# Construction de $\mathbb{Z}$ et de $\mathbb{Q}$.

Dany-Jack Mercier

IUFM de Guadeloupe, Morne Ferret,
BP399, Pointe-à-Pitre cedex 97159, France
dany-jack.mercier@univ-ag.fr

5 octobre 2003

## 1 Construction de $\mathbb{Z}$

### 1.1 Introduction

On suppose que la construction axiomatique de l'ensemble $\mathbb{N}$ des entiers naturels est connue. Si $m \in \mathbb{N}$ (resp. $m \in \mathbb{N}^*$), on note $m+1$ (resp. $m-1$) le successeur de $m$ (resp. le prédécesseur de $m$). On rappelle que l'addition dans $\mathbb{N}$ est définie par récurrence en posant :

(1) $\forall n \in \mathbb{N} \quad n+0=n$,
(2) $\forall n \in \mathbb{N} \quad \forall p \in \mathbb{N}^* \quad n+p=(n+(p-1))+1$.

L'addition ainsi définie est commutative, associative, possède 0 comme élément neutre, et tout entier est régulier. On rappelle aussi qu'il existe une relation d'ordre totale $\leq$ sur $\mathbb{N}$ compatible avec l'addition.

Si $a, b$ sont deux entiers naturels tels que $a \leq b$, alors l'équation $a+x=b$ admet une unique solution dans $\mathbb{N}$, solution que l'on appelle la différence de $b$ et $a$, et que l'on note $b-a$.

L'unicité provient du fait que tout élément de $\mathbb{N}$ est régulier, ce qui permet d'affirmer que l'équation $a+x=b=a+x'$ entraîne $x=x'$. L'existence se montre par récurrence sur $b$. Soit $H(b)$ la propriété "toute équation $a+x=b$ avec $a \leq b$ possède au moins une solution $x \in \mathbb{N}$". $H(0)$ est vraie. Si $H(b)$ est vraie, l'équation $a+x=b+1$ admet clairement une solution si $a=0$. Si $a \neq 0$, $a$ possède un prédécesseur $a-1$ et notre équation équivaut à $(a-1)+x=b$. Comme $a-1 \leq b$, on peut appliquer l'hypothèse récurrence et affirmer l'existence d'une solution $x$.

Malheureusement l'équation $a+x=b$ avec $a>b$ ne possède pas de solution dans $\mathbb{N}$ (en effet, si $x \in \mathbb{N}$, $a+x \geq a > b$ ne laisse aucun espoir). Il s'agit donc de construire un ensemble plus vaste que $\mathbb{N}$ et contenant $\mathbb{N}$, de généraliser les lois $+$ et $\times$ à ce nouvel ensemble en conservant leurs propriétés si agréables, et de s'arranger pour que tout élément de cet ensemble possède un opposé, c'est-à-dire un symétrique pour la loi $+$. On obtiendra ainsi le groupe $(\mathbb{Z}, +)$.

### 1.2 Symétrisation de la loi + de $\mathbb{N}$

**Définition 1** *Un **semi-groupe** est un magma associatif (i.e. un ensemble $E$ muni d'une loi de composition interne associative) dont tous les éléments sont réguliers.*

[0] [cari0005] v1.01 http://perso.wanadoo.fr/megamaths

$(\mathbb{N},+)$ est un semi-groupe commutatif d'élément neutre 0. De même $(\mathbb{N}\times\mathbb{N},+)$ est un semi-groupe commutatif d'élément neutre $(0,0)$ pour la loi produit

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

On définit une relation d'équivalence $\mathcal{R}$ dans $\mathbb{N}\times\mathbb{N}$ en posant

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

La relation $\mathcal{R}$ est compatible avec la loi + puisque

$$\forall\,(x,y)\in\mathbb{N}\times\mathbb{N}\quad (a,b)\,\mathcal{R}\,(c,d)\Rightarrow((a,b)+(x,y))\;\mathcal{R}\;((c,d)+(x,y)).$$

**Définition 2** *L'ensemble $\mathbb{Z}$ des* ***entiers relatifs*** *est l'ensemble quotient $\mathbb{N}\times\mathbb{N}/\mathcal{R}$. Si l'on note $\overline{(a,b)}=\{(x,y)\in\mathbb{N}\times\mathbb{N}/\ (x,y)\,\mathcal{R}\,(a,b)\}$ la classe d'équivalence du couple $(a,b)$, on peut écrire*

$$\mathbb{Z}=\mathbb{N}\times\mathbb{N}/\mathcal{R}=\left\{\overline{(a,b)}\,/\,a,b\in\mathbb{N}\right\}.$$

