Dev 10

lundi 17 janvier 2022 09:59

Dev n° 10

Ref : Jean Etienne Rombaldi "Mathématique par l'agrégation : Algèbre et géométrie" p 249
+ Felix Ulmer "Anneaux, corps, résultants" p58

Titre : Théorème Chinois

Soit $\mathbb{A}$ un anneau unitaire principal.

Le but de ce jour va être de démontrer ce thm :

Thm :
Soit $a_1, \dots, a_r$ deux à deux premier entre eux et non nuls.
L'application :

$$\mathcal{L} : x \in \mathbb{A} \mapsto (\pi_1(x), \dots, \pi_r(x)) \in \prod_{j=1}^{r} \frac{\mathbb{A}}{(a_j)}$$

est un morphisme (1) d'anneaux (2) surjectif de noyau $\ker(\mathcal{L}) = \left(\prod_{j=1}^{r} a_j\right) = a$. (3)

Et $\mathcal{L}$ induit (4) un isomorphisme d'anneaux

$$\mathcal{I} : \pi(x) \in \frac{\mathbb{A}}{(a)} \mapsto (\pi_j(x))_{1 \le j \le r} \in \prod_{j=1}^{r} \frac{\mathbb{A}}{(a_j)},$$

d'inverse :

(5) $$\mathcal{I}^{-1} : (\pi_j(x_j))_{1 \le j \le r} \in \prod_{j=1}^{r} \frac{\mathbb{A}}{(a_j)} \mapsto \sum_{i=1}^{r} x_i u_i b_i \in \frac{\mathbb{A}}{(a)},$$

où $(u_j)_{1 \le j \le r}$ est une suite d'éléments de $\mathbb{A}$ telle que $\sum_{j=1}^{r} u_j b_j = 1$

On montre un lemme en préliminaire.

Lemme :
Soit $(b_j)_{1 \le j \le r}$ la suite d'élément de $\mathbb{A}$ définit par $b_j = \frac{a}{a_j} = \prod_{\substack{i=1 \\ i \neq j}}^{r} a_i$.
Si les a_j sont deux à deux premiers entre eux $\forall j$.
Alors,
les b_j sont premiers entre eux dans leur ensemble.

Démo : (lemme)
Procédons par l'absurde.
S.q. b_j ne sont pas premier entre eux dans leur ensemble.
Alors, $\exists\, p \in \mathbb{A}$ qui divise tous les b_j. ($\mathbb{A}$ anneau principal est factoriel).
Comme p divise $\begin{cases} b_1 = \prod_{i=1}^{r} a_i, & \text{il divise un } a_j \text{ par } i \in [\![2, r]\!]. \\ b_i, & \text{il divise un } a_k \text{ par } k \neq i. \end{cases}$ ↯
car les a_i et a_k sont premiers entre eux ⊡

sont premiers entre eux □

Demo: (Thm)

(1) • Il est clair que l'application $f : x \in \mathbb{A} \mapsto (\pi_j(x))_{1\le j\le r} \in \prod_{j=1}^{r} \frac{\mathbb{A}}{(a_j)}$ est un morphisme d'anneaux. par la surj. canonique.

(2) • Q.q $\ker f = a$:

Son noyau est formé des multiples de tous les a_j.

Donc, de leur ppcm. Or ces a_j sont premiers entre eux alors $\text{ppcm}(a_1,\dots,a_r) = a$. On a montrer une inclusion. L'autre est directe.

• Q.q $\pi_j(b_j)$ est inversible :

Comme les $b_i = \frac{a}{a_i}$ sont premier entre eux dans leur ensemble (remme), on peut appliquer le thm de Bézout.

$\exists (u_i)_{1\le i\le r} \in \mathbb{A}$ t.q. $\sum_{i=1}^{r} u_i b_i = 1$.

Pour $j \in [\![1,r]\!]$, on a $\pi_j(b_i) = \pi_j(0) = 0$ pour $i \neq j$ comme b_i a a_j.

