Université Claude Bernard LYON 1
Master MA Mathématiques générales
Algèbre et calcul formel

Systèmes d'équations algébriques

1 Ensembles algébriques

Soient K un corps et Ω une K-extension algébriquement close [1] ; pour une partie S de $K[X_1, \cdots, X_n]$ on pose [2]

$$Z(S) = \{(x_1, \cdots, x_n) \in \Omega^n \,/\, f(x_1, \cdots, x_n) = 0 \text{ pour tout } f \in S\}$$

Soit $I = \langle S \rangle$ l'idéal de $K[X_1, \cdots, X_n]$ engendré par S ; on a $Z(I) = Z(S)$.
De plus, tout idéal I de $K[X_1, \cdots, X_n]$ étant de la forme $I = \langle f_1, \cdots, f_r \rangle$ (théorème de l*a base finie* de Hilbert) on a $Z(I) = Z(f_1, \cdots, f_r)$.
Pour tout idéal I de $K[X_1, \cdots, X_n]$, le *sous-Ω-espace vectoriel* $I_{(\Omega)}$ de $\Omega[X_1, \cdots, X_n]$ engendré par I est un idéal [3] de $\Omega[X_1, \cdots, X_n]$; et l'on a :

$$Z(I) = Z(I_{(\Omega)}) \text{ pour tout idéal } I \text{ de } K[X_1, \cdots, X_n]$$

Proposition 1
Soit $\mathbf{G}$ une base de Gröbner, pour un ordre monomial $\preceq$, d'un idéal I de $K[X_1, \cdots, X_n]$; alors $\mathbf{G}$ est une base de Gröbner, pour l'ordre $\preceq$ de l'idéal $I_{(\Omega)}$ de $\Omega[X_1, \cdots, X_n]$.
En particulier on a :

$$\mathrm{lm}_{\preceq}(I) = \mathrm{lm}_{\preceq}(I_{(\Omega)})$$

$\triangledown$ Considérons une base de Gröbner $\mathbf{G}$ de I ; comme $\mathbf{G}$ est un système générateur de I, c'est aussi un système générateur de $I_{(\Omega)}$. Pour $f, g \in \mathbf{G}$, $f \neq g$, le reste de la division multivariée de $S_{\preceq}(f, g)$ par $\mathbf{G}$ est nul [4] de sorte que $S_{\preceq}(f, g) = \sum_{h \in \mathbf{G}} q_h\, h$ avec $\mathrm{lm}_{\preceq}(q_h\, h) \preceq \mathrm{lm}_{\preceq}(S_{\preceq}(f, g))$ pour tout h tel que $q_h \neq 0$. Comme $q_h \in K[X_1, \cdots, X_n] \subset \Omega[X_1, \cdots, X_n]$ pour tout $h \in \mathbf{G}$, le critère de Buchberger est vérifié et $\mathbf{G}$ est une base de Gröbner de $I_{(\Omega)}$. $\triangle$

Corollaire 1
Pour tout idéal I de $K[X_1, \cdots, X_n]$ on a :

$$I = I_{(\Omega)} \cap K[X_1, \cdots, X_n]$$

de sorte que l'application : $I \longrightarrow I_{(\Omega)}$ de l'ensemble des idéaux de $K[X_1, \cdots, X_n]$ dans l'ensemble des idéaux de $\Omega[X_1, \cdots, X_n]$ est injective [5].

$\triangledown$ On a évidemment $I \subset I_{(\Omega)} \cap K[X_1, \cdots, X_n]$. Réciproquement soit $f \in I_{(\Omega)} \cap K[X_1, \cdots, X_n]$; alors [6] le reste de la division multivariée de f par une base de Gröbner $\mathbf{G}$ de I, qui est aussi une base de Gröbner de $I_{(\Omega)}$ est nul de sorte que l'on a $f = \sum_{g \in \mathbf{G}} q_g\, g$ avec, pour tout $g \in \mathbf{G}$, $q_g \in \Omega[X_1, \cdots, X_n]$ donc $q_g \in K[X_1, \cdots, X_n]$ par *rationalité* de la division multivariée. $\triangle$

