DOCUMENT 1

Axiomatique de $\mathbb{N}$. Construction de l'anneau $\mathbb{Z}$

1. Les entiers naturels

La première définition axiomatique des entiers naturels apparaît dans un ouvrage de Dedekind, "Was sind und was sollen die Zahlen ? ", publié en 1888. En 1861, Hermann Grassmann, dans son livre "Lehrbuch der Arithmetik" avait donné une approche axiomatique des entiers relatifs où figure le principe de récurrence.

L'axiomatique des entiers naturels de Dedekind est plus connu sous le nom d'axiomatique de Peano et elle peut être décrite de la façon suivante.

Il existe un ensemble $\mathbb{N}$, dit ensemble des entiers naturels, vérifiant les propriétés :

(1) 0 est un entier,
(2) Pour tout entier n, il existe un unique entier $s(n)$ appelé son successeur,
(3) Aucun entier n'a 0 comme successeur,
(4) Deux entiers ayant le même successeur sont égaux,
(5) Si un ensemble d'entiers contient 0 et contient le successeur de chacun de ses éléments alors cet ensemble est égal à $\mathbb{N}$.

On peut donner une définition plus moderne d'un ensemble d'entiers naturels.

DÉFINITION 1.1. *Soit A un ensemble, 0 un élément de A et s une application de A dans A. Le triplet $(A, 0, s)$ est un ensemble d'entiers naturels si*

A_1 *L'application s est une injection de A dans $A - \{0\}$;*
A_2 *Pour toute partie B de A, $0 \in B$ et $s(B) \subset B$ impliquent $B = A$.*

Remarques. 1) L'image $Im\ s$ de s est $A - \{0\}$. En effet, soit $B = Im\ s \cup \{0\}$. On a $0 \in B$ et $s(B) \subset Im\ s \subset B$ et donc, par A_2, $B = A$ et $Im\ s = A - \{0\}$ car $0 \notin Im\ s$.

2) L'axiome A_1 entraine qu'il existe une injection de A dans l'une de ses parties strictes. L'ensemble A est donc infini au sens de Dedekind.

3) On peut se demander si, dans le cadre de la théorie des ensembles usuelle, il existe un ensemble d'entiers naturels. La réponse est heureusement oui mais la preuve est un peu difficile. On peut montrer que les cardinaux finis forment un ensemble X et que si l'on pose $0 = \emptyset$ alors $0 \in X$ et l'application s qui a un cardinal fini Y fait correspondre $s(Y) = Y \cup \{Y\}$ est une injection de X dans $X - \{0\}$ qui vérifie l'axiome A_2. Le triplet $(X, 0, s)$ est donc un ensemble d'entiers naturels.

On va maintenant montrer que sur tout ensemble d'entiers naturels on peut définir deux lois de composition et une relation d'ordre.

Construction d'une addition sur un ensemble d'entiers naturels $(A, 0, s)$.

Soit B l'ensemble des $x \in A$ tels qu'il existe une application $f_x : A \to A$ vérifiant :

$$(S)\begin{cases} f_x(0) = x, \\ f_x(s(y)) = s(f_x(y)) \text{ pour tout } y \in A. \end{cases}$$

On a $0 \in B$ car si l'on pose $f_0(y) = y$ alors $f_0(0) = 0$ et $f_0(s(y)) = s(y) = s(f_0(y))$.

Supposons $x \in B$ et soit f_x tel que $f_x(0) = x$ et $f_x(s(y)) = s(f_x(y))$. Posons $f_{s(x)}(y) = s(f_x(y))$. On a

$$\begin{cases} f_{s(x)}(0) = s(f_x(0)) = s(x), \\ f_{s(x)}(s(y)) = s(f_x(s(y))) = s(s(f_x(y))) = s(f_{s(x)}(y)). \end{cases}$$

On a donc $s(x) \in B$ et, par A_2, $B = A$. On a donc pour tout $x \in A$ une application f_x qui satisfait (S).