De plus,

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

Donc, $\pi_j(b_j)$ est inversible, d'inverse $\pi_j(u_j)$. (dans $\frac{\mathbb{A}}{(a_j)}$)

(3) • Q.q. f est surjectif :

Soit $(\pi_j(x_j))_{1\le j\le r} \in \prod_{j=1}^{r} \frac{\mathbb{A}}{(a_j)}$ fixé, avec $x = \sum_{i=1}^{r} x_i u_i b_i$.

On a :

$$\pi_j(x) = \pi_j(x_j)\underbrace{\pi_j(u_j)\,\pi_j(b_j)}_{=1} = \pi_j(x_j) \qquad \forall j \in [\![1,r]\!]$$

Soit $f(x) = (\pi_j(x_j))_{1\le j\le r}$.

Le morphisme f est donc surjectif

(4) • En appliquant le 1er thm d'isomorphisme, on a :

$$\overline{f} : \frac{\mathbb{A}}{(a)} = \frac{\mathbb{A}}{\ker(f)} \to \prod_{j=1}^{r} \frac{\mathbb{A}}{(a_j)}, \ \pi(x) \mapsto (\pi_j(x))_{1\le j\le r}$$

(5) • L'inverse (par construction et surjectivité) :

$$\overline{f}^{-1} : \prod_{j=1}^{r} \frac{\mathbb{A}}{(a_j)} \to \frac{\mathbb{A}}{(a)} ; \ (\pi_j(x_j))_{1\le j\le r} \mapsto \sum_{i=1}^{r} x_i u_i b_i. \ \square$$

Faisons une application de ce theoreme :

Application:

On cherche à résoudre :

$$\begin{cases} x \equiv 1 \ [3] \\ x \equiv 3 \ [5] \\ x \equiv 0 \ [7] \end{cases}$$

On a bien 3, 5 et 7 premiers entre eux.

Posons $\Pi = 3\times5\times7 = 21\times5 = 100+5 = 105$

$\Pi_1 = 5\times7 = 35$ $\quad m_1 = 3$

$\Pi_2 = 3\times7 = 21$ $\quad m_2 = 5$

$\Pi_3 = 3\times5 = 15$ $\quad m_3 = 7$

Donc on doit résoudre :

$n_3 = 3 \times 5 = 15$ $\quad m_3 = 7$

Donc on doit résoudre :

$$\begin{cases} y_1 \equiv 35^{-1} \ [3] \\ y_2 \equiv 21^{-1} \ [5] \\ y_3 \equiv 15^{-1} \ [7] \end{cases}$$

- $35 \equiv 2 \ [3] \rightsquigarrow 2 y_1 \equiv 1 \ [3]$
  $2y_1 + 3p = 1$
  $\Rightarrow y_1 = 2, \ p = -1$
- $21 \equiv 1 \ [5] \rightsquigarrow y_2 \equiv 1 \ [5] \Rightarrow y_2 = 1$
- $15 \equiv 8 \ [7] \rightsquigarrow 8 y_3 \equiv 1 \ [7]$
  $8y_3 + 7p = 1 \Rightarrow y_3 = 1, \ p = -1$

On obtient donc : $x \equiv 2 \times 35 \times 1 + 1 \times 21 \times 3 + 1 \times 15 \times 0 \ [105]$
$\equiv 70 + 63 \ [105] \equiv 133 \ [105] \equiv 28 \ [105]$

Donc, $x = 28 + 105k$, $k \in \mathbb{N}$ est solution du système.

