COURS DE L'INSTITUT FOURIER

MONIQUE LEJEUNE-JALABERT

Chapitre 0 Rappels et préliminaires

Cours de l'institut Fourier, tome 19 (1984-1985), p. 19-31

<http://www.numdam.org/item?id=CIF_1984-1985__19__19_0>

Chapitre 0

RAPPELS ET PRÉLIMINAIRES

Un système d'équations algébriques est la donnée d'un nombre fini de polynômes $f_1, \ldots, f_s$ en un nombre fini de variables $X_1, \ldots, X_n$ à coefficients dans un corps k. Si k' est une extension de k, on dit que $x = (x_1, \ldots, x_n) \in k'^n$ est une solution ou une racine dans k' du système $f_1, \ldots, f_s$ si $f_i(x_1, \ldots, x_n) = 0$, $i = 1 \ldots s$.

$$I = \{f \in k[X_1, \ldots, X_n] : \exists h_i \in k[X_1, \ldots, X_n],\ i = 1 \ldots s,\ f = \sum_{i=1 \ldots s} h_i f_i\}$$

est le plus petit idéal de $k[X_1, \ldots, X_n]$ contenant $f_1, \ldots, f_s$. On dit que $f_1, \ldots, f_s$ est un système de générateurs de I et on note $I = (f_1, \ldots, f_s)$.

Nous considérons comme équivalents 2 systèmes $f_1, \ldots, f_s$; $g_1, \ldots, g_t$ tels que $(f_1, \ldots, f_s) = (g_1, \ldots, g_t)$. Si x est une solution de $f_1, \ldots, f_s$, x est une solution de tout $f \in (f_1, \ldots, f_s)$. 2 systèmes équivalents ont donc le même ensemble de solutions.

Etant donné un système d'équations algébriques, nous allons décrire des procédés pour obtenir d'autres systèmes équivalents au sens précédent sur lequel des informations par exemple sur l'ensemble des solutions (existence, dimension, etc.) mais aussi sur la structure algébrique de l'idéal engendré seront immédiatement lisibles.

A titre d'illustration, nous allons d'abord développer deux cas particuliers élémentaires et bien connus, les systèmes d'équations algébriques à 1 variable, les systèmes linéaires.

1. Le cas $n = 1$

Nous allons d'abord examiner la structure des idéaux de $k[X]$.

1.1. PROPOSITION. — *Tout idéal de $k[X]$ est principal.*

Démonstration. — Soit I l'idéal. Si $I = (0)$, c'est vrai. Si $I \neq (0)$, soit $d = \inf\{\deg f\ ,\ f \in I - \{0\}\}$. Si $d = 0$, il existe $\lambda \in k - \{0\}$, $\lambda \in I$. L'idéal engendré par λ est $k[X_1, \ldots, X_n]$. A fortiori $I = k[X_1, \ldots, X_n]$. 1 est aussi un générateur de I.

Si $d \neq 0$, soit $g \in I$ de degré d. Montrons que $I = (g)$. Soit $f \in I$, $f \neq 0$, $\deg f \geq d$. Effectuons la division euclidienne de f par g. Il existe $h \in k[X]$ et $r \in k[X]$ tels que

$$f = hg + r$$

et ou bien $r = 0$ ou bien $\deg r < d$.

Par définition, $r \in I$. Si $r \neq 0$, $\deg r \geq d$. Par suite, $r = 0$ et $f = hg \in (g)$. On a donc $(g) \subset I \subset (g)$ et $I = (g)$.

1.2. REMARQUE. — Tout système d'équations algébriques $f_1, \ldots, f_s$, à 1 variable est équivalent à un système contenant 1 seule équation f. f est le plus grand commun diviseur $(PGCD)$ de $f_1, \ldots, f_s$.

1.3. REMARQUE. — Pour que le système $f_1, \ldots, f_s$ n'ait aucune solution dans $\overline{k}$ une clôture algébrique de k , il faut et il suffit que $1 \in (f_1, \ldots, f_s)$.

