$\mathbb{Q}$

Marc Lorenzi

16 septembre 2022

L'anneau $(\mathbb{Z}, +, \times)$ des entiers relatifs est un anneau commutatif intègre. En revanche ce n'est pas un corps : seuls -1 et 1 sont inversibles dans $\mathbb{Z}$. Nous allons dans cet article construire un corps qui, d'une certaine façon, est le plus petit corps contenant $\mathbb{Z}$. Il s'agit du corps $\mathbb{Q}$ des nombres rationnels.

1 Une relation d'équivalence

Notons $\mathcal{Q} = \mathbb{Z} \times \mathbb{Z}^*$. On définit sur $\mathcal{Q}$ une relation $\simeq$ en posant pour tous (a, b) et (c, d) éléments de $\mathcal{Q}$,

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

Proposition 1. *La relation $\simeq$ est une relation d'équivalence sur $\mathcal{Q}$.*

Démonstration.

- Réflexivité. Soit $(a, b) \in \mathcal{Q}$. On a $ab = ba$, donc $(a, b) \simeq (a, b)$.
- Symétrie. Soient (a, b) et $(c, d) \in \mathcal{Q}$. Supposons $(a, b) = (c, d)$. On a donc $ad = bc$, ce qui peut s'écrire $cb = da$. Ainsi, $(c, d) \simeq (a, b)$.
- Soient (a, b), (c, d) et (e, f) trois éléments de $\mathcal{Q}$. Supposons $(a, b) \simeq (c, d)$ et $(c, d) \simeq (e, f)$. On a

  $$afd = (ad)f = (bc)f = b(cf) = b(de) = bed$$

  Comme d est non nul et $\mathbb{Z}$ est intègre, on en déduit que $af = be$ et donc $(a, b) \simeq (e, f)$.

□

Si $(a, b) \in \mathcal{Q}$, nous noterons $[a \,/\, b]$ la classe de (a, b) modulo $\simeq$. Nous noterons $\mathbb{Q}$ l'ensemble quotient $\mathcal{Q}/\simeq$. On a donc

$$\mathbb{Q} = \{[a \,/\, b] : a \in \mathbb{Z}, b \in \mathbb{Z}^*\}$$

Les éléments de $\mathbb{Q}$ sont les *nombres rationnels*, ou plus simplement les *rationnels*.

2 Addition

Lemme 2. *Soient* $(a,b),(c,d) \in \mathcal{Q}$. *On a*

$$(ad+bc, bd) \in \mathcal{Q}$$

Démonstration. En effet, b et d sont sont nuls. Comme $\mathbb{Z}$ est intègre, $bd \in \mathbb{Z}^*$. □

Proposition 3. *Soient* $(a,b),(a',b'),(c,d),(c',d') \in \mathcal{Q}$. *On suppose* $(a,b) \simeq (a',b')$ *et* $(c,d) \simeq (c,d')$. *Alors,*

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

Démonstration. On a

$$\begin{aligned}(ad+bc)b'd' &= (ab')dd' + bb'(cd') \\ &= (ba')dd' + bb'(dc') \\ &= bd(a'd'+b'c')\end{aligned}$$

□

Définition 1. Pour tous $[a\,/\,b],[c\,/\,d] \in \mathbb{Q}$,

$$[a\,/\,b] + [c\,/\,d] = [ad+bc\,/\,bd]$$

Par la proposition précédente, cette opération est bien définie : la quantité $[a\,/\,b]+[c\,/\,d]$ ne dépend que des *classes* $[a\,/\,b]$ et $[c\,/\,d]$, et pas de leurs représentants (a,b) et (c,d).

Proposition 4. $(\mathbb{Q},+)$ *est un groupe abélien.*

Démonstration.

