3 Interlude : le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Proposition. Pour $n \in \mathbb{N}$, la relation de **congruence modulo** n sur $\mathbb{Z}$ est définie par :

$$\begin{aligned} a \equiv b\ [n] &\iff a - b \in n\mathbb{Z} \\ &\iff n \mid a - b \end{aligned}$$

C'est une relation d'équivalence.

Remarque. *Si $n = 0$, il s'agit simplement de l'égalité. Si $n = 1$, tous les entiers sont en relation.*

Preuve :

• Réflexive : Soit $a \in \mathbb{Z}$, $a - a = 0 . n$ donc $a \equiv a\ [n]$

• Symétrique Soit $a, b \in \mathbb{Z}$ tq $a \equiv b\ [n]$

alors $\exists k \in \mathbb{Z}$ tq $a - b = k . n$

donc $b - a = (-k) . n$

donc $b \equiv a\ [n]$

• Transitive Soit $a, b, c \in \mathbb{Z}$ tq $a \equiv b\ [n]$

$b \equiv c\ [n]$

$\exists k, k' \in \mathbb{Z}$ tq $a - b = k . n$

$b - c = k' . n$

donc $a - c = (k + k') . n$

donc $a \equiv c\ [n]$

Donc c'est une relation d'équivalence

Proposition. Pour $n \geqslant 2$, il y a exactement n classes d'équivalences :

$$\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

Définition. On note $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, appelé « $\mathbb{Z}$ sur $n\mathbb{Z}$ ».

Remarque. *On a bien* Card $(\mathbb{Z}/n\mathbb{Z}) = n$.

$\overline{0}$ regroupe tous les entiers congrus à 0 modulo n

$\overline{1}$ " " " 1 " "

$\{1, 1+n, 1+2n, \ldots 1-n, 1-2n \ldots\}$

- Si $a \in \mathbb{Z}$, on effectue la div euclidienne de a par n :

$$\begin{cases} a = nq + r \\ 0 \leq r \leq n-1 \end{cases}$$

alors $a \equiv r \ [n]$

donc $\overline{a} = \overline{r} \in \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$

- Si on considère deux éléments de $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$

notés x_1, x_2

ce sont des classes d'équivalences

donc $\exists a_1, a_2 \in \{0, \ldots, n-1\}$ tq $x_1 = \overline{a_1}$ $x_2 = \overline{a_2}$

si $x_1 = x_2$ alors $\overline{a_1} = \overline{a_2}$

ie $a_1 \equiv a_2 \ [n]$

donc $a_1 - a_2 \equiv 0 \ [n]$

ie $\exists k \in \mathbb{Z}$ tq $a_1 - a_2 = kn$

car $a_1, a_2 \in \{0, \dots, n-1\}$

donc $a_1 - a_2 \in \{-(n-1), \dots, +(n-1)\}$

0 est le seul multiple de n

donc $a_1 - a_2 = 0$ ie $a_1 = a_2$

Donc les classes d'équivalence $\bar{0}, \bar{1}, \dots, \overline{n-1}$

sont 2 à 2 distinctes, donc au nombre de n.

On note $\{\bar{0}, \bar{1}, \dots, \overline{n-1}\} = \mathbb{Z}/n\mathbb{Z}$

Proposition. Pour $n \geqslant 2$, il existe une unique loi de groupe sur $\mathbb{Z}/n\mathbb{Z}$, encore notée $+$, pour laquelle l'application $\pi : k \mapsto \overline{k}$ soit un morphisme de groupes, i.e. :

$$\forall a, b \in \mathbb{Z},\ \overline{a+b} = \overline{a} + \overline{b}$$

De plus, $\operatorname{Ker} \pi = n\mathbb{Z}$.

