Algèbre et Arithmétique Effectives — 05/11/25
Cours 8

Hier on a vu que l'application

$$\begin{aligned}\theta : \mathbb{Z}/15\mathbb{Z} &\longrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ [a]_{15} &\longmapsto ([a]_3, [a]_5)\end{aligned}$$

est une bijection qui est compatible avec les opérations définies sur $\mathbb{Z}/15\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

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

On écrit :

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

Conséquences :

- $\mathbb{Z}/15\mathbb{Z}$ est cyclique $\Longrightarrow$ $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ est cyclique

- 1 est un générateur de $\mathbb{Z}/15\mathbb{Z}$ $\Longrightarrow$ $\theta(1) = (1,1)$ est un générateur de $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

- $\langle 3 \rangle \leq \mathbb{Z}/15\mathbb{Z}$ est sous-groupe de $\mathbb{Z}/15\mathbb{Z}$ d'ordre 5

  $\Longrightarrow$ $\theta(\langle 3 \rangle) = \langle \theta(3) \rangle = \langle (0,3) \rangle$ est un sous-groupe d'ordre 5 de $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

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

Une application $\varphi : G \to H$ est dite un <u>homomorphisme</u> (ou <u>morphisme</u>) de groupes si

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

opération dans G

opération dans H

L'<u>image</u> de φ est

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

Le <u>noyau</u> de φ est

$$\mathrm{Ker}(\varphi) = \{a \in G : \varphi(a) = 1_H\} \subseteq G$$

<u>Exemples</u>

1) $n \in \mathbb{Z}_{>0}$

$$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$a \longmapsto [a]_n$$

φ est un homomorphisme de groupes, car $\forall\, a, b \in \mathbb{Z}$:

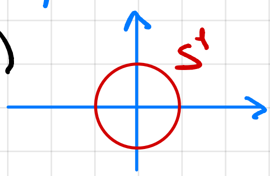
$$\varphi(a+b) = [a+b]_n = [a]_n + [b]_n = \varphi(a) + \varphi(b).$$

déf. de l'addition dans $\mathbb{Z}/n\mathbb{Z}$

$$\mathrm{Ker}(\varphi) = \{a \in \mathbb{Z} : \varphi(a) = [0]_n\} =$$
$$= \{a \in \mathbb{Z} : a \equiv 0 \pmod n\} = n\mathbb{Z}$$

2) $$f : (\mathbb{R}, +) \longrightarrow (S^1, \cdot)$$
$$x \longmapsto e^{ix} = \cos(x) + i\sin(x)$$

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



f est un homomorphisme de groupes ?

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

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

Donc oui, f est homom. de groupes.

<u>Remarques</u>

Soit $\varphi : (G, *) \to (H, \Delta)$ un homomorphisme de groupes.

Alors :

1) $\varphi(1_G) = 1_H$.

<u>dém</u> : $\varphi(1_G) = \varphi(1_G * 1_G) = \varphi(1_G) \Delta \varphi(1_G) \Rightarrow$

$\Rightarrow \varphi(1_G)^{-1} \Delta \varphi(1_G) = \varphi(1_G)^{-1} \Delta \varphi(1_G) \Delta \varphi(1_G) \Rightarrow$

$\Rightarrow 1_H = 1_H \Delta \varphi(1_G) = \varphi(1_G)$

2) $\forall\, a \in G, \quad \varphi(a^{-1}) = (\varphi(a))^{-1}$

<u>dém</u> : $1_H = \varphi(1_G) = \varphi(a * a^{-1}) = \varphi(a) \Delta \varphi(a^{-1})$

$\Rightarrow (\varphi(a))^{-1} = \varphi(a^{-1})$.

<u>Proposition</u> : Soient $(G, *)$ et (G', Δ) deux groupes et soit $\varphi : G \to G'$ un homomorphisme de groupes. Alors on a :

1) Si H est un sousgroupe de $G \Rightarrow \varphi(H)$ est un sous-groupe de G'

2) Si H' est un sous-groupe de $G' \Rightarrow$ $\Rightarrow \varphi^{-1}(H') := \{ a \in G : \varphi(a) \in H' \}$ est un sous-groupe de G.

