

# Algèbre et Arithmétique Effectives -

06 / 11 / 26  
cours 8

Soit  $(A, +, \cdot)$  un anneau commutatif.

On rappelle que  $(A, +)$  est un groupe abélien.

Def: Soit  $(A, +, \cdot)$  un anneau commutatif.

Un idéal de  $A$  est un sous-ensemble  $I$  de  $A$  tel que  $(I, +)$  est un sous-groupe de  $(A, +)$  et tel que  $\forall x \in I, \forall a \in A, ax \in I$ .

Exemple:  $(\mathbb{Z}, +, \cdot)$  est un anneau commutatif.

On montre que  $\forall n \in \mathbb{Z}_{\geq 0}, I = n\mathbb{Z}$  est un idéal.

On a déjà vu que  $(n\mathbb{Z}, +)$  est un sous-groupe de  $(\mathbb{Z}, +)$ .

Soient  $x \in n\mathbb{Z}$  et  $a \in \mathbb{Z} \Rightarrow \exists k \in \mathbb{Z}$  tel que  $x = nk$ . Donc on a :

$$xa = nka = n(\underbrace{ka}_{\in \mathbb{Z}}) \in n\mathbb{Z}.$$

Soient  $(A, +, \cdot)$  un anneau commutatif et  $I$  un idéal de  $A$ . On considère la relation suivante :

$$\forall a, b \in A, a \sim_I b \Leftrightarrow a - b \in I$$

On a vu hier que  $\sim_I$  est une relation d'équivalence dont,  $\forall a \in A$ , la classe d'équivalence de  $a$  est :

$$[a]_I = \{a + x : x \in I\}$$

On note l'ensemble des classes d'équivalence :

$$A/I = \{[a]_I, a \in A\}$$

On peut définir deux opérations sur  $A/I$  :

$$(\text{addition}) : + : A/I \times A/I \rightarrow A/I$$

$$([a]_I, [b]_I) \mapsto [a]_I + [b]_I := [a+b]_I$$

$$(\text{multiplication}) : \cdot : A/I \times A/I \rightarrow A/I$$

$$([a]_I, [b]_I) \mapsto [a]_I \cdot [b]_I := [ab]_I$$

On a déjà vu que l'addition est bien définie.

Montrons que la multiplication est aussi bien définie :

Soient  $a' \sim_I a$  et  $b' \sim_I b$ . On veut montrer que  $a'b' \sim_I ab$ .

$$a' \sim_I a, b' \sim_I b \Rightarrow a'-a \in I \text{ et } b'-b \in I \Rightarrow$$

$$\Rightarrow \exists x, y \in I \text{ tels que } a'-a=x \text{ et } b'-b=y.$$

Alors on a :

$$a'b' = (x+a)(y+b) = xy + xb + ay + ab \Rightarrow$$

$$\Rightarrow a'b' - ab = \underbrace{xy + xb + ay}_{\in I \text{ parce que } I \text{ est un idéal.}} + ab$$

$$\Rightarrow a'b' \sim_I ab$$

(Note que si  $I$  n'était pas un idéal l'opération de multiplication ne serait pas bien définie).

Proposition : Soit  $(A, +, \cdot)$  un anneau commutatif et soit  $I$  un idéal de  $A$ .

Alors  $(A/I, +, \cdot)$  est un anneau commutatif, appelé anneau quotient.

# Homomorphismes (ou morphismes) de groupes

Considérons les groupes suivants :

- $\mathbb{Z}/15\mathbb{Z}$  avec l'addition classique

- $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$  avec l'opération suivante

$$+ : (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \rightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

$$((a_1, b_1), (a_2, b_2)) \mapsto (a_1 + a_2, b_1 + b_2)$$

exemple :  $(2, 4) + (1, 3) = (0, 2)$

Par le théorème des restes chinois on a déjà vu qu'il existe une bijection :

$$\Theta : \mathbb{Z}/15\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

$$[a]_{15} \longmapsto ([a]_3, [a]_5)$$

exemple :  $\Theta(7) = (1, 2)$

$$\Theta(10) = (1, 0)$$

etc.

De plus  $\Theta$  est "compatible" avec les lois d'addition de  $\mathbb{Z}/15\mathbb{Z}$  et  $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ .

En effet on a :

$$\Theta([a]_{15} + [b]_{15}) = \Theta([a+b]_{15}) = ([a+b]_3, [a+b]_5) =$$

$$\begin{aligned}
 &= \left( [\alpha]_3 + [\beta]_3, [\alpha]_5 + [\beta]_5 \right) = \left( [\alpha]_3, [\alpha]_5 \right) + \left( [\beta]_3, [\beta]_5 \right) \\
 &\quad + \text{dans } \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\
 &= \Theta([\alpha]_{15}) + \Theta([\beta]_{15}).
 \end{aligned}$$

Donc on a montré que  $\forall a, b \in \mathbb{Z}/15\mathbb{Z}$

$$\Theta(a+b) = \Theta(a) + \Theta(b)$$

compatibilité avec les opérations

En conclusion  $\Theta$  est une bijection entre  $\mathbb{Z}/15\mathbb{Z}$  et  $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$  qui est compatible avec leurs lois

de groupe. On dit que  $\Theta$  est un isomorphisme de groupes et que  $\mathbb{Z}/15\mathbb{Z}$  et  $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$  sont deux groupes isomorphes, c'est à dire qu'ils sont la même chose d'un point de vue algébrique.

On écrit :

$$\mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

Consequences :

- $\mathbb{Z}/15\mathbb{Z}$  est cyclique  $\Rightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$  est cyclique
- $l$  est un générateur de  $\mathbb{Z}/15\mathbb{Z} \Rightarrow \Theta(l) = (1,1)$  est un générateur de  $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ .
- $\langle 3 \rangle$  est un sous-groupe de  $\mathbb{Z}/15\mathbb{Z}$  d'ordre 5  
 $\Rightarrow \Theta(\langle 3 \rangle) = \langle \Theta(3) \rangle = \langle (0,3) \rangle$  est un sous-groupe d'ordre 5 de  $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$
- etc.

Déf : Soient  $(G, *)$  et  $(H, \Delta)$  deux groupes.

Une application  $\varphi: G \rightarrow H$  est dite un homomorphisme de groupes si

$$\forall a, b \in G, \varphi(a * b) = \varphi(a) \Delta \varphi(b).$$

L'image de  $\varphi$  est

$$\varphi(G) := \{\varphi(a) : a \in G\} \subseteq H$$

Le noyau de  $\varphi$  est

$$\text{Ker}(\varphi) := \{a \in G : \varphi(a) = \text{id}_H\} \subseteq G.$$

### Exemples

1)  $\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$

$$a \longmapsto [a]_n$$

$\varphi$  est un homomorphisme car  $\forall a, b \in \mathbb{Z}$

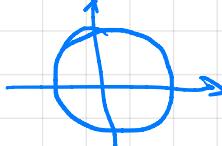
$$\varphi(a+b) = [a+b]_n = [a]_n + [b]_n = \varphi(a) + \varphi(b).$$

def d'addition  
dans  $\mathbb{Z}/n\mathbb{Z}$

2)  $f: (\mathbb{R}, +) \longrightarrow (S^1, \cdot)$

$$x \longmapsto e^{ix} = \cos(x) + i \sin(x)$$

$S^1 = \{z \in \mathbb{C} : |z| = 1\}$



On a :

Soient  $x, y \in \mathbb{R}$ ,

$$f(x+y) = e^{i(x+y)} = e^{ix} \cdot e^{iy} = f(x) \cdot f(y)$$

Donc  $f$  est un homomorphisme de groupes.