# HAX501X – Groupes et anneaux 1

CM3 14/09/2023

Clément Dupont

# Retour sur les exercices du cours

**Exercice 13**

On définit une relation $\sim$ sur $\mathbb{R}^2$ par :

$$\vec{u} \sim \vec{v} \quad \Longleftrightarrow \quad \exists \lambda > 0 \ , \ \vec{u} = \lambda \vec{v}.$$

Montrer que c'est une relation d'équivalence.

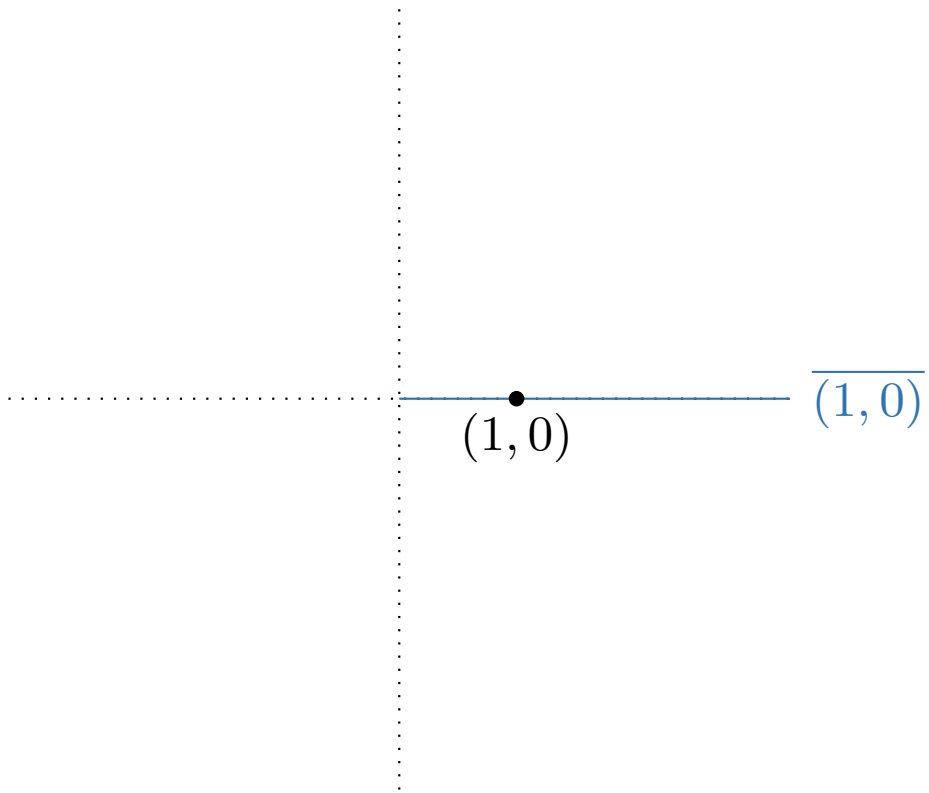
- Réflexivité. Soit $\vec{u} \in \mathbb{R}^2$. On a $\vec{u} = 1\vec{u}$ et $1 > 0$, donc $\vec{u} \sim \vec{u}$.
- Symétrie. Soient $\vec{u}, \vec{v} \in \mathbb{R}^2$ tels que $\vec{u} \sim \vec{v}$. Alors il existe $\lambda > 0$ tel que $\vec{u} = \lambda \vec{v}$. On a donc $\vec{v} = \frac{1}{\lambda}\vec{u}$, et comme $\frac{1}{\lambda} > 0$ on en conclut que $\vec{v} \sim \vec{u}$.
- Transitivité. Soient $\vec{u}, \vec{v}, \vec{w} \in \mathbb{R}^2$ tels que $\vec{u} \sim \vec{v}$ et $\vec{v} \sim \vec{w}$. Alors il existe $\lambda, \mu > 0$ tels que $\vec{u} = \lambda \vec{v}$ et $\vec{v} = \mu \vec{w}$. On a donc $\vec{u} = \lambda\mu\vec{w}$, et comme $\lambda\mu > 0$ on en conclut que $\vec{u} \sim \vec{w}$.

