LEÇON N° 9 :

Propriétés axiomatiques de $\mathbb{N}$. Construction de $\mathbb{Z}$.

Pré-requis :
– *Notions d'algèbre (injection, relation d'équivalence, classes, groupes, anneaux, morphismes) ;*
– *Relation d'ordre total.*

9.1 Axiomatiques définissant $\mathbb{N}$

9.1.1 De Péano

Il existe un ensemble N non vide, et vérifiant les axiomes suivants :

(i) Il existe une injection $\sigma : N \mapsto N$ appelé *succession* ;

(ii) Il existe un élément de N, noté 0, tel que $0 \notin \sigma(N)$;

(iii) Tout sous-ensemble E de N contenant 0 et stable par σ est égal à N.

Le successeur de 0, $\sigma(0)$, est noté 1. Le successeur $\sigma(1)$ de 1 est noté 2, etc. L'ensemble $N\backslash\{0\}$ sera noté N^*.

Le dernier axiome est appelé *axiome de récurrence*. En effet, soit E un sous-ensemble de N. Dans ce cas,

$$E \text{ stable par } \sigma \quad \Leftrightarrow \quad \sigma(E) \subset E \quad \Leftrightarrow \quad \forall\, n \in E, \sigma(n) \in E \quad \Leftrightarrow \quad \big(n \in E \Rightarrow \sigma(n) \in E\big).$$

L'existence d'un tel ensemble peut être établie par une construction très usuelle dans le cadre de la théorie des ensembles. L'unicité s'obtient en montrant que tous les ensembles vérifiant ces trois axiomes sont isomorphes, ce qui nous permettra d'en choisir un, que nous noterons $\mathbb{N}$ et qui sera appelé *ensemble des entiers naturels*.

9.1.2 Ordinale

Il existe un ensemble N non vide, et vérifiant les axiomes suivants :

(I) N est bien ordonné (N est muni d'une relation d'ordre $\leqslant$ et toute partie non vide de N admet un plus petit élément) ;

(II) N n'est pas majoré ;

(III) Toute partie non vide majorée de N possède un plus grand élément.

L'existence est ici admise, et on montre que deux ensembles vérifiant ces trois axiomes sont isomorphes, ce qui permet également d'en choisir un qui sera également noté $\mathbb{N}$ et appelé *ensemble des entiers naturels*. Nous verrons plus loin que ces deux axiomatiques sont équivalentes, ce qui nous a permis de donner le même nom aux deux ensembles qui en résultent.

Dans la suite, nous supposerons $\mathbb{N}$ construit grâce à l'axiomatique de Péano.

9.1.3 Théorème de récurrence

Théorème 1 : Soit $P(n)$ une proposition dépendant d'un entier naturel n. Si $P(0)$ est vraie et si pour tout $n \in \mathbb{N}$, on a $P(n) \Rightarrow P\big(\sigma(n)\big)$, alors $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

démonstration *: Soit $E = \{n \in \mathbb{N} \mid P(n)$ vraie$\}$. Alors $0 \in E$ est évident. De plus, on a $\Big(P(n) \Rightarrow P\big(\sigma(n)\big)\Big) \Leftrightarrow \big(n \in E \Rightarrow \sigma(n) \in E\big) \Leftrightarrow E$ stable par σ. E vérifie donc l'axiome de récurrence, d'où $E = \mathbb{N}$, et il vient que $P(n)$ est vraie pour tout $n \in \mathbb{N}$.* ■

`Remarque 1` : Inversement, on peut montrer que si un ensemble E vérifie l'axiome de récurrence, il vérifie aussi le théorème de récurrence : en effet, définissons pour tout entier naturel n la proposition $P(n)$ par $P(n)$: n appartient à E. Alors $0 \in E$ implique que $P(0)$ est vraie, et E stable par σ implique que $n \in E \Rightarrow \sigma(n) \in E$, soit $P(n) \Rightarrow P(n+1)$.

9.1.4 Construction de l'addition

Théorème 1 : Il existe une unique application $\varphi : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ telle que

a. pour tout entier p, $\quad \varphi(p, 0) = p$;

b. pour tous entiers p, q, $\quad \varphi\big(p, \sigma(q)\big) = \sigma\big(\varphi(p, q)\big)$.

démonstration *:*

Existence : *Notons P l'ensemble des entiers naturels n tels qu'il existe $\varphi_n : \mathbb{N} \longrightarrow \mathbb{N}$ vérifiant $\varphi_n(0) = n$ et $\varphi_n\big(\sigma(m)\big) = \sigma\big(\varphi_n(m)\big)$ pour tout $m \in \mathbb{N}$. Remarquons déjà que φ_0, l'identité sur $\mathbb{N}$, vérifie les propriétés requises permettant d'affirmer que $0 \in P$.*

