Chapitre III

Construction des ensembles de nombres $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$

1 Construction de $\mathbb{N}$

Dans cette section nous allons voir comment on peut établir les propriétés essentielles de $\mathbb{N}$ à partir des axiomes introduits en 1889 par le mathématicien Italien Giuseppe Peano (1858-1932).

Axiomes de Peano - *Il existe un ensemble* $\mathbb{N}$*, une application* s *de* $\mathbb{N}$ *dans* $\mathbb{N}$ *et un élément (noté* 0*) de* $\mathbb{N}$ *tels que :*

(i) $\forall x \in \mathbb{N}, \forall y \in \mathbb{N}, \quad s(x) = s(y) \Longrightarrow x = y$,

(ii) $0 \notin s(\mathbb{N})$,

*(iii) (*Axiome d'induction*)* *Soit* $P \subset \mathbb{N}$*. Si* P *vérifie*

$$\begin{cases} 0 \in P \\ \forall x \in \mathbb{N}, \quad x \in P \Longrightarrow s(x) \in P \end{cases}$$

Alors $P = \mathbb{N}$*.*

Définitions - L'image $s(x)$ d'un entier x par l'application s est appelée le *successeur* de x, et s est appelée l'*application successeur*.

Le symbole 1 désignera le nombre $s(0)$.

Remarques - L'axiome (i) signifie que l'application s est injective et l'axiome (ii) exprime que 0 n'est le successeur d'aucun entier. Quant à l'axiome (iii), il traduit le *principe de récurrence*.

Un outil essentiel des démonstrations qui vont suivre est l'usage de *suites définies par une relation de récurrence*. Le théorème suivant garantit la pertinence de leur définition.

Théorème 1.1 *Soient* E *un ensemble non vide,* f *une application de* E *dans* E *et* $a \in E$*. Il existe une unique suite* $u : \mathbb{N} \longrightarrow E$ *vérifiant les deux conditions*

$$\begin{cases} u(0) = a \\ \forall n \in \mathbb{N}, \quad u(s(n)) = f(u(n)) \ . \end{cases}$$

Remarque - Pour les besoins des rédactions de cette section, on utilise ici la notation $u(n)$ au lieu de u_n pour le terme de rang n de la suite : il est considéré comme l'image de l'élément n de $\mathbb{N}$ par l'application u.
Preuve - L'existence de la suite u est admise (la démonstration n'est pas très difficile mais fait appel à la caractérisation des *applications* comme *graphes* de relations binaires, non rappelée dans ce cours).

On établit donc seulement l'unicité. Soient deux suites u et u' satisfaisant

$$\left\{ \begin{array}{l} u(0) = a \\ \forall n \in \mathbb{N}, \quad u(s(n)) = f(u(n)) \end{array} \right. \quad \text{et} \quad \left\{ \begin{array}{l} u'(0) = a \\ \forall n \in \mathbb{N}, \quad u'(s(n)) = f(u'(n)) \ . \end{array} \right.$$

Posons $P = \{n \in \mathbb{N} \ / \ \ u(n) = u'(n)\}$. Cet ensemble vérifie $P \subset \mathbb{N}$ et $0 \in P$ (puisque $u(0) = u'(0) = a$).

De plus si $n \in P$, on a

$$u(s(n)) = f(u(n)) = f(u'(n)) = u'(s(n)) \ ,$$

de sorte que $s(n) \in P$. On peut donc conclure grâce à l'axiome (iii) que $P = \mathbb{N}$. Ainsi pour tout $n \in \mathbb{N}$, $u(n) = u'(n)$, c'est-à-dire $u = u'$. □

1.1 Construction de l'addition

Théorème 1.2 *Il existe une application* $\sigma \ : \ \left(\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \to & \mathbb{N} \\ (k,n) & \mapsto & k+n \end{array} \right)$ *(appelée addition) vérifiant :*

(1)	$\forall k \in \mathbb{N}, \forall m \in \mathbb{N}, \forall n \in \mathbb{N},$	$(k+m)+n = k+(m+n)$	(l'addition est associative)
(2)	$\forall k \in \mathbb{N}, \forall n \in \mathbb{N},$	$k+n = n+k$	(l'addition est commutative)
(3)	$\forall k \in \mathbb{N},$	$k+0 = 0+k = k$	(0 est élément neutre)
(4)	$\forall k \in \mathbb{N},$	$k+1 = s(k)$	

Preuve - Pour définir l'application σ, on fixe un entier k et on applique le Théorème 1.1 avec $E = \mathbb{N}$, $f = s$ et $a = k$.

Il existe donc une unique application $s_k \ : \ \mathbb{N} \longrightarrow \mathbb{N}$ telle que

$$(\star) \quad s_k(0) = k \quad \text{et} \quad (\star\star) \quad \forall n \in \mathbb{N} \ \ s_k(s(n)) = s(s_k(n)) \ .$$

Cette construction étant valable pour tout $k \in \mathbb{N}$, on peut poser pour tout $(k,n) \in \mathbb{N} \times \mathbb{N}$:

$$k + n = s_k(n) \ .$$

On démontre d'abord la propriété (4) en écrivant pour k entier quelconque,

$$k + 1 = s_k(1) = s_k(s(0)) = s(s_k(0)) = s(k) \ .$$

On démontre ensuite la propriété (3).

On a d'une part pour tout $k \in \mathbb{N}$ la relation $s_k(0) = k$, c'est-à-dire $k + 0 = k$.

D'autre part, considérons l'ensemble $P = \{n \in \mathbb{N} \ / \ s_0(n) = n\}$. On a $0 \in P$ puisque $s_0(0) = 0$. De plus, si $n \in P$, n vérifie la relation $s_0(n) = n$. On en tire grâce à $(\star\star)$:

$$s_0(s(n)) = s(s_0(n)) = s(n) \ ,$$

de sorte que $s(n) \in P$. Par application de l'axiome (iii), il vient $P = \mathbb{N}$, c'est-à-dire

$$\forall k \in \mathbb{N}, \quad 0 + k = k \ .$$

Finalement la propriété (3) est valide : 0 est élément neutre pour l'addition.

On établit ensuite la propriété (1). Pour cela on pose

$$P = \{n \in \mathbb{N} \ / \ \forall k \in \mathbb{N}, \ \forall m \in \mathbb{N}, \quad (k + m) + n = k + (m + n)\} \ .$$

L'entier 0 appartient à P, puisque pour tout $k \in \mathbb{N}$ et tout $m \in \mathbb{N}$, on a d'après (3)

$$(k + m) + 0 = k + m = k + (m + 0) \ .$$

Soit $n \in P$. En remarquant que $(k+m)+n = k+(m+n)$ peut s'écrire $s_{k+m}(n) = s_k(m+n)$, on peut écrire

$$\begin{array}{rcll}
(k + m) + s(n) & = & s_{k+m}(s(n)) & \text{(par définition de } \sigma) \\
& = & s(s_{k+m}(n)) & \text{(d'après } (\star\star)) \\
& = & s(s_k(m + n)) & \text{(par la remarque ci-dessus)} \\
& = & s_k(s(m + n)) & \text{(d'après } (\star\star)) \\
& = & s_k(s(s_m(n))) & \text{(par définition de } \sigma) \\
& = & s_k(s_m(s(n))) & \text{(d'après } (\star\star)) \\
& = & k + (m + s(n)) & \text{(par définition de } \sigma) \ .
\end{array}$$

Cela montre qu'alors $s(n) \in P$. L'axiome (iii) permet encore de conclure que $P = \mathbb{N}$, c'est-à-dire que (1) est satisfaite : l'addition est associative .

On ne détaillera pas la preuve de la propriété (2). Signalons seulement qu'elle résulte aussi de l'axiome (iii). On applique d'abord cet axiome à

$$P = \{n \in \mathbb{N} \ / \ \forall m \in \mathbb{N}, \quad s(m + n) = s(m) + n\}$$

pour vérifier que

$$\forall m \in \mathbb{N}, \ \forall n \in \mathbb{N}, \quad s(m + n) = s(m) + n \ .$$

Puis on l'applique à

$$P' = \{n \in \mathbb{N} \ / \ \forall k \in \mathbb{N}, \quad k + n = n + k\}$$

pour obtenir (2). □

1.2 Construction de la multiplication

Théorème 1.3 *Il existe une application* $\pi \ : \ \begin{pmatrix} \mathbb{N} \times \mathbb{N} & \to & \mathbb{N} \\ (k, n) & \mapsto & k.n \end{pmatrix}$ *(appelée multiplication) vérifiant :*

(1)	$\forall k \in \mathbb{N}, \forall m \in \mathbb{N}, \forall n \in \mathbb{N},$	$(k.m).n = k.(m.n)$	(la multiplication est associative)
(2)	$\forall k \in \mathbb{N}, \forall n \in \mathbb{N},$	$k.n = n.k$	(la multiplication est commutative)
(3)	$\forall k \in \mathbb{N},$	$k.1 = 1.k = k$	(1 est élément neutre)
(4)	$\forall k \in \mathbb{N}, \forall m \in \mathbb{N}, \forall n \in \mathbb{N},$	$k.(m + n) = k.m + k.n$ $(m + n).k = m.k + n.k$	(la multiplication est distributive par rapport à l'addition)
(5)	$\forall n \in \mathbb{N},$	$n.0 = 0.n = 0$	(0 est élément absorbant)

Preuve - La preuve repose sur des arguments analogues à ceux utilisés pour démontrer le théorème 1.2.