1. on considérera principalement $K = \mathbb{Q}$ et $\Omega = \overline{\mathbb{Q}}$ ou $\Omega = \mathbb{C}$ ou bien $K = \mathbb{F}_p$ et $\Omega = \overline{\mathbb{F}_p}$
2. ou bien $Z_\Omega(S)$ lorsqu'il est nécessaire de préciser Ω.
3. on a $I_{(\Omega)} = I \otimes_K \Omega$.
4. d'après le th. de Macaulay puisque $S_{\preceq}(f, g) \in I$.
5. un idéal appartenant à l'image de l'application $I \longrightarrow I_{(\Omega)}$ est dit *défini sur K*.
6. on a $f = \sum_{i=1}^{r} a_i f_i$ avec $a_i \in \Omega$ et $f_i \in I$. Le sous-K-espace vectoriel de Ω engendré par 1 et par les coefficients a_i, $1 \leq i \leq r$, est de dimension finie et possède une base $(b_j)_{1 \leq j \leq s}$ avec $b_1 = 1$. Pour tout i on a alors $a_i = \sum_{j=1}^{s} c_{i,j} b_j$ avec $c_{i,j} \in K$ de sorte que $f = \sum_{j=1}^{s} \left(\sum_{i=1}^{r} c_{i,j} f_i\right) b_j$ et finalement, *par identification des coefficients*, on a $f = \sum_{i=1}^{r} c_{i,1} f_i \in I$.

Lemme 1

1. *$Z(\Omega[X_1,\cdots,X_n]) = \emptyset$ et $Z((0)) = \Omega^n$*
2. *Soit $(I_\lambda)_{\lambda\in\Lambda}$ une famille d'idéaux de $\Omega[X_1,\cdots,X_n]$; alors on a :*

$$Z(\sum_{\lambda\in\Lambda} I_\lambda) = \bigcap_{\lambda\in\Lambda} Z(I_\lambda)$$

3. *Soient I et J des idéaux de $\Omega[X_1,\cdots,X_n]$, alors on a :*

$$Z(I)\cup Z(J) = Z(I.J) = Z(I\cap J)$$

$\triangledown$ Posons $J = \sum_{\lambda\in\Lambda} I_\lambda$; puisque $I_\lambda \subset J$ pour tout $\lambda\in\Lambda$, on a $Z(J) \subset \bigcap_{\lambda\in\Lambda} Z(I_\lambda)$.
Réciproquement, soit $x \in \bigcap_{\lambda\in\Lambda} Z(I_\lambda)$; pour tout $f = \sum_{\lambda\in\Lambda} f_\lambda \in J$ (on a $f_\lambda = 0$ sauf pour un nombre fini d'indices $\lambda\in\Lambda$), on a $f(x) = \sum_{\lambda\in\Lambda} f_\lambda(x) = 0$ de sorte que $x\in Z(J)$ d'où le premier point.
Pour le second, on a $I.J \subset I\cap J \subset I, J$ de sorte que $Z(I)\cup Z(J) \subset Z(I\cap J) \subset Z(I.J)$.
Réciproquement supposons qu'il existe $x \in Z(I.J)\setminus(Z(I)\cup Z(J))$; il existe $f\in I$ tel que $f(x)\neq 0$ et $g\in J$ tel que $g(x)\neq 0$ de sorte que $(fg)(x)\neq 0$ ce qui contredit le fait que $x\in Z(I.J)$. $\triangle$
Une partie $E\subset\Omega^n$ est un ensemble algébrique s'il existe un idéal I de $\Omega[X_1,\cdots,X_n]$ tel que $E = Z(I)$. Ainsi les ensembles algébriques sont les ensembles fermés d'une topologie sur Ω^n appelée la topologie de Zariski.