Supposons maintenant que $n \in P$ et montrons que $\sigma(n) \in P$. Posons pour tout entier naturel m, $\varphi_{\sigma(n)}(m) = \sigma\big(\varphi_n(m)\big)$. Nous avons d'une part que $\varphi_{\sigma(n)}(0) = \sigma\big(\varphi_n(0)\big) = \sigma(n)$, et d'autre part, pour tout entier m,

$$\varphi_{\sigma(n)}\big(\sigma(m)\big) = \sigma\big(\varphi_n(\sigma(m))\big) \overset{n \in P}{=} \sigma\big(\sigma(\varphi_n(m))\big) = \sigma\big(\varphi_{\sigma(n)}(m)\big).$$

On a donc bien $\sigma(n) \in P$, et on en déduit que $P = \mathbb{N}$ (axiome de récurrence), impliquant l'existence pour tout $n \in \mathbb{N}$ de l'application φ_n, impliquant enfin l'existence de la fonction φ en posant $\varphi(n, m) = \varphi_n(m)$.

Unicité : *Supposons qu'il existe une autre fonction $\psi : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ telle que pour tous $p, q \in \mathbb{N}$, on ait*

$$\psi(p, 0) = p \qquad \text{et} \qquad \psi\big(p, \sigma(q)\big) = \sigma\big(\psi(p, q)\big).$$

Soit $n \in \mathbb{N}$. Posons $P_n = \{m \in \mathbb{N} \mid \varphi(n, m) = \psi(n, m)\}$, et vérifions que $0 \in P_n$: nous remarquons que $\varphi(n, 0) = n = \psi(n, 0)$.

Supposons maintenant qu'un entier m soit dans P_n. Montrons que $\sigma(m) \in P_n$. On a

$$\varphi\big(n, \sigma(m)\big) = \sigma\big(\varphi(n, m)\big) = \sigma\big(\psi(n, m)\big) = \psi\big(n, \sigma(m)\big).$$

Il s'en suit que $P_n = \mathbb{N}$ (axiome de récurrence). Puisque n est arbitraire, nous en déduisons que $\varphi = \psi$.

■

Nous convenons de noter $\varphi(p,q) = p+q$ et d'appeler l'application infixe φ l'*addition des entiers*.

Proposition 1 : L'addition des entiers possède les propriétés suivantes (pour tous $p, q, r \in \mathbb{N}$) :

1. $p + 0 = p$ **et** $\sigma(p) = p + 1$ **;**
2. $(p+q)+r = p+(q+r)$ **: l'addition est *associative* ;**
3. $p + q = q + p$ **: l'adition est *commutative* ;**
4. $p + r = q + r \Rightarrow p = q$ **: l'addition est *régulière* ;**
5. $p + q = 0 \Leftrightarrow p = q = 0$.

démonstration *:*

1. *Il suffit d'introduire la notation fraîchement introduite dans le théorème précédent : pour b., on a :*
$$p+1 = p+\sigma(0) = \varphi\big(p,\sigma(0)\big) = \sigma\big(\varphi(p,0)\big) = \sigma(p).$$

2. *Montrons l'**associativité** par récurrence sur l'entier r. Soient $p, q \in \mathbb{N}$ des entiers quelconques.*
Initialisation : $(p+q)+0 = \varphi(p+q,0) = p+q = p+\varphi(q,0) = p+(q+0)$.
Hérédité : *L'hypothèse de récurrence est : "$(p+q)+r = p+(q+r)$" (équivalente à $\varphi(p+q,r) = \varphi(p,q+r)$). Montrons que $(p+q)+\sigma(r) = p+\big(q+\sigma(r)\big)$. Alors*
$$\begin{array}{rcl}(p+q)+\sigma(r) & = & \varphi\big(p+q,\sigma(r)\big) = \sigma\big(\varphi(p+q,r)\big) \overset{H.R.}{=} \sigma\big(\varphi(p,q+r)\big)\\ & = & \varphi\big(p,\sigma(q+r)\big) = \varphi(p,q+r+1) = p+(q+r+1)\\ & = & p+\big(q+\sigma(r)\big).\end{array}$$

3. *Montrons la **commutativité** par récurrence sur l'entier q. Soit $p \in \mathbb{N}$ un entier quelconque.*
Initialisation : *On sait déjà que $p+0 = p$. Montrons alors que $0+p = p$ par récurrence sur p. Lorsque $p = 0$, on a $0+0 = 0$ (d'après a.). En supposant que $0+p = p$, on a*
$$0+(p+1) = (0+p)+1 \overset{H.R.}{=} p+1.$$
La récurrence s'achève ici, et on en déduit que $p+0 = 0+p$. Bien que l'initialisation soit montrée, montrons que cette égalité est aussi vraie au rang 1 :
On sait déjà que $p+1 = \varphi(p,1) = \varphi\big(p,\sigma(0)\big) = \sigma\big(\varphi(p,0)\big) = \sigma(p)$. Montrons alors par récurrence sur p que $1+p = \sigma(p)$. Pour $p = 0$, on a $1+0 = \varphi(1,0) = 1 = \sigma(0)$. Lorsqu'on suppose que l'égalité $1+p = \sigma(p)$ est vraie, on a
$$1+(p+1) = (1+p)+1 \overset{H.R.}{=} \sigma(p)+1 = (p+1)+1 = \sigma(p+1).$$
La récurrence s'achève, prouvant que $p+1 = 1+p$.

