Chap 5 :

Construction des ensembles de nombres usuels

1 L'ordinal ω– Construction de $\mathbb{N}$

Nous allons commencer par définir la fonction «Successeur», qui joue un rôle fondamental dans l'arithmétique des ordinaux, et en particulier dans celle de l'ordinal ω.

Définition 1 *:* $S(\alpha) = \alpha \cup \{\alpha\}$

Lemme 1 *:* $\forall\alpha$, *$S(\alpha)$ est un ordinal,* $\alpha < S(\alpha)$ *et* $\forall\beta$ $(\beta < S(\alpha) \Longleftrightarrow \beta \leq \alpha)$

Démonstration : $\rightarrow$ Soit $x \in S(\alpha)$
On a $x \in \alpha$ ou $x = \alpha$
$x \in \alpha \Rightarrow x \subset \alpha$ car α ordinal $\Rightarrow x \subset S(\alpha)$
$x = \alpha \Rightarrow x \subset S(\alpha)$
donc $S(\alpha)$ est transitif.

$\rightarrow$ Soit $A \subset S(\alpha), A \neq \emptyset$
$*$ Si $\alpha \notin A$, alors $A \subset \alpha$, donc A possède un plus petit élément.
$**$ Si $\alpha \in A$, posons $A' = A - \{\alpha\}$
Si $A' = \emptyset$, $A = \{\alpha\}$, donc $\alpha = \min(A)$
Si $A' \neq \emptyset$, soit $x = \min(A')$, on a $x \in \alpha$, donc $x < \alpha \Rightarrow x = \min(A)$
donc $S(\alpha)$ est un ordinal.

$\rightarrow$ $\alpha \notin \alpha$ car sinon $\in$ ne serait plus un ordre total strict sur α.
donc $S(\alpha)$ contient strictement α.
par ailleurs, $\alpha \in S(\alpha)$, donc $\alpha < S(\alpha)$.

$\rightarrow$ $\beta \leq S(\alpha) \Rightarrow \beta \in S(\alpha)$ et $\beta \neq S(\alpha)$
donc $\exists x \in S(\alpha), x \notin \beta$
mais, comme β est un ordinal, si $\alpha \in \beta$, alors $x \in \beta$
donc $\alpha \notin \beta$
donc $\beta \subset \alpha$, i.e. $\beta \leq \alpha$

$\rightarrow$ $\beta \leq \alpha \Rightarrow \beta \in \alpha$ ou $\beta = \alpha$
$*$ $\beta \in \alpha$, comme $\alpha \in S(\alpha)$, alors $\beta \in S(\alpha)$, donc $\beta < S(\alpha)$
$**$ $\beta = \alpha \Rightarrow \beta < S(\alpha)$

Définition 2 *:* α *est un ordinal successeur (ou de* $1^{\text{ère}}$ *espèce) ssi* $\exists\beta$ $(\alpha = S(\beta))$
α *est un ordinal limite (ou de* $2^{\text{ème}}$ *espèce) ssi* $\alpha \neq \emptyset$ *et* α *n'est pas un ordinal successeur.*

Définition 3 *:* $0 = \emptyset$

$1 = S(0)$
$2 = S(1)$
$3 = S(2)$
$4 = S(3)$ *etc.*

On a donc :
$0 = \emptyset$
$1 = \{0\}$
$2 = \{0, 1\}$
$3 = \{0, 1, 2\}$
$4 = \{0, 1, 2, 3\}$ etc.

Définition 4 *:* *α est un entier naturel ssi $\forall \beta \leq \alpha$ ($\beta = 0$ ou β est un ordinal successeur).*

Remarque 1 *:* *Il est clair, d'après la définition, que les entiers naturels forment une section commençante de la «famille» des ordinaux.*

Toutefois, comme les ordinaux ne constituent pas un ensemble, rien ne permet d'affirmer qu'il existe un ensemble de tous les entiers naturels.

On peut pallier cet inconvénient en supposant l'existence d'un ordinal limite α. La famille des ordinaux limites possède alors un plus petit élément ω. Les éléments de ω, qui sont plus petits que le plus petit des ordinaux limites, sont donc tous des entiers naturels.

Traditionnellement, on remplace le postulat d'existence d'un ordinal limite par l'axiome de l'infini, dont voici l'énoncé, mais cela revient au même.