## Exercice 14

Dans le contexte de l'exercice précédent, quelle est la classe d'équivalence de $(1,0)$ ? de $(1,2)$ ? de $(0,0)$ ? Décrire la partition de $\mathbb{R}^2$ en classes d'équivalence.

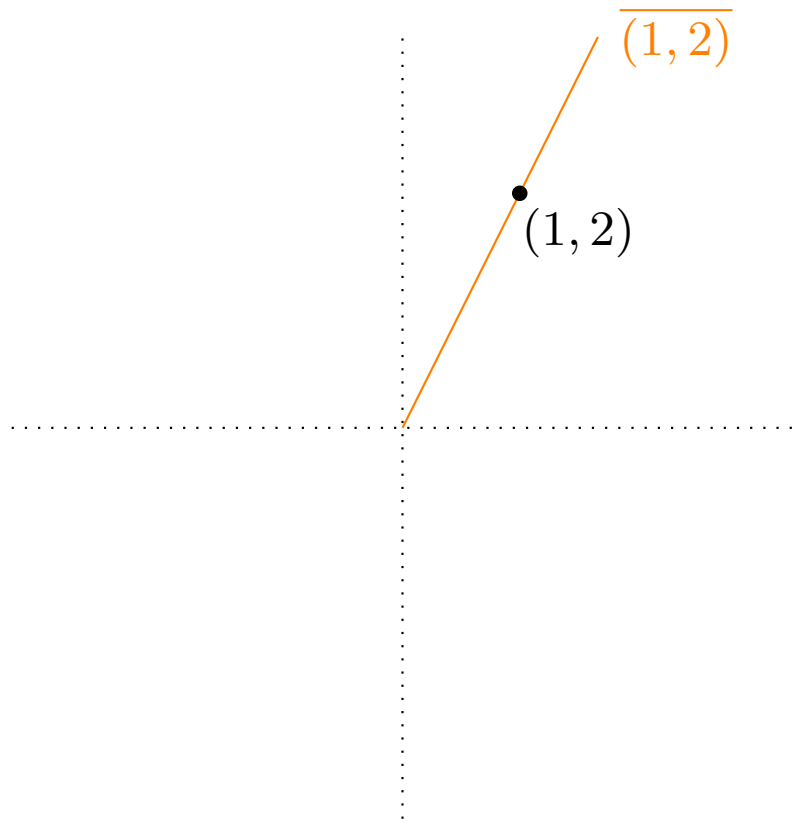
- La classe d'équivalence de $(1,0)$ est :

$$\overline{(1,0)} = \{\lambda(1,0),\ \lambda > 0\} = \{(\lambda,0),\ \lambda > 0\}$$



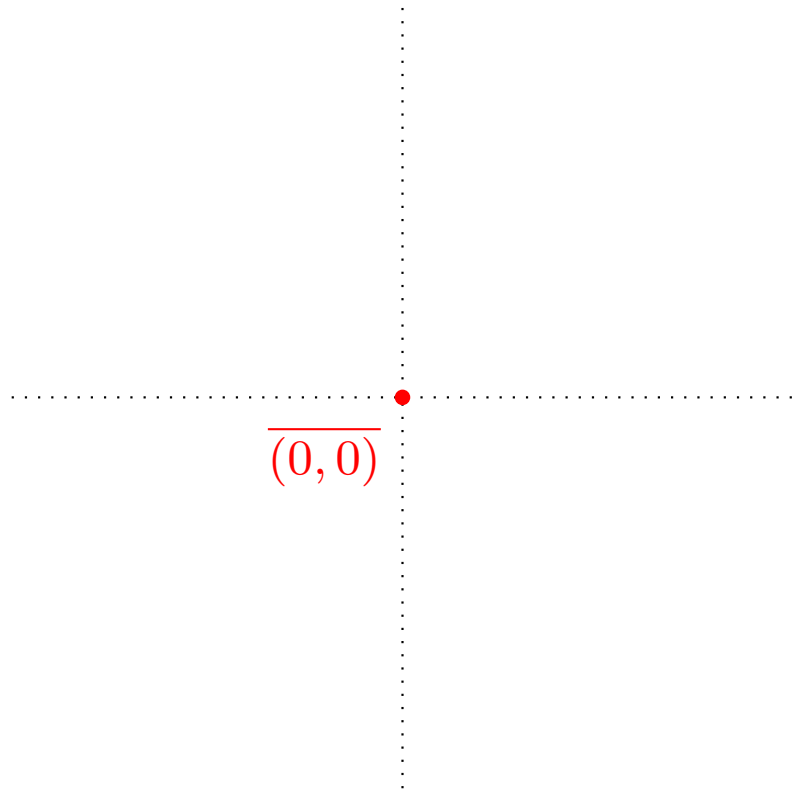
- La classe d'équivalence de $(1, 2)$ est :