Etant donné $f_1, \ldots, f_s$ un système d'équations algébriques à 1 variable, nous allons décrire un algorithme pour déterminer le $PGCD$ de $f_1, \ldots, f_s$. En réordonnant au besoin les f_i on peut supposer que $\deg f_1 \geq \cdots \geq \deg f_s$. Cherchons d'abord le $PGCD$ de f_s et f_{s-1}. Puisque $\deg f_{s-1} \geq \deg f_s$ on peut effectuer la division euclidienne de f_{s-1} par f_s. Il existe $h_s, f_{s+1} \in k[X]$ tels que

$$f_{s-1} = h_s f_s + f_{s+1}$$

et ou bien $f_{s+1} = 0$ ou bien $\deg f_{s+1} < \deg f_s$. On a

$$(f_{s-1}, f_s) = (f_s, f_{s+1}) \quad .$$

Si $f_{s+1} = 0$, f_s est le $PGCD$ de f_{s-1}, f_s. Si $f_{s+1} \neq 0$, on peut effectuer la division euclidienne de f_s par $f_{s+1} \ldots$ etc. Si $f_{s+1}, \ldots, f_t$, $h_s, \ldots, h_{t-1}$ ont été déterminés de sorte que

$$f_{i-1} = h_i f_i + f_{i+1} \ , \quad i = s, \ldots, t-1 \tag{1}$$

$$f_i \neq 0 \ , \quad i = s+1, \ldots, t \tag{2}$$

$$\deg f_{i+1} < \deg f_i \ , \quad i = s, \ldots, t-1 \quad . \tag{3}$$

On a

$$(f_{s-1}, f_s) = (f_s, f_{s+1}) = \cdots = (f_{t-1}, f_t) \quad .$$

Effectuant la division euclidienne de f_{t-1} par f_t, nous déterminons f_{t+1} , h_t tels que $(f_{t-1}, f_t) = (f_t, f_{t+1})$ et ou bien $f_{t+1} = 0$ ou bien $\deg f_{t+1} < \deg f_t$. Un tel processus s'arrête.

Ou bien, on détermine f_n tel que $f_n = 0$ et $(f_{s-1}, f_s) = \cdots (f_{n-1})$. f_{n-1} le dernier reste obtenu non nul est le $PGCD$ cherché. Ou bien on détermine $f_n \neq 0$ tel que $\deg f_n = 0$. f_n se réduit à une constante non nulle et $(f_{s-1}, f_s) = (f_{n-1}, f_n) = (1)$. f_{s-1} et f_s sont premiers entre eux.

Soit maintenant F_{s-1} le $PGCD$ de f_{s-1} et f_s. On a $(f_1, \ldots, f_s) = (f_1, \ldots, f_{s-2}, F_{s-1})$. Remarquons que

$$\deg F_{s-1} \leq \deg f_{s-1} \leq \deg f_{s-2} \leq \cdots \leq \deg f_1.$$

Par le même procédé que ci-dessus, on détermine F_{s-2} le $PGCD$ de f_{s-2} et F_{s-1}. Alors $(f_1, \ldots, f_{s-2}, F_{s-1}) = (f_1, \ldots, f_{s-3}, F_{s-2})$. Ce processus s'arrête ou bien si on trouve $F_i = 1$, $i \geq 2$, ou conduit à déterminer F_1 tel que $(f_1, \ldots, f_s) = (F_1)$.

Cet algorithme apparaît également comme un ingrédient élémentaire dans la fabrication d'autres algorithmes. Nous allons voir par exemple comment il permet de déterminer *la décomposition sans carrés d'un polynôme à 1 variable sur un corps k de caractéristique* 0.

Si $f \in k[X]$ et si $f = a_0 X^d + a_1 X^{d-1} + \cdots + a_d$, $a_0 \neq 0$, $\overline{k}$ étant une clôture algébrique de k , il existe $\alpha_1, \ldots, \alpha_n \in \overline{k}$, $1 \leq n \leq d$, et $m_1, \ldots, m_n \in \mathbf{N}$, $m_i \geq 1$, $i = 1, \ldots, n$ tels que

$$f = a_0 (X - \alpha_1)^{m_1} \ldots (X - \alpha_n)^{m_n};$$

m_i est l'ordre de multiplicité de la racine α_i . Si $m_i = 1$, α_i est une racine simple. Si $m_i \geq 2$, α_i est une racine multiple, et f' désignant la dérivée de f par rapport à X, il en est ainsi si et seulement si α_i est une racine commune à f et f'.

1.4. LEMME. — *Soit k un corps de caractéristique* 0. *Il existe* $f_1, \ldots, f_s \in k[X]$, $s \geq 1$, *tels que :*

i) ou bien $f_i = 1$ *ou bien* f_i *ne possède que des racines simples dans* $\overline{k}$, $i = 1 \ldots s$.

ii) f_i *et* f_j *sont premiers entre eux,* $i \neq j$.

iii) $f = f_1 f_2^2 \ldots f_s^s$.