Remarque. *Ainsi, pour additionner deux classes d'équivalences, on additionne deux représentants de ces classes d'équivalences.*

Corollaire. Pour $n \in \mathbb{N}^*$, $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ et $k \in \mathbb{Z}$,

$$k \cdot \overline{a} = \overline{ka}$$

$\pi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}/n\mathbb{Z}, ?)$ surjective par déf de $\mathbb{Z}/n\mathbb{Z}$

$a \longmapsto \overline{a}$

On définit $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$

$(x, y) \longmapsto x+y$ défini par

$x+y = \overline{(a+b)}$ où $x = \overline{a}$ et $y = \overline{b}$

Cette déf est indépendante du choix de a, b représentant x et y (rmq)

Si $x = \overline{a'}$ et $y = \overline{b'}$

$$(a'+b') - (a+b) = \underbrace{(a'-a)}_{k_1 n} + \underbrace{(b'-b)}_{k_2 n}$$

$$= (k_1 + k_2)\, n$$

donc $a' + b' \equiv a + b \ [n]$

donc $\overline{a'+b'} = \overline{a+b}$

Remarque : Π morphisme de groupes.

Sous-entend que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe.

→ $+$ est une loi de comp. interne ✓

→ $+$ est associative [...]

→ $+$ admet un neutre : $\bar{0}$

$\forall x \in \mathbb{Z}/n\mathbb{Z} \quad \exists a \in \mathbb{Z}$ tq $x = \bar{a}$

$$x + \bar{0} = \bar{a} + \bar{0}$$
$$= \overline{(a+0)}$$
$$= \bar{a} \qquad = \bar{0} + x$$

→ Tout élément admet un symétrique

Soit $x \in \mathbb{Z}/n\mathbb{Z}$. $\exists a \in \mathbb{Z}$ tq $x = \bar{a}$

$$x + \overline{(-a)} = \bar{a} + \overline{(-a)}$$
$$= \overline{(a + (-a))}$$
$$= \bar{0} \quad \text{neutre}$$
$$= \overline{(-a)} + x$$

donc x admet un symétrique, qui est $\overline{(-a)}$.

Abus : $-\bar{a} = \overline{(-a)}$

→ $+$ est commutative.

Π morphisme de groupe : bien ouï !

$$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$a \longmapsto \overline{a}$$

$$\pi(a+b) = \pi(a) + \pi(b)$$
$$\overline{(a+b)} = \overline{a} + \overline{b}$$

Conséquence :

$$\forall k \in \mathbb{Z} \quad \overline{(ka)} = k.(\overline{a})$$

Propriété : $\ker \pi = n\mathbb{Z}$

$$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$a \longmapsto \overline{a}$$

En effet :