$$\overline{(1,2)} = \{\lambda(1,2),\ \lambda > 0\} = \{(\lambda, 2\lambda),\ \lambda > 0\}$$

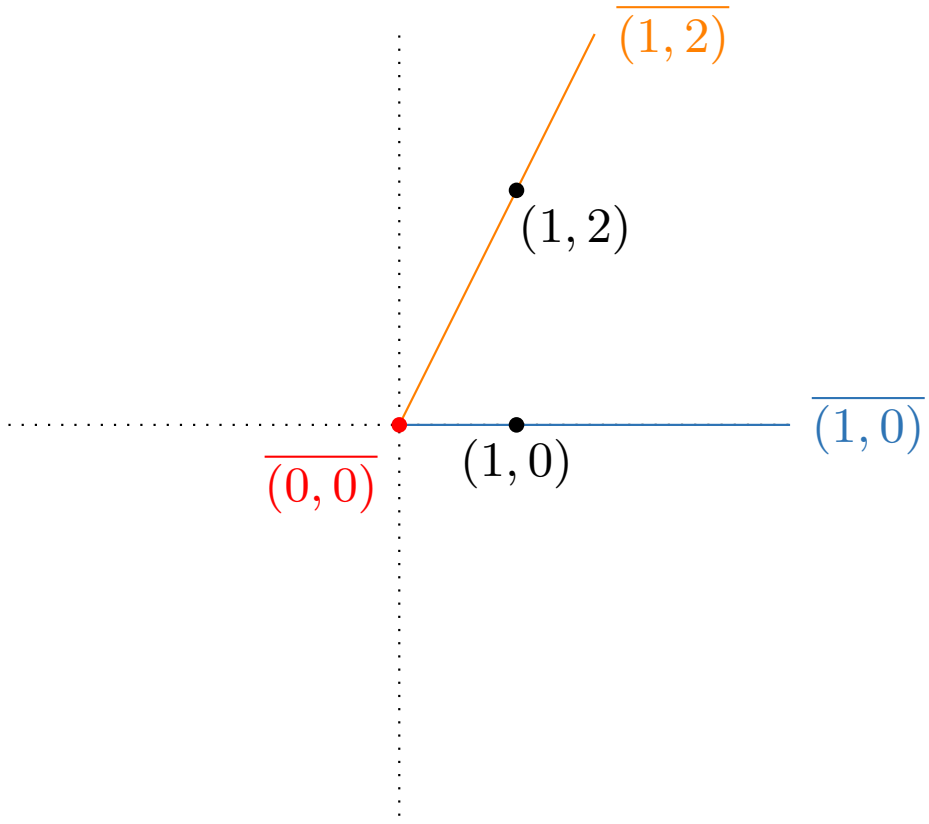


- La classe d'équivalence de $(0,0)$ est :

$$\overline{(0,0)} = \{\lambda(0,0),\ \lambda > 0\} = \{(0,0)\}$$



- Les classes d'équivalence sont toutes les demi-droites (ouvertes) issues de $(0,0)$, et le singleton $\{(0,0)\}$.



