{N}}\ \forall_{m \in \mathbf{N}}\ s(n) = s(m) \Rightarrow n = m$,
- *Pour tout énoncé $P(n)$ dépendant de l'entier naturel n,*

$$(P(0) \wedge (\forall_{n \in \mathbf{N}}\ P(n) \Rightarrow P(s(n)))) \Rightarrow \forall_{n \in \mathbf{N}}\ P(n).$$

[1] Le procédé que nous utilisons ici s'appelle "Curryfication".

Démonstration du premier axiome. Soit $E = \{a, b\}$ un ensemble à deux éléments (distincts). Notons $h : E \longrightarrow E$ l'application constante, envoyant a et b sur b. Le principe de récursion simple entraine qu'il existe une application $\varphi : \mathbf{N} \longrightarrow E$, telle que (pour tout $n \in \mathbf{N}$) :

$$\begin{array}{rcl} \varphi(0) & = & a, \\ \varphi(s(n)) & = & h(\varphi(n)). \end{array}$$

On voit alors que pour tout $n \in \mathbf{N}$, $\varphi(s(n)) = b$. Comme $a \neq b$, on a $0 \neq s(n)$.

Démonstration du deuxième axiome. Soient n et m dans $\mathbf{N}$ tels que $s(n) = s(m)$. En utilisant la fonction "prédécesseur" définie plus haut, on voit que :

$$n = p(s(n)) = p(s(m)) = m.$$

Démonstration du troisième axiome. Supposons $P(0)$ et $\forall_{n\in\mathbf{N}}\ P(n) \Rightarrow P(s(n))$, et démontrons $\forall_{n\in\mathbf{N}}\ P(n)$. Considérons la partie A de $\mathbf{N}$ définie par :

$$A = \{n \in \mathbf{N} \mid P(n)\}.$$

On a $0 \in A$, et A est stable par l'application s. Il en résulte que s induit une application (encore notée s) : $s : A \longrightarrow A$. Le principe de récursion simple montre alors qu'il existe une unique application $\varphi : \mathbf{N} \longrightarrow A$, telle que :

$$\begin{array}{rcl} \varphi(0) & = & 0, \\ \varphi(s(n)) & = & s(\varphi(n)). \end{array}$$

Soit $i : A \longrightarrow \mathbf{N}$ l'inclusion de A dans $\mathbf{N}$. On a :

$$\begin{array}{rcl} (i \circ \varphi)(0) & = & 0, \\ (i \circ \varphi)(s(n)) & = & s((i \circ \varphi)(n)), \end{array}$$

ce qui montre que $i \circ \varphi$ est l'application identique de $\mathbf{N}$. Il en résulte que i est surjective, donc que $A = \mathbf{N}$, donc que $\forall_{n\in\mathbf{N}}\ P(n)$. □

Le troisième axiome de Peano est aussi appelé "principe du raisonnement par récurrence". Nous allons l'utiliser de nombreuses fois dans la suite de ce texte.

2 Arithmétique dans N.

Dans cette section, nous allons construire les opérations fondamentales de $\mathbf{N}$, comme l'addition, la multiplication, la division euclidienne.

2.1 L'addition.

L'addition $+ : \mathbf{N}\times\mathbf{N} \longrightarrow \mathbf{N}$ peut se définir à l'aide du principe de récursion primitive (avec paramètre) :

$$\begin{array}{rcl} +(0, m) & = & m \\ +(s(n), m) & = & s(+(n, m)) \end{array}$$

Bien entendu, nous utiliserons la notation $n + m$ à la place de $+(n, m)$. Ces mêmes égalités peuvent donc se réécrire :

$$\begin{array}{rcl} 0 + m & = & m \\ s(n) + m & = & s(n + m) \end{array}$$

THÉORÈME. *L'addition des entiers natuels est associative, c'est–à–dire qu'on a pour tous n, m et p dans* $\mathbf{N}$ *:*

$$(n+m)+p = n+(m+p)$$

On procède par récurrence sur n. On a :

$$\begin{aligned}(0+m)+p &= m+p\\ 0+(m+p) &= m+p\\ (s(q)+m)+p &= s(q+m)+p = s((q+m)+p)\\ s(q)+(m+p) &= s(q+(m+p))\end{aligned}$$

