Exemple de brouillon de concours

Dany-Jack Mercier

7 mars 2010

Voici le scan du brouillon que j'ai écrit pour rechercher des réponses aux questions de la première composition de l'agrégation interne 2010. Pourquoi proposer un brouillon sur MégaMaths ? Pour mettre l'accent sur ce moment crucial dans la recherche d'une solution et la gestion du temps pendant une épreuve écrite.

Ce document n'est pas un modèle. Chacun doit agencer son brouillon avec une liberté totale, et le structurer au minimum de façon à le rendre utile pour pouvoir ensuite directement rédiger une solution "au propre". On ne peaufine pas un brouillon, car celui-ci "partira à la poubelle", mais on le structure : on marque les numéros des pages, on signale clairement les questions que l'on traite pour pouvoir les retrouver facilement quelques instants plus tard à l'occasion, on établit des liens, par exemple en dessinant des flèches, pour retrouver un ordre de développement, on barre les passages qui seront a priori inutiles.

Le texte suivant est fourni "en l'état". C'est celui qui m'a permis de passer à l'acte de rédaction. Il contient des méprises et quelques erreurs qui devraient apparaître au moment de la rédaction effective. C'est un exemple de brouillon...

Site MégaMaths : http ://megamaths.perso.neuf.fr/

Contacter le webmestre : dany-jack.mercier@hotmail.fr

BROUILLON PARTIE I

$\sigma \in \mathcal{L}(S(E))$ (1) $P(\sigma)(u) \in S(E)$ $[\sigma(u)]_n = u_{n+1}$

$\boxed{I.1}$ $[P(\sigma)(u)]_n = \mathcal{F}[\sum$

$$P(\sigma) = \sum_{k=0}^{r} p_k \sigma^k$$

$$P(\sigma)(u) = \sum_{k=0}^{r} p_k \sigma^k(u) \qquad u = (u_n) \in S(E)$$

$$\boxed{[P(\sigma)(u)]_n = \sum_{k=0}^{r} p_k [\sigma^k(u)]_n = \sum_{k=0}^{r} p_k u_{k+n}}$$

$\boxed{I.2.a}$ $u \in S(E)$

u linéairement récurrente $\Longleftrightarrow$ $Ann(u) \neq \{0\}$

$\Updownarrow$

$\exists r \in \mathbb{N}$ $\exists q_0, \dots, q_r$, $q_0 \neq 0$ $\forall n$ $q_0 u_{n+r} + \dots + q_r u_n = 0$

$\Updownarrow$

$\exists Q \in K[X]$ $\forall n$ $\sum_{k=0}^{r} q_{r-k} u_{n+k}$

$\Updownarrow$

$\exists Q \in K[X]$ $\forall n$ $[Q(\sigma)(u)]_n = 0$ où $Q = \sum_{k=0}^{r} q_{r-k} X^k$

$\Updownarrow$

$\exists Q \in K[X]$, $\deg Q = r$ $Q(\sigma)(u) = 0$

$\Updownarrow$

$\exists Q \in K[X]$ $\deg Q = r \in \mathbb{N}$ et $Q \in Ann(u)$

$\Updownarrow$

$Ann(u) \neq \{0\}$

②

$\boxed{\text{I.2.b}}$ Facile $\mathrm{Ann}(u)$ = idéal de $K[X]$, qui est un an. principal.

$\boxed{\text{I.3.a}}$ $(2^n+3^n) = u$

$u_n = 2^n + 3^n$

$$(2^{n+1}+3^{n+1}) - 2(2^n+3^n) = 0$$

$$3^{n+1} - 2.3^n$$

$$\alpha(2^{n+1}+3^{n+1}) + \beta(2^n+3^n) = 0$$

$\forall n$ $\quad a(2^{n+2}+3^{n+2}) + b(2^{n+1}+3^{n+1}) + c(2^n+3^n) \stackrel{?}{=} 0$

$(4a+2b+c)2^n + (9a+3b+c)3^n \stackrel{?}{=} 0$

$\begin{cases} 4a+2b+c=0 \\ 9a+3b+c=0 \end{cases}$ oui $\rightarrow$ $c = -2$ $\begin{cases} 2a+b=1 \\ 9a+3b=2 \end{cases}$

$a = \dfrac{\begin{vmatrix} 1 & 1 \\ 2 & 3 \end{vmatrix}}{D} = \dfrac{1}{D}$

$b = \dfrac{\begin{vmatrix} 2 & 1 \\ 9 & 2 \end{vmatrix}}{D} = \dfrac{4-9}{D} = -$

$D = 6-9 = -3$

donc $\begin{cases} a = -\frac{1}{3} \\ b = \frac{5}{3} \end{cases}$

Avec 2 : $\quad a(\quad) + b(\quad) = 0$

$\begin{cases} 2a+b=0 \\ 3a+b=0 \end{cases}$ non

$\forall n \quad -\frac{1}{3}u_{n+2} + \frac{5}{3}u_{n+1} - 2u_n = 0$

$$\boxed{\forall n \quad u_{n+2} - 5u_{n+1} - 6u_n = 0}$$

$q_0 \qquad q_1 \qquad q_2 \qquad\qquad r = 2$

$$P = \sum_{k=0}^{2} q_{2-k}X^k = q_0X^2 + q_1X + q_2$$

$$\boxed{P = X^2 - 5X + 6 \in \mathrm{Ann}(u)}$$

$q_0 X^2$ $q_n X^n + \ldots$ $a_0 X^n + \ldots a_n$

3

$P = X^2 - 5X + 6 \qquad \Delta = 25 - 24 = 1$

$= (X-2)(X-3) \qquad \frac{5 \pm 1}{2} \quad \begin{cases} 3 \\ 2 \end{cases}$

~~[illegible]~~ !

Si 3 : $\mathrm{Ann}(u) = (\Pi_u) = \Pi_u . K[X]$ ~~[illegible]~~.

$P \in \mathrm{Ann}(u) \Rightarrow \Pi_u \mid P \Rightarrow \underset{\text{unitaire}}{\Pi_u} \in \{1, X-2, X-3, P\}$

impossible

$(\text{sinon } \mathrm{Ann}(u) = K[X])$

car $P = 1 \notin \mathrm{Ann}(u)$ car

$1 \in \mathrm{Ann}(u) \Rightarrow u = 0$

Non !

car

Si $X-2 \in \mathrm{Ann}(u)$

alors

$(\tau - 2\,\mathrm{Id})(u) = 0$

i.e. $u_{n+1} - 2u_n = 0$ faux

$(2^{n+1} + 3^{n+1}) - 2(2^n + 3^n) = 0$

$3^{n+1} - 2 \cdot 3^n = 0$

$3 - 2 = 0$!

Donc $\Pi_u = X^2 - 5X + 6$

$\boxed{\text{I.3.b}}$ $u_n = n^2 2^n$

$a u_{n+1} + b u_n = 0$

$a(n+1)^2 2^{n+1} + b n^2 2^n = 0$

$\forall n \quad 2a(n+1)^2 + bn^2 = 0$

$2a(n^2+2n+1)$

$(2a+b)n^2 + 4an + 2a = 0 \Rightarrow a = 0 = b$ impossible

donc $\deg \pi_u \geqslant 2$

$a(n+2)^2 2^{n+2} + b(n+1)^2 2^{n+1} + c n^2 2^n = 0$

$a(n^2+4n+4)\times 4 + 2b(n^2+2n+1) + cn^2 = 0$

$\forall n \quad (4a+2b+c)n^2 + (16a+4b)n + 16a + 2b = 0$

$\begin{cases} 4a+2b+c = 0 \\ 4a+b = 0 \\ 8a+b = 0 \end{cases} \Rightarrow a = b = 0 \Rightarrow a = b = c = 0$ impossible

donc $\deg \pi_u \geqslant 3$

$a(n+3)^2 2^{n+3} + \dots + d n^2 2^n = 0$

$\cancel{(\dots)(n^2+6n+9)\times 8}$

$\cancel{\forall n \quad (8a + 4b + 2c + d)n^2 + (48a}$

$a(n+3)^2 \times 8 + b(n+2)^2 \times 4 + c(n+1)^2 \times 2 + dn^2 = 0$

$8a(n^2+6n+9) + 4b(n^2+4n+4) + 2c(n^2+2n+1) + dn^2 = 0$

$(8a+4b+2c+d)n^2 + (48a+16b+4c)n + (72a+16b+2c) = 0$

$\begin{cases} 8a+4b+2c+d = 0 \\ 12a+4b+c = 0 \\ 36a+8b+c = 0 \end{cases}$

Prenons $c = -2$.

$\begin{cases} 8a+4b+d = 4 \\ 6a+2b = 1 \\ 18a+4b = 1 \end{cases} \longrightarrow D = 24 - 36 = -12$

$a = \frac{1}{D}\begin{vmatrix} 1 & 2 \\ 1 & 4 \end{vmatrix} = \frac{2}{-12} = -\frac{1}{6}$

$b = \frac{1}{D}\begin{vmatrix} 6 & 1 \\ 18 & 1 \end{vmatrix} = \frac{-12}{-12} = 1$

$\Rightarrow d = 4 - 8a - 4b = \cancel{4} + \frac{4}{3} - \cancel{4} = \frac{4}{3}$

donc

$P(X) = -\frac{1}{6}X^3 + X^2 - 2X + \frac{4}{3} \in \mathrm{Ann}(u)$ or $\deg \pi_u = \deg P \Rightarrow \boxed{\pi_u = X^3 - 6X^2 + 12X}$

$\boxed{\text{I.3.c}}$ $(n!)$ suite récurrente ?