$$a \in \ker \pi \iff \pi(a) = 0_{\mathbb{Z}/n\mathbb{Z}} = \overline{0}$$

$$\iff \overline{a} = \overline{0}$$

$$\iff a \equiv 0 \ [n]$$

$$\iff a \text{ multiple de } n$$

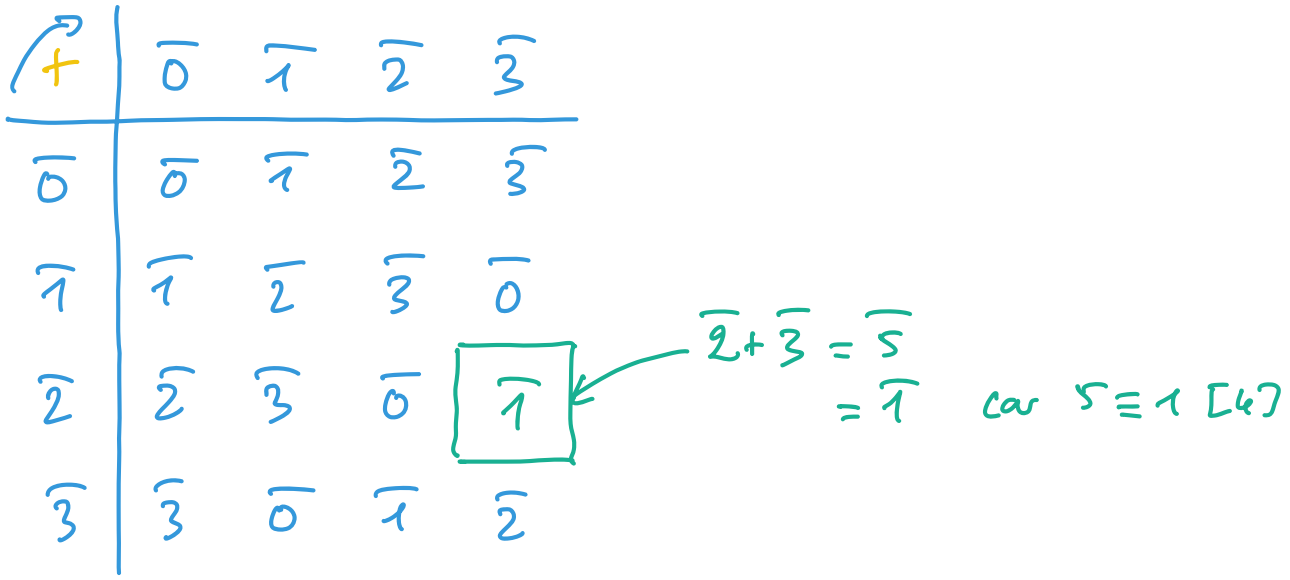
Donc $\ker \pi = n\mathbb{Z}$

$$\pi(n+1) = \overline{n+1} = \overline{n} + \overline{1} = \overline{0} + \overline{1} = \overline{1}$$

$$= \overline{n+1} \quad \text{or} \quad n+1 \equiv 1 \ [n]$$

Proposition. Muni de cette loi, $\big(\mathbb{Z}/n\mathbb{Z}, +\big)$ est donc bien un groupe commutatif.

Exemple. Construire la table de la loi $+$ dans $\mathbb{Z}/4\mathbb{Z}$.



Générateurs de $\mathbb{Z}/n\mathbb{Z}$.

Soit n entier $\geqslant 2$. Sont équivalentes :

(*i*) $\mathbb{Z}/n\mathbb{Z} = \langle \overline{a} \rangle$

(*ii*) il existe $k \in \mathbb{N}$ tel que $\overline{ka} = \overline{1}$ $\quad \overline{k} \times \overline{a} = \overline{1}$

(*iii*) $a \wedge n = 1$

Remarque. *Ainsi, $(\mathbb{Z}/n\mathbb{Z}, +)$ est engendré par chaque $\overline{k}$, où $k \in \{0, \dots, n-1\}$ est premier avec n.*

Exemple. Donner la liste des éléments qui engendrent $(\mathbb{Z}/12\mathbb{Z}, +)$.

(ii) $\Leftrightarrow$ (iii)

$a \wedge n = 1 \iff \exists k, v \in \mathbb{Z}$ tq $ka + vn = 1$

(Bézout)

$\iff \exists k \in \mathbb{Z}$ tq $(\exists v \in \mathbb{Z}$ tq $ka - 1 = vn)$

$\iff \exists k \in \mathbb{Z} \quad ka \equiv 1 \ [n]$

$\iff \overline{ka} = \overline{1}$

(ii) $\Rightarrow$ (i)

On suppose $\exists k \in \mathbb{Z}$ tq $\overline{ka} = \overline{1}$

Mque $\mathbb{Z}/n\mathbb{Z} = \langle \overline{a} \rangle$

$\supset$ $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ groupe.

$\subset$ Soit $x \in \mathbb{Z}/n\mathbb{Z}$.

$\exists b \in \mathbb{Z}$ tq $x = \overline{b}$

Alors $x = \overline{b}$

$= \overline{b \cdot 1}$

$= b\,\overline{1}$

$= b.\,\overline{ka}$

$= b.k.\,\overline{a}$

$\in \langle \overline{a} \rangle$

(i) ⇒ (ii)

Un sup $\mathbb{Z}/n\mathbb{Z} = \langle \overline{a} \rangle$

donc $\overline{1} \in \langle \overline{a} \rangle$ donc $\exists k \in \mathbb{Z}$ tq $\overline{1} = k\,\overline{a}$

$= \overline{ka}$

Exemple: $\mathbb{Z}/12\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{11}\}$