Démonstration. — L'existence de $f_i \in \overline{k}[X]$ vérifiant i), ii), iii) est évidente. Il suffit de regrouper les différentes racines suivant leur ordre de multiplicité. Il reste à voir que les coefficients des f_i sont dans k.

En fait $f_2 \ldots f_s^{s-1}$ est le $PGCD$ de f et f'. En effet :

$$f' = f_1' f_2^2 \ldots f_s^s + 2 f_2' f_1 f_2 \ldots f_s^s + \cdots + i f_i' f_1 f_2^2 \ldots f_i^{i-1} \ldots f_s^s + \cdots + s f_s' f_1 f_2^2 \ldots f_s^{s-1}$$

on a

$$f = (f_1 f_2 \dots f_s)(f_2 \dots f_s^{s-1})$$

$$f' = (f_1' f_2 \dots f_s + \dots + i f_i' f_1 f_2 \dots \widehat{f_i} \dots f_s + \dots + s f_s' f_1 f_2 \dots \widehat{f_s})$$
$$\times (f_2 \dots f_s^{s-1})$$

où $\widehat{\ }$ surmontant un f_i signifie qu'il ne figure pas. $f_2 \dots f_s^{s-1}$ est donc un diviseur commun à f et f'. Pour s'assurer qu'il s'agit bien du $PGCD$, il suffit de montrer que $f/f_2 \dots f_s^{s-1}$ et $f'/f_2 \dots f_s^{s-1}$ sont premiers entre eux ou encore qu'ils n'ont aucune racine commune dans $\overline{k}$. Or $f/f_2 \dots f_s^{s-1} = f_1 \dots f_s$. Si x est une racine de $f/f_2 \dots f_s^{s-1}$, il existe un seul i tel que x soit racine de f_i . Si x était racine de $f'/f_2 \dots f_s^{s-1}$, il serait également racine de $i f_i' f_1 \dots \widehat{f_i} \dots f_s$, donc puisque k a été supposé de caractéristique 0 , x serait racine de f_i' . Mais x serait alors racine commune à f_i et f_i' , donc racine multiple de f_i contrairement à i).

Il en résulte que $f_2 \dots f_s^{s-1} \in k[X]$. Soit $g = f_2 \dots f_s^{s-1}$. Le calcul ci-dessus montre que $f_3 \dots f_s^{s-2} = PGCD(g, g') \in k[X]$. De même $f_4 \dots f_s^{s-3}, \dots, f_{s-1} f_s^2, f_s \in k[X]$. Finalement $f_1, \dots, f_s$ appartiennent à $k[X]$.

1.5. DÉFINITION. — *$h = f_1 \dots f_s$ est la décomposition sans carré de f .*

Pour obtenir h il suffit donc de diviser f par le $PGCD$ de f et f' . Pour obtenir $f_1, \dots, f_s$, on procède de la façon suivante :

Soit $g_0 = f$, et soit $g_i = PGCD(g_{i-1}, g_{i-1}')$ $i \geq 1$. Si $f = f_1 \dots f_s^s$ comme dans 1.4, on a $g_1 = f_2 \dots f_s^{s-1}, \dots$, $g_i = f_{i+1} \dots f_s^{s-i}, \dots$, $g_{s-1} = f_s$, $g_s = 1, \dots, g_n = 1, \dots$ et $\deg g_0 > \deg g_1 > \dots > \deg g_{s-1} > \deg g_s = 0$. s est donc le plus petit entier i tel que $\deg g_i = 0$.

De plus, $g_{i-1}/g_i = f_i \dots f_s$ et $f_i = g_{i-1}/g_i / g_i/g_{i+1} = \frac{g_{i-1} \cdot g_{i+1}}{g_i^2}$, $i = 1 \dots s$.

Etant donné un système d'équations algébriques $f_1, \dots f_s$ à 1 variable, nous avons montré comment obtenir un système équivalent $PGCD(f_1, \dots, f_s)$ au vu duquel, on puisse dire immédiatement si le système donné au départ possède ou non une solution dans $\overline{k}$. Précisément, il en est ainsi si $\deg PGCD(f_1, \dots, f_s) \geq 1$.

Classiquement, la question de savoir si un système d'équations algébriques $f_1, \dots, f_s$ possédait ou non une solution dans $\overline{k}$ a été également abordée d'un autre point de vue. Il s'agissait de trouver des conditions (algébriques) sur les coefficients des monômes apparaissant dans $f_1, \dots, f_s$ pour qu'il en soit ainsi.