S'il existait Π_u unitaire ... $q_0(n+r)! + \dots + q_r n! = 0$

$$\Downarrow$$

$$q_0 + q_1 \frac{1}{n+r} + \dots + q_r \frac{1}{(n+r)\dots(n+1)} =$$

$\lim\limits_{+\infty} (\quad) = 0 = q_0$ absurde

donc NON

$\boxed{\text{I.4}}$ $S(E) \longrightarrow S(F)$ $\quad T \in \mathcal{L}(E,F)$

$u \longrightarrow T(u)$ $\quad [T(u)]_n = T(u_n)$

u lin. récurr. $\Leftrightarrow \exists r \in \mathbb{N}\ \exists\ q_0, \dots, q_r$ $\quad q_0 u_{n+r} + \dots + q_r u_n = 0$

$$\Downarrow$$

$$q_0 T(u_{n+r}) + \dots + q_r T(u_n) = 0$$

$$\Downarrow$$

$$q_0 [T(u)]_{n+r} + \dots + q_r [T(u)]_n =$$

$$\Downarrow$$

$T(u)$ lin récurr

$\boxed{\text{I.5}}$ $\mathcal{R}(E)$ = sous-ens. de $S(E)$ formé des suites lin récurrentes.

$\mathcal{R}(E)$ = s.e.v de $S(E)$?

~~Non car ... $u_{n+2} + \beta u_{n+1} + \gamma u_n = 0$~~ ~~$(u_n + v_n)$ non récurrente ?~~

$\lambda \in K$ $\quad u \in \mathcal{R}(E) \Rightarrow \lambda u \in \mathcal{R}(E)$ ok

$u, v \in \mathcal{R}(E) \Rightarrow u + v \in \mathcal{R}(E)$ oui

Preuve :

$\exists P \quad P(\tau)(u) = 0$

$\exists Q \quad Q(\tau)(v) = 0$

$u, v \in \mathcal{R}(E)$

$$\Longrightarrow (PQ)(\tau)(u+v) = (PQ)(\tau)(u) + (PQ)(\tau)(v)$$

$$= Q(\tau)\underbrace{(P(\tau))(u)}_{0} + P(\tau)\underbrace{[Q(\tau)](v)}_{0}$$

$$= 0 \Longrightarrow u + v \in \mathcal{R}(E)$$

I.6.a

Soit m le poly. minimal de A.

$$P \in \mathrm{Ann}((A^n)) \iff P(\sigma)((A^n)) = 0$$
$$\iff \forall n \in \mathbb{N} \quad [P(\sigma)((A^n))]_n = 0$$
$$\iff \forall n \in \mathbb{N} \quad \sum_{k=0}^{r} p_k A^{n+k} = 0 \qquad (*)$$

En particulier, pour $n=0$,

$$P \in \mathrm{Ann}((A^n)) \Rightarrow \sum_{k=0}^{r} p_k A^k = 0 \iff m \mid P$$

Donc m divise P. En fait, m appartient à $\mathrm{Ann}((A^n))$ car $m(A) = \sum p_k A^k = 0$ entraîne

$$\forall n \in \mathbb{N} \quad A^n \circ \left(\sum_{k=0}^{r} p_k A^k\right) = 0$$

soit : $\forall n \in \mathbb{N} \quad \sum_{k=0}^{r} p_k A^{k+n} = 0$

ce qui signifie que $m \in \mathrm{Ann}((A^n))$ en remontant les équiv. à partir de $(*)$.

Donc :

$$\begin{cases} \forall P \in \mathrm{Ann}((A^n)) & m \mid P \\ m \in \mathrm{Ann}((A^n)) \end{cases}$$

et cela implique que $\mathrm{Ann}((A^n)) = m.K[X]$, comme m est unitaire, on en déduit $m = \Pi_{(A^n)}$ (où $\Pi_{(A^n)}$ désigne le poly. minimal de la suite (A^n))

En parti. $\mathrm{Ann}((A^n)) \neq \{0\}$ donc (A^n) est une suite linéaire récurrente

$\boxed{\text{I. 6. b}}$

$\beta = (A^n V)_{n \in \mathbb{N}}$

- ~~...~~ On a :

$$\mathrm{Ann}((A^n)) \subset \mathrm{Ann}(\beta) \subset \mathrm{Ann}(u)$$

car $P \in \mathrm{Ann}((A^n)) \Leftrightarrow P(\sigma)((A^n)) = 0$ $\qquad P = \sum_{k=0}^{\wedge} p_k X^k$

$$\Leftrightarrow \forall n \sum p_k A^{n+k} = 0$$

$$\Rightarrow \forall n \sum p_k A^{n+k} V = 0 \Rightarrow P \in \mathrm{Ann}(\beta)$$

~~$\Rightarrow \forall n \sum p_k {}^t W A^{n+k} V = 0 \Rightarrow P \in \mathrm{Ann}($~~

et $\quad P \in \mathrm{Ann}(\beta) \Leftrightarrow \forall n \sum p_k A^{n+k} V = 0$

$$\Rightarrow \forall n \sum p_k {}^t W A^{n+k} V = 0$$

$$\Rightarrow P \in \mathrm{Ann}(u).$$

- Les incl ~~pr~~ démontrées et ~~...~~ sont des inclusions d'idéaux principaux, à savoir :

$$\Pi_A . K[X] \subset \Pi_\beta . K[X] \subset \Pi_u . K[X]$$

ce qui se traduit en termes de divisibilité des générateurs, par :

$$\boxed{\Pi_u \mid \Pi_\beta \text{ et } \Pi_\beta \mid \Pi_A}$$

I.6.c

$$\Pi_u \mid \Pi_\beta \mid \Pi_A \implies \deg \Pi_u \leq \deg \Pi_A$$

$$\boxed{\deg \Pi_{W,A,v} \leq \deg \Pi_A}$$

I.6.d

$\Pi_{W,A,v}(A) = 0$

$\Downarrow$ déf d'1 pol. min. d'endo.

$\Pi_A \mid \Pi_{W,A,v}$

Comme on a vu que $\Pi_{W,A,v} \mid \Pi_\beta \mid \Pi_A \mid \Pi_{W,A,v}$

$\longrightarrow$ les poly Π_A et $\Pi_{W,A,v}$ seront associés.

Il existe une cte non nulle de K tq $\Pi_{W,A,v} = c\,\Pi_A$

et. Ces pol. sont unit. donc $c = 1$

Ainsi $\Pi_{W,A,v} = \Pi_A$.

Car $\Pi_A \mid \Pi_\beta$ et $\Pi_\beta \mid \Pi_A$, on a aussi mq $\Pi_{A,v} = \Pi_A$

Ccl : $\boxed{\Pi_{W,A,v} = \Pi_{A,v} = \Pi_A}$

(1)

$\boxed{II.1.a}$

$H_m(u) = (u_{i+j-2})_{ij}$ = $\begin{pmatrix} u_0 & u_1 & u_2 & \cdots & u_m \\ u_1 & u_2 & u_3 & \cdots & u_{m+1} \\ u_2 & u_3 & u_4 & \cdots & \\ \vdots & & & & \\ u_m & & & \cdots & u_{2m} \end{pmatrix}$

$D_m(u) = \det H_m(u)$

$m = 1$ $\quad \begin{vmatrix} u_0 & u_1 \\ u_1 & u_2 \end{vmatrix} = u_2 u_0 - u_1^2$

$\quad \| $

$\begin{vmatrix} u_0 & u_1 \\ u_0+u_1 & u_1+u_2 \end{vmatrix} = \begin{vmatrix} 0 & 1 \\ 1 & 1+1 \end{vmatrix} = -1$

$u_0 = 0$

$u_1 = 1$

$u_2 = 1$

$u_3 = 2$

$m = 2$ $\quad D_2(u) = \begin{vmatrix} u_0 & u_1 & u_2 \\ u_1 & u_2 & u_3 \\ u_2 & u_3 & u_4 \end{vmatrix}$

$= \begin{vmatrix} u_0 & u_1 & u_0+u_1 \\ u_1 & u_0+u_1 & u_1+u_2 \\ u_2 & u_1+u_2 & u_2+u_3 \end{vmatrix}$

2

oui

$\boxed{\text{II.1.b}}$ $\forall n$ $u_{n+2} - u_{n+1} - u_n = 0$

$\Updownarrow$

$P(\sigma)(u) = 0$

or $P(X) = X^2 - X - 1$

$\Delta = 1 + 4 = 5$ $\qquad \dfrac{1 \pm \sqrt{5}}{2}$

Relation de la forme $\forall n$ $a u_{n+1} + b u_n = 0$?

Si oui, $\quad a u_{n+2} + b u_{n+1} = 0$

$a(u_{n+1} + u_n) + b u_{n+1} = 0$

$\begin{cases} a u_{n+1} + b u_n = 0 \\ (a+b) u_{n+1} + a u_n = 0 \end{cases}$ $\quad$ si $n = 0$ $\quad \begin{cases} a = 0 \\ a + b = 0 \end{cases}$

$\Downarrow$

$a = b = 0$

non !

$\cancel{\begin{vmatrix} a & b \\ a+b & a \end{vmatrix} = a^2 - ab - b^2}$

$\boxed{\text{II}.2}$ Par hyp $\Pi_u(\sigma)(u)=0$, i.e.

$\forall n\in\mathbb{N}$ $\quad \underbrace{u_{n+s}}_{u_m} + q_1 u_{n+s-1} + \dots + q_{s-1} u_{n+1} + q_s u_n = 0$

Si $m \geqslant s$, $H_m(u)$ possède $m+1$ colonnes et la dern. col.

$n+s=m$ $\longrightarrow$ l'écrire pour $n=0$.

$\boxed{\text{II}.3.a}$

$D_{s-1}(u)\neq 0 \Rightarrow \operatorname{rg} H_{s-1}(u) = s$

Si $m\geqslant s$, $D_m(u)=0$ donc $\operatorname{rg} H_m(u) = s$.