Soit $g : A \to A$ vérifiant $g(0) = x$ et $g(s(y)) = s(g(y))$. On montre en utilisant l'axiome A_2 que si $B = \{y \in A \mid f_x(y) = g(y)\}$ alors $B = A$. Pour tout $X \in A$, l'application f_x vérifiant (S) est donc unique.

On change de notations en posant $f_x(y) = x + y$. Par définition on a donc

$$(S)\begin{cases} x + 0 = x, \\ x + s(y) = s(x + y). \end{cases}$$

En faisant $y = 0$ on obtient $x + s(0) = s(x + 0) = s(x)$. On peut démontrer par récurrence (i.e. en utilisant l'axiome A_2) sur n les propriétés suivantes de $+$:

- $x + s(n) = s(x) + n$,
- $n + 0 = 0 + n$,
- $n + x = x + n$,
- $(x + y) + n = x + (y + n)$,
- $x + n = y + n$ implique $x = y$.

En général on pose $s(0) = 1$ d'où la nouvelle écriture de deux relations précédentes : $x+1 = s(x)$ et $x + (n + 1) = (x + 1) + n$.

Construction d'une multiplication sur un ensemble d'entiers naturels $(A, 0, s)$.

En remplaçant (S) par

$$\begin{cases} g_x(0) = 0, \\ g_x(s(y)) = g_x(y) + x \text{ pour tout } y \in A. \end{cases}$$

on définit une multiplication sur A et on prouve par récurrence ses propriétés usuelles. On montre aussi qu'elle est distributive par rapport à l'addition.

Construction d'un ordre sur un ensemble d'entiers naturels $(A, 0, s)$.

Une relation binaire $\leq$ est définie sur A par

$$x \leq y \Leftrightarrow \text{il existe } z \in A \text{ tel que } x + z = y.$$

Cette relation est une relation d'ordre total vérifiant

O_1 **:** $x \leq y$ implique, pour tout $z \in A$, $x + z \leq y + z$.
O_2 **:** $x \leq y$ implique, pour tout $z \in A$, $xz \leq yz$.

On remarque que $0 + x = x$ entraine que 0 est le plus petit élément de A.

Plus généralement, toute partie non vide de A possède un plus petit élément. On dit que $\leq$ est une relation de bon ordre ou que A est bien ordonné par $\leq$.

Preuve. Soit B une partie non vide de A et C l'ensemble des minorants stricts de B: $C = \{b \in A \mid a \in B \Rightarrow b < a\}$. Si C est vide alors $0 \in B$ et 0 est le plus petit élément de B. Supposons

$C \neq \emptyset$. Alors, $0 \in C$ et, comme $C \neq A$ (car $B \neq \emptyset$), l'axiome A_2 entraine qu'il existe $b_0 \in C$ tel que $c = b_0 + 1 \notin C$ (car si $s(C) \subset C$ alors $C = A$). L'entier c n'étant pas un minorant strict de B, il existe $a \in B$ tel que $a \leq c$. Si $a < c$ alors $a \leq b_0$ (pourquoi ?) ce qui contredit $b_0 \in C$. On a donc $a = c$ et $c \in B$. Pour tout $n \in B$, $b_0 < n$ d'où $c \leq n$ et c est donc le plus petit élément de B.

Dans la suite on désigne par $\mathbb{N}$ un ensemble d'entiers naturels. On suppose que l'on a démontré comme précédemment ou admis que $\mathbb{N}$ est muni de deux lois de composition internes $+$ et $.$ telles que

- Ces lois sont associatives et commutatives ;
- $+$ posséde un élément neutre 0 et $.$ un élément neutre 1 ;
- $.$ est distributive par rapport à $+$;
- $x + n = y + n$ implique $x = y$.