L'hypothèse de récurrence nous donne $(q+m)+p = q+(m+p)$. □

THÉORÈME. *L'addition des entiers naturels est commutative, c'est–à–dire que pour tous n et m dans* $\mathbf{N}$*, on a :*

$$n+m = m+n$$

De plus, on a aussi, pour tous n et m de $\mathbf{N}$ *:*

$$\begin{aligned}n+0 &= n\\ s(n) &= n+s(0)\\ s(n+m) &= n+s(m)\end{aligned}$$

(1) Commençons par montrer par récurrence sur n que $n+0=n$. On a bien sûr $0+0=0$. Par ailleurs, pour $n \neq 0$, on a $n+0 = s(p)+0 = s(p+0) = s(p) = n$ par hypothèse de récurrence.

(2) Montrons maintenant que pour tout n, on a $s(n) = n+s(0)$. On le fait par récurrence sur n. On a $s(0) = 0+s(0)$, et

$$\begin{aligned}s(s(p)) &= s(p+s(0)) && \text{par hypothèse de récurrence,}\\ &= s(p)+s(0) && \text{par définition de l'addition.}\end{aligned}$$

(3) Montrons maintenant que pour tous n et m, on a $s(n+m) = n+s(m)$. On le fait par récurrence sur n (qu'on appellera ci–dessous première récurrence).

Cas $n=0$. On a $s(0+m) = s(m) = 0+s(m)$.

Cas $n = s(p)$. On doit montrer que $s(s(p)+m) = s(p)+s(m)$. On le fait par récurrence sur m (qu'on appellera ci-dessous deuxième récurrence). On a $s(s(p)+0) = s(s(p))$ (par (1)) et $s(s(p)) = s(p)+s(0)$ (par (2)). Par ailleurs,

$$\begin{aligned}s(s(p)+s(q)) &= s(s(s(p)+q)) && \text{par hypothèse de la seconde récurrence,}\\ &= s(s(s(p+q))) && \text{par définition de l'addition,}\\ &= s(s(p+s(q))) && \text{par hypothèse de la première récurrence,}\\ &= s(p+s(s(q))) && \text{par hypothèse de la première récurrence,}\\ &= s(p)+s(s(q)) && \text{par définition de l'addition.}\end{aligned}$$

On a donc démontré que $s(n+m) = n+s(m)$ pour tous n et m.

(4) On peut maintenant montrer que $n+m = m+n$, pour tous n et m. On procède par récurrence sur n.

Si $n=0$, on a $0+m = m = m+0$.

Si $n = s(p)$, on a

$$\begin{array}{rcll} s(p)+m & = & s(p+m) & \text{par définition de l'addition,} \\ & = & s(m+p) & \text{par hypothèse de récurrence,} \\ & = & m+s(p) & \text{par (3). } \square \end{array}$$

THÉORÈME. *Tout élément de* $\mathbf{N}$ *est "régulier" pour l'addition, c'est-à-dire que de l'égalité* $n+p = m+p$*, on peut déduire* $n = m$*.*

Par récurrence sur p. De $n+0 = m+0$ on déduit immédiatement $n = m$. Par ailleurs, supposons qu'on ait $n+s(p) = m+s(p)$. Alors on a successivement :

$$\begin{array}{rcll} s(n+p) & = & s(m+p) & \text{par le théorème précédent,} \\ n+p & = & m+p & \text{par le second axiome de Peano,} \\ n & = & m & \text{par hypothèse de récurrence. } \square \end{array}$$

2.2 La multiplication.

On peut de même définir la multiplication $\times$ comme suit :

$$\begin{array}{rcl} 0 \times m & = & 0 \\ s(n) \times m & = & (n \times m) + m \end{array}$$

Désormais, $n \times m$ pourra être noté nm.

