Théorème des restes chinois :

Référence : [Rombaldi 244] [Esc 463]

Énoncé : Soit A un anneau principal, $a_1, \dots, a_n$ des éléments de A premiers entre eux

Alors $A/(a_1 \dots a_n) \simeq A/(a_1) \times \dots \times A/(a_n)$

Étapes et remarques : Det entier

Étape 1 : $\varphi : A \longmapsto A/(a_1) \times \dots \times A/(a_n)$ morphisme d'anneaux

Étape 2 : $\ker(\varphi) = (a_1 \dots a_n)$

Étape 3 : φ surjective

Étape 3.1 : $b_i = \prod_{j \neq i} a_j$ (b_i) sont premiers dans leur ensemble

Étape 3.2 : $u_1 b_1 + \dots + u_n a_n = 1$ $x = \sum_{i=1}^{n} u_i b_i x_i$

$\varphi(x) = (x_1, \dots, x_n)$ (Bézout)

Rq 1 : Dans $\mathbb{Z}$, $|\mathbb{Z}/(a_1 \dots a_n)| = |\mathbb{Z}/(a_1) \times \dots \times \mathbb{Z}/(a_n)|$

Rq 2 : Résolu^{e} de $x \equiv 2[3]$ $x \equiv 3[5]$ $x \equiv 2[7]$

Rq 3 : Polynôme de Lagrange

Rq 3.1 : $\mathbb{K}[X]$ ppal $(X - a_i)$ premiers 2-à-2 $\rightarrow$ Thm Chin.

Rq 3.2 : $\mathbb{K}[X]/(a_i) \simeq \mathbb{K} \Rightarrow \mathbb{K}[X]/(a_1 \dots a_n) \simeq \mathbb{K}^n$

Soit A un anneau principal.

Soit $a_1, \dots, a_n \in A^*$ premiers entre eux deux-à-deux.

ssi $A/(a_1 \dots a_n) \cong A/(a_1) \times \dots \times A/(a_n)$

Etape 1 : Construction d'un isomorphisme.

Soit $\varphi : A \longrightarrow A/(a_1) \times \dots \times A/(a_n)$

$$x \longmapsto (\overline{x}^1, \dots, \overline{x}^n)$$

φ est un morphisme d'anneaux :

- $\varphi(x+y) = (\overline{x+y}^1, \dots, \overline{x+y}^n) = (\overline{x}^1, \dots, \overline{x}^n) + (\overline{y}^1, \dots, \overline{y}^n) = \varphi(x) + \varphi(y)$
- $\varphi(xy) = (\overline{xy}^1, \dots, \overline{xy}^n) = (\overline{x}^1\overline{y}^1, \dots, \overline{x}^n\overline{y}^n) = \varphi(x)\varphi(y)$.

Soit $x \in \ker(\varphi)$,

$\overline{x}^i = 0$ pour tout $i \in \{1 \dots n\}$

donc $\forall i \in \{1, \dots, n\}$ $x \in (a_i)$

Donc x est multiple commun aux a_i. Comme A est principal $\ker(\varphi) = (\mu)$, où μ est le ppcm de $a_1, \dots, a_n$. Or $a_1, \dots, a_n$ sont premiers entre eux donc leur ppcm est $\mu = a_1 \dots a_n$ (*) ← démo à maîtriser

Donc $\ker(\varphi) = (a_1 \dots a_n)$

On peut donc factoriser φ :

On a alors $\tilde{\varphi} : A/(a_1 \dots a_r) \longrightarrow \mathrm{Im}(\varphi)$

Étape 2 : mq $\mathrm{Im}(\varphi) = A/(a_1) \times \dots \times A/(a_r)$. Pour cela, il nous faut mq φ est surjectif

Soit $(\overline{x_1}^1, \overline{x_2}^2 \dots, \overline{x_r}^r) \in A/(a_1) \times \dots \times A/(a_r)$

on cherche un antécédent sous la forme $x \in A$ et

$$x = \nu_1 x_1 + \dots + \nu_r x_r$$

et on voudrait que $\forall i \in \{1 \dots r\}$, $\overline{x}^i = \overline{x_i}^i$ donc il nous faut $\overline{\nu_i}^i = 1$ et $\forall j \in \{1 \dots r\}$, $i \neq j$ $\overline{\nu_j x_j}^i = \overline{0}^i$

une idée serait donc que :

$\forall j \in \{1 \dots r\}$ $a_i \mid \nu_j$ pour tout $i \neq j$

on va poser $\forall j \in \{1 \dots r\}$ $b_j = \dfrac{a_1 \dots a_r}{b_j} = \prod_{\substack{i=1 \\ j \neq i}}^{r} a_i$

Mq les b_i sont premiers dans leur ensemble.