Lemme 2
Pour tout $x = (x_1,\cdots,x_n)\in\Omega^n$, l'idéal $\mathfrak{m}_x = \{f\in\Omega[X_1,\cdots,X_n] \,/\, f(x) = 0\}$ est maximal, $\{X_1 - x_1,\cdots,X_n - x_n\}$ est une base de Gröbner universelle[7] de $\mathfrak{m}_x$ et l'on a $Z(\mathfrak{m}_x) = \{x\}$.
En particulier l'application $x\longrightarrow \mathfrak{m}_x$ de Ω^n dans l'ensemble des idéaux maximaux de $\Omega[X_1,\cdots,X_n]$ est injective.

$\triangledown$ Soit $\mathfrak{m}' = \langle X_1 - x_1,\cdots,x_n - x_n\rangle$; on a évidemment $\mathfrak{m}'\subset\mathfrak{m}_x$. Réciproquement soit $f\in\mathfrak{m}_x$; la division multivariée de f par $(X_1 - x_1,\cdots,X_n - x_n)$ (pour un ordre admissible quelconque) ; on a $\mathrm{lm}(X_i - x_i) = X_i$ pour $1\leq i\leq n$)) dans l'anneau $\Omega[X_1,\cdots,X_n]$ donne $f = \sum_{i=1}^{n}(X_i - x_i)q_i + c$ avec $c\in\Omega$ et l'on a $c = f(x) = 0$ donc $f\in\mathfrak{m}'$ et $\mathfrak{m}' = \mathfrak{m}_x$. Soit $\preceq$ un ordre monomial ; on a $\mathrm{lm}(X_i - x_i) = X_i$ pour $1\leq i\leq n$; soit $f\in\mathfrak{m}'$ *non nul* alors f n'est pas constant de sorte que $\mathrm{lm}(f)\neq 1$ et il existe i, $1\leq i\leq n$, tel que $X_i|\mathrm{lm}(f)$. Ainsi $\{X_1 - x_1,\cdots,X_n - x_n\}$ est une base de Gröbner de $\mathfrak{m}_x$.
On a $z = (z_1,\cdots,z_n)\in\mathfrak{m}_x$ si et seulement si $(X_i - x_i)(z) = 0$ *ie.* $z_i = x_i$ pour $1\leq i\leq n$ de sorte que $Z(\mathfrak{m}_x) = \{x\}$.. $\triangle$.

2 Théorème d'élimination de Kronecker

Théorème 1 (élimination de Kronecker)
On considère la projection canonique :

$$\begin{array}{rccc} \pi : & \Omega^n & \longrightarrow & \Omega^{n-1} \\ & (x_1,\cdots,x_{n-1},x_n) & \longrightarrow & (x_1,\cdots,x_{n-1}) \end{array}$$

7. *ie.* pour tout ordre monomial

Soient $f_1, \cdots, f_r \in K[X_1, \cdots, X_n]$ des polynômes non constants ; on suppose l'un des polynômes f_i, $1 \leq i \leq r$ quasi-unitaire[8] *en X_n. Soient $I = \langle f_1, \cdots, f_r \rangle$ l'idéal engendré par $f_1, \cdots, f_r$ et $J = I \cap K[X_1, \cdots, X_{n-1}]$ l'idéal d'élimination de X_n ; on a :*

$$\pi(Z(I)) = Z(J)$$

$\triangledown$ Supposons par exemple que f_1 est *quasi-unitaire* en X_n, de degré $d \geq 1$ (comme f_1 n'est pas *constant*) , et s'écrit donc :

$$f_1 = cX_n^d + a_{d-1}(X_1, \cdots, X_{n-1})X_n^{d-1} + \cdots + a_0(X_1, \cdots, X_{n-1}) \text{ avec } c \in K^\star$$