~~La matrice~~ ~~Le mineur~~ $H_{s-1}(u)$ est une sous-matrice carrée de $H_m(u)$, de déterminant non nul car $\det H_{s-1}(u) = D_{s-1}(u)\neq 0$. Il s'agit donc d'un mineur non nul de $H_m(u)$. On en déduit

$\operatorname{rg} H_m(u) \geqslant s$

Bon

Toutes les dernières colonnes de $H_n(u)$ après la colonne $^t(u_s, u_{s+1}, \dots)$
$(s+1)$-ième

Notons $\ell_1, \ell_2, \dots, \ell_{m+1}$ les colonnes de H_m. Ce sont des vect.-col. de $\mathbb{R}^{m+1}$

$\operatorname{rg} H_s(u)$?

$H_{s-1}(u)$ mineur non nul $\Rightarrow$ $\boxed{\operatorname{rg} H_s(u) \geq s.}$

~~Soit $H_s(u)$~~

$H_s(u) \in \mathcal{M}_{s+1}(K)$ donc $s \leq \operatorname{rg} H_s(u) \leq s+1$

Si l'on avait $\operatorname{rg} H_s(u) = s+1$, on aurait $D_s(u) \neq 0$, faux. Donc ....

$\boxed{\text{II.3.b}}$

$$H_s(u) : K^{s+1} \to K^{s+1}$$

$$\dim K^{s+1} = \dim \operatorname{Ker} H_s(u) + \underbrace{\operatorname{rg} H_s(u)}_{s}$$

$$\Downarrow$$

$$\dim \operatorname{Ker} H_s(u) = (s+1) - s = 1$$

Donc $\exists \begin{pmatrix} q_s \\ \vdots \\ q_1 \\ q_0 \end{pmatrix} \in K^{s+1}$ $\quad \operatorname{Ker} H_s(u) = K \begin{pmatrix} q_s \\ \vdots \\ q_0 \end{pmatrix} = \operatorname{Vect}\left(\begin{pmatrix} q_s \\ \vdots \\ q_0 \end{pmatrix}\right)$

~~Pos~~ $\exists \begin{pmatrix} q_s \\ \vdots \\ q_1 \\ 1 \end{pmatrix}$ existe + unique ssi $q_0 \neq 0$.

Si $q_0 = 0$, $\quad H_s(u) \begin{pmatrix} q_s \\ \vdots \\ q_1 \\ 0 \end{pmatrix} = \begin{pmatrix} \\ \\ u_s q_s + u_{s+1} q_{s-1} + \dots + u_{2s-1} q_1 \end{pmatrix}$

$$\left(\begin{array}{c|c} H_{s-1}(u) & \\ \hline & \end{array}\right) \begin{pmatrix} q_s \\ \vdots \\ q_1 \\ 0 \end{pmatrix} = \begin{pmatrix} H_{s-1}(u) \begin{pmatrix} q_s \\ \vdots \\ q_1 \end{pmatrix} \\ \hline \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \end{pmatrix}$$

car $H_{s-1}(u)$ bij. $(q_s, \dots, q_1) = (0, \dots, 0)$, ABSURDE

$\boxed{\text{II.3.c}}$

$s \leq m \leq 2s$

$H_s(u) = (u_{i+j-2})_{1\leq i,j\leq s+1}$

$$\underbrace{H_s(u)\begin{pmatrix} q_s \\ q_{s-1} \\ \vdots \\ q_1 \\ 1 \end{pmatrix}}_{\begin{pmatrix} x_1 \\ | \\ x_{s+1}\end{pmatrix}} = l\left(\sum_{j=1}^{s+1} u_{l+j-2}\, x_j\right) \quad \underbrace{\sum_{j=1}^{s+1} u_{l+j-2}\cdot q_{s-j+1} = 0}$$

$x_j = q_{s-j+1}$ $\quad \forall l \in \{1,\dots,s+1\}\ \sum_{j=1}^{s} q_{s+1-j}\, u_{l+j-2} + u_{s+j-1} =$

$q_0 = 1$

$$\begin{pmatrix} u_0 & u_1 & u_2 & \cdots & u_s \\ u_1 & u_2 & u_3 & \cdots & u_{s+1} \\ \\ u_s & u_{s+1} & \cdots & & u_{2s} \end{pmatrix}\begin{pmatrix} q_s \\ q_{s-1} \\ \vdots \\ q_1 \\ 1 \end{pmatrix}$$

$$\|$$

Si $m \in \{s,\dots,2s\}$:

$$m - \begin{pmatrix} u_0 q_s + u_1 q_{s-1} + \cdots + u_{s-1} q_1 + u_s \\ \cdots \\ u_{m-s} q_s + u_{m-s+1} q_{s-1} + \cdots + u_{m-1} q_1 + u_m \\ \cdots \\ u_s q_s + u_{s+1} q_{s-1} + \cdots + u_{2s-1} q_1 + u_{2s} \end{pmatrix} = \begin{pmatrix} 0 \\ | \\ 0 \end{pmatrix}$$

$\lambda_m = 0$

II.3.d

$$D_{s+1}(u) = \begin{array}{cccccc} c_1 & c_2 & & c_s & c_{s+1} & c_{s+2} \\ \end{array}$$
$$\begin{vmatrix} u_0 & u_1 & \cdots & u_{s-1} & u_s & u_{s+1} \\ u_1 & u_2 & \cdots & u_s & u_{s+1} & u_{s+2} \\ \vdots & & & & & \\ u_{s-1} & u_s & \cdots & u_{2s-2} & u_{2s-1} & u_{2s} \\ u_s & u_{s+1} & \cdots & u_{2s-1} & u_{2s} & u_{2s+1} \\ u_{s+1} & u_{s+2} & \cdots & u_{2s} & u_{2s+1} & u_{2s+2} \end{vmatrix}$$

colonne $c_{s+1} \leftarrow$ colonne $c_{s+1} + q_1 c_s + \cdots + q_s c_1$

$c_{s+2} \leftarrow c_{s+2} + q_1 c_{s+1} + \cdots + q_s c_2$

$\Downarrow$

~~expression~~ déterminant de l'énoncé que l'on développe suivant la $(s+1)$-ème colonne : oui

$$0 = D_{s+1}(u) = \lambda_{2s+1} \times \underbrace{D_{s-1}(u)}_{\neq 0} \Longrightarrow \boxed{\lambda_{2s+1} = 0}$$

$\boxed{\text{III.3.e}}$

On applique les mêmes soustractions de colonnes que dans la ~~question~~ réponse à la question III.3.d.

$$D_m(u) = \begin{array}{cccccccccc} c_1 & c_2 & & & c_s & c_{s+1} & & & & c_{m+1} \\ \left| \begin{matrix} u_0 & u_1 & - & - & u_{s-1} & 0 & 0 & & \text{---} & 0 \\ & & & & & & & & & \\ & & & & & & & & & \end{matrix} \right| \end{array}$$

$c_{s+1} \leftarrow c_{s+1} + q_1 c_s + \dots + q_s c_1$

$c_{s+2} \leftarrow c_{s+2} + q_1 c_{s+1} + \dots + q_s c_2$

$\dots$

$c_{m+1} \leftarrow c_{m+1} + q_1 c_m + \dots + q_s c_{m+1-s}$

ordre inverse à dire

On obtient les 0 ~~...~~ tant que les indices permettent d'appliquer la relation obtenue en II.3.c, ie tant que l_s.

Les colonnes qui suivent la colonne c_s sont alors formées des ~~o~~ coeff λ_i, qui sont nuls tant que $i \leq m+s$. Les premiers coeff qu'on voit apparaître dans la nouvelle matrice sont donc ~~...~~ les λ_{m+s}..

III, 3, f Avec la question préc., on tire $\lambda_{m+1} = 0$.

Ainsi on montre par réc. que tous les λ_i sont nuls.

Propriété : $H(k)$: $\lambda_s = \cdots = \lambda_{s+k} = 0$

III 3 d $\Rightarrow$ $H(s), H(s+1), \ldots, H(2s)$ sont vraies.

III .3. e $\Rightarrow$ si $H(m+s-1)$ vrai, alors $H(m+s)$ vrai. (ceci pour $m \geq s+1$). ~~Lhéo~~ Cela prouve l'hérédité.

Cl : $\forall m \geq s \quad \lambda_m = 0$

$$\forall m \geq s \quad u_m + q_1 u_{m-1} + \ldots + q_s u_{m-s} = 0$$

$$\forall n \in \mathbb{N} \quad u_{n+s} + q_1 u_{n+s-1} + \ldots + q_s u_n = 0$$

$m - s \leftrightarrow n$

$m = n+s$

$\Updownarrow$

$Q(X) = X^s + q_1 X^{s-1} + \ldots + q_s$

vérifie $Q(\sigma)(u) = 0$.

$\Downarrow$

$u \in S(E)$ et $\pi_u \mid Q$.

Aucun poly. P unitaire de deg $\leq s-1$ ~~et ...~~ ne peut vérifier $P(\sigma)(u) = 0$. Autrement, notons

$$P(X) = X^{s'} + q'_1 X^{s'-1} + \cdots + q'_{s'}$$

$$s' \leq s-1$$

On peut répéter l'équiv. en ⊛ et obtenir,

~~$\forall\, n \geq s$~~

$$\forall n \in \mathbb{N} \quad u_{n+s'} + q'_1 u_{n+s'-1} + \cdots + q'_{s'} u_n = 0$$

et un travail sur les colon de $H_{s'}(u)$ (comme on l'a déjà fait en II.2) montre que $D_{s'}(u) = D_{s'+1}(u) = \cdots = 0$,

~~C'est absurde car~~ ce qui implique $D_{s-1}(u) \neq 0$ ~~...~~) absurde.

(1)

III 1.a

$\boxed{\deg F = m \geq 1}$

$$\Phi : K[X] \times K[X] \longrightarrow K$$
$$(P, Q) \longmapsto \operatorname{coeff}(PQ \bmod F, m-1)$$

$\Phi(P+\lambda T, Q) = \Phi(P,Q) + \lambda\, \Phi(T,Q)$?

