Chapitre 4

L'ensemble $\mathbb{Z}$ des entiers relatifs

4.1 Une construction de l'ensemble $\mathbb{Z}$

4.1.1 Proposition

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

$$\left(\forall\,(n,p) \in \mathbb{N}^2\right)\left(\forall\,(n',p') \in \mathbb{N}^2\right)\left((n,p)\,\mathcal{R}\,(n',p') \Longleftrightarrow n+p' = n'+p\right)$$

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

Démonstration

1. De manière évidente, **cette relation est réflexive.**
   En effet, soit $(n,p) \in \mathbb{N}^2$; alors $n+p = n+p$ et donc $(n,p)\,\mathcal{R}\,(n,p)$
2. De même, **cette relation est symétrique**
   Soient $(n,p) \in \mathbb{N}^2$ et $(n',p') \in \mathbb{N}^2$ tels que $(n,p)\,\mathcal{R}\,(n',p')$ alors $n+p' = n'+p$ et $n'+p = n+p'$, c'est à dire $(n',p')\,\mathcal{R}\,(n,p)$
3. Et pour terminer, soient $(n,p) \in \mathbb{N}^2$, $(n',p') \in \mathbb{N}^2$ et $(n'',p'') \in \mathbb{N}^2$ tels que $(n,p)\,\mathcal{R}\,(n',p')$ et $(n',p')\,\mathcal{R}\,(n'',p'')$.
   Alors $n+p' = n'+p$ et $n'+p'' = n''+p'$ et donc, $n+p'+n'+p'' = n'+p+n''+p'$, c'est à dire, par régularité de l'addition dans $\mathbb{N}$ *(cf point 1-d de2.1.1)*, $n+p'' = n''+p$, c'est à dire $(n,p)\,\mathcal{R}\,(n'',p'')$
   La **relation est donc transitive**

La relation $\mathcal{R}$ est bien une relation d'équivalence sur $\mathbb{N}^2$

Remarque 1 :

On peut remarquer que $(n,p)\,\mathcal{R}\,(n',p)$ veut dire que $n-p = n'-p'$....sauf que la soustraction n'est pas définie sur $\mathbb{N}$ *(Donc, patience ! !)*

4.1.2 Définition

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

Remarque 2 :

1. Rappelons que l'ensemble quotient est un ensemble de classes d'équivalence
2. Pour $(n,p) \in \mathbb{N}^2$, nous notons $\mathcal{C}_{\mathcal{R}}\left[(n,p)\right]$, la classe d'équivalence modulo $\mathcal{R}$ du couple (n,p), c'est à dire :
$$\mathcal{C}_{\mathcal{R}}\left[(n,p)\right] = \left\{(a,b) \in \mathbb{N}^2 \text{ tels que } (n,p)\,\mathcal{R}\,(a,b)\right\}$$

3. Ainsi :
   - ▷ La classe d'équivalence du couple d'entiers naturels $(1,4)$ définit l'entier relatif
   $$\mathcal{C}_{\mathcal{R}}\left[(1,4)\right]=\left\{(a,b)\in\mathbb{N}^2 \text{ tels que } (1,4)\,\mathcal{R}\,(a,b)\right\}=\{(k,k+3) \text{ avec } k\in\mathbb{N}\}$$
   - ▷ La classe d'équivalence du couple d'entiers naturels $(7,2)$ définit l'entier relatif
   $$\mathcal{C}_{\mathcal{R}}\left[(7,2)\right]=\left\{(a,b)\in\mathbb{N}^2 \text{ tels que } (7,2)\,\mathcal{R}\,(a,b)\right\}=\{(k+5,k) \text{ avec } k\in\mathbb{N}\}$$
   - ▷ La classe d'équivalence du couple d'entiers naturels $(0,0)$ définit l'entier relatif
   $$\mathcal{C}_{\mathcal{R}}\left[(0,0)\right]=\left\{(a,b)\in\mathbb{N}^2 \text{ tels que } (0,0)\,\mathcal{R}\,(a,b)\right\}=\{(k,k) \text{ avec } k\in\mathbb{N}\}$$

4.1.3 Définition et proposition

1. Définition de l'addition dans $\mathbb{N}^2$
   Pour tout $(a,b)\in\mathbb{N}^2$ et tout $(c,d)\in\mathbb{N}^2$, nous avons :
   $$(a,b)+(c,d)=(a+c,b+d)$$
   Cette addition est associative, commutative et possède un élément neutre : $(0,0)$
2. La relation d'équivalence $\mathcal{R}$ est compatible avec l'addition de $\mathbb{N}^2$
   C'est à dire que pour $(a,b)\in\mathbb{N}^2$, $(a_1,b_1)\in\mathbb{N}^2$, $(c,d)\in\mathbb{N}^2$ et $(c_1,d_1)\in\mathbb{N}^2$, si $(a,b)\,\mathcal{R}\,(c,d)$ et $(a_1,b_1)\,\mathcal{R}\,(c_1,d_1)$, alors :
   $$(a,b)+(a_1,b_1)\,\mathcal{R}\,(c,d)+(c_1,d_1)\Longleftrightarrow(a+a_1,b+b_1)\,\mathcal{R}\,(c+c_1,d+d_1)$$

Démonstration

1. La démonstration du premier point est simple et laissée aux lecteurs. Il suffit d'utiliser les propriétés de l'addition dans $\mathbb{N}$. A ce sujet, il faut bien voir que le signe d'addition dans $(a,b)+(c,d)$ est un signe d'addition dans $\mathbb{N}^2$, alors que le signe addition dans les composantes du couple $(a+c,b+d)$ sont des additions dans $\mathbb{N}$
2. Soient $(a,b)\in\mathbb{N}^2$, $(a_1,b_1)\in\mathbb{N}^2$, $(c,d)\in\mathbb{N}^2$ et $(c_1,d_1)\in\mathbb{N}^2$, tels que $(a,b)\,\mathcal{R}\,(c,d)$ et $(a_1,b_1)\,\mathcal{R}\,(c_1,d_1)$, alors :
   - ▷ $(a,b)\,\mathcal{R}\,(c,d)\Longleftrightarrow a+d=b+c$
   - ▷ $(a_1,b_1)\,\mathcal{R}\,(c_1,d_1)\Longleftrightarrow a_1+d_1=b_1+c_1$

   En additionnant, nous obtenons :
   $$(a+d)+(a_1+d_1)=(b+c)+(b_1+c_1)\Longleftrightarrow(a+a_1)+(d+d_1)=(b+b_1)+(c+c_1)$$
   C'est à dire $(a+a_1,b+b_1)\,\mathcal{R}\,(c+c_1,d+d_1)$