Axiome 7 (Axiome de l'infini) :

$$\exists x\,(0 \in x \wedge (y \in x) \Rightarrow (S(y) \in x))$$

Conséquence : Un tel x contient tous les entiers naturels.

Démonstration : Si n entier et $n \notin x$

Comme $n \neq 0, \exists m$, m entier, $S(m) = n$

$$\left.\begin{array}{l} m < n \\ m \text{ entier} \\ \text{et } m \notin x \text{ [sinon } n = S(m) \in x] \end{array}\right\} \Rightarrow n \setminus x \neq \emptyset$$

Soit n' le plus petit élément de $n \setminus x$
$n' \neq 0$ car $0 \in x$
donc $\exists m'$, m' entier, $S(m') = n'$
On a donc $m' \notin x$, i.e. $m' \in n \setminus x$
Contradiction car $m' < n'$, et n' était le plus petit élément de $n \setminus x$.

Moralité : On a donc (n entier) $\Rightarrow (n \in x)$

D'après le schéma de compréhension, il existe donc un «ensemble de tous les entiers naturels», qui est défini comme un sous-ensemble de x.

$\omega = \{n : n \in x \wedge n \text{ entier}\}$

d'où la définition suivante, qui est maintenant parfaitement justifiée :

Définition 5 *: ω est l'ensemble de tous les entiers naturels.*

Remarque 2 *: ω est un ordinal limite, et c'est le plus petit des ordinaux limites.*

Remarque 3 *: Nous connaissons pour l'instant 2 sortes d'ordinaux :*
$\rightarrow$ *les entiers naturels*
$\rightarrow$ *l'ordinal ω, qui est l'ensemble des entiers naturels.*

Nous aurons l'occasion d'approfondir un peu plus tard l'étude des ordinaux et d'en citer quelques exemples moins triviaux. Mais nos connaissances actuelles vont nous suffire pour réaliser l'objectif que nous nous sommes fixé, à savoir la construction des ensembles de nombres usuels $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Théorème 1 *: L'ensemble ω vérifie les axiomes de Peano :*
(1) $0 \in \omega$
(2) $\forall n \in \omega \ (S(n) \in \omega)$
(3) $\forall n, m \in \omega \ (n \neq m \Rightarrow S(n) \neq S(m))$
(4) $\forall n \in \omega, \ S(n) \neq 0$
(5) $\forall X \subset \omega, \ [((0 \in X) \wedge \forall n \in X \ \ (S(n) \in X)) \Rightarrow X = \omega]$

Démonstration : (1) (2) (3) (4) évident
(5) Si $X \neq \omega$, alors $\omega \setminus X \neq \emptyset$
Soit γ le plus petit élément de $\omega \setminus X$.
Si $n < \gamma$, $n \in X \Rightarrow S(n) \in X \Rightarrow S(n) < \gamma$
donc γ est un ordinal limite, et $\gamma < \omega$, contradiction.

Le théorème précédent prouve que l'ordinal ω que nous avons construit en utilisant les axiomes de la théorie des ensembles vérifie les propriétés que Peano attribuait intuitivement à l'ensemble $\mathbb{N}$.

Rien ne prouve effectivement que l'ordinal ω représente le «bon» ensemble des entiers naturels, au sens naïf du mot. Mais, comme tous les critères de «ressemblance» sont vérifiés, nous prendrons comme postulat le fait que notre arithmétique à nous (dérivée des axiomes 0-1-3-4-5-6-7) coïncide avec ce que les logiciens appellent «l'arithmétique du 1^{er} ordre».

Postulat de base : $\mathbb{N} = \omega$

Dans toute la suite, nous utiliserons indifféremment les lettres $\mathbb{N}$ et ω pour désigner l'ensemble des entiers naturels.

