2

Théorème des restes chinois dans $\mathbb{Z}/m\mathbb{Z}$.

Références :
- Skandalis p. 33

Recasages :
(- 101 : Groupes monogènes, groupes cycliques. Exemples)
- 103 : Anneau $\mathbb{Z}/n\mathbb{Z}$. Applications.
- 106 : PGCD dans $\mathbb{Z}$ et $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps commutatif, thm de Bézout. Applications.
- 159 : Algorithme d'Euclide dans $\mathbb{Z}$ et $\mathbb{K}[X]$ où... Calcul de PGCD et de coefficients de Bézout. Applications.
- 302 : Exercices faisant intervenir les notions de congruence et de divisibilité dans $\mathbb{Z}$.
- 304 : Exercices faisant intervenir le thm de Bézout

Les conditions suivantes sont équivalentes
① $m \wedge \ell = 1$
② $\mathbb{Z}/m\ell\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ pour les anneaux.
③ $\mathbb{Z}/m\ell\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ pour les groupes.

Notations :
- $a \wedge b = \text{pgcd}(a,b)$
- $\simeq$ = isomorphes
- $\dot{x}$ = classe d'équivalence de x dans $\mathbb{Z}/m\ell\mathbb{Z}$
- $\bar{x}$ = ——— $\mathbb{Z}/m\mathbb{Z}$
- $\bar{\bar{x}}$ = ——— $\mathbb{Z}/\ell\mathbb{Z}$

① **Sens (1) ⇒ (2) :**
On suppose que $m \wedge \ell = 1$.

On pose $\varphi : \mathbb{Z}/m\ell\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ (anneaux)
$\dot{x} \longmapsto (\bar{x}, \bar{\bar{x}})$

On vérifie facilement les points suivants :

* φ est bien définie :
$\dot{x} = \dot{y} \Rightarrow \exists k \in \mathbb{Z}$ tq $x = y + k \cdot m\ell = \begin{cases} \bar{x} = \bar{y} \\ \bar{\bar{x}} = \bar{\bar{y}} \end{cases}$

* φ est un morphisme d'anneaux :
$\varphi(\dot{x}+\dot{y}) = \varphi(\dot{x+y}) = (\bar{x+y}, \bar{\bar{x+y}}) = (\bar{x}+\bar{y}, \bar{\bar{x}}+\bar{\bar{y}})$
$= (\bar{x}, \bar{\bar{x}}) + (\bar{y}, \bar{\bar{y}}) = \varphi(\dot{x}) + \varphi(\dot{y})$.
$\varphi(\dot{x} \times \dot{y}) = \varphi(\dot{xy}) = (\bar{xy}, \bar{\bar{xy}}) = (\bar{x}\bar{y}, \bar{\bar{x}}\bar{\bar{y}})$
$= (\bar{x}, \bar{\bar{x}})(\bar{y}, \bar{\bar{y}}) = \varphi(\dot{x}) \times \varphi(\dot{y})$.

* φ est injectif :
$\ker(\varphi) = \{ \dot{x} \in \mathbb{Z}/m\ell\mathbb{Z} \mid \varphi(\dot{x}) = (\bar{0}, \bar{\bar{0}}) \}$
$= \{ x \in \mathbb{Z} \mid \bar{x} = \bar{0}, \bar{\bar{x}} = \bar{\bar{0}} \}$
car $m \wedge \ell = 1$ $= \{ x \in \mathbb{Z} \mid m \mid x \text{ et } \ell \mid x \}$
$= \{ x \in \mathbb{Z} \mid m\ell \mid x \}$
$= \dot{0}$

* φ est surjectif :
Comme $m \wedge \ell = 1$, on a d'après le thm de Bézout :
$\exists \alpha, \beta \in \mathbb{Z}$ tq $\underbrace{m\alpha}_{a} + \underbrace{\ell\beta}_{b} = 1$.
On pose alors : $\begin{cases} a = m\alpha \equiv 0 [m] \\ b = \ell\beta \equiv 0 [\ell] \end{cases} \Rightarrow \underline{a+b=1}$
On a donc aussi :
$\begin{cases} a = 1 - \ell\beta \equiv 1 [\ell] \\ b = 1 - m\alpha \equiv 1 [m] \end{cases}$
Ainsi : $\varphi(\dot{a}) = (\bar{0}, \bar{\bar{1}})$ et $\varphi(\dot{b}) = (\bar{1}, \bar{\bar{0}})$
Donc $\forall (\bar{x}, \bar{\bar{y}}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ on a : (φ morphisme)
$(\bar{x}, \bar{\bar{y}}) = x \cdot (\bar{1}, \bar{\bar{0}}) + y(\bar{0}, \bar{\bar{1}}) = x \times \varphi(\dot{b}) + y \times \varphi(\dot{a}) = \varphi(xb + ya)$
$\Rightarrow$ φ est bien un isomorphisme d'anneaux.

② Sens (2) ⇒ (3) :

Morphisme de gpe "C" Morphisme d'anneaux.

③ Sens (3) ⇒ (1) :

On suppose que :

$\exists \varphi : \mathbb{Z}/m\ell\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ un isomorphisme de groupes (inconnu !)

Notons $\varphi(\dot{1}) = (\bar{x}, \bar{\bar{y}})$ et $k = \text{ppcm}(m, \ell)$.

Alors :

$\varphi(\dot{k}) = k \cdot \varphi(\dot{1}) = k \cdot (\bar{x}, \bar{\bar{y}}) = (k\bar{x}, k\bar{\bar{y}})$

$= (\overline{kx}, \overline{\overline{ky}}) = (\bar{0}, \bar{\bar{0}})$

↑ car k multiple de m et de ℓ.

Donc $\dot{k} \in \text{Ker}(\varphi)$, qui est un isomorphisme, donc injectif, donc $\text{Ker}(\varphi) = \{\dot{0}\}$, donc $\underline{\dot{k} = \dot{0}}$, c'est-à-dire : $\underline{m\ell \mid k}$ (*)

De plus par définition de k (ppcm), on a aussi $\underline{k \mid m\ell}$ (**)

(*) et (**) ⇒ $k = m\ell$

On $k = m\ell = \underbrace{\text{pgcd}(m,\ell)}_{m\wedge\ell} \times \underbrace{\text{ppcm}(m,\ell)}_{k}$

⇒ $k = m\wedge\ell \times k$ ⇒ $\underline{m\wedge\ell = 1}$.