Annexe :

- Anneau : $(A, +, \times)$ anneaux si : $(A,+)$ groupe commutatif
  $\times$ associative
  $\times$ distributive p/r à $+$.
- Anneau unitaire : $(A,+,\times)$ anneaux + la loi $\times$ a un élément neutre
- Anneau principal : si $(A, +, \times)$ est commutatif + unitaire + intègre (= pas de div. de 0) + tous ses idéaux sont principaux (= engendré par 1 élé.)
  (ex : $\mathbb{Z}$, $\mathbb{R}[X]$ et $\mathbb{Z}[X]$ non)
- Morphisme d'anneau : $f : A \to B$ toute application vérifiant $f(x+y) = f(x) + f(y)$ et $f(xy) = f(x) \times f(y)$.
- Thm Bézout :
  Soit $a, b \in \mathbb{Z}$. $a \wedge b = 1 \iff \exists u, v \in \mathbb{Z}$ t.q. $ua + vb = 1$.
  Thm Égalité Bezout :
  $a, b \in \mathbb{Z}$. et $a \wedge b = d \Rightarrow \exists u, v \in \mathbb{Z}$ t.q. $au + bv = d$.

Démo :

(Identité)

Preuve. Un anneau principal est intègre. L'existence de δ se déduit du fait que $(a_1, \cdots, a_r)$ est un idéal de l'anneau principal $\mathbb{A}$. Comme $\delta \in (\delta) = (a_1, \cdots, a_r)$, il existe $(u_1, \cdots, u_r) \in \mathbb{A}^r$ tel que $\delta = \sum_{k=1}^{r} u_k a_k$. De $(a_k) \subset (\delta)$ pour tout k compris entre 1 et r, on déduit que δ divise a_k. Si $d \in \mathbb{A}$ est un diviseur commun aux a_k, il divise aussi $\delta = \sum_{k=1}^{r} u_k a_k$. □

La relation (8.2) est l'identité de Bézout.

(Thm Bézout)

Preuve. L'égalité de Bézout pour le pgcd dans un anneau principal nous donne la condition est nécessaire. Réciproquement s'il existe $u_1, \cdots, u_p$ dans $\mathbb{A}$ tels que $\sum_{k=1}^{r} u_k a_k = 1$, on en déduit alors que $\delta = a_1 \wedge \cdots \wedge a_r$, qui divise tous les a_k, va diviser $1 = \sum_{k=1}^{r} u_k a_k$, ce qui signifie qu'il est inversible, c'est-à-dire que $a_1, \cdots, a_r$

Preuve. L'égalité de Bézout pour le pgcd dans un anneau principal nous donne la condition est nécessaire. Réciproquement s'il existe $u_1, \cdots, u_p$ dans $\mathbb{A}$ tels que $\sum_{k=1}^{r} u_k a_k = 1$, on en déduit alors que $\delta = a_1 \wedge \cdots \wedge a_r$, qui divise tous les a_k, va diviser $1 = \sum_{k=1}^{r} u_k a_k$, ce qui signifie qu'il est inversible, c'est-à-dire que $a_1, \cdots, a_r$ sont premiers entre eux dans leur ensemble. □

- 1er thm d'isomorphisme :

Premier théorème d'isomorphisme : Soit G et G' deux groupes et $f : G \to G'$ un morphisme de groupes. Alors f induit un isomorphisme $\hat{f}$ de $G/\ker f$ sur $f(G)$ défini par $\hat{f}(xH) = f(x)$ où H est le noyau de f.

- Application :

Soit x le plus petit entier positif t.q.
$$\begin{cases} x \equiv 3 [17] \\ x \equiv 4 [11] \\ x \equiv 5 [6] \end{cases}$$
On a bien que 6, 11 et 17 sont premiers entre eux.
Posons : $\Pi := 6 \times 11 \times 17 = 1122$.
$\Pi_1 := 6 \times 11 = 66$ $\quad m_1 := 17$
$\Pi_2 := 6 \times 17 = 102$ $\quad m_2 := 11$
$\Pi_3 := 11 \times 17 = 187$ $\quad m_3 := 6$
Donc, on doit résoudre : $\begin{cases} y_1 \equiv 66^{-1} [17] \\ y_2 \equiv 102^{-1} [11] \\ y_3 \equiv 187^{-1} [6] \end{cases}$

