

TD 5 - EXERCICE 4

$(\mathbb{C}, +, \otimes)$

$$\mathbb{C} = \{a+ib : a, b \in \mathbb{R}\}$$

① + est l'addition classique $\Rightarrow (\mathbb{C}, +)$ est un groupe abélien

$$\otimes : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$$

$$(z_1, z_2) \longmapsto z_1 \otimes z_2 := z_1 z_2 + \Im(z_1)\Im(z_2)$$

$$\begin{aligned} z_1 &= a+ib \\ z_2 &= c+id \end{aligned} \quad \left\{ \Rightarrow z_1 \otimes z_2 = (a+ib)(c+id) + bd = ac + i(bc+ad) \right.$$

Montrons que :

1) \otimes est associatif, c'est à-dire

$$\forall z_1, z_2, z_3, z_1 \otimes (z_2 \otimes z_3) = (z_1 \otimes z_2) \otimes z_3$$

$$\begin{aligned} z_1 &= a+ib \\ z_2 &= c+id \\ z_3 &= e+if \end{aligned}$$

$$\begin{aligned} z_1 \otimes (z_2 \otimes z_3) &= (a+ib) \otimes [ce + i(de+cf)] = \\ &= ace + i(bce + ade +acf) \end{aligned}$$

$$\begin{aligned} (z_1 \otimes z_2) \otimes z_3 &= (ac + i(bc+ad)) \otimes (e+if) = \\ &= ace + i(bce + ade +acf) \end{aligned} //$$

2) \otimes est commutative (laissez pour exercice)

3) Il existe $e \in \mathbb{C}$ tel que $z \otimes e = e \otimes z = z, \forall z \in \mathbb{C}$

On remarque que $e = 1$ vérifie $z \otimes 1 = 1 \otimes z = z, \forall z \in \mathbb{C}$.

4) \otimes est distributive sur $+$, c'est-à-dire :

$$\forall z_1, z_2, z_3, z_1 \otimes (z_2 + z_3) = z_1 \otimes z_2 + z_1 \otimes z_3$$
$$(z_1 + z_2) \otimes z_3 = z_1 \otimes z_3 + z_2 \otimes z_3$$

(laissez pour exercice)

② Quels sont les éléments inversibles de \mathbb{C} par rapport à \otimes ?

$$\text{Inv} = \{ z \in \mathbb{C} : \exists z' \in \mathbb{C} \text{ tel que } z \otimes z' = 1 \}$$

$$z = a + ib$$

je cherche, s'il existe, $z' = c + id$ tel que
 $z \otimes z' = 1$.

$$z \otimes z' = ac + i(bc + ad) = 1 \iff$$

$$\iff \begin{cases} ac = 1 \\ bc + ad = 0 \end{cases}$$

Si $a = 0 \Rightarrow z = ib$ n'est pas inversible

$$\text{Si } a \neq 0 \Rightarrow \begin{cases} c = \frac{1}{a} \\ \frac{b}{a} + ad = 0 \end{cases} \iff d = -\frac{b}{a^2}$$

Donc si $a \neq 0$ $z^{-1} = \frac{1}{a} - i \frac{b}{a^2}$

En conclusion :

$$\text{Inv} = \{a+ib \in \mathbb{C} : a \neq 0\}$$

$$\forall z = a+ib \in \text{Inv}, \quad z^{-1} = \frac{1}{a} - i \frac{b}{a^2}$$

En particulier $(\mathbb{C}, +, \otimes)$ n'est pas un corps, car par exemple i n'est pas inversible.

EXERCICE 5

$$1. \quad m \cdot \mathbb{Z}/n\mathbb{Z} = \{m \cdot [a]_n : [a]_n \in \mathbb{Z}/n\mathbb{Z}\} = \\ = \{[ma]_n : a \in \mathbb{Z}\}$$

$$3. \quad \mathbb{Z}/5\mathbb{Z} = \{ \begin{matrix} 3 \cdot 0 & \text{III} \\ 3 \cdot 1 & \text{III} \\ 3 \cdot 2 & \text{III} \\ 3 \cdot 3 & \text{III} \\ 3 \cdot 4 & \text{III} \end{matrix} \} = \{0, 1, 2, 3, 4\} \quad \text{mod } 5$$

i) Montrer que $\forall m \in \mathbb{Z}, n \in \mathbb{Z}_{>0}, m\mathbb{Z}/n\mathbb{Z}$ est idéal :

ii) $(m\mathbb{Z}/n\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$

iii) $\forall x \in m\mathbb{Z}/n\mathbb{Z}, \forall a \in \mathbb{Z}/n\mathbb{Z}, xa \in m\mathbb{Z}/n\mathbb{Z}$


Proposition : Soit $(G, +)$ un groupe. Un sous-ensemble $H \subseteq G$ est un sous-groupe si et seulement si $\forall a, b \in H, a - b \in H$.