4.1.4 Addition dans $\mathbb{Z}=\mathbb{N}^2/\mathcal{R}$

1. Définition de l'addition dans $\mathbb{Z}$
   Soient $(a,b)\in\mathbb{N}^2$ et $(c,d)\in\mathbb{N}^2$ de classe d'équivalence modulo $\mathcal{R}$, $\mathcal{C}_{\mathcal{R}}\left[(a,b)\right]$ et $\mathcal{C}_{\mathcal{R}}\left[(c,d)\right]$.
   Nous définissons ainsi l'addition dans $\mathbb{Z}$ par :
   $$\mathcal{C}_{\mathcal{R}}\left[(a,b)\right]+\mathcal{C}_{\mathcal{R}}\left[(c,d)\right]=\mathcal{C}_{\mathcal{R}}\left[(a+c,b+d)\right]$$
2. Si nous fixons deux entiers relatifs n et p dans $\mathbb{Z}$, nous pouvons choisir n'importe quel représentant $(a,b)\in\mathbb{N}^2$ de n
   C'est-à-dire que n'importe quel couple d'entiers naturels $(a,b)\in\mathbb{N}^2$ tel que $n=\mathcal{C}_{\mathcal{R}}\left[(a,b)\right]$ et n'importe quel représentant $(c,d)\in\mathbb{N}^2$ de p tel que $p=\mathcal{C}_{\mathcal{R}}\left[(c,d)\right]$, la somme $(a+c,b+d)$ définira toujours la même classe d'équivalence $\mathcal{C}_{\mathcal{R}}\left[(a+c,b+d)\right]=n+p$

Démonstration

Soit $n \in \mathbb{Z}$ et $p \in \mathbb{Z}$, $(a,b) \in \mathbb{N}^2$ et $(c,d) \in \mathbb{N}^2$ tels que $n = \mathcal{C}_{\mathcal{R}}[(a,b)]$ et $p = \mathcal{C}_{\mathcal{R}}[(c,d)]$.
Alors, par définition de l'addition dans $\mathbb{Z}$, $n+p = \mathcal{C}_{\mathcal{R}}[(a,b)] + \mathcal{C}_{\mathcal{R}}[(c,d)] = \mathcal{C}_{\mathcal{R}}[(a+c,b+d)]$
Soit $(a_1,b_1) \in \mathbb{N}^2$ tel que $(a_1,b_1)\,\mathcal{R}\,(a,b)$, c'est à dire que $\mathcal{C}_{\mathcal{R}}[(a,b)] = \mathcal{C}_{\mathcal{R}}[(a_1,b_1)] = n$
De même, soit $(c_1,d_1) \in \mathbb{N}^2$ tel que $(c_1,d_1)\,\mathcal{R}\,(c,d)$, c'est à dire que $\mathcal{C}_{\mathcal{R}}[(c,d)] = \mathcal{C}_{\mathcal{R}}[(c_1,d_1)] = p$. Alors :

$$n+p = \mathcal{C}_{\mathcal{R}}[(a,b)] + \mathcal{C}_{\mathcal{R}}[(c,d)] = \mathcal{C}_{\mathcal{R}}[(a+c,b+d)] = \mathcal{C}_{\mathcal{R}}[(a_1,b_1)] + \mathcal{C}_{\mathcal{R}}[(c_1,d_1)] = \mathcal{C}_{\mathcal{R}}[(a_1+c_1,b_1+d_1)]$$

Comme $(a_1,b_1)\,\mathcal{R}\,(a,b)$ et $(c_1,d_1)\,\mathcal{R}\,(c,d)$, alors, d'après 4.1.3, nous avons $(a_1+c_1,b_1+d_1)\,\mathcal{R}\,(a+c,b+d)$, c'est à dire $\mathcal{C}_{\mathcal{R}}[(a_1+c_1,b_1+d_1)] = \mathcal{C}_{\mathcal{R}}[(a+c,b+d)] = n+p$.
La somme est donc indépendante du représentant choisi.

4.1.5 Proposition :$(\mathbb{Z},+)$ est un groupe commutatif.

L'addition définie dans $\mathbb{Z}$ en 4.1.4 est commutative, associative et admet la classe $\mathcal{C}_{\mathcal{R}}[(0,0)]$ 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.

Démonstration

1. Démontrons la commutativité
   Soient $n \in \mathbb{Z}$, $p \in \mathbb{Z}$, $(a,b) \in \mathbb{N}^2$ et $(c,d) \in \mathbb{N}^2$ tels que $n = \mathcal{C}_{\mathcal{R}}[(a,b)]$ et $p = \mathcal{C}_{\mathcal{R}}[(c,d)]$.
   Alors :

   $$n+p = \mathcal{C}_{\mathcal{R}}[(a,b)]+\mathcal{C}_{\mathcal{R}}[(c,d)] = \mathcal{C}_{\mathcal{R}}[(a+c,b+d)] = \mathcal{C}_{\mathcal{R}}[(c+a,d+b)] = \mathcal{C}_{\mathcal{R}}[(c,d)]+\mathcal{C}_{\mathcal{R}}[(a,b)] = p+n$$

   L'addition est donc commutative
2. Démontrons l'associativité
   Soient $n \in \mathbb{Z}$ $m \in \mathbb{Z}$, $p \in \mathbb{Z}$, $(a,b) \in \mathbb{N}^2$, $(c,d) \in \mathbb{N}^2$ et $(e,f) \in \mathbb{N}^2$ tels que $n = \mathcal{C}_{\mathcal{R}}[(a,b)]$, $m = \mathcal{C}_{\mathcal{R}}[(c,d)]$ et $p = \mathcal{C}_{\mathcal{R}}[(e,f)]$; alors :

   $$\begin{aligned} n+(m+p) &= \mathcal{C}_{\mathcal{R}}[(a,b)] + (\mathcal{C}_{\mathcal{R}}[(c,d)] + \mathcal{C}_{\mathcal{R}}[(e,f)]) \\ &= \mathcal{C}_{\mathcal{R}}[(a,b)] + \mathcal{C}_{\mathcal{R}}[(c+e,d+f)] \\ &= \mathcal{C}_{\mathcal{R}}[(a+c+e,b+d+f)] = \mathcal{C}_{\mathcal{R}}[((a+c)+e,(b+d)+f)] \\ &= (\mathcal{C}_{\mathcal{R}}[(a+c,b+d)]) + \mathcal{C}_{\mathcal{R}}[(e,f)] \\ &= (\mathcal{C}_{\mathcal{R}}[(a,b)] + \mathcal{C}_{\mathcal{R}}[(c,d)]) + \mathcal{C}_{\mathcal{R}}[(e,f)] \\ &= (n+m)+p \end{aligned}$$