Hérédité : *L'hypothèse de récurrence est : "$p+q = q+p$" (rappelons que p est un entier quelconque). Montrons que $p+\sigma(q) = \sigma(q)+p$. Alors*
$$\begin{array}{rcl}p+\sigma(q) & = & p+(q+1) = p+(1+q) = (p+1)+q \overset{H.R.}{=} q+(p+1)\\ & = & q+(1+p) = (q+1)+p = \sigma(q)+p.\end{array}$$

4. *Montrons la **régularité** par récurrence sur l'entier r. Soient $p, q \in \mathbb{N}$ deux entiers quelconques.*
Initialisation : *Puisque $p+0 = p$ et $q+0 = q$, on a directement que $p+0 = q+0 \Rightarrow p = q$.*

Hérédité : *L'hypothèse de récurrence est : "$p+r=q+r \Rightarrow p=q$". Montrons que $p+\sigma(r)=q+\sigma(r) \Rightarrow p=q$. Alors*

$$\begin{aligned} p+\sigma(r)=q+\sigma(r) &\Leftrightarrow p+(r+1)=q+(r+1) \Leftrightarrow p+(1+r)=q+(1+r) \\ &\Leftrightarrow (p+1)+r=(q+1)+r \overset{H.R.}{\Leftrightarrow} p+1=q+1 \\ &\Leftrightarrow \sigma(p)=\sigma(q) \Rightarrow p=q \qquad \textit{(car } \sigma \textit{ est injective).} \end{aligned}$$

5. *Le sens indirect est trivial. Montrons alors le sens direct par contraposée : supposons que l'un des entiers ne soit pas nul, par exemple q (cela implique qu'il existe $q' \in \mathbb{N}$ tel que $q=\sigma(q')$), et montrons que dans ce cas, $p+q \neq 0$. Puisque $q \neq 0$,*

$$p+q=\varphi(p,q)=\varphi\big(p,\sigma(q')\big)=\sigma\big(\varphi(p,q')\big).$$

On constate que $p+q$ est le successeur d'un entier naturel, donc $p+q$ ne peut pas être nul.

■

9.1.5 Construction de la multiplication

Nous utilisons l'addition que nous venons de définir afin d'énoncer le théorème suivant :

Théorème 2 : Il existe une unique application $\pi : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$ telle que :

a. Pour tout entier p, $\quad \pi(p,0)=0 \quad$ (0 est dit *élément absorbant*) ;

b. Pour tous entiers p, q, $\quad \pi\big(p,\sigma(q)\big)=\pi(p,q)+p$.

démonstration :

Existence : *Posons Q l'ensemble des entiers naturels n tel qu'il existe $\pi_n : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$ vérifiant $\pi_n(0)=0$ et $\pi_n\big(\sigma(p)\big)=\pi_n(p)+n$ pour tout $p \in \mathbb{N}$. On remarque que la fonction π_0 définie par $\pi_0(m)=0$ (pour tout entier m) possède les propriétés requises, permettant d'affirmer que $0 \in Q$. Supposons alors que $n \in Q$ et montrons que $\sigma(n) \in Q$. Posons*

$$\pi_{\sigma(n)}(m)=\pi_n(m)+m.$$

Nous avons d'une part que $\pi_{\sigma(n)}(0)=\pi_n(0)+0=0$, et d'autre part

$$\pi_{\sigma(n)}\big(\sigma(m)\big)=\pi_n\big(\sigma(m)\big)+\sigma(m) \overset{n\in Q}{=} \pi_n(m)+n+\sigma(m)=\pi_{\sigma(n)}(m)+\sigma(n).$$

D'où $Q=\mathbb{N}$, et l'application π_n existe pour tout entier naturel n. Nous définissons alors $\pi : \mathbb{N} \longrightarrow \mathbb{N}$ par $\pi(n,m)=\pi_n(m)$. Il est clair, d'après ce qui précède, que π possède les propriétés a. et b.

Unicité : *Supposons qu'il existe une autre fonction $\theta : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$ telle que pour tous $p, q \in \mathbb{N}$,*

$$\theta(p,0)=0 \qquad \textit{et} \qquad \theta\big(p,\sigma(q)\big)=\theta(p,q)+p.$$

Prenons un entier n et posons $Q_n=\{m \in \mathbb{N} \mid \theta(n,m)=\pi(n,m)\}$. Il est facile de vérifier par récurrence (sur m) que $Q_n=\mathbb{N}$ car $0 \in Q_n$ et le successeur de tout élément de Q_n est dans Q_n :

$$\pi\big(n,\sigma(m)\big)=\pi(n,m)+n=\theta(n,m)+n=\theta\big(n,\sigma(m)\big).$$

D'où $\theta=\pi$.