~~Et Qi~~ $P = FP_0 + P_1$

$T = FT_0 + T_1$ $\Rightarrow P + \lambda T = F(P_0 + \lambda T_0) + P_1 + \lambda T_1$

$Q = FQ_0 + Q_1$ $\quad (P+\lambda T)\cdot Q \equiv \underbrace{(P_1 + \lambda T_1)}_{\deg \leq m-1} \cdot \underbrace{Q_1}_{\deg \leq m-1}$ (F)

deg $\leq 2m-2$

mod F : pas

$P_1 = \sum_{i=0}^{m-1} p_i X^i$

$T_1 = \sum t_i X^i$

$Q_1 = \sum q_i X^i$

$$(P_1 + \lambda T_1) \cdot Q_1 = \left(\sum_{i=0}^{m-1} (p_i + \lambda t_i) X^i\right)\left(\sum_{j=0}^{m-1} q_j X^j\right)$$

$= \sum$

$\varphi : K[X] \to K_{m-1}[X]$

$P \mapsto P \bmod F$

~~φ est linéaire (cf. I.a.4)~~

EVIDENT en fait !

$$\Phi(P+T, Q) = \operatorname{coeff}((P+T)Q \bmod F, m-1)$$
$$= \operatorname{coeff}((PQ + TQ) \bmod F, m-1)$$
$$= \operatorname{coeff}(PQ \bmod F, m-1) + \operatorname{coeff}(TQ \bmod F, m-1)$$
$$= \Phi(P,Q) + \Phi(T,Q) \quad \text{oui.}$$

$$\Phi(\lambda P, Q) = \operatorname{coeff}((\lambda P)Q \bmod F, m-1)$$
$$= \lambda \operatorname{coeff}(PQ \bmod F, m-1) \quad \text{oui}$$
$$= \lambda\, \Phi(P, Q)$$

+ $\boxed{\text{Symétrie évidente}}$ ($PQ = QP$)

$\boxed{\text{III.1.b}}$

- $\forall Q \quad \Phi(P,Q) = 0 \implies F \mid P$

$$\Updownarrow$$

$$\forall Q \quad \text{coeff}(PQ \bmod F, m-1) = 0$$

$$\Updownarrow$$

$$\deg(PQ \bmod F) \leq m-2$$

$$\begin{cases} r \doteq \deg(P \bmod F) = \deg R < m \\ P = F P_0 + R \quad \text{où } R = P \bmod F \end{cases}$$

Mq $R = 0$?

Si $R \neq 0$, $R = a_r X^r + \dots + a_0$ où $a_r \neq 0$

$\forall Q \quad PQ \bmod F = RQ \bmod F$ — prenons $Q = X^{m-1-r}$

$$= R X^{m-1-r}$$

$$= a_r X^{m-1} + \dots$$

Par hyp $\text{coeff}(PQ \bmod F, m-1) = 0$, donc $a_r = 0$. Absurde.

Donc $R = 0$, $P = F P_0$ et $F \mid P$.

- Réciproque : Si $F \mid P$, $P = F P_0 \implies \forall Q \quad \Phi(P,Q) = \Phi(FP_0, Q) = \text{coeff}(FP_0 Q \bmod F, n)$

Comme $FP_0Q \bmod F = 0$, on a bien $\Phi(P,Q) = 0$.

La réc. est VRAIE.

- Ccl $\quad \forall Q \quad \Phi(P,Q) = 0 \iff F \mid P$

$\boxed{\text{III.1.c}}$

$$\Phi_{m-1} : K_{m-1}[X] \times K_{n-1}[X] \longrightarrow K$$
$$(P, Q) \longmapsto \text{coeff}(PQ \bmod F, m-1)$$

sera ~~[illegible]~~ non dégénérée ssi :

$$\forall Q \in K_{m-1}[X] \quad \Phi_{m-1}(P,Q) = 0 \implies P = 0 \qquad (\gamma)$$

$\Downarrow$ (≡) $\qquad\qquad\qquad \Uparrow$ car $\underset{\Phi_{m-1}}{\deg P} < \deg F = m$

$$\forall \tilde{Q} \in K[X] \quad \Phi(P, \tilde{Q}) = 0 \underset{(b)}{\implies} F \mid P$$

Donc $\boxed{\Phi_{n-1} \text{ est } \underline{\text{non}} \text{ dégénérée !}}$

$\boxed{\text{III.1.d}}$ $\quad G \in K_{m-1}[X] \qquad u_k = \Phi(X^k, G)$

i) $P \in \text{Ann}(u) \iff \forall i \quad \Phi(PG, X^i) = 0$

$\Updownarrow$ $P = p_r X^r + \dots + p_0$

$P(\sigma)(u) = 0$

$\Updownarrow$

$\forall n \quad p_r u_{n+r} + \dots + p_0 u_n = 0$

$\Updownarrow$

$\forall n \quad p_r \Phi(X^{n+r}, G) + \dots + p_0 \Phi(X^n, G) = 0$

$\Updownarrow$

$\forall n \quad \Phi(\underbrace{p_r X^{n+r} + \dots + p_0 X^n}_{= X^n P(X)}, G) = 0$

$\Updownarrow$

OUI

$\forall n \quad \Phi(PG, X^n) = 0$

$\Updownarrow$

$\forall n \quad \text{coeff}((PG)X^n \bmod F, m-1)$

$\Updownarrow$

$\forall n \quad \text{coeff}(X^n PG \bmod F, m-1) = 0$

ii) $u \in \mathcal{R}(E)$ et $\pi_u = \dfrac{F}{F \wedge G}$?

$P \in \mathrm{Ann}(u) \iff \forall i \in \mathbb{N}\ \Phi(PG, X^i) = 0$

$\Updownarrow$ bilinéarité

$\forall Q \in K[X]\ \Phi(PG, Q) = 0$

$\Updownarrow$ (a)

$\iff F \mid PG$

$\dfrac{F}{F \wedge G} \mid P \times \dfrac{G}{F \wedge G}$

$\iff$ gauss $\dfrac{F}{F \wedge G} \mid P$ OK

$\boxed{\text{II.2}}$ $E = \mathrm{Vect}\{A^k V \,/\, k \in \mathbb{N}\} \subset K^n$

$\begin{cases} \deg \pi_{A,V} = m \\ \pi_{A,V} \doteq F \end{cases}$

pol. min de $(A^k V)_k$

$\theta : K_{m-1}[X] \longrightarrow E$ isom d'ev ?

$P \longmapsto P(A)V$

* Bien défini
* linéaire : $(P + \lambda Q) \mapsto ((P+\lambda Q)(A))V = \ldots$ OK
* Injectif : $P(A)V = 0 \Rightarrow \forall k\ P(B)(A^k V) = 0 \Rightarrow P(X) \in \mathrm{Ann}((A^k V)_k)$

$\Downarrow$

$\pi_{A,V} \mid P$

$\Downarrow$ $\deg \pi_{A,V} = m$, $\deg P \leq m-1$

$P = 0$

oui

* Surjectif : Tt él de E est comb lin. des $A^k V$, donc de la forme $P(A)V$ oui.

$\boxed{\text{II}.3}$ $\quad \rho : K^n \to E^*$

$$W \mapsto \rho(W) \ / \ \rho(W) : E \to K, \quad z \mapsto {}^tWz$$

est linéaire surjective ?

$\forall z \quad \rho(W+\lambda T)(z) = {}^t(W+\lambda T)z = {}^tWz + \lambda\, {}^tTz$
$= (\rho(W) + \lambda \rho(T))(z)$

$\Downarrow$

linéari ok

Si $\ell \in E^*$, trouver $W \in K^n$ tq $\forall z \in E \quad {}^tWz = \ell(z)$.

E = sous-esp. de K^n engendré par $\{A^k V / k \in \mathbb{N}\}$. C'est donc un e v de dim finie

$\ell \in E^*$ est seulement définie sur E. Prolongeons-la en une forme linéaire $\tilde{\ell} \in (K^n)^*$ pour tout K (par ex : $K^n = E \oplus E'$ et $\tilde{\ell}|_{E'} = 0$, $\tilde{\ell}|_E = \ell$). Alors $\tilde{\ell}$:

$$\forall z \in K^n \quad \tilde{\ell}(z) = \tilde{\ell}\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = z_1 \tilde{\ell}\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \dots + z_n \tilde{\ell}\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

$$= a_1 z_1 + \dots + a_n z_n \quad (\text{où } a_i \in K)$$

$$= {}^tWz \quad \text{où } W = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

Donc à fortiori

$\forall \ell \in E^* \ \exists W \ \forall z \in E \quad \ell(z) = {}^tWz = \rho(W)(z)$

donc $\forall \ell \in E^* \ \exists W \ \ell = \rho(W)$

ie $\boxed{\rho \text{ surjective}}$ OK

II.4

La [illegible] $\Phi_{m,n}$ de Φ à $K_m[X] \times K_n[X]$ est non dégénérée (cf III.1.c) donc φ est un isom. d'ev.

. [illegible] appl. [illegible]

. [illegible]

[illegible] $\Phi_{m,n}(P, Q) = 0$ [illegible]

([illegible] non dég.)

. [illegible] de $\hat{}$ dim $m+1$

oui

II.5 a

$$\begin{array}{l} K_{m+1}[X] \xrightarrow{\varphi} K_{m+1}[X]^* \xrightarrow{t_\theta} \\ P \longmapsto \varphi(P) \\ \forall Q \quad \varphi(P)(Q) = \Phi(P, Q) \end{array}$$

Γ

$$K^n \xrightarrow[\text{lin. surj}]{\rho} E^* \xrightarrow[\sim]{t_\theta} K_{m-1}[X]^* \xrightarrow[\sim]{\varphi^{-1}} K_m[X]$$

$W \longmapsto \rho(W)$

$\forall q \quad \rho(W)(z) = {}^t W_z$

$\forall P \quad \Phi(T, P) = {}^t\rho(W)(\theta(P))$

$= \rho(W)(P(A, V))$

Γ est bien définie, c'est une appl. linéaire de K^n dans $K_m[X]$ ${}^{\shortparallel}_{t} W P(A$

et :

$$\boxed{\begin{array}{lcl} \Gamma : K^n & \longrightarrow & K_m[X] \\ W & \longmapsto & T \ / \ \forall P \in K_{m-1}[X] \quad \Phi(T, P) = {}^t W P(A \end{array}}$$

(4) pour la question qui suit !