Nous allons illustrer ce point de vue dans le cas particulièrement simple d'un système de 2 équations à 1 variable où la condition algébrique en question est frappante. Dans la suite du cours, nous généraliserons le premier point de vue - algorithme de transformation des équations - mais pas le second de nature plus théorique et moins immédiatement adapté au calcul.

Soit

$$f_1 = a_0 X^l + a_1 X^{l-1} + \dots + a_l \ , \ a_i \in k \ , \ i = 0 \dots l \ , \ l \geq 1,$$

$$f_2 = b_0 X^m + b_1 X^{m-1} + \dots + b_m \ , \ b_j \in k \ , \ j = 0 \dots m \ , \ m \geq 1.$$

Soit S la matrice à $m+l$ lignes et colonnes définie comme suit :

$$\left|\begin{array}{ccccccccc}
a_0 & a_1 & \cdots & \cdots & a_l & 0 & \cdots & \cdots & 0 \\
0 & a_0 & \cdots & \cdots & a_{l-1} & a_l & \cdots & \cdots & 0 \\
\vdots & & \ddots & & & & & & \vdots \\
\vdots & & & \ddots & & & & & \vdots \\
0 & 0 & \cdots & \cdots & a_0 & a_1 & \cdots & \cdots & a_l \\
b_0 & b_1 & \cdots & \cdots & \cdots & b_m & \cdots & \cdots & 0 \\
0 & b_0 & \cdots & \cdots & \cdots & b_{m-1} & b_m & & 0 \\
\vdots & & \ddots & & & & & \ddots & \vdots \\
0 & \cdots & \cdots & b_0 & b_1 & \cdots & \cdots & \cdots & b_m
\end{array}\right| \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\\a\end{array}}\right\} m \text{ lignes} \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} l \text{ lignes} \end{array}$$

1.6. DÉFINITION . — *S est la matrice de Sylvester associée à f_1 et f_2 .*

1.7. PROPOSITION . — *Les conditions suivantes sont équivalentes :*

i) Le système f_1, f_2 possède au moins une racine dans une clôture algébrique de k ou bien $a_0 = b_0 = 0$.

ii) $\det S = 0$.

Démonstration. — *i)* $\Rightarrow$ *ii)*. Si $a_0 = b_0 = 0$, $\det S = 0$. Si le système f_1, f_2 possède une racine x , on a :

$$(*) \qquad a_0x^l + a_1x^{l-1} + \cdots + a_l = 0$$

$$(**) \qquad b_0x^m + b_1x^{m-1} + \cdots\cdots + b_m = 0$$

En multipliant successivement $(*)$ par $x^{m-1}, x^{m-2}, \ldots, x, 1$ et $(**)$ par $x^{l-1}, \ldots, x, 1$, on obtient $m+l$ identités.

$$\left.\begin{array}{l} \\ \\ \\ \end{array}\right\} m \text{ lignes} \quad \left\{\begin{array}{llll}
a_0x^{m+l-1} & +a_1x^{m+l-2} & +\cdots & +a_lx^{m-1} = 0 \\
 & a_0x^{m+l-2} & +\cdots & \cdots \qquad +a_lx^{m-2} = 0 \\
 & \vdots & & \\
b_0x^{m+l-1} & +b_1x^{m+l-2} & +\cdots & +b_mx^{l-1} = 0 \\
 & b_0x^{m+l-2} & +\cdots & \cdots \qquad +b_mx^{l-2} = 0 \\
 & \vdots & &
\end{array}\right. \quad \left.\begin{array}{l} \\ \\ \\ \end{array}\right\} l \text{ lignes}$$

Le système linéaire homogène associé à la matrice S :

$$\begin{array}{llll}
a_0X_{m+l-1} & +a_1X_{m+l-2} & +\cdots & +a_lX_{m-1} = 0 \\
 & a_0X_{m+l-2} & +\cdots & \cdots \qquad +a_lX_{m-2} = 0 \\
 & \vdots & & \\
b_0X_{m+l-1} & +b_1X_{m+l-2} & +\cdots & +b_mX_{l-1} = 0 \\
 & b_1X_{m+l-2} & +\cdots & \cdots \qquad +b_mX_{l-2} = 0 \\
 & \vdots & &
\end{array}$$

possède donc la solution $X_0 = 1$, $X_1 = x, \ldots, X_{m+l-1} = x^{m+l-1}$.