On peut aussi effectuer dans $\mathbb{N}$ des raisonnements par récurrence : si une propriété $P(n)$ est vraie pour 0 et si, pour tout entier n, $P(n)$ implique $P(n+1)$ est vrai alors la propriété P est vraie pour tout $n \in \mathbb{N}$. Cela équivaut à l'axiome A_2 précédent comme on le voit en introduisant $B = \{n \mid P(n) \text{ vrai}\}$.

On suppose aussi que sur $\mathbb{N}$ la relation

$$x \leq y \Leftrightarrow \text{ il existe } z \in \mathbb{N} \text{ tel que } x + z = y$$

est une relation d'ordre total qui satisfait les axiomes O_1 et O_2 précédents.

2. Symétrisation d'un semi-groupe régulier unitaire et commutatif

Nous allons voir maintenant comment l'anneau $\mathbb{Z}$ des entiers relatifs peut être construit à partir de $\mathbb{N}$. Cette construction étant un peu longue, la fin du document est consacré à une approche axiomatique de $\mathbb{Z}$, c'est-à-dire à la liste des propriétés de $\mathbb{Z}$ qu'il faut admettre pour pouvoir développer ensuite rigoureusement l'arithmétique.

La propriété de $\mathbb{N}$, $x + n = y + n$ implique $x = y$ signifie que comme dans un groupe, tout élément de $\mathbb{N}$ est simplifiable. On dit encore que tout élément de $\mathbb{N}$ est régulier et on définit un semi-groupe régulier comme étant un ensemble muni d'une loi de composition associative et où tout élément est régulier.

Toute partie stable d'un groupe est un semi-groupe régulier et pour qu'un ensemble muni d'une loi de composition associative soit isomorphe à une partie stable d'un groupe il est nécessaire que ce soit un semi-groupe régulier. On peut se demander si cette condition est suffisante et en particulier poser le problème suivant.

Problème. Pour tout semi-groupe régulier S unitaire et commutatif, existe-t-il un groupe commutatif G et un morphisme injectif $\varphi : S \to G$ tel que, pour pour tout morphisme injectif f de S dans un groupe commutatif G', il existe un morphisme injectif g de G dans G' vérifiant $f = g \circ \varphi$.

De façon moins formelle, on se pose la question de savoir si tout semi-groupe régulier S unitaire et commutatif est (isomorphe à) une partie stable d'un groupe G. On souhaite aussi que G soit minimal en ce sens que si S est aussi (isomorphe à) une partie stable d'un groupe G' alors G est (isomorphe à) un sous-groupe de G'. L'intérêt du problème provient en particulier du fait que l'existence dans un groupe d'un symétrique pour tout élément facilite beaucoup les calculs.

Analyse du problème.
Dans cette partie, on suppose le problème résolu et on va essayer de caractériser une solution G uniquement à l'aide de ce qui est connu, c'est-à-dire à l'aide de l'ensemble S et de sa loi de composition.

S'il existe un morphisme injectif φ de S dans un goupe G alors $\varphi(S)$ est une partie stable de G isomorphe à S. On peut donc identifier S et $\varphi(S)$ et considrer $G' = \{m - n | m, n \in S\}$. L'ensemble G' est un sous-groupe de G et, plus précisemment, c'est le sous-groupe de G engendré par S :

- $G' \neq \emptyset$ car $0 = 0 - 0 \in G'$;
- Si $m - n$ et $m' - n'$ sont dans G' $(m, n, m', n' \in S)$ alors $(m - n) - (m' - n') = (m + n') - (n + m') \in G'$.
- Tout sous-groupe de G qui contient S contient les différences de deux éléments de S et donc contient G'.