Supposons d'abord que $r = 1$. Pour tout $(x_1, \cdots, x_{n-1}) \in \Omega^{n-1}$ le polynôme :

$$cX_n^d + a_{n-1}(x_1, \cdots, x_{n-1})X_n^{d-1} + \cdots + a_0(x_1, \cdots, x_{n-1}) \in \Omega[X_n]$$

a une racine $x_n \in \Omega$ et l'on a $(x_1, \cdots, x_{n-1}, x_n) \in Z(f_1)$ de sorte que :

$$\pi(Z(f_1)) = \Omega^{n-1} = Z(0)$$

On suppose maintenant que $r = 2$. On a :

$$R = R_{X_n}(f_1, f_2) \in I \cap K[X_1, \cdots, X_{n-1}] = J$$

d'où :

$$R(x_1, \cdots, x_{n-1}) = 0 \text{ pour tout } x = (x_1, \cdots, x_n) \in Z(I)$$

de sorte que :

$$\pi(Z(I)) \subset Z(J) \subset Z(R)$$

Réciproquement, soit $(x_1, \cdots, x_{n-1}) \in \Omega^{n-1}$ tel que :

$$R(x_1, \cdots, x_{n-1}) = 0$$

Le *théorème de spécialisation du résultant* s'applique (puisque f_1 est *quasi-unitaire*) *via* :

$$\begin{array}{rl} K[X_1, \cdots, X_{n-1}] & \longrightarrow \Omega \\ X_1 & \longrightarrow x_1 \\ & \vdots \\ X_{n-1} & \longrightarrow x_{n-1} \end{array}$$

si $\widetilde{R}$ est le résultant (relativement à X_n) des polynômes :

$$\left\{ \begin{array}{l} f_1(x_1, \cdots, x_{n-1}, X_n) \\ f_2(x_1, \cdots, x_{n-1}, X_n) \end{array} \right.$$

on a :

$$\widetilde{R} = R(x_1, \cdots, x_{n-1}) = 0$$

de sorte que les polynômes

$$\left\{ \begin{array}{l} f_1(x_1, \cdots, x_{n-1}, X_n) \\ f_2(x_1, \cdots, x_{n-1}, X_n) \end{array} \right.$$

8. Un polynôme $f \in A[X]$, où A est un anneau commutatif, est *quasi-unitaire* si le coefficient dominant de f est un élément inversible de A.

de $\Omega[X_n]$ ont *une racine commune* x_n.
Ainsi $x = (x_1, \cdots, x_n) \in Z(I)$; on a alors $Z(R) \subset \pi(Z(I))$ et finalement

$$\pi(Z(I)) = Z(J) = Z(R)$$

On suppose maintenant que $r \geq 3$.
On introduit une nouvelle indéterminée U et les polynômes

$$\begin{cases} g = f_1 \\ h = f_2 + U\, f_3 + \cdots + U^{r-2}\, f_r \end{cases}$$

On a :

$$g, h \in K[U, X_1, \cdots, X_{n-1}, X_n] \text{ et } R = R_{X_n}(g, h) \in K[U, X_1, \cdots, X_{n-1}]$$

De plus :

$$R = \sum_{k=0}^{s} R_k U^k \text{ avec } R_k \in K[X_1, \cdots, X_{n-1}] \text{ pour tout } 0 \leq k \leq s$$

Alors, la *formule de Bezout sans dénominateur* :

$$R = S\, g + T\, h \text{ où } S, T \in K[U, X_1, \cdots, X_{n-1}, X_n]$$

montre, *par identification des coefficients en* U, que l'on a :

$$R_k \in I \cap K[X_1, \cdots, X_{n-1}] = J \text{ pour tout } 0 \leq k \leq s$$

En particulier on a :

$$R_k(x_1, \cdots, x_{n-1}) = 0 \text{ pour tout } 0 \leq k \leq s \text{ et pour tout } x = (x_1, \cdots, x_n) \in Z(I)$$

de sorte que :

$$\pi(Z(I)) \subset Z(J) \subset Z(R_0, \cdots, R_s)$$

Réciproquement, soit $(x_1, \cdots, x_{n-1}) \in \Omega^{n-1}$ tel que :

$$R_k(x_1, \cdots, x_{n-1}) = 0 \text{ pour } 0 \leq k \leq s$$

Pour tout $u \in \Omega$, le *théorème de spécialisation du résultant* s'applique (puisque f_1 est *quasi-unitaire*) *via* :

$$\begin{array}{rl} K[U, X_1, \cdots, X_{n-1}] & \longrightarrow \Omega \\ U & \longrightarrow u \\ X_1 & \longrightarrow x_1 \\ & \vdots \\ X_{n-1} & \longrightarrow x_{n-1} \end{array}$$