Pour définir l'application π, on fixe un entier k et on applique le Théorème 1.1 avec $E = \mathbb{N}$, $f = s_k$ et $a = 0$.

Il existe donc une unique application $p_k : \mathbb{N} \longrightarrow \mathbb{N}$ telle que

$$(*) \quad p_k(0) = 0 \quad \text{et} \quad (**) \quad \forall n \in \mathbb{N},\ p_k(s(n)) = p_k(n) + k\ .$$

Cette construction étant valable pour tout $k \in \mathbb{N}$, on pose ensuite pour tout $(k, n) \in \mathbb{N}\times\mathbb{N}$:

$$k.n = p_k(n)\ .$$

Les propriétés (1) à (5) s'obtiennent ensuite en appliquant l'axiome (*iii*) à des ensembles P convenablement choisis. □

1.3 Construction de la relation d'ordre

Le but est de retrouver la relation d'ordre usuelle sur les entiers naturels (notée $\leq$), en la définissant à partir des notions introduites précédemment.

On peut le faire par exemple en disant que pour n et p entiers,

$$n \leq p \qquad \Longleftrightarrow \qquad \exists k \in \mathbb{N},\ p = n + k\ . \tag{1}$$

On établit ensuite les propriétés suivantes, en faisant un large usage de l'axiome d'induction (*iii*) (nous ne détaillerons pas les preuves ici).

Théorème 1.4 *a) La relation $\leq$ définie par (1) est une* relation d'ordre *: elle est*

réflexive :	$\forall n \in \mathbb{N},$	$n \leq n,$
anti-symétrique :	$\forall n \in \mathbb{N}, \forall p \in \mathbb{N},$	$(n \leq p) \wedge (p \leq n) \Longrightarrow (n = p),$
transitive :	$\forall n \in \mathbb{N}, \forall p \in \mathbb{N}, \forall q \in \mathbb{N},$	$(n \leq p) \wedge (p \leq q) \Longrightarrow (n \leq q).$

b) C'est une relation d'ordre total *: $\forall n \in \mathbb{N}, \forall p \in \mathbb{N}, \quad (n \leq p) \vee (p \leq n)$.*

c) Elle est compatible *avec l'addition et la multiplication :*

$$\begin{array}{ll} \forall n \in \mathbb{N}, \forall p \in \mathbb{N}, \forall q \in \mathbb{N} & n \leq p \Longrightarrow n + q \leq p + q\ , \\ \forall n \in \mathbb{N}, \forall p \in \mathbb{N}, \forall q \in \mathbb{N} & n \leq p \Longrightarrow n.q \leq p.q\ . \end{array}$$

d) Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

On montre de plus que lorsque $n \leq p$, l'entier k figurant dans (1) est *unique*. On l'appelle la *différence* de p et n et on note $k = p - n$.

1.4 Différentes formulations du principe de récurrence

Soit $\mathcal{H}_n$ une propriété dépendant de l'entier n. On peut lui associer le sous-ensemble P de $\mathbb{N}$ défini par

$$P = \{n \in \mathbb{N}\ /\ \mathcal{H}_n \text{ est vraie } \}\ .$$

L'axiome d'induction (le troisième axiome de Peano) prend alors la forme du théorème suivant.

Théorème 1.5 - Principe de récurrence (faible) - *Supposons qu'une propriété $\mathcal{H}_n$ (dépendant de $n \in \mathbb{N}$) vérifie :*
(1) - il existe $n_0 \in \mathbb{N}$ tel que $\mathcal{H}_{n_0}$ est vraie,
(2) - pour tout $n \in \mathbb{N}$ tel que $n \geq n_0$, on a $\mathcal{H}_n \Longrightarrow \mathcal{H}_{n+1}$.
Alors la propriété $\mathcal{H}_n$ est vraie pour tout entier naturel $n \geq n_0$.

Preuve - Soit $P = \{k \in \mathbb{N} \ / \ \mathcal{H}_{n_0+k} \text{ est vraie}\}$. On a $P \subset \mathbb{N}$ et $0 \in P$ (d'après (1)).

Par ailleurs, si $k \in P$, l'entier $n = n_0 + k$ vérifie $n \geq n_0$ et $\mathcal{H}_n$ est vraie. Il résulte de (2) que $\mathcal{H}_{n+1}$ est vraie également, c'est-à-dire (puisque $(n_0 + k) + 1 = n_0 + (k + 1)$), $k + 1 \in P$.

Finalement l'axiome d'induction permet d'affirmer que $P = \mathbb{N}$, et donc que $\mathcal{H}_n$ est vraie pour tout $n \geq n_0$ (puisque $n \geq n_0$ si et seulement si $n = n_0 + k$ avec $k \in \mathbb{N}$). □

Remarques - Dans un raisonnement par récurrence, la propriété $\mathcal{H}_n$ est appelée l'*hypothèse de récurrence*, la preuve de (1) est appelée l'*initialisation* du raisonnement et on traduit la propriété (2) en disant que $\mathcal{H}_n$ est *héréditaire*.

On déduit de ce théorème les trois corollaires suivants (démontrés en TD).

Corollaire 1.6 - Principe de récurrence (forte) - *Supposons qu'une propriété $\mathcal{H}_n$ (dépendant de $n \in \mathbb{N}$) vérifie :*
(1) - il existe $n_0 \in \mathbb{N}$ tel que $\mathcal{H}_{n_0}$ est vraie,
(2) - pour tout $n \in \mathbb{N}$ tel que $n \geq n_0$, on a $(\mathcal{H}_{n_0} \wedge \cdots \wedge \mathcal{H}_n) \Longrightarrow \mathcal{H}_{n+1}$.
Alors la propriété $\mathcal{H}_n$ est vraie pour tout entier naturel $n \geq n_0$.

Corollaire 1.7 - Principe de récurrence (à deux termes) - *Supposons qu'une propriété $\mathcal{H}_n$ (dépendant de $n \in \mathbb{N}$) vérifie :*
(1) - il existe $n_0 \in \mathbb{N}$ tel que $\mathcal{H}_{n_0}$ et $\mathcal{H}_{n_0+1}$ sont vraies,
(2) - pour tout $n \in \mathbb{N}$ tel que $n \geq n_0 + 1$, on a $(\mathcal{H}_{n-1} \wedge \mathcal{H}_n) \Longrightarrow \mathcal{H}_{n+1}$.
Alors la propriété $\mathcal{H}_n$ est vraie pour tout entier naturel $n \geq n_0$.

Corollaire 1.8 - Principe de récurrence (finie) - *Supposons qu'une propriété $\mathcal{H}_n$ (dépendant de $n \in \mathbb{N}$) vérifie :*
(1) - il existe $n_0 \in \mathbb{N}$ tel que $\mathcal{H}_{n_0}$ est vraie,
(2) - il existe un entier $N > n_0$ tel que : $\forall n \in \{n_0, \ldots, N-1\}$, $\mathcal{H}_n \Longrightarrow \mathcal{H}_{n+1}$.
Alors la propriété $\mathcal{H}_n$ est vraie pour tout entier naturel $n \in \{n_0, \ldots, N\}$.

2 Relations d'équivalences

2.1 Définition

Définitions - a) Un ensemble E étant donné, une *relation binaire* $\mathcal{R}$ sur $E \times E$ est appelée une *relation d'équivalence* si et seulement si elle est

$$\begin{array}{lrl}
\text{réflexive :} & \forall x \in E, & x\mathcal{R}x, \\
\text{symétrique :} & \forall x \in E, \forall y \in E, & x\mathcal{R}y \Longrightarrow y\mathcal{R}x, \\
\text{transitive :} & \forall x \in E, \forall y \in E, \forall z \in E, & (x\mathcal{R}y) \wedge (y\mathcal{R}z) \Longrightarrow (x\mathcal{R}z).
\end{array}$$

b) Soient $\mathcal{R}$ une relation d'équivalence sur un ensemble E et $x \in E$. On appelle *classe d'équivalence* de x suivant $\mathcal{R}$ l'ensemble $C_{\mathcal{R}}(x) = \{y \in E \ / \ x\mathcal{R}y\}$.

On appelle *ensemble quotient* de E pour la relation $\mathcal{R}$ l'ensemble de toutes les classes d'équivalences d'éléments de E selon $\mathcal{R}$. On le note $E/\mathcal{R}$. Ainsi

$$E/\mathcal{R} = \{C_{\mathcal{R}}(x),\ x \in E\}\ .$$

C'est un sous-ensemble de l'ensemble $\mathcal{P}(E)$ des parties de E.
Exemple - Dans l'ensemble $\mathbb{N}$, la relation définie par « $n\,\mathcal{R}\,p$ si et seulement si n a même reste que p dans la division par 2 » est une relation d'équivalence. Il y a deux classes d'équivalences : l'ensemble des entiers pairs (qui constitue la classe de 0) et l'ensemble des entiers impairs (qui constitue la classe de 1). Ainsi $E/\mathcal{R} = \{C_{\mathcal{R}}(0), C_{\mathcal{R}}(1)\}$.

Proposition 2.1 $\forall x \in E, \quad \forall y \in C_{\mathcal{R}}(x), \quad C_{\mathcal{R}}(y) = C_{\mathcal{R}}(x)\ .$

Preuve - Soit $y \in C_{\mathcal{R}}(x)$, autrement dit $x\mathcal{R}y$.