   Nous avons donc $n+(m+p) = (n+m)+p$ et l'addition est bien associative sur $_Z$
3. Recherche de l'élément neutre
   Nous n'allons pas chercher très loin!! Il est évident que $\mathcal{C}_{\mathcal{R}}[(0,0)]$ est l'élément neutre pour l'addition
4. Recherche de l'élément symétrique
   Soit $(a,b) \in \mathbb{N}^2$ et $n = \mathcal{C}_{\mathcal{R}}[(a,b)]$.
   Il est donc évident que $n_1 = \mathcal{C}_{\mathcal{R}}[(b,a)]$ est tel que

   $$n+n_1 = \mathcal{C}_{\mathcal{R}}[(a,b)] + \mathcal{C}_{\mathcal{R}}[(b,a)] = \mathcal{C}_{\mathcal{R}}[(a+b,a+b)] = \mathcal{C}_{\mathcal{R}}[(0,0)]$$

   Ainsi $n_1 = \mathcal{C}_{\mathcal{R}}[(b,a)]$ est l'opposé de $n = \mathcal{C}_{\mathcal{R}}[(a,b)]$

$(\mathbb{Z},+)$ est donc un groupe commutatif.

4.1.6 Écriture canonique des entiers relatifs

Tout entier relatif $n \in \mathbb{Z}$ admet un unique représentant dont au moins l'un des termes est nul.

Démonstration

Soit $n = \mathcal{C}_{\mathcal{R}}[(a,b)]$ un entier relatif.

- ▷ Si n admet un représentant de la forme $(m,0)$, cela signifie alors que $(a,b)\,\mathcal{R}\,(m,0)$ et donc $a+0=m+b$. Cela suppose donc que $b \leqslant a$, et dans ce cas on a nécessairement $m = a-b$.
- ▷ Si, n admet un représentant de la forme $(0,m)$, cela signifie que alors que $(a,b)\,\mathcal{R}\,(0,m)$ et donc que $a+m=0+b$. Cela suppose donc que $a \leqslant b$, et dans ce cas m vaut nécessairement $b-a$.

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

4.1.7 Notations

1. Pour tout $m \in \mathbb{N}$ la classe $\mathcal{C}_{\mathcal{R}}[(m,0)]$ est notée $+m$, et la classe $\mathcal{C}_{\mathcal{R}}[(0,m)]$ est notée $-m$.
2. Dans les deux cas, m est appelé la valeur absolue de l'entier relatif, et on écrit $m = |+m| = |-m|$

Remarque 3 :

1. Les notations $\mathcal{C}_{\mathcal{R}}[(m,0)] = +m$ et $\mathcal{C}_{\mathcal{R}}[(0,m)] = -m$ ne sont pas si innocentes que cela puisque, pour l'addition dans $\mathbb{Z}$,$\mathcal{C}_{\mathcal{R}}[(m,0)]$ et $\mathcal{C}_{\mathcal{R}}[(0,m)]$ sont symétriques.
2. Les notations précédentes donnent pour $m=0$, $\mathcal{C}_{\mathcal{R}}[(m,0)] = +0 = -0$. Et 0 est le seul entier naturel m tel que $+m = -m$.

   En effet, si m vérifie $+m = -m$, on a $\mathcal{C}_{\mathcal{R}}[(m,0)] = \mathcal{C}_{\mathcal{R}}[(0,m)]$, c'est-à-dire $m+m=0$. Mais alors $m=0$. On convient alors de noter plus simplement 0 la classe de $(0,0)$, qui coïncide avec $+0$ et -0.
3. Nous sommes désormais en mesure de définir les notations classiques

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

4.1.8 Proposition

1. Nous avons $\mathbb{Z} = \mathbb{Z}^+ \cup \mathbb{Z}^-$ et $\mathbb{Z}^+ \cap \mathbb{Z}^- = \{0\}$
2. Les ensembles $\mathbb{Z}^+$ et $\mathbb{Z}^-$ sont stables par l'addition.

Démonstration

1. Démonstration du premier point
   (a) Soit $m \in \mathbb{Z}$.
   → Alors, d'après 4.1.6, il existe $a \in \mathbb{N}$ tel que $m = \mathcal{C}_{\mathcal{R}}[(a,0)]$ ou $m = \mathcal{C}_{\mathcal{R}}[(0,a)]$
   → Donc $m \in \mathbb{Z}^+$ ou $m \in \mathbb{Z}^-$ et donc $m \in \mathbb{Z}^+ \cup \mathbb{Z}^-$. C'est à dire $\mathbb{Z} \subset \mathbb{Z}^+ \cup \mathbb{Z}^-$
   → La démonstration de la réciproque $\mathbb{Z}^+ \cup \mathbb{Z}^- \subset \mathbb{Z}$ est évidente
   Donc $\mathbb{Z} = \mathbb{Z}^+ \cup \mathbb{Z}^-$
   (b) Soit, maintenant $m \in \mathbb{Z}^+ \cap \mathbb{Z}^-$
   Toujours d'après 4.1.6, il existe $a \in \mathbb{N}$ et $b \in \mathbb{N}$ tel que $m = \mathcal{C}_{\mathcal{R}}[(a,0)]$ et $m = \mathcal{C}_{\mathcal{R}}[(0,b)]$
   Nous avons alors $\mathcal{C}_{\mathcal{R}}[(a,0)] = \mathcal{C}_{\mathcal{R}}[(0,b)]$, c'est à dire $(a,0)\,\mathcal{R}\,(0,b)$. Or :
   $$(a,0)\,\mathcal{R}\,(0,b) \iff a+b=0$$
   Comme $a \in \mathbb{N}$ et $b \in \mathbb{N}$, nous avons $a+b=0 \iff a=b=0$ et donc $m = \mathcal{C}_{\mathcal{R}}[(0,0)] = 0$
2. Démonstration du second point
   → Soient $m \in \mathbb{Z}^+$ et $p \in \mathbb{Z}^+$; nous allons monter que $m+p \in \mathbb{Z}^+$
   Il existe $a \in \mathbb{N}$ et $b \in \mathbb{N}$ tels que $m = \mathcal{C}_{\mathcal{R}}[(a,0)]$ et $p = \mathcal{C}_{\mathcal{R}}[(b,0)]$.
   Alors :
   $$m+p = \mathcal{C}_{\mathcal{R}}[(a,0)] + \mathcal{C}_{\mathcal{R}}[(b,0)] = \mathcal{C}_{\mathcal{R}}[(a+b,0)]$$
   Ce qui démontre bien que $m+p \in \mathbb{Z}^+$
   → Nous démontrerions de la même manière que si $m \in \mathbb{Z}^-$ et $p \in \mathbb{Z}^-$ alors $m+p \in \mathbb{Z}^-$