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

Définition 6 *: α entier naturel fixé*
On définit $\alpha + \beta$ par récurrence sur β de la façon suivante :
(1) $\alpha + 0 = \alpha$
(2) $\alpha + S(\beta) = S(\alpha + \beta)$

Exercice 1 *: Calculer* $7 + 4$

$7 + 4 = 7 + S(3) = S(7+3) = S(7 + S(2)) = S(S(7+2)) = S(S(7 + S(1))) = S(S(S(7+1))) = S(S(S(7 + S(0)))) = S(S(S(S(7+0)))) = S(S(S(S(7)))) = S(S(S(8))) = S(S(9)) = S(10) = 11$

Remarque 4 *: Qu'est-ce qu'on est bons!*

Remarque 5 *(**fondamentale**, celle-là) : Il y a une «pseudo-arnaque» dans cette démarche soi-disant axiomatique. Tout le monde aura remarqué que l'assertion n°(5) du dernier théorème du §I n'est rien d'autre que le célèbre «principe de récurrence». Ici, on admet sans que le coup fasse rire qu'il est possible de définir une application de* $\mathbb{N}$ *dans un ensemble quelconque par «récurrence». C'est vrai, mais cela mérite démonstration. L'auteur en est conscient mais n'a pas voulu rentrer dans les détails pour ne pas trop alourdir l'exposé.*

On trouvera l'énoncé exact et la démonstration du «théorème de récursion», soit au Chap 8, soit dansJacobson : Basic Algebra I.

Propriétés de l'addition dans $\mathbb{N}$:

(1) Stabilité de l'ordinal ω : $\forall (n,p) \in \omega^2$, $n+p \in \omega$

Démonstration : Fixons $n \in \omega$, et démontrons la propriété par récurrence sur p
$\rightarrow n+0=0$, donc $n+0 \in \omega$
$\rightarrow n+S(p)=S(n+p)$
Soit $\alpha \leq S(n+p)$
Si $\alpha = S(n+p)$, alors α est un ordinal successeur
Sinon, $\alpha < S(n+p)$, donc $\alpha \leq n+p$
D'après l'HR, $n+p \in \omega$, donc $\alpha = 0$ ou α est un ordinal successeur.

(2) Commutativité : $\forall (n,p) \in \omega^2$, $n+p=p+n$

(3) Associativité : $\forall (n,p,q) \in \omega^3$, $(n+p)+q = n+(p+q)$

(4) Elément neutre : $\exists 0 \in \omega$, $\forall n \in \omega$, $n+0=0+n=n$

(5) Tout élément est régulier : $\forall (n,p,q) \in \omega^3$, $n+p=n+q \Rightarrow p=q$

Conclusion : $(\mathbb{N},+)$ monoïde commutatif à éléments réguliers, ou demi-groupe.

On trouvera des démonstrations de ces propriétés et des propriétés analogues pour la multiplication, par exemple dans :
René Cori, Daniel Lascar : Logique mathématique, Tome 2.
(Attention : aussi trivial que cela puisse paraître, ces démonstrations sont un peu fastidieuses).

3 La multiplication dans $\mathbb{N}$

Définition 7 *:* α *entier naturel fixé*
On définit $\alpha.\beta$ *par récurrence sur* β :
(1) $\alpha.0=0$
(2) $\alpha.S(\beta) = \alpha.\beta + \alpha$

Exemple 1 *:* $3 \times 4 = 3 \times S(3) = 3 \times 3 + 3 = 3 \times S(2) + 3 = 3 \times 2 + 3 + 3 = 3 \times S(1) + 3 + 3 = 3 \times 1 + 3 + 3 + 3 = 3 \times S(0) + 3 + 3 + 3 = 3 \times 0 + 3 + 3 + 3 + 3 = 0 + 3 + 3 + 3 + 3$

... et il reste encore à démontrer successivement que :

$0 + 3 = 3$
$3 + 3 = 6$
$6 + 3 = 9$
$9 + 3 = 12$

Propriétés de la multiplication dans $\mathbb{N}$:

(1) Stabilité de l'ordinal ω :
$\forall (n,p) \in \omega^2,\ n.p \in \omega$
(2) Commutativité : $\forall (n,p) \in \omega^2,\ n.p = p.n$
(3) Associativité : $\forall (n,p,q) \in \omega^3,\ (n.p).q = n.(p.q)$
(4) Distributivité par rapport à l'addition :
$\forall (n,p,q) \in \omega^3,\ n.(p+q) = n.p + n.q$
(5) Elément neutre : $\exists 1 \in \omega,\ \forall n \in \omega,\ 1.n = n.1 = n$
(6) Tout élément non nul est régulier :
$\forall (n,p,q) \in \omega^3,\ (n \neq 0 \wedge n.p = n.q) \Rightarrow (p = q)$

4 Construction de $\mathbb{Z}$

On construit $\mathbb{Z}$ par le procédé de symétrisation d'un demi-groupe.

