

Les entiers relatifs

Marc Lorenzi

11 septembre 2022

1 L'ensemble $\mathbb{Z}$

1.1 Introduction

Nous allons dans cet article construire l'anneau $\mathbb{Z}$ des entiers relatifs à partir de l'ensemble $\mathbb{N}$. Une approche consisterait à rajouter à $\mathbb{N}$ une copie de $\mathbb{N}^*$ qui serait l'ensemble des entiers négatifs. L'inconvénient de cette approche est qu'elle ne permet pas de définir de façon très jolie l'addition dans $\mathbb{Z}$. Nous allons ici adopter une autre approche.

1.2 Une relation d'équivalence

L'idée est que tout (futur) entier relatif n s'écrit $n = a - b$ où a et b sont des entiers naturels. On ne peut pas représenter directement n par le couple (a, b) , parce qu'il n'y a pas unicité. Étant donnés $a, b, c, d \in \mathbb{N}$, on a $a - b = c - d$ si et seulement si $a + d = b + c$. Nous allons donc identifier les couples d'entiers naturels vérifiant cette dernière égalité.

Définition 1. On définit sur $E = \mathbb{N} \times \mathbb{N}$ la relation $\simeq$ en posant pour tous $a, b, c, d \in \mathbb{N}$,

$$(a, b) \simeq (c, d) \iff a + d = b + c$$

Proposition 1. $\simeq$ est une relation d'équivalence sur E .

Démonstration.

- Réflexivité. Soit $(a, b) \in E$. On a $a + b = b + a$, donc $(a, b) \simeq (a, b)$.
- Symétrie. Soient $(a, b), (c, d) \in E$. Supposons $(a, b) \simeq (c, d)$. On a donc $a + d = b + c$, d'où $c + b = d + a$, c'est à dire $(c, d) \simeq (a, b)$.
- Transitivité. Soient $(a, b), (c, d), (e, f) \in E$. Supposons $(a, b) \simeq (c, d)$ et $(c, d) \simeq (e, f)$. On a $a + d = b + c$ et $c + f = e + d$. De là, $a + d + f = b + c + f = b + e + d$ et donc, en simplifiant par d , $a + f = b + e$. Ainsi, $(a, b) \simeq (e, f)$.

□

Définition 2. $\mathbb{Z} = E / \simeq$.

Les éléments de $\mathbb{Z}$ sont les *entiers relatifs*.

Un entier relatif est donc une classe d'équivalence modulo $\simeq$. Nous noterons $\langle a, b \rangle$ la classe d'équivalence du couple (a, b) pour la relation $\simeq$. On a ainsi

$$\mathbb{Z} = \{\langle a, b \rangle : a, b \in \mathbb{N}\}$$

1.3 Une injection de $\mathbb{N}$ dans $\mathbb{Z}$

Dans la suite de l'article, nous noterons $\varphi : \mathbb{N} \longrightarrow \mathbb{Z}$ l'application définie par

$$\forall n \in \mathbb{N}, \varphi(n) = \langle n, 0 \rangle$$

Proposition 2. φ est injective.

Démonstration. Soient $m, n \in \mathbb{N}$. Supposons $\varphi(m) = \varphi(n)$. On a donc $\langle m, 0 \rangle = \langle n, 0 \rangle$, c'est à dire $m + 0 = 0 + n$, d'où $m = n$. $\square$

2 Addition

2.1 La définition

Définition 3. Pour tous entiers relatifs $\langle a, b \rangle$ et $\langle c, d \rangle$, on pose

$$\langle a, b \rangle + \langle c, d \rangle = \langle a + c, b + d \rangle$$

Il convient de vérifier que notre définition de l'addition dépend bien des *classes* modulo $\simeq$ et pas de leurs représentants. Donnons-nous $a, a', b, b', c, c', d, d' \in \mathbb{N}$. Supposons $(a, b) \simeq (a', b')$ et $(c, d) \simeq (c', d')$. On a alors

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

Ainsi,

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

Nous venons donc de définir une addition dans $\mathbb{Z}$. Nous allons maintenant montrer que cette addition possède toutes les propriétés algébriques souhaitées.