Si $z \in C_{\mathcal{R}}(y)$, alors $y\mathcal{R}z$ d'où par transitivité, $x\mathcal{R}z$ c'est-à-dire $z \in C_{\mathcal{R}}(x)$. Ainsi $C_{\mathcal{R}}(y) \subset C_{\mathcal{R}}(x)$. On montre de même l'inclusion inverse. □

2.2 Lien avec les partitions d'un ensemble

Définition - Soit $\mathcal{F}$ un sous-ensemble de $\mathcal{P}(E)$. On dit que $\mathcal{F}$ est une *partition* de E s'il vérifie :

(1) $\forall F \in \mathcal{F}, \quad F \neq \emptyset,$
(2) $\forall F \in \mathcal{F}, \forall G \in \mathcal{F}, \quad F \neq G \Longrightarrow F \cap G = \emptyset,$
(3) $\bigcup_{F \in \mathcal{F}} F = E.$

Théorème 2.2 *Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. L'ensemble quotient $E/\mathcal{R}$ est une partition de E.*

Preuve - (1) Pour $F \in E/\mathcal{R}$, il existe $x \in E$ tel que $F = C_{\mathcal{R}}(x)$. Or $\mathcal{R}$ étant réflexive, on a $x \in C_{\mathcal{R}}(x)$. Ainsi $F \neq \emptyset$.

(2) Soient F et G deux éléments de $E/\mathcal{R}$. Il existe $x \in E$ et $y \in E$ tels que $F = C_{\mathcal{R}}(x)$ et $G = C_{\mathcal{R}}(y)$. On raisonne par contraposition. Si $F \cap G \neq \emptyset$, il existe $z \in F \cap G$. On déduit de la proposition 2.1 que $C_{\mathcal{R}}(x) = C_{\mathcal{R}}(z) = C_{\mathcal{R}}(y)$ soit $F = G$.

(3) Pour tout $x \in E$, on a $C_{\mathcal{R}}(x) \subset E$, de sorte que $\bigcup_{x \in E} C_{\mathcal{R}}(x) \subset E$. Par ailleurs, on a pour tout $x_0 \in E$, $x_0 \in C_{\mathcal{R}}(x_0)$ d'où $x_0 \in \bigcup_{x \in E} C_{\mathcal{R}}(x)$ et finalement $E \subset \bigcup_{x \in E} C_{\mathcal{R}}(x)$. □

Théorème 2.3 *Soit $\mathcal{F}$ une partition d'un ensemble E. Il existe une unique relation d'équivalence sur E telle que $\mathcal{F} = E/\mathcal{R}$.*

Preuve - Si une telle relation $\mathcal{R}$ existe, elle doit nécessairement vérifier

$$\forall x \in E, \forall y \in E, \quad x\mathcal{R}y \Longleftrightarrow (\exists F \in \mathcal{F},\ x \in F \text{ et } y \in F).$$

Ceci détermine $\mathcal{R}$ de manière unique.

Reste à voir que la relation ainsi définie est bien une relation d'équivalence, et que l'on a bien $E/\mathcal{R} = \mathcal{F}$.

La réflexivité découle de (3) : $x \in E$ donc il existe $F \in \mathcal{F}$ tel que $x \in F$. Alors $x\mathcal{R}x$.

La symétrie provient du fait que $x \in F$ et $y \in F$ si et seulement si $y \in F$ et $x \in F$.

La transitivité s'obtient grâce à (2). En effet, si $x\mathcal{R}y$ et $y\mathcal{R}z$, il existe d'une part $F \in \mathcal{F}$ tel que $x \in F$ et $y \in F$, et d'autre part $G \in \mathcal{F}$ tel que $y \in G$ et $z \in G$. Comme $y \in F \cap G$ il vient $F = G$, de sorte que $x \in F$ et $z \in F$. Mais alors $x\mathcal{R}z$.

Pour montrer que $\mathcal{F} = E/\mathcal{R}$, on remarque d'abord que pour tout $F \in \mathcal{F}$ et tout $x \in F$, on a $F = \mathcal{C}_{\mathcal{R}}(x)$. En effet d'une part la relation $y \in F$ entraîne que $x\mathcal{R}y$, et donc $y \in \mathcal{C}_{\mathcal{R}}(x)$. D'autre part, la relation $y \in \mathcal{C}_{\mathcal{R}}(x)$ entraîne $x\mathcal{R}y$, c'est-à-dire qu'il existe $G \in \mathcal{F}$ tel que x et y soient tous deux dans G. Mais alors $F \cap G \neq \emptyset$, d'où $F = G$. Ainsi $y \in F$.

On en déduit d'abord que $\mathcal{F} \subset E/\mathcal{R}$: car si $F \in \mathcal{F}$, on sait que $F \neq \emptyset$. Considérant $x \in F$, on obtient $F = \mathcal{C}_{\mathcal{R}}(x)$ et donc $F \in E/\mathcal{R}$.

On vérifie ensuite que $E/\mathcal{R} \subset \mathcal{F}$: si $G \in E/\mathcal{R}$, il existe $x \in E$ tel que $G = \mathcal{C}_{\mathcal{R}}(x)$. Par ailleurs, il existe $F \in \mathcal{F}$ tel que $x \in F$. On en tire $F = \mathcal{C}_{\mathcal{R}}(x) = G$, de sorte que $G \in \mathcal{F}$. □

3 Construction de $\mathbb{Z}$

3.1 Introduction

Si un ensemble E est muni d'une loi interne $*$ associative :

$$\forall x \in E, \forall y \in E, \forall z \in E, \quad (x * y) * z = x * (y * z) \ ,$$

admettant un élément neutre e :

$$\forall x \in E, \quad x * e = e * x = x \ ,$$

et telle que tout élément admette un symétrique pour cette loi :

$$\forall x \in E, \exists x' \in E, \quad x * x' = x' * x = e \ ,$$

on dit que $(E, *)$ est un *groupe*. Le groupe est dit *commutatif* lorsque la loi $*$ est commutative :

$$\forall x \in E, \forall y \in E, \quad x * y = y * x \ .$$

Une propriété importante est que dans un groupe, tout élément est *régulier*, c'est-à-dire que tout élément x vérifie :

$$\begin{cases} \forall y \in E, \forall z \in E, & x * y = x * z \implies y = z \\ \forall y \in E, \forall z \in E, & y * x = z * x \implies y = z \end{cases}$$

Cette propriété est importante car elle permet d'effectuer des simplifications lorsqu'on résout des équations. On la prouve en utilisant l'existence de l'élément symétrique x' de x : on écrit par exemple

$$x*y = x*z \implies x'*(x*y) = (x'*x)*z \implies (x'*x)*y = (x'*x)*z \implies e*y = e*z \implies y = z \ .$$

Revenons à l'ensemble des entiers naturels. L'addition dans $\mathbb{N}$ est associative et admet 0 pour élément neutre. Mais $(\mathbb{N}, +)$ n'est pas un groupe, car 0 est le seul élément admettant un élément symétrique (on a vu en TD que $\forall (n, p) \in \mathbb{N} \times \mathbb{N}, \quad n + p = 0 \implies n = p = 0$). Cependant, on a la proposition suivante.

Proposition 3.1 *Tout élément de $\mathbb{N}$ est régulier pour l'addition.*

Preuve - On raisonne par récurrence. En effet il s'agit de montrer (compte tenu de la commutativité de l'addition) que pour tout entier n, la propriété

$$\mathcal{H}_n \ : \quad \forall p \in \mathbb{N}, \forall q \in \mathbb{N}, \quad p+n = q+n \implies p = q$$

est vraie.

• $\mathcal{H}_0$ est vraie du fait que 0 est élément neutre.

• Supposons que $\mathcal{H}_n$ soit vraie pour un certain $n \in \mathbb{N}$. Montrons que $\mathcal{H}_{n+1}$ est vraie. Considérons deux entiers p et q tels que $p+(n+1) = q+(n+1)$. On tire de l'associativité de l'addition que $(n+p)+1 = (n+q)+1$ c'est-à-dire $s(n+p) = s(n+q)$ (où s désigne l'application « successeur »). Comme l'application s est injective, on a nécessairement $n+p = n+q$. On peut alors conclure grâce à $\mathcal{H}_n$ que $p = q$. On a ainsi établi que $\mathcal{H}_{n+1}$ est vraie.

Finalement, le principe de récurrence permet de conclure : $\mathcal{H}_n$ est vraie pour tout $n \in \mathbb{N}$. □

On cherche à construire un ensemble $\mathbb{Z} \supset \mathbb{N}$, muni d'une loi interne qui en fasse un groupe, et qui coïncide avec l'addition lorsqu'on l'applique à des entiers naturels.

La construction va utiliser la remarque suivante.

Si n, p sont deux entiers naturels, on a vu que la différence $n-p$ (c'est-à-dire l'entier k tel que $n = p+k$) est définie seulement dans le cas où $p \leq n$.

De plus, lorsque $p \leq n$ et $p' \leq n'$, on a l'équivalence suivante :

$$n-p = n'-p' \quad \iff \quad n+p' = n'+p \ .$$

En effet, notons $k = n-p$.

Si $n-p = n'-p'$, alors $n' = p'+k$ et donc $n+p' = p+k+p' = p+n'$.

Réciproquement, si $n+p' = n'+p$, on peut écrire $p+k+p' = n'+p$, c'est-à-dire $(p'+k)+p = n'+p$: par usage de la proposition 3.1 (p est régulier), on obtient $n' = p'+k$, soit $n'-p' = n-p$..