- $66 \equiv -15 [17]$. $\quad -15\, y_1 \equiv 1 [17]$
$\Rightarrow -15 y_1 + 17 p = 1$
$\Rightarrow 15 \times 8 - 7 \times 17 = 1 \Rightarrow y_1 = 8$
- $102 \equiv 3 [11]$. $\quad 3b \equiv 1 [11]$
$\Rightarrow 3b + 11 p = 1$
$\Rightarrow 3 \times 4 - 11 \times 1 = 1 \Rightarrow y_2 = 4$
- $187 \equiv 1 [6] \Rightarrow y_3 \equiv 1 [6] \Rightarrow y_3 = 1$.

On obtient donc : $x \equiv 3 \times 66 \times 8 + 4 \times 102 \times 4 + 5 \times 187 \times 1 [1122]$
$\equiv 785 [1122]$.
Donc $y = 785 + 1122k$, $k \in \mathbb{N}$ les sol. du système et $x = 785$.

- Indicatrice d'Euler :

si $n \wedge m = 1$ alors $\phi(nm) = \phi(n) \cdot \phi(m)$

Démo :

Si $n \wedge m = 1$ alors $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ par le thm
Et $\underbrace{(\mathbb{Z}/nm\mathbb{Z})^\times}_{\text{card } \phi(nm)} \simeq \underbrace{(\mathbb{Z}/n\mathbb{Z})^\times}_{\text{Card } \phi(n)} \times \underbrace{(\mathbb{Z}/m\mathbb{Z})^\times}_{\text{Card } \phi(m)}$ □

- Exemple :

$$\begin{cases} x \equiv 5 [20] \\ x \equiv 4 [6] \end{cases} \Leftrightarrow \begin{cases} x \equiv 5 [4] \\ x \equiv 5 [5] \\ x \equiv 4 [2] \\ x \equiv 4 [3] \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 [4] \\ x \equiv 0 [5] \\ x \equiv 0 [2] \\ x \equiv 1 [3] \end{cases}$$ IMPOSSIBLE

$\begin{cases} x \equiv 5 \ [20] \\ x \equiv 4 \ [6] \end{cases} \Leftrightarrow \begin{cases} x \equiv 5 \ [5] \\ x \equiv 4 \ [2] \\ x \equiv 4 \ [3] \end{cases} \Leftrightarrow \begin{cases} x \equiv 0 \ [5] \\ x \equiv 0 \ [2] \\ x \equiv 1 \ [3] \end{cases}$ IMPOSSIBLE

- Questions colles.

1) Soient I, J idéal de $\mathbb{A}$.

* Quels opérations peut-on faire entre I et J?

$I+J = \{i+j \mid i \in I, j \in J\}$

$I \times J = \{ij \mid i \in I, j \in J\}$ toujours des idéaux

$I \cap J = \{a \mid a \in I \text{ et } a \in J\}$

* Quels inclusions existent-ils ?

$IJ \subset I+J \supset I \cap J \subset IJ$

$I \cup J$

* Est-ton égalité entre $I \cap J \subset IJ$?

Non ex: $A = \mathbb{Z}$, $I = (2)$ et $J = (4)$ on a $I \cap J = (4)$, $IJ = (8)$

2) $\mathbb{A} = \mathbb{Q}[x,y]$ $I = (x^2, y)$, $J = (x, y^2)$

* Est-ce $\mathbb{A}/_{IJ} \cong \mathbb{A}/_I \times \mathbb{A}/_J$?