## Exercice 15

Les applications suivantes passent-elles au quotient par la relation de congruence modulo $6$ ?

$$f_1 : \mathbb{Z} \longrightarrow \mathbb{Z}\ ,\ n \mapsto (-1)^n\ ;$$

$$f_2 : \mathbb{Z} \longrightarrow \mathbb{Z}\ ,\ n \mapsto n^2 - 1\,.$$

- On montre que $f_1$ passe au quotient par la relation de congruence modulo $6$. Soient $n, n' \in \mathbb{Z}$ tels que $n \equiv n' \pmod 6$. Alors il existe $k \in \mathbb{Z}$ tel que $n = n' + 6k$. Alors :

  $$f_1(n) = (-1)^n = (-1)^{n'+6k} = (-1)^{n'}(-1)^{6k} = f_1(n').$$

  Elle induit donc une application

  $$g_1 : \mathbb{Z}/6\mathbb{Z} \longrightarrow \mathbb{Z}\ ,\ \overline{n} \mapsto (-1)^n.$$

- $f_2$ ne passe **pas** au quotient par la relation de congruence modulo $6$. En effet, on a $0 \equiv 6 \pmod 6$ et

  $$f_2(0) = -1 \quad \neq \quad f_2(6) = 35.$$

# Rappels

## Définition

*On définit $\mathbb{Z}/n\mathbb{Z}$ comme le quotient de l'ensemble $\mathbb{Z}$ par la relation de congruence modulo $n$. Pour un entier $k \in \mathbb{Z}$, on note donc $\overline{k}$ sa classe d'équivalence dans $\mathbb{Z}/n\mathbb{Z}$.*

- On a donc, pour $a, b \in \mathbb{Z}$ :

$$\overline{a} = \overline{b} \quad \text{dans} \quad \mathbb{Z}/n\mathbb{Z} \qquad \Longleftrightarrow \qquad a \equiv b \pmod{n}$$

et donc notamment, pour $a \in \mathbb{Z}$ :

$$\overline{a} = \overline{0} \quad \text{dans} \quad \mathbb{Z}/n\mathbb{Z} \qquad \Longleftrightarrow \qquad n|a.$$