- Commutativité. Soient $[a\,/\,b]$ et $[c\,/\,d]$ deux rationnels.. On a

$$\begin{aligned}[a\,/\,b] + [c\,/\,d] &= [ad+bc\,/\,bd] \\ &= [cb+da\,/\,db] \\ &= [c\,/\,d] + [a\,/\,b]\end{aligned}$$

- Associativité. Soient $[a\,/\,b]$, $[c\,/\,d]$ et $[e\,/\,f]$ trois rationnels. On a

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

- Neutre. Soit $[a\,/\,b]\in\mathbb{Q}$. On a

$$[a\,/\,b]+[0\,/\,1]=[a\times 1+b\times 0\,/\,b\times 1]=[a\,/\,b]$$

  Ainsi, $[0\,/\,1]$ est neutre pour l'addition dans $\mathbb{Q}$.
- Opposé. Soit $[a\,/\,b]\in\mathbb{Q}$. On a

$$[a\,/\,b]+[-a\,/\,b]=[ab+b(-a)\,/\,b^2]=[0\,/\,b^2]=[0\,/\,1]$$

  Ainsi, $[-a\,/\,b]$ est l'opposé de $[a\,/\,b]$.

□

3 Multiplication

Lemme 5. *Soient $(a,b),(c,d)\in\mathcal{Q}$. On a*

$$(ac,bd)\in\mathcal{Q}$$

Démonstration. En effet, b et d sont sont nuls. Comme $\mathbb{Z}$ est intègre, $bd\in\mathbb{Z}^*$.
□

Proposition 6. *Soient $(a,b),(a',b'),(c,d),(c',d')\in\mathcal{Q}$. On suppose $(a,b)\simeq(a',b')$ et $(c,d)\simeq(c,d')$. Alors,*

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

Démonstration. On a

$$\begin{aligned}(ac)(b'd') &= (ab')(cd')\\ &= (ba')(dc')\\ &= (bd)(a'c')\end{aligned}$$

□

Définition 2. Pour tous $[a\,/\,b],[c\,/\,d]\in\mathbb{Q}$,

$$[a\,/\,b]\times[c\,/\,d]=[ac\,/\,bd]$$

Tout comme pour l'addition, la proposition précédente nous dit que cette opération est bien définie : la quantité $[a\ /\ b] \times [c\ /\ d]$ ne dépend que des *classes* $[a\ /\ b]$ et $[c\ /\ d]$, et pas de leurs représentants (a, b) et (c, d).

Proposition 7. $(\mathbb{Q}, +, \times)$ *est un anneau commutatif.*

Démonstration.

- Nous avons déjà vu que $(\mathbb{Q}, +)$ est un groupe abélien.
- Neutre. Soit $[a\ /\ b] \in \mathbb{Q}$. On a

$$[a\ /\ b] \times [1\ /\ 1] = [a \times 1\ /\ b \times 1] = [a\ /\ b]$$

  Ainsi, $[1\ /\ 1]$ est neutre pour la multiplication dans $\mathbb{Q}$.
- Associativité. Soient $[a\ /\ b], [c\ /\ d], [e\ /\ f] \in \mathbb{Q}$. On a

$$\begin{aligned} ([a\ /\ b] \times [c\ /\ d]) \times [e\ /\ f] &= [ac\ /\ bd] \times [e\ /\ f] \\ &= [(ac)e\ /\ (bd)f] \\ &= [a(ce)\ /\ b(df)] \\ &= [a\ /\ b] \times [ce\ /\ df] \\ &= [a\ /\ b] \times ([c\ /\ d] \times [e\ /\ f]) \end{aligned}$$

- Distributivité. Soient $[a\ /\ b], [c\ /\ d], [e\ /\ f] \in \mathbb{Q}$. On a

$$\begin{aligned} [a\ /\ b] \times ([c\ /\ d] + [e\ /\ f]) &= [a\ /\ b] \times [cf + de\ /\ df] \\ &= [a(cf + de)\ /\ bdf] \\ &= [a(cf + de)b\ /\ bdfb] \\ &= [(ac)(bf) + (bd)(ae)\ /\ (bd)(bf)] \\ &= [ac\ /\ bd] + [ae\ /\ bf] \\ &= [a\ /\ b] \times [c\ /\ d] + [a\ /\ b] \times [e\ /\ f] \end{aligned}$$

□

Nous avons utilisé à la troisième ligne de la preuve de la distributivité que si $(a, b) \in \mathcal{Q}$ et $c \in \mathbb{Z}^*$, alors $(ac, bc) \simeq (a, b)$.