si $\widetilde{R}$ est le résultant (relativement à X_n) des polynômes :

$$\begin{cases} f_1(x_1, \cdots, x_{n-1}, X_n) \\ f_2(x_1, \cdots, x_{n-1}, X_n) + u f_3(x_1, \cdots, x_{n-1}, X_n) \cdots + u^{r-2} f_r(x_1, \cdots, x_{n-1}, X_n)) \end{cases}$$

on a :

$$\widetilde{R} = R(u, x_1, \cdots, x_{n-1}) = \sum_{k=0}^{s} R_k(x_1, \cdots, x_{n-1}) u^k = 0$$

Il en résulte que, pour tout $u \in \Omega$, les polynômes

$$\begin{cases} f_1(x_1, \cdots, x_{n-1}, X_n) \\ f_2(x_1, \cdots, x_{n-1}, X_n) + uf_3(x_1, \cdots, x_{n-1}, X_n) \cdots + u^{r-2} f_r(x_1, \cdots, x_{n-1}, X_n) \end{cases}$$

de $\Omega[X_n]$ ont *une racine commune*.
Comme cette *racine commune* ne peut prendre qu'un nombre fini de valeurs, il existe une racine x_n du polynôme $f_1(x_1, \cdots, x_{n-1}, X_n) \in \Omega[X_n]$ qui est racine du polynôme

$$f_2(x_1, \cdots, x_{n-1}, X_n) + uf_3(x_1, \cdots, x_{n-1}, X_n) \cdots + u^{r-2} f_r(x_1, \cdots, x_{n-1}, X_n) \in \Omega[X_n]$$

pour une infinité d'entiers de $u \in \Omega$. Finalement le polynôme :

$$f_2(x_1, \cdots, x_{n-1}, x_n) + f_3(x_1, \cdots, x_{n-1}, x_n)U \cdots + f_r(x_1, \cdots, x_{n-1}, x_n)U^{r-2} \in \Omega[U]$$

est *nul*. Ainsi, il existe $x_n \in \Omega$ tel que $x = (x_1, \cdots, x_n) \in Z(I)$. Finalement on obtient que :

$$\pi(Z(I)) = Z(R_0, \cdots, R_s) = Z(J)$$

$\triangle$
Remarque : Le résultat est *faux* si aucun des polynômes $f_1, \cdots, f_r$ n'est quasi-unitaire par rapport à l'une des indéterminées X_i, $1 \leq i \leq n$. Pour $f = XY - 1 \in \mathbb{Q}[X, Y]$, $\pi(Z(f)) = \mathbb{C}^\star$ ne peut pas être de la forme $E = Z(R_0, \cdots, R_s)$ pour $R_0, \cdots, R_s \in \mathbb{C}[X]$, car E est fini ou égal à $\mathbb{C}$.

3 Le théorème des zéros de Hilbert

3.1 Une tranformation linéaire

Etant donné $c = (c_1, \cdots, c_{n-1}) \in \Omega^{n-1}$, on définit l'application linéaire injective :

$$\begin{array}{rccc} \widetilde{\varphi_c} : & \Omega^n & \longrightarrow & \Omega^n \\ & (x_1, \cdots, x_n) & \longrightarrow & (x_1 + c_1 x_n, \cdots, x_{n-1} + c_{n-1} x_n, x_n) \end{array}$$

Par ailleurs on a l'automorphisme d'algèbres : d'algèbres :

$$\begin{array}{rccc} \varphi_c : \Omega[X_1, \cdots, X_n] & \longrightarrow & \Omega[X_1, \cdots, X_n] \\ f & \longrightarrow & f \circ \widetilde{\varphi_c} \end{array}$$

tel que :

$$\varphi_c(f) = f(X_1 + c_1 X_n, \cdots, X_{n-1} + c_{n-1} X_n, X_n) \text{ pour tout } f \in \Omega[X_1, \cdots, X_n]$$