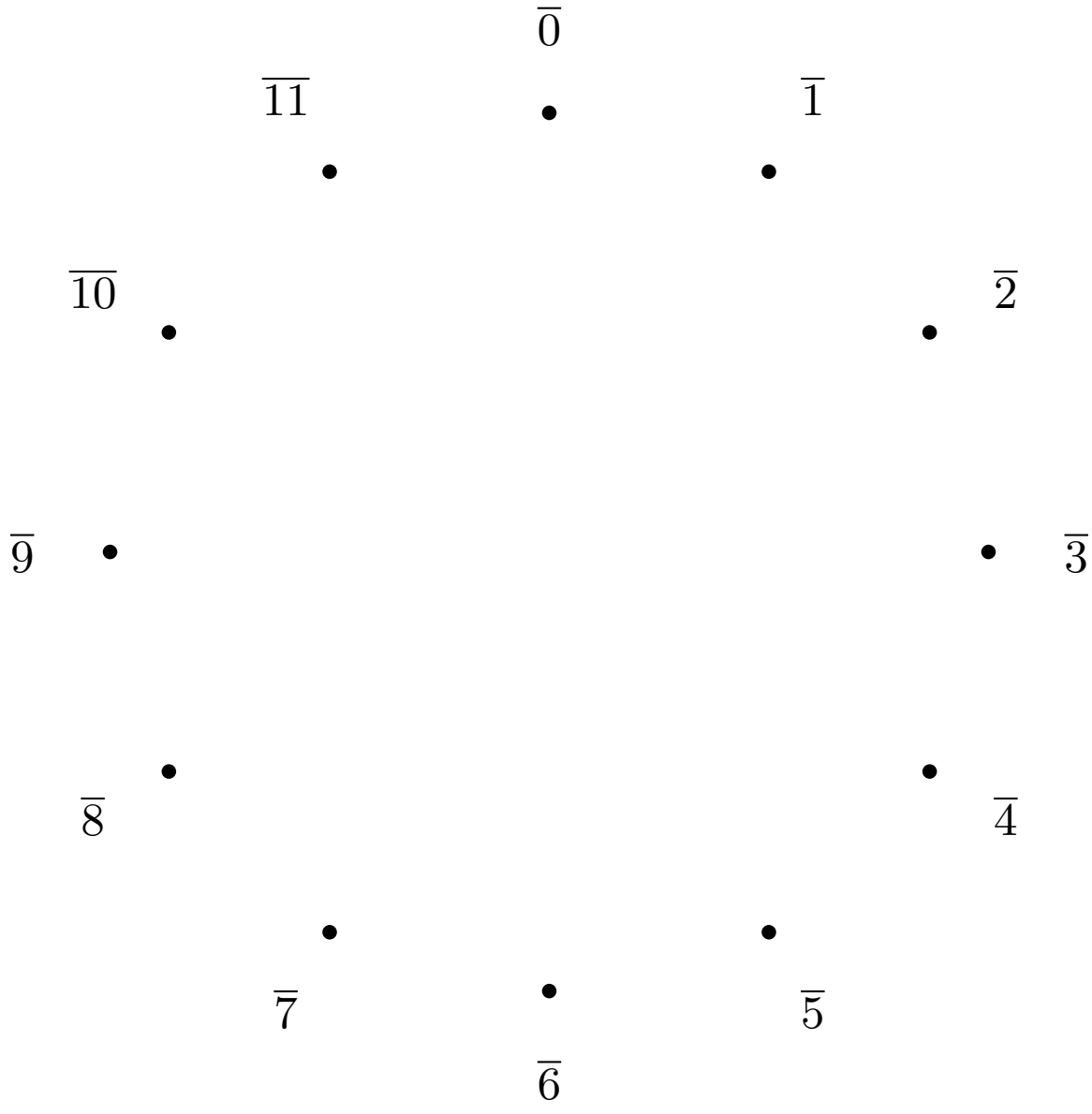
## Exemple

Dans $\mathbb{Z}/7\mathbb{Z}$ on a $\overline{3} = \overline{10} = \overline{73} = \overline{-4}$, qui est l'ensemble des entiers $a \equiv 3 \pmod{7}$, c'est-à-dire l'ensemble des $a \in \mathbb{Z}$ dont le reste dans la division euclidienne par $7$ est $3$, ou encore l'ensemble $\{7k + 3\,,\ k \in \mathbb{Z}\}$.

## Proposition

*L'ensemble $\mathbb{Z}/n\mathbb{Z}$ a $n$ éléments : $\overline{0}$, $\overline{1}, \ldots, \overline{n-1}$.*

# $\mathbb{Z}/12\mathbb{Z}$ est une horloge



# Les lois $+$ et $\times$ dans $\mathbb{Z}/n\mathbb{Z}$

**Proposition**

*L'addition dans $\mathbb{Z}$ passe au quotient et induit une loi $+$ dans $\mathbb{Z}/n\mathbb{Z}$ définie par*