On remarque cependant que, contrairement au membre de gauche qui ne peut prendre de sens que pour $p \leq n$ et $p' \leq n'$, le membre de droite a un sens quelque soit l'ordre des entiers p, n (et p', n').

3.2 Définition de $\mathbb{Z}$

On définit sur $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ la relation $\mathcal{R}$ par

$$\forall (n,p) \in \mathbb{N}^2, \forall (n',p') \in \mathbb{N}^2, \quad (n,p) \ \mathcal{R} \ (n',p') \iff n+p' = n'+p \ .$$

Proposition 3.2 *La relation $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{N}^2$.*

Preuve - Le réflexivité et la symétrie sont immédiates. Vérifions la transitivité.

Soient (n,p), (n',p') et (n'',p'') trois éléments de $\mathbb{N}^2$ tels que (n,p) $\mathcal{R}$ (n',p') et (n',p') $\mathcal{R}$ (n'',p''). On a alors

$$n+p' = n'+p \qquad \text{et} \qquad n'+p'' = n''+p' \ ,$$

d'où en ajoutant membre à membre, $n + p'' + (n' + p') = n'' + p + (n' + p')$. Comme $n' + p'$ est régulier pour l'addition (proposition 3.1), on en tire $n + p'' = n'' + p$, c'est-à-dire $(n, p)\ \mathcal{R}\ (n'', p'')$. □

Définition - L'ensemble quotient $\mathbb{N}^2/\mathcal{R}$ est noté $\mathbb{Z}$ et ses éléments sont appelés les *entiers relatifs.*

Exemples - Le couple d'entiers naturels $(1, 4)$ définit l'entier relatif

$$C_{\mathcal{R}}((1,4)) = \{(0,3),\ (1,4),\ (2,5),\ \ldots\} = \{(k, k+3),\ k \in \mathbb{N}\}\ ,$$

et le couple $(0, 0)$ définit l'entier relatif $C_{\mathcal{R}}((0,0)) = \{\{(k,k),\ k \in \mathbb{N}\}$.

3.3 Addition dans $\mathbb{Z}$

On commence par définir l'addition dans $\mathbb{N}^2$, à partir de celle de $\mathbb{N}$. Pour tous (a, b) et (c, d) dans $\mathbb{N}^2$, on pose

$$(a, b) + (c, d) = (a + c, b + d)\ .$$

Proposition 3.3 *L'addition ainsi définie dans* $\mathbb{N}^2$ *est associative, commutative et admet le couple* $(0, 0)$ *pour élément neutre.*

Preuve - Cela découle directement des propriétés de l'addition dans $\mathbb{N}$. □

Une propriété *essentielle* pour la suite de la construction est la suivante.

Proposition 3.4 *La relation* $\mathcal{R}$ *est* COMPATIBLE *avec l'addition dans* $\mathbb{N}^2$ *: si les couples* (a, b), (a', b'), (c, d), (c', d') *vérifient* $(a, b)\,\mathcal{R}\,(a', b')$ *et* $(c, d)\,\mathcal{R}\,(c', d')$, *alors*

$$[(a, b) + (c, d)]\,\mathcal{R}\,[(a', b') + (c', d')]\ .$$

Preuve - Si $(a, b)\,\mathcal{R}\,(a', b')$ et $(c, d)\,\mathcal{R}\,(c', d')$, on a $a + b' = a' + b$ et $c + d' = c' + d$. En ajoutant membre à membre ces deux égalités, on obtient :

$$(a + c) + (b' + d') = (a' + c') + (b + d)\ ,$$

c'est-à-dire $(a + c, b + d)\,\mathcal{R}\,(a' + c', b' + d')$. □

Cela signifie que si on fixe deux entiers relatifs n et p dans $\mathbb{Z}$, on peut choisir n'importe quel représentant $(a, b) \in \mathbb{N}^2$ de n (c'est-à-dire n'importe quel couple d'entiers naturels (a, b) tel que $n = C_{\mathcal{R}}((a, b))$) et n'importe quel représentant (c, d) de p (c'est-à-dire n'importe quel couple (c, d) tel que $n = C_{\mathcal{R}}((c, d))$), la somme $(a + c, b + d)$ définira toujours la *même* classe d'équivalence $C_{\mathcal{R}}((a + c, b + d))$.

Il est alors possible de définir l'addition de deux entiers relatifs de la façon suivante.

Définition - Soient n, p deux entiers relatifs et (a, b), (c, d) des représentants respectifs de n et p. On pose

$$n + p = C_{\mathcal{R}}((a + c, b + d))\ .$$

Proposition 3.5 *L'addition ainsi définie dans* $\mathbb{Z}$ *est commutative, associative et admet la classe* $C_{\mathcal{R}}((0, 0))$ *pour élément neutre. De plus, tout entier relatif admet un élément symétrique pour l'addition (qu'on appelle son* opposé*).*

Autrement dit, $(\mathbb{Z}, +)$ *est un groupe commutatif.*

Preuve - Les trois premières propriétés découlent de la proposition 3.3.

L'existence de l'élément symétrique d'un entier relatif s'obtient en remarquant que pour tout $(a,b) \in \mathbb{N}^2$, $(a,b)+(b,a) = (a+b, a+b)$ et que $(a+b, a+b)\,\mathcal{R}\,(0,0)$. Ainsi on a $C_{\mathcal{R}}((a,b)) + C_{\mathcal{R}}((b,a)) = C_{\mathcal{R}}((0,0))$: la classe de (b,a) est l'opposée de la classe de (a,b). □

3.4 Écriture canonique des entiers relatifs

Proposition 3.6 *Tout entier relatif admet un* unique *représentant dont au moins l'un des termes est nul.*

Preuve - Soit $n = C_{\mathcal{R}}((a,b))$ un entier relatif. S'il admet un représentant de la forme $(m,0)$, cela signifie que $a+0 = m+b$. Cela suppose donc que $b \leq a$, et dans ce cas on a nécessairement $m = a-b$.

Si n admet un représentant de la forme $(0,m)$, cela signifie que $a+m = 0+b$. Cela suppose donc que $a \leq b$, et dans ce cas m vaut nécessairement $b-a$.

Finalement, comme $\leq$ est une relation d'ordre total sur $\mathbb{N}$, on a nécessairement $a \leq b$ ou $b \leq a$. Si $b \leq a$, alors $n = C_{\mathcal{R}}(a-b,0))$, et si $a \leq b$, alors $n = C_{\mathcal{R}}(0,b-a))$. □

Notations - Pour tout $m \in \mathbb{N}$, la classe $C_{\mathcal{R}}(m,0)$ est notée $+m$, et la classe $C_{\mathcal{R}}(0,m)$ est notée $-m$. Dans les deux cas, m est appelé la *valeur absolue* de l'entier relatif, et on écrit

$$m = |+m| = |-m| \,.$$

Remarque - Les notations précédentes donnent pour $m=0$, $C_{\mathcal{R}}(0,0) = +0 = -0$. Et 0 est le seul entier naturel m tel que $+m = -m$. En effet, si m vérifie $+m = -m$, on a $C_{\mathcal{R}}((m,0)) = C_{\mathcal{R}}((0,m))$, c'est-à-dire $m+m=0$. Mais alors $m=0$ (on a vu en TD que dans $\mathbb{N}$, $k+m=0 \Longrightarrow k=m=0$). On convient alors de noter plus simplement 0 la classe de $(0,0)$, qui coïncide avec $+0$ et -0. On est désormais en mesure de définir les notations classiques

$$\mathbb{Z}^+ = \{+m,\ m \in \mathbb{N}\},\ \mathbb{Z}^- = \{-m,\ m \in \mathbb{N}\},\ \mathbb{Z}^{+*} = \{+m,\ m \in \mathbb{N}^*\},\ \mathbb{Z}^{-*} = \{-m,\ m \in \mathbb{N}^*\}\,.$$

Proposition 3.7 *(i) On a* $\mathbb{Z}^+ \cup \mathbb{Z}^- = \mathbb{Z}$, $\mathbb{Z}^+ \cap \mathbb{Z}^- = \{0\}$.

(ii) Les ensembles $\mathbb{Z}^+$ *et* $\mathbb{Z}^-$ *sont stables par l'addition.*

Preuve - Le point (i) provient de la proposition 3.6 : tout entier relatif n s'écrit $+m$ ou $-m$ avec $m \in \mathbb{N}$, et s'il peut s'écrire à la fois $+m$ et $-m'$, on a $C_{\mathcal{R}}((m,0)) = C_{\mathcal{R}}((0,m'))$ d'où $m+m'=0$, ce qui impose $m=m'=0$ et donc $n=0$.

Le point (ii) signifie que pour tous n, p dans $\mathbb{Z}$,

$$n \in \mathbb{Z}^+ \text{ et } p \in \mathbb{Z}^+ \implies n+p \in \mathbb{Z}^+\,, \qquad n \in \mathbb{Z}^- \text{ et } p \in \mathbb{Z}^- \implies n+p \in \mathbb{Z}^-\,.$$

Cela découle du fait que pour tous m, m' dans $\mathbb{N}$,

$$(m,0)+(m',0) = (m+m',0)\,, \qquad (0,m)+(0,m') = (0,m+m')\,, \tag{2}$$

par définition de l'addition dans $\mathbb{N}^2$. □

La proposition suivante permet d'*identifier* les éléments de $\mathbb{Z}^+$ et ceux de $\mathbb{N}$.

