

Exemple (ter théorème d'isomorphisme)

$$G = \mathbb{Z} \times \mathbb{Z} = \{(x, y) : x, y \in \mathbb{Z}\}$$

$$+ : (\mathbb{Z} \times \mathbb{Z}) \times (\mathbb{Z} \times \mathbb{Z}) \longrightarrow \mathbb{Z} \times \mathbb{Z}$$

$$((x, y), (x', y')) \longmapsto (x, y) + (x', y') = (x+x', y+y')$$

On peut facilement montrer que $(\mathbb{Z} \times \mathbb{Z}, +)$ est un groupe commutatif.

On considère l'application suivante :

$$\varphi : (\mathbb{Z} \times \mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$$

$$(x, y) \longmapsto x+y$$

Montrons que φ est un homomorphisme.

Soient $(x, y), (x', y') \in \mathbb{Z} \times \mathbb{Z}$. Alors on a :

$$\begin{aligned} \varphi((x, y) + (x', y')) &= \varphi(x+x', y+y') = x+x'+y+y' = \\ &= (x+y)+(x'+y') = \\ &= \varphi(x, y) + \varphi(x', y') \end{aligned}$$

$$\begin{aligned} \text{Ker}(\varphi) &= \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : \varphi(x, y) = 0\} = \\ &= \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x+y = 0\} = \\ &= \{(x, -x) \in \mathbb{Z} \times \mathbb{Z}\} \end{aligned}$$

$$\text{Image}(\varphi) = \mathbb{Z}, \text{ car } \forall y \in \mathbb{Z} \text{ on a que } \varphi(0, y) = y.$$

Donc d'après le théorème d'isomorphisme, on a que :

$$\frac{\mathbb{Z} \times \mathbb{Z}}{\text{Ker}(\varphi)} \cong \mathbb{Z}$$

On peut facilement voir que $\text{Ker}(\varphi)$ est isomorphe à \mathbb{Z} et un isomorphisme est donné par :

$$\psi : \begin{array}{ccc} \text{Ker}(\varphi) = \{(x, -x) : x \in \mathbb{Z}\} & \longrightarrow & \mathbb{Z} \\ (x, -x) & \longmapsto & x \end{array}$$

Donc, en conclusion, on a montré que :

$$\frac{\mathbb{Z} \times \mathbb{Z}}{\mathbb{Z}} \cong \mathbb{Z}.$$

Homomorphismes (Morphismes) d'anneaux

(A_{i,j}) (B_{i,j})

Def: Soient A, B deux anneaux. Une application

$$\varphi: A \rightarrow B$$

est un homomorphisme d'anneaux si :

- 1) $\forall a, b \in A, \varphi(a+b) = \varphi(a) + \varphi(b)$.
- 2) $\forall a, b \in A, \varphi(ab) = \varphi(a) \cdot \varphi(b)$.
- 3) $\varphi(1_A) = 1_B$

L'image de φ est $\text{Im}(\varphi) = \{\varphi(a) : a \in A\}$ et le najau de φ est $\text{Ker}(\varphi) = \{a \in A : \varphi(a) = 0_B\}$

Un isomorphisme d'anneaux est un homomorphisme bijectif. Si $\varphi: A \rightarrow B$ est un isomorphisme alors A et B sont dits isomorphes.

Remarque : Si $\varphi: A \rightarrow B$ est un homomorphisme d'anneaux, alors $\varphi: A \rightarrow B$ est un homomorphisme de groupes additifs $\Rightarrow \varphi(0_A) = 0_B$.

Proposition : Soit $\varphi: A \rightarrow B$ un homomorphisme d'anneaux.

Alors :

- 1) Si I est un idéal de A , alors $\varphi(I)$ est un idéal de $\varphi(A)$. $\stackrel{Def(\varphi)}{=}$
- 2) Si J est un idéal de $\varphi(A)$, alors $\varphi^{-1}(J)$ est un idéal de A .

Par conséquent, $\text{Im}(\varphi) = \varphi(A)$ est un idéal de B et $\text{Ker}(\varphi) = \varphi^{-1}(\{0_B\})$ est un idéal de A .

Démonstration : On démontre juste (1). On laisse (2) par exercice.

Soit I un idéal de A . $((I, +))$ est un sous-groupe additif de $(A, +)$ et $\forall x \in I, \forall a \in A, \exists z \in I$.