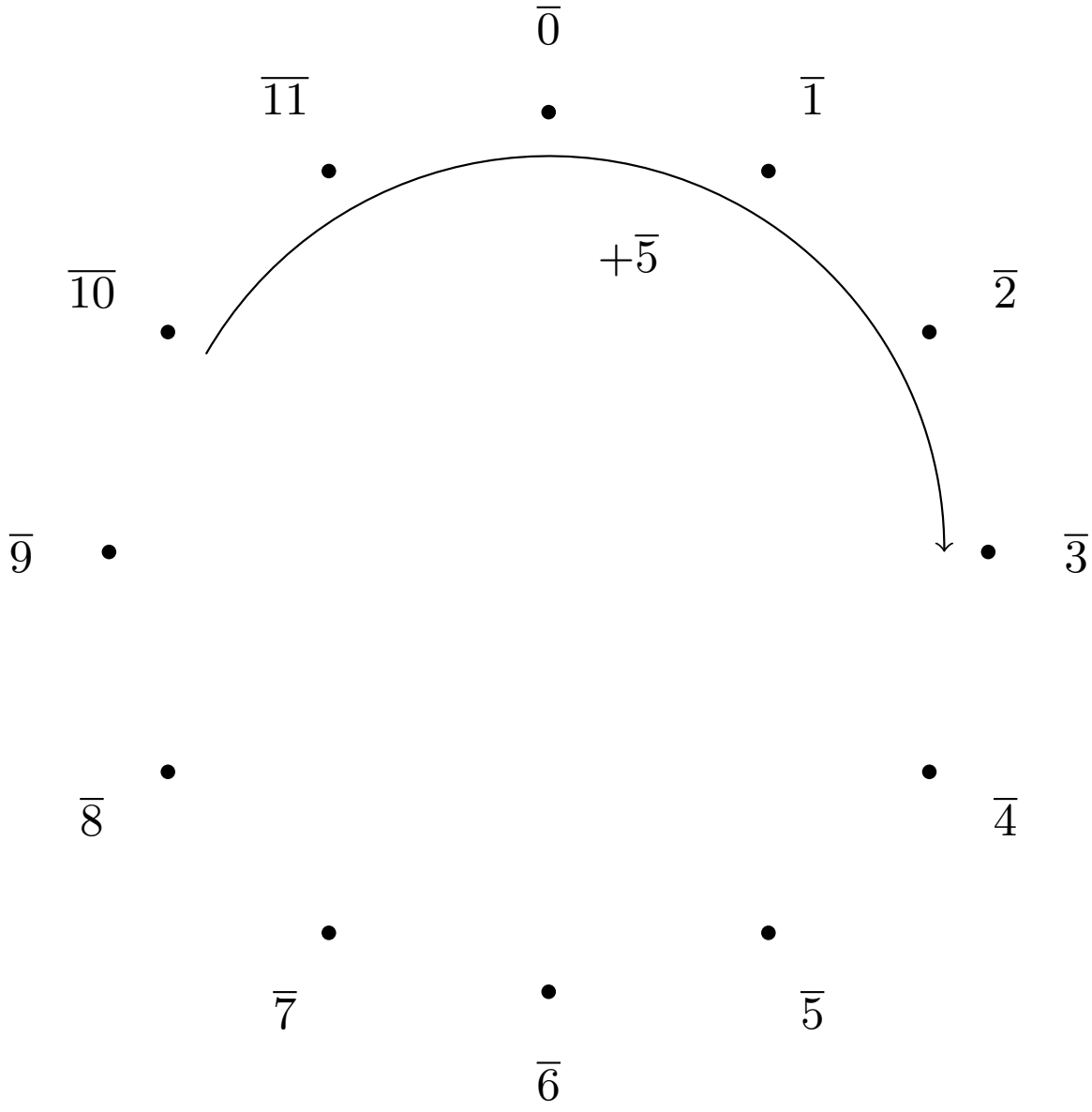
$$\overline{a} + \overline{b} = \overline{a + b}.$$

*La multiplication dans $\mathbb{Z}$ passe au quotient et induit une loi $\times$ dans $\mathbb{Z}/n\mathbb{Z}$ définie par*

$$\overline{a} \times \overline{b} = \overline{a \times b}.$$

## Illustration

- Voici une illustration de l'addition dans $\mathbb{Z}/12\mathbb{Z}$, vu comme une horloge.



# Une table d'addition

**Exercice 16**
Écrire la table d'addition de $\mathbb{Z}/7\mathbb{Z}$.

| $+$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ | $\overline{6}$ |
|---|---|---|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ | $\overline{6}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ | $\overline{6}$ | $\overline{0}$ |
| $\overline{2}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ | $\overline{6}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{3}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ | $\overline{6}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |
| $\overline{4}$ | $\overline{4}$ | $\overline{5}$ | $\overline{6}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
| $\overline{5}$ | $\overline{5}$ | $\overline{6}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
| $\overline{6}$ | $\overline{6}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ |

# $\mathbb{Z}/n\mathbb{Z}$ est un groupe abélien

**Proposition**

$(\mathbb{Z}/n\mathbb{Z}, +)$ *est un* **groupe abélien**, *au sens où on a les propriétés suivantes.*

1) *La loi* $+$ *est associative : pour tous* $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$, $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$.
2) *L'élément* $\overline{0}$ *est élément neutre pour* $+$ *: pour tout* $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{a} + \overline{0} = \overline{a} = \overline{0} + \overline{a}$.
3) *Tout élément* $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ *a un inverse pour la loi* $+$*, qui est* $\overline{-a}$ *:* $\overline{a} + \overline{-a} = \overline{0} = \overline{-a} + \overline{a}$. *On note aussi* $-\overline{a} = \overline{-a}$.
4) *La loi* $+$ *est commutative : pour tous* $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{a} + \overline{b} = \overline{b} + \overline{a}$.

# Exemples (multiplication)

**Exemple**

Dans $\mathbb{Z}/7\mathbb{Z}$ on a $\overline{3} \times \overline{6} = \overline{3 \times 6} = \overline{18} = \overline{11} = \overline{4} = \overline{-10} = \overline{74}$.

**Exercice 17**

Écrire la table de multiplication de $\mathbb{Z}/7\mathbb{Z}$.

# $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif

**Proposition**

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ *est un* **anneau commutatif**, *au sens où on a les propriétés suivantes.*

1) $(\mathbb{Z}/n\mathbb{Z}, +)$ *est un groupe abélien.*
2) *La loi* $\times$ *est associative : pour tous* $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$, $(\overline{a} \times \overline{b}) \times \overline{c} = \overline{a} \times (\overline{b} \times \overline{c})$.
3) *L'élément* $\overline{1}$ *est élément neutre pour* $\times$ *: pour tout* $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{a} \times \overline{1} = \overline{a} = \overline{1} \times \overline{a}$.
4) *La loi* $\times$ *est distributive par rapport à la loi* $+$ *: pour tous* $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{a} \times (\overline{b} + \overline{c}) = (\overline{a} \times \overline{b}) + (\overline{a} \times \overline{c})$ *et* $(\overline{a} + \overline{b}) \times \overline{c} = (\overline{a} \times \overline{c}) + (\overline{b} \times \overline{c})$.
5) *La loi* $\times$ *est commutative : pour tous* $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{a} \times \overline{b} = \overline{b} \times \overline{a}$.

# Inversion dans $\mathbb{Z}/n\mathbb{Z}$

**Définition**

*On dit qu'un élément $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ est* **inversible dans** *$\mathbb{Z}/n\mathbb{Z}$ s'il existe $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{a} \times \overline{b} = \overline{1}$. Dans ce cas, $\overline{b}$ est appelé* **l'inverse** *de $\overline{a}$ dans $\mathbb{Z}/n\mathbb{Z}$ et noté*

$$\overline{b} = \overline{a}^{-1}.$$

- Vu que $\overline{a} \times \overline{b} = \overline{ab}$ par définition, c'est une manière de reformuler la notion d'inversibilité modulo $n$ :

  $$a \text{ est inversible modulo } n \iff \overline{a} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z}.$$

- Ce qu'on gagne à travailler avec $\mathbb{Z}/n\mathbb{Z}$ est la possibilité de parler de

  **l'**inverse de $\overline{a}$.

**Proposition**

*Si $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$, il existe un unique $\overline{b}$ tel que $\overline{a} \times \overline{b} = \overline{1}$.*

# Un rappel... dans le nouveau langage

**Proposition**

*Un élément $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $a \wedge n = 1$.*

- Rappelons que l'inverse de $\overline{a}$ dans $\mathbb{Z}/n\mathbb{Z}$, quand il existe, se calcule en cherchant une relation de Bézout entre $a$ et $n$ : si $au + nv = 1$ alors on a $\overline{au + nv} = \overline{1}$ et donc $\overline{au} = \overline{1}$, d'où $\overline{a} \times \overline{u} = \overline{1}$ et donc

$$\overline{a}^{-1} = \overline{u}.$$

**Exercice 18**

Montrer que $\overline{13}$ est inversible dans $\mathbb{Z}/57\mathbb{Z}$ et calculer son inverse.