$\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \mathcal{R}$, où $(a,b)\mathcal{R}(c,d)$ ssi $a + d = b + c$, muni de l'addition des classes :

$Cl\left((a,b)\right) + Cl\left((c,d)\right) = Cl\left((a+c, b+d)\right)$, et les nouvelles notations habituelles.

La multiplication étant définie sur ω (alias $\mathbb{N}$), on la prolonge sur $\mathbb{Z}$ grâce à la règle des signes, et on montre que $(\mathbb{Z}, +, \times)$ anneau commutatif, unitaire et intègre.

5 Construction de $\mathbb{Q}$

On construit $\mathbb{Q}$ comme étant le corps des fractions de l'anneau intègre $\mathbb{Z}$.

$\mathbb{Q} = Frac\mathbb{Z} = \mathbb{Z} \times \mathbb{Z}^* / \sim$

où $(a,b) \sim (c,d)$ ssi $ad = bc$, muni des opérations et de l'ordre habituels.

Remarque 6 ***fondamentale :*** *L'arithmétique du* 1^{er} *ordre (qui n'est qu'un sous-produit de la théorie constituée par les axiomes* $0-1-3-4-5-6-7$ *de ZFC) permet de construire les ensembles* $\mathbb{N}, \mathbb{Z}, \mathbb{D}, \mathbb{Q}$, *et même* $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, ...)$, *bref tout ce qui ne fait intervenir que des constructions dénombrables.*

Pour pouvoir construire $\mathbb{R}$, quelle que soit la méthode envisagée, nous aurons besoin de supposer que l'on peut parler de l'ensemble de tous les sous-ensembles de $\mathbb{Q}$, proposition qui ne peut pas se déduire du reste de la théorie des ensembles.

[Pour s'en convaincre, on démontre (mais c'est d'un niveau d'abstraction largement au-delà de notre propos), que, si la théorie $ZF^- - P$, constituée des axiomes $0-1-3-4-5-6-7$, est consistante, alors il en est de même de cette théorie augmentée du postulat : «Tout est dénombrable», ce qui interdit par exemple à des ensembles comme $\mathbb{R}$ d'exister].

D'où la nécessité de poser un axiome supplémentaire, ce que nous allons faire de suite.

6 L'axiome de l'ensemble des parties

Axiome 8 (Axiome de l'ensemble des parties $\longleftrightarrow$ Power Set) :

$$\forall x \exists y \forall z \ \ (z \subset x \Rightarrow z \in y)$$

Conséquence immédiate : D'après le schéma de compréhension, on peut maintenant parler de l'ensemble des parties de x, qui est défini comme un sous-ensemble de y.

Définition 8 *:* $\mathcal{P}(x) = \{z : z \subset x\}$

7 Construction de $\mathbb{R}$

L'ensemble $\mathcal{P}(\mathbb{Q})$ étant maintenant défini, on pose :
$\mathbb{R} = \{X \in \mathcal{P}(\mathbb{Q}) : X \neq \emptyset \wedge X \neq \mathbb{Q} \wedge \forall x \in X, \forall y \in \mathbb{Q}, (y < x \Rightarrow y \in X) \wedge \forall x \in X, \exists y \in X, x < y\}$
[$\mathbb{R}$ existe d'après le schéma de compréhension].
Le reste fera l'objet du Chap 7.

Remarque 7 ***d'ordre philosophique :*** *Les «purs et durs» parmi les logiciens considèrent cette méthode comme meilleure que les suites de Cauchy car, pour connaître parfaitement un nombre réel, il suffit de connaître l'ensemble des rationnels qui le précèdent, à savoir une famille dénombrable d'objets. En revanche, chez Cauchy, un nombre réel est la donnée de toutes les suites de Cauchy de nombres rationnels, toutes équivalentes entre elles, qui convergent vers ce nombre. Or, il y en a autant que de nombres réels. Le nombre d'objets nécessaires pour définir un nombre réel est donc égal au cardinal de* $\mathbb{R}$ *tout entier...ce qui laisse songeur...*

8 Construction de $\mathbb{C}$

$\mathbb{C} = \mathbb{R} \times \mathbb{R}$, muni des opérations usuelles :
$(a, b) + (c, d) = (a + c, b + d)$
$(a, b) \times (c, d) = (ac - bd, ad + bc)$