En tant qu'ensemble G' est lié à S^2 : l'application h de S^2 dans G' définie par $h(m, n) = m - n$ est surjective mais n'est pas injective en général (Penser à $\mathbb{N}^2$ et $\mathbb{Z}$.). Pour en déduire une application bijective, on utilise la technique habituelle en considérant la relation d'équivalence θ sur S^2 définie par

$$(m, n)\theta(m', n') \Leftrightarrow h(m, n) = h(m', n') \Leftrightarrow m - n = m' - n' \Leftrightarrow m + n' = m' + n.$$

L'application $\overline{h}$ de S^2/θ dans G' donnée par $\overline{h}(\overline{(m, n)}) = m - n$ est alors bijective et on peut en faire un morphisme en définissant une loi $+$ sur S^2/θ par

$$\overline{(m, n)} + \overline{(m', n')} = \overline{(m + m', n + n')}.$$

Le groupe G' est isomorphe à S^2/θ et la solution éventuelle de notre problème a été entièrement caractérisée à l'aide de S.

Construction
Soit S un semi-groupe commutatif régulier et unitaire. Considérons la relation binaire θ définie sur S par

$$(m, n)\theta(m', n') \Leftrightarrow m + n' = m' + n.$$

Cette relation est réflexive et symétrique et, en utilisant le fait que tout élément de S est régulier, on montre qu'elle est aussi transitive ; c'est donc une relation d'équivalence sur S.

LEMME 1.1. *Pour tous les éléments $m, n, p, q, m', n', p', q'$ de S*

$$\overline{(m, n)} = \overline{(m', n')},\ \ \overline{(p, q)} = \overline{(p', q')} \Rightarrow \overline{(m + p, n + q)} = \overline{(m' + p', n' + q')}.$$

Il suffit de remarquer que $m + n' = n + m'$ et $p + q' = q + p'$ impliquent $(m + p) + (n' + q') = (n + q) + (m' + q')$. Ce lemme montre que l'on peut définir une loi de composition, notée $+$, sur l'ensemble quotient S^2/θ en posant :

$$\overline{(m, n)} + \overline{(p, q)} = \overline{(m + p, n + q)}.$$

Remarque. On aurait pu aussi définir sur S^2 la loi

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

et montrer que cette loi est compatible avec θ (c'est la signification du lemme 1.1).

THÉORÈME 1.1. *L'ensemble S^2/θ, muni de la loi +, est un groupe commutatif. L'application φ de S dans S^2/θ définie par $\varphi(n) = \overline{(n,0)}$ est un morphisme injectif. Pour tout morphisme injectif f de S dans un groupe commutatif G, il existe un morphisme injectif g de S^2/θ dans G tel que $f = g \circ \varphi$.*
(Autrement dit, notre problème est résolu positivement.)

En utilisant l'associativité et la commutativité de la loi + de S, on voit facilement que la loi + de S^2/θ est associative et commutative. On a $\overline{(0,0)} = \{(n,n)|n \in S\}$ et il est clair que c'est un élément neutre pour + qui sera encore noté 0. Pour tout $(m,n) \in S^2$, $\overline{(m,n)} + \overline{(n,m)} = \overline{(m+n, m+n)} = \overline{(0,0)}$ et donc l'opposé de $\overline{(m,n)}$ existe et vaut $\overline{(n,m)}$. Finalement, $(S^2/\theta, +)$ est un groupe commutatif.

Si $\varphi(n) = \varphi(m)$ alors on a $(m,0)\theta(n,0)$ d'où $m = n$ et φ est donc injective. D'autre part

$$\varphi(n) + \varphi(m) = \overline{(m,0)} + \overline{(n,0)} = \overline{(m+n,0)} = \varphi(m+n)$$

ce qui montre que φ est un morphisme.