Ainsi φ_c est l'unique automorphisme de l'algèbre $\Omega[X_1, \cdots, X_n]$ tel que

$$\varphi_c(X_i) = \begin{cases} X_i + c_i X_n & \text{pour } 1 \leq i \leq n-1 \\ X_n & \text{pour } i = n \end{cases}$$

On a alors :

$$Z(\varphi_c(f_1), \cdots, \varphi_c(f_r)) = \widetilde{\varphi_c}^{-1}(Z(f_1, \cdots, f_r))$$

Lemme 3
Soient $f_1, \cdots, f_r \in K[X_1, \cdots, X_n]$ avec K infini ; il existe $c \in K^{n-1}$ tel que les polynômes $\varphi_c(f_i) \in K[X_1, \cdots, X_n]$, $1 \leq i \leq r$, soient quasi-unitaires en X_n.

$\triangledown$ Soit $f = \sum_{\alpha} a_\alpha X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in K[X_1, \cdots, X_n]$ de degré d ; pour tout $c \in K^{n-1}$ on a :

$$\begin{aligned}
\varphi_c(f) &= f(X_1 + c_1 X_n, \cdots, X_{n-1} + c_{n-1} X_n, X_n) \\
&= \sum_{\alpha} a_\alpha (X_1 + c_1 X_n)^{\alpha_1} \cdots (X_{n-1} + c_{n-1} X_{n-1})^{\alpha_{n-1}} X_n^{\alpha_n} \\
&= \gamma(c) X_n^d + P_{d-1}(X_n, \cdots, X_{n-1}, c) X_n^{d-1} + \cdots + P_0(X_n, \cdots, X_{n-1}, c)
\end{aligned}$$

avec :

$$\gamma(c) = \sum_{\substack{\alpha \\ |\alpha| = d}} a_\alpha c_1^{\alpha_1} \cdots c_{n-1}^{\alpha_{n-1}}$$

Pour chaque f_i $(1 \leq i \leq r)$ soit $\gamma_i(c)$ le coefficient dominant relativement à X_n de $\varphi_c(f_i)$; en considérant le produit des γ_i, puisque K est infini, il existe $c \in K^{n-1}$ tel que $\gamma_i(c) \neq 0$ pour tout i. $\triangle$

3.2 Le théorème des zéros de Hilbert

Théorème 2 (théorème des zéros de Hilbert)
Soit $I = (f_1, \cdots, f_r)$ un idéal de $K[X_1, \cdots, X_n]$; les conditions suivantes sont équivalentes :

1. $Z(I) = \emptyset$.
2. $1 \in I$.
3. *pour un (resp. pour tout) ordre monomial $\preceq$, si $\boldsymbol{G}$ est la base de Gröbner réduite de I, relativement à $\preceq$, on a $\boldsymbol{G} = \{1\}$.*

$\triangledown$ Si $1 \in I$ on a évidemment $Z(I) = \emptyset$.
Comme $Z(I) = Z(I_{(\Omega)})$ et que $1 \in I$ si et seulement si $1 \in I_{(\Omega)}$ on peut supposer que $K = \Omega$ et l'on établit la réciproque *par récurrence* sur le nombre d'indéterminées n.
Pour $n = 1$ la propriété résulte de ce que Ω est *algébriquement clos* et de ce que l'anneau $\Omega[X]$ est principal[9] . Supposons par hypothèse de récurrence le théorème vérifié pour $n-1$ et considérons $I = \langle f_1, \cdots, f_r \rangle$ un idéal de $\Omega[X_1, \cdots, X_n]$. De plus, on peut supposer que les polynômes $f_1, \cdots, f_n$ sont *quasi-unitaires* en X_n. Par le théorème d'élimination de Kronecker, on a alors $\pi(Z(I)) = Z(I \cap \Omega[X_1, \cdots, X_{n-1}])$ si $Z(I) = \emptyset$, on a $Z(I \cap \Omega[X_1, \cdots, X_{n-1}]) = \emptyset$ d'où $1 \in I$. $\triangle$

3.2.1 Idéaux radiciels

La *racine* d'un idéal I de $K[X_1, \cdots, X_n]$ est l'idéal $\mathrm{rac}(I)$ de $K[X_1, \cdots, X_n]$ formé des polynômes $f \in K[X_1, \cdots, X_n]$ pour lesquels il existe un entier $k \geq 1$ tel que $f^k \in I$. On a évidemment $I \subset \mathrm{rac}(I)$ et $Z(\mathrm{rac}(I)) = Z(I)$. Un idéal I est *radiciel* si l'on a $I = \mathrm{rac}(I)$.