$1 \wedge 12 = 1$ $\qquad$ $12 = 2.2.3$

$5 \wedge 12 = 1$

$7 \wedge 12 = 1$

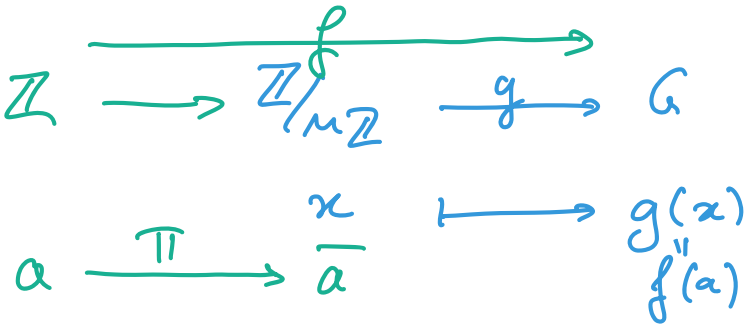
$11 \wedge 12 = 1$

donc $\mathbb{Z}/12\mathbb{Z} = \langle \overline{1} \rangle$

$= \langle \overline{5} \rangle$

$= \langle \overline{7} \rangle$

$= \langle \overline{11} \rangle$



ℤ/4ℤ
$\bar{5} = \bar{1}$

Comment définir un morphisme $\mathbb{Z}/n\mathbb{Z} \to G$.

Soit n entier $\geqslant 2$, et $\pi : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ k & \mapsto & \bar{k} \end{array}$.

Si G est un groupe et $f : \mathbb{Z} \to G$ un morphisme de groupes, alors les propriétés suivantes sont équivalentes :

(i) il existe un morphisme $g : \mathbb{Z}/n\mathbb{Z} \to G$ tel que $f = g \circ \pi$

(ii) $n\mathbb{Z} \subset \operatorname{Ker} f$

Remarque. *Ainsi, pour définir un morphisme de groupe $\mathbb{Z}/n\mathbb{Z} \to G$, on définit un morphisme de groupe $\mathbb{Z} \to G$ dont le noyau contient $n\mathbb{Z}$, et on « passe au quotient ».*

Proposition. Les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{U}_n, \times)$ sont isomorphes.

En effet : $f : \mathbb{Z} \longrightarrow G$ morphisme de groupes.

$\Rightarrow$ On suppose $\exists g : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$ morphisme de groupes tq $f = g \circ \pi$

$\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \xrightarrow{g} G$, f

Alors $n\mathbb{Z} \subset \operatorname{Ker} f$

Soit $a \in n\mathbb{Z}$ ie $\exists k \in \mathbb{Z}$ tq $a = nk$

$$\begin{aligned} f(a) &= f(nk) \\ &= g \circ \pi(nk) \\ &= g(\overline{nk}) \\ &= g(\bar{0}) \\ &= 0_G \end{aligned}$$

car g morphisme de groupes.

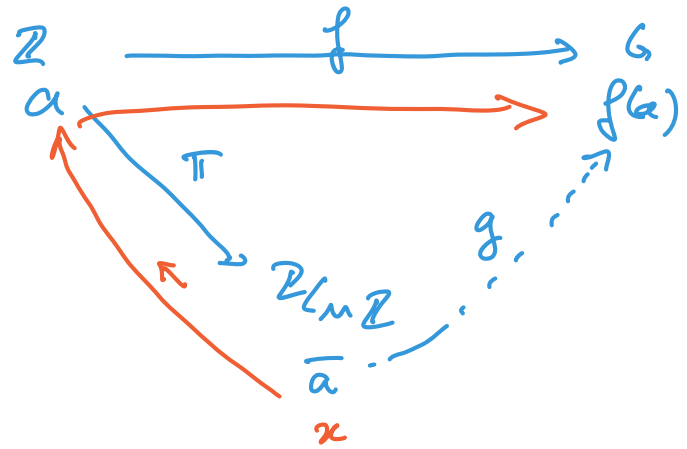
donc $a \in \operatorname{Ker} f$.

$\Leftarrow$ Supposons $n\mathbb{Z} \subset \ker f$.