4.1.9 Plongement de $\mathbb{N}$ dans $\mathbb{Z}$

L'application $\Phi : \mathbb{N} \longrightarrow \mathbb{Z}$ définie par :

$$\left\{ \begin{array}{ccc} \Phi : \mathbb{N} & \longrightarrow & \mathbb{Z}^+ \\ n & \longmapsto & \Phi(n) = +n = \mathcal{C}_{\mathcal{R}}[(n,0)] \end{array} \right.$$

est une bijection telle que, pour tout $m \in \mathbb{N}$ et tout $n \in \mathbb{N}$, nous avons $\Phi(m+n) = \Phi(m) + \Phi(n)$

Démonstration

1. L'application Φ est bien bijective
   → Elle est injective
   Supposons en effet que, pour $m \in \mathbb{N}$ et $n \in \mathbb{N}$, nous ayons $\Phi(m) = \Phi(n)$. Alors :
   $$\Phi(m) = \Phi(n) \Longleftrightarrow \mathcal{C}_{\mathcal{R}}[(m,0)] = \mathcal{C}_{\mathcal{R}}[(n,0)] \Longleftrightarrow (m,0)\,\mathcal{R}\,(n,0) \Longleftrightarrow m = n$$
   Φ est donc bien injective
   → L'application Φ est surjective
   Soit $m \in \mathbb{Z}^+$; il existe alors $a \in \mathbb{N}$ tel que $m = \mathcal{C}_{\mathcal{R}}[(a,0)]$ et nous avons alors $\Phi(a) = m$
2. Soient $m \in \mathbb{N}$ et $n \in \mathbb{N}$. Alors :
   $$\Phi(m+n) = \mathcal{C}_{\mathcal{R}}[(m+n,0)] = \mathcal{C}_{\mathcal{R}}[(n,0)] + \mathcal{C}_{\mathcal{R}}[(m,0)] = \Phi(m) + \Phi(n)$$
   Nous avons donc bien $\Phi(m+n) = \Phi(m) + \Phi(n)$

Remarque 4 :

1. La proposition 4.1.9 permet d'identifier $\mathbb{N}$ à $\mathbb{Z}^+$
2. **Notation** : Finalement, nous écrirons, pour tout $m \in \mathbb{N}$, $m = +m = \mathcal{C}_{\mathcal{R}}[(m,0)] = |+m| = |-m|$

4.1.10 Définition

Pour $n \in \mathbb{Z}$, nous notons $-n$ l'opposé de n pour l'addition

Remarque 5 :

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.

4.1.11 Proposition

1. Pour $n \in \mathbb{Z}$ et $p \in \mathbb{Z}$, 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 : $d = p + (-n)$.
2. Le nombre d défini ci-dessus est appelé la différence de p et n et est noté $p - n$.

Démonstration

→ Le nombre $d = p + (-n)$ convient puisque
$$n + (p + (-n)) = (n + (-n)) + p = 0 + p = p$$
→ C'est le seul possible car si d_1 vérifie $p = n + d_1$, nous avons $n + d_1 = n + d$ et donc $d_1 = d$ par régularité.

Remarque 6 :

1. Notez que le symbole « - » recouvre trois sens bien distincts :
   (a) Dans l'écriture -3, c'est le signe de l'entier relatif $\mathcal{C}_{\mathcal{R}}[(0,3)]$
   (b) Dans l'écriture $-n$ (où $n \in \mathbb{Z}$) il sert à désigner l'opposé de n.
   (c) Dans l'écriture $p-n$,il désigne la différence de p et n.
2. La proposition 4.1.11 est en fait valable dans n'importe quel groupe commutatif dont la loi est notée additivement.

4.1.12 Proposition

Pour tout $(n,p) \in \mathbb{Z}^2$, nous avons $-(n+p) = (-n)+(-p)$ et $n-p = -(p-n)$.

Démonstration

Soit $(n,p) \in \mathbb{Z}^2$

1. Alors $(-n)+(-p)$ est l'opposé de $n+p$ puisque
$$(-n)+(-p)+n+p = (-n)+n+(-p)+p = ((-n)+n)+((-p)+p) = 0+0 = 0$$
2. De même $n-p$ est l'opposé de $p-n$ puisque
$$(n-p)+(p-n) = n+(-p)+p+(-n) = (n+(-n))+((-p)+p) = 0+0 = 0$$

4.1.13 Définition d'une multiplication dans $\mathbb{N}^2$

1. Définition de la multiplication dans $\mathbb{N}^2$
   Pour tout $(a,b) \in \mathbb{N}^2$ et tout $(c,d) \in \mathbb{N}^2$, nous avons :
$$(a,b) \times (c,d) = (ac+bd, ad+bc)$$
   Cette multiplication est associative, commutative, possède un élément neutre : $(1,0)$ et est distributive par rapport à l'addition
2. La relation d'équivalence $\mathcal{R}$ est compatible avec la multiplication de $\mathbb{N}^2$
   C'est à dire que pour $(a,b) \in \mathbb{N}^2$, $(a_1,b_1) \in \mathbb{N}^2$, $(c,d) \in \mathbb{N}^2$ et $(c_1,d_1) \in \mathbb{N}^2$, si $(a,b)\,\mathcal{R}\,(c,d)$ et $(a_1,b_1)\,\mathcal{R}\,(c_1,d_1)$, alors :
$$(a,b)\times(a_1,b_1)\,\mathcal{R}\,(c,d)\times(c_1,d_1) \Longleftrightarrow (aa_1+bb_1, ab_1+a_1b)\,\mathcal{R}\,(cc_1+dd_1, cd_1+dc_1)$$

