Complément 3

Une brève introduction à $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}\backslash\{0,1\}$. Rappelons que l'on dispose d'une relation d'équivalence sur $\mathbb{Z}$ qui est la relation de congruence modulo n :

$$a \equiv b\,[n] \;\Leftrightarrow\; \exists k \in \mathbb{Z},\, a-b = kn \;\Leftrightarrow\; n \mid (a-b).$$

Si $a \in \mathbb{Z}$, on note $\overline{a}$ sa classe d'équivalence, de sorte que :

$$\overline{a} = \{b \in \mathbb{Z} \mid \exists k \in \mathbb{Z},\, b = a + kn\} = a + n\mathbb{Z}.$$

Notons $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient, c'est-à-dire l'ensemble des classes d'équivalence pour la relation de congruence. Nous avions montré qu'il y a exactement n classes d'équivalence pour la congruence modulo n, qui sont $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. Ainsi :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Nous allons à présent définir deux lois de compositions internes sur $\mathbb{Z}/n\mathbb{Z}$.

Propriété 1 (LCI sur l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$)

On définit deux lois de compositions internes $\oplus$ et $\otimes$ sur $\mathbb{Z}/n\mathbb{Z}$ en posant, pour tous $a, b \in \mathbb{Z}$:

$$\overline{a} \oplus \overline{b} = \overline{a+b} \quad \text{et} \quad \overline{a} \otimes \overline{b} = \overline{a \times b}.$$

Le triplet $(\mathbb{Z}/n\mathbb{Z}, \oplus, \otimes)$ est un anneau commutatif d'éléments neutres $\overline{0}$ pour $\oplus$ et $\overline{1}$ pour $\otimes$.

Preuve. On commence par vérifier que les définitions des opérations $\oplus$ et $\otimes$ ne dépendent pas des représentants choisis dans les classes d'équivalence :

- la congruence modulo n est compatible avec l'addition :

$$\forall a, a', b, b' \in \mathbb{Z}, \quad a' \equiv a\,[n] \text{ et } b' \equiv b\,[n] \;\Rightarrow a' + b' \equiv a + b\,[n].$$

  Donc $\overline{a} \oplus \overline{b} = \overline{a+b}$ est bien définie.

- la congruence modulo n est compatible avec la multiplication :

$$\forall a, a', b, b' \in \mathbb{Z}, \quad a' \equiv a\,[n] \text{ et } b' \equiv b\,[n] \;\Rightarrow a' \times b' \equiv a \times b\,[n].$$

  Donc $\overline{a} \otimes \overline{b} = \overline{a \times b}$ est bien définie.

On montre que l'addition est une loi de groupe commutatif :

- elle est commutative car pour tout couple $(a, b) \in \mathbb{Z}^2$:

$$\overline{a} \oplus \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} \oplus \overline{a}.$$

- elle est associative car pour tout triplet $(a, b, c) \in \mathbb{Z}^3$:

$$(\overline{a} \oplus \overline{b}) \oplus \overline{c} = \overline{a+b} \oplus \overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a} \oplus \overline{b+c} = \overline{a} \oplus (\overline{b} \oplus \overline{c}).$$

- elle admet $\overline{0}$ pour élément neutre car pour tout $a \in \mathbb{Z}$:

$$\overline{a} \oplus \overline{0} = \overline{a+0} = \overline{a} \qquad \text{et} \qquad \overline{0} \oplus \overline{a} = \overline{0+a} = \overline{a}.$$

- tout élément $\overline{a}$ a pour opposé $\overline{-a}$ car pour tout $a \in \mathbb{Z}$:

$$\overline{a} \oplus \overline{-a} = \overline{a+(-a)} = \overline{0} \qquad \text{et} \qquad \overline{-a} \oplus \overline{a} = \overline{(-a)+a} = \overline{0}.$$

De la même façon, on vérifie que la multiplication est commutative, associative et qu'elle a pour élément neutre $\overline{1}$, qui est distinct de l'élément neutre $\overline{0}$ de l'addition.

