Théorème chinois : Cas général

Geoffrey Deperle

Leçons associées :
— 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
— 142 : PGCD et PPCM, algorithmes de calcul. Applications.

Le but de ce développement est de montrer le théorème suivant :

Théorème. *Soit $m, n \in \mathbb{N}$, on dispose de la décomposition*

$$\mathbb{Z}/\text{ppcm}(m,n)\mathbb{Z} \overset{\varphi}{\hookrightarrow} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \overset{\psi}{\twoheadrightarrow} \mathbb{Z}/\text{pgcd}(m,n)\mathbb{Z}$$

avec φ un morphisme injectif et ψ un morphisme surjectif tel que $\text{Im}\phi = \text{Ker}\psi$.

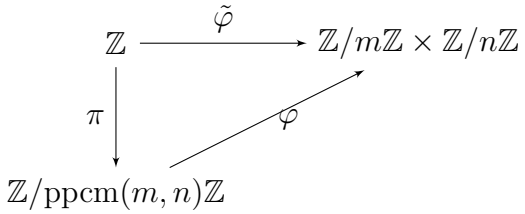
Preuve: Notons pour la suite $\delta = \text{pgcd}(m,n)$ et $\mu = \text{ppcm}(m,n)$.

Étape 1 : Construction de ϕ

Posons $\begin{array}{ccccc} \tilde{\varphi} & : & \mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ & & x & \mapsto & (\overline{x_m}, \overline{x_n}) \end{array}$, $\tilde{\varphi}$ est un morphisme de groupe de noyau :

$$\text{Ker}\tilde{\varphi} = \{x \in \mathbb{Z} \,|\, \overline{x_m} = 0 \text{ et } \overline{x_n} = 0\} = \{x \in \mathbb{Z} \,|\, m|x \text{ et } n|x\}$$

Donc $\text{Ker}\tilde{\varphi} = \text{ppcm}(m,n)\mathbb{Z}$.



En passant au quotient, il existe $\varphi : \mathbb{Z}/\mu\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ tel que

$$\begin{cases} \varphi \text{ est un morphisme de } \mathbb{Z}/\mu\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \varphi \text{ est injectif} \\ \text{Im}\varphi = \text{Im}\tilde{\varphi} \end{cases}$$

Étape 2 : Construction de ψ

Posons $\begin{array}{rccc}\psi & : & \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/\delta\mathbb{Z} \\ & & (\overline{x_m},\overline{y_n}) & \mapsto & \overline{x_\delta}-\overline{y_\delta}\end{array}$. Montrons qu'il s'agit d'un morphisme :
Comme $\delta|m$, $m\mathbb{Z}\subset\delta\mathbb{Z}$ donc par passage au quotient du morphisme de projection $\mathbb{Z}\to\mathbb{Z}/\delta\mathbb{Z}$ par $m\mathbb{Z}$, on obtient un morphisme $\begin{array}{rccc} & : & \mathbb{Z} & \to & \mathbb{Z}/\delta\mathbb{Z} \\ & & \tilde{x_m} & \mapsto & \tilde{x_\delta}\end{array}$ est bien définie.
Ainsi, $\overline{x_\delta}$ est bien définie. De même $\overline{y_\delta}$ est bien définie. Comme les applications $\overline{x_m}\mapsto\overline{x_\delta}$ et $\overline{y_n}\mapsto\overline{y_\delta}$ définissent des morphismes. ψ est bien définie et définie un morphisme d'anneaux.
Montrons la surjectivité de ψ,
Soit $\overline{x_\delta}\in\mathbb{Z}/\delta\mathbb{Z}$, on a $\psi(\overline{x_m},0)=\overline{x_\delta}$ d'où la surjectivité.

Étape 3 : Montrons que $\mathrm{Ker}\psi=\mathrm{Im}\varphi$

Soit $(\overline{x_m},\overline{x_n})\in\mathrm{Im}\varphi$ avec $x\in\mathbb{Z}$, alors $\psi(\overline{x_m},\overline{x_n})=\overline{x_\delta}-\overline{x_\delta}=0$. Donc $\mathrm{Im}\varphi\subset\mathrm{Ker}\psi$.
De plus,

$$\begin{aligned}|\mathrm{Im}\varphi|=|\mathbb{Z}/\mu\mathbb{Z}|=\mathrm{ppcm}(m,n)&=\frac{mn}{\mathrm{pgcd}(m,n)}\\&=\frac{|\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}|}{|\mathbb{Z}/\delta\mathbb{Z}|}\\&=|\mathrm{Ker}\psi|\end{aligned}$$

d'où l'égalité entre les ensembles. □

Application. *Soit $x,a,b\in\mathbb{Z}$, $m,n\in\mathbb{N}$, en posant $\delta=\mathrm{pgcd}(m,n)$,*
Le système $(S):\begin{cases}x &\equiv a\,[m]\\ x &\equiv b\,[n]\end{cases}$ admet une solution si et seulement si $\overline{a_\delta}=\overline{b_\delta}$

Preuve:
Soit a,b tel que $\overline{a_\delta}\neq\overline{b_\delta}$ alors si (S) admet une solution x, on a $\tilde{\varphi}(x)=(\overline{x_m},\overline{x_n})=(\overline{a_m},\overline{b_n})$ et $(\overline{a_m},\overline{b_n})\in\mathrm{Im}\varphi=\mathrm{Ker}\psi$ d'où $\psi((\overline{a_m},\overline{b_n}))=\overline{a_\delta}-\overline{b_\delta}=0$. Absurde.

Supposons à présent que a,b est telle que $\overline{a_\delta}=\overline{b_\delta}$, alors il existe $k\in\mathbb{Z}$ tel que $a=b+k\delta$.
Soit $u,v\in\mathbb{Z}$ tel que $um+vn=\delta$, et posons $x_0=\frac{1}{\delta}(avn+bum)\in\mathbb{Z}$.
On a $x_0=\frac{1}{\delta}((b+k\delta)vn+bum)=b\frac{vn+um}{\delta}+kvn$.
D'où $x_0\equiv b\,[n]$.
De même $x_0=\frac{1}{\delta}(avn+(a-k\delta)um)=\frac{vn+um}{\delta}-kum$.
D'où $x_0\equiv a\,[m]$ donc x_0 est solution.

Soit x une autre solution de (S), alors $var\tilde{p}hi(x)=var\tilde{p}hi(x_0)$ d'où $x-x_0\in\mathrm{Ker}\tilde{\varphi}=\mathrm{ppcm}(m,n)\mathbb{Z}$.
L'ensemble des solution est $\{x_0+k\mathrm{ppcm}(m,n),k\in\mathbb{Z}\}$. □

Références

[1] Philippe Caldero et Marie Peronnier. *Carnet de voyage en Algébrie*. Calvage Mounet, 2019.