Non on n'est pas $\mathbb{A}$ principal

* Décrire IJ:

$IJ = (x^3, x^2y^2, xy, y^3)$

* Trouver P t.q. $\overline{P} = \overline{0}$ dans $\mathbb{A}/_I \times \mathbb{A}/_J$ mais $\neq \overline{0}$ dans $\mathbb{A}/_{IJ}$:

$P(X) = x^2$ $\rightsquigarrow$ dans $\mathbb{A}/_I \times \mathbb{A}/_J$ vaut $\overline{0}$

$\rightsquigarrow$ dans $\mathbb{A}/_{IJ}$ ne vaut pas $\overline{0}$

* Conclure:

$I \cap J \not\subseteq IJ$ car $P \in I \cap J$ mais $P \notin IJ$.

Démo : (Pemmme)

Par l'absurde, s.q. b_j ne sont pas premier entre eux dans leurs ensembles.

Alors, $\exists p \in \mathbb{A}$ t.q. $p \mid b_j$, $\forall j \in [\![1,r]\!]$.

Comme p divise : $\begin{cases} b_1 = \prod_{i\neq 1}^{r} a_i & \text{: p divise un } a_i \Rightarrow p \mid a_1 \neq a_i \\ b_i \end{cases}$ ↯ ⊡

Démo: (thm)

- Morphisme d'anneaux:

$f : x \in \mathbb{A} \mapsto (\pi_j(x))_{1\leq j\leq r} \in \mathbb{A}/(a_1) \times \dots \times \mathbb{A}/(a_r)$ OK

- Π.q $\ker f = (a)$:

Le noyau de f: multiple des a_j.

Donc leur ppcm: $\text{ppcm}(a_1,\dots,a_r) = a_1 \times \dots \times a_r = a$.

- Π.q. $\pi_j(b_j)$ inversible:

$b_i = \frac{a}{a_i}$ premiers entre eux (Pemmme)

Par Bezout, $\exists u_1,\dots,u_r \in \mathbb{A}$ t.q. $u_1 b_1 + \dots + u_r b_r = 1$.

Par $j \in [\![1,r]\!]$, on a: $\pi_j(b_i) = 0$ pour $i \neq j$

car b_i prop à a_j.

De plus,

$$\pi_j(1) = 1 = \pi_j(u_1 b_1 + \dots + u_r b_r) = \pi_j(u_j)\pi_j(b_j).$$

Donc, $\pi_j(b_j)^{-1} = \pi_j(u_j)$ dans $\mathbb{A}/(a_j)$.

- Π.q: f surjective:

Soit $(\pi_1(x_1),\dots,\pi_r(x_r))$ fixé.

Posons $x = x_1 u_1 b_1 + \dots + x_r u_r b_r$.

On a par $j \in [\![1,r]\!]$:

$$\pi_j(x) = \pi_j(x_j)\underbrace{\pi_j(u_j)\pi_j(b_j)}_{=1} = \pi_j(x_j).$$

Donc, f surjective.

- Obtention I:

Par le 1er thm d'isomorphisme

- L'inverse:

Par construction de la surjectivité on obtient f^{-1} ⊡

Application:

$$\begin{cases} x \equiv 1\ [3] \\ x \equiv 3\ [5] \\ x \equiv 0\ [7] \end{cases}$$

3, 5, 7 premiers entre eux

$3\times5\times7 = 105$

On resoud :

$$\begin{cases} y_1 \equiv 35^{-1}\ [3] \\ y_2 \equiv 21^{-1}\ [5] \\ y_3 \equiv 15^{-1}\ [7] \end{cases}$$

On a :

* $35 \equiv 2\ [3] \rightsquigarrow 2y_1 \equiv 1\ [3] \Rightarrow y_1 = 2$
* $21 \equiv 1\ [5] \rightsquigarrow y_2 \equiv 1\ [5] \Rightarrow y_2 = 1$
* $15 \equiv 8\ [7] \rightsquigarrow 8y_3 \equiv 1\ [7] \Rightarrow y_3 = -1$

On obtient donc :

$$x \equiv 1\times2\times35 + 3\times1\times21 + 0\times1\times15\ [105]$$
$$\equiv 28\ [105]$$

Donc $x \in \{28 + 105k \mid k \in \mathbb{Z}\}$.