Supposons $\exists \delta \in A^\times$, tel que $\delta \mid b_j$ pour tout $j \in \{1 \dots r\}$

comme A est principal il est factoriel donc δ a une DPFI. Et premier est équivalent à irréductible dans un anneau factoriel donc $\exists p \in A^* \setminus A^\times$ premier tel que $p \mid b_j$ pour tout $j \in \{1 \dots r\}$.

Donc en particulier $p \mid b_1$. $\exists i \in \{2 \dots r\}$ $p \mid a_i$

De même $p \mid b_i$ donc $\exists k \in \{1 \dots r\}$ $k \neq i$ $p \mid a_k$. Absurde.

Ainsi les b_j sont premiers entre eux dans leur ensemble.

Donc par le théorème de Bézout, $\exists u_1 \dots u_n \in A$ tq

$$\sum_{j=1}^{n} u_j b_j = 1$$

Soit $i \in \{1, \dots, n\}$, pour tout $j \neq i$, $a_i \mid b_j$ donc $\overline{u_j}^i \overline{b_j}^i = \overline{0}^i$

$$\overline{\sum_{j=1}^{n} u_j b_j}^i = \sum_{j=1}^{n} \overline{u_j b_j}^i = \overline{u_i}^i \overline{b_i}^i = \overline{1}^i$$

Donc on a trouvé les v_i dont on parlait :

Soit $x = \sum_{j=1}^{n} x_j u_j b_j$

Donc $\forall i \in \{1 \dots n\}$ $\overline{x}^i = \overline{x_i u_i b_i}^i = \overline{x_i}^i$

D'où φ surjective.

Donc on a bien $A/(a_1 \dots a_n) \cong A/(a_1) \times \dots \times A/(a_n)$

<u>Applications et remarques</u> : (à faire si possible le jour J)

- <u>Rq démo dans $\mathbb{Z}$</u> : l'étape 2 est très longuement raccourcie en effet, $\mathbb{Z}/(a_1 \dots a_n)$ est de cardinal $a_1 \dots a_n$ et $\mathrm{Im}(\varphi) \subseteq \underbrace{\mathbb{Z}/(a_1)}_{\text{cardinal } a_1} \times \dots \times \underbrace{\mathbb{Z}/(a_r)}_{\text{cardinal } a_r}$, de cardinal $a_1 \dots a_r$

Avec l'injectivité et l'égalité des cardinaux, on peut conclure tout de suite.

· Application 45 : 3, 5 et 7 sont premiers entre eux deux-à-deux. Par surjectivité de $\tilde{\varphi}$ on sait qu'il existe $x \in \mathbb{Z}$ tq

$$x \equiv 2\,[3]$$
$$x \equiv 3\,[5]$$
$$x \equiv 2\,[7]$$

$a_1 = 3,\ a_2 = 5,\ a_3 = 7$ $\qquad \mathbb{Z}/105\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$

$b_1 = 35 \quad b_2 = 21 \quad b_3 = 15$

On cherche u_1, u_2, u_3 tq $u_1 b_1 + u_2 b_2 + u_3 b_3 = 1$

$-1 \times 35 + 1 \times 21 + 1 \times 15 = 1$

On pose $x = -1 \times 35 \times 2 + 1 \times 21 \times 3 + 1 \times 15 \times 2$

$$x = -70 + 63 + 30 = 23$$

Donc il y a 23 objets [Esc 19.8]

· Application [polynômes interpolateur de lagrange] :

Soit $A = \mathbb{K}[X]$, $\mathbb{K}$ un corps et pour tout $i \in \{1 \dots r\}$

$P_i = (X - a_i)$ où les $a_i \in \mathbb{K}$ sont distincts deux-à-deux

$\forall i, j \in \{1 \dots n\},\ i \neq j,\ \operatorname{pgcd}(P_i, P_j) = -a_i + a_j \in \mathbb{K}^*$ donc inversible. Les polynômes P_i sont premiers entre eux deux-à-deux et $\mathbb{K}[X]$ est principal. On peut appliquer le thm de restes chinois

$$\mathbb{K}[X]/((X-a_1)(X-a_2)\dots(X-a_r)) \cong \mathbb{K}[X]/(X-a_1) \times \dots \times \mathbb{K}[X]/(X-a_r)$$