L'entier relatif $\langle 0, 0 \rangle$ va jouer un rôle important dans la suite. Notons-le 0. Remarquons que pour tout $a \in \mathbb{N}$, $a + 0 = 0 + a$ et donc

$$\langle a, a \rangle = 0$$

2.2 Propriétés

Proposition 3. *Pour tout $n \in \mathbb{Z}$, $n + 0 = 0$.*

Démonstration. Soit $n = \langle a, b \rangle \in \mathbb{Z}$. On a

$$\begin{aligned}n + 0 &= \langle a, b \rangle + \langle 0, 0 \rangle \\&= \langle a + 0, b + 0 \rangle \\&= \langle a, b \rangle \\&= n\end{aligned}$$

□

Proposition 4. *Pour tous $m, n \in \mathbb{Z}$, $m + n = n + m$.*

Démonstration. Soient $m = \langle a, b \rangle$ et $n = \langle c, d \rangle$ deux entiers relatifs. On a

$$\begin{aligned}m + n &= \langle a, b \rangle + \langle c, d \rangle \\&= \langle a + c, b + d \rangle \\&= \langle c + a, d + b \rangle \\&= \langle c, d \rangle + \langle a, b \rangle \\&= n + m\end{aligned}$$

□

Proposition 5. *Pour tous $m, n, p \in \mathbb{Z}$, $(m + n) + p = m + (n + p)$.*

Démonstration. Soient $m = \langle a, b \rangle$, $n = \langle c, d \rangle$ et $p = \langle e, f \rangle$ trois entiers relatifs. On a

$$\begin{aligned}(m + n) + p &= \langle a + c, b + d \rangle + \langle e, f \rangle \\&= \langle (a + c) + e, (b + d) + f \rangle \\&= \langle a + (c + e), b + (d + f) \rangle \\&= \langle a, b \rangle + \langle c + e, d + f \rangle \\&= m + (n + p)\end{aligned}$$

□

Proposition 6. *Pour tout $m \in \mathbb{Z}$, il existe $n \in \mathbb{Z}$ tel que $m + n = 0$.*

Démonstration. Soit $m = \langle a, b \rangle \in \mathbb{Z}$. Soit $n = \langle b, a \rangle$. On a

$$m + n = \langle a + b, b + a \rangle = \langle 0, 0 \rangle = 0$$

□

Corollaire 7. $(\mathbb{Z}, +)$ est un groupe abélien.

Démonstration. Ceci résulte des propositions précédentes. $\square$

2.3 Le morphisme φ

Proposition 8. Pour tous $a, b \in \mathbb{N}$, $\varphi(a + b) = \varphi(a) + \varphi(b)$.

Démonstration. Soient $a, b \in \mathbb{N}$. On a

$$\varphi(a + b) = \langle a + b, 0 \rangle = \langle a, 0 \rangle + \langle b, 0 \rangle = \varphi(a) + \varphi(b)$$

$\square$

Proposition 9. Soit $n \in \mathbb{Z}$. On est dans un et un seul des trois cas suivants.

- $n = 0$.
- Il existe un unique $c \in \mathbb{N}^*$ tel que $n = \varphi(c)$.
- Il existe un unique $c \in \mathbb{N}^*$ tel que $n = -\varphi(c)$.

Démonstration. L'unicité de a résulte de l'injectivité de φ . Soient $c, c' \in \mathbb{N}$. Supposons $\varphi(c) = -\varphi(c')$. On a alors

$$\varphi(c + c') = \varphi(c) + \varphi(c') = 0$$

et donc, par l'injectivité de φ , $c + c' = 0$. Comme $c, c' \in \mathbb{N}$, il en résulte que $c = c' = 0$. Le fait que les trois cas s'excluent mutuellement en découle facilement.