Démonstration

1. Nous laissons la démonstration du premier point aux soins du lecteur. C'est essentiellement calculatoire.
2. Nous allons faire la démonstration du second point en 2 temps.
   - Dans un premier temps, soient $(a,b) \in \mathbb{N}^2$, $(c,d) \in \mathbb{N}^2$ tels que $(a,b)\,\mathcal{R}\,(c,d)$.
     Nous allons démontrer que pour tout couple $(a_1,b_1) \in \mathbb{N}^2$, alors $(a,b)\times(a_1,b_1)\,\mathcal{R}\,(c,d)\times(a_1,b_1)$.
     Nous avons $(a,b)\,\mathcal{R}\,(c,d) \Longleftrightarrow a+d = b+c$ et
$$(a,b)\times(a_1,b_1) = (aa_1+bb_1, ab_1+a_1b) \text{ et } (c,d)\times(a_1,b_1) = (ca_1+db_1, cb_1+a_1d)$$
     Alors :
$$\begin{aligned}(aa_1+bb_1)+(cb_1+a_1d) &= a_1(a+d)+b_1(b+c)\\ &= a_1(b+c)+b_1(a+d) \text{ puisque } a+d=b+c\\ &= a_1b+a_1c+ab_1+b_1d\\ &= (a_1c++b_1d)+(ab_1+a_1b)\end{aligned}$$
     Et nous avons donc bien $(a,b)\times(a_1,b_1)\,\mathcal{R}\,(c,d)\times(a_1,b_1)$

- Soient $(a,b) \in \mathbb{N}^2$, $(a_1,b_1) \in \mathbb{N}^2$, $(c,d) \in \mathbb{N}^2$ et $(c_1,d_1) \in \mathbb{N}^2$ tels que $(a,b)\,\mathcal{R}\,(c,d)$ et $(a_1,b_1)\,\mathcal{R}\,(c_1,d_1)$. Alors, d'après le point précédent :

$$(a,b)\times(a_1,b_1)\,\mathcal{R}\,(c,d)\times(a_1,b_1) \text{ et } (a_1,b_1)\times(c,d)\,\mathcal{R}\,(c_1,d_1)\times(c,d)$$

Et donc, par transitivité, nous avons $(a,b)\times(a_1,b_1)\,\mathcal{R}\,(c,d)\times(c_1,d_1)$

4.1.14 Définition de la multiplication dans $\mathbb{Z}$ et premières propriétés

1. Pour $(a,b) \in \mathbb{N}^2$ et $(c,d) \in \mathbb{N}^2$, nous définissons la multiplication dans $\mathbb{Z}$ par :
$$\mathcal{C}_{\mathcal{R}}[(a,b)] \times \mathcal{C}_{\mathcal{R}}[(c,d)] = \mathcal{C}_{\mathcal{R}}[(a,b)\times(c,d)]$$
2. Cette multiplication est commutative, associative, admet un élément neutre $\mathcal{C}_{\mathcal{R}}[(1,0)]$ et est distributive par rapport à l'addition de $\mathbb{Z}$
3. Comme dans le cas de l'addition, la multiplication est indépendante du représentant choisi.

Démonstration

La démonstration doit beaucoup à 4.1.13 et 4.1.4 et est laissée au lecteur.

4.1.15 Proposition

1. Si $n \in \mathbb{Z}^+$ et $m \in \mathbb{Z}^-$ alors $m \times n \in \mathbb{Z}^-$
2. Si $n \in \mathbb{Z}^-$ et $m \in \mathbb{Z}^-$ alors $m \times n \in \mathbb{Z}^+$
3. Si $n \in \mathbb{Z}^+$ et $m \in \mathbb{Z}^+$ alors $m \times n \in \mathbb{Z}^+$

Démonstration

1. Si $n \in \mathbb{Z}^+$ et $m \in \mathbb{Z}^-$, alors $n = \mathcal{C}_{\mathcal{R}}[(n,0)]$ et $m = \mathcal{C}_{\mathcal{R}}[(0,m)]$. Alors :
$$m \times n = \mathcal{C}_{\mathcal{R}}[(n,0)] \times \mathcal{C}_{\mathcal{R}}[(0,m)] = \mathcal{C}_{\mathcal{R}}[(n,0)\times(0,m)] = \mathcal{C}_{\mathcal{R}}[(0,mn)]$$
Et donc $m \times n \in \mathbb{Z}^-$
2. Si $n \in \mathbb{Z}^-$ et $m \in \mathbb{Z}^-$, alors $n = \mathcal{C}_{\mathcal{R}}[(0,n)]$ et $m = \mathcal{C}_{\mathcal{R}}[(0,m)]$. Alors :
$$m \times n = \mathcal{C}_{\mathcal{R}}[(0,n)] \times \mathcal{C}_{\mathcal{R}}[(0,m)] = \mathcal{C}_{\mathcal{R}}[(0,n)\times(0,m)] = \mathcal{C}_{\mathcal{R}}[(mn,0)]$$
Et donc $m \times n \in \mathbb{Z}^+$
3. Si $n \in \mathbb{Z}^+$ et $m \in \mathbb{Z}^+$, alors $n = \mathcal{C}_{\mathcal{R}}[(n,0)]$ et $m = \mathcal{C}_{\mathcal{R}}[(m,0)]$. Alors :
$$m \times n = \mathcal{C}_{\mathcal{R}}[(n,0)] \times \mathcal{C}_{\mathcal{R}}[(m,0)] = \mathcal{C}_{\mathcal{R}}[(n,0)\times(m,0)] = \mathcal{C}_{\mathcal{R}}[(mn,0)]$$
Et donc $m \times n \in \mathbb{Z}^+$

4.1.16 Théorème

1. $(\mathbb{Z},+,\times)$ est un anneau unitaire commutatif
2. Les nombres 1 et -1 sont les seuls éléments de $\mathbb{Z}^*$ inversibles *(admettant un symétrique pour la multiplication)*.
3. $\mathbb{Z}$ est un anneau intègre, c'est à dire que, pour tout $n\in\mathbb{Z}$ et tout $p\in\mathbb{Z}$:
$$np=0\Longrightarrow n=0 \text{ ou } p=0$$
4. Pour tout $n\in\mathbb{Z}$, tout $p\in\mathbb{Z}$ et tout $q\in\mathbb{Z}$:
$$n\times 0=0,\quad n\left(-p\right)=-\left(np\right) \text{ et } n\times(p-q)=np-nq$$
5. Tout élément non nul de $\mathbb{Z}$ est régulier pour la multiplication, c'est à dire :
$$\left(\forall n\in\mathbb{Z}^*\right),\left(\forall p\in\mathbb{Z}\right),\left(\forall q\in\mathbb{Z}\right),\left((np=nq)\Longrightarrow(p=q)\right)$$

Démonstration

La plupart des démonstrations de ce théorème utilisent les propriétés des entiers de l'ensemble $\mathbb{N}$ vues au chapitre 2