■

Nous convenons alors de noter $\pi(p,q) = p \times q$ (ou encore $p \cdot q$ ou simplement pq), et d'appeler π la *multiplication* des entiers naturels.

Proposition 2 : La multiplication des entiers possède les propriétés suivantes (pour tous $p, q, r \in \mathbb{N}$) :

1. $p \cdot 0 = 0$ **et** $p \cdot 1 = p$ **;**
2. $p \cdot q = 0 \Leftrightarrow p = 0$ **ou** $q = 0$ **;**
3. $p \cdot (q + r) = p \cdot q + p \cdot r$ **: la multiplication est *distributive* par rapport à l'addition ;**
4. $p \cdot q = q \cdot p$ **: la multiplication est *commutative* ;**
5. $(p \cdot q) \cdot r = p \cdot (q \cdot r)$ **: la multiplication est *associative* ;**
6. $\forall\, r \in \mathbb{N}^*, p \cdot r = q \cdot r \Rightarrow p = q$ **: la multiplication est *régulière*.**

démonstration *:*

1. *Découlent de la démonstration précédente.*
2. *D'après 1., le sens indirect est trivial. Montrons alors le sens direct. Pour cela, nous supposons l'équivalence entre les axiomatiques démontrée, ce qui nous permet d'utiliser la relation d'ordre de $\mathbb{N}$. Supposons $q \neq 0$. Alors $q \geqslant 1$, donc il existe $s \in \mathbb{N}$ tel que $q = 1 + s$. Dans ce cas, $pq = p(1+s) = p + ps$. Or $ps \in \mathbb{N}$, donc $ps \geqslant 0 \Rightarrow pq \geqslant p$, et $p \geqslant 1$. D'où $pq \neq 0$, ce qui est absurde.*

3. *Montrons la **distributivité** par récurrence sur l'entier r. Soient $p, q \in \mathbb{N}$ des entiers quelconques.*

   Initialisation : *Lorsque $r = 0$, on a $p(q+0) = pq \overset{1.}{=} pq + p \cdot 0$, d'où l'égalité.*

   Hérédité : *Supposons que $p(q+r) = pq + pr$ et montrons que $p\big(q + \sigma(r)\big) = pq + p\sigma(r)$:*

$$\begin{aligned} p\big(q+\sigma(r)\big) &= p\big(q+(r+1)\big) = p\big((q+r)+1\big) && \text{(d'après 2. de prop. 1)} \\ &= p\sigma(q+r) \overset{\text{déf.}}{=} p(q+r) + p \overset{\text{H.R.}}{=} (pq+pr)+p \\ &= pq + (pr+p) = pq + (pr + p\cdot 1) \overset{\text{H.R.}}{=} pq + p(r+1). \end{aligned}$$

4. *Avant de montrer la **commutativité**, montrons par récurrence sur un entier b que pour tout $a \in \mathbb{N}$, on a $ab + b = (a+1)b$.*

   Initialisation : *Lorsque $b = 0$, on a $a \cdot 0 + 0 = 0$ et $(a+1) \cdot 0 = 0$, d'où l'égalité.*

   Hérédité : *L'hypothèse de récurrence est : "$ab + b = (a+1)b$". Montrons alors que $a\sigma(b) + \sigma(b) = (a+1)\sigma(b)$:*

$$\begin{aligned} a\sigma(b) + \sigma(b) &= a(b+1) + (b+1) \overset{2.}{=} (ab+a) + (b+1) = ab + b + a + 1 \\ &\overset{\text{H.R.}}{=} (a+1)b + (a+1) \overset{2.}{=} (a+1)(b+1) = (a+1)\sigma(b). \end{aligned}$$

   Nous noterons cette propriété ($\flat$). On souhaite maintenant montrer la commutativité par récurrence sur l'entier p. Soit q un entier quelconque.

   Initialisation : *On sait déjà que $q \cdot 0 = 0$. Montrons alors que $0 \cdot q = 0$ par récurrence sur q. Lorsque $q = 0$, on a $0 \cdot 0 = 0$ (d'après 1.). En supposant ensuite que $0 \cdot q = 0$, on a*

$$0 \cdot \sigma(q) = \pi\big(0, \sigma(q)\big) = \pi(0,q) + 0 \overset{\text{H.R.}}{=} 0 + 0 = 0.$$

   La récurrence s'achève ici, et on en déduit que $0 \cdot q = q \cdot 0 = 0$.