Il reste à prouver l'existence. Soit $n = \langle a, b \rangle$ un entier relatif. Si $a \geq b$, il existe $c \in \mathbb{N}$ tel que $a = b + c$. De là,

$$n = \langle b + c, b \rangle = \langle c, 0 \rangle = \varphi(c)$$

Si $a \leq b$, il existe $c \in \mathbb{N}$ tel que $b = a + c$. De là,

$$n = \langle a, a + c \rangle = \langle 0, c \rangle = -\varphi(c)$$

$\square$

2.4 Inclusion de $\mathbb{N}$ dans $\mathbb{Z}$

Dorénavant, si $n \in \mathbb{N}$, nous identifierons l'entier naturel n et l'entier relatif $\langle n, 0 \rangle$. Avec cette identification, par la proposition précédente, tous les entiers relatifs sont de la forme $\pm n$ où $n \in \mathbb{N}$. Remarquons qu'avec notre identification, on a pour tous $a, b \in \mathbb{N}$,

$$\langle a, b \rangle = \langle a, 0 \rangle + \langle 0, b \rangle = a - b$$

On a ainsi pour tous $a, b, c, d \in \mathbb{N}$,

$$\langle a, b \rangle = \langle c, d \rangle \iff a - b = c - d$$

où $a - b$ et $c - d$ sont des entiers relatifs.

Notons que

$$\mathbb{Z} = \{a - b : a, b \in \mathbb{N}\}$$

La proposition précédente devient, avec l'identification :

Proposition 10. *Soit $n \in \mathbb{Z}$. On est dans un et un seul des trois cas suivants.*

- $n = 0$.
- $n \in \mathbb{N}^*$.
- $-n \in \mathbb{N}^*$.

On a donc aussi

$$\mathbb{Z} = \{-n : n \in \mathbb{N}^*\} \cup \{0\} \cup \mathbb{N}^*$$

et les trois ensembles ci-dessus sont disjoints.

3 Multiplication

3.1 La définition

Définition 4. Pour tous entiers relatifs $\langle a, b \rangle$ et $\langle c, d \rangle$, on pose

$$\langle a, b \rangle \langle c, d \rangle = \langle ac + bd, ad + bc \rangle$$

Il convient de vérifier que notre définition de l'addition dépend bien des *classes* modulo $\simeq$ et pas de leurs représentants. Donnons-nous $a, a', b, b', c, c', d, d' \in \mathbb{N}$. Supposons $(a, b) \simeq (a', b')$ et $(c, d) \simeq (c', d')$.

- Cas 1, $a \geq b$ et $c \geq d$. De $a + b' = a' + b$, on déduit $a - b = a' - b'$. De même, $c - d = c' - d'$. Ainsi,

$$(a - b)(c - d) = (a' - b')(c' - d')$$

En développant, il vient

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

d'où

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

Ainsi,

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

- Cas 2, $a \geq b$ et $c \leq d$. On a cette fois ci $a - b = a' - b'$ et $d - c = d' - c'$.
De là,

$$(a - b)(d - c) = (a' - b')(d' - c')$$

En développant, il vient

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

d'où

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

Ainsi,

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

- Les deux derniers cas se traitent de la même manière.

Nous venons donc de définir une multiplication dans $\mathbb{Z}$. Nous allons maintenant montrer que cette multiplication possède toutes les propriétés algébriques souhaitées.

3.2 Propriétés

Posons $1 = \langle 1, 0 \rangle$.

Proposition 11. Pour tout $n \in \mathbb{Z}$, $n \times 1 = n$.

Démonstration. Soit $n = \langle a, b \rangle$ un entier relatif. On a

$$\begin{aligned} n \times 1 &= \langle a, b \rangle \times \langle 1, 0 \rangle \\ &= \langle a \times 1 + b \times 0, a \times 0 + b \times 1 \rangle \\ &= \langle a, b \rangle \\ &= n \end{aligned}$$

□

Proposition 12. Pour tous $m, n \in \mathbb{Z}$, $mn = nm$.

Démonstration. Soient $m = \langle a, b \rangle$ et $n = \langle c, d \rangle$ deux entiers relatifs. On a

$$\begin{aligned} mn &= \langle ac + bd, ad + bc \rangle \\ &= \langle ca + db, cb + da \rangle \\ &= nm \end{aligned}$$

□

Proposition 13. Pour tous $m, n, p \in \mathbb{Z}$, $(mn)p = m(np)$.