THÉORÈME. *Pour tout entier naturel* n*, on a :*

$$0n = 0 = n0$$

L'égalité $0n = 0$ fait partie de la définition de la multiplication. L'autre se montre par récurrence sur n. On a : $00 = 0$, et $s(p)0 = p0 + 0 = 0$. $\square$

THÉORÈME. *La multiplication des entiers naturels est commutative, c'est–à–dire que pour tous* n *et* m *dans* $\mathbf{N}$*, on a :*

$$nm = mn$$

Par récurrence sur n. Pour $n = 0$, on a $0m = 0 = m0$. Pour $n \neq 0$, on doit donc montrer que $s(p)m = ms(p)$. On le fait par récurrence sur m. Le cas $m = 0$ est trivial. Par ailleurs,

$$\begin{array}{rcl} s(p)s(q) & = & ps(q) + s(q) \\ & = & s(q)p + q + 1 \\ & = & pq + p + q + 1 \\ & = & qp + q + p + 1 \\ & = & s(q)p + s(p) \\ & = & s(q)s(p) \end{array}$$

THÉORÈME. *La multiplication est distributive sur l'addition, autrement–dit, on a pour tous* n*,* m *et* p *dans* $\mathbf{N}$ *:*

$$\begin{array}{rcl} n(m+p) & = & nm + np \\ (n+m)p & = & np + mp \end{array}$$

Comme la multiplication est commutative, il suffit de le faire d'un coté. Par récurrence sur n. On a $0(m+p) = 0 = 0+0 = 0m+0p$. Par ailleurs,

$$\begin{aligned} s(q)(m+p) &= q(m+p)+m+p \\ &= qm+qp+m+p \\ &= qm+m+qp+p \\ &= s(q)m+s(q)p \end{aligned}$$

THÉORÈME. *La multiplication des entiers naturels est associative, c'est–à–dire que pour tous nn, m et p dans* $\mathbf{N}$*, on a :*

$$n(mp) = (nm)p$$

Par récurrence sur n. On a $0(mp) = 0 = 0p = (0m)p$. Par ailleurs,

$$\begin{aligned} s(q)(mp) &= q(mp)+mp \\ &= (qm)p+mp \\ &= (qm+m)p \\ &= (s(q)m)p \end{aligned}$$

Exercice. Montrer que si n est distinct de 0, de $nm = np$, on peut déduire $m = p$.

2.3 Puissances.

On définit l'élévation à une puissance comme suit.

DÉFINITION. *Soient n et m deux entiers. On définit l'application $p : \mathbf{N}\times\mathbf{N} \longrightarrow \mathbf{N}$ par récursion primitive :*

$$\begin{aligned} p(0,m) &= 1 \\ p(s(n),m) &= p(n,m)m \end{aligned}$$

On pose $m^n = p(n,m)$ (notez l'interversion de l'ordre des lettres).

On a donc $n^0 = 1$ pour tout n.

Exercice : Démontrer que pout tous n, m et p entiers, on a :

$$\begin{aligned} n^1 &= n \\ (nm)^p &= (n^p)(m^p) \\ n^{m+p} &= n^m n^p \\ (n^m)^p &= n^{mp} \end{aligned}$$

2.4 L'ordre.

À partir de maintenant, nous utiliserons la notation $n+1$ à la place de $s(n)$.

DÉFINITION. *Soient x et y deux éléments de* $\mathbf{N}$*, l'énoncé :*

$$x \leq y$$

est une abbréviation pour :

$$\exists_{z\in\mathbf{N}}\ y = x + z.$$

THÉORÈME. *$\leq$ est une relation d'ordre total sur* $\mathbf{N}$.

Elle est réflexive, puisque $x = x + 0$.

Elle est transitive. En effet, supposons $x \leq y$ et $y \leq z$. On a des entiers u et v tels que $y = x + u$ et $z = y + v$. On a donc $z = x + u + v$, c'est–à–dire $x \leq z$.

Elle est antisymétrique. En effet, supposons que $x \leq y$ et que $y \leq x$. On a des entiers u et v tels que $y = x + u$ et $x = y + v$. On a donc $y = y + v + u$, c'est–à–dire $0 = u + v$. Par définition de l'addition, et par le second axiome de Peano, $u + v = 0$ ne peut arriver que si u et v sont 0. Il en résulte que $x = y$.

Remarquons que pour tout n, on a $n \leq s(n)$, puisque $s(n) = n + 1$.