3) $\mathrm{Ker}(\varphi)$ est un sous-groupe de G et $\mathrm{Im}(\varphi)$ est un sous-groupe de G'

4) φ est injective $\Longleftrightarrow$ $\mathrm{Ker}(\varphi) = \{1_G\}$

<u>Dém</u>

1) Soient $\alpha, \beta \in \varphi(H)$. On montre que $\alpha \triangle \beta^{-1} \in \varphi(H)$

Si $\alpha, \beta \in \varphi(H) \Rightarrow \exists\ a, b \in H$ tels que $\varphi(a) = \alpha$ et $\varphi(b) = \beta$.

Donc

$$\alpha \triangle \beta^{-1} = \varphi(a) \triangle [\varphi(b)]^{-1} = \varphi(a) \triangle \varphi(b^{-1}) =$$
$$= \varphi(\underbrace{a * b^{-1}}_{\in H, \text{ car } H \text{ est un sous-groupe}}) \Rightarrow \alpha \triangle \beta^{-1} \in \varphi(H)$$

2) Laissé par exercice.

$$\overbrace{H'}^{\{1_{G'}\}}$$

3) $\mathrm{Ker}(\varphi) = \{a \in G : \varphi(a) = 1_{G'}\} = \{a \in G : \varphi(a) \in \{1_{G'}\}\} = \varphi^{-1}(\{1_{G'}\})$

Puisque $\{1_{G'}\}$ est un sous-groupe de G', avec ② on conclut que $\mathrm{Ker}(\varphi)$ est un sous-groupe de G

$\mathrm{Im}(\varphi) = \varphi(G)$ et G est un sous-groupe de G. Donc ① nous dit que $\mathrm{Im}(\varphi)$ est un sous-groupe de G'.

4) $\Rightarrow$) Supposons que φ est injective.

On sait que $\varphi(1_G) = 1_{G'}$ et puisque φ est injective, $\forall\ a \neq 1_G$ on $\varphi(a) \neq 1_{G'}$.

Donc $\mathrm{Ker}(\varphi) = \{1_G\}$

$\Leftarrow$) Supposons que $\mathrm{Ker}(\varphi) = \{1_G\}$.

Soient $a, b \in G$ tels que $\varphi(a) = \varphi(b)$

$\Rightarrow \varphi(a) \triangle (\varphi(b))^{-1} = 1_{G'} \Rightarrow \varphi(a) \triangle \varphi(b^{-1}) = 1_{G'}$

$\Rightarrow \varphi(a * b^{-1}) = 1_{G'} \Rightarrow a * b^{-1} \in \operatorname{Ker}(\varphi) = \{1_G\}$

$\Rightarrow a * b^{-1} = 1_G \Rightarrow a = b \Rightarrow \varphi$ est injective.

<u>Proposition</u> : Si $\varphi : G \to G'$ et $\psi : G' \to G''$ sont deux homomorphismes de groupes, alors

$$\psi \circ \varphi : G \to G''$$

est un homomorphisme de groupes.

<u>Dém</u> : laissée par exercice

<u>Déf</u> : Un homomorphisme de groupe $\varphi : G \to H$ est un <u>isomorphisme</u> si φ est bijective.

Dans ce cas les groupes G et H sont dits <u>isomorphes</u> et on écrit $G \simeq H$.

Si $G = H$, un homomorphisme $\varphi : G \to G$ est appelé un <u>endomorphisme</u> de G et un endomorphisme bijectif est appelé un <u>automorphisme</u> de G.

<u>Exemples</u>

1) $\left(\mathbb{Z}/4\mathbb{Z}\right)^\times = \{1, 3\}$

Donc $\left(\mathbb{Z}/4\mathbb{Z}\right)^\times$ est un groupe d'ordre 2.

On montre que $\left(\mathbb{Z}/4\mathbb{Z}\right)^\times$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ en exhibant un isomorphisme :

$$\varphi : \underbrace{\left(\mathbb{Z}/4\mathbb{Z}\right)^\times}_{\leftarrow \text{ multiplicatif}} \longrightarrow \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\leftarrow \text{ additif}}$$

$$1 \longmapsto 0$$

$$3 \longmapsto 1$$

Remarque : $\varphi(1\cdot 3) = \varphi(3) = 1 = 0+1 = \varphi(1)+\varphi(3)$.

