

Théorème chinois et application

Leçons : 120, 122, 142

Référence : *Mathématiques pour l'agrégation : Algèbre et géométrie*, J.-E. Rombaldi, p. 249.

Soit A un anneau principal. Soit $(a_j)_{1 \leq j \leq r}$ une suite de r éléments non nuls et non inversibles de A . On note $a = \prod_{j=1}^r a_j$. On note $\pi_j : A \rightarrow A/(a_j)$ et $\pi : A \rightarrow A/(a)$. On note également $b_j = \prod_{i \neq j} a_i$.

Lemme 1. *Si les a_j sont deux à deux premiers entre eux, alors les b_j sont premiers entre eux dans leur ensemble.*

Démonstration du lemme. Par contraposée, supposons que les (b_j) ne soient pas premiers entre eux. Soit donc $p \in A$ un élément premier qui divise tous les b_j .

p divise $\prod_{j \neq 1} a_j$, donc il existe $i \neq 1$ tel que $p \mid a_i$. Mais p divise $b_i = \prod_{j \neq i} a_j$, donc il existe $j \neq i$ tel que $p \mid a_j$, donc a_i et a_j ne sont pas premiers entre eux. CQFD

Théorème 2 (Théorème chinois). *Supposons les (a_j) deux à deux premiers entre eux. Alors, l'application*

$$\begin{aligned} \varphi : A &\longrightarrow \prod_{j=1}^r A/(a_j) \\ x &\longmapsto (\pi_j(x))_{j \in \llbracket 1, r \rrbracket} \end{aligned}$$

est un morphisme d'anneaux, et

$$\text{Ker}(\varphi) = (a) = \left(\prod_{j=1}^r a_j \right),$$

et φ induit alors un isomorphisme

$$\begin{aligned} \bar{\varphi} : A/(a) &\longrightarrow \prod_{j=1}^r A/(a_j) \\ \pi(x) &\longmapsto (\pi_j(x))_{j \in \llbracket 1, r \rrbracket}, \end{aligned}$$

d'inverse

$$\begin{aligned} \bar{\varphi}^{-1} : \prod_{j=1}^r A/(a_j) &\longrightarrow A/(a) \\ (\pi_j(x_j))_{j \in \llbracket 1, r \rrbracket} &\longmapsto \overline{\sum_{i=1}^r x_i u_i b_i}, \end{aligned}$$

où $(u_i)_{i \in \llbracket 1, r \rrbracket} \subset A$ vérifie $\sum_{i=1}^r u_i b_i = 1$.

Démonstration. Il est clair que φ est un morphisme d'anneaux.

Montrons que $\text{Ker}(\varphi) = \left(\prod_{j=1}^r a_j \right)$: Si $x \in \text{Ker}(\varphi)$, alors $\forall j, \pi_j(x) = 0$, donc $\forall j, x \in (a_j)$, i.e. $a_j \mid x$, et les a_j étant premiers entre eux deux à deux, $\prod a_j \mid x$. Donc $x \in (a)$.

Réciproquement, si $x \in \left(\prod a_j \right)$, alors $\pi_j(x) = 0, \forall j$. Donc $\text{Ker}(\varphi) = (a)$.

Montrons maintenant que φ est surjectif : D'après le lemme, les b_j sont premiers entre eux dans leur ensemble, donc, d'après Bézout, il existe $(u_i)_{i \in \llbracket 1, r \rrbracket} \subset A$ tels que $\sum_{i=1}^r u_i b_i = 1$.

Soit $(\pi_j(x_j))_{j \in \llbracket 1, r \rrbracket} \in \prod_{j=1}^r A/(a_j)$.

De plus, on a, $\forall j \in \llbracket 1, r \rrbracket$,

$$\sum_{i=1}^r \pi_j(u_i) \pi_j(b_i) = \pi_j(u_j) \pi_j(b_j) = 1 \quad (\text{le terme } i \neq j \text{ vaut } 0),$$

donc $\pi_j(u_j)$ est l'inverse de $\pi_j(b_j)$ dans $A/(a_j)$.

Posons alors $x = \sum_{i=1}^r u_i x_i b_i$. On a alors $\varphi(x) = (\pi_j(x))_{j \in \llbracket 1, r \rrbracket}$, et

$$\pi_j(x) = \sum_{i=1}^r \pi_j(u_i) \pi_j(x_i) \pi_j(b_i) = \pi_j(x_j),$$

donc φ est bien surjectif.

Donc, par le théorème d'isomorphisme, φ induit un isomorphisme

$$\begin{aligned} \bar{\varphi} : A/(a) &\longrightarrow \prod_{j=1}^r A/(a_j) \\ \pi(x) &\longmapsto (\pi_j(x))_{j \in \llbracket 1, r \rrbracket}, \end{aligned}$$

d'inverse $\bar{\varphi}^{-1} : (\pi_j(x_j)) \mapsto \overline{\sum x_i u_i b_i}$. □

Application : Indicatrice d'Euler

On appelle indicatrice d'Euler la fonction

$$\begin{aligned} \varphi : \mathbb{N}^* &\longrightarrow \mathbb{N} \\ n &\longmapsto \sum_{\substack{d \leq n \\ \text{pgcd}(n, d) = 1}} 1. \end{aligned}$$

On a alors $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.

On remarque aussi que $\varphi(p) = p - 1$ et $\forall \alpha, \varphi(p^\alpha) = (p - 1)p^{\alpha-1}$.

Notons $n = \prod_{i=1}^r p_i^{\alpha_i}$. D'après le théorème chinois, on a

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^r \mathbb{Z}/(p_i^{\alpha_i})\mathbb{Z},$$

donc

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^r (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times,$$

et donc

$$\varphi(n) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$