Pour voir que la relation est totale, il faut montrer que si x et y sont des entiers quelconques, on a $x \leq y$ ou $y \leq x$. On le fait par récurrence sur x. Si $x = 0$ on a $x \leq y$, car alors $y = 0+y = x+y$. Supposons maintenant que $x = s(p)$. On procède par récurrence sur y. Si $y = 0$, on a $y \leq x$ comme ci-dessus. Sinon, on a $y = s(q)$. On a alors par hypothèse de la première récurrence, soit $p \leq q$ soit $q \leq p$, c'est–à–dire soit $q = p + u$, soit $p = q + v$. Dans le premier cas, on a $y = q + 1 = p + u + 1 = p + 1 + u = x + u$, donc $x \leq y$. On traite de même l'autre cas. □

Exercice. Montrer que pour tous n, m et p de $\mathbf{N}$, on a :

$$\begin{array}{rcl} & & 0 \leq n \\ & & n \leq n + m \\ & & m \leq n + m \\ n \leq m & \Rightarrow & n + p \leq m + p \\ n \leq m & \Rightarrow & np \leq mp \\ n \neq 0 \wedge nm \leq np & \Rightarrow & m \leq p \\ n \neq 0 \wedge m \leq p & \Rightarrow & nm \leq np \end{array}$$

Notez que si on a $x \leq y$, alors z tel que $y = x + z$ est unique, car x est régulier pour l'addition. Dans ce cas on peut donc parler de la "différence" $y - x$, qui est égale à ce z.

On note $x < y$ la relation $(x \leq y) \wedge (x \neq y)$.

THÉORÈME. *Tout partie non vide de* $\mathbf{N}$ *a un plus petit élément (autrement–dit,* $\mathbf{N}$ *est "bien ordonné").*

Soit A une partie non vide de $\mathbf{N}$. Soit l'énoncé (dépendant d'un n de $\mathbf{N}$) :

$$\forall_{n\in\mathbf{N}}\ (n \in A \Rightarrow A \text{ a un plus petit élément})$$

Nous allons démontrer cet énoncé par récurrence sur n.

Si $n = 0$, alors $0 \in A$, et 0 est le plus petit élément de A.

Supposons maintenant que $n = s(m)$. Posons $B = s^{-1}(A)$, c'est–à–dire que B est l'image réciproque de A par la fonction successeur s. Comme $n \in A$, on a $m \in s^{-1}(A)$. Donc par hypothèse de récurrence, $s^{-1}(A)$ a un plus petit élément β, c'est–à–dire qu'on a $\beta \leq x$, pour tout x de $s^{-1}(A)$. Autrement–dit, on a $s(\beta) \leq s(x)$, pour tout x tel que $s(x) \in A$. Définissons $\alpha \in A$ par :

$$\begin{array}{rcll} \alpha & = & 0 & \text{si } 0 \in A, \\ \alpha & = & s(\beta) & \text{sinon.} \end{array}$$

Alors, α est le plus petit élément de A. En effet, c'est clair si $\alpha = 0$. Sinon, $\alpha = s(\beta)$, et tous les éléments de A sont de la forme $s(x)$, donc minorés par α.

Si maintenant A est une partie non vide de $\mathbf{N}$, on a un $n \in A$, donc en particularisant ce qui vient d'être prouvé à cet n, on voit que A a un plus petit élément. □

2.5 La division euclidienne.

THÉORÈME. *Pour tout $n \in \mathbf{N}$, et tout $d \in \mathbf{N}$, tel que $d \neq 0$, il existe une unique paire (q, r) dans $\mathbf{N} \times \mathbf{N}$, telle que :*

$$\begin{aligned} n &= dq + r \\ r &< d \end{aligned}$$

q s'appelle le "quotient" et r s'appelle le "reste" de la "division euclidienne de n par d".

Démonstration. L'existence se démontre par récurrence sur n. Dans le cas $n = 0$, il suffit de prendre $(q, r) = (0, 0)$.

Si maintenant $n = p + 1$, on a par hypothèse de récurrence une paire (q_1, r_1), telle que :

$$\begin{aligned} p &= dq_1 + r_1 \\ r_1 &< d \end{aligned}$$

Il y a deux cas.

