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.

I) Axiomatiques définissant $\mathbb{N}$

1) Axiomatiques De Péano

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

(i) Il existe une injection σ: N → 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.

Rem : Ces ensembles s'avèrent être tous isomorphe à $\mathbb{N}$ que l'on appelle ensemble des entiers naturels

Oral :Le successeur de 0, $\sigma(0)$, est noté 1. Le successeur $\sigma(1)$ de 1 est noté 2, etc.

2) Théorème de récurrence

Oral : du 3eme axiome de Péano souvent nommé axiome de récurrence, on tire le théorème suivant

Théorème : 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 $P(n) \Longrightarrow P(\sigma(n))$, alors P(n) est vraie pour tout $n \in \mathbb{N}$.

3) Construction de l'addition

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

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

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

On convient de noter $\varphi\,(p, q) = p + q$ et d'appeler cette application l'*addition des entiers*

Proposition : 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'addition est *commutative* ;
4. $p + r = q + r \Rightarrow p = q$: l'addition est *régulière* ;
5. $p + q = 0 \Leftrightarrow p = q = 0$.

4) Construction de la multiplication

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

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

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

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 : La multiplication des entiers possède les propriétés suivantes (pour tous p, q, r ∈ ℕ) :
1. p x 0 = 0 et p x 1 = p ;
2. p x q = 0 , p = 0 ou q = 0 ;
3. p x (q + r) = p x q + p x r : la multiplication est *distributive* par rapport à l'addition ;
4. p x q = q x p : la multiplication est *commutative* ;
5. (p x q) x r = p x (q x r) : la multiplication est *associative* ;
6.$\forall r \in \mathbb{N}\backslash\{0\}$, p x r = q x r $\Longrightarrow$ p = q : la multiplication est *régulière*.

5) Relation d'ordre sur ℕ

Définition : on définit la relation ≤ par l'équivalence suivante

$$\forall p, q \in \mathbb{N}\,, q \leq p \iff \exists r \in \mathbb{N}\,, p = q + r$$

Théorème : La relation ≤ est une relation d'ordre et $(\mathbb{N}, \leq)$ est un ensemble totalement ordonné.

Propriété : (i) 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.

Oral : ces trois propriétés sont en fait les 3 axiomes de l'axiomatique ordinale qui peut également servir à la définition axiomatique de ℕ

Démonstration :
Par la relation d'ordre, on peut définir pour tous p, q ∈ ℕ $p < q \iff p + 1 \leq q$

(i) Pour toute partie E de 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∈ M tel que p+1∉ M (sinon le 3eme axiome de Péano entrainerait que $M = \mathbb{N}$ et donc $E = \emptyset$). Supposons que p ∉ E, dans ce cas pour tout n∈ E l'inégalité p<n implique p+1≤n et p+1 est un minorant de E, ce qui est absurde. D'où p∈ E et on en déduit que p est le plus petit élément de E.

Propriété : ℕ est archimédien c'est à dire $\forall a, b \in \mathbb{N}\ b \leq a, \exists n \in \mathbb{N}, a \leq b \times n$

II) Construction de ℤ

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

1) Construction

On note N × N l'ensemble des couples d'entiers naturels. Dans cet ensemble de couples, on a trivialement que (a, b) = (a′, b′) ⇔ a = a′ et b = b′.

Définition : On définit alors la relation R entre couple d'entiers par

(a, b) R (a′, b′) ⇔ a + b′ = a′ + b.

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

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

2) Addition dans $\mathbb{Z}$

Soient x, y ∈ $\mathbb{Z}$. 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 ⊕ :

∀ a, a′, b, b′∈ $\mathbb{N}$, $\overline{(a,b)} \oplus \overline{(a',b')} = \overline{(a + a', b + b')}$.

Théorème : ($\mathbb{Z}$, ⊕) est un groupe commutatif

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

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

Théorème : 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 ≥ 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.

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

Théorème : 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 ∈ $\mathbb{N}$, on a :
f(a) × f(b) = $\overline{(a,0)} \times \overline{(b,0)} = \overline{(ab,0)}$ = f(ab).