5. Nombres et structures algébriques

But du jeu

1. Définir l'ensemble $\mathbb{Z}$: c'est un quotient de $\mathbb{N} \times \mathbb{N}$;
2. Définir l'addition dans $\mathbb{Z}$, et montrer que $(\mathbb{Z}, +, 0)$ est un groupe commutatif ;
3. Définir le produit. On va montrer qu'il n'y a qu'une façon de faire, si on veut de bonnes propriétés ;
4. On en déduira une multiplication qui satisfera "moins par moins donne plus" ;
5. Montrer que $(\mathbb{Z}, +, 0, \cdot, 1)$ est un anneau commutatif ;
6. Faire la même chose pour $\mathbb{Q}$, et montrer que $(\mathbb{Q}, +, 0, \cdot, 1)$ est un champ.

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.

Le groupe addititif $(\mathbb{Z}, +, 0)$

L'idée : On fait comme les comptables pour ne compter qu'avec des nombres positifs.

Définition 5.1.1

On note $\mathcal{R}$ la relation sur $\mathbb{N} \times \mathbb{N}$ définie par $(a, b)\mathcal{R}(a', b')$ si, et seulement si, $a + b' = a' + b$.

Remarques :

1. C'est l'égalité des "sommes croisées" (somme des moyens égale somme des extrêmes) ;
2. L'idée est que (a, b) va correspondre à $a - b$, et donc que $a - b = a' - b'$, mais on ne veut pas l'écrire comme cela.

Proposition 5.1.1

La relation $\mathcal{R}$ définie ci-dessus est une relation d'équivalence. De plus, on a $(a, b)\mathcal{R}(a', b')$ si, et seulement si, il existe $k \in \mathbb{N}$ tel que

$$\left\{\begin{array}{lcl} a' & = & a + k \\ b' & = & b + k \end{array}\right. \quad \text{ou} \quad \left\{\begin{array}{lcl} a & = & a' + k \\ b & = & b' + k \end{array}\right.$$

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.

L'addition

L'idée : Additionner les gains d'un côté, et les pertes de l'autre.

Définition 5.1.2

L'ensemble $\mathbb{Z}$ est le quotient $\mathbb{N} \times \mathbb{N}/\mathcal{R}$. L'addition est l'application

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : ([(a, b)], [(c, d)]) \mapsto [(a + c, b + d)].$$

Oui mais Raoul...

Proposition 5.1.2

Pour tout $a, b, a', b', c, d, c', d' \in \mathbb{N}$, si $(a, b)\mathcal{R}(a', b')$ et $(c, d)\mathcal{R}(c', d')$, alors $(a + c, b + d)\mathcal{R}(a' + c', b' + d')$.

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.

Structure de groupe, en général

Définition 5.1.3 (rappel)

Un groupe est un triplet $(G, \circ, e)$ où G est un ensemble (non vide), $e \in G$ et $\circ : G \times G \to G$ satisfait les propriétés suivantes :

1. L'application $\circ$ est associative : on a $a \circ (b \circ c) = (a \circ b) \circ c$ pour tous $a, b, c \in G$;
2. L'élément e est neutre : on a $e \circ a = a \circ e = a$ pour tout $a \in G$;
3. Pour tout $a \in G$, il existe $a' \in G$ tel que $a \circ a' = a' \circ a = e$.

Un tel groupe est commutatif si $a \circ b = b \circ a$ pour tous $a, b \in G$.

Exemples :

1. $G = \{0, 1\}$, avec 0 neutre et $1 + 1 = 0$,
2. L'ensemble des bijections de A dans A, muni de la composition des bijections.

Propositions 5.1.3 et 5.1.4 (rappel)

Le neutre est unique, l'inverse de tout élément est unique. On a $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ pour tous $a, b \in G$.

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.

Structure de groupe de $\mathbb{Z}$, et l'inclusion $\mathbb{N} \subset \mathbb{Z}$

Quel est le neutre dans $\mathbb{Z}$? $[(0,0)] = [(1,1)] = \ldots$

Quel est l'opposé de $[(a,b)]$? $[(b,a)]$ (attention, pas $[(-a,-b)]$!).