Si $r_1 + 1 < d$, on a $n = dq_1 + (r_1 + 1)$, et on peut donc prendre $(q, r) = (q_1, r_1 + 1)$. On a bien $r_1 + 1 < d$.

Si au contraire $r_1 + 1 = d$, on a $n = dq_1 + r_1 + 1 = d(q_1 + 1) + 0$, et on peut prendre $(q, r) = (q_1 + 1, 0)$. On a bien $0 < d$, puisque d n'est pas nul.

Démontrons maintenant l'unicité de la division euclidienne. Supposons donc que :

$$dq_1 + r_1 = dq_2 + r_2$$

Si $q_1 = q_2$, on déduit aussitôt $r_1 = r_2$ et l'unicité est démontrée. On peut supposer par exemple $q_1 \leq q_2$. On a alors :

$$r_1 = d(q_2 - q_1) + r_2$$

et donc $d(q_2 - q_1) \leq r_1$. Comme $r_1 < d$, on doit nécessairement avoir $q_2 - q_1 = 0$. □

2.6 Bases de numération.

THÉORÈME. *Donnons-nous un entier d non nul (c'est–à–dire que $d \neq 0$) et un entier k. Alors tout entier n tel que $n < d^{k+1}$ s'écrit de manière unique sous la forme :*

$$n = a_0 + a_1 d + a_2 d^2 + \ldots + a_k d^k$$

où pour tout i, on a $a_i < d$.

Par récurrence qur k. Si $k = 0$, la condition est $n < d^1 = d$. On a alors $n = a_0$, et un tel a_0 est bien sûr unique.

Si $k = s(l)$, on a des entiers q et r, tels que :

$$\begin{aligned} n &= dq + r \\ r &< d \end{aligned}$$

Comme $n < d^{k+1}$, on a $dq + r \leq dd^k$, donc $dq \leq dd^k$, donc $q \leq d^k$. Par hypothèse de récurrence, on a :

$$q = b_0 + b_1 d + b_2 d^2 + \ldots + b_l d^l$$

donc :

$$n = r + b_0 d + b_1 d^2 + b_2 d^3 + \ldots + b_k d^k$$

L'unicité est laissée au lecteur. □

3 Ensembles finis et cardinaux.

Les démonstrations concernant les ensembles finis sont assez troublantes, car tout ce qu'on affirme est tellement évident intuitivement qu'on peut se demander ce qu'il y a à démontrer, ou même s'il y a quelquechose à démontrer. Le formalisme développé jusqu'ici est utile pour comprendre ce qu'il est nécessaire de démontrer.

Afin d'éviter qu'on ne se fie trop facilement à son intuition concernant le sens de l'adjectif "fini", nous allons employer (concernant les ensembles) l'adjectif "numérotable" (à ne pas confondre avec "dénombrable") au lieu de "fini".

3.1 Définitions.

DÉFINITION. *Pour tout entier naturel n, on pose :*

$$[n] = \{x \in \mathbf{N} \mid x < n\}.$$

Par exemple, $[0]$ est vide, $[1] = \{0\}$, $[2] = \{0, 1\}$, etc...

DÉFINITION. *Un ensemble E est dit "numérotable", s'il existe un entier naturel n et une bijection $f : [n] \longrightarrow E$. La fonction f s'appellera un "numérotage de E", et on dira que E est "numéroté" par f. L'entier n sera appelé le "compte" du numérotage f.*[2]

3.2 Théorème fondamental.

THÉORÈME. *Soit n un entier naturel. Tout partie A de $[n]$ est numérotable. De plus le compte de tout numérotage de A est inférieur ou égal à n, et égal à n si et seulement si $A = [n]$.*

Démonstration. On raisonne par récurrence sur n.

Si $n = 0$, $[n]$ est vide, et donc A est vide. On a donc une bijection entre $[0]$ et A, et les conclusions de l'énoncé sont satisfaites.

Si $n = p + 1$, alors $[n]$ contient l'entier p (qui n'est autre que $n - 1$). On a deux cas.