Enfin, la multiplication $\otimes$ est distributive sur l'addition $\oplus$. En effet, pour tout triplet $(a,b,c) \in \mathbb{Z}^3$,

$$(\overline{a} \oplus \overline{b}) \otimes \overline{c} = \overline{a+b} \otimes \overline{c} = \overline{(a+b) \times c} = \overline{(a \times c) + (b \times c)} = \overline{a \times c} \oplus \overline{b \times c} = (\overline{a} \otimes \overline{c}) \oplus (\overline{b} \otimes \overline{c}).$$

Ainsi, $(\mathbb{Z}/n\mathbb{Z}, \oplus, \otimes)$ est un anneau commutatif d'éléments neutres $\overline{0}$ pour $\oplus$ et $\overline{1}$ pour $\otimes$. □

✎ **Notation.**

On pourra noter plus simplement $+$ et $\times$ ces deux lois $\oplus$ et $\otimes$, mais on veillera à ne pas les confondre avec les opérations dans $\mathbb{Z}$.

Exemples.

- **Tables des opérations de $\mathbb{Z}/2\mathbb{Z}$.**

  Voici les tables de $\mathbb{Z}/2\mathbb{Z}$, dressées à partir de la définition des lois $\oplus$ et $\otimes$, compte tenu du fait que la classe d'un entier modulo 2 est la classe de son reste dans la division par 2 (et c'est $\overline{0}$ si cet entier est pair et $\overline{1}$ si cet entier est impair) :

$\oplus$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

;

$\otimes$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

- **Tables des opérations de $\mathbb{Z}/6\mathbb{Z}$.**

  Voici les tables de $\mathbb{Z}/6\mathbb{Z}$, dressées à partir de la définition des lois $\oplus$ et $\otimes$, compte tenu du fait que la classe d'un entier modulo 2 est la classe de son reste dans la division par 6.

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

;

$\otimes$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Propriété 2 (Étude du groupe abélien $(\mathbb{Z}/n\mathbb{Z}, \oplus)$)

Le groupe $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ est cyclique, isomorphe à $(\mathbb{U}_n, \times)$.

Preuve. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique car il est fini et monogène engendré par $\overline{1}$.

Montrons que l'application

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{U}_n \\ \overline{k} & \mapsto & e^{\frac{2ik\pi}{n}} \end{array} \right.$$

est un isomorphisme de $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ dans $(\mathbb{U}_n, \times)$.

- Elle est bien définie : si $\overline{a} = \overline{b}$, alors il existe $k \in \mathbb{Z}$ tel que $a = b + kn$ et donc

$$\varphi(\overline{a}) = e^{\frac{2ia\pi}{n}} = e^{\frac{2i(b+kn)\pi}{n}} = e^{\frac{2ib\pi}{n} + 2i\pi} = e^{\frac{2ib\pi}{n}} = \varphi(\overline{b}).$$

- C'est un morphisme de groupe : si $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$,

$$\varphi(\overline{a} \oplus \overline{b}) = \varphi(\overline{a+b}) = e^{\frac{2i(a+b)\pi}{n}} = e^{\frac{2ia\pi}{n}} \times e^{\frac{2ib\pi}{n}} = \varphi(\overline{a}) \times \varphi(\overline{b}).$$

- On détermine son noyau :

$$\overline{a} \in \mathrm{Ker}(\varphi) \Leftrightarrow \varphi(\overline{a}) = 1 \Leftrightarrow e^{\frac{2ia\pi}{n}} = 1 \Leftrightarrow a \in n\mathbb{Z} \Leftrightarrow \overline{a} = \overline{0}.$$

  Donc $\mathrm{Ker}(\varphi) = \{\overline{0}\}$ et φ est injective.

- Comme $\mathrm{Card}(\mathbb{Z}/n\mathbb{Z}) = \mathrm{Card}(\mathbb{U}_n) = n$ et φ injective, on en déduit que φ est bijective.

Ainsi, $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ est isomorphe à $(\mathbb{U}_n, \times)$. □

Propriété 3 (Morphisme canonique d'anneaux de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$)

L'application $\pi : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ k & \mapsto & \overline{k} \end{array} \right.$ est un morphisme d'anneaux surjectif, de noyau $n\mathbb{Z}$.