Montrer $\exists g : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$ morphisme tq $f = g \circ \pi$

montrer une existence

trouver g !



Posons : $g : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$

$x \longmapsto f(a)$ où $\bar{a} = x$

Justifions que g est bien définie :

Si $x = \bar{a} = \bar{b}$, est-ce que $f(a) = f(b)$?

$\bar{a} = \bar{b}$ donc $a - b \equiv 0 \ [n]$

donc $f(a) - f(b) = f(a-b) = f(k.n)$

$= 0_G$ car $k.n \in n\mathbb{Z} \subset \ker f$.

donc la déf de g est correcte.

g est un morphisme de groupes

Soit $x, y \in \mathbb{Z}/n\mathbb{Z}$, $a, b \in \mathbb{Z}$ tq $x = \bar{a}$, $y = \bar{b}$

$g(x+y) = g(\bar{a} + \bar{b})$

$$= g(\overline{a+b})$$

$$= f(a+b)$$

$$= f(a) + f(b) \quad \text{car } f \text{ morphisme}$$

$$= g(x) + g(y)$$

$$\underline{f = g \circ \pi}$$

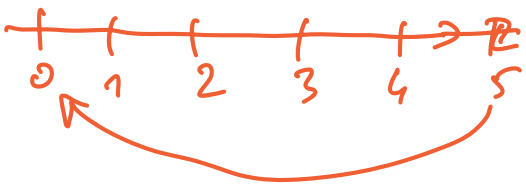
Bon sinon ...

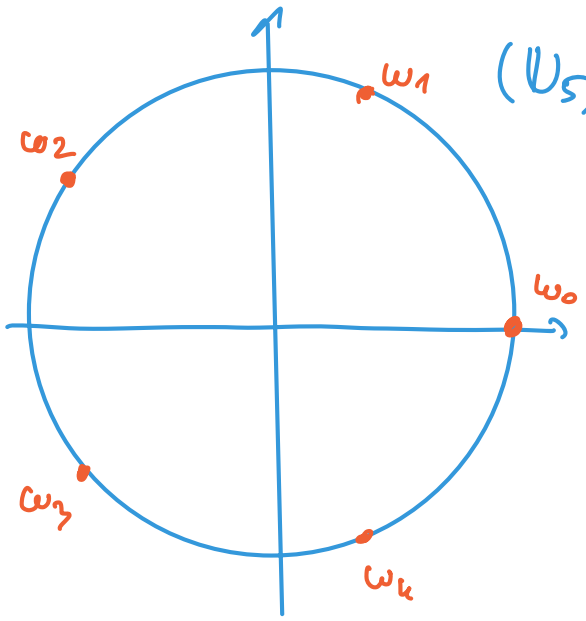
$$g \circ \pi(a) = g(\bar{a}) = f(a)$$

Exemple:

$\mathbb{Z}/5\mathbb{Z}$ $\xrightarrow{\text{isomorphe}}$ $(U_5, \times)$

$\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$





$$\omega_k = e^{i\frac{2k\pi}{5}}$$

Preuve:

On veut définir un isomorphisme entre $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(U_n, \times)$

Posons : $f : (\mathbb{Z}, +) \longrightarrow (\mu_n, \times)$

$$k \longmapsto e^{i\frac{2k\pi}{n}}$$

f est un morphisme de groupes

surjectif.

$$k \in \ker f \iff e^{i\frac{2k\pi}{n}} = 1_{\mu_n} = 1_{\mathbb{C}} = 1$$

$$\iff \frac{2k\pi}{n} \equiv 0 \quad [2\pi]$$

$$\iff k \in n\mathbb{Z}$$

donc $n\mathbb{Z} = \ker f$.

On note donc

$$g : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mu_n$$

$$x \longmapsto e^{i\frac{2k\pi}{n}}$$

où $\overline{k} = x$

et on a $f = g \circ \pi$, g morphisme

donc g est surjective (ça l'est !)

si $x \in \ker g$, $x = \pi(k)$ où $k \in \ker f$

donc $x = \overline{0}$

donc g injective.