Or, si $\det S$ était non nul, il s'agirait d'un système de Cramer dont l'unique solution serait $X_0 = X_1 = \cdots = X_{m+l-1} = 0$. $\det S$ est donc nul.

ii) $\Rightarrow$ *i)*. Supposons maintenant que $\det S = 0$ et que a_0, b_0 ne sont pas tous les deux nuls. Le problème étant symétrique en f_1 et f_2 , on peut supposer que $b_0 \neq 0$, autrement dit que f_2 est de degré m exactement. Il s'agit de voir que le système f_1, f_2 possède une racine dans une clôture algébrique de k au moins. (La considération du système linéaire homogène de la partie précédente ne suffit pas ici. $\det S$ étant non nul, on en déduit seulement l'existence d'une solution $(x_0, x_1, \ldots, x_{m+l-1}) \in k^{m+l}$ non identiquement nulle, solution qui n'est pas a priori de la forme $(1, x, x^2, \ldots, x^{m+l-1})$). Si f_1, f_2 ne possédait pas de racine, d'après 1.3, $1 \in (f_1, f_2)$. Il existerait donc $h_1, h_2 \in k[X]$ tels que $1 = h_1 f_1 + h_2 f_2$. Plus précisément, on a le

1.7.1. LEMME . — *Soit $f_1, f_2 \in k[X]$ tels que $\deg f_i \geq 1$, $i = 1,2$. Si $PGCD(f_1, f_2) = 1$, il existe $h_1 \in k[X]$ tel que $\deg h_1 < \deg f_2$, $h_2 \in k[X]$ tel que $\deg h_2 < \deg f_1$ et que $1 = h_1 f_1 + h_2 f_2$.*

Si $h_1', h_2' \in k[X]$ et si $\deg h_1' < \deg f_2$ et $1 = h_1' f_1 + h_2' f_2$ alors $h_1 = h_1'$, $h_2 = h_2'$.

Démonstration. — Puisque $PGCD(f_1, f_2) = 1$, il existe $H_1, H_2 \in k[X]$ tels que $1 = H_1 f_1 + H_2 f_2$. $H_i \neq 0$, $i = 1.2$ puisque $\deg f_i \geq 1$, $i = 1.2$ et $\deg H_1 + \deg f_1 = \deg H_2 + \deg f_2$. Si $\deg H_1 < \deg f_2$, on a donc $\deg H_2 < \deg f_1$.

Si maintenant $\deg H_1 \geq \deg f_2$, on peut diviser H_1 par f_2 . Il existe $Q \in k[X]$ et $h_1 \in k[X]$ tel que $\deg h_1 < \deg f_2$ et que $H_1 = Qf_2 + h_1$. Alors $1 = h_1 f_1 + (H_2 + Qf_1) f_2$. Soit $h_2 = H_2 + Qf_1$. Le raisonnement ci-dessus montre que $\deg h_2 < \deg f_1$.

Si maintenant $1 = h_1' f_1 + h_2' f_2$ avec $\deg h_1' < \deg f_2$, on a $(h_1 - h_1') f_1 = (h_2' - h_2) f_2$.

$$\begin{aligned}(h_1 - h_1') &= (h_1 - h_1')(h_1 f_1 + h_2 f_2) = h_1(h_1 - h_1') f_1 + h_2(h_1 - h_1') f_2 \\ &= h_1(h_2' - h_2) f_2 + h_2(h_1 - h_1') f_2 = (h_1 h_2' - h_2 h_1') f_2\end{aligned}$$

Si donc $h_1 - h_1' \neq 0$ $\deg h_1 - h_1' \geq \deg f_2$. Mais par ailleurs $\deg h_1$ et $\deg h_1'$ sont inférieurs strictement à $\deg f_2$. C'est donc que $h_1 = h_1'$ et $h_2 = h_2'$.

Puisque $\deg f_2 = m \geq 1$, si $f_1 = 0$, le système (f_1, f_2) possède au moins une racine dans $\bar{k}$. $f_1 \neq 0$, $\deg f_1 = 0$ est impossible car alors $f_1 = a_l$ et $\det S = a_l^m b_0^l \neq 0$. On a donc $\deg f_i \geq 1$, $i = 1.2$. Dans l'identité $1 = h_1 f_1 + h_2 f_2$, on peut donc supposer d'après 1.7.1, que $\deg h_1 < \deg f_2 = m$ et $\deg h_2 < \deg f_1 \leq l$.