Hérédité : *L'hypothèse de récurrence est : "$pq = qp$". Montrons alors que $\sigma(p)q = q\sigma(p)$:*

$$q\sigma(p) = q(p+1) = qp + q \overset{H.R.}{=} pq + q \overset{(\flat)}{=} (p+1)q = \sigma(p)q.$$

5. *Montrons l'**associativité** par récurrence sur l'entier p. Soient $q, r \in \mathbb{N}$ des entiers quelconques.*

   Initialisation : *D'après 1, on a que $(0 \cdot q)r = 0 \cdot r = 0$ et $0 \cdot (qr) = 0$, d'où le résultat.*

   Hérédité : *L'hypothèse de récurrence est : "$(pq)r = p(qr)$" (équivalente à $\pi(pq, r) = \pi(p, qr)$). Montrons que $\big(\sigma(p)q\big)r = \sigma(p)(qr)$. Alors*

$$\begin{aligned} \big(\sigma(p)q\big)r &= \big(q\sigma(p)\big)r = (qp+q)r \\ &= r(qp+q) = rqp + rq = qrp + qr = (qr)\sigma(p) \\ &= \sigma(p)(qr). \end{aligned}$$

6. *A nouveau, nous utiliserons la relation d'ordre sur $\mathbb{N}$. Quitte à inverser les rôles de p et q, on peut supposer que $p \geqslant q$, impliquant l'existence d'un entier naturel s tel que $p = q + s$. Alors $pr = qr = (q+s)r = qr + sr$. Par régularité de l'addition, ceci implique que $sr = 0$, donc (d'après 2.) que $r = 0$ ou $s = 0$. Or $r \in \mathbb{N}^*$, donc il vient que $s = 0$, soit $p = q$.*

■

9.1.6 Équivalence entre les axiomatiques

Pour pouvoir appeler deux ensembles définis de manière différente avec le même nom, il faut au préalable prouver que ces deux axiomatiques sont équivalentes.

Montrons déjà que l'axiomatique de Péano implique l'axiomatique ordinale.

démonstration :

Montrons que $(\mathbb{N}, \leqslant)$ est un ensemble bien ordonné : *Définissons tout d'abord la relation $\leqslant$:*

$$\forall\, p, q \in \mathbb{N}, \quad q \leqslant p \Leftrightarrow \exists\, r \in \mathbb{N} \mid p = q + r.$$

- *$r = 0$ donne la réflexivité de la relation.*
- *Soient $p, q \in \mathbb{N}$. Supposons que $p \leqslant q$ et $q \leqslant p$. Alors il existe $r, r' \in \mathbb{N}$ tels que $q = p + r$ et $p = q + r'$. Dans ce cas, $q = (q + r' + r)$, et par régularité de l'addition, $r + r' = 0$. La proposition 1 permet de conclure que $r = r' = 0$, c'est-à-dire $p = q$. la relation $\leqslant$ est donc antisymétrique.*
- *Soient $a, b, c \in \mathbb{N}$. Alors $a \leqslant b$ et $b \leqslant c$ impliquent l'existence de $r, r' \in \mathbb{N}$ tels que $b = a + r$ et $c = b + r'$. D'où $c = (a + r) + r' = a + (r + r')$. En posant $r'' = r + r' \in \mathbb{N}$, on trouve bien $a \leqslant c$, ce qui rend la relation $\leqslant$ transitive.*

Dans tous les cas, on aura toujours $p = q + r$, ou alors $q = p + r$ si la précédente égalité est impossible, car les deux membres sont des éléments égaux de $\mathbb{N}$. Cela rend la relation totale.

On peut alors définir pour tous $p, q \in \mathbb{N}$:

$$p < q \Leftrightarrow p + 1 \leqslant q.$$

Montrons que toute partie non vide de $\mathbb{N}$ admet un plus petit élément. Pour toute partie $E \subset \mathbb{N}$ non vide, on note M l'ensemble des minorants de E. M est non vide puisqu'il contient nécessairement 0. De plus, il existe $p \in M$ tel que $p + 1 \notin M$ (en effet, (III) entraînerait que $M = \mathbb{N}$ et donc

$E = \varnothing$). Supposons alors que $p \notin E$: dans ce cas, pour tout $n \in E$, l'inégalité $p < n$ implique $p + 1 \leqslant n$ et $p + 1$ sera un minorant de E, ce qui est absurde. D'où $p \in E$, et on en déduit que p est le plus petit élément de E.