II.5.b

$T = \Gamma(W)$ dans (Δ) à la p. 6.

Donc : $\forall P \in K_{m-1}[X] \quad \forall W \in K^n \quad \Phi(\Gamma(W), P) = {}^tW P(A) V$

II 5 c

Si $P \in K[X]$ $\quad \Phi(\Gamma(W), P) = \text{coeff}(\Gamma(W) P \bmod F, m-1)$

soit $P_0 = P \bmod F$ $\quad = \text{coeff}(\Gamma(W) P_0 \bmod F, m-1)$

$= \Phi(\Gamma(W), P_0)$

$P = FQ + P_0$ $\quad = {}^tW P_0(A) V$ d'après II.5.b

${}^tW P(A) V = \cancel{{}^tW F(A) Q(A) V} + {}^tW P_0(A) V$ $\quad = ?$ ${}^tW P(A) V$

nul ?

oui

Si $k \geq m$, $\quad \Phi(\Gamma(W), X^k) = 0$?

$\text{coeff}(\Gamma(W) . X^k \bmod F, m-1)$

$\underbrace{\in K_m[X]}_{\deg \leq m+k}$ $\quad \deg F = m$

valuation $\geq k$

$= R$ $\quad \Gamma(W) X^k = FQ + R \quad \deg R < \deg F = m$

$\underbrace{\Gamma(W) X^k}_{\text{valuation} \geq k \geq m}$ $\Rightarrow$ $R = 0$ $\quad$ oui !!

$\boxed{\text{III}.5.d}$ Soit $F = \Pi_{A,V}$

~~On prend $G = \Gamma(W)$~~ ~~pour~~ on a

On applique III.1.d avec $G = \Gamma(W)$ et $u_k = \Phi(X^k, \Gamma(W))$

d'où $u_k = \Phi(X^k, \Gamma(W)) \underset{\text{III.5.b}}{=} {}^tW.A^k.V$

donc $u = ({}^tWA^kV)_k$

D'après III.1.d :

$$\Pi_u = \Pi_{W,A,V} = \frac{F}{F \wedge G} = \frac{\Pi_{A,V}}{\Pi_{A,V} \wedge \Gamma(W)}$$

oui

$\boxed{\text{III}.5.e}$ ok Toujours.

$\boxed{\text{III } 6}$ $R \in K[X_1, \dots, X_n]$

$S \subset_{\text{fini}} K \quad S \neq \emptyset$

$\Omega_S = \{(s_1, \dots, s_n) \in S^n \,/\, R(s_1, \dots, s_n) = 0\}$

Réc sur n

• $\underline{n = 1}$; $\left.\begin{array}{l} R \in K[X] \\ K \text{ corps comm} \\ \deg R = d \in \mathbb{N} \end{array}\right\} \Rightarrow$ R possède au plus d racines dans K

$d \times |S|^{n-1} \quad (n=1)$ OK

• $\underline{\mathcal{P}(n-1) \Rightarrow \mathcal{P}(n)}$:

~~$R(X_1, \dots, X_n) = A_{d_n}(X_1, \dots, X_{n-1}) X_n^{d_n} + \dots + A_1(X_1, \dots, X_{n-1}) X_n + A_0(X_1, \dots)$~~

~~$\in \underbrace{K[X_1, \dots, X_{n-1}]}_{\text{anneau comm intègre (factoriel)}} [X_n]$~~

~~admet au plus $|S|$ racines dans S~~

~~Notons $\{\alpha_1, \dots, \alpha_k\}$ ces racines $(k \leq |S|)$~~

~~$R(s_1, \dots, s_n) = 0$~~

~~$\exists i \in \{1, \dots, k\}$ $\underbrace{R(s_1, \dots, s_{n-1}, \alpha_i) = 0}$~~

~~$\downarrow$ hyp. réc~~

~~au plus $(d|S|^{n-2}) \times |S| = d \times |S|^{n-1}$ OK~~

$R(s_1, \dots, s_{n-1}, s_n) = 0$

$|S|$ possibilités. Une fois s_n choisi, $R(X_1, \dots, X_{n-1}, s_n) = 0$

possède au plus $N = \deg R(X_1, \dots, X_{n-1}, s_n) \times |S|^{n-2}$

racines dans S^{n-1}

Au total, il y aura donc au plus : $|S| \times N = \deg_{X_1, \dots, X_{n-1}} R(X_1, \dots, X_{n-1}, s_n) \times |S|^{n-1}$

$\leq d\,|S|^{n-1}$ racines dans S.

OK

IDÉE BONNE MAIS INCOMPLÈTE. A COMPLÉTER PLUS TARD

(9)a

NB: DECOUVERTE D'UNE ERREUR A LA RELECTURE, AU MOMENT DU RETOUR SUR MON BROUILLON POUR PASSER A LA REDACTION. C'EST LÀ OÙ L'ON FAIT PARFOIS D'ABOMINABLES DECOUVERTES ...

$t \in S$ fixé

$$R(X_1, \ldots, X_n, t) \neq 0$$

S'il est nul ?

Hyp : ~~tout P~~ $\forall i \ \deg_{X_i} R \geq 1$

Sinon R est un pol. à k indét. dans $K[X_{i_1}, \ldots, X_{i_k}]$, et on appliqu- ce q- [illegible]

$|\Omega_S| \leq$

$R(X_1, \ldots, X_n)$ n'est pas nul, donc il existe une partie non vide $\{X_{i_1}, \ldots, X_{i_k}\}$ de $\{X_1, \ldots, X_n\}$

$I = \{i_1, \ldots, i_k\}$ de $\{1, \ldots, n\}$ tq

pour tout $i \in I$, X_i soit un monôme présent dans l'écriture réduite de $R(X_1, \ldots, X_n)$ sous la forme

$$R(X_1, \ldots, X_n) = \sum a_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n}$$

et pour tout $i \notin I$, X_i n'apparaisse pas dans $R(X_1, \ldots, X_n)$.

Quitte à changer l'indexation des indéterminées,

on peut donc supposer que

$$R(X_1, \ldots, X_n) = R(X_1, \ldots, X_p) \quad \text{où } p \leq n$$

et où $\deg_{X_i} R \geq 1$ pour tout $i \in \{1, \ldots, p\}$.

De 2 choses l'une :

- Si $p < n$, l'hyp. réc. s'applique à $R(X_1, \ldots, X_p)$

$$|\Omega_S| \leq \deg R(X_1, \ldots, X_p) \times |S|^{p-1}$$
$$\leq d\,|S|^{n-1}$$

- Si $p = n$,

$\boxed{\text{III } 7\, a}$

$$\Big|\overbrace{\{W=(w_1,\dots,w_n)\in S^n \;/\; \Pi_{A,V}\wedge\Gamma(W)=1\}}^{\Lambda}\Big| \geq |S|^n - m|S|^{n-1}\ ?$$

Hyp. $|S|\geq m$

$$\Updownarrow$$

$$m|S|^{n-1} \geq \underbrace{|S|^n - |\Lambda|}_{=|\overline{\Lambda}|} \quad \text{où } \overline{\Lambda} = S^n\setminus\Lambda = \{W=(w_1,\dots,w_n)\in S^n / \Pi_{A,V}\wedge\Gamma(W)=0\}$$

Il faut

Majorer le nbre de n-uplets $W=(w_1,\dots,w_n)$ dans S^n tq

$\Pi_{A,V}\wedge\Gamma(W)\neq 1$, ie tq $\underline{\mathrm{Res}(\Pi_{A,V},\Gamma(W))=0}$.

A, V donnés

$\deg \Pi_{A,V} = m$

$\Pi_{A,V}$ unitaire

~~Polynôme à variables de degré~~ m

$\deg\Gamma(W)\leq m-1$

lui

Poly. fixé, $\deg\Pi_{A,V}=m$

$\overset{m-1}{\longleftrightarrow}$ $\overset{m}{\longleftrightarrow}$

a_0 b_0

a_0 b_{m-1} b_0

b_{m-1}

m variables

Variables $b_0,\dots,b_{m-1}$ $\longrightarrow$ mais les b_i sont des fcts linéaires des $(w_1,\dots,w_n)$.

$a_0\neq 0$

$a_0=1$

(car $\Pi_{A,V}$ unitaire)

~~Res = poly. de $K_{m-1}[X]$ des coeff. $b_0,\dots,b_{m-1}$~~

~~Γ(W)~~

~~W donné Γ(W) fixé.~~

~~Res (Π_{A,V}, Γ(W))~~

~~poly. en X de degré m~~

~~Poly en $b_0,\dots,b_{m-1}$~~

~~m variables~~

~~$W \xrightarrow{\Gamma} \Gamma(W) \in K_{m-1}[X]$~~ ~~identifié~~ ~~$\Gamma(W) = \sum_{i=0}^{m-1} b_i X^i \in K_{m-1}[X]$~~

~~$\Uparrow$~~

~~S~~

~~Toujours donc $|\{\Gamma(W) / W\in S\}|\leq|S|$.~~ (2)

$\cancel{\mathcal{S} = \{\Gamma(W) / W \in S\}}$

$\mathcal{S} = \left\{ (b_0, \dots, b_{m-1}) \,/\, \exists W \in S \quad \Gamma(W) = \sum_{i=0}^{m-1} b_i X^i \right\}$

D'après ⊛ :

$|\mathcal{S}| \leq |S|$

$R \doteq \mathrm{Res}(\Pi_{A,V}, \Gamma(W))$ = polynôme de degré total m en $(b_0, \dots, b_{m-1})$. Il y a donc m indéterminées.