Il existe donc $c_0, \ldots, c_{m-1}$, $d_0, \ldots, d_{l-1} \in k$ tels que

$$h_1 = c_0 X^{m-1} + \cdots + c_{m-1}$$
$$h_2 = d_0 X^{l-1} + \cdots + d_{l-1}$$

$1 = h_1 f_1 + h_2 f_2$ est alors équivalent aux $m + l$ relations :

$$a_0 c_0 + b_0 d_0 = 0$$
$$a_1 c_0 + a_0 c_1 + b_1 d_0 + b_0 d_1 = 0$$
$$\vdots$$
$$\sum_{i+j=k} a_i c_j + \sum_{i'+j'=k} b_{i'} d_{j'} = 0 \qquad 0 \leq k \leq m + l - 2$$
$$\vdots$$
$$a_l c_{m-1} + b_m d_{l-1} = 1$$

Considérons maintenant le système linéaire (avec 2e membre) dont la matrice est la transposée de S :

$$a_0 U_0 + b_0 V_0 = 0$$
$$a_1 U_0 + a_0 U_1 + b_1 V_0 + b_0 V_1 = 0$$
$$\vdots$$
$$\sum_{i+j=k} a_i U_j + \sum_{i'+j'=k} b_{i'} V_{j'} = 0 \qquad 0 \leq k \leq m + l - 2$$
$$\vdots$$
$$a_l U_{m-1} + b_m V_{l-1} = 1$$

Ce système possède donc une solution : $U_j = c_j$, $j = 0 \ldots m-1$, $V_{j'} = d_{j'}$, $j' = 0 \ldots l-1$. Il possède même une solution unique. En effet, si $c'_0, \ldots, c'_{m-1}$; $d'_0, \ldots, d'_{l-1}$ est une autre solution, posant :

$$h'_1 = c'_0 X^{m-1} + \cdots + c'_{m-1}$$
$$h'_2 = d'_0 X^{l-1} + \ldots + d'_{l-1}$$

on a $1 = h'_1 f_1 + h'_2 f_2$ et $\deg h'_1 < m = \deg f_2$. Il résulte alors de 1.7.1 que $h_1 = h'_1$ et $h_2 = h'_2$ ou encore $c_j = c'_j$, $j = 0 \ldots m-1$; $d_{j'} = d'_{j'}$, $j' = 0 \ldots l-1$.

Le système linéaire précédent est donc un système de Cramer et $\det {}^t S = \det S \neq 0$ contrairement à l'hypothèse. C'est que le système f_1, f_2 possède au moins une racine dans $\overline{k}$.

1.8. DÉFINITION . — *Le déterminant de la matrice de Sylvester associée à f_1 et f_2 est appelé le résultant de f_1 et f_2.*

2. Les systèmes linéaires - L'algorithme de Gauss

Un système linéaire est la donnée d'un nombre fini de polynômes de degré ≤ 1, $f_1, \ldots, f_s$ en un nombre fini de variables $X_1, \ldots, X_n$ à coefficients dans un corps k .

Si $f_i = \sum_{j=1\ldots n} a_{ij} X_j + b_i \quad , \quad i = 1 \ldots s \quad , \quad a_{ij}, b_i \in k$, on sait que :

1) Si $b_i = 0, \quad i = 1 \ldots s$, les solutions du système $f_1, \ldots, f_s$ dans k forment un k-espace vectoriel S_k dont la dimension est $n - \rho$ où ρ est le rang de la matrice $A = (a_{ij})$ i.e. la taille maximale d'un mineur non nul extrait de A .

Si k' est une extension de k , les solutions dans k' forment un k'-espace vectoriel $S_{k'}$ ayant pour k'-base toute k- base de S_k.

2) En général, les conditions suivantes sont équivalentes :

i) S_k (les solutions dans k) $\neq \emptyset$.

ii) Pour toute extension k' de k, $S_{k'}$ (les solutions dans k') $\neq \emptyset$.

iii) Si $A = (a_{ij})$, $A' = (A^{b_i}_{b_s})$ $\operatorname{rg} A = \operatorname{rg} A'$.

Si $S_{k'} \neq \emptyset$, $S_{k'}$ est une sous- variété linéaire affine de k'^n de dimension $n - \rho$ où $\rho = \operatorname{rg} A = \operatorname{rg} A'$.

Comme l'algorithme du $PGCD$, l'algorithme de Gauss permet de déterminer un système équivalent au système donné sur lequel on lit immédiatement quelles sont ses solutions.

Soit donc $f_i = \sum_{j=1\ldots n} a_{ij} X_j + b_i$, $a_{ij}, b_i \in k$, $1 \leq i \leq s$, $s \geq 2$ un système linéaire.