Soit maintenant f un morphisme injectif de S dans un groupe commutatif G. Si $\overline{(m,n)} = \overline{(p,q)}$ alors $m+q = n+p$ d'où $f(m) + f(q) = f(n) + f(p)$ et $f(m) - f(n) = f(p) - f(q)$ ce qui montre que $f(m) - f(n)$ ne dépend que de $\overline{(m,n)}$. On peut donc définir une application g de S^2/θ dans G par

$$g(\overline{(m,n)}) = f(m) - f(n).$$

On a $g \circ \varphi(n) = g(\overline{(n,0)}) = f(n) - f(o) = f(n)$ et donc $f = g \circ \varphi$. Il reste à montrer que g est un morphisme injectif :

$$\begin{aligned} g(\overline{(m,n)}) + g(\overline{(p,q)}) &= (f(m) - f(n)) + (f(p) - f(q)) = f(m+p) - f(n+q) \\ &= g(\overline{(m+p, n+q)}) = g(\overline{(m,n)} + \overline{(p,q)}) \end{aligned}$$

et $g(\overline{(m,n)}) = 0$ entraine $f(m) - f(n) = 0$ d'où, f étant injective, $m = n$ et donc $\overline{(m,n)} = 0$.

Ecriture des éléments de $\mathbf{S^2/\theta}$. Le morphisme injectif φ permet d'identifier l'élément n de S et $\varphi(n) = \overline{(n,o)}$. Comme $-\overline{(0,n)} = \overline{(n,0)}$, par cette identification, $-\overline{(0,n)}$ devient $-n$ et $\overline{(m,n)} = \overline{(m,0)} + \overline{(0,n)}$ entraine que tout élément $\overline{(m,n)}$ de S^2/θ s'écrit $m - n$ avec $m,\ n \in S$.

DÉFINITION 1.2. *Soit S un semi-groupe commutatif, unitaire et régulier. Le groupe commutatif $(S^2/\theta, +)$ est appelé le symétrisé du semi-groupe S.*

Lorsque $S = (\mathbb{N}, +)$ son symétrisé est appelé l'ensemble des entiers relatifs et on le note $\mathbb{Z}$. Soit $(m,n) \in \mathbb{N}^2$. Si $n \leq m$ alors $m - n \in \mathbb{N}$ et $\overline{(m,n)} = \overline{(m-n, 0)}$, ce qui fait que $\overline{(m,n)}$ est identifié à l'entier $m - n$. Maintenant, si $m \leq n$ alors $n - m \in \mathbb{N}$ et $\overline{(m,n)} = \overline{(o, n-m)} = -\overline{(n-m, 0)}$ et donc $\overline{(m,n)}$ est l'opposé d'un entier et s'écrit $-(n-m)$. Tout élément de $\mathbb{Z}$ s'identifie donc à un entier ou à l'opposé d'un entier. Autrement dit, $\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}$.

Il existe aussi sur $\mathbb{N}$ une multiplication et une relation d'ordre. L'objet du prochain paragraphe est de montrer que ces notions se prolongent à $\mathbb{Z}$.

3. Relation d'ordre sur ℤ. Structure d'anneau.

3.1. Relation d'ordre sur ℤ. La relation binaire $\leq$ définie sur $\mathbb{N}$ par

$$n \leq m \Leftrightarrow \text{il existe } p \in \mathbb{N} \text{ tel que } n + p = m$$

est une relation d'ordre total sur $\mathbb{N}$ qui vérifie les deux propriétés suivantes :

O_1 **:** $n \leq m$ implique, pour tout $p \in \mathbb{N}$, $n + p \leq m + p$.
O_2 **:** $n \leq m$ implique, pour tout $p \in \mathbb{N}$, $np \leq mp$.

Nous allons d'abord montrer que l'ordre sur $\mathbb{N}$ possède un unique prolongement à $\mathbb{Z}$ vérifiant O_1 et qui est total.