Premier cas. $p \notin A$. Dans ce cas, A est une partie de $[p]$, et l'hypothèse de récurrence nous dit que A est numérotable, et que le compte de tout numérotage de A est au plus p. Ici, A est une partie stricte de $[n]$, et le compte en question étant inférieur à p est strictement inférieur à n. Les conclusions de l'énoncé sont donc satisfaites.

[2] Notez que la raison pour laquelle on ne parle pas de cardinal de E à ce stade est qu'on ne sait pas si tous les numérotages de E ont le même compte.

Deuxième cas. $p \in A$. Posons $B = A \cap [p] = A - \{p\}$. On peut appliquer à B les conclusions du premier cas. B est donc numérotable, par un numérotage $g : B \longrightarrow [k]$, et on a $k \leq p$, quelque soit ce numérotage. De plus, on a $k = p$ si et seulement si $B = [p]$. Définissons une fonction f de A vers $[k+1]$ comme suit :

$$\begin{array}{rcll} f(x) & = & g(x) & \text{si } x \in B \\ f(p) & = & k & \end{array}$$

Il est immédiat que f est une bijection, donc un numérotage de A. Le compte de ce numérotage est $k+1$. Comme $k \leq p$, on a $k+1 \leq n$. Par ailleurs $A = [n]$ si et seulement si $B = [p]$, c'est à dire si et seulement si $p = k$, donc si et seulement si $n = k+1$. □

3.3 Premières conséquences.

THÉORÈME. *Tous les numérotages d'un ensemble numérotable E ont le même compte. Ce compte commun est appelé le "cardinal" de E, et noté* $\mathrm{Card}(E)$.

En effet, supposons que $f : E \longrightarrow [n]$ et $g : E \longrightarrow [m]$ soient deux numérotages de E. Alors, le composé $\varphi = g \circ f^{-1} : [n] \longrightarrow [m]$ est une bijection, c'est–à–dire un numérotage de la partie pleine de $[n]$, de compte m. Le théorème précédent montre alors que $n = m$. □

THÉORÈME. *Si E est numérotable de cardinal n, et si F est en bijection avec E, alors F est numérotable de même cardinal n.* □

Désormais, nous dirons "fini" à la place de "numérotable".

THÉORÈME. *Soit $f : E \longrightarrow F$ une injection où F est un ensemble fini. Alors E est fini et* $\mathrm{Card}(E) \leq \mathrm{Card}(F)$. *De plus, f est bijective si et seulement si E et F ont même cardinal.*

En effet, soit $g : F \longrightarrow [m]$ une bijection ($m = \mathrm{Card}(F)$). L'image A de $g \circ f$ est une partie de $[m]$. A est donc finie et son cardinal n est tel que $n \leq m$. Comme $g \circ f$ est injective, E est en bijection avec A. On a donc $\mathrm{Card}(E) = n \leq m = \mathrm{Card}(F)$. De plus, les énoncés suivants sont équivalents :

f est bijective,
$g \circ f$ est bijective,
$A = [m]$,
$\mathrm{Card}(A) = \mathrm{Card}(F)$,
$\mathrm{Card}(E) = \mathrm{Card}(F)$. □

THÉORÈME. *Si $f : E \longrightarrow F$ est une surjection, et si E est fini, alors F est fini et* $\mathrm{Card}(F) \leq \mathrm{Card}(E)$. *De plus, f est bijective si et seulement si* $\mathrm{Card}(E) = \mathrm{Card}(F)$.

Comme E est fini, on a une bijection $\varphi : [n] \longrightarrow E$. Le composé $\psi = f \circ \varphi : [n] \longrightarrow F$ est alors surjectif. Pour tout $y \in F$, $\psi^{-1}(\{y\})$ est donc une partie non vide de $\mathbf{N}$. Elle a donc un plus petit élément qu'on va noter $\theta(y)$.

On vient donc de définir une fonction $\theta : F \longrightarrow [n]$ qui est une "section" de ψ, c'est–à–dire qu'on a $\psi \circ \theta$ est l'application identique de F.[3] θ est donc une application injective de F vers $[n]$, ce qui démontre que F est fini avec un cardinal au plus égal à n. Bien sûr, les propositions suivantes sont équivalentes :

f est bijective,
ψ est bijective,
θ est bijective,
$n = \mathrm{Card}(F)$. □

[3] Bien qu'on ait évité l'usage de l'axiome du choix ici, cette démonstration reste non constructive, car le théorème affirmant que tout partie non vide de $\mathbf{N}$ a un plus petit élément est elle–même non constructive. On peut remarquer en effet, qu'on y a fait usage du principe du tiers exclu.