1. On montre que $(\mathbb{Z},+,\times)$ est un anneau unitaire
   ▷ D'après 4.1.5, on sait que $(\mathbb{Z},+)$ est un groupe commutatif
   ▷ D'après 4.1.14, la multiplication est commutative, associative, admet un élément neutre $1=\mathcal{C}_{\mathcal{R}}\left[(1,0)\right]$ et est distributive par rapport à l'addition de $\mathbb{Z}$
   Donc $(\mathbb{Z},+,\times)$ est un anneau unitaire commutatif
2. On montre que 1 et -1 sont les seuls éléments inversibles de $\mathbb{Z}^*$
   Soit $n\in\mathbb{Z}^*$ que nous supposons inversible et $(a,b)\in\mathbb{N}^2$, avec $a\neq b$, tel que $p=\mathcal{C}_{\mathcal{R}}\left[(a,b)\right]$ soit l'inverse de n
   → Supposons $a>b$, alors $p=\mathcal{C}_{\mathcal{R}}\left[(a,b)\right]=\mathcal{C}_{\mathcal{R}}\left[(a-b,0)\right]$; alors $p\in\mathbb{N}^*$ et $p=\mathcal{C}_{\mathcal{R}}\left[(p,0)\right]$.
   ▷ Supposons que $n\in\mathbb{Z}^{*+}$ et que $n=\mathcal{C}_{\mathcal{R}}\left[(n,0)\right]$ Alors :
$$\begin{aligned}n\times p=1 &\Longleftrightarrow \mathcal{C}_{\mathcal{R}}\left[(n,0)\right]\times\mathcal{C}_{\mathcal{R}}\left[(p,0)\right]=\mathcal{C}_{\mathcal{R}}\left[(1,0)\right]\\ &\Longleftrightarrow \mathcal{C}_{\mathcal{R}}\left[(np,0)\right]=\mathcal{C}_{\mathcal{R}}\left[(1,0)\right]\end{aligned}$$
   Ce qui signifie que $(np,0)\,\mathcal{R}\,(1,0)$, c'est à dire $np=1$ et donc $n=p=1$
   Nous en concluons que si $n\in\mathbb{Z}^{*+}$ est inversible, alors $n=1$ et son inverse p est telque $p=n=1$
   ▷ Supposons que $n\in\mathbb{Z}^{*-}$ et que $n=\mathcal{C}_{\mathcal{R}}\left[(0,-n)\right]$ Alors :
$$\begin{aligned}n\times p=1 &\Longleftrightarrow \mathcal{C}_{\mathcal{R}}\left[(0,-n)\right]\times\mathcal{C}_{\mathcal{R}}\left[(p,0)\right]=\mathcal{C}_{\mathcal{R}}\left[(1,0)\right]\\ &\Longleftrightarrow \mathcal{C}_{\mathcal{R}}\left[(0,(-n)\,p)\right]=\mathcal{C}_{\mathcal{R}}\left[(1,0)\right]\end{aligned}$$
   Ce qui signifie que $(0,(-n)\,p)\,\mathcal{R}\,(1,0)$, c'est à dire $0=1+(-n)\,p$ et donc $(-n)\,p=-1$, ce qui est impossible puisque $-n\in\mathbb{Z}^{*+}$ et $p\in\mathbb{Z}^{*+}$
   → Supposons $a<b$, alors $p=\mathcal{C}_{\mathcal{R}}\left[(a,b)\right]=\mathcal{C}_{\mathcal{R}}\left[(0,b-a)\right]$; alors $p\in\mathbb{Z}^{-}$ et $p=\mathcal{C}_{\mathcal{R}}\left[(0,-p)\right]$.
   ▷ Supposons que $n\in\mathbb{Z}^{*+}$ et que $n=\mathcal{C}_{\mathcal{R}}\left[(n,0)\right]$ Alors :
$$\begin{aligned}n\times p=1 &\Longleftrightarrow \mathcal{C}_{\mathcal{R}}\left[(n,0)\right]\times\mathcal{C}_{\mathcal{R}}\left[(0,-p)\right]=\mathcal{C}_{\mathcal{R}}\left[(1,0)\right]\\ &\Longleftrightarrow \mathcal{C}_{\mathcal{R}}\left[(0,(-p)\,n)\right]=\mathcal{C}_{\mathcal{R}}\left[(1,0)\right]\end{aligned}$$
   Ce qui signifie que $(0,(-p)\,n)\,\mathcal{R}\,(1,0)$, c'est à dire $0=1+(-p)\,n$ et donc $(-p)\,n=-1$, ce qui est impossible puisque $n\in\mathbb{Z}^{*+}$ et $p\in\mathbb{Z}^{*-}$
   ▷ Supposons que $n\in\mathbb{Z}^{*-}$ et que $n=\mathcal{C}_{\mathcal{R}}\left[(0,-n)\right]$ Alors :
$$\begin{aligned}n\times p=1 &\Longleftrightarrow \mathcal{C}_{\mathcal{R}}\left[(0,-n)\right]\times\mathcal{C}_{\mathcal{R}}\left[(0,-p)\right]=\mathcal{C}_{\mathcal{R}}\left[(1,0)\right]\\ &\Longleftrightarrow \mathcal{C}_{\mathcal{R}}\left[((-n)\,(-p)\,,0)\right]=\mathcal{C}_{\mathcal{R}}\left[(1,0)\right]\end{aligned}$$

Ce qui signifie que $((-n)(-p),0)\,\mathcal{R}\,(1,0)$, c'est à dire $(-n)(-p)=1$ et donc $-n=1 \iff n=-1$ et $-p=1 \iff p=-1$
Nous en concluons que si $n\in\mathbb{Z}^{*-}$ est inversible, alors $n=-1$ et son inverse p est tel que $p=n=-1$
Ce que nous voulions

3. On démontre que $\mathbb{Z}$ est un anneau intègre
Soient $n\in\mathbb{Z}$ et $p\in\mathbb{Z}$ tels que $np=0$
▷ Supposons $n\in\mathbb{Z}^+$ et $p\in\mathbb{Z}^+$, alors $n=\mathcal{C}_{\mathcal{R}}[(n,0)]$ et $p=\mathcal{C}_{\mathcal{R}}[(p,0)]$ et nous avons alors :

$$\begin{aligned}\mathcal{C}_{\mathcal{R}}[(n,0)]\times\mathcal{C}_{\mathcal{R}}[(p,0)]=\mathcal{C}_{\mathcal{R}}[(0,0)] &\iff \mathcal{C}_{\mathcal{R}}[(n,0)\times(p,0)]=\mathcal{C}_{\mathcal{R}}[(0,0)]\\ &\iff \mathcal{C}_{\mathcal{R}}[(np,0)]=\mathcal{C}_{\mathcal{R}}[(0,0)]\end{aligned}$$