Soit $\preceq$ une relation d'ordre total sur $\mathbb{Z}$ prolongeant celle de $\mathbb{N}$ et vérifiant O_1. Pour tout $n \in \mathbb{N}$, $0 \preceq n$. Réciproquement, si $O \preceq m$, $m \in \mathbb{Z}$ et $m \neq 0$, alors $m \notin \mathbb{N}$ implique $-m \in \mathbb{N}$ d'où $0 \preceq -m$ et, par O_1, $m \preceq 0$ et finalement $m = 0$, ce qui est contradictoire. On a donc $\mathbb{N} = \{n \in \mathbb{Z} \mid 0 \preceq n\}$. Supposons $m \preceq n$. Par O_1, $0 \preceq p = n - m$ d'où $p \in \mathbb{N}$ et $m + p = n$. Réciproquement, s'il existe $p \in \mathbb{N}$ vérifiant $m+p = n$ alors $0 \preceq p = n-m$ et $m \preceq n$. Finalement, $m \preceq n$ équivaut à l'existence de $p \in \mathbb{N}$ tel que $m + p = n$. L'ordre sur $\mathbb{N}$ possède donc au plus un prolongement à $\mathbb{Z}$ qui est total et qui vérifie O_1.

Il reste à montrer que la relation binaire $\preceq$ sur $\mathbb{Z}$

$$m \preceq n \Leftrightarrow \text{il existe } p \in \mathbb{N} \text{ tel que } m + p = n$$

est bien une relation d'ordre total vérifiant O_1. Les différentes vérifications sont faciles.

Un groupe muni d'une relation d'ordre total vérifiant la propriété O_1 est appelé un groupe totalement ordonné. On a donc montré :

PROPOSITION 1.1. *Il existe une unique relation d'ordre total sur $\mathbb{Z}$ qui prolonge celle de $\mathbb{N}$ et qui en fait un groupe totalement ordonné. Cette relation, notée maintenant $\leq$, est définie par:*

$$m \leq n \Leftrightarrow \textit{il existe } p \in \mathbb{N} \textit{ tel que } m + p = n$$

La relation d'ordre sur $\mathbb{N}$ possède une propriété plus forte que le fait d'être totale : toute partie non vide de $\mathbb{N}$ possède un plus petit élément, ce que l'on traduit en disant que $\mathbb{N}$ est un ensemble bien ordonné. Ce résultat se généralise partiellement à $\mathbb{Z}$.

PROPOSITION 1.2. *Tout intervalle de $\mathbb{Z}$ de la forme $[a, \rightarrow [$ est isomorphe à $\mathbb{N}$. Toute partie non vide et minorée de $\mathbb{Z}$ possède un plus petit élément.*

Considérons l'application f de $[a, \rightarrow [$ dans $\mathbb{N}$ définie par $f(x) = x - a$. Il est clair que cette application est bijective et, comme $x \leq y$ équivaut à $x - a \leq y - a$, c'est un isomorphisme entre les ensembles ordonnés $[a, \rightarrow [$ et $\mathbb{N}$. Toute partie non vide et minorée de $\mathbb{Z}$ est contenue dans un intervalle du type $[a, \rightarrow [$. Elle possède donc un plus petit élément.

3.2. La structure d'anneau de ℤ. Pour introduire une multiplication sur $\mathbb{Z}$ on définit une multiplication sur $\mathbb{N}^2$ par

$$(m, n).(p, q) = (mp + nq, mq + np).$$

Montrons que cette loi est compatible avec θ.

Si $(m, n)\theta(m', n')$ et $(p, q)\theta(p', q')$ alors $m + n' = n + m'$ et $p + q' = q + p'$ d'où par des multiplications par p, q, m' et n' :

$$\begin{aligned} mp + n'p &= np + m'p \\ nq + m'q &= n'q + mq \\ m'p + m'q' &= m'q + m'p' \\ n'p + n'q &= n'p + n'q'. \end{aligned}$$

En ajoutant ces égalités, on obtient après quatre simplifications

$$mp + nq + m'q' + n'p' = mq + np + m'p' + n'q'$$

ce qui traduit

$$(m, n)(p, q)\theta(m', n')(p', q')$$

et montre la compatibilité de cette multiplication avec θ. On peut donc considérer sur $\mathbb{Z}$ la loi quotient définie par

$$\overline{(m, n)}\ \overline{(p, q)} = \overline{(m, n)(p, q)}.$$

PROPOSITION 1.3. *Le triplet $(\mathbb{Z}, +, .)$ est un anneau commutatif, unitaire, sans diviseur de zéro et totalement ordonné. De plus, la multiplication sur $\mathbb{Z}$ prolonge celle de $\mathbb{N}$.*

Il est clair que la multiplication est commutative. Pour prouver l'associativité de la multiplication et sa distributivité par rapport à l'addition on utilise ces propriétés dans $\mathbb{N}$ et il est clair que $1 = \overline{(1, 0)}$ est neutre pour la multiplication. La non existence de diviseur de zéro est un peu plus difficile à montrer.