Proposition 3.8 *L'application* $\varphi : \begin{pmatrix} \mathbb{N} & \to & \mathbb{Z}^+ \\ m & \mapsto & +m \end{pmatrix}$ *est une bijection qui vérifie*

$$\forall m \in \mathbb{N},\ \forall m' \in \mathbb{N}, \quad \varphi(m+m') = \varphi(m) + \varphi(m')\ .$$

On dit que φ *est un* isomorphisme *de* $(\mathbb{N}, +)$ *sur* $(\mathbb{Z}^+, +)$.

Preuve - L'application φ est bien bijective, car pour tout $n \in \mathbb{Z}^+$, il existe un unique $m \in \mathbb{N}$ tel que $n = C_{\mathcal{R}}((m,0))$, d'après la preuve de la proposition 3.6. L'égalité proposée provient simplement de la première égalité dans (2). □

Notation - Finalement, on pourra écrire pour tout $m \in \mathbb{N}$, $m = +m = |+m| = |-m|$.

3.5 Différence de deux entiers relatifs

On introduit d'abord la notation $(-n)$ pour l'opposé de l'entier relatif n (cette notation est bien cohérente avec les notions précédemment introduites : si $n \in \mathbb{N}$, $-n$ est l'entier relatif opposé de $+n$, que l'on a identifié avec n lui-même).

Proposition 3.9 *Pour* n *et* p *dans* $\mathbb{Z}$*, il existe un unique élément* d *de* $\mathbb{Z}$ *tel que* $p = n+d$*. Cet élément est la somme de* p *et de l'opposé de* n *:* $d = p + (-n)$.

Preuve - Le nombre $d = p + (-n)$ convient puisque $n + (p + (-n)) = (n + (-n)) + p = 0 + p = p$. C'est le seul possible car si d' vérifie $p = n + d'$, on a $n + d' = n + d$ et donc $d' = d$. □

Définition - Le nombre d défini ci-dessus est appelé la *différence* de p et n et noté $p - n$.

Remarques - a) Notez que le symbole « $-$ » recouvre trois sens bien distincts :
- dans l'écriture -3, c'est le *signe* de l'entier relatif $C_{\mathcal{R}}((0,3))$,
- dans l'écriture $-n$ (où $n \in \mathbb{Z}$) il sert à désigner l'*opposé* de n,
- dans l'écriture $p - n$, il désigne la *différence* de p et n.

b) La proposition 3.9 est en fait valable dans n'importe quel *groupe commutatif* dont la loi est notée additivement.

Proposition 3.10 *Pour tout* $(n,p) \in \mathbb{Z}^2$*, on a* $-(n+p) = (-n)+(-p)$ *et* $n-p = -(p-n)$.

Preuve - Soient $(n,p) \in \mathbb{Z}^2$. L'entier $-(n) + (-p)$ est bien l'opposé de $n + p$ puisque $(n+p) + (-n) + (-p) = n + (-n) + p + (-p) = (n + (-n)) + (p + (-p)) = 0 + 0 = 0$.

De même $n - p$ est bien l'opposé de $p - n$ car

$$(n-p) + (p-n) = n + (-p) + p + (-n) = (n + (-n)) + ((-p) + p) = 0 + 0 = 0\ . \quad \square$$

3.6 Multiplication dans $\mathbb{Z}$

La méthode choisie dans ce cours pour définir la multiplication dans $\mathbb{Z}$ correspond à l'introduction qui est faite au collège (une deuxième méthode, fondée sur un procédé analogue à celui utilisé pour la construction de l'addition, est proposée en appendice).

Les entiers relatifs n et p étant donnés, on définit leur produit $q = np$ en précisant sa valeur absolue et son signe :

- $|q| = |n|.|p|$,
- Si $(n,p) \in (\mathbb{Z}^+)^2 \cup (\mathbb{Z}^-)^2$, alors $q \in \mathbb{Z}^+$; si $(n,p) \in (\mathbb{Z}^+ \times \mathbb{Z}^-) \cup (\mathbb{Z}^- \times \mathbb{Z}^+)$, alors $q \in \mathbb{Z}^-$.

La proposition suivante résume les propriétés de cette opération.

Proposition 3.11 *a) La multiplication dans $\mathbb{Z}$ prolonge celle de $\mathbb{N}$.*

b) La multiplication dans $\mathbb{Z}$ est commutative, associative et distributive par rapport à l'addition. Elle admet le nombre $1 = +1 = C_{\mathcal{R}}((1,0))$ pour élément neutre.

c) Les nombres 1 et -1 sont les seuls éléments de $\mathbb{Z}$ admettant un symétrique pour la multiplication.

d) Pour tout n et p dans $\mathbb{Z}$, $np = 0 \Longrightarrow n = 0$ ou $p = 0$.

e) Pour tout n, p, q dans $\mathbb{Z}$, $n.0 = 0$, $n(-p) = -(np)$ et $n(p-q) = np - nq$.

f) Tout élément non nul de $\mathbb{Z}$ est régulier pour la multiplication :

$$\forall n \in \mathbb{Z}^*,\ \forall p \in \mathbb{Z},\ \forall q \in \mathbb{Z}, \quad np = nq \Longrightarrow p = q\ .$$

Remarques - L'ensemble $\mathbb{Z}$ est muni des deux lois internes $+$ et $\times$ qui vérifient : $(\mathbb{Z}, +)$ est un groupe commutatif, et la loi $\times$ est associative et distributive par rapport à l'addition. On traduit ceci en disant que $(\mathbb{Z}, +, \times)$ est un *anneau*. Cet anneau est dit *commutatif* du fait que la loi $\times$ est commutative, et *unitaire* du fait qu'elle admet un élément neutre. Enfin on traduit la propriété d) en disant que $\mathbb{Z}$ est un anneau *intègre*.

Preuve de la proposition 3.11 - a) Ce point découle directement de la définition de la multiplication et de l'identification entre $\mathbb{N}$ et $\mathbb{Z}^+$.

b) La commutativité se lit directement sur la définition. Pour montrer l'associativité, on observe que si n, p, q sont trois entiers relatifs, les entiers relatifs $(np)q$ et $n(pq)$ ont la mème valeur absolue :

$$|(np)q| = |np|\,|q| = (|n|\,|p|)\,|q| = |n|\,(|p|\,|q|) = |n|\,|pq| = |n(pq)|\ ,$$

mais aussi le même signe. Cela se voit en dressant un tableau présentant toutes les combinaisons possibles de signes pour n, p et q :

n	p	q	np	$(np)q$	pq	$n(pq)$
$+$	$+$	$+$	$+$	$+$	$+$	$+$
$+$	$+$	$-$	$+$	$-$	$-$	$-$
$+$	$-$	$+$	$-$	$-$	$-$	$-$
$+$	$-$	$-$	$-$	$+$	$+$	$+$
$-$	$+$	$+$	$-$	$-$	$+$	$-$
$-$	$+$	$-$	$-$	$+$	$-$	$+$
$-$	$-$	$+$	$+$	$+$	$-$	$+$
$-$	$-$	$-$	$+$	$-$	$+$	$-$

La distributivité est plus fastidieuse à démontrer : il faut d'abord établir que si n et p sont deux entiers relatifs de même signe, alors $|n+p| = |n| + |p|$ et si ce sont des entiers relatifs de signes contraires, alors $|n+p| = ||n| - |p||$. Pour cela il suffit de remarquer que

- si $(n,p) \in (\mathbb{Z}^+)^2$, on a $n = |n|$, $p = |p|$ et $n + p \in \mathbb{Z}^+$, donc $|n+p| = n + p = |n| + |p|$;
- si $(n,p) \in (\mathbb{Z}^-)^2$, on a $n = -|n|$, $p = -|p|$ et $n+p \in \mathbb{Z}^-$, donc $|n+p| = -(n+p) = |n|+|p|$;

- si $(n,p) \in \mathbb{Z}^+ \times \mathbb{Z}^-$, on a $n = |n|$, $p = -|p|$ donc $|n+p| = ||n| - |p||$.

Ensuite on montre que pour n, p, q dans $\mathbb{Z}$, $n(p+q) = np + nq$ en détaillant tous les cas de figure dépendant des signes de n, p, q. Par exemple, lorsque tous trois sont positifs, on remarque que les nombres $n(p+q)$ et $np+nq$ sont tous deux positifs (car n, $p+q$, np et nq le sont), puis qu'ils ont même valeur absolue. Ce dernier point s'obtient en utilisant que la valeur absolue d'un produit est le produit des valeurs absolues (définition du produit) et que la valeur absolue de la somme de deux entiers positifs est la somme de leurs valeurs absolues (propriété qu'on vient d'établir) :

$$|n(p+q)| = |n|\,|p+q| = |n|\,(|p| + |q|) = |n||p| + |n||q| = |np| + |nq| = |np + nq|\ .$$

c) et d) proviennent des propriétés suivantes (qu'il faudrait établir...) de la multiplication dans $\mathbb{N}$: $[mm' = 0 \Longrightarrow m = 0$ ou $m' = 0]$ et $[mm' = 1 \Longrightarrow m = m' = 1]$ (raisonner sur les valeurs absolues de n, p et np).

e) Les deux premières égalités peuvent s'établir facilement à l'aide des valeurs absolues et de la règle des signes. Voici une autre preuve, plus générale, valable dans tout anneau.