Or pour tout $i \in \{1, \dots, r\}$

$\Psi : \mathbb{K}[X] \longrightarrow \mathbb{K}$ est un morphisme d'anneaux

$P \longmapsto P(a_i)$

$(\Psi(P+Q) = (P+Q)(a_i) = P(a_i) + Q(a_i)$

$\Psi(PQ) = (PQ)(a_i) = P(a_i)Q(a_i)$

$\Psi(1) = 1)$

Son noyau est $\ker(\Psi) = \{P \in \mathbb{K}[X] \mid a_i \text{ est racine de } P\}$

$= \{(X-a_i)Q \mid Q \in \mathbb{K}[X]\}$

$= (X-a_i)$

Ainsi, par thm de factorisation, on a l'isomorphisme

$\overline{\Psi} : \mathbb{K}[X]/(X-a_i) \xrightarrow{\sim} \mathrm{Im}(\Psi) \quad \overline{P} \longrightarrow P(a_i)$

Or $\forall x \in \mathbb{K}$, on pose $P(X) = x \in \mathbb{K}(x)$ et $\Psi(P) = x$

Donc Ψ est surjective donc $\mathbb{K}[X]/(X-a_i) \simeq \mathbb{K}$

Ainsi, $\mathbb{K}[X]/((X-a_1)\cdots(X-a_r)) \simeq \mathbb{K} \times \mathbb{K} \times \cdots \times \mathbb{K}$

Ainsi $\mathbb{K}[X]/((X-a_1)\cdots(X-a_r)) \longmapsto \mathbb{K} \times \cdots \times \mathbb{K}$ est

$\overline{P} \longrightarrow (P(a_1), \dots, P(a_r))$

un isomorphisme.

Ainsi pour tout $(x_1, \dots, x_r) \in \mathbb{K} \times \cdots \times \mathbb{K}$, il existe une unique classe de polynômes $\overline{Q}$ tq $\forall P \in \overline{Q}$

$\forall i \in \{1 \dots r\} \quad P(a_i) = x_i$

Or $\overline{Q} \in \mathbb{K}[X]/((X-a_1)\cdots(X-a_r))$ donc il existe un

unique polynôme P de degré $\deg(P) < r$ tel que $P \in \overline{Q}$ (faire la division euclidienne de Q par $(X-a_1)\cdots(X-a_r)$)

Finalement, pour tout $(a_1, \dots, a_r) \in \mathbb{K}^r$, $(x_1, \dots, x_r) \in \mathbb{K}^r$, il existe un unique polynôme $P \in \mathbb{K}[X]^*$ de degré (*) inférieur à r tel que $\forall i \in \{1, \dots, r\}$ $P(a_i) = x_i$. □

(*) strictement

Supplément : [Rom p238]

- Appal ⇒ A à pgcd : Soient $a_1, \dots, a_n \in A^*$ $(a_1, \dots, a_n)$ est un idéal de A. Donc $\exists \delta \in A^*$ tq $(\delta) = (a_1, \dots, a_n)$ et $\exists (u_1, \dots, u_n) \in A$ $\delta = a_1u_1 + \cdots + a_nu_n$. Soit $d \in A^*$ tq $d \mid a_i$ $\forall i$. Comme $\delta = \sum a_iu_i$, $d \mid \delta$. Donc δ pgcd.
- Bézout [Rom 247] $(a_1, \dots, a_r)$ premiers dans leur ensemble ssi $\exists (u_1, \dots, u_n) \in A$ tq $\sum a_iu_i = 1$

⇒ ok

⇐ Supp $u_1a_1 + \cdots + u_na_n = 1$. Si $\delta \mid a_i$ $\forall i$, $\delta \mid 1$ donc $\delta \in A^\times$ donc $a_1, \dots, a_n$ premiers dans leur ensemble

Supplément ppcm ⇝ pgcd : [Rom 341]

A est à pgcd ssi $\forall (a;b) \in A^*$, a et b admettent un ppcm et $ab = ppcm(a;b)\, pgcd(a;b)$.

⇒ Soit $\delta = pgcd(a;b)$ premiers entre eux

$\delta | a$, $\delta | b$ donc $\exists (\alpha;\beta) \in A^*$ tq $\delta\alpha = a$ $\delta\beta = b$

On pose $\mu = \alpha b = \alpha\beta\delta = a\beta$. est un commun mult

Soit m un multiple commun.