Démonstration. Soient $m = \langle a, b \rangle$, $n = \langle c, d \rangle$ et $p = \langle e, f \rangle$ trois entiers relatifs. On a

$$\begin{aligned}
 (mn)p &= \langle ac + bd, ad + bc \rangle \langle e, f \rangle \\
 &= \langle (ac + bd)e + (ad + bc)f, (ac + bd)f + (ad + bc)e \rangle \\
 &= \langle a(ce + df) + b(cf + de), a(cf + de) + b(ce + df) \rangle \\
 &= \langle a, b \rangle \langle ce + df, cf + de \rangle \\
 &= m(np)
 \end{aligned}$$

□

Proposition 14. *Pour tous $m, n, p \in \mathbb{Z}$, $m(n + p) = mn + mp$.*

Démonstration. Soient $m = \langle a, b \rangle$, $n = \langle c, d \rangle$ et $p = \langle e, f \rangle$ trois entiers relatifs. On a

$$\begin{aligned}
 m(n + p) &= \langle a, b \rangle \langle c + e, d + f \rangle \\
 &= \langle a(c + e) + b(d + f), a(d + f) + b(c + e) \rangle \\
 &= \langle (ac + bd) + (ae + bf), (ad + bc) + (af + be) \rangle \\
 &= \langle ac + bd, ad + bc \rangle + \langle ae + bf, af + be \rangle \\
 &= mn + mp
 \end{aligned}$$

□

Corollaire 15. *$(\mathbb{Z}, +, \times)$ est un anneau commutatif.*

Démonstration. Ceci résulte des propositions précédentes. □

3.3 Le morphisme φ

Proposition 16. *Pour tous $a, b \in \mathbb{N}$, $\varphi(ab) = \varphi(a)\varphi(b)$.*

Démonstration. Soient $a, b \in \mathbb{N}$. On a

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

□

L'identification que nous avons faite en égalant, pour tout $a \in \mathbb{N}$, l'entier naturel a et l'entier relatif $\langle a, 0 \rangle$, est donc toujours la bienvenue. Remarquons que nous avons aussi $\varphi(1) = \langle 1, 0 \rangle = 1$. Ainsi, φ est un morphisme injectif du semi-anneau $\mathbb{N}$ vers l'anneau $\mathbb{Z}$.

3.4 Intégrité

Proposition 17. $\mathbb{Z}$ est un anneau intègre.

Démonstration. Soient m et n deux entiers relatifs. Supposons que $mn = 0$.

- Cas 1, $m, n \in \mathbb{N}$. Le produit mn est aussi le produit des entiers naturels m et n dans $\mathbb{N}$ donc, par les propriétés de la multiplication dans $\mathbb{N}$, $m = 0$ ou $n = 0$.
- Cas 2, $m \in \mathbb{N}$ et $-n \in \mathbb{N}$. On a alors $-mn = m(-n) = 0$, d'où $m = 0$ ou $-n = 0$, c'est à dire $m = 0$ ou $n = 0$.
- Les deux cas restants se traitent de la même façon.

□

4 Un ordre sur $\mathbb{Z}$

4.1 Introduction

La construction de l'anneau intègre $(\mathbb{Z}, +, \times)$ est maintenant terminée. Nous pouvons oublier comment $\mathbb{Z}$ a été construit et retenir que

$$\mathbb{Z} = \mathcal{N} \cup \{0\} \cup \mathcal{P}$$

où $\mathcal{P} = \mathbb{N}^*$ et $\mathcal{N} = \{-n : n \in \mathbb{N}^*\}$ et les opérations dans $\mathcal{P}$ coïncident avec les opérations usuelles dans $\mathbb{N}$. Remarquons que les ensembles $\mathcal{N}$, $\{0\}$ et $\mathbb{N}^*$ sont disjoints. En effet, si $a, b \in \mathbb{N}$ et $a = -b$, alors $a + b = 0$. Ceci est aussi une égalité dans $\mathbb{N}$, donc $a = b = 0$.

Nous allons voir comment ceci permet de définir l'ordre usuel $\leq$ sur $\mathbb{Z}$ et de montrer les principales propriétés de cette relation.

