

Théorème chinois

On montre le théorème chinois et on propose une application à la résolution d'un système de congruences.

Soit A un anneau principal. Soient $r \geq 2$ un entier et $a_1, \dots, a_r \in A$ des éléments premiers entre eux deux à deux.

NOTATION 1

Pour tout $i \in \llbracket 1, r \rrbracket$, on note

$$\pi_i = \pi_{(a_i)} : A \rightarrow A/(a_i)$$

la surjection canonique de A sur $A/(a_i)$. On note également $\pi = \pi_{(a_1 \dots a_r)} : A \rightarrow A/(a_1 \dots a_r)$.

THÉORÈME 2

Théorème chinois.

Alors :

(i) L'application :

$$\begin{aligned} \varphi : A &\rightarrow A/(a_1) \times \dots \times A/(a_r) \\ x &\mapsto (\pi_1(x), \dots, \pi_r(x)) \end{aligned}$$

est un morphisme d'anneaux de noyau $\text{Ker}(\varphi) = (a_1 \dots a_r)$.

(ii) Il existe $u_1, \dots, u_r \in A$ tels que

$$\sum_{i=1}^r u_i b_i = 1$$

où $\forall i \in \llbracket 1, r \rrbracket$, $b_i = \frac{a}{a_i}$ et $a = a_1 \dots a_r$.

(iii) φ est surjectif et induit un isomorphisme $\bar{\varphi} : A/(a_1 \dots a_r) \rightarrow A/(a_1) \times \dots \times A/(a_r)$. On a,

$$\begin{aligned} \bar{\varphi}^{-1} : A/(a_1) \times \dots \times A/(a_r) &\rightarrow A/(a_1 \dots a_r) \\ (\pi_1(x_1), \dots, \pi_r(x_r)) &\mapsto \pi\left(\sum_{i=1}^r x_i u_i b_i\right) \end{aligned}$$

où π est la surjection canonique de A sur le quotient $A/(a_1 \dots a_r)$.

Démonstration. (i) On vérifie sans difficulté que φ est un morphisme d'anneaux (du fait que les projections canoniques sur les quotients en sont). De là,

$$\begin{aligned} \text{Ker}(\varphi) &= \{x \in A \mid \forall i \in \llbracket 1, r \rrbracket, \pi_i(x) = 0\} \\ &= \{x \in A \mid \forall i \in \llbracket 1, r \rrbracket, a_i \mid x\} \\ &= \{x \in A \mid \text{ppcm}(a_1, \dots, a_r) \mid x\} \end{aligned}$$

Mais, $a_1, \dots, a_r$ sont premiers entre eux deux à deux. Donc,

$$\text{ppcm}(a_1, \dots, a_r) = a_1 \dots a_r$$

et on conclut que $\text{Ker}(\varphi) = (a_1 \dots a_r)$.

(ii) Supposons par l'absurde que $b_1, \dots, b_r$ ne sont pas premiers entre eux dans leur ensemble.

Comme A est principal, donc factoriel, il existe un premier $p \in A$ tel que

$$\forall i \in \llbracket 1, r \rrbracket, p \mid b_i$$

Comme p divise $b_1 = a_2 \dots a_r$, il existe $i \in \llbracket 2, r \rrbracket$ tel que $p \mid a_i$. Mais, divisant b_i , il divise a_j où $j \in \llbracket 1, r \rrbracket \setminus \{i\}$. Contradiction car a_1 et a_j sont premiers entre eux. La fin du raisonnement est une conséquence directe du théorème de Bézout valable dans les anneaux principaux.