On applique III.6 :

Si $\Omega_{\mathcal{S}} = \{ (b_0, \dots, b_{m-1}) \in \mathcal{S} \,/\, R(b_0, \dots, b_{m-1}) = 0 \}$

alors $|\Omega_{\mathcal{S}}| \leq \deg R \times |\mathcal{S}|^{m-1}$

$\leq m\, |\mathcal{S}|^{m-1}$

$\leq m\, |S|^{m-1}$

$\Gamma : K^n \longrightarrow K_{m-1}[X]$

$W = (w_1, \dots, w_n) \mapsto \Gamma(W)$ linéaire, donc :

$\Gamma : K^n \longrightarrow K$

$W = (w_1, \dots, w_n) \longmapsto R = \mathrm{Res}(\Pi_{A,V}, \Gamma(W))$

est polynômiale *(par composition !) en $w_1, \dots, w_n$ de degré m. On la note $R(w_1, \dots, w_n)$.

~~donc~~

$\Omega_S = \{ W = (w_1, \dots, w_n) \in S^n \,/\, R(w_1, \dots, w_n) = 0 \}$

$\overset{\text{III.6}}{\Rightarrow} |\Omega_S| \leq m\, |S|^{n-1}$

(12)

$\boxed{\text{III } 7b}$ $W \in S^n$ $|S|^n$ choix possibles

Alors $\pi_{W,A,V} = \pi_{A,V}$ ssi $\pi_{A,V} \wedge \Gamma(W)$, donc ssi on tombe sur un n-uplet W appartenant à l'ensemble Λ introduit en III 7a. On a :

$$|W| \geq |S^n| - m|S|^{n-1}$$

Donc $\boxed{\text{prob}(\pi_{W,A,V} = \pi_{A,V}) \geq \dfrac{|S|^n - m|S|^{n-1}}{|S|^n} = 1 - \dfrac{m}{|S|}}$

$\boxed{\text{PARTIE IV}}$

$\boxed{\text{IV.1.a}}$

$\forall i \in [0, \ell+1]$ $S_iA + T_iB = R_i$?

Réc. sur i.

$i=0$: $1.A + 0.B = R_0 = A$

$i=1$: $0A + 1.B = R_1 = B$

$i \Rightarrow i+1$: $S_{i+1}A + T_{i+1}B = (S_{i-1} - Q_iS_i)A + (T_{i-1} - Q_iT_i)B$

$= S_{i-1}A + T_{i-1}B - Q_i(S_iA + T_iB)$

$= R_{i-1} - Q_iR_i$

$= R_{i+1}$ oui

$\boxed{\text{IV.1.b}}$ $\forall i \in [0, \ell)$ $\boxed{S_{i+1}T_i - S_iT_{i+1} \overset{?}{=} (-1)^{i+1}}$ $\Rightarrow$ $\boxed{S_i \wedge T_i = 1}$

Réc.

$i=0$ $S_1 . 0 - \underbrace{S_0}_{=1} 1 = (-1)^1$ oui

$i=1$ ok

$i-1 \Rightarrow i$:

$S_{i+1}T_{i} - S_{i}T_{i+1} =$

$(S_{i-1} - Q_i\cancel{S_i})T_i - S_i(T_{i-1} - Q_i\cancel{T_i})$

$S_{i-1}T_i - S_iT_{i-1} \underset{HR}{=} -(-1)^i = (-1)^{i+1}$ oui

$\boxed{\text{IV.1.c}}$ $\boxed{\forall i \in [0, l+1] \quad R_i \wedge T_i = A \wedge T_i}$

Vu $\overset{(a)}{(*)} \Rightarrow S_i A + T_i B = R_i$

Si $P | R_i$ et $P | T_i$, alors $P | S_i A$, mais (b) $S_i \wedge T_i = 1$,
donc ~~(gauss)~~ ~~et~~ a fortiori $S_i \wedge P = 1$, donc (gauss) $P | A$.

Ainsi $(P | R_i$ et $P | T_i) \Rightarrow (P | A$ et $P | T_i)$.

Réc. vraie (m̂ chose). Donc ($\Leftrightarrow$) donc OK

$\boxed{\text{IV.1.d}}$

- $\underset{0}{\underset{\shortparallel}{\deg T_1}} \leq \underset{\text{OK}}{\underset{\shortparallel}{\deg T_2}}$ $\quad$ $T_2 = T_0 - Q_1 T_1 = -Q_1$ $\quad$ $Q_1 \neq 0$ donc $\deg Q_1 \geq 0$.

$l \geq i \geq 2$
- $\deg T_i < \deg T_{i+1}$?

① ~~A montrer en premier~~

par récurrence : $\deg T_i \leq \deg T_{i+1}$

$T_{i+1} = T_{i-1} - Q_i T_i \quad (i \geq 2)$

$\deg T_{i-1}$ $\leq$ $\deg T_i$ Plus ②

$\deg Q_i \geq 1$ si sinon $Q_i = $ cte

~~$R_{i-1} = Q_i R_i + R_{i+1}$~~

~~$\deg R_{i-1} \leq \deg R_i$~~

~~$\deg (R_{i-1} - Q_i R_i)$~~

~~$\deg R_{i+1} \leq \deg$~~

~~le plus~~ le monôme impose dominant,
alors $\deg T_{i+1} > \deg T_i$

oui

$i \geq 2 \quad R_{i-1} = Q_i R_i + R_{i+1}$

Si $\deg Q_i = 0$, alors $\deg (R_{i-1}) \leq \operatorname{Max}(\deg R_i, \underbrace{\deg R_{i+1}}_{< \deg R_i}) = \deg R_i$

Mais $\deg R_i < \deg R_{i-1}$ (dès que ~~R_i~~ $i \geq 2$)

$\boxed{IV.1.e}$

$\forall i \in [1, \ell+1] \quad \deg T_i = \overset{\deg A}{\overset{\shortparallel}{m}} - \deg R_{i-1}$

$\deg T_1 < \deg T_2$

$\forall i \geq 2 \quad \deg T_i < \deg T_{i+1}$

Vrai si $i=1$
$$\left\{\begin{array}{l} \deg T_1 = m - \underbrace{\deg R_0}_{\overset{\shortparallel}{\deg A}} = 0 \\ T_1 = 1 \end{array}\right.$$

$i=2$ vrai

$\deg T_2 \overset{?}{=} m - \deg R_1 \iff \deg Q_1 = m - \deg R_1$

$= \deg A - \deg R_1$ OK

$T_2 = \underbrace{T_0}_{0} - Q_1 \underbrace{T_1}_{1} = -Q_1$

$\Uparrow \deg A = \deg Q_1 + \deg R_1$

$\Uparrow$

$(i=1) \quad A = Q_1 R_1 + R_2$

$\deg R_{i+1} < \deg R_i$

Si vrai jusqu'à i, en $i+1$?

$\underbrace{T_{i+1} = T_{i-1} - Q_i T_i}$

$$\left\{\begin{array}{l} \deg T_{i-1} = m - \deg R_{i-2} \\ \wedge \\ \deg T_i = m - \deg R_{i-1} \end{array}\right.$$

$\deg R_{i-1} < \deg R_{i-2}$

$\deg T_{i+1} = \deg(Q_i T_i)$

$= \deg Q_i + \deg T_i$

$= \deg Q_i + m - \deg R_{i-1}$

$= m - \underbrace{(\deg R_{i-1} - \deg Q_i)}_{\overset{\shortparallel}{\deg R_i}}$ car oui

$\Leftarrow \left\{\begin{array}{l} R_{i-1} = Q_i R_i + R_{i+1} \\ \deg R_{i+1} < \deg R_i \end{array}\right.$

IV.2.a

4

* $\deg A = m$ $\quad m \geq n \geq 1$
$\deg B = n$

$j \ / \ \deg R_j < k \leq \deg R_{j-1}$

(R_j, T_j) solution de (P_2) car :

- $\boxed{T_j B \equiv R_j \bmod A}$ $\Leftarrow S_j A + T_j B = R_j$ (IV.1.a)
- $\boxed{\deg R_j < k}$ $\quad \deg R_j < \dots < \deg R_2 < \deg R_1 = \deg B \leq \deg R_0 = \deg A$
- $\boxed{\deg T_j \leq m - k}$

$\deg T_j = m - \deg R_{j-1} \leq m - k$ ouais (IV.1.e)

---

* Solution de (P_1) ?? A condition d'avoir $T_j \wedge A = 1$, i.e. $\boxed{R_j \wedge T_j = 1}$ (cf IV.1.c)

IV.2.b $\quad (R, T)$ sol. de (P_1)

$\Downarrow$

$R_j \wedge T_j = 1$?