La compatibilité de $\mathcal{R}$ et de la loi + permet de définir la loi-quotient + en posant

$$\overline{(a,b)}+\overline{(c,d)}=\overline{(a+c,b+d)}$$

et l'on peut vérifier que cette loi + dans $\mathbb{Z}$ est commutative, associative et admet $\overline{(0,0)}$ comme élément neutre. En outre tout élément de $\mathbb{Z}$ est symétrisable car :

$$\forall\overline{(a,b)}\in\mathbb{Z}\quad\exists\overline{(b,a)}\in\mathbb{Z}\quad\overline{(a,b)}+\overline{(b,a)}=\overline{(a+b,a+b)}=\overline{(0,0)}.$$

On notera $-\overline{(a,b)}$ l'opposé de l'élément $\overline{(a,b)}$, de sorte que

$$-\overline{(a,b)}=\overline{(b,a)}.$$

En résumé :

**Théorème 1** *$(\mathbb{Z},+)$ est un groupe commutatif.*

L'application

$$\begin{array}{rccc} f: & \mathbb{N} & \to & \mathbb{Z} \\ & a & \mapsto & \overline{(a,0)} \end{array}$$

est un homomorphisme injectif pour les lois + puisque

$$f(a+b)=\overline{(a+b,0)}=\overline{(a,0)}+\overline{(a,0)}=f(a)+f(b).$$

et

$$\overline{(a,0)}=\overline{(b,0)}\Leftrightarrow a+0=b+0\Leftrightarrow a=b.$$

L'application $f$ est un plongement de $\mathbb{N}$ dans $\mathbb{Z}$ qui permet d'identifier $\mathbb{N}$ et $f(\mathbb{N})$ en écrivant $a=\overline{(a,0)}$ pour tout $a\in\mathbb{N}$. Avec cette identification, l'ensemble $\mathbb{N}$ devient une partie de $\mathbb{Z}$. L'opposé $-a$ de $a\in\mathbb{N}$ dans $\mathbb{Z}$ est $\overline{(0,a)}$, ce que l'on écrit $-a=\overline{(0,a)}$.

**Théorème 2** *Soit $-\mathbb{N}$ la partie de $\mathbb{Z}$ formée des opposés des éléments de $\mathbb{N}$. On a*
*1) $\mathbb{Z}=\mathbb{N}\cup(-\mathbb{N})$,*
*2) $\mathbb{N}\cap(-\mathbb{N})=\{0\}$,*
*3) Si $a\geq b$, l'unique entier naturel (noté $a-b$) solution de l'équation $b+x=a$ coïncide avec la somme $a+(-b)$ de $a$ et de l'opposé $(-b)$ de $b$.*

**Preuve :** 1) $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$ puisque

$$\forall \overline{(a,b)} \in \mathbb{Z} \quad \overline{(a,b)} = \begin{cases} \overline{(a-b,0)} = a - b \in \mathbb{N} \text{ si } a \geq b, \\ \overline{(0,b-a)} = -(b-a) \in -\mathbb{N} \text{ sinon.} \end{cases}$$

où $b - a$ désigne l'unique entier naturel solution de l'équation $a + x = b$ (pour $b \geq a$).
2) Si $a, b \in \mathbb{N}$,

$$a = -b \Leftrightarrow \overline{(a,0)} = \overline{(0,b)} \Leftrightarrow a + b = 0 \Leftrightarrow a = b = 0.$$

3) En effet $b + [a + (-b)] = a$ entraîne $a + (-b) = a - b$ quand $a \geq b$. ■

**Définition 3** *Si $a, b \in \mathbb{N}$, on pose $a - b = a + (-b)$.*

**Théorème 3** *La relation $\leq$ dans $\mathbb{Z}$ définie par*

$$a \leq b \Leftrightarrow b - a \in \mathbb{N}$$

*est une relation d'ordre sur $\mathbb{Z}$ qui généralise celle de $\mathbb{N}$.*

**Preuve :** Cette relation généralise celle de $\mathbb{N}$ puisque si $a, b \in \mathbb{N}$,

$$a \leq_{\mathbb{Z}} b \Leftrightarrow b - a = x \in \mathbb{N} \Leftrightarrow b + (-a) = x \in \mathbb{N} \Leftrightarrow b = a + x \Leftrightarrow a \leq_{\mathbb{N}} b.$$

On vérifie sans peine que $\leq_{\mathbb{Z}}$ est une réflexive et transitive. L'antisymétrie provient de

$$\begin{cases} a \leq b \\ b \leq a \end{cases} \Rightarrow \begin{cases} b - a \in \mathbb{N} \\ a - b = -(b-a) \in \mathbb{N} \end{cases} \Rightarrow b - a \in \mathbb{N} \cap (-\mathbb{N}) = \{0\}. \blacksquare$$