i) Soient $[a]_n, [b]_n \in m \cdot \mathbb{Z}/n\mathbb{Z}$. Alors

$$\exists \alpha, \beta \in \mathbb{Z} \text{ tels que } [\alpha]_n = [m\alpha]_n, \\ [\beta]_n = [m\beta]_n \Rightarrow [\alpha]_n - [\beta]_n = [m\alpha]_n - [m\beta]_n \\ = [m(\alpha - \beta)]_n \in m \mathbb{Z}/n\mathbb{Z}.$$

$\Rightarrow (m \mathbb{Z}/n\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$

ii) Soient $[x]_n \in m \mathbb{Z}/n\mathbb{Z}$ et $[\alpha]_n \in \mathbb{Z}/n\mathbb{Z}$
 $\Rightarrow \exists \alpha \in \mathbb{Z}$ tel que $[x]_n = [\alpha n]_n$.

$$\text{On a : } [x]_n [\alpha]_n = [\alpha n]_n [\alpha]_n = \\ = [\underbrace{\alpha n \alpha}_{\in \mathbb{Z}}]_n \in m \cdot \mathbb{Z}/n\mathbb{Z}.$$

Donc $m \mathbb{Z}/n\mathbb{Z}$ est un idéal de $\mathbb{Z}/n\mathbb{Z}$.

$$2) 4. \mathbb{Z}/12\mathbb{Z} = \{[0]_{12}, [4]_{12}, [B]_{12}\}$$

$$5. \mathbb{Z}/12\mathbb{Z} = \{[0]_{12}, [5]_{12}, [10]_{12}, [3]_{12}, [8]_{12}, \\ [1]_{12}, [6]_{12}, [11]_{12}, [4]_{12}, [9]_{12}, \\ [2]_{12}, [7]_{12}\} = \mathbb{Z}/12\mathbb{Z}$$

3) Démontrer que $\forall m \in \mathbb{Z}, \forall n \in \mathbb{Z}_{>0}$,
 $m \cdot \mathbb{Z}/n\mathbb{Z} = d \cdot \mathbb{Z}/n\mathbb{Z}$, avec $d = \text{pgcd}(n, m)$.

Puisque $d = \text{pgcd}(m, n) \Rightarrow d = mu + nv, \\ u, v \in \mathbb{Z}$

$$m \mathbb{Z}/n\mathbb{Z} = \{ [ma]_n, a \in \mathbb{Z} \}$$

$$d \cdot \mathbb{Z}/n\mathbb{Z} = \{ [da]_n, a \in \mathbb{Z} \}$$

- On montre que $m \mathbb{Z}/n\mathbb{Z} \subseteq d \mathbb{Z}/n\mathbb{Z}$:

Soit $[ma]_n \in m \mathbb{Z}/n\mathbb{Z} \implies [ma]_n =$

$$\begin{matrix} m = dK, \\ K \in \mathbb{Z} \end{matrix}$$

$$= [d \cdot \underbrace{K a}_n]_n \in d \mathbb{Z}/n\mathbb{Z}.$$

$\in \mathbb{Z}$

- On montre que $d \mathbb{Z}/n\mathbb{Z} \subseteq m \mathbb{Z}/n\mathbb{Z}$:

Soit $[da]_n \in d \mathbb{Z}/n\mathbb{Z} \stackrel{\uparrow}{=} [(mu+nv)a]_n =$

$$d = mu + nv$$

$$= [mu + nv a]_n = [mu a]_n \in m \mathbb{Z}/n\mathbb{Z}.$$

- Le point 4 est laissé pour exercice.

On réprend la définition d'homomorphisme (ou morphisme) de groupes :

Déf.: Soient $(G, *)$ et (H, Δ) 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 φ est

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

et le noyau de φ est

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

Remarque:

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

$$\underline{\text{dém}}: \varphi(1_G) = \varphi(1_G * 1_G) = \varphi(1_G) \Delta \varphi(1_G)$$

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

↑
les je multiplie
deux membres
par $(\varphi(1_G))^{-1}$

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

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

$$\underline{\text{dém}}: 1_H = \varphi(1_G) = \varphi(a * a^{-1}) =$$

$$= \varphi(a) \Delta \varphi(a^{-1}) \Rightarrow \varphi(a^{-1}) = [\varphi(a)]^{-1}$$

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

- 1) Si H est un sous-groupe de G
 $\Rightarrow \varphi(H)$ est un sous-groupe de G'
- 2) Si H' est un sous-groupe de G'
 $\Rightarrow \varphi^{-1}(H') = \{a \in G : \varphi(a) \in H'\}$ est un sous-groupe de G .
- 3) $\text{Ker}(\varphi)$ est un sous-groupe de G et $\text{Im}(\varphi)$ est un sous-groupe de G' .
- 4) φ est injectif $\Leftrightarrow \text{Ker}(\varphi) = \{e_G\}$.

Dém : par exercice

Proposition : Si $\varphi: G \rightarrow G'$ et $\psi: G' \rightarrow G''$ sont deux homomorphismes de groupes, alors $\psi \circ \varphi: G \rightarrow G''$ est un homomorphisme de groupes.

Dém par exercice.

Déf : Un homomorphisme de groupes $\varphi: G \rightarrow H$ est un isomorphisme si φ est bijective. Dans ce cas G et H sont dit isomorphes et on écrit $G \cong H$. Si $G = H$ alors on appelle φ un automorphisme.