$\exists u, v \in A^*$ tq $m = au = bv$

donc $\alpha\delta u = \beta\delta v$ donc $\alpha u = \beta v$ donc $\alpha | \beta v$

donc $\alpha | v$ car α et β sont premiers entre eux

Donc $\exists \tilde{v} \in A$ tq $v = \tilde{v}\alpha$ donc $m = b\alpha\tilde{v} = \mu\tilde{v} \in (\mu)$

Donc μ ppcm de a et b.

Donc $\mu\delta = ab$

⇐ Soient $a;b \in A$, $\mu = ppcm(a;b)$. Comme ab est multiple commun à a et b, $\mu | ab$ donc $\exists \delta \in A^*$ tq $\delta\mu = ab$ Mq $\delta = pgcd(a;b)$. $\delta\mu = ab$ or $\mu = \alpha a = \beta b$

donc $\delta\alpha a = ab$ donc $\delta\alpha = b$ donc $\delta | b$. De même $\delta | a$.

Soit d un diviseur commun à a, b. Mq $d | \delta$

$ud = a$ et $vd = b$ donc $uvd = av = ub$

donc $uvd \in (\mu)$ donc $v\mu = uvd$

Donc $w\mu = uvd$

Donc $w\mu = a\upsilon$

Donc $dw\mu = ab = \delta\mu$

donc $dw = \delta$

donc $d | \delta$.

Supplément ppcm = $a_1 \dots a_n$: [Rom 343]

Soit $a_1, \dots, a_n$ premiers entre eux deux-à-deux.

alors $ppcm(a_1, \dots, a_n) = a_1 \dots a_n$.

Par récurrence :

▷ $(a_1) \cap (a_2) = (\mu)$ et $\mu = ppcm(a_1; a_2)$

$a_1 a_2 = pgcd(a_1; a_2)\, ppcm(a_1; a_2) = \mu \times 1$.

Donc $\mu = a_1 a_2$

▷ $(a_1) \cap (a_2 \dots a_n) = (\mu)$ et $\mu = a_1 \dots a_n$.

⇒ $(a_1) \cap \dots \cap (a_n) = (\mu) = (a_1 \dots a_n)$

$\|$

$(ppcm(a_1, \dots, a_n))$.

Thm des restes chinois - dvt : ✓

Soit A un anneau principal et $a_1, \dots, a_n$ des éléments premiers entre eux deux-à-deux. Alors

$$A/(a_1 a_2 \dots a_n) \cong A/(a_1) \times \dots \times A/(a_n)$$

Démo : $\varphi : A \to A/(a_1) \times \dots \times A/(a_n)$ est un morphisme d'anneaux ($\varphi(a+b) = \varphi(a) + \varphi(b)$ et $\varphi(ab) = \varphi(a)\varphi(b)$).
$\ker(\varphi) = \{a \in A \mid \Pi_i(a) = 0 \ \forall i \in \{1 \dots n\}\}$. Donc a est un multiple commun à tous les a_i. Or comme A est principal, les a_i ont un ppcm et $\ker(\varphi) = (\text{ppcm}(a_1, \dots, a_n))$
Dans A principal, $\text{ppcm}(a_1, \dots, a_n) = a_1 \dots a_n$ donc finalement $\ker(\varphi) = (a_1 \dots a_n)$.
Par thm de factorisation $\tilde{\varphi} : A/(a_1 \dots a_n) \xrightarrow{\sim} \text{Im}(\varphi)$.