Soient $(n,p,q) \in \mathbb{Z}^3$. La distributivité de la multiplication par rapport à l'addition permet d'écrire d'une part $n.0 = n(0+0) = n.0 + n.0$ d'où on tire $n.0 = 0$, et d'autre part

$$np + n(-p) = n(p + (-p)) = n \times 0 = 0\ ,$$

ce qui montre que $n(-p)$ est bien l'opposé de np.

La troisième égalité s'obtient en écrivant :

$$n(p-q) = n(p + (-q)) = np + n(-q) = np + (-(nq)) = np - nq\ .$$

On a utilisé successivement la définition de la différence, la distributivité de la multiplication par rapport à l'addition, et la propriété qui vient d'être établie.

f) est une conséquence de d) et e) : plus généralement, dans un anneau intègre, tout élément non nul est régulier pour la multiplication. Pour le voir il suffit d'écrire que $np = nq$ entraîne $np - nq = 0$ et donc $n(p-q) = 0$ (d'après e)), puis de déduire de d) que $n \neq 0$ implique $p - q = 0$. □

3.7 Relation d'ordre sur $\mathbb{Z}$

On définit ainsi la relation $\leq$ sur $\mathbb{Z}$:

$$\forall n \in \mathbb{Z},\ \forall p \in \mathbb{Z}, \quad n \leq p \iff p - n \in \mathbb{Z}^+\ .$$

Proposition 3.12 *La relation $\leq$ est une relation d'ordre total sur $\mathbb{Z}$, compatible avec l'addition et la multiplication par un entier positif.*

Preuve - La relation $\leq$ est réflexive, car pour tout $n \in \mathbb{Z}$, $n - n = 0 \in \mathbb{Z}^+$, donc $n \leq n$.

Elle est antisymétrique car $n \leq p$ et $p \leq n$ entraînent d'une part $p - n \in \mathbb{Z}^+$ et d'autre part $n - p \in \mathbb{Z}^+$ d'où $p - n = -(n-p) \in \mathbb{Z}^-$; alors $p - n \in \mathbb{Z}^+ \cap \mathbb{Z}^- = \{0\}$ soit $p = n$.

Elle est transitive car si $n \leq p$ et $p \leq q$, on a $p - n \in \mathbb{Z}^+$ et $q - p \in \mathbb{Z}^+$, donc $q - n = (q-p) + (p-n) \in \mathbb{Z}^+$, c'est-à-dire que $n \leq q$.

C'est donc une relation d'ordre, et cet ordre est total car $\mathbb{Z} = \mathbb{Z}^+ \cup \mathbb{Z}^-$, donc pour n et p dans $\mathbb{Z}$ on a $p - n \in \mathbb{Z}^+$ (et alors $n \leq p$) ou $p - n \in \mathbb{Z}^-$ (et alors $n - p \in \mathbb{Z}^+$ d'où $p \leq n$).

Elle est compatible avec l'addition et la multiplication par un entier positif, car si les entiers n et p vérifient $n \leq p$, on a

- pour tout q dans $\mathbb{Z}$, $(p+q)-(n+q) = p-n \in \mathbb{Z}^+$ donc $n+q \leq p+q$,
- pour tout r dans $\mathbb{Z}^+$, $rp - rn = r(p-n) \in \mathbb{Z}^+$ donc $rn \leq rp$. □

Annexe A

Appendice

On présente dans cet appendice des compléments, non exposés dans le cours.

1 Une autre construction de la multiplication dans $\mathbb{Z}$

Il s'agit d'utiliser le même procédé que lors de la construction de l'addition. On définit d'abord une opération convenable sur $\mathbb{N}^2$, qu'on notera aussi multiplicativement. Mais celle-ci est définie de façon moins immédiate que l'addition. On souhaite en effet que cette multiplication dans $\mathbb{N}^2$ soit distributive par rapport à l'addition, mais aussi qu'elle conduise aux résultats attendus suivants, correspondant à la « règle des signes » :

$$(m,0)\times(m',0) = (0,m)\times(0,m') = (mm',0)\ ,$$

$$(m,0)\times(0,m') = (0,m)\times(m',0) = (0,mm')\ .$$

Ces contraintes imposent alors pour tous (a,b) et (a',b') dans $\mathbb{N}^2$:

$$\begin{aligned}(a,b)\times(c,d) &= [(a,0)+(0,b)]\times[(c,0)+(0,d)]\\ &= (a,0)\times(c,0)+(a,0)\times(0,d)+(0,b)\times(c,0)+(0,b)\times(0,d)\\ &= (ac,0)+(0,ad)+(0,cb)+(bd,0)\\ &= (ac+bd,ad+cb)\ ,\end{aligned}$$

d'où la définition suivante.

On pose pour tous (a,b), (c,d) dans $\mathbb{N}^2$, $(a,b)\times(c,d) = (ac+bd, ad+bc)$.

Proposition 1.1 *La multiplication définie ci-dessus est commutative, associative et distributive par rapport à l'addition (de $\mathbb{N}^2$). Elle admet le couple $(1,0)$ pour élément neutre.*

Preuve - La commutativité et le fait que $(1,0)$ soit élément neutre se voient directement sur la définition. L'associativité et la distributivité par rapport à l'addition demandent plus d'efforts. On considère trois couples d'entiers (a,b), (c,d) et (e,f), et on vérifie d'une

part que

$$\begin{aligned}
[(a,b)\times(c,d)]\times(e,f) &= (ac+bd,ad+bc)\times(e,f)\\
&= ((ac+bd)e+(ad+bc)f,(ac+bd)f+(ad+bc)e)\\
&= (ace+bde+adf+bcf,acf+bdf+ade+bce)\\
&= (a(ce+df)+b(cf+de),a(cf+de)+b(ce+df))\\
&= (a,b)\times(ce+df,cf+de)\\
&= (a,b)\times[(c,d)\times(e,f)]\,,
\end{aligned}$$

et d'autre part que

$$\begin{aligned}
(a,b)\times[(c,d)+(e,f)] &= (a,b)\times(c+e,d+f)\\
&= (a(c+e)+b(d+f),a(d+f)+b(c+e))\\
&= (ac+ae+bd+bf,ad+af+bc+be)\\
&= (ac+bd,ad+bc)+(ae+bf,af+be)\\
&= [(a,b)\times(c,d)]+[(a,b)\times(e,f)]\,.
\end{aligned}$$

Comme dans le cas de l'addition, il faut se préoccuper de la propriété suivante.

Proposition 1.2 *La relation $\mathcal{R}$ est compatible avec la multiplication dans $\mathbb{N}^2$: si les couples (a,b), (a',b'), (c,d), (c',d') vérifient $(a,b)\,\mathcal{R}\,(a',b')$ et $(c,d)\,\mathcal{R}\,(c',d')$, alors*

$$[(a,b)\times(c,d)]\,\mathcal{R}\,[(a',b')\times(c',d')]\,.$$

Preuve - Si $(a,b)\,\mathcal{R}\,(a',b')$ et $(c,d)\,\mathcal{R}\,(c',d')$, on a $a+b'=a'+b$ et $c+d'=c'+d$.

On commence par établir que $[(a,b)\times(c,d)]\,\mathcal{R}\,[(a',b')\times(c,d)]$. Pour cela on tire de la relation $a+b'=a'+b$ les deux égalités

$$ac+b'c=a'c+bc \quad \text{et} \quad a'd+bd=ad+b'd\,,$$

que l'on ajoute membre à membre : $(ac+bd)+(b'c+a'd)=(a'c+b'd)+(ad+bc)$. Cela exprime que

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

c'est-à-dire la relation cherchée.

La multiplication dans $\mathbb{N}^2$ étant commutative, on peut réutiliser ce résultat et déduire de la relation $(c,d)\,\mathcal{R}\,(c',d')$ que $[(a',b')\times(c,d)]\,\mathcal{R}\,[(a',b')\times(c',d')]$. On achève alors la preuve grâce à la transitivité de la relation $\mathcal{R}$: $[(a,b)\times(c,d)]\,\mathcal{R}\,[(a',b')\times(c,d)]$ et $[(a',b')\times(c,d)]\,\mathcal{R}\,[(a',b')\times(c',d')]$ entraînent $[(a,b)\times(c,d)]\,\mathcal{R}\,[(a',b')\times(c',d')]$. □

On peut alors procéder comme on l'a fait pour l'addition.

Définition - Soient n, p deux entiers relatifs, et (a,b), (c,d) des représentants respectifs de n et p. On pose

$$np=C_{\mathcal{R}}((ac+bd,ad+bc))\,.$$

On établit enfin l'ensemble des propriétés attendues de la multiplication.