4.2 La définition

Définition 5. Soient $m, n \in \mathbb{N}$. On pose

$$m \leq n \iff n - m \in \mathbb{N}$$

Remarquons que cette relation prolonge l'ordre usuel dans $\mathbb{N}$. Si $a, b \in \mathbb{N}$, alors $a \leq b$ en tant qu'entiers naturels si et seulement si il existe $c \in \mathbb{N}$ tel que $b = a + c$. Cela revient à dire que l'entier relatif $c = b - a$ est un entier naturel.

4.3 Propriétés

Proposition 18. $\leq$ est un ordre total sur $\mathbb{Z}$.

Démonstration.

- Réflexivité. Soit $n \in \mathbb{N}$. On a $n - n = 0 \in \mathbb{N}$ donc $n \leq n$.
- Antisymétrie. Soient $m, n \in \mathbb{N}$. Supposons $m \leq n$ et $n \leq m$. On a donc Notons $p = n - m$. On a $p \in \mathbb{N}$ et $-p \in \mathbb{N}$, donc $p = 0$, c'est à dire $m = n$.
- Transitivité. Soient $m, n, p \in \mathbb{N}$. Supposons $m \leq n$ et $n \leq p$. On a alors

$$p - m = (p - n) + (n - m)$$

La somme de deux éléments de $\mathbb{N}$ étant encore dans $\mathbb{N}$, on en déduit que

$$p - m \in \mathbb{N}$$

c'est à dire que $m \leq p$.

- Totalité. Soient $m, n \in \mathbb{N}$. Soit $p = n - m$. Si $p \in \mathbb{N}$, alors $m \leq n$. Sinon, $-p \in \mathbb{N}$, et donc $m - n \in \mathbb{N}$, c'est à dire $n \leq m$. Ainsi, l'ordre est total.

□

Définition 6. Pour tous $m, n \in \mathbb{Z}$, on pose

$$m < n \iff m \leq n \text{ et } m \neq n$$

Proposition 19. Pour tous $m, n, p \in \mathbb{N}$, $m < n \implies m + p < n + p$.

Démonstration. Soient $m, n, p \in \mathbb{Z}$. Supposons $m < n$. On a alors

$$(n + p) - (m + p) = n - m \in \mathbb{N}^*$$

et donc $m + p < n + p$. □

Proposition 20. Pour tous $m, n, p \in \mathbb{N}$ tels que $p > 0$, $m < n \implies mp < np$.

Démonstration. Soient $m, n, p \in \mathbb{Z}$. Supposons $p > 0$ et $m < n$. On a donc $n - m \in \mathbb{N}^*$ et $p \in \mathbb{N}^*$. De là

$$np - mp = (n - m)p \in \mathbb{N}^*$$

et donc $mp < np$. □

Proposition 21. Pour tous $m, n \in \mathbb{Z}$,

- $m < n \iff m + 1 \leq n$.
- $m \leq n \iff m < n + 1$.

Démonstration.

- On a

$$m < n \iff n - m \in \mathbb{N}^* \iff n - m - 1 \in \mathbb{N} \iff m + 1 \leq n$$

- On a

$$m \leq n \iff n - m \in \mathbb{N} \iff n + 1 - m \in \mathbb{N}^* \iff m < n + 1$$

□

4.4 Parties de $\mathbb{Z}$

Proposition 22. *Toute partie de $\mathbb{Z}$ non vide et minorée possède un plus petit élément.*

Démonstration. Soit $A \subseteq \mathbb{Z}$. Supposons A non vide et minorée par un entier p . Considérons

$$B = \{n - p : n \in A\}$$

L'ensemble B est une partie de $\mathbb{N}$ non vide et minorée. B possède donc un plus petit élément b . Facilement, $b + p$ est le plus petit élément de A . $\square$

Proposition 23. *Toute partie de $\mathbb{Z}$ non vide et majorée possède un plus grand élément.*

Démonstration. Soit $A \subseteq \mathbb{Z}$. Supposons A non vide et majorée par un entier p . Considérons

$$B = \{-n : n \in A\}$$

L'ensemble B est une partie de $\mathbb{Z}$ non vide et minorée par $-p$. B possède donc un plus petit élément b . Facilement, $-b$ est le plus grand élément de A . $\square$