Proposition 5.1.5

Le triplet $(\mathbb{Z}, +, 0)$, où $0 = [(0,0)]$ est un groupe commutatif.

Preuve : C'est direct. On se ramène aux propriétés dans $\mathbb{N}$.

Mais on n'a pas $\mathbb{N} \subset \mathbb{Z}$!...

On doit identifier $\mathbb{N}$ à une partie de $\mathbb{Z}$, identifiant n à un gain de n, et pas de perte.

Proposition 5.1.6

L'application

$$\varphi : \mathbb{N} \to \mathbb{Z} : n \mapsto [(n,0)]$$

est injective. De plus elle satisfait

$$\varphi(n+n') = \varphi(n) + \varphi(n') \quad \text{et} \quad \varphi(0) = 0.$$

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.

Notations, nombres négatifs, soustractions

- On identifie $\mathbb{N}$ à $\varphi(\mathbb{N})$, et on écrit $\mathbb{N} \subset \mathbb{Z}$.
- On note donc n le nombre $[(n,0)]$. De même $[(0,n)] = -[(n,0)]$ est noté $-n$.
- De même, on note $-\mathbb{N}$ l'ensemble $\{-n : n \in \mathbb{N}\}$.

Proposition 5.1.7

On a $\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}$ et $\mathbb{N} \cap -\mathbb{N} = \{0\}$.

L'idée : Le couple (a,b) correspond à un élément de $\mathbb{N}$ si le gain est supérieur à la perte.

Proposition 5.1.8

Pour tous $x, y \in \mathbb{Z}$, il existe un unique $z \in \mathbb{Z}$ tel que $x + z = y$.

Preuve : C'est $y + (-x)$.

Définition 5.1.5

L'unique nombre z tel que $x + z = y$ est noté $y - x$. C'est la différence entre y et x, ou la soustraction de x à y.

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.

Dernières notions sur l'addition

Proposition 5.1.9

On a $-(x+y) = (-x) + (-y) = -x - y$ pour tous $x, y \in \mathbb{Z}$.

Définition 5.1.6

La relation d'ordre usuelle sur $\mathbb{Z}$ est définie par

$$x \leqslant y \Leftrightarrow \exists k \in \mathbb{N} : y = x + k.$$

Remarque :

1. L'ordre prolonge donc en quelque sorte celui de $\mathbb{N}$
2. On a donc $x \leqslant y \Leftrightarrow y - x \in \mathbb{N}$.

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.

L'anneau $(\mathbb{Z}, +, 0, \cdot, 1)$

On pourrait donner la définition, et vérifier que cela marche, mais montrons qu'on n'a pas le choix, si on veut respecter le cahier des charges suivant :

1. Les nombres naturels se multiplient dans $\mathbb{Z}$ comme dans $\mathbb{N}$. Autrement dit, le plongement φ de $\mathbb{N}$ dans $\mathbb{Z}$ doit satisfaire
$$\varphi(n \cdot n') = \varphi(n) \cdot \varphi(n'), \quad n, n' \in \mathbb{N}.$$
2. Il existe un neutre pour la multiplication, c'est-à-dire un élément $e \in \mathbb{Z}$ tel que $e \cdot x = x \cdot e = x$ pour tout $x \in \mathbb{Z}$.
3. La multiplication distribue l'addition : on a $x \cdot (y + z) = x \cdot y + x \cdot z$ et $(y + z) \cdot x = y \cdot x + z \cdot x$ pour tous $x, y, z \in \mathbb{Z}$.

On suppose avoir une multiplication satisfaisant ces propriétés, et on déduit ses propriétés et enfin son expression.

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.

Premières propriétés

Proposition 5.2.1

Si la multiplication distribue l'addition ~~et admet un neutre~~, alors 0 est absorbant : on a $0 \cdot x = x \cdot 0 = 0$ pour tout $x \in \mathbb{Z}$.

Preuve : ~~Calculer $(e+0)\cdot x$.~~ Calculer $(0+0)\cdot x$ et $x \cdot (0+0)$.