Proposition 1.3 *a) La multiplication sur $\mathbb{Z}$ prolonge celle de $\mathbb{N}$.*

b) La multiplication dans $\mathbb{Z}$ est commutative, associative, distributive par rapport à l'addition et admet le nombre $1 = +1 = C_{\mathcal{R}}((1,0))$ pour élément neutre.

c) Pour tous $n \in \mathbb{Z}$ et $p \in \mathbb{Z}$:

- $|np| = |n|\,|p|$,

- si $(n,p) \in (\mathbb{Z}^+)^2 \cup (\mathbb{Z}^-)^2$, alors $np \in \mathbb{Z}^+$,

- si $(n,p) \in (\mathbb{Z}^+ \times \mathbb{Z}^-) \cup (\mathbb{Z}^- \times \mathbb{Z}^+)$, alors $np \in \mathbb{Z}^-$.

d) Les entiers relatifs 1 et -1 sont les seuls éléments de $\mathbb{Z}$ qui admettent un symétrique pour la multiplication.

e) L'anneau $\mathbb{Z}$ est intègre.

f) Pour tout n, p, q dans $\mathbb{Z}$, $\quad n.0 = 0, \quad n(-p) = -(np) \quad$ et $\quad n(p-q) = np - nq$.

g) Tout élément <u>non nul</u> de $\mathbb{Z}$ est régulier *pour la multiplication.*

Preuve - a) provient du fait que pour tout a, c dans $\mathbb{N}$, $(a,0) \times (c,0) = (ac,0)$.

b) est une conséquence de la proposition 1.1.

c) En posant $m = |n|$, $m' = |p|$ et en appliquant la définition du produit, on obtient $np = +mm'$ lorsque $(n,p) \in (\mathbb{Z}^+)^2 \cup (\mathbb{Z}^-)^2$, et $np = -mm'$ lorsque $(n,p) \in (\mathbb{Z}^+ \times \mathbb{Z}^-) \cup (\mathbb{Z}^- \times \mathbb{Z}^+)$.

d), e), f) et g) se démontrent comme les points c), d), e), f) de la proposition 3.11. □

2 Construction de $\mathbb{Q}$

2.1 Définition de $\mathbb{Q}$

On a vu que dans $\mathbb{Z}$, seuls deux éléments (1 et -1) admettent un *inverse* (c'est-à-dire un symétrique pour la multiplication).

On cherche à construire un ensemble $\mathbb{Q} \supset \mathbb{Z}$, muni de deux lois internes, qui coïncident avec l'addition et la multiplication déjà définies lorsqu'on les applique à des entiers relatifs, et qui *en plus* de toutes les propriétés énoncées ci-dessus pour les opérations dans $\mathbb{Z}$, permettent d'attribuer à tout élément <u>non nul</u> un inverse.

Pour cela, on s'inspire de l'écriture attendue des rationnels comme quotients d'entiers : on veut que les fractions $\dfrac{p}{q}$ et $\dfrac{p'}{q'}$ soient égales si et seulement si $pq' = p'q$.

On définit donc la relation $\mathcal{S}$ sur $\mathbb{Z} \times \mathbb{Z}^*$ par

$$\forall (p,q) \in \mathbb{Z} \times \mathbb{Z}^*, \forall (p',q') \in \mathbb{Z} \times \mathbb{Z}^*, \quad (p,q)\ \mathcal{S}\ (p',q') \iff pq' = p'q\ .$$

Notez la similitude de cette définition avec celle de la relation $\mathcal{R}$ qui a servi à définir $\mathbb{Z}$.

Proposition 2.1 *La relation $\mathcal{S}$ est une relation d'équivalence sur $\mathbb{Z} \times \mathbb{Z}^*$.*

Preuve - Comme pour la proposition 3.2, la réflexivité et la symétrie sont immédiates. Détaillons la transitivité.

Soient (p,q), (p',q') et (p'',q'') trois éléments de $\mathbb{Z} \times \mathbb{Z}^*$ tels que $(p,q)\ \mathcal{S}\ (p',q')$ et $(p',q')\ \mathcal{S}\ (p'',q'')$. On a alors d'une part $pq' = p'q$, d'où l'on tire $pq'q'' = p'qq''$, et d'autre part $p'q'' = p''q'$ qui permet d'écrire $p'q''q = p''q'q$. en observant les deux égalités obtenues, on obtient $pq'q'' = p''q'q$ soit $(pq'')q' = (p''q)q'$. Or q' est régulier pour la multiplication puisqu'il est non nul (cf. proposition 3.11). On a donc $pq'' = p''q$ c'est-à-dire $(p,q)\ \mathcal{S}\ (p'',q'')$. □

Définition - L'ensemble quotient $(\mathbb{Z}\times\mathbb{Z}^*)/\mathcal{S}$ est noté $\mathbb{Q}$ et ses éléments sont appelés les *nombres rationnels*. La classe d'équivalence d'un couple (p,q) de $\mathbb{Z}\times\mathbb{Z}^*$ pour la relation $\mathcal{S}$ se note sous forme fractionnaire $C_{\mathcal{S}}((p,q)) = \dfrac{p}{q}$.

Exemples - Le couple d'entiers relatif $(-1,4)$ définit le rationnel $\dfrac{-1}{4}$ c'est-à-dire

$$C_{\mathcal{S}}(-1,4) = \{(-1,4),\ (1,-4),\ (-2,8),\ (2,-8),\ (-3,12),(3,-12),\ \ldots\} = \{(-k,4k),\ k\in\mathbb{Z}^*\}\ ,$$

et les couples $(0,1)$ et $(1,1)$ définissent respectivement les rationnels

$$\frac{0}{1} = C_{\mathcal{R}}(0,1) = \{(0,k),\ k\in\mathbb{Z}^*\} \quad \text{et} \quad \frac{1}{1} = C_{\mathcal{R}}(1,1) = \{(k,k),\ k\in\mathbb{Z}^*\}\ .$$

2.2 Multiplication dans $\mathbb{Q}$

La construction est analogue à celle de l'addition dans $\mathbb{Z}$. On commence par définir une multiplication sur $\mathbb{Z}\times\mathbb{Z}^*$, en posant pour tous (p,q) et (p',q') dans $\mathbb{Z}\times\mathbb{Z}^*$:

$$(p,q)\times(p',q') = (pp',qq')\ .$$

Les entiers relatifs q et q' étant tous deux non nuls, le produit qq' est bien dans $\mathbb{Z}^*$.

Proposition 2.2 *La multiplication ainsi définie dans $\mathbb{Z}\times\mathbb{Z}^*$ est commutative, associative, et admet le couple $(1,1)$ pour élément neutre.*

Preuve - Cela découle directement des propriétés de la multiplication dans $\mathbb{Z}$. □

Puis on établit la propriété suivante.

Proposition 2.3 *La relation $\mathcal{S}$ est compatible avec la multiplication dans $\mathbb{Z}\times\mathbb{Z}^*$: si les couples (a,b), (a',b'), (c,d), (c',d') vérifient $(a,b)\,\mathcal{S}\,(a',b')$ et $(c,d)\,\mathcal{S}\,(c',d')$, alors*

$$[(a,b)\times(c,d)]\,\mathcal{S}\,[(a',b')\times(c',d')]\ .$$

Preuve - Si $(a,b)\,\mathcal{S}\,(a',b')$ et $(c,d)\,\mathcal{S}\,(c',d')$, on a $ab' = a'b$ et $cd' = c'd$. En multipliant membre à membre ces deux égalités, on obtient :

$$(ac)(b'd') = (a'c')(bd)\ ,$$

c'est-à-dire $(ac,bd)\,\mathcal{S}\,(a'c',b'd')$. □

Il est alors possible de définir la multiplication de deux rationnels de la façon suivante.

Définition - Soient x, y deux rationnels, et (a,b), (c,d) des représentants respectifs de x et y. On pose

$$xy = C_{\mathcal{S}}((ac,bd)) \text{ c'est-à-dire } \frac{a}{b}\times\frac{c}{d} = \frac{ac}{bd}\ .$$

Proposition 2.4 *La multiplication ainsi définie dans $\mathbb{Q}$ est commutative, associative et admet le rationnel $\dfrac{1}{1} = C_{\mathcal{S}}((1,1))$ pour élément neutre. De plus, tout rationnel non nul admet un élément symétrique pour la multiplication (qu'on appelle son* inverse*).*

En particulier, $(\mathbb{Q}^*,\times)$ est un groupe commutatif.

Preuve - Les trois premières propriétés découlent de la proposition 2.2.

L'existence de l'élément symétrique d'un rationnel non nul s'obtient en remarquant que pour tout $(a,b)\in\mathbb{Z}^*\times\mathbb{Z}^*$, $(a,b)\times(b,a) = (ab,ab)$ et que $(ab,ab)\,\mathcal{S}\,(1,1)$. Autrement dit l'inverse du rationnel non nul $\dfrac{a}{b}$ est le rationnel $\dfrac{b}{a}$. □

2.3 Addition dans $\mathbb{Q}$

Là encore, on définit d'abord une opération, notée additivement, dans $\mathbb{Z} \times \mathbb{Z}^*$. Pour qu'elle corresponde à l'addition des fractions (avec la réduction au même dénominateur), on pose pour (a, b) et (c, d) dans $\mathbb{Z} \times \mathbb{Z}^*$:

$$(a, b) + (c, d) = (ad + bc, bd) \ .$$

Proposition 2.5 *L'addition ainsi définie dans $\mathbb{Z} \times \mathbb{Z}^*$ est commutative, associative et admet le couple $(0, 1)$ pour élément neutre.*

Preuve - La commutativité et le fait que $(0, 1)$ soit élément neutre sont immédiats. Montrons l'associativité. Soient (a, b), (c, d) et (e, f) trois éléments de $\mathbb{Z} \times \mathbb{Z}^*$.

$$\begin{aligned}
[(a, b) + (c, d)] + (e, f) &= (ad + bc, bd) + (e, f) \\
&= ((ad + bc)f + bde, bdf) \\
&= (adf + b(cf + de), bdf) \\
&= (a, b) + (cf + de, df) \\
&= (a, b) + [(c, d) + (e, f)] \ .
\end{aligned}$$