Lemme 4 (Rabinowitch)
Soit I un idéal de $K[X_1, \cdots, X_n]$; on a $f \in \mathrm{rac}(I)$ si et seulement si $\langle I, 1 - T f \rangle = K[X_1, \cdots, X_n, T]$

$\triangledown$ Supposons que $1 \in \langle I, 1 - T f \rangle$; il existe donc $f_1, \cdots, f_r \in I, g_1, \cdots, g_r, g_{r+1} \in K[X_1, \cdots, X_n, T]$ tels que :

$$\sum_{i=1}^{r} g_i(X_1, \cdots, X_n, T) f_i(X_1, \cdots, X_n) + g_{r+1}(X_1, \cdots, X_n, T)(1 - X_{n+1} f(X_1, \cdots, X_n)) = 1$$

9. Si $I = \langle g \rangle$ est un idéal principal, $\{g\}$ est la base de Gröbner réduite de I.

il vient alors :

$$\sum_{i=1}^{r} g_i(X_1,\cdots,X_n,\frac{1}{f(X_1,\cdots,X_n)})f_i(X_1,\cdots,X_n)=1$$

et finalement :

$$\sum_{i=1}^{r} \widetilde{g}_i(X_1,\cdots,X_n)f_i(X_1,\cdots,X_n)=f(X_1,\cdots,X_n)^k$$

avec $\widetilde{g}_i(X_1,\cdots,X_n)\in K[X_1,\cdots,X_n]$ pour $1\leq i\leq r$ de sorte que $f^k\in I$.
Réciproquement supposons que $f^k\in I$; on a alors

$$1=(1-Tf)(T^{k-1}f^{k-1}+\cdots+Tf+1)+T^kf^k\in\langle I,1-T\,f\rangle$$

$\triangle$

Proposition 2
Pour tout idéal I de $K[X_1,\cdots,X_n]$, on a :

$$\mathrm{rac}(I)=\mathcal{I}(Z(I))$$

où, pour $E\subset\Omega^n$, on pose $\mathcal{I}(E)=\{f\in K[X_1,\cdots,X_n]\,/\,f(x)=0$ pour tout$x\in E\}$.
En particulier on a $\mathrm{rac}(I_{(\Omega)})=\mathrm{rac}(I)\cap K[X_1,\cdots,X_n]$.

$\triangledown$ Soit $f\in\mathrm{rac}(I)$; on $f^k\in I$ pour un entier $k\geq 1$, d'où $f^k(x)=0$ et donc $f(x)=0$ pour tout $x\in Z(I)$.
Réciproquement supposons que $f(x)=0$ pour tout $x\in Z(I)$ et considérons l'idéal :

$$J=(I,1-X_{n+1}f)$$

de $K[X_1,\cdots,X_n,X_{n+1}]$. On a $Z(J)=\emptyset$ d'où $1\in Z(J)$ d'après le théorème des zéros de Hilbert. On a donc $f\in\mathrm{rac}(I)$. $\triangle$

Corollaire 2
Pour I et J idéaux de $K[X_1,\cdots,X_n]$, on a $Z(I)=Z(J)$ si et seulement si $\mathrm{rac}(I)=\mathrm{rac}(J)$.