Preuve. L'application π est un morphisme d'anneaux car pour tout $a, b \in \mathbb{Z}$,

$$\pi(a+b) = \overline{a+b} = \overline{a} \oplus \overline{b} = \pi(a) \oplus \pi(b) \qquad \text{et} \qquad \pi(a \times b) = \overline{a \times b} = \overline{a} \otimes \overline{b} = \pi(a) \otimes \pi(b).$$

Elle est surjective par définition. On détermine enfin son noyau :

$$a \in \mathrm{Ker}(\pi) \Leftrightarrow \pi(a) = \overline{0} \Leftrightarrow \overline{a} = \overline{0} \Leftrightarrow a \equiv 0\ [n] \Leftrightarrow a \in n\mathbb{Z}.$$

□

Propriété 4 (Inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$)

(1) Soit $a \in \mathbb{Z}$. Alors $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, $a \wedge n = 1$.

(2) Les assertions suivantes sont équivalentes :

(i) $\mathbb{Z}/n\mathbb{Z}$ est un corps ; (ii) $\mathbb{Z}/n\mathbb{Z}$ est intègre ; (iii) n est premier.

Preuve.

(1) On raisonne directement par équivalence :

$$\begin{aligned} \overline{a} \text{ est inversible } &\Leftrightarrow \exists \overline{u} \in \mathbb{Z}/n\mathbb{Z},\ \overline{u} \otimes \overline{a} = \overline{1} \\ &\Leftrightarrow \exists u \in \mathbb{Z},\ u \times a \equiv 1\ [n] \\ &\Leftrightarrow \exists u, v \in \mathbb{Z},\ u \times a - v \times n = 1 \\ &\Leftrightarrow a \wedge n = 1 \qquad \text{(avec le théorème de Bézout)} \end{aligned}$$

(2) Pour montrer l'équivalence des assertions, on montre (i) ⇒ (ii), (ii) ⇒ (iii) et (iii) ⇒ (i).

(i) ⇒ (ii) : Supposons que $\mathbb{Z}/n\mathbb{Z}$ est un corps. Soient $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$ tels que $\overline{a} \otimes \overline{b} = \overline{0}$. Si $\overline{a} = \overline{0}$, c'est terminé. Sinon, $\overline{a}$ est inversible (car $\mathbb{Z}/n\mathbb{Z}$ est un corps) et en multipliant par $\overline{a}^{-1}$ l'égalité $\overline{a} \otimes \overline{b} = \overline{0}$, on obtient $\overline{b} = \overline{0}$. Donc $\mathbb{Z}/n\mathbb{Z}$ est intègre.

(ii) ⇒ (iii) : Si n n'est pas premier, il existe deux entiers p et q tels que $n = p \times q$ avec $1 < p, q < n$ et on en déduit donc que $\overline{p} \otimes \overline{q} = \overline{pq} = \overline{0}$ avec $\overline{p} \neq \overline{0}$ et $\overline{q} \neq \overline{0}$. Dans ce cas, $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

(iii) ⇒ (i) : Si n est premier, il est premier avec ses prédécesseurs $1, 2, \ldots, n-1$ et d'après le (1), on en déduit que $\overline{1}, \overline{2}, \ldots, \overline{n-1}$ sont inversibles dans $\mathbb{Z}/n\mathbb{Z}$. Ainsi, tous les éléments non nuls de $\mathbb{Z}/n\mathbb{Z}$ sont inversibles et c'est donc un corps.

□

Exemple. L'anneau $\mathbb{Z}/10\mathbb{Z}$ n'est pas intègre car 10 n'est pas premier. L'élément $\overline{7}$ est inversible dans $\mathbb{Z}/10\mathbb{Z}$ car $7 \wedge 10 = 1$. Comme

$$3 \times 7 - 2 \times 10 = 1 \quad \text{et donc} \quad \overline{3} \otimes \overline{7} = \overline{1},$$

l'inverse dans $\mathbb{Z}/10\mathbb{Z}$ de $\overline{7}$ est $\overline{3}$.