Proposition 2.6 *La relation $\mathcal{S}$ est compatible avec l'addition dans $\mathbb{Z} \times \mathbb{Z}^*$: si les couples (a, b), (a', b'), (c, d), (c', d') vérifient $(a, b)\,\mathcal{S}\,(a', b')$ et $(c, d)\,\mathcal{S}\,(c', d')$, alors*

$$[(a, b) + (c, d)]\,\mathcal{S}\,[(a', b') + (c', d')] \ .$$

Preuve - Comme $(a, b)\,\mathcal{S}\,(a', b')$ et $(c, d)\,\mathcal{S}\,(c', d')$, on a $ab' - a'b = cd' - c'd = 0$. Par ailleurs, $(a, b) + (c, d) = (ad + bc, bd)$ et $(a', b') + (c', d') = (a'd' + b'c', b'd')$. En calculant

$$(ad + bc)b'd' - (a'd' + b'c')bd = (ab' - a'b)dd' + (cd' - c'd)bb' = 0 \ ,$$

on voit que $(ad + bc, bd)\,\mathcal{S}\,(a'd' + b'c', b'd')$. □

On peut donc définir une addition sur $\mathbb{Q}$ en posant

$$C_{\mathcal{S}}((a, b)) + C_{\mathcal{S}}((c, d)) = C_{\mathcal{S}}((a, b) + (c, d)))$$

c'est-à-dire

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \ .$$

Proposition 2.7 *L'addition ainsi définie dans $\mathbb{Q}$ est commutative, associative et admet le rationnel $\dfrac{0}{1} = C_{\mathcal{S}}((0, 1))$ pour élément neutre. De plus, tout rationnel admet un élément symétrique pour l'addition (qu'on appelle son* opposé*), et la multiplication dans $\mathbb{Q}$ est distributive par rapport à l'addition.*

Preuve - Les trois premières propriétés découlent de la proposition 2.5.

L'existence de l'élément symétrique d'un rationnel s'obtient en remarquant que pour tout $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, $(a, b) + (-a, b) = (ab + (-a)b, b^2) = (0, b^2)$ et que $(0, b^2)\,\mathcal{S}\,(0, 1)$. Ainsi on a $C_{\mathcal{S}}((a, b)) + C_{\mathcal{S}}((-a, b)) = C_{\mathcal{S}}((0, 1))$: le rationnel $\dfrac{-a}{b}$ est l'opposée de $\dfrac{a}{b}$.

Pour établir la distributivité, on calcule

$$(a,b)[(c,d)+(e,f)] = (a,b)(cf+de,df) = (acf+ade,bdf)$$

puis

$$(a,b)(c,d)+(a,b)(e,f) = (ac,bd)+(ae,bf) = (b(acf+ade),b(bdf)) \ .$$

On en tire que $(a,b)[(c,d)+(e,f)]\,\mathcal{S}\,[(a,b)(c,d)+(a,b)(e,f)]$ ce qui traduit bien que $\frac{a}{b}\left(\frac{c}{d}+\frac{e}{f}\right) = \frac{a}{b}\frac{c}{d}+\frac{a}{b}\frac{e}{f}$. □

Remarque - Finalement $(\mathbb{Q},+,\times)$ est un anneau unitaire tel que tout élément non nul admet un inverse : on dit que $(\mathbb{Q},+,\times)$ est un *corps*. De plus ce corps est dit commutatif du fait que la multiplication est commutative.

La proposition suivante permet d'identifier $\mathbb{Z}$ au sous-ensemble $A = \left\{\frac{p}{1}\ ;\ p\in\mathbb{Z}\right\}$ de $\mathbb{Q}$ et montre que les opérations définies sur $\mathbb{Q}$ prolongent celles de $\mathbb{Z}$.

Proposition 2.8 *L'ensemble A est stable pour l'addition et la multiplication de $\mathbb{Q}$ et l'application ψ : $\begin{pmatrix} \mathbb{Z} & \to & A \\ p & \mapsto & p/1 \end{pmatrix}$ est un isomorphisme de $(\mathbb{Z},+,\times)$ sur $(A,+,\times)$.*

Preuve - La stabilité s'obtient en calculant pour p et q dans $\mathbb{Z}$:

$$\frac{p}{1}+\frac{q}{1} = \frac{p.1+1.q}{1^2} = \frac{p+q}{1} \text{ et } \frac{p}{1}\times\frac{q}{1} = \frac{pq}{1^2} = \frac{pq}{1} \ .$$

Ces calculs montrent au passage que $\psi(p+q)=\psi(p)+\psi(q)$ et $\psi(pq)=\psi(p).\psi(q)$. Pour voir que l'application ψ est un isomorphisme, il ne reste qu'à montrer qu'elle est bijective. Elle est surjective par construction, et injective du fait que $\psi(p)=\psi(q)$ entraîne $p\times 1 = 1\times q$ c'est-à-dire $p=q$. □

2.4 Relation d'ordre sur $\mathbb{Q}$

On commence par définir les ensembles $\mathbb{Q}^+$ et $\mathbb{Q}^-$.

Proposition 2.9 *Soient $x\in\mathbb{Q}$ et $(a,b)\in\mathbb{Z}\times\mathbb{Z}^*$ tel que $x=\frac{a}{b}$.*
- Ou bien $a=0$. Tout autre représentant (a',b') de x vérifie alors $a'=0$.
- Ou bien $ab\in\mathbb{Z}^{+*}$. Tout autre représentant (a',b') de x vérifie alors $a'b'\in\mathbb{Z}^{+*}$.
- Ou bien $ab\in\mathbb{Z}^{-*}$. Tout autre représentant (a',b') de x vérifie alors $a'b'\in\mathbb{Z}^{-*}$.

Preuve - Comme $b\neq 0$, les trois cas $ab=0$, $ab\in\mathbb{Z}^{+*}$ et $ab\in\mathbb{Z}^{-*}$ conduisent aux trois situations envisagées dans la proposition.

Considérons un couple (a',b') de $\mathbb{Z}\times\mathbb{Z}^*$ tel que $x=\frac{a'}{b'}$ c'est-à-dire tel que $ab'=a'b$.

Si $a=0$, on a nécessairement $a'b=0$ et donc $a'=0$.

Lorsque $a\neq 0$, le produit $aa'bb'$ est le carré de l'entier non nul ab' et est donc dans $\mathbb{Z}^{+*}$.

Si $ab\in\mathbb{Z}^{+*}$, on a nécessairement $a'b'\in\mathbb{Z}^{+*}$ puisque sinon $aa'bb'$ serait dans $\mathbb{Z}^{-*}$.

On montre de même que si $ab\in\mathbb{Z}^{-*}$, alors $a'b'\in\mathbb{Z}^{-*}$. □

Avec les notations de la proposition précédente, le fait que $a = 0$, $ab \in \mathbb{Z}^{+*}$ ou $ab \in \mathbb{Z}^{-*}$ est indépendant du représentant (a, b) choisi pour le rationnel x. Le premier cas est caractéristique de $x = 0$. On appelle $\mathbb{Q}^{+*}$ l'ensemble des rationnels x qui vérifient la deuxième propriété et $\mathbb{Q}^{-*}$ l'ensemble des rationnels x qui vérifient la troisième. Ainsi les ensembles $\{0\}$, $\mathbb{Q}^{+*}$ et $\mathbb{Q}^{-*}$ constituent une partition de $\mathbb{Q}$.

On pose $\mathbb{Q}^{+} = \mathbb{Q}^{+*} \cup \{0\}$ et $\mathbb{Q}^{-} = \mathbb{Q}^{-*} \cup \{0\}$.

On peut alors procéder comme on l'a fait pour $\mathbb{Z}$ au paragraphe 3.7 du chapitre III. On note $(-x)$ l'opposé d'un rationnel x, puis on définit la différence $y - x = y + (-x)$ de deux rationnels x et y (comme dans la proposition 3.9), qui vérifie les mêmes propriétés que dans $\mathbb{Z}$ (proposition 3.10 et distributivité de la multiplication sur la soustraction énoncée à la proposition 3.11-e).

On définit alors la relation $\leq$ ainsi : pour x, y dans $\mathbb{Q}$,

$$x \leq y \Longleftrightarrow y - x \in \mathbb{Q}^{+} \ .$$

Proposition 2.10 *La relation $\leq$ ainsi définie est une relation d'ordre total sur $\mathbb{Q}$, compatible avec l'addition et la multiplication par un rationnel positif.*

Preuve - La preuve est la même que dans $\mathbb{Z}$ (cf proposition 3.12 du chapitre III). Pour la développer, on a besoin d'établir que $\mathbb{Q}^{+}$ est stable pour l'addition et la multiplication.

Cela vient de ce que si (a, b) et (c, d) sont des éléments de $\mathbb{Z} \times \mathbb{Z}^{*}$ tels que $ab \in \mathbb{Z}^{+}$ et $cd \in \mathbb{Z}^{+}$, alors d'une part la fraction $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{ad + bc}{bd}$ vérifie

$$(ad + bc)bd = (ab)d^2 + b^2(cd) \in \mathbb{Z}^{+} \ .$$

Et d'autre part la fraction $\dfrac{a}{b} \times \dfrac{c}{d} = \dfrac{ac}{bd}$ vérifie $(ac)(bd) = (ab)(cd) \in \mathbb{Z}^{+}$. □