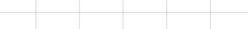
Examples

$$1) \quad \left(\frac{\pi}{\ln \pi}\right)^x = 1,37$$

Alors $(\mathbb{Z}/n\mathbb{Z})^*$ $\simeq \mathbb{Z}/\varphi(n)$ et un isomorphisme est donné par :
multiplicatif additif

$$\varphi : \left(\mathbb{Z}/\ell\mathbb{Z}\right)^{\times} \longrightarrow \mathbb{Z}/\frac{\ell}{2\mathbb{Z}}$$



 1  0

3  1

$$2) f: (\mathbb{R}, +) \xrightarrow{x} (\mathbb{R} \setminus \{0\}, \cdot)$$

f est un homomorphisme ?

$$\forall x, y \in \mathbb{R}, \quad f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$$

\uparrow
propriétés de e^x

$$\Rightarrow \text{oui, c'est un homomorphisme!}$$

est un isomorphisme ?

- $\text{Ker}(f) = \{x \in \mathbb{R} : f(x) = 1\} = \{x \in \mathbb{R} : e^x = 1\}$
 $= \{0\} \Rightarrow f \text{ est injective}$
 - f n'est pas surjective, car $e^x > 0, \forall x \in \mathbb{R}$

Pour contre $\tilde{f} : (\mathbb{R}, +) \rightarrow (\mathbb{R}^+ \setminus \{1\}, \cdot)$ est un isomorphisme de groupes.

Théorème (Premier théorème d'isomorphisme)

Soit $\varphi : G \rightarrow G'$ un homomorphisme de groupes. Alors

$$G / \text{Ker}(\varphi) \simeq \text{Im}(\varphi)$$

via l'isomorphisme :

$$\varphi(a) : a \in G \subset G'$$

$$\hat{\varphi} : G / \text{Ker}(\varphi) \longrightarrow \text{Im}(\varphi)$$

$$[a]_{\text{Ker}(\varphi)} \longmapsto \varphi(a)$$

$$[a]_{\text{Ker}(\varphi)} = \\ = \{ah, h \in \text{Ker}(\varphi)\}$$

Démo

• Montrons d'abord que $\hat{\varphi}$ est bien définie :

Soient $a, b \in G$ tel que $[a]_{\text{Ker}(\varphi)} = [b]_{\text{Ker}(\varphi)}$
 $\Rightarrow b = ah$, $h \in \text{Ker}(\varphi) \Rightarrow \varphi(b) = \varphi(ah) =$
 $= \varphi(a)\varphi(h) \stackrel{h \in \text{Ker}(\varphi)}{=} \varphi(a) \quad \checkmark$

• Montrons que $\hat{\varphi}$ est un homomorphisme de groupes.

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

$$\hat{\varphi}([a]_{\text{Ker}(\varphi)} [b]_{\text{Ker}(\varphi)}) = \hat{\varphi}([ab]_{\text{Ker}(\varphi)}) =$$

def. de multiplication dans $G / \text{Ker}(\varphi)$

$$=\varphi(ab) = \varphi(a)\varphi(b) = \hat{\varphi}\left(\begin{bmatrix} a \\ \text{ker}(\varphi) \end{bmatrix}\right) \cdot \hat{\varphi}\left(\begin{bmatrix} b \\ \text{ker}(\varphi) \end{bmatrix}\right)$$

\uparrow
 φ est un homom.

$\Rightarrow \hat{\varphi}$ est un homomorphisme de groupes

- Montrons que $\hat{\varphi}$ est injective. De façon équivalente on montre que :

$$\text{Ker}(\hat{\varphi}) = \left\{ \begin{bmatrix} e \\ \text{ker}(\varphi) \end{bmatrix} \right\}.$$

$$\begin{aligned} \text{Ker}(\hat{\varphi}) &= \left\{ \begin{bmatrix} a \\ \text{ker}(\varphi) \end{bmatrix} : \hat{\varphi}\left(\begin{bmatrix} a \\ \text{ker}(\varphi) \end{bmatrix}\right) = \begin{bmatrix} e \\ \text{ker}(\varphi) \end{bmatrix} \right\} = \\ &= \left\{ \begin{bmatrix} a \\ \text{ker}(\varphi) \end{bmatrix} : \varphi(a) = e \right\} = \\ &= \left\{ \begin{bmatrix} a \\ \text{ker}(\varphi) \end{bmatrix} : a \in \text{Ker}(\varphi) \right\} = \\ &= \left\{ \begin{bmatrix} e \\ \text{ker}(\varphi) \end{bmatrix} \right\} \end{aligned}$$

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

- Montrons que $\hat{\varphi}$ est surjective.

Soit $b \in \text{Im}(\varphi) \Rightarrow \exists a \in G$ tel que

$$b = \varphi(a) = \hat{\varphi}\left(\begin{bmatrix} a \\ \text{ker}(\varphi) \end{bmatrix}\right) \Rightarrow \hat{\varphi}$$
 est surjective.

En conclusion $\hat{\varphi}$ est un isomorphisme de groupes.