Si pour deux entiers naturels a et b, $ab = 0$ alors $a = 0$ ou $b = 0$: la propriété est vraie pour $a = 0$ et si elle est vraie pour a alors $(a + 1)b = 0$ entraine $(a + 1)b = ab + b = ab + b' + 1 = 0$ si $b \neq 0$. C'est absurde car 1 n'est le successeur d'aucun entier positif et donc $b = 0$. La propriété est démontrée par récurrence. Remarquons aussi que pour deux éléments a et b de $\mathbb{Z}$, $(-a)b = -(ab)$ car $(-a)b + ab = (-a + a)b = 0b = 0$. Maintenant si $ab = 0$ avec a et b dans $\mathbb{Z}$ alors

- si $a \in \mathbb{N}$ et $b \in \mathbb{N}$ alors $a = 0$ ou $b = 0$.
- si $-a \in \mathbb{N}$ et $b \in \mathbb{N}$, $ab = 0$ équivaut à $0 = -(ab) = (-a)b$ et donc $-a = 0$ ou $b = 0$. Mais $-a = 0$ équivaut à $a = 0$ et donc $a = 0$ ou $b = 0$.
- la preuve des deux autres cas est analogue.

Montrons que l'application φ du théorème 1.1 est un homomorphisme pour la multiplication. Pour deux éléments a et b de $\mathbb{N}$ on a :

$$\varphi(a)\varphi(b) = (a, 0)(b, 0) = (ab, 0) = \varphi(ab)$$

et donc le produit de deux éléments de $\varphi(\mathbb{N})$ est un élément de $\varphi(\mathbb{N})$. Après identification de $\mathbb{N}$ et $\varphi(\mathbb{N})$, le produit de deux éléments de $\mathbb{N}$ est dans $\mathbb{N}$.

Soit a, b, $c \in \mathbb{Z}$. Si $a \leq b$ et $c \geq 0$ alors $b - a \in \mathbb{N}$ et $c \in \mathbb{N}$ d'où $(b - a)c \in \mathbb{N}$ ou encore $bc - ac \in \mathbb{N}$ et donc $ac \leq bc$. La propriété O_2 est vérifiée et l'anneau $\mathbb{Z}$ est un anneau totalement ordonné.

Remarque. Un anneau commutatif, unitaire, sans diviseur de zéro et distinct de $\{0\}$ est dit intègre. L'anneau $\mathbb{Z}$ est donc intègre. On verra qu'il est aussi euclidien et donc principal (i.e. intègre et tout idéal est principal).

4. Une approche plus intuitive de la construction de ℤ

Dans ℕ, la relation d'ordre est définie par

$$m \leq n \Leftrightarrow \text{il existe } d \in \mathbb{N} \text{ tel que } m + d = n.$$

Si $m \leq n$ on peut appeler l'entier d tel que $m + d = n$ la différence entre n et m et le noter $[n - m]$. Par définition, on a $m + [n - m] = n$ mais l'opération différence $(n, m) \mapsto [n - m]$ n'est définie que si $m \leq n$. C'est seulement une loi de composition partielle et la construction de ℤ a pour but de donner un sens à $[n - m]$ même si $n < m$.

Si $m \leq n$ il existe une infinité de couples (p, q), $q \geq p$ qui ont la même différence que le couple (n, m). Le résultat suivant montre que cela peut se traduire sans utiliser la notion de différence.