2) $f : (\mathbb{R},+) \longrightarrow (\mathbb{R}\setminus\{0\}, \cdot\,)$
$x \longmapsto e^x$

f est un homomorphisme ?
Soient $x,y \in \mathbb{R}$. Alors on a :
$$f(x+y) = e^{x+y} = e^x e^y = f(x)f(y)$$
Donc f est un homomorphisme.

Est-ce que f est injectif ?
$\mathrm{Ker}(f) = \{x \in \mathbb{R} : f(x) = 1\} = \{x \in \mathbb{R} : e^x = 1\} =$
$= \{0\} \Rightarrow f$ est injectif

Est-ce que f est surjectif ?
Non, car $e^x > 0$, $\forall x \in \mathbb{R}$. En particulier $-1 \notin \mathrm{Im}(f)$.

Par contre $\tilde{f} : (\mathbb{R},+) \longrightarrow (\mathbb{R}^+\setminus\{0\}, \cdot\,)$ est
$x \longmapsto e^x$

un isomorphisme de groupes.

<u>Théorème</u> (Premier théorème d'isomorphisme)
Soit $\varphi : G \to G'$ un homomorphisme de groupes. Alors
$$G/_{\mathrm{Ker}(\varphi)} \simeq \mathrm{Im}(\varphi)$$
via l'isomorphisme :
$$\hat{\varphi} : G/_{\mathrm{Ker}(\varphi)} \longrightarrow \mathrm{Im}(\varphi)$$
$$[a]_{\mathrm{Ker}(\varphi)} \longmapsto \varphi(a)$$

<u>Rappel</u> : $[a]_{\ker(\varphi)} = \{ah : h \in \ker(\varphi)\}$

<u>DÉM</u>

On va montrer que

$$\hat{\varphi} : G/_{\ker(\varphi)} \longrightarrow \operatorname{Im}(\varphi)$$
$$[a]_{\ker(\varphi)} \longmapsto \varphi(a)$$

est un isomorphisme.

Pour cela il faut montrer que :

① $\hat{\varphi}$ est bien définie

② $\hat{\varphi}$ est homomorphisme de groupes

③ $\hat{\varphi}$ est bijective.

① Soient $a, b \in G$ tels que $[a]_{\ker(\varphi)} = [b]_{\ker(\varphi)}$

$\Rightarrow \exists\, h \in \ker(\varphi)$ tel que $a = bh \Rightarrow$

$\Rightarrow \varphi(a) = \varphi(bh) = \varphi(b)\varphi(h) = \varphi(b)\cdot 1_{G'} = \varphi(b)$

$\Rightarrow \varphi(a) = \varphi(b)$.

② Soient $[a]_{\ker(\varphi)}, [b]_{\ker(\varphi)} \in G/_{\ker(\varphi)}$. Alors on a :

$\hat{\varphi}\left([a]_{\ker(\varphi)} [b]_{\ker\varphi}\right) = \hat{\varphi}\left([ab]_{\ker(\varphi)}\right) =$

$= \varphi(ab) = \varphi(a)\varphi(b) = \varphi([a]_{\ker(\varphi)})\, \varphi([b]_{\ker(\varphi)})$.

③ Montrons que $\hat{\varphi}$ est injective et surjective :

- $\ker(\hat{\varphi}) = \{ [a]_{\ker(\varphi)} \in G/_{\ker(\varphi)} : \hat{\varphi}([a]_{\ker(\varphi)}) = 1_{G'} \}$

$$= \{ [a]_{\ker(\varphi)} \in G/_{\ker(\varphi)} : \varphi(a) = 1_{G'} \} =$$

$$= \{ [a]_{\ker(\varphi)} \in G/_{\ker(\varphi)} : a \in \ker(\varphi) \} =$$

$$= \{ [1_G]_{\ker(\varphi)} \} .$$

$\Rightarrow \hat{\varphi}$ est injective

- Soit $b \in \mathrm{Im}(\varphi) \Rightarrow \exists\, a \in G$ tel que $b = \varphi(a) = \hat{\varphi}\left([a]_{\ker(\varphi)}\right) \Rightarrow \hat{\varphi}$ est surjective

En conclusion $\hat{\varphi} : G/_{\ker(\varphi)} \to \mathrm{Im}(\varphi)$ est un isomorphisme de groupes.