(iii) Pour $i, j \in \llbracket 1, r \rrbracket$ tels que $i \neq j$, on a

$$\pi_j(b_i) = \pi_j(0)$$

puisque b_i est multiple de a_j . Ceci permet d'écrire

$$\pi_j(1) = \pi_j\left(\sum_{i=1}^r u_i b_i\right) = \pi_j(u_j) \pi_j(b_j)$$

Donc, $\pi_j(b_j)$ est inversible dans $A/(a_j)$, d'inverse $\pi_j(u_j)$. Ainsi, soient $\pi_1(x_1), \dots, \pi_r(x_r) \in A/(a_1) \times \dots \times A/(a_r)$. En posant

$$x = \sum_{i=1}^r x_i u_i b_i$$

on a

$$\pi_j(x) = \pi_j(x_j) \pi_j(u_j) \pi_j(b_j) = \pi_j(x_j)$$

donc $\varphi(x) = (\pi_1(x_1), \dots, \pi_r(x_r))$. Le morphisme φ est surjectif. Par le théorème de factorisation des morphismes, il induit un isomorphisme

$$\begin{array}{ccc} \overline{\varphi}: A/(a_1 \dots a_r) & \rightarrow & A/(a_1) \times \dots \times A/(a_r) \\ \pi(x) & \mapsto & (\pi_1(x), \dots, \pi_r(x)) \end{array}$$

et on a même prouvé que l'inverse $\overline{\varphi}^{-1}$ est défini par

$$\begin{array}{ccc} \overline{\varphi}^{-1}: A/(a_1) \times \dots \times A/(a_r) & \rightarrow & A/(a_1 \dots a_r) \\ (\pi_1(x_1), \dots, \pi_r(x_r)) & \mapsto & \pi\left(\sum_{i=1}^r x_i u_i b_i\right) \end{array}$$

□

EXEMPLE 3

Le système

$$\begin{cases} u \equiv 1 \pmod{3} \\ u \equiv 3 \pmod{5} \\ u \equiv 0 \pmod{7} \end{cases}$$

admet une unique solution dans $\mathbb{Z}/105\mathbb{Z} : \overline{28}$. Les solutions dans $\mathbb{Z}$ sont donc de la forme $28 + 105k$ avec $k \in \mathbb{Z}$.

Démonstration. On se place dans l'anneau principal $A = \mathbb{Z}$. Les entiers 3, 5 et 7 sont premiers entre eux : le triplet $(1 + (3), 3 + (5), 0 + (7)) = (x_1 + (3), x_2 + (5), x_3 + (7))$ admet un unique antécédent

par $\overline{\varphi}^{-1}$ du Théorème 2. On a ainsi existence et unicité d'une solution modulo $3 \times 5 \times 7 = 105$. On explicite une relation de Bézout pour 15, 21, 35 :

$$\underbrace{-1}_{=u_1} \times \underbrace{35}_{=b_1} + \underbrace{6}_{=u_2} \times \underbrace{21}_{=b_2} + \underbrace{(-6)}_{=u_3} \times \underbrace{15}_{=b_3} = 1$$

Reste à calculer

$$\begin{aligned} \overline{\varphi}^{-1}(1 + (3), 3 + (5), 0 + (7)) &= \sum_{i=1}^3 x_i u_i b_i + (105) \\ &= 1 \times (-1) \times 35 + 3 \times 6 \times 21 + 0 \times (-6) \times 15 + (105) \\ &= 343 + (105) \\ &= 28 + (105) \end{aligned}$$

Les solutions sont bien de la forme escomptée. □

[ULM18] utilise un autre algorithme pour trouver la solution. Le fait de chercher un antécédent permet de faire un lien “direct” avec le Théorème 2. Attention, il faut réussir à trouver les coefficients de Bézout...

Bibliographie

Mathématiques pour l'agrégation

[ROM21]

Jean-Étienne ROMBALDI. *Mathématiques pour l'agrégation. Algèbre et géométrie*. 2^e éd. De Boeck Supérieur, 20 avr. 2021.

<https://www.deboecksuperieur.com/ouvrage/9782807332201-mathematiques-pour-l-agregation-algebre-et-geometrie>.

Anneaux, corps, résultants

[ULM18]

Felix ULMER. *Anneaux, corps, résultants. Algèbre pour L3/M1/agrégation*. Ellipses, 28 août 2018.

<https://www.editions-ellipses.fr/accueil/9852-20186-anneaux-corps-resultants-algebre-pour-l3-m1-agregation-9782340025752.html>.