3.4 Quelques calculs de cardinaux.

THÉORÈME. *Soient E et F deux ensembles finis. Alors, le produit cartésien $E \times F$ est fini, et on a :*

$$\mathrm{Card}(E \times F) = \mathrm{Card}(E) \times \mathrm{Card}(F).$$

En effet, donnons–nous des numérotages $\varphi : [n] \longrightarrow E$ et $\psi : [m] \longrightarrow F$. Il s'agit de construire un numérotage $f : [nm] \longrightarrow E \times F$. Pour cela, il suffit de construire une bijection $\theta : [n] \times [m] \longrightarrow [nm]$, car le numérotage cherché sera le composé $(\varphi \times \psi) \circ \theta^{-1}$ (où $(\varphi \times \psi)(x, y)$ est défini comme $(\varphi(x), \psi(y))$).

On pose $\theta(x, y) = x + ny$. Il s'agit de vérifier que c'est une bijection. Si $n = 0$, on a aussi $nm = 0$, et les ensembles $[nm]$ et $[n] \times [m]$ sont tous les deux vides et θ est une bijection.

Si $n \neq 0$, soit z un élément de $[nm]$. On a des entiers q et r, tels que $z = nq + r$, et $r < n$. De $z < nm$, on déduit $nq < nm$ et $q < m$. On voit donc que la paire (r, q) est un antécédent de z par θ. La propriété d'unicité de la division euclidienne montre d'ailleurs que c'est l'unique antécédent. θ est donc bijective.

THÉORÈME. *Soient E et F deux ensembles finis. Alors, l'ensemble F^E des applications de E vers F est fini, et on a ;*

$$\mathrm{Card}(F^E) = \mathrm{Card}(F)^{\mathrm{Card}(E)}.$$

Comme précédemment, il suffit de construire une bijection $\theta : [m]^{[n]} \longrightarrow [m^n]$. On pose :

$$\theta(f) = f(0) + mf(1) + m^2 f(2) + \ldots + m^{n-1} f(n-1).$$

La vérification du fait qu'il s'agit bien d'une bijection est laissée au lecteur. □

4 L'axiome des choix dépendants.

Le principe de récursion simple permet de déduire aisément l'axiome des choix dépendants de l'axiome du choix. Rappelons que l'axiome du choix est le suivant (où A et B sont des ensembles quelconques, et $P(x, y)$ un énoncé dépendant de $x \in A$ et de $y \in B$) :

$$(\forall_{x \in A}\ \exists_{y \in B}\ P(x, y)) \Rightarrow (\exists_{f \in B^A}\ \forall_{x \in A}\ P(x, f(x))).$$

L'axiome des choix dépendants est le suivant (où A est un ensemble non vide quelconque, et $P(x, y)$ un énoncé dépendant de $x \in A$ et $y \in A$) :

$$(\forall_{x \in A}\ \exists_{y \in A}\ P(x, y)) \Rightarrow (\exists_{g \in A^{\mathbf{N}}}\ \forall_{n \in \mathbf{N}}\ P(g(n), g(s(n)))).$$

En effet, supposons que $\forall_{x \in A}\ \exists_{y \in A}\ P(x, y)$. L'axiome du choix nous donne une fonction $f : A \longrightarrow A$, telle que $\forall_{x \in A}\ P(x, f(x))$. Comme A est non vide, on a un $a \in A$. Le principe de récursion simple nous donne alors l'application $g : \mathbf{N} \longrightarrow A$ telle que :

$$\begin{array}{rcl} g(0) & = & a, \\ g(s(n)) & = & f(g(n)), \end{array}$$

et on a clairement $\forall_{n \in \mathbf{N}}\ P(g(n), g(s(n)))$.

L'axiome des choix dépendants est très utile en mathématiques élémentaires, par exemple, pour démontrer le théorème de Bolzano–Weierstrass.