Montrons que $\mathbb{N}$ n'est pas majoré : *Si μ était un majorant de $\mathbb{N}$, on aurait que $\mu + 1 \leqslant \mu$. Mais puisque $\mu \leqslant \mu + 1$, on aurait $\mu = \mu + 1$, soit $0 = 1$ par régularité de l'addition. Ceci est absurde.*

Montrons que toute partie non vide majorée de N possède un plus grand élément : *Soient $F \subset \mathbb{N}$ une partie non vide et majorée, et $\mathscr{M}$ l'ensemble des majorants de F. $\mathscr{M}$ n'est pas vide donc possède un plus petit élément m. Nécéssairement, $m \in F$ (procéder par l'absurde en utilisant le prédécesseur de m) et m est le plus grand élément de F.*

■

Montrons maintenant que l'axiomatique ordinale implique l'axiomatique de Péano.

démonstration :

Montrons qu'il existe une injection $\sigma : \mathbb{N} \longrightarrow \mathbb{N}$: *Soit $\sigma : \mathbb{N} \longrightarrow \mathbb{N}$ définie par $\sigma(n) = n + 1$. Alors pour tous $n, m \in \mathbb{N}$,*

$$\sigma(n) = \sigma(m) \quad \Leftrightarrow \quad n + 1 = m + 1 \quad \Leftrightarrow \quad n = m.$$

σ est donc injective.

Montrons que $0 \notin \sigma(\mathbb{N})$: *Supposons que $0 \in \sigma(\mathbb{N})$. Alors il existe un entier n tel que $n + 1 = 0$. D'après la proposition 1, on a donc $n = 1 = 0$, en particulier $1 = 0$, ce qui est absurde.*

Montrons l'axiome de récurrence : *Soit $E \in \mathbb{N}$. Supposons (par l'absurde) que $E \neq \mathbb{N}$. Dans ce cas, le complémentaire de E dans $\mathbb{N}$ n'est pas vide, donc possède un plus petit élément que nous noterons m. Puisque $0 \in E$ par hypothèse, $m \neq 0$ donc admet un prédécesseur n (tel que $n + 1 = m$) qui appartient à E. Mais l'hypothèse implique que $n + 1 = m \in E$, ce qui est absurde, donc $E = \mathbb{N}$, et l'axiome de récurrence est démontré.*

■

9.2 Construction de $\mathbb{Z}$

Nous venons de voir la "construction" de $\mathbb{N}$ et de ses lois. Par contre, étant donnés $p, q \in \mathbb{N}$, la question de savoir s'il existe un entier naturel r tel que $p = q + r$ ne trouve de solution que lorsque $p \geqslant q$. Nous allons donc construire un ensemble contenant $\mathbb{N}$ tel que l'équation $p = q + r$ trouve toujours une solution.

9.2.1 Construction

On note $\mathbb{N} \times \mathbb{N}$ l'ensemble des couples d'entiers naturels. Dans cet ensemble de couples, on a trivialement que $(a, b) = (a', b') \Leftrightarrow a = a'$ et $b = b'$. On définit alors une relation (d'équivalence - facile à montrer) R entre couple d'entiers par

$$(a, b)\ R\ (a', b') \quad \Leftrightarrow \quad a + b' = a' + b.$$

Les classes d'équivalence de $\mathbb{N} \times \mathbb{N}$ pour la relation d'équivalence R forment un ensemble noté $\mathbb{Z}$ et appelé *ensemble des entiers relatifs*. On peut donc écrire que :

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/R = \left\{ \overline{(a, b)}, a, b \in \mathbb{N} \right\}.$$

9.2.2 Addition dans $\mathbb{Z}$

Soient $x, y \in \mathbb{Z}$. Choisissons $(p,q),(p',q')$ deux représentants de x et $(r,s),(r',s')$ deux représentants de y. On remarque que

$$(p+r, q+s)\ R\ (p'+r', q'+s'),$$

ce qui implique que $(p+r, q+s)$ et $(p'+r', q'+s')$ déterminent la même classe dans $\mathbb{Z}$. On peut donc définir l'opération notée provisoirement $\oplus$:

$$\forall\ a, a', b, b' \in \mathbb{N}, \quad \overline{(a,b)} \oplus \overline{(a',b')} = \overline{(a+a', b+b')}.$$

Théorème 2 : $(\mathbb{Z}, \oplus)$ est un groupe commutatif.

démonstration *:*

Associativité : *Elle est assurée par celle de la loi $+$ dans $\mathbb{N}$. En effet, on a*

$$\big(\overline{(a,b)} \oplus \overline{(a',b')}\big) \oplus \overline{(a'',b'')} = \overline{(a+a', b+b')} \oplus \overline{(a'',b'')} = \overline{(a+a'+a'', b+b'+b'')},$$

et

$$\overline{(a,b)} \oplus \big(\overline{(a',b')} \oplus \overline{(a'',b'')}\big) = \overline{(a,b)} \oplus \overline{(a'+a'', b'+b'')} = \overline{(a+a'+a'', b+b'+b'')},$$

d'où l'égalité $\big(\overline{(a,b)} \oplus \overline{(a',b')}\big) \oplus \overline{(a'',b'')} = \overline{(a,b)} \oplus \big(\overline{(a',b')} \oplus \overline{(a'',b'')}\big)$.