Lemme 1.2. *Deux couples (n, m) et (p, q), $m \leq n$ et $q \leq p$, ont la même différence si et seulement si $n + q = p + m$.*

En effet, s'ils ont la même différence d alors $m+d = n$ et $q+d = p$ d'où $n+q+d = p+m+d$ et $n + q = p + m$. Réciproquement, si $n + q = p + m$ alors $(m + [n - m]) + q = p + m$ d'où (en utilisant l'associativité et la régularité) $[n - m] + q = p$ ce qui signifie $[n - m] = [p - q]$.

Chaque différence $[n - m]$, $m \leq n$, est donc associée à l'ensemble de couples $\Delta(n, m) = \{(p, q) \in \mathbb{N}^2 | n + q = p + m\}$. Si $m \leq n$ alors tout élément (p, q) de $\Delta(n, m)$ vérifie $q \leq p$ mais l'ensemble $\Delta(n, m)$ peut être défini même si $m > n$. Pour donner un sens à $[n - m]$ lorsque $n < m$, on va considérer, pour tout $(n, m) \in \mathbb{N}^2$, les ensembles $\Delta(n, m)$. Ces ensembles sont en fait les classes d'équivalence pour la relation d'équivalence θ définie sur ℕ par

$$(n, m)\theta(p, q) \Leftrightarrow n + q = p + m$$

Il reste ensuite à définir sur $\mathbb{Z} = \mathbb{N}^2/\theta$ deux lois de composition + et . et à montrer que $(\mathbb{Z}, +, .)$ est un anneau intègre avec une partie stable $\{\overline{(n, 0)} | n \in \mathbb{N}\}$ isomorphe à $(\mathbb{N}, +, .)$. Il est alors intéressant de remarquer, qu'après identification de ces deux ensembles d'entiers, les différences $[n-m]$, $m \leq n$, sont devenues $n-m$, la somme de n et de l'opposé de m. En effet, si $d = [n - m]$ alors $m + d = n$ d'où $\overline{(m, 0)} + \overline{(d, 0)} = \overline{(n, 0)}$ et $\overline{(d, 0)} = \overline{(n, 0)} - \overline{(m, 0)}$ ce qui, après identification, s'écrit $d = n-m$ [1] . Pour $n < m$ $\overline{(n, 0)} - \overline{(m, 0)} = \overline{(n, m)} = \overline{(0, m - n)} = -[m-n]$. On voit ainsi que maintenant tout couple d'entiers (n, m) possède une différence, identifiée à un élément de ℕ si $n \geq m$ et à l'opposé d'un élément de ℕ sinon .

Cette approche intuitive peut remplacer l'analyse du problème du début de ce document.

5. Introduction axiomatique de ℤ.

Pour introduire ℤ de manière axiomatique, on peut admettre la proposition 1.3 et prendre comme axiomes les affirmations suivantes :

- $(\mathbb{Z}, +, .)$ est un anneau commutatif , unitaire et sans diviseur de zéro ;
- $(\mathbb{N}, +, .)$ est une partie stable de cet anneau ;

[1] Il est important de bien voir la différence de signification des deux signes $-$ dans $[n - m]$ et $n - m$: $[n - m]$ est une notation qui désigne l'entier qu'il faut ajouter dans ℕ à m pour obtenir n tandis que $-m$ est la notation traditionnelle de l'opposé de m lorsque la loi de composition est notée $+$.

- $\mathbb{Z}$ est un anneau totalement ordonné par la relation

$$m \leq n \Leftrightarrow \text{ il existe } p \in \mathbb{N} \text{ tel que } m + p = n.$$

On peut ensuite démontrer la proposition 1.2 qui donne une propriété supplémentaire de l'anneau ordonné $\mathbb{Z}$.

Ces résultats nous permettrons de démontrer dans le prochain document une propriété essentielle de $\mathbb{Z}$: l'anneau $\mathbb{Z}$ est euclidien.