Proposition 5.2.2

Si la multiplication distribue l'addition ~~et admet un neutre~~, alors

$$x \cdot (-y) = (-x) \cdot y = -(x \cdot y) \quad \text{et} \quad (-x)\cdot(-y) = x \cdot y$$

pour tous $x, y \in \mathbb{Z}$.

Preuve : Définition de l'opposé, et opposé deux fois.

Proposition 5.2.4

Si une multiplication $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ satisfait les ~~trois~~ deux conditions, alors

$$[(a,b)] \cdot [(c,d)] = [(ac+bd, ad+bc)],$$

pour tous a, b, c, d dans $\mathbb{N}$.

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.

La définition, et la synthèse

Définition 5.2.1

La multiplication des nombres entiers est l'application

$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : ([(a,b)],[(c,d)]) \mapsto [(ac+bd, ad+bc)].$$

Proposition 5.2.5

La multiplication définie ci-dessus est indépendante du choix des représentants.

Preuve : Traiter le cas $a' = a+k$ et $b' = b+k$ et $c' = c+l$ et $d' = d+l$, pour un $k, l \in \mathbb{N}$.

Proposition 5.2.6

La structure $(\mathbb{Z}, +, 0, \cdot, 1)$ est un anneau commutatif (avec unité).

Preuve : Ecrire les propriétés à vérifier, et utiliser les propriétés sur $\mathbb{N}$.

Proposition 5.2.7

L'application $\varphi : \mathbb{N} \to \mathbb{Z} : n \mapsto [(n,0)]$ satisfait la condition

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

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.

Intégrité et division

Définition 5.2.6

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}_0$. On dit que b divise a si il existe $c \in \mathbb{Z}$ tel que $a = b \cdot c$. On écrit alors $b|a$ et $c = a : b$ ou $c = \frac{a}{b}$.

Définition 5.2.7

Un anneau $(A, +, 0, \cdot, 1)$ est intègre si pour tous $x, y \in A$, si $x \cdot y = 0$ alors $x = 0$ ou $y = 0$.

Proposition 5.2.8

L'anneau $(\mathbb{Z}, +, 0, \cdot, 1)$ est intègre.

Corollaire 5.2.1

Soient $a \in \mathbb{Z}$, $b \in \mathbb{Z}_0$. Si $a = b \cdot c$ et $a = b \cdot c'$, pour $c, c' \in \mathbb{Z}$, alors $c = c'$.

Proposition 5.2.9

Soient $a \in \mathbb{Z}$, $b \in \mathbb{Z}_0$, tels que $b|a$. Alors $-b|a$, $b|-a$ et $-b|-a$. On a de plus $\frac{a}{-b} = \frac{-a}{b} = -\frac{a}{b}$ et $\frac{-a}{-b} = \frac{a}{b}$.

Le champ $\mathbb{Q}$

- On peut faire lamême construction pour le champ $\mathbb{Q}$. L'idée est de définir les fractions comme des classes de couples équivalents.
- On considère $(a, b) \in \mathbb{Z} \times \mathbb{Z}_0$ (ou $\mathbb{Z} \times \mathbb{N}_0$), et on écrit

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

- Il s'agit de l'égalité des produits croisés.
- L'ensemble $\mathbb{Q}$ est le quotient $(\mathbb{Z} \times \mathbb{Z}_0)/\mathcal{E}$.
- C'est une relation d'équivalence.
- On définit les opérations pour que cela rende ce que l'on pense : L'addition de $\mathbb{Q}$ est l'application définie par

$$+ : \mathbb{Q} \times \mathbb{Q} : ([(a, b)], [(c, d)]) \mapsto [(a, b)] + [(c, d)] = [(ad + bc, bd)].$$

  La multiplication de $\mathbb{Q}$ est l'application définie par

$$\cdot : \mathbb{Q} \times \mathbb{Q} : ([(a, b)], [(c, d)]) \mapsto [(a, b)] \cdot [(c, d)] = [(ac, bd)].$$

- On montre que les opérations sont bien définies et font de $\mathbb{Q}$ un champ.
- Il manque encore l'écriture avec des virgules, mais ce n'est pas difficile à faire.

P. Mathonet, Université de Liège, Faculté des Sciences, Département de Mathématique.