Ce qui veut dire que $(np,0)\,\mathcal{R}\,(0,0)$, autrement dit $np=0$.
D'après les propriétés de $\mathbb{N}$, alors, $n=0$ ou $p=0$
▷ La démonstration est tout à fait semblable si nous supposons $n\in\mathbb{Z}^-$ et $p\in\mathbb{Z}^-$.
En effet, dans ce cas, $n=\mathcal{C}_{\mathcal{R}}[(0,-n)]$ et $p=\mathcal{C}_{\mathcal{R}}[(0,-p)]$ et nous avons alors :

$$\begin{aligned}\mathcal{C}_{\mathcal{R}}[(0,-n)]\times\mathcal{C}_{\mathcal{R}}[(0,-p)]=\mathcal{C}_{\mathcal{R}}[(0,0)] &\iff \mathcal{C}_{\mathcal{R}}[(0,-n)\times(0,-p)]=\mathcal{C}_{\mathcal{R}}[(0,0)]\\ &\iff \mathcal{C}_{\mathcal{R}}[((-n)(-p),0)]=\mathcal{C}_{\mathcal{R}}[(0,0)]\end{aligned}$$

Ce qui veut dire que $((-n)(-p),0)\,\mathcal{R}\,(0,0)$, autrement dit $(-n)(-p)=0$.
D'après les propriétés de $\mathbb{N}$, alors, $(-n)=0$ ou $(-p)=0$, ce qui est équivalent à $n=0$ ou $p=0$
▷ Supposons $n\in\mathbb{Z}^-$ et $p\in\mathbb{Z}^+$, alors $n=\mathcal{C}_{\mathcal{R}}[(0,-n)]$ et $p=\mathcal{C}_{\mathcal{R}}[(p,0)]$ et nous avons alors :

$$\begin{aligned}\mathcal{C}_{\mathcal{R}}[(0,-n)]\times\mathcal{C}_{\mathcal{R}}[(p,0)]=\mathcal{C}_{\mathcal{R}}[(0,0)] &\iff \mathcal{C}_{\mathcal{R}}[(0,-n)\times(p,0)]=\mathcal{C}_{\mathcal{R}}[(0,0)]\\ &\iff \mathcal{C}_{\mathcal{R}}[(0,(-n)p)]=\mathcal{C}_{\mathcal{R}}[(0,0)]\end{aligned}$$

Ce qui veut dire que $(0,(-n)p)\,\mathcal{R}\,(0,0)$, autrement dit $(-n)p=0$.
D'après les propriétés de $\mathbb{N}$, alors, $(-n)=0$ ou $p=0$, autrement dit $n=0$ ou $p=0$
$\mathbb{Z}$ est bien un anneau intègre

4. ▷ Montrons que $n\times 0=0$
Nous avons $n\times 0=n\times(0+0)$.
Par la distributivité, nous obtenons

$$n\times 0=n\times 0+n\times 0\iff n\times 0+0=n\times 0+n\times 0$$

Par la régularité de l'addition, nous avons $n\times 0=0$
▷ Montrons que $n(-p)=-(np)$
Nous avons :

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

Ainsi, $n\times(-p)$ apparaît comme l'opposé de $n\times p$ pour l'addition, et donc

$$n(-p)=-(np)=-np$$

▷ Montrons que $n\times(p-q)=np-nq$
Cette question ne pose pas de difficulté.

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

▷ Montrons que tout élément non nul de $\mathbb{Z}$ est régulier pour la multiplication
Soient $n\in\mathbb{Z}^*$, $p\in\mathbb{Z}$ et $q\in\mathbb{Z}$ tels que $np=nq$. Alors :

$$np=nq\iff np-nq=0\iff n\times(p-q)=0$$

Comme $n\neq 0$, alors $p-q=0$, c'est à dire $p=q$.
Ce que nous voulions

Remarque 7 :

La multiplication dans $\mathbb{Z}$ prolonge celle de $\mathbb{N}$.

4.1.17 Relation d'ordre dans $\mathbb{Z}$

1. Dans $\mathbb{Z}$, nous définissons la relation suivante :
$$(\forall x \in \mathbb{Z})\,(\forall y \in \mathbb{Z})\,((x \leqslant y) \iff ((\exists p \in \mathbb{N})\,(y = x + p)))$$
2. La relation « $\leqslant$ » est une relation d'ordre, compatible avec l'addition et la multiplication par un nombre positif

Démonstration

1. **La relation « $\leqslant$ » est une relation d'ordre**
   - ▷ La relation « $\leqslant$ » est réflexive
     En effet, soit $x \in \mathbb{Z}$; alors, $x = x + 0$ et donc $x \leqslant x$
   - ▷ La relation « $\leqslant$ » est antisymétrique
     Soient $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$ tels que $x \leqslant y$ et $y \leqslant x$. Alors, il existe $p \in \mathbb{N}$ et $q \in \mathbb{N}$ tels que $y = x + p \iff y - x = p$ et $x = y + q \iff y - x = -q$
     Ce qui veut dire que $p = -q$. Comme $q \in \mathbb{N}$, alors $p \in \mathbb{Z}^-$ et donc de $p \in \mathbb{N}$ et de $p \in \mathbb{Z}^-$, nous en déduisons que $p = q = 0$ et que donc $x = y$
   - ▷ La relation « $\leqslant$ » est transitive
     Soient $x \in \mathbb{Z}$, $y \in \mathbb{Z}$ et $z \in \mathbb{Z}$ tels que $x \leqslant y$ et $y \leqslant z$. Alors, il existe $p \in \mathbb{N}$ et $q \in \mathbb{N}$ tels que $y = x + p$ et $z = y + q$
     Alors, très simplement $z = y + q = (x + p) + q = x + (p + q)$ et donc $x \leqslant z$.
     La relation « $\leqslant$ » est donc transitive