# $\mathbb{Z}/p\mathbb{Z}$ est un corps si $p$ est premier

**Théorème**

*Soit $p$ un nombre premier. Alors l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un* **corps**, *au sens où tout élément $\neq \overline{0}$ de $\mathbb{Z}/p\mathbb{Z}$ est inversible.*

# Quelques exercices

## Exercice 19

Calculer les inverses de $\overline{1}, \ldots, \overline{12}$ dans $\mathbb{Z}/13\mathbb{Z}$.

## Exercice 20

Soit $p$ un nombre premier. Montrer qu'on a, pour tous $\overline{a}, \overline{b} \in \mathbb{Z}/p\mathbb{Z}$ :

$$\overline{a} \times \overline{b} = \overline{0} \iff (\overline{a} = \overline{0} \text{ ou } \overline{b} = \overline{0}).$$

Montrer que cette propriété est fausse dans $\mathbb{Z}/n\mathbb{Z}$ si $n$ est composé.

## Exercice 21

Soit $n$ un nombre composé. Montrer que $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps, c'est-à-dire qu'il existe un élément $\neq \overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$ qui n'est pas inversible.

# L'indicatrice d'Euler

**Définition**
*L'***indicatrice d'Euler** *est la fonction* $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ *définie par*

$\varphi(n) =$ *le nombre d'entiers* $k \in \{1, \ldots, n\}$ *qui sont premiers avec* $n$.

- D'après ce qu'on vient de voir, $\varphi(n)$ est le nombre d'éléments parmi $\overline{1}, \ldots, \overline{n}$ qui sont inversibles dans $\mathbb{Z}/n\mathbb{Z}$.
- Donc $\varphi(n)$ est le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

**Exercice 22**

1) Pour $n = 1, \ldots, 12$, lister les inversibles de $\mathbb{Z}/n\mathbb{Z}$ et calculer $\varphi(n)$.
2) Pour un nombre premier $p$, calculer $\varphi(p)$.
3) Pour un nombre premier $p$ et un entier $r \geqslant 1$, calculer $\varphi(p^r)$.

# Le théorème chinois des restes... formulation abstraite

**Théorème (Théorème chinois des restes)**

*Soient $m, n \in \mathbb{N}$ tels que $m \wedge n = 1$. L'application*

$$g : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

*définie par*

$$g(\overline{k}) = (\,\widetilde{k}\,,\,\widehat{k}\,)$$

*est une bijection. (Où l'on utilise les notations $\overline{k}$, $\widetilde{k}$ et $\widehat{k}$ pour désigner les classes d'équivalence dans $\mathbb{Z}/mn\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$, et $\mathbb{Z}/n\mathbb{Z}$ respectivement.)*

**Exercice 23**

Écrire explicitement l'application $g$ dans le cas $m = 3$, $n = 4$, et vérifier qu'elle est bijective. Faire de même dans le cas $m = 2$, $n = 4$, et montrer que dans ce cas-là elle n'est pas bijective.

# Multiplicativité de l'indicatrice d'Euler

**Théorème**

*Soient $m, n \in \mathbb{N}^*$ tels que $m \wedge n = 1$. Alors on a :*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

**Exercice 24**

Déduire du théorème précédent et de l'exercice 22 la formule suivante pour l'indicatrice d'Euler :

$$\varphi(n) = n \times \prod_{\substack{p \text{ premier} \\ p|n}} \left(1 - \tfrac{1}{p}\right).$$

# Définition

## Définition

*Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Le* **sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par $\overline{a}$** *est le sous-ensemble formé par les classes des multiples de $a$ dans $\mathbb{Z}/n\mathbb{Z}$ :*

$$\langle \overline{a} \rangle = \{\overline{ka}\,,\ k \in \mathbb{Z}\}.$$

## Exemple

Dans $\mathbb{Z}/12\mathbb{Z}$ on a $\langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}$.