$\exists R, T$ $\begin{cases} TB \equiv R \bmod A \\ T \wedge A = 1 \\ \deg R < k \\ \deg T \leq m - k \end{cases}$

$\deg T \leq m-k$, $\deg B = n \leq m$, $\deg R < k < m$, $\deg A = m$

$W \in K[X]$ $\begin{cases} W \mid R_j \\ W \mid T_j \end{cases} \xRightarrow{(a) : S_j A + T_j B = R_j} W \mid S_j A \Longrightarrow W \mid A \Longrightarrow W \mid A \quad (1)$

(b) $S_j \wedge T_j = 1$ donc $S_j \wedge W = 1$

(IV.1.c car $R_j \wedge T_j = A \wedge T_j$)

IV.2 (a) $\Rightarrow$ (R_j, T_j) est solution de (P_2), i.e. $\begin{cases} T_j B = R_j \bmod A \\ \deg R_j < k \\ \deg T_j \leq m - k \end{cases}$

⑤

~~Donc~~

$\cancel{TB \equiv R \equiv T_j B \mod A}$

$\cancel{(T - T_j) B \equiv 0 \mod A}$

~~Comme $W | T_j$ et $W | A$, on en déduit que $W \nmid TB$~~

$\deg A = m$

$R_j T - R T_j$

$$\left.\begin{array}{l} TB \equiv R \Rightarrow R_j T B \equiv R_j R \\ T_j B \equiv R_j \Rightarrow R T_j B \equiv R R_j \end{array}\right\} \Rightarrow (R_j T - R T_j) B \equiv \mod A$$

$\deg < k$, $\deg \leq a-k$, $< k$, $\leq m$

$R_j \equiv T_j B \quad (A)$

$\deg < k$

$S_j T - T S_j$

$\deg(R_j T - R T_j) < k = \deg A$

- Si l'on a montré que $\exists P \quad R = PR_j$ et $T = PT_j$, alors on peut prouver que $R_j \wedge T_j = 1$ ainsi :

$$\left.\begin{array}{l} W | R_j \\ W | T_j \end{array}\right\} \underset{\text{IV.1.c}}{\Longrightarrow} \left.\begin{array}{l} W | A \\ W | T_j \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} W | A \\ W | T \end{array}\right. \Longrightarrow W = 1 \text{ car } T \wedge A = 1$$

car $T = PT_j \Rightarrow W | T$

- <u>Facile</u> : Si l'on sait que $R = PR_j$ et $T = PT_j$, alors $P \wedge A = 1$. En effet :

$$\left.\begin{array}{l} W | P \\ W | A \end{array}\right\} \Rightarrow \left\{\begin{array}{l} W | T \\ W | A \end{array}\right. \Rightarrow W = 1 \text{ car } T \wedge A = 1.$$

(5 bis) $R_j T - R T_j \equiv T_j B T - T B T_j \equiv 0 \quad (A)$

$\Downarrow$

$\cancel{T_j T = 1}$

$R_j T = R T_j$

$R_j \mid R T_j$

$R_j \wedge T_j = 1$ non

$\Downarrow$

$\underbrace{R_j T - R T_j}_{\deg < k} = 0 \quad \underbrace{(A)}_{\deg A = n}$

$\Downarrow$

$R_j T - R T_j = 0$

$\Downarrow$

donc $\boxed{R_j T = R T_j}$

$\cancel{S_j T - T S_j = 0} \longrightarrow$ ~~erreur dans l'énoncé~~ ?

$\cancel{S_j T - S T_j}$?

$\deg S_j \underset{(e)}{=} n - \deg R_{j-1} \underset{(e)}{=} n - (m - \deg T_j) = n - m + \deg T_j \leq n - m + (m - k$

$\leq n - k$

$\deg T \leq m - k$

* | Il manque la preuve de $R_j \wedge T_j = 1$.

voir page (6) b

Solution trouvée par Freddy Dirkmand ~~⑥~~ ⑥ bis

$\forall i$ $\qquad \exists Q \,/\, TB = R + AQ$

$$\left.\begin{array}{l} A \mid R_i T - R T_i \\ \deg(R_j T - R T_j) < \deg A \end{array}\right\} \Longrightarrow R_j T = R T_j$$

$$\Downarrow$$

$$(S_j A + T_j B) T = \cancel{RT_j}\ (TB + AQ)$$

$$\cancel{S_j A T = T_j}$$

$$\Downarrow$$

$$S_j A T + \cancel{T_j B T} = \cancel{T B T_j} + A Q T_j$$

$$S_j A T = A Q T_j$$

$$\boxed{S_j T = Q T_j}$$

$$\Downarrow$$

$$\left.\begin{array}{l} T_j \mid S_j T \\ T_j \wedge S_j = 1 \end{array}\right\} \Longrightarrow T_j \mid T \qquad T \wedge A = 1$$

$$\Downarrow$$

$$T_j \wedge A = 1$$

// IV.1.c

oui $\qquad \boxed{R_j \wedge T_j = 1}$

$\boxed{\text{IV}.3}$ $\quad B_r = \sum_{k=0}^{2r-1} u_k X^k \qquad u \in S(K)$

$\exists H = \sum_{k=0}^{s} q_k X^k$

$\exists R$

$$\begin{cases} q_0 = 1 \ ; \ \deg R < s \\ \forall r \geq s \quad \underbrace{HB_r}_{} \equiv R \mod X^{2r} \end{cases}$$

$\Downarrow \qquad \deg HB = \deg H + \deg B \leq s + 2r - 1$

$$\begin{cases} u \text{ linéaire récurrente} \\ \text{et } \sum_{k=0}^{s} q_{s-k} X^k \in \mathrm{Ann}(u) \end{cases}$$

$$HB_r = \left(\sum_{k=0}^{s} q_k X^k\right)\left(\sum_{k'=0}^{2r-1} u_{k'} X^{k'}\right)$$

$$= \sum_{t=0}^{2r+s-1} \Big(\underbrace{\sum_{k+k'=t} q_k u_{k'}}_{\sum_{k=0}^{t} q_k u_{t-k}}\Big) X^t$$

$$= \sum_{t=0}^{2r+s-1} \Big(\underbrace{\sum_{k=0}^{t} q_k u_{t-k}}_{q_0 u_t + q_1 u_{t-1} + \dots + q_t u_0}\Big) X^t$$

$$\underbrace{\forall r \geq s}_{} \quad \underbrace{\sum_{t=0}^{2r-1} \left(\sum_{k=0}^{t} q_k u_{t-k}\right) X^t}_{} \equiv \underbrace{R}_{\deg R < s} \quad (X^{2r})$$

$\Downarrow \qquad \deg < 2r \text{ donc égaux}$

$s < r < 2r$

si $r \geq 1$

$\Downarrow$

$$\forall r \geq s \quad \sum_{t=0}^{2r-1} \left(\sum_{k=0}^{t} q_k u_{r-k}\right) X^t = \underbrace{R}_{\deg R < s} \Rightarrow \boxed{\forall r \geq s \ \forall t \in \{s, \dots, 2r-1\} \ \sum_{k=0}^{t} q_k u_{t-k} = 0} \quad (\Delta)$$

~~$\forall r \geq s \ \dots q_{2r-1} \dots q_{2r-2} \dots q_{2r-1} u_0 = 0$~~

~~$\forall r \leq s$~~

~~$\text{Id } B_r = \left(\sum_{k=0}^{2r-1} q_k X^k\right)\left(\sum_{k'=0}^{2r-1} u_{k'} X^{k'}\right)$~~

A montrer :

$$\forall n \quad q_0 u_{n+s} + q_1 u_{n+s-1} + \dots + q_s u_n = 0$$

(Δ) $\Leftrightarrow \forall r \geq s \quad \forall t \in \{s, \dots, 2r-1\}$

$$\sum_{k=0}^{t} q_k u_{t-k} = 0$$

$$\underset{1}{\overset{\shortparallel}{q_0}} u_t + q_1 u_{t-1} + \dots + q_t u_0 = 0$$

$t = s+1$

$t = s$

$$\boxed{q_0 u_s + q_1 u_{s-1} + \dots + q_s u_0 = 0} \longrightarrow \text{BIEN}$$

prouvé si $n = 0$!!

$$\boxed{q_0 u_{s+1} + q_1 u_s + \dots + q_s u_1} + \underbrace{q_{s+1} u_0}_{} = 0$$

n'est ~~nullement pas nul~~ !

~~$\leq$ ... Bien !~~

0 car $q_{s+1} = 0$

(puisque ~~des~~ $t \leq s$

BIEN

prouvé si $n = 1$!!

etc

jusqu'à $t = 2r - 1$

jusqu'à $t = 2r - 2$

$$q_0 u_{\underset{n+s}{2r-2}} + q_1 u_{2r-3} + \dots + q_s u_{2r-2-s} = 0$$

$$q_0 u_{2r-1} + q_1 u_{2r-2} + \dots + q_s u_{2r-1-s} = 0$$

$n+s$ ~~n +~~

$\overset{\shortparallel}{n}$

n

$\exists r \geq s \quad n = 2r - 2 - s$

$2r = n + 2 + s$

si $n + 2 + s$ pair

~~$\forall n$~~ $n = 2r - 1 - s$

$\forall n \ \exists r \geq s$ ~~[...]~~ $\longrightarrow 2r = n + 1 + s$) OK si $n + 1 + s$ pair

OK

Dans les 2 cas, on conclut.

9

$\boxed{\text{IV. 4. a(i)}}$ $\left(\begin{array}{l} \forall n \\ q_0 u_{n+s} + q_1 u_{n+s-1} + \dots + q_s u_n = 0 \end{array} \right.$

$\exists R \quad \deg R < s$

$\forall n \geq s \quad Q^* B_n \equiv R \mod X^{2n}$ où $Q^*(X) = X^s Q\left(\frac{1}{X}\right) = \sum_{k=0}^{s} q_k X^k$

$A = X^{2n}$

$$Q^* B_n = \left(\sum_{k=0}^{s} q_k X^k\right)\left(\sum_{k=0}^{2n-1} u_k X^k\right)$$

$$= \sum_{t=0}^{2n+s-1} \left(\sum_{k=0}^{t} q_k u_{t-k}\right) X^t$$

$$\equiv \sum_{t=0}^{2n-1} \left(\sum_{k=0}^{t} q_k u_{t-k}\right) X^t$$

$\forall n \geq s$

$\Downarrow$

$s \leq n \leq 2n-1$

$$\equiv \sum_{t=0}^{s} \underbrace{\left(\sum_{k=0}^{t} q_k u_{t-k}\right)}_{\text{ne dépend que de } u \text{ fixé et de } Q \text{ fixé.}} X^t$$

Si $t = s \quad \underbrace{q_0 u_s + \dots + q_s u_0 = 0}$

donc

poly. de degré $< s$.

$$\equiv \underbrace{\sum_{t=0}^{s-1} \left(\sum_{k=0}^{t} q_k u_{t-k}\right) X^t}_{\doteq R} \quad \Rightarrow \deg R \leq s-1$$