### 1.3 Cas général : symétrisation d'un semi-groupe

On peut reprendre la construction de la section 1.2 dans le cas général où $(E, .)$ est un semi-groupe commutatif en prenant seulement garde de remplacer l'application $f(a) = \overline{(a,e)}$ par $f(a) = \overline{(a+x,x)}$ puisque, cette fois-ci, $E$ ne possède pas forcément d'élément neutre $e$. Cette application $f$ est toujours bien définie puisque les couples $(a + x, x)$ sont tous dans la même classe d'équivalence quand $x$ décrit $E$.

Cette technique de symétrisation d'un semi-groupe nous permettra bientôt de construire le corps des rationnels $\mathbb{Q}$ à partir de $\mathbb{Z}^*$, et permet plus généralement la construction du corps des fractions d'un anneau intègre.

### 1.4 Multiplication dans $\mathbb{Z}$

Posons $\overline{(a,b)} \times \overline{(c,d)} = \overline{(ac+bd, bc+ad)}$. Cette définition a un sens puisque les égalités

$$\overline{(a,b)} = \overline{(a',b')} \text{ et } \overline{(c,d)} = \overline{(c',d')}$$

entraînent

$$\overline{(ac+bd, bc+ad)} = \overline{(a'c'+b'd', b'c'+a'd')} \quad (*).$$

En effet

$$\begin{cases} a + b' = b + a' \\ c + d' = d + c' \end{cases} \Rightarrow \begin{cases} (a+b')c' = (b+a')c' \\ (a+b')d' = (b+a')d' \\ a(c+d') = a(d+c') \\ b(c+d') = b(d+c') \end{cases} \Rightarrow \begin{cases} ac' + b'c' = bc' + a'c' \\ bd' + a'd' = ad' + b'd' \\ ac + ad' = ad + ac' \\ bd + bc' = bc + bd'. \end{cases}$$

En additionnant membre à membre les égalités du dernier système, on trouve

$$(ac+bd)+\left(b'c'+a'd'\right)=(bc+ad)+\left(a'c'+b'd'\right),$$

c'est-à-dire $(*)$.
On vérifie que cette multiplication est commutative, associative et distributive par rapport à l'addition. L'élément $\overline{(1,0)}$ est le neutre pour cette multiplication. De plus cette opération généralise la multiplication dans $\mathbb{N}$ puisque pour tous $a,b\in\mathbb{N}$ et en notant $f:\mathbb{N}\to\mathbb{Z}$ le plongement de $\mathbb{N}$ dans $\mathbb{Z}$ défini par $f(a)=\overline{(a,0)}$, on a

$$f(a)\times f(b)=\overline{(a,0)}\times\overline{(b,0)}=\overline{(ab,0)}=f(ab).$$

On peut énoncer :

**Théorème 4** *$(\mathbb{Z},+,\times)$ est un anneau commutatif unitaire, et l'application $f:\mathbb{N}\to\mathbb{Z}$ définie par $f(a)=\overline{(a,0)}$ est un homomorphisme injectif pour les lois $+$ et $\times$.*

# 2 Construction de $\mathbb{Q}$

## 2.1 Avertissement

La méthode de ce paragraphe est valide si l'on remplace l'anneau des entiers relatifs $\mathbb{Z}$ par un anneau intègre $A$. Elle permet alors de construire le corps des fractions $Q$ de l'anneau intègre $A$. Ce corps $Q$ est caractérisé par la propriété universelle donnée à la section 2.3.
En particulier, le corps $K(X)$ des fractions rationnelles sur un corps $K$ est défini comme le corps des fractions de l'anneau $K[X]$ des polynômes à une indéterminée à coefficients dans $K$.

## 2.2 Définitions

La relation $\mathcal{R}$ définie dans $\mathbb{Z}\times\mathbb{Z}^*$ par

$$(a,b)\,\mathcal{R}\,(c,d)\Leftrightarrow ad=bc$$

est une relation d'équivalence.