On veut montrer que $\varphi(I) = \{\varphi(x) : x \in I\}$ est un idéal de $\varphi(A)$

- $(\varphi(I), +)$ est un sous-groupe de $(\varphi(A), +)$, car φ est aussi un homomorphisme de groupes additifs.
- Soient $y \in \varphi(I)$ et $b \in \varphi(A) \Rightarrow \exists x \in I$ tel que $\varphi(x) = y$, $\exists a \in A$ tel que $\varphi(a) = b$. Alors on a.
 $yb = \varphi(x)\varphi(a) = \varphi(xa) \in \varphi(I)$.
 $\xrightarrow{x \in I} \xrightarrow{a \in A}$
 $\Rightarrow za \in I$ (car I est un idéal de A)

Proposition : Soit $\varphi: A \rightarrow B$ un isomorphisme d'anneaux. Alors :

- (1) $a \in A$ est un diviseur de zéro $\Leftrightarrow \varphi(a) \in B$ est un diviseur de zéro.
- (2) $a \in A$ est inversible $\Leftrightarrow \varphi(a) \in B$ est inversible
- (3) φ induit un isomorphisme $\varphi: A^\times \xrightarrow{\sim} B^\times$ entre les groupes des inversibles de A et B .

Proposition : Soient A, B_1, \dots, B_k des anneaux et soit $\varphi: A \rightarrow B_i$

un morphisme d'anneaux $\forall i$.

Alors $B_1 \times \dots \times B_k$ est un anneau avec les opérations suivantes :

$$+ : (B_1 \times \dots \times B_k) \times (B_1 \times \dots \times B_k) \rightarrow B_1 \times \dots \times B_k \\ ((b_1, \dots, b_k), (b'_1, \dots, b'_k)) \mapsto (b_1 b'_1, \dots, b_k b'_k)$$

et

$$\cdot : (B_1 \times \dots \times B_k) \times (B_1 \times \dots \times B_k) \rightarrow B_1 \times \dots \times B_k \\ ((b_1, \dots, b_k), (b'_1, \dots, b'_k)) \mapsto (b_1 b'_1, \dots, b_k b'_k)$$

De plus :

$$\begin{array}{ccc} \varphi: A & \longrightarrow & B_1 \times \dots \times B_k \\ a & \longmapsto & (\varphi_1(a), \dots, \varphi_k(a)) \end{array}$$

est un homomorphisme d'anneau.

Théorème (Premier théorème d'isomorphisme)

Soit $\varphi: A \rightarrow B$ un homomorphisme d'anneau.

Alors $\frac{A}{\text{Ker}(\varphi)} \simeq \text{Im}(\varphi)$ (en tant qu'anneau)

via l'isomorphisme :

$$\begin{array}{ccc} \hat{\varphi}: A/\text{Ker}(\varphi) & \longrightarrow & \text{Im}(\varphi) \\ [a]_{\text{Ker}(\varphi)} & \longmapsto & \varphi(a) \end{array}$$

Exemple : Le théorème chinois des restes peut être aussi énoncé de la façon suivante :

Soient n_1, \dots, n_k des entiers premiers deux à deux et soit $N = \prod_{i=1}^k n_i$.

Alors l'application :

$$\theta: \mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

$$[a]_N \longmapsto ([a]_{n_1}, \dots, [a]_{n_k})$$

est un isomorphisme d'anneaux.

De plus θ induit un isomorphismes de groupes multiplicatifs

$$(\mathbb{Z}/N\mathbb{Z})^\times \simeq (\mathbb{Z}/n_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})^\times$$

Exemple

- $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z} \Rightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est cyclique

théorème chinois des restes

De plus $(\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/2\mathbb{Z})^\times \simeq (\mathbb{Z}/6\mathbb{Z})^\times$.