Si il existe k, $1 \leq k \leq n$, tel que $a_{ik} \neq 0$, soit

$l_i = \{\inf j \ , \ 1 \leq j \leq n \quad a_{ij} \neq 0\}$, $1 \leq l_i \leq n$, sinon soit $l_i = +\infty$. (On convient que $+\infty$ est strictement plus grand que tout entier).

On dit que

$$\tau(f_1, \ldots, f_s) = 0$$

si ou bien $l_1 \neq +\infty$ et $\exists j \in 2 \ldots s$ tel que $l_j \leq l_1$,
ou bien $l_1 = +\infty$ et $\exists j \in 2 \ldots s$ tel que $l_j < l_1$,

$$\tau(f_1, \ldots, f_s) = k \quad , \quad 1 \leq k \leq s - 2$$

si $l_1 < l_2 < \ldots < l_k \quad , \quad l_j > l_k \quad , \quad j \in k+1 \ldots s$,
et si ou bien $l_{k+1} \neq +\infty$ et $\exists j \in k+2 \ldots s$ tel que $l_j \leq l_{k+1}$,
ou bien $l_{k+1} = +\infty$ et $\exists j \in k+2 \ldots s$ tel que $l_j < l_{k+1}$,

$$\tau(f_1, \ldots, f_s) = \infty$$

si $l_1 \leq \ldots \leq l_s$ et si $l_i = l_{i+1} \Rightarrow l_i = +\infty$.

Si $\tau(f_1, \ldots, f_s) = \infty$, le système est triangulaire. Si il existe $\rho \in 0 \ldots s-1$ tel que $l_1 < \ldots < l_\rho < \infty$, $l_i = \infty$, $i > \rho$, il est de la forme

$$\begin{aligned}
f_1 &= a_{1l_1} X_{l_1} + \sum_{j>l_1} a_{1j} X_j + b_1 && a_{1l_1} \neq 0 \\
f_2 &= a_{2l_2} X_{l_2} + \sum_{j>l_2} a_{2j} X_j + b_2 && a_{2l_2} \neq 0 \\
&\vdots \\
f\rho &= a_{\rho l_\rho} X_{l_\rho} + \sum_{j>l_\rho} a_{\rho j} X_j + b_\rho && a_{\rho l_\rho} \neq 0 \\
f_{\rho+1} &= b_{\rho+1} \\
&\vdots \\
f_s &= b_s
\end{aligned}$$

Il possède des solutions si et seulement si $b_{\rho+1} = \cdots = b_s = 0$ et dans ce cas il est de rgρ .

Si $l_1 < \cdots < l_s < \infty$, le système possède des solutions et est de rang s .

Si $\tau(f_1, \ldots, f_s) \neq \infty$, soit :

$$f_j^1 = f_j \qquad \text{si} \quad j \leq k = \tau(f_1, \ldots, f_s)$$

Soit $\Lambda = \inf l_j$, $j \in k+1 \ldots s$, $l_k < \Lambda \leq n$ et soit

$$t = \inf\{s' : k+1 \leq s' \leq s \ , \ a_{s'\Lambda} \neq 0\} \quad , \quad k+1 \leq t \leq s$$

$$\begin{aligned}
f_{k+1}^1 &= f_t \\
f_j^1 &= f_{j-1} && k+2 \leq j \leq t \\
f_j^1 &= f_j - \frac{a_{j\Lambda}}{a_{t\Lambda}} f_t && t < j \leq s
\end{aligned}$$

Le système $f_1^1, \ldots, f_s^1$ est équivalent au système $f_1, \ldots, f_s$.

$$\begin{aligned}
l_j^1 &= l_j \cdot && \text{si} \quad j \leq k \\
l_{k+1}^1 &= \Lambda \\
l_j^1 &> \Lambda && \text{si} \quad j > k+1
\end{aligned}$$

Par suite, $\tau(f_1^1, \ldots, f_s^1) = k_1 > k$.

Si $k_1 = \infty$, $f_1^1, \ldots, f_s^1$ est un système triangulaire, si $k_1 \neq \infty$, on applique au système $f_1^1, \ldots, f_s^1$ la même transformation. Au bout d'un nombre fini d'étapes, le système obtenu aura une forme triangulaire.