Proposition 8. $(\mathbb{Q}, +\times)$ *est un corps.*

Démonstration. Tout d'abord, $[0\ /\ 1] \neq [1\ /\ 1]$ puisque $0 \times 1 = 0 \neq 1 = 1 \times 1$. Les neutres de $\mathbb{Q}$ pour l'addition et la multiplication sont donc distincts. Soit $[a\ /\ b] \in \mathbb{Q}$. Supposons que $[a\ /\ b] \neq [0\ /\ 1]$, c'est à dire $a \neq 0$ (et aussi $b \neq 0$ puisque $(a, b) \in \mathcal{Q}$). On a alors $(b, a) \in \mathcal{Q}$. De là,

$$[a\ /\ b] \times [b\ /\ a] = [ab\ /\ ba] = [1\ /\ 1]$$

Ainsi, $[a\ /\ b]$ est inversible pour la multiplication, et son inverse est $[b\ /\ a]$. □

4 Une injection de $\mathbb{Z}$ dans $\mathbb{Q}$

Soit $\varphi : \mathbb{Z} \longrightarrow \mathbb{Q}$ définie pour tout $a \in \mathbb{Z}$ par $\varphi(a) = [a\,/\,1]$.

Proposition 9. *φ est un morphisme injectif d'anneaux.*

Démonstration.

- Soient $a, a' \in \mathbb{Z}$. On a

$$\begin{array}{llll} \varphi(a) + \varphi(a') = & [a\,/\,1] + [a'\,/\,1] = & [a + a'\,/\,1] = & \varphi(a + a') \\ \varphi(a) \times \varphi(a') = & [a\,/\,1] \times [a'\,/\,1] = & [aa'\,/\,1] = & \varphi(aa') \end{array}$$

- $\varphi(1) = [1\,/\,1]$ qui est le neutre pour la multiplication dans $\mathbb{Q}$.
- Soit $a \in \ker\varphi$. On a $[a\,/\,1] = [0\,/\,1]$, c'est à dire $a \times 1 = 1 \times 0$, d'où $a = 0$. Ainsi, $\ker\varphi = \{0\}$ et φ est donc injective.

□

Proposition 10. *Pour tout $x \in \mathbb{Q}$, il existe $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ tel que*

$$x = \frac{\varphi(a)}{\varphi(b)}$$

Démonstration. Soit $x \in \mathbb{Z}^*$. Il existe $(a, b) \in E$ tel que $x = [a\,/\,b]$. Il suffit de remarquer que

$$\begin{array}{rcl} [a\,/\,b] & = & [a\,/\,1] \times [1\,/\,b] \\ & = & [a\,/\,1] \times [b\,/\,1]^{-1} \\ & = & \varphi(a) \times \varphi(b)^{-1} \end{array}$$

□

L'application φ est un isomorphisme d'anneaux de $\mathbb{Z}$ sur $\overline{\mathbb{Z}} = \varphi(\mathbb{Z})$. Nous pouvons identifier les éléments de $\overline{\mathbb{Z}}$ et les entiers relatifs et, donc, convenir d'écrire a au lieu de $\varphi(a)$ pour tout entier relatif a. Avec cette identification, $\overline{Z} = \mathbb{Z}$ devient un sous-anneau de $\mathbb{Q}$, et pour tout $x \in \mathbb{Q}$, il existe $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ tel que $x = \frac{a}{b}$. Ainsi,

$$\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z}^* \right\}$$

Les éléments de $\mathbb{Q}$ sont ainsi les *fractions* d'entiers relatifs. Le corps $\mathbb{Q}$ est le *corps des fractions* de l'anneau $\mathbb{Z}$. Avec notre identification, on retrouve les règles bien connues

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc$$

$$\begin{array}{rcl} \dfrac{a}{b} + \dfrac{c}{d} & = & \dfrac{ad + bc}{bd} \\ \dfrac{a}{b} \times \dfrac{c}{d} & = & \dfrac{ac}{bd} \end{array}$$

Nous allons voir pour terminer que, d'une certaine façon, notre construction de $\mathbb{Q}$ est la seule possible.

Proposition 11. *Soit $(\mathbb{K}, +\times)$ un corps. On suppose qu'il existe un morphisme d'anneaux $\psi : \mathbb{Z} \longrightarrow \mathbb{K}$ tel que*

$$\mathbb{K} = \left\{ \frac{\psi(a)}{\psi(b)} : a \in \mathbb{Z}, b \in \mathbb{Z}^* \right\}$$

Il existe alors un unique isomorphisme de $\mathbb{Q}$ sur $\mathbb{K}$.