   La relation « $\leqslant$ » est donc une relation d'ordre
2. **La relation « $\leqslant$ » est compatible avec l'addition et la multiplication par un nombre positif**
   - ▷ La relation « $\leqslant$ » est compatible avec l'addition
     Soient $x \in \mathbb{Z}$, $y \in \mathbb{Z}$ et $z \in \mathbb{Z}$ tels que $x \leqslant y$. Alors, il existe $p \in \mathbb{N}$ tel que $y = x + p$
     Alors $y + z = x + p + z = (x + z) + p$ et donc $x + z \leqslant y + z$
     La relation « $\leqslant$ » est donc compatible avec l'addition
   - ▷ La relation « $\leqslant$ » est compatible avec la multiplication par un entier positif
     Soient $x \in \mathbb{Z}$, $y \in \mathbb{Z}$ et $z \in \mathbb{Z}^+$ tels que $x \leqslant y$. Alors, il existe $p \in \mathbb{N}$ tel que $y = x + p$
     Alors $y \times z = (x + p) \times z = (x \times z) + p \times z$. Comme $p \in \mathbb{N}$ et $z \in \mathbb{N}$, alors $pz \in \mathbb{N}$ et donc $x \times z \leqslant y \times z$
     La relation « $\leqslant$ » est donc compatible avec la multiplication par un entier positif

Remarque 8 :

Lorsque, pour $x \in \mathbb{Z}$, $y \in \mathbb{Z}$ nous avons $x \leqslant y$, il existe alors $p \in \mathbb{N}$ tel que $y = x + p$. Cette égalité est donc équivalente à $y - x \in \mathbb{N} = \mathbb{Z}^+$

4.1.18 Proposition

La relation « $\leqslant$ » est une relation d'ordre total dans $\mathbb{Z}$

Démonstration

Nous avons, dans tous les cas $\mathbb{Z} = \mathbb{Z}^- \cup \mathbb{Z}^+$ et $\mathbb{Z}^- \cap \mathbb{Z}^+ = \{0\}$
Soit donc $n \in \mathbb{Z}$ et $p \in \mathbb{Z}$.
Alors $n - p \in \mathbb{Z}^+$ et, dans ce cas $p \leqslant n$
Ou bien $n - p \in \mathbb{Z}^- \iff p - n \in \mathbb{Z}^+$ et, dans ce cas $n \leqslant p$
A chaque fois n et p sont comparables et la relation d'ordre est donc totale.

Remarque 9 :

1. On définit la relation **strictement inférieur** « $<$ » par :
$$(\forall x \in \mathbb{Z})\,(\forall y \in \mathbb{Z})\,((x < y) \iff ((x \leqslant y) \text{ et } (x \neq y)))$$
2. En utilisant la définition de la relation d'ordre « $\leqslant$ » vue en 4.1.17, notons les relation immédiates :
   - ▷ $(x \in \mathbb{N}) \iff (x \geqslant 0) \iff (-x \leqslant 0)$
   - ▷ $(x \in \mathbb{N}^*) \iff (x > 0) \iff (x \geqslant 1)$
   - ▷ $(x \in \mathbb{Z}^-) \iff (x \leqslant 0) \iff (-x \geqslant 0)$
3. Second type de relation : $x \leqslant y \iff -x \geqslant -y$
   En effet, $x \leqslant y \iff y - x \in \mathbb{N}$
   Or, $y - x = -x - (-y)$ et nous avons donc $-x - (-y) \in \mathbb{N}$, c'est à dire $-y \leqslant -x \iff -x \geqslant -y$
4. Remarquons aussi que $((x \leqslant y) \text{ et } (z \leqslant 0)) \Longrightarrow (xz \geqslant xy)$
   En effet, $x \leqslant y \iff y - x \in \mathbb{N}$ et donc, si $z \leqslant 0$, alors $z\,(y - x) \in \mathbb{Z}^- \iff z\,(x - y) \in \mathbb{N}$.
   Comme $z\,(x - y) = zx - zy$, nous avons $zx - zy \in \mathbb{N} \iff zx \geqslant zy$

4.1.19 Proposition

$\mathbb{Z}$ est archimédien
C'est à dire que pour tout $y \in \mathbb{Z}$ et tout $x \in \mathbb{N}^*$, il existe $n \in \mathbb{N}$ tel que $nx > y$

Démonstration

Soient $y \in \mathbb{Z}$ et $x \in \mathbb{N}^*$.
- ▷ Si $y \in \mathbb{Z}^-$, alors, il n'y a pas de difficulté ; il suffit de prendre $n = 1$, et comme $y \leqslant 0$ et $x \geqslant 1$, nous avons bien $y < 1 \times x$
- ▷ Supposons, cette fois ci $y \in \mathbb{N}^*$, c'est à dire que y est un entier strictement positif, c'est à dire $y > 0$
  Alors, comme $x \geqslant 1$, nous avons $x\,(y + 1) \geqslant y + 1 > y$ et l'entier $n = y + 1$ convient.

4.1.20 Sous-ensembles de $\mathbb{Z}$

1. Tout sous ensemble non vide et minoré de $\mathbb{Z}$ admet un élément minimum unique
2. Tout sous ensemble non vide et majoré de $\mathbb{Z}$ admet un élément maximum unique

Démonstration

1. Soit $M \subset \mathbb{Z}$ non vide et minoré. Soit $a \in \mathbb{Z}$, ce minorant.
   Alors, pour tout $y \in M$, $a \leqslant y$. On considère l'ensemble M' défini par :
   $$M' = \{x \in \mathbb{Z} \text{ tels que } x = y + a \text{ où } y \in M\}$$
   Alors puisque tout $x \in M'$ est tel que $x \geqslant 0$, nous avons $M' \subset \mathbb{N}$, et d'après l'axiôme 2.1.2 M' est un ensemble non vid ede $\mathbb{N}$ qui admet un plus petit élément unique appelé t.
   Par construction, il existe un nombre $y_0 \in M$ tel que $t = a + y_0$ et ce plus petit élément est de manière évidente le nombre $y_0 = t - a$, et cet élément y_0 est, lui aussi unique
2. Supposons, maintenant, $M \subset \mathbb{Z}$ non vide et majoré.
   Soit $b \in \mathbb{Z}$, ce majorant. Alors, pour tout $y \in M$, $b \geqslant y$
   Considère maintenant l'ensemble M_1 défini par :
   $$M_1 = \{x \in \mathbb{Z} \text{ tels que } x = -y \text{ où } y \in M\}$$
   Alors cette fais ci, M_1 est une partie de $\mathbb{Z}$ non vide et minorée par $-b$.
   D'après la question précédente, M_1 admet un plus petit élément $z_1 \in M_1$, c'est à dire que pour tout $x \in M_1$, $z_1 \leqslant x \iff -x \geqslant -z_1$
   Comme $-x \in M$ et $-z_1 \in M$, M admet donc un plus grand élément unique