**Définition 4** *L'ensemble quotient $\mathbb{Q}=(\mathbb{Z}\times\mathbb{Z}^*)/\mathcal{R}$ est encore appelé ensemble des **nombres rationnels**. Si $(a,b)\in\mathbb{Z}\times\mathbb{Z}^*$, on désigne par $\frac{a}{b}$ la classe d'équivalence de $(a,b)$ par cette relation.*

Définissons les opérations $+$ et $\times$ dans $\mathbb{Q}$ en posant :

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}\text{ et }\frac{a}{b}\times\frac{c}{d}=\frac{ac}{bd}.$$

Pour vérifier que ces deux définitions ont un sens il faut être sûr que les résultats de ces opérations ne dépendent pas du choix des représentants $(a,b)$ et $(c,d)$ respectifs des classes $\frac{a}{b}$ et $\frac{c}{d}$. Supposons donc $\frac{a}{b}=\frac{a'}{b'}$ et $\frac{c}{d}=\frac{c'}{d'}$. On aura $ab'=a'b$ et $cd'=c'd$ et par conséquent

$$(ad+bc)\,b'd'=bd\left(a'd'+b'c'\right)\text{ et }acb'd'=a'c'bd$$

ce qui équivaut à

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

On vérifie ensuite que :

**Théorème 5** $(\mathbb{Q}, +, \times)$ *est un corps commutatif.*

**Définition 5** $\mathbb{Q}$ *est le* ***corps des fractions*** *de l'anneau* $\mathbb{Z}$.

L'application $\varphi : \mathbb{Z} \to \mathbb{Q}$ qui à $a \in \mathbb{Z}$ associe $\frac{a}{1}$ est un monomorphisme d'anneaux et permet de plonger $\mathbb{Z}$ dans $\mathbb{Q}$. Dans la pratique, on identifier les ensembles $\mathbb{Z}$ et $\varphi(\mathbb{Z})$ en posant $a = \frac{a}{1}$ pour tout $a \in \mathbb{Z}$.

## 2.3 Propriété universelle du corps des fractions

Les Théorèmes suivants montrent que le corps $\mathbb{Q}$ est caractérisé, à isomorphisme près, par une propriété de factorisation de morphismes d'anneaux appelée "propriété universelle". Ils permettent de définir $\mathbb{Q}$ en faisant seulement référence à cette propriété universelle.

**Théorème 6** ***Propriété universelle***
*Soient $K$ un corps commutatif et $f : \mathbb{Z} \to K$ un monomorphisme d'anneaux. Il existe un unique monomorphisme de corps $g : \mathbb{Q} \to K$ tel que $f = g \circ \varphi$.*

**Preuve :** S'il existe un morphisme $g$ rendant le diagramme

$$\begin{array}{ccc} & \mathbb{Z} & \xrightarrow{f} K \\ \varphi & \downarrow & \nearrow_{g} \\ & \mathbb{Q} & \end{array}$$

commutatif, alors $g(\varphi(a)) = f(a)$ pour tout $a \in \mathbb{Z}$, soit $g(a) = f(a)$. La fraction $\frac{1}{b}$ est l'inverse de $b$ (non nul) dans le corps $\mathbb{Q}$. Comme $g$ est un morphisme de corps, on devra avoir

$$\forall (a, b) \in \mathbb{Z} \times \mathbb{Z}^* \quad g\left(\frac{a}{b}\right) = g(a)\, g\left(\frac{1}{b}\right) = g(a)\, g(b)^{-1} = f(a)\, f(b)^{-1}. \tag{1}$$

Cette relation détermine parfaitement $g$ à partir de $f$. L'unicité de la décomposition est ainsi prouvée.
Il s'agit maintenant de vérifier que la relation (1) détermine bien un morphisme de corps $g$. Tout d'abord $f(a) f(b)^{-1}$ a un sens puisque $f(b)$ est inversible dans $K$ dès que $b \neq 0$ (c'est ici qu'intervient l'injectivité de $f$). Ensuite (1) définit $g$ de façon indépendante du choix des représentants $(a, b)$ de la fraction $\frac{a}{b}$. En effet,

$$\begin{aligned} \frac{a}{b} &= \frac{a'}{b'} \Leftrightarrow ab' = ba' \Rightarrow f(a) f\left(b'\right) = f(b) f\left(a'\right) \\ &\Rightarrow f(a) f(b)^{-1} = f\left(a'\right) f\left(b'\right)^{-1}. \end{aligned}$$

Ensuite, puisque $f$ est un morphisme d'anneaux,

$$\begin{aligned} g\left(\frac{a}{b} + \frac{c}{d}\right) &= g\left(\frac{ad + bc}{bd}\right) = f(ad + bc)\, f(bd)^{-1} \\ &= (f(a) f(d) + f(b) f(c))\, f(b)^{-1} f(d)^{-1} \\ &= f(a) f(b)^{-1} + f(c) f(d)^{-1} = g\left(\frac{a}{b}\right) + g\left(\frac{c}{d}\right) \end{aligned}$$

et

$$\begin{aligned} g\left(\frac{a}{b} \times \frac{c}{d}\right) &= g\left(\frac{ac}{bd}\right) = f(ac)\, f(bd)^{-1} \\ &= f(a) f(b)^{-1} f(c) f(d)^{-1} = g\left(\frac{a}{b}\right) g\left(\frac{c}{d}\right). \end{aligned}$$