Démonstration. Supposons qu'il existe un morphisme de corps $f : \mathbb{Q} \longrightarrow \mathbb{K}$. Les neutres de $\mathbb{Q}$ et $\mathbb{K}$ pour la multiplication sont 1 et $\psi(1)$. On a donc $f(1) = \psi(1)$. De là, pour tout $a \in \mathbb{Z}$,

$$f(a) = af(1) = a\psi(1) = \psi(a)$$

Soit $x \in \mathbb{Q}$. Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$ tels que $x = \frac{a}{b}$. On a

$$xb = a$$

De là,

$$f(xb) = f(x)f(b) = f(a)$$

ou encore

$$f(x)\psi(b) = \psi(a)$$

et donc

$$f(x) = \frac{\psi(a)}{\psi(b)}$$

Il existe donc au plus un morphisme de corps de $\mathbb{Q}$ dans $\mathbb{K}$.

Inversent, soient $(a, b), (a', b') \in \mathcal{Q}$ tels que $(a, b) \simeq (a', b')$. De $ab' = ba'$ on déduit

$$\psi(a)\psi(b') = \psi(b)\psi(a')$$

et donc

$$\frac{\psi(a)}{\psi(b)} = \frac{\psi(a')}{\psi(b')}$$

L'application $f : \mathbb{Q} \longrightarrow \mathbb{K}$ définie par

$$f\left(\frac{a}{b}\right) = \frac{\psi(a)}{\psi(b)}$$

est donc bien définie. Montrons que f est un isomorphisme de corps.

- On a

$$f(1) = \left(\frac{1}{1}\right) = \frac{\psi(1)}{\psi(1)} = 1_{\mathbb{K}}$$

- Soient $x = \frac{a}{b}$ et $y = \frac{c}{d}$ deux rationnels. On a

$$\begin{aligned} f(x+y) &= f\left(\frac{ad+bc}{bd}\right) = \frac{\psi(ad+bc)}{\psi(bd)} \\ &= \frac{\psi(a)\psi(d)+\psi(b)\psi(c)}{\psi(b)\psi(d)} \\ &= \frac{\psi(a)}{\psi(b)} + \frac{\psi(c)}{\psi(d)} \\ &= f(x)+f(y) \end{aligned}$$

  De même,

$$\begin{aligned} f(xy) &= f\left(\frac{ac}{bd}\right) = \frac{\psi(ac)}{\psi(bd)} \\ &= \frac{\psi(a)\psi(c)}{\psi(b)\psi(d)} = \frac{\psi(a)}{\psi(b)}\frac{\psi(c)}{\psi(d)} \\ &= f(x)f(y) \end{aligned}$$

- Par définition du corps $\mathbb{K}$, on a $\mathbb{K} = f(\mathbb{Q})$, donc f est surjective.

f est ainsi un morphisme de corps surjectif, et donc un isomorphisme de corps. □

5 Conclusion

Ce que nous avons montré dans cet article pour l'anneau $\mathbb{Z}$ des entiers relatifs et le corps $\mathbb{Q}$ des nombres rationnels utilisait essentiellement le fait que $(\mathbb{Z}, +, \times)$ est un anneau commutatif intègre. On peut, sans modifier les preuves, remplacer $\mathbb{Z}$ par un anneau commutatif intègre $\mathbb{A}$ quelconque, et obtenir le résultat très général suivant.

Proposition 12. *Soit $(\mathbb{A}, +, \times)$ un anneau commutatif intègre. Il existe un corps $(\mathbb{K}, +, \times)$ et un morphisme injectif $\varphi : \mathbb{A} \longrightarrow \mathbb{K}$ tels que*

$$\mathbb{K} = \left\{ \frac{\varphi(a)}{\varphi(b)} : a \in \mathbb{A}, b \in \mathbb{A} \setminus \{0\} \right\}$$

Un tel corps est unique à isomorphisme unique près.

En identifiant, comme nous l'avons fait pour $\mathbb{Q}$, l'élément a de $\mathbb{A}$ et l'élément $\varphi(a)$ de $\mathbb{K}$, on a

$$\mathbb{K} = \left\{ \frac{a}{b} : a \in \mathbb{A}, b \in \mathbb{A} \setminus \{0\} \right\}$$

$\mathbb{K}$ est appelé « le » corps des fractions de l'anneau $\mathbb{A}$.