IV 4 a ii)

$$Q=\Pi_u \Rightarrow \begin{cases} s = \mathrm{Max}\,(1+\deg R, \deg Q^*) \\ Q^* \wedge R = 1 \end{cases}$$

$Q=\Pi_u$ Coeff. dominant de R : $\left(\underbrace{\sum_{k=0}^{s-1} q_k\, u_{s-1-k}}\right) X^{s-1}$

$$q_0 u_{s-1} + q_1 u_{s-1-1} + \dots + q_{s-1} u_0$$

$\forall Q \in \mathrm{Ann}(u) \qquad Q^* B_n \equiv R \mod X^{2n}$

$$Q^* \wedge R \neq 1 \Rightarrow \begin{cases} Q^* = W Q_0^* \\ R = W R_0 \end{cases}$$

$$W Q_0^* B_n \equiv W R_0 \mod X^{2n}$$

DEBUT

---

* 2 cas

- Si $q_s \neq 0$, $\deg Q^* = s$

  $s \leq \mathrm{Max}(1+\deg R, \deg Q^*)$ donc $s = \mathrm{Max}(1+\deg R, \deg Q^*)$

  $\deg R \leq s-1 \Rightarrow 1+\deg R \leq s$

- Si $q_s = 0$, $Q = q_0 X^s + \dots + q_{s-1} X \in \mathrm{Ann}(u)$

  ie

  $\forall n \qquad q_0 u_{n+s} + \dots + q_{s-1} u_{n+1} = 0$

  $\Downarrow$

  $q_0 X^{s-1} + \dots + q_{s-1} X \in \mathrm{Ann}\, u$ impossible car de deg

(11)

$\forall n \in \mathbb{N} \quad q_0 u_{n+s} + \cdots + q_{s-1} u_{n+1} + q_s u_n = 0$

Si $q_s = 0$,

$\forall n \in \mathbb{N} \quad q_0 u_{n+s} + \cdots + q_{s-1} \underbrace{u_{n+1}}_{m} = 0$

$\Downarrow$

$\forall m \in \mathbb{N}^* \quad q_0 u_{m+s-1} + \cdots + q_{s-1} u_m = 0$

$\Downarrow$

$q_0 X^{s-1} + \cdots + q_{s-1} \in \mathrm{Ann}\left((u_n)_{n \in \mathbb{N}^*}\right) \quad (1)$

Mais a fortiori ~~Π_u~~ ~~B~~ :

Π_u engendre l'idéal $\mathrm{Ann}\left((u_n)_{n\in\mathbb{N}}\right)$

$\Downarrow$

Π_u ~~engendre~~ $\underset{\text{seulement}}{\in}$ $\mathrm{Ann}\left((u_n)_{n\in\mathbb{N}^*}\right) \quad (2)$

(1) et (2)

$\Downarrow$

$q_0 X^{s-1} + \cdots + q_{s-1}$ et Π_u sont divisible par un m polynôm,

- le poly. Π_u annulateu de $(u)_{n\in\mathbb{N}^*}$

~~do Π~~

~~(1) et (2) $\Rightarrow \Pi_u \mid q_0 X^{s-1} + \cdots + q_{s-1}$~~

~~absurde car $\boxed{\deg \Pi_u = s}$~~

~~Donc $q_s \neq 0$, et on est très dans le 1er cas.~~

~~NB $\to$ On a donc toujours $Q = \Pi_u \Rightarrow$ $\overset{\Rightarrow q_s \neq 0}{\boxed{\deg Q^* = s}}$~~

* $Q^* \wedge R = 1$?

$\cancel{Q^* B_r \equiv R \mod X^{2r}}$

$\cancel{\deg R < s \leq r \leq 2r}$ $\cancel{(r \geq 0)}$

$\cancel{\deg = \deg Q^* + \deg B_r}$

$\cancel{s + 2r - 1 \leq 3r - 1}$ bouh!

$\leq 1 + \deg R$

$Q^*(0) = q_0 = 1$

$\Downarrow$

$\cancel{Q^* B_r = R + W X^{2r}}$

$X \not| Q^*$

$\Downarrow$

Si $\begin{cases} Q^* = W\tilde{Q}^* \\ R = W\tilde{R} \end{cases}$ $\quad X \not| W \Rightarrow X \wedge W = 1 \Rightarrow X^{2r} \wedge W = 1$

$Q^* B_r \equiv R \mod X^{2r} \Rightarrow W \tilde{Q}^*_{B_r} \equiv W\tilde{R} \mod X^{2r}$

$\Downarrow$

$\begin{cases} X^{2r} \mid W(\tilde{Q}^*_{B_r} - \tilde{R}) \\ X^{2r} \wedge W = 1 \end{cases}$

$\Downarrow$ gauss

$X^{2r} \mid \tilde{Q}^*_{B_r} - \tilde{R}$

$\Downarrow$

$\forall r \geq s \quad \tilde{Q}^* B_r \equiv \tilde{R} \mod X^{2r}$

plus haut degré possible $\deg \tilde{Q}^* \leq \deg Q^* \leq s$ OK

$\Downarrow$ IV.3

$(\tilde{Q}^*)^* = \tilde{Q} \in Ann(u)$

Mais $\tilde{Q} \mid Q = \Pi_u$ $\longrightarrow$ donc ABSURDE, sauf si $\deg \tilde{Q} = \deg Q$

Les seuls div. de Q^* et R sont donc les constantes $W = cte$.
et donc $Q^* \wedge R = 1$.

$\boxed{\text{IV}.4.b.i}$

$A = X^{2r}$

$B = B_r = \sum_{k=0}^{2r-1} u_k X^k \quad r \geq s$

$k = r$; $j \in \{1, .., l+1\}$ / $\deg R_j < k = r \leq \deg R_{j-1}$

On applique IV.2 (a) et (b).

D'après IV.2.(a), (R_j, T_j) est sol. de $(\mathcal{P}_2)$ donc

$$\begin{cases} T_j B_r \equiv R_j \mod X^{2r} \\ \deg R_j < k = r \\ \deg T_j \leq m - k = 2r - r = r \end{cases}$$

On a vu au IV.4.a qu'il existait (R, Q^*) solution du problème $(\mathcal{P}_1)$, autrement dit que :

prendre $Q = \Pi_u$ pour pouvoir utiliser (IV.4.a.ii)

$$\begin{cases} Q^* B_r \equiv R \mod X^{2r} \\ \deg R < s \leq r = k \\ \deg Q^* \leq s \leq m - k = 2r - r = r \quad (\text{OK}) \end{cases}$$

et que choisir $Q = \Pi_u$ nous permet même d'avoir $\deg Q^* = s$ (cf question préc.) et $Q^* \wedge R = 1$

On a aussi ici $\boxed{Q^* \wedge A = Q^* \wedge X^{2r} = 1}$ car $X \nmid Q^*$.

pas encore obligé !

On applique IV.2.(b) : Comme (R, Q^*) est une solution de $(\mathcal{P}_1)$, on aura :

$\boxed{\text{IV}.b.(i)}$ aussi

$$\begin{cases} R_j \wedge T_j = T_j \wedge A = T_j \wedge X^{2r} = 1 \\ \exists P \in K[X] \setminus \{0\} \quad R = P R_j \text{ et } Q^* = P T_j \end{cases}$$

On applique le i) avec $Q = \Pi_u$. Alors :

$\exists P \quad R = P R_j$ et $Q^* = P T_j$

Π_u^*

De plus $P | Q^*$ et $Q^*(0) \neq 0$ donc $\boxed{P \wedge X^{2r} = 1}$

$\boxed{\text{IV. 4 b ii}}$

$\Pi_u^*(0) = Q^*(0) \neq 0$ donc le terme constant de $\Pi_u^* = P T_j$ n'est pas nul. Il en est de m̂ du terme constant de T_j. On peut donc multiplier T_j par un él. non nul de K pour avoir $T_j(0) = 1$, ce qu'on supposera par la suite.

$$(\text{IV 4 a ii}) \Rightarrow s = \mathrm{Max}(1 + \deg R_{j-1}, \deg Q^*)$$

P est une constante ?

$$\deg T_j \leq r \quad \cancel{\leq \deg R_{j-1}}$$

$$\cancel{= \ldots - \deg R_{j-1} \ \ldots \ \deg R_j}$$

$$\deg \Pi_u^* = \deg Q^* = s \ (\text{cf IV. a. ii}) \leq r$$

$$\underbrace{\Pi_u^*}_{\deg = s \leq r} = P \underbrace{T_j}_{\deg T_j \leq r}$$

$$\underbrace{R}_{\deg < s \leq r} = P \underbrace{R_j}_{\deg < r}$$

A1

$\boxed{\text{IV 4 a ii}}$ Retour sur le problème

Si $Q = \Pi_u$,

$$\underbrace{Q^* B_r}_{} \equiv \underbrace{R}_{} \bmod X^{2r}$$

$\deg R < s \leq r < 2r$

$$\deg Q^* B_r = \underbrace{\deg Q^*}_{\leq s} + \underbrace{\deg B_r}_{?}$$

$Q = \Pi_u \Rightarrow s$ est le plus petit degré possible d'1 polyn. Q $\left(\sum_{k=0}^{s} q_k X^k\right)$

qui est dans $\mathrm{Ann}(u) \setminus \{0\}$.

$s \overset{?}{=} \mathrm{Max}(1 + \deg R, \deg Q^*) \Leftrightarrow \begin{cases} \text{Si } 1 + \deg R < \deg Q^*, & s = \deg Q^* \ \boxed{1} \\ \text{Si } \deg Q^* < 1 + \deg R, & s = 1 + \deg R \ \boxed{2} \end{cases}$

- **Cas $\boxed{1}$** : Si $1 + \underbrace{\deg R}_{< s \leq r} < \underbrace{\deg Q^*}_{\leq s}$