Elément neutre : *Remarquons que pour tout $\overline{(a,b)} \in \mathbb{Z}$, $\overline{(a,b)} \oplus \overline{(0,0)} = \overline{(a+0, b+0)} = \overline{(a,b)}$. De même, on montre que $\overline{(0,0)} \oplus \overline{(a,b)} = \overline{(a,b)}$, donc $\overline{(0,0)}$ est bien l'élément neutre recherché.*

Symétrique : *Pour tout $\overline{(a,b)} \in \mathbb{Z}$, il existe $\overline{(b,a)} \in \mathbb{Z}$ tel que*

$$\overline{(a,b)} \oplus \overline{(b,a)} = \overline{(a+b, a+b)} = \overline{(0,0)}.$$

Commutativité : *La commutativité est assurée par celle de la loi $+$ dans $\mathbb{N}$.*

■

On note $-\overline{(a,b)} \in \mathbb{Z}$ l'opposé de l'élément $\overline{(a,b)} \in \mathbb{Z}$, de sorte que $-\overline{(a,b)} = \overline{(b,a)}$.

Proposition 3 : L'application $f : \mathbb{N} \longrightarrow \mathbb{Z}$ définie par $f(a) = \overline{(a,0)}$ est un homomorphisme injectif de monoïdes.

démonstration *: En effet, pour tous $a, b \in \mathbb{N}$,*

$$f(a+b) = \overline{(a+b, 0)} = \overline{(a,0)} \oplus \overline{(b,0)} = f(a) \oplus f(b).$$

Par ailleurs, cette application est clairement injective, puisque demander que les classes de $(a,0)$ et $(b,0)$ soient égales revient justement à demander que $a = b$. ■

L'application f est un plongement de $\mathbb{N}$ dans $\mathbb{Z}$ qui permet d'identifier $\mathbb{N}$ et $f(\mathbb{N})$ en écrivant $a = \overline{(a,0)}$ pour tout $a \in \mathbb{N}$. Avec cette identification, l'ensemble $\mathbb{N}$ devient une partie de $\mathbb{Z}$. L'opposé de $a \in \mathbb{N}$ dans $\mathbb{Z}$ est $\overline{(0,a)} = -\overline{(a,0)}$, ce que l'on écrit $-a$.

De plus, la démonstration précédente nous informe que f généralise l'addition dans $\mathbb{N}$, nous permettant désormais d'écrire $+$ à la place de $\oplus$.

Théorème 3 : Soit $-\mathbb{N}$ la partie de $\mathbb{Z}$ formée des opposés des éléments de $\mathbb{N}$. Alors

1. $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$;
2. $\mathbb{N} \cap (-\mathbb{N}) = \{0\}$;
3. **Si $a \geqslant b$, l'unique entier naturel (noté $a - b$) solution de l'équation $b + x = a$ coïncide avec la somme $a + (-b)$ de a et de l'opposé $(-b)$ de b.**

démonstration :

3. $b + \big(a + (-b)\big) = a \Rightarrow a + (-b) = a - b$ *quand* $a \geqslant b$.

1. *Pour tout* $\overline{(a,b)} \in \mathbb{Z}$, *on a :*

$$\overline{(a,b)} = \overline{(a-b,0)} = \begin{cases} \overline{(a-b,0)} = a - b \in \mathbb{N} & \text{si} \quad a \geqslant b \\ \overline{(0,b-a)} = -(b-a) \in -\mathbb{N} & \text{si} \quad a \leqslant b. \end{cases}$$

2. *Pour tous* $a, b \in \mathbb{N}$,

$$a = -b \quad \Leftrightarrow \quad \overline{(a,0)} = \overline{(0,b)} \quad \Leftrightarrow \quad a + b = 0 \quad \Leftrightarrow \quad a = b = 0.$$

■

9.2.3 Multiplication dans $\mathbb{Z}$

Soient $\overline{(a,b)} = \overline{(a',b')}$ et $\overline{(c,d)} = \overline{(c',d')}$. Alors

$$\begin{cases} a + b' = b + a' \\ c + d' = c' + d \end{cases} \Rightarrow \begin{cases} (a+b')c' = (b+a')c' \\ (a+b')d' = (b+a')d' \\ a(c+d') = a(d+c') \\ b(c+d') = b(d+c') \end{cases} \Rightarrow \begin{cases} ac' + b'c' = bc' + a'c' \\ bd' + a'd' = ad' + b'd' \\ ac + ad' = ad + ac' \\ bd + bc' = bc + bd'. \end{cases}$$

En additionnant membre à membre, les égalités du dernier système, on trouve :

$$(ac + bd) + (b'c' + a'd') = (bc + ad) + (a'c' + b'd'),$$

c'est-à-dire

$$\overline{(ac + bd, bc + ad)} = \overline{(a'c' + b'd', b'c' + a'd')},$$

égalité qui nous permet de poser la définition suivante :

$$\forall\, \overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}, \quad \overline{(a,b)} \times \overline{(c,d)} = \overline{(ac + bd, bc + ad)}.$$

