

Théorème chinois et plus...

(BERMUT, Algèbre, le grand combat p463)

Récapitulons: 132, 142, 120, 447

Proposition:

A commutatif. $I_1, \dots, I_m \triangleleft A$ deux à deux comaximales.
Alors pour tout $x_1, \dots, x_m \in A$, il existe $x \in A$ tel que:

$$\begin{cases} x \equiv x_1 \pmod{I_1} \\ \vdots \\ x \equiv x_m \pmod{I_m} \end{cases}$$

Preuve:

On procède par récurrence sur m .

→ Si $m=1$, x_1 est solution.

→ Supposons que $m=2$: I_1 et I_2 sont comaximales, donc il existe $a_1 \in A_1$ et $a_2 \in A_2$ tels que $a_1 + a_2 = 1$.

Encore x autre manière

Soit alors $x = x_1 a_1 + x_2 a_2$.

Alors, on a:

$$x = x_1(1 - a_2) + x_2 a_2 = x_1 + a_2(x_2 - x_1) \quad \text{donc } x \equiv x_1 \pmod{I_1}$$

De même:

$$x = x_1 a_1 + x_2(1 - a_1) = x_2 + a_1(x_1 - x_2) \quad \text{donc } x \equiv x_2 \pmod{I_2}$$

Donc ok!

→ Supposons que le théorème soit vrai pour $m \geq 2$ et montrons le au rang $m+1$.

$I_1, \dots, I_{m+1} \triangleleft A$ sont comaximales et par hypothèse, il existe $y \in A$ tel que $y \equiv x_i \pmod{I_i} \quad \forall i \in \{1, m\}$.

$I_1 \cap \dots \cap I_m$ et I_{m+1} étant comaximales à leur tour, on a:

D'après le cas $m=2$, il existe $x \in A$ tel que:

x peut autrement

$$x \equiv y \pmod{I_1 \cap \dots \cap I_m} \quad \text{et} \quad x \equiv x_{m+1} \pmod{I_{m+1}}$$

Donc alors $x \equiv y \equiv x_i \pmod{I_i}$ pour tout $i \in \{1, m\}$ et $x \equiv x_{m+1} \pmod{I_{m+1}}$ donc de

la récurrence, ok!

Théorème (Chinois):

Soient $I_1, \dots, I_m \triangleleft A$ deux à deux comaximales.

Pour $i \in \{1, m\}$ et $a \in A$, on note $[a]_i$ la classe de a modulo I_i .

Alors le morphisme $\beta: A \rightarrow A/I_1 \times \dots \times A/I_m$ est surjectif, de

noyau $I_1 \cap \dots \cap I_m$.

En particulier, on a un isomorphisme d'anneaux $A/I_1 \cap \dots \cap I_m \simeq A/I_1 \times \dots \times A/I_m$.

Rq: Si A principal, il existe $a_1, \dots, a_m \in A$ deux à deux étrangers /p/ $I_1 = (a_1), \dots, I_m = (a_m)$ et $I_1 \cap \dots \cap I_m = (a_1 \dots a_m)$

Preuve: → Surjectivité par la prop. précédente.

$$\rightarrow \text{Ker}(\beta) = \{x \in A \mid [x]_i = 0 \quad \forall i \in \{1, m\}\}$$

$$= \{x \in A \mid \forall i \in \{1, m\}, x \in I_i\}$$

$$= I_1 \cap \dots \cap I_m$$

→ L'isomorphisme est une application d'un thm d'isomorphisme

Proposition:

On pose $\bar{e}_i = \Psi^{-1}(\varepsilon_i)$ avec $\varepsilon_i = (\pi_{1,i}(0), \dots, \pi_{i,i}(0), \pi_{i,i}(1), \pi_{i,i}(0), \dots, \pi_{n,i}(0))$
 Alors l'inverse de $\Psi: A/(a_1 \dots a_n) \xrightarrow{\sim} A/(a_1) \times \dots \times A/(a_n)$
 $\bar{x} \mapsto ([x]_1, \dots, [x]_n)$

$$\text{et } \Psi^{-1}: A/(a_1) \times \dots \times A/(a_n) \xrightarrow{\sim} A/(a_1 a_2 \dots a_n) \\ ([x_1]_1, \dots, [x_n]_n) \mapsto \sum_{i=1}^n \bar{e}_i \bar{x}_i.$$

Preuve:

On remarque que l'on a:

$$([x_1]_1, \dots, [x_n]_n) = \varepsilon_1([x_1]_1, \dots, [x_n]_n) + \dots + \varepsilon_n([x_1]_1, \dots, [x_n]_n) \\ = \Psi(\bar{e}_1)\Psi(\bar{x}_1) + \dots + \Psi(\bar{e}_n)\Psi(\bar{x}_n) \\ = \Psi\left(\sum_{i=1}^n \bar{e}_i \bar{x}_i\right)$$

□

Application: Déterminer l'inverse de $\Psi: \mathbb{Z}/84\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$
 $\bar{x} \mapsto (\bar{x}, \bar{x}, \bar{x})$

$$\bar{e}_1 = \Psi^{-1}(1, 0, 0) \\ \begin{cases} e_1 \equiv 1 [3] \\ e_1 \equiv 0 [28] \end{cases} \quad \bar{e}_1 = 28 \text{ convient}$$

$$\bar{e}_2 = \Psi^{-1}(0, 1, 0) \\ \begin{cases} e_2 \equiv 1 [4] \\ e_2 \equiv 0 [21] \end{cases} \quad \bar{e}_2 = 21 \text{ convient}$$

$$\bar{e}_3 = \Psi^{-1}(0, 0, 1) \\ \begin{cases} e_3 \equiv 1 [7] \\ e_3 \equiv 0 [12] \end{cases} \quad e_3 = h \cdot 12, \quad h \in \mathbb{N} \text{ et } h \cdot 12 \equiv 1 [7] \\ h \equiv (5)^{-1} [7] \\ h \equiv 3 [7]. \quad h = 3 \text{ donc.} \\ \bar{e}_3 = 36 \text{ convient.}$$

$$\text{Donc } \Psi^{-1}: \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/84\mathbb{Z} \\ (\bar{x}, \bar{y}, \bar{z}) \mapsto 28\bar{x} + 21\bar{y} + 36\bar{z}$$

Application: Déterminer l'inverse de $\Psi: \mathbb{R}[X]/(x^4+x^2) \xrightarrow{\sim} \mathbb{R}[X]/(x^2) \times \mathbb{R}[X]/(x^2+1)$
 $\bar{p} \mapsto (\bar{p}, \bar{p})$

$$\bar{e}_1 = \Psi^{-1}(1, 0) \\ \begin{cases} e_1 \equiv 1 [x^2] \\ e_1 \equiv 0 [x^2+1] \end{cases} \quad \bar{e}_1 = x^2 + 1 \text{ convient}$$

$$\bar{e}_2 = \Psi^{-1}(0, 1) \\ \begin{cases} e_2 \equiv 0 [x^2] \\ e_2 \equiv 1 [x^2+1] \end{cases} \quad e_2 = Q \cdot x^2, \quad Q \in \mathbb{R}[X] \text{ et } Q \cdot x^2 \equiv 1 [x^2+1] \\ \bar{e}_2 = -x^2 \text{ convient} \quad \text{de } Q = -1 [x^2+1]$$

$$\Psi^{-1}: \mathbb{R}[X]/(x^2) \times \mathbb{R}[X]/(x^2+1) \xrightarrow{\sim} \mathbb{R}[X]/(x^4+x^2) \\ (\bar{p}, \bar{q}) \mapsto (x^2+1)\bar{p} + (-x^2)\bar{q}$$