$\left\{ \begin{matrix} 1 \\ 2 \end{matrix} \right\}$	$\left\{ \begin{matrix} 1 \\ 4 \end{matrix} \right\}$	$\left\{ \begin{matrix} 1, 5 \end{matrix} \right\}$
-------------------------------------------------------	-------------------------------------------------------	-----------------------------------------------------

- $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \simeq \mathbb{Z}/55\mathbb{Z}$

- Attention : $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \not\simeq \mathbb{Z}/4\mathbb{Z}$

TD6

1) $\mathbb{Z}/8\mathbb{Z} = \{0, 1, 2, 3\} \quad \Rightarrow \quad |\mathbb{Z}/8\mathbb{Z}| = |(\mathbb{Z}/8\mathbb{Z})^\times| = 4$

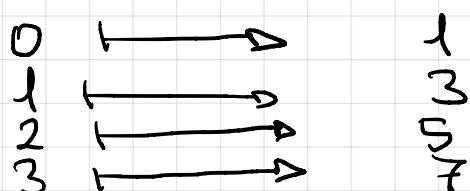
$(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\} \quad \Rightarrow \quad$

Il existe $\frac{4!}{24}$ bijections entre $\mathbb{Z}/6\mathbb{Z}$ et

$(\mathbb{Z}/8\mathbb{Z})^\times$. Parmi ces bijections y

a-t-il une qui est aussi un homomorphisme de groupes?

Tentatif 1 : $f: \mathbb{Z}/6\mathbb{Z} \rightarrow (\mathbb{Z}/8\mathbb{Z})^\times$



$$\left. \begin{aligned} f(1+2) &= f(3) = 7 \\ f(1) \cdot f(2) &= 3 \cdot 5 \equiv 7 \pmod{8} \end{aligned} \right\} \rightarrow \text{la chance!}$$

$$f(-1+1) = f(0) = 1 \quad \text{H}$$

$$f(1) \cdot f(1) = 3 \cdot 3 \equiv 1 \pmod{8}$$

Donc f n'est pas un homomorphisme.

En effet il n'existe pas d'isomorphismes entre $\mathbb{Z}/6\mathbb{Z}$ et $(\mathbb{Z}/8\mathbb{Z})^\times$.

Notons que l'a ordre 4 dans $\mathbb{Z}/6\mathbb{Z}$

et que tous les éléments de $(\mathbb{Z}/8\mathbb{Z})^\times$ sont d'ordre 1 ou 2.

Identifié
par l'absurde,
Supposons, V qu'il existe un isomorphisme :

$$f: \frac{\pi}{6\pi} \rightarrow \left(\frac{\pi}{3\pi}\right)^x$$

$$f(1+x) = f(1) \cdot f(x) = f(1)^2 = 1$$

$f(2)$ f est homom. \nearrow tous les éléments de $(\mathbb{Z}/3\mathbb{Z})^*$ sont d'ordre 1 ou 2.

1 cour $f(0) = 1$ et f est bijective

Donc $\ell \neq l$  Donc un isomorphisme f
ne peut pas exister.

Exercice 1b (n'est pas dans le TD)

Montrer que si $\varphi: G \rightarrow G'$ est un isomorphisme. Alors :

- 1) $a \in G$ et $\varphi(a) \in G'$ ont le même ordre.
 - 2) Si G est cyclique alors G' est cyclique.

Skushima

Montrons (1) et (2) lorsque G est un groupe

fini ($\Rightarrow G'$ est aussi fini).

e) Muestra que si $\text{ord}(a) = n \Rightarrow \text{ord}(c(a)) = n$.

$$\bullet \quad a^n = 1_G \Rightarrow \varphi(a^n) = \varphi(1_G) = 1_G$$

\Downarrow

$$\varphi(a)^n$$

- Il reste à montrer que si $0 < m < n$, alors $\varphi(a)^m \neq 1_G$

Supposons, par l'absurde, que $\varphi(a)^m = \lg$

$$\Rightarrow \varphi(a^m) = \lg \Rightarrow a^m = \lg$$

\uparrow

φ est injectif

$\Leftrightarrow \ker(\varphi) = \{\lg\}$

Car a à n ordre

$n > m.$

2) Si G est cyclique $\Rightarrow G = \langle g \rangle$ et
 $\text{ord}(g) = |G|$.

De plus, $|G| = |G'|$, car $\varphi: G \rightarrow G'$ est bijective et G est fini.

D'après le point 1, $\text{ord}(\varphi(g)) = \text{ord}(g) = |G'|$
 $\Rightarrow \varphi(g)$ est un générateur de G' et
 donc G' est cyclique. ($G' = \langle \varphi(g) \rangle$)

On a aussi prouvé que si g est un générateur de G et $\varphi: G \rightarrow G'$ est un isomorphisme, alors $\varphi(g)$ est un générateur de G' .