Mq φ est surjective. Soit $(\overline{x_1}^1, \dots, \overline{x_n}^n) \in A/(a_1) \times \dots \times A/(a_n)$.
On cherche $x \in A$ tq $\varphi(a) = (\overline{x_1}^1, \dots, \overline{x_n}^n)$
Analyse : on veut $\forall i \in \{1, \dots, n\}$ $\Pi_i(x) = \overline{x_i}^i$, i.e. $x = a_i \times y_i + x_i \times v_i$ avec $a_i \wedge v_i$ et $\Pi_i(v_i) = \overline{1}^i$.
On cherche x sous la forme $x = x_1 v_1 + x_2 v_2 + \dots + x_n v_n$ avec $\forall i \neq j$ $a_i \mid v_j$ et $\Pi_i(v_i) = \overline{1}^i$.
Pour tout $i \in \{1, \dots, n\}$ on pose $b_i = \prod_{\substack{j=1 \\ j \neq 1}}^{n} a_j$. Mq les b_j sont premiers dans leur ensemble :
Supp $\delta = \text{pgcd}(b_1, \dots b_j)$, $\delta \notin A^\times$. A principal donc factoriel donc $\exists p \in A$, p premier tq $p \mid \delta$ donc $p \mid b_1$ p premier et $b_1 = a_2 \dots a_n$ donc $\exists i \in \{1, \dots, n\}$ tq $p \mid a_i$.
Et $p \mid b_i$ donc $\exists j \in \{1 \dots n\} \setminus \{i\}$ tq $p \mid a_j$: Impossible. $\delta \in A^\times$ et les b_j sont premiers entre eux dans leur ensemble.
Donc par le thm de Bézout $\exists u_1, \dots, u_n \in A$ tq $\sum_{i=1}^{n} b_i u_i = 1$.
Synthèse : On pose $x = \sum_{i=1}^{n} x_i b_i u_i$. On a alors $\forall j \in \{1, \dots, n\}$ $\Pi_j(x) = \sum_{i=1}^{n} \Pi_j(x_i b_i u_i)$. $\forall i \neq j$ b_i multiple de a_j donc $\Pi_j(x_i b_i u_i) = \overline{0}^j$. Donc $\Pi_j(x) = \Pi_j(x_j b_j u_j)$ par ailleurs $\sum_{i=1}^{n} b_i u_i = 1$ donc $\overline{1}^j = \sum_{i=1}^{n} \Pi_j(u_i b_i) = \Pi_j(u_j b_j)$ donc $\Pi_j(x) = \Pi_j(x_j b_j u_j) = \Pi_j(x_j) = \overline{x_j}^j$. Donc φ surjective. Donc

$$A/(a_1 \dots a_n) \cong A/(a_1) \times \dots \times A/(a_n) \quad \square$$

Rq : Dans $\mathbb{Z}$ $|\mathbb{Z}/(a_1 \dots a_n)| = a_1 \dots a_n$ et $|\mathbb{Z}(a_1) \times \dots \times \mathbb{Z}/(a_n)| = a_1 \dots a_n$. Normal.

Théorème des restes chinois - Polynôme de Lagrange : ✓

Soit n un entier, $E = \mathbb{K}[X]$ et $a_1, \dots, a_{n+1}$ des éléments de $\mathbb{K}$ deux-à-deux distincts et $b_1, \dots, b_{n+1}$ des éléments quelconques de $\mathbb{K}$. Alors il existe un unique polynôme P de degré inférieur ou égal à n tel que $\forall i \in \{1, \dots, n+1\}$ $P(a_i) = b_i$

Démo : les polynômes $(X - a_i)$ sont premiers entre eux deux-à-deux car $\text{pgcd}(X - a_i ; X - a_j) = -a_i + a_j \in \mathbb{K}^*$ car $a_i \neq a_j$ et $\mathbb{K}[X]$ est principal car $\mathbb{K}$ corps donc d'après le Thm des chinois on a $\mathbb{K}[X]/((X-a_1)\dots(X-a_{n+1})) \cong \mathbb{K}[X]/(X-a_1) \times \dots \times \mathbb{K}[X]/(X-a_{n+1})$

Mq $\mathbb{K}/(a_i) \cong \mathbb{K}$

Soit $\varphi_i : \mathbb{K}[X] \longrightarrow \mathbb{K}$, $P \longmapsto P(a_i)$

$\ker(\varphi) = \{P \in \mathbb{K}[X] \mid a_i \text{ est racine de } P\}$

$\ker(\varphi) = \{(X - a_i)Q \mid Q \in \mathbb{K}[X]\}$

$\ker(\varphi) = (X - a_i)$

Alors $\tilde{\varphi}_i : \mathbb{K}[X]/(X-a_i) \xrightarrow{\sim} \text{Im}(\varphi_i)$ or φ_i est surjective

$\forall x \in \mathbb{K}$ $P(X) = x$ est tq $\varphi_i(P) = x$

Donc $\mathbb{K}[X]/(X-a_i) \cong \mathbb{K}$. On en déduit un isomorphisme d'anneaux : $\mathbb{K}[X]/((X-a_1)\dots(X-a_n)) \xrightarrow{\sim} \mathbb{K} \times \dots \times \mathbb{K}$

$\overline{P} \longmapsto (P(a_1), \dots, P(a_{n+1}))$

Ainsi $\forall (b_1, \dots, b_{n+1}) \in \mathbb{K}^{n+1}$, $\exists ! \overline{Q} \in \mathbb{K}[X]/((X-a_1)\cdots(X-a_n))$

Donc il existe un unique polynôme P tel que $\deg(P) \leq n$

(faire la $\div$ eucl de Q par $(X-a_1)\cdots(X-a_n)$ $\square$