Théorème 4 : Cette multiplication est commutative, associative et distributive par rapport à l'addition. L'élément $\overline{(1,0)}$ est l'élément neutre pour cette multiplication. De plus, cette opération généralise la multiplication dans $\mathbb{N}$ puisque tous $a, b \in \mathbb{N}$, on a :

$$f(a) \times f(b) = \overline{(a,0)} \times \overline{(b,0)} = \overline{(ab,0)} = f(ab).$$

démonstration *:*

Commutativité et associativité : *Conséquence de la commutativité et de l'associativité des lois $+$ et $\times$ dans $\mathbb{N}$.*

Ditributive : *Pour tous $x_1, x_2, y_1, y_2, z_2, z_2 \in \mathbb{N}$, on a :*

$$\begin{aligned} & \overline{(x_1,y_1)} \times \overline{(y_1,y_2)+(z_1,z_2)} \\ = \ & \overline{(x_1,x_2)} \times \overline{(y_1+z_1,y_2+z_2)} \\ = \ & \overline{\big(x_1(y_1+z_1)+x_2(y_2+z_2), x_2(y_1+z_1)+x_1(y_2+z_2)\big)}, \end{aligned}$$

et

$$\begin{aligned} & \overline{(x_1,y_1)} \times \overline{(y_1,y_2)} + \overline{(x_1,y_1)} \times \overline{(z_1,z_2)} \\ = \ & \overline{(x_1y_1+x_2y_2, x_2y_1+x_1y_2)} + \overline{(x_1z_1+x_2z_2, x_2z_1+x_1z_2)} \\ = \ & \overline{\big(x_1(y_1+z_1)+x_2(y_2+z_2), x_2(y_1+z_1)+x_1(y_2+z_2)\big)}, \end{aligned}$$

d'où l'égalité.

Élément neutre : *Pour tous $a, b \in \mathbb{N}$, on a*

$$\overline{(a,b)} \times \overline{(1,0)} = \overline{(a\cdot 1, b\cdot 0, b\cdot 1, a\cdot 0)} = \overline{(a,b)}.$$

■

`Remarque 2` : Comme pour l'addition, nous nous sommes permis d'utiliser le même symbole pour la multiplication dans $\mathbb{N}$ et $\mathbb{Z}$ grâce à la généralisation exprimée par ce théorème.

Avec les notations précédemment établies, on peut donner les premières propriétés de la multiplication dans $\mathbb{Z}$: pour tous entiers naturels a et b,

- ◇ $(a,0) \times (b,0) = (ab,0) \quad \Rightarrow \quad a \times b = ab$;
- ◇ $(a,0) \times (0,b) = (0,ab) \quad \Rightarrow \quad a \times (-b) = -(ab)$;
- ◇ $(0,a) \times (0,b) = (ab,0) \quad \Rightarrow \quad (-a) \times (-b) = ab.$

Théorème 5 : $(\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire, et l'application f est un homomorphisme injectif pour les lois $+$ et $\times$.

démonstration *: Conséquence du théorème 3.* ■

9.3 Remarques

L'idée pour la construction de $\mathbb{Z}$ est de partir de l'idée intuitive qu'on en a : trouver un inverse à chaque élément de $\mathbb{N}$! Si l'on veut définir -2 avec des entiers naturels, on a envie de le voir comme $0-2$ ou $3-5$, etc. Les difficultés sont que l'écriture n'est pas unique et que la "soustraction" n'a aucun sens dans $\mathbb{N}$. Pour nous enlever cette difficulté, on va donc considérer qu'une paire d'entiers naturels (a,b) correspondra à l'"entier relatif" $a-b$. Malheureusement, cela n'enlève pas le problème d'unicité, empêchant ainsi le choix de $\mathbb{N}\times\mathbb{N}$ pour l'ensemble $\mathbb{Z}$. On va donc regrouper les paires qui correspondent au même "entier relatif" (par exemple $(0,-2)$ et $(3,5)$).

La relation d'équivalence $(a,b)\ R\ (a',b') \Leftrightarrow a+b'=a'+b$ permet de supprimer cette autre difficulté. On notera qu'intuitivement, cela correspond aussi à $b-a=b'-a'$, traduisant bien qu'il s'agit du même "entier relatif" !

Le morphisme de monoïdes f sert à voir un entier naturel comme cas particulier d'un entier relatif (ce qui est conforme à l'idée qu'on se faisait de $\mathbb{Z}$). Il faut alors vérifier que ce morphisme prolonge bien l'addition et la multiplication de $\mathbb{N}$ à $\mathbb{Z}$, ce qui est facile à faire. Il en découle aussi que les propositions 1 et 2 restent valables pour tous éléments $p,q,r\in\mathbb{Z}$.