Exercice

Soit k un corps et soit $R = k[X, Y_0, \ldots, Y_l, Z_0, \ldots, Z_m]$ l'anneau de polynômes à $l + m + 3$ indéterminées sur k . On suppose $l \geq 1$ et $m \geq 1$. Soit

$$F_1 = \sum_{i=0\ldots l} Y_i X^{l-i}$$

$$F_2 = \sum_{j=0\ldots m} Z_j X^{m-j} .$$

On pose :

$$\Delta(Y_0, \ldots, Y_l, Z_0, \ldots, Z_m) = \det \underbrace{\begin{vmatrix} Y_0 & & 0 \\ Y_1 & \ddots & \\ \vdots & & Y_0 \\ \vdots & & Y_1 \\ Y_l & & \vdots \\ & \ddots & \vdots \\ 0 & & Y_l \end{vmatrix}}_{m \text{ colonnes}} \underbrace{\begin{vmatrix} Z_0 & & & 0 \\ Z_1 & \ddots & & \\ \vdots & \ddots & \ddots & \\ Z_m & & \ddots & Z_0 \\ & \ddots & & Z_1 \\ & & \ddots & \vdots \\ 0 & & & Z_m \end{vmatrix}}_{l \text{ colonnes}}$$

1) Montrer que Δ est non identiquement nul dans $k[Y_0, \ldots, Y_l, Z_0, \ldots, Z_m]$. Soit

$$\Delta = \sum_{\alpha=(\alpha_0,\ldots,\alpha_l)\in \mathbf{N}^{l+1}, \beta=(\beta_0,\ldots,\beta_m)\in \mathbf{N}^{m+1}} C_{\alpha\beta} Y_0^{\alpha_0} \ldots Y_l^{\alpha_l} Z_0^{\beta_0} \ldots Z_m^{\beta_m} .$$

Montrer que $C_{\alpha\beta} \neq 0$ entraîne :

i) $\alpha_0 + \alpha_1 + \cdots + \alpha_l = m$

ii) $\beta_0 + \beta_1 + \cdots + \beta_m = l$

iii) $\sum_{i=0\ldots l} i\alpha_i + \sum_{j=0\ldots m} j\beta_j = lm$.

(Pour ce faire, on calculera successivement

$$\Delta(tY_0, \ldots, tY_l, Z_0, \ldots, Z_m)$$
$$\Delta(Y_0, \ldots, Y_l, tZ_0, \ldots, tZ_l),$$
$$\Delta(Y_0, tY_1, \ldots, t^l Y_l, Z_0, tZ_1, \ldots, t^m Z_m)$$

en multipliant colonnes et lignes du déterminant par des puisssances convenables de t).

2) Montrer qu'il existe $A_i \in k[Y_0, \ldots, Y_l, Z_0, \ldots, Z_{m-1}]$, $i = 1 \ldots l$, tels que

$$\Delta = Y_0^m Z_m^l + \left[(-1)^m Z_0 Y_1^m + Y_0 A_1\right] Z_m^{l-1} + A_2 Z_m^{l-2} + \cdots + A_l .$$

En déduire que Δ est un polynôme irréductible de $k[Y_0, \ldots, Y_l, Z_0, \ldots, Z_m]$ (on utilisera 1), i) et ii))).

3) Montrer qu'il existe $H_i \in k[Y_0, \ldots, Y_l, Z_0, \ldots, Z_m][X]$, $i = 1, 2$ tels que le degré de H_1 par rapport à la variable X soit inférieur ou égal à $m-1$, le degré de H_2 par rapport à la variable X soit inférieur ou égal à $l-1$ et $\Delta = H_1 F_1 + H_2 F_2$.

4) Soit $P \in k[Y_0, \ldots, Y_l, Z_0, \ldots, Z_m][X]$ de degré $s \geq m$ par rapport à la variable X . Montrer qu'il existe Q et $R \in k[Y_0, \ldots, Y_l, Z_0, \ldots, Z_m][X]$ tels que $R = 0$ ou $\deg_X R \leq m-1$ et $Z_0^{s-m+1} P = QF_2 + R$. En déduire que

$$\big((F_1, F_2)k[X, Y_0, \ldots, Y_l, Z_0, \ldots, Z_m]\big) \cap k[Y_0, \ldots, Y_l, Z_0, \ldots, Z_m]$$

est l'idéal principal engendré par Δ . On utilisera le fait que si un polynôme Δ irréductible divise un produit PQ sans diviser P , il divise Q .

5) Soit maintenant $f_1 \in k[X, Y]$, $f_2 \in k[X, Y]$ 2 polynômes en 2 variables de degré respectivement l et m . On suppose que $f_1 = f_2 = 0$ possède un nombre fini s de solutions. Montrer que $s \leq ml$.