Et pour terminer, $g$ est injective puisque

$$g\left(\frac{a}{b}\right) = 0 \Leftrightarrow f(a) f(b)^{-1} = 0 \Leftrightarrow f(a) = 0 \Rightarrow a = 0 \Rightarrow \frac{a}{b} = 0. \blacksquare$$

**Théorème 7** *A isomorphisme près, il esiste un et un seul couple $(\mathbb{Q}, \varphi)$ formé d'un corps $\mathbb{Q}$ et d'un monomorphisme d'anneaux $\varphi : \mathbb{Z} \to \mathbb{Q}$, qui vérifie la propriété universelle du Théorème 6. En ce sens on peut dire que $\mathbb{Q}$ est le plus petit corps contenant $\mathbb{Z}$.*

**Preuve :** Supposons que le couple $(F, \varphi_F)$ vérifie la propriété universelle. Les morphismes $\varphi$ et $\varphi_F$ se factorisent suivant le diagramme

$$\begin{array}{ccc} & & \mathbb{Q} \\ & \overset{\varphi}{\nearrow} & \uparrow h \\ \mathbb{Z} & \overset{\varphi_F}{\to} & F \\ & \underset{\varphi}{\searrow} & \uparrow g \\ & & \mathbb{Q} \end{array}$$

et l'unicité de la factorisation entraîne $h \circ g = Id_{\mathbb{Q}}$. On montre de la même façon que $g \circ h = Id_F$, de sorte que $g$ réalise un isomorphisme de corps entre $\mathbb{Q}$ et $F$. $\blacksquare$

## 2.4 Quelques propriétés de $\mathbb{Q}$

**Théorème 8** *$\mathbb{Q}$ est dense dans $\mathbb{R}$.*

**Preuve :** Si $x \in \mathbb{R}$ et $n \in \mathbb{N}$, notons $[10^n x]$ la partie entière de $10^n x$. On a

$$[10^n x] \leq 10^n x < [10^n x] + 1$$

donc $0 \leq x - r < \frac{1}{10^n}$ en posant $r = \frac{[10^n x]}{10^n} \in \mathbb{D} \subset \mathbb{Q}$. $\blacksquare$

**Théorème 9** *Tout rationnel $r$ s'écrit de façon unique sous la forme $r = \frac{a}{b}$ avec $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ et $\operatorname{pgcd}(a, b) = 1$. Dans ce cas $r = \frac{a'}{b'}$ si, et seulement si, il existe $t \in \mathbb{Z}$ avec $(a', b') = (ta, tb)$.*

**Preuve :** Tout rationnel $r$ s'écrit $r = \frac{a'}{b'}$ avec $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$, et il suffit de poser $\delta = \operatorname{pgcd}(a', b')$, $a' = \delta a$ et $b' = \delta b$ pour obtenir

$$r = \frac{\delta a}{\delta b} = \frac{a}{b} \text{ avec } \operatorname{pgcd}(a, b) = 1.$$

Si $r = \frac{a}{b} = \frac{c}{d}$ avec $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$, $(c, d) \in \mathbb{Z} \times \mathbb{N}^*$ et $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(c, d) = 1$, alors $ad = bc$. Le Théorème de Gauss montre que $a$ divise $c$. Il existe donc $u \in \mathbb{Z}$ tel que $c = ua$, et l'on obtient $d = ub$. Comme $\operatorname{pgcd}(ua, ub) = u \operatorname{pgcd}(a, b)$, on déduit $u = \pm 1$. Les signes de $a, b, c, d$ permettent de conclure à $(a, b) = (c, t)$. L'unicité du couple $(a, b)$ est démontrée.
Pour conclure, le Théorème de Gauss permet d'écrire les équivalences suivantes :

$$r = \frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = ba' \Leftrightarrow \exists t \in \mathbb{Z} \quad \begin{cases} a' = ta \\ b' = tb \end{cases} . \blacksquare$$

**Définition 6** *Une fraction $\frac{a}{b}$ est dite **irréductible** si $\operatorname{pgcd}(a, b) = 1$. Un représentant $(a, b)$ de $r$ tel que $\frac{a}{b}$ soit une fraction irréductible est appelé **représentant irréductible** de $r$.*