$\triangledown$ On a $Z(\mathrm{rac}(I))=Z(I)$ et $Z(\mathrm{rac}(J))=Z(J)$ de sorte que si $\mathrm{rac}(I)=\mathrm{rac}(J)$ on a $Z(I)=Z(J)$.
Réciproquement supposons que $Z(I)=Z(J)$. Pour $f\in\mathrm{rac}(I)$, on a donc $f(x)=0$ pour tout $x\in Z(J)$ de sorte que $f\in\mathrm{rac}(J)$ et donc $\mathrm{rac}(I)\subset\mathrm{rac}(J)$. De même $\mathrm{rac}(J)\subset\mathrm{rac}(I)$. $\triangle$

Corollaire 3
Les applications $E\longrightarrow\mathcal{I}(E)$ et $I\longrightarrow Z(I)$ sont des bijections décroissantes réciproques l'une de l'autre entre l'ensemble des parties algébriques de Ω^n et l'ensemble des idéaux radiciels de $\Omega[X_1,\cdots,X_n]$

$\triangledown$ Pour tout $E\subset\Omega^n$, $\mathcal{I}(E)$ est un idéal *radiciel*. Pour I idéal *radiciel* on a $\mathcal{I}(Z(I))=\mathrm{rac}(I)=I$ donc l'application $\mathcal{I}$ de l'ensemble des ensembles algébriques dans l'ensemble des idéaux radiciels est surjective.
Cette application est injective puisque si $E=Z(I)$ et $F=Z(J)$ sont des ensembles algébriques avec I et J radiciels[10] tels que $\mathcal{I}(E)=\mathcal{I}(F)$, on a $I=\mathcal{I}(Z(I))=\mathcal{I}(Z(J))=J$ donc $E=F$ $\triangle$

Corollaire 4
L'application $x\longrightarrow\mathfrak{m}_x$ de Ω^n dans l'ensemble des idéaux maximaux de $\Omega[X_1,\cdots,X_n]$ est une bijection.

$\triangledown$ Puisque $Z(\mathfrak{m}_x)=\{x\}$ l'application $x\longrightarrow\mathfrak{m}_x$ est injective.
Soit $\mathfrak{m}$ un idéal maximal de $\Omega[X_1,\cdots,X_n]$; on a $Z(\mathfrak{m})\neq\emptyset$. Pour $x\in Z(\mathfrak{m})$ on a $Z(\mathfrak{m}_x)\subset Z(\mathfrak{m})$ de sorte que $\mathrm{rac}(\mathfrak{m})=\mathfrak{m}\subset\mathrm{rac}(\mathfrak{m}_x)=\mathfrak{m}_x$ et finalement $\mathfrak{m}=\mathfrak{m}_x$. $\triangle$

10. ce que l'on peut supposer puisque $Z(I)=Z(\mathrm{rac}(I))$

4 Systèmes d'équations algébriques avec un nombre fini de solutions.

Proposition 3
Soit I un idéal de $K[X_1, \cdots, X_n]$; les conditions suivantes sont équivalentes :

1. *On a $I \cap K[X_i] \neq \{0\}$ pour $1 \leq i \leq n$.*
2. *$K[X_1, \cdots, X_n]/I$ est un K-espace vectoriel de dimension finie d.*
3. *$\Omega[X_1, \cdots, X_n]/I_{(\Omega)}$ est un Ω-espace vectoriel de dimension finie d.*
4. *$\mathrm{Z}(I)$ est une partie finie de K^n.*
5. *Pour un (resp. pour tout) ordre monomial $\preceq$ pour tout i, $1 \leq i \leq n$, $X_i^{k_i}$ ne soit pas un monôme réduit pour $k_i >> 0$.*
6. *Pour un (resp. pour tout) ordre monomial $\preceq$ et pour une (resp. pour toute) base de Gröbner $\boldsymbol{G}$ de I, relativement à $\preceq$, pour tout i, $1 \leq i \leq n$ il existe $g_i \in \boldsymbol{G}$ tel que $\mathrm{lm}_{\preceq}(g_i) = X_i^{d_i}$, $k_i \geq 1$.*

Lorsque ces conditions sont vérifiées on dit que l'idéal I est de dimension nulle et l'on a[11] :

$$\dim_K(K[X_1, \cdots, X_n]/I) = \dim_\Omega(\Omega[X_1, \cdots, X_n]/I_{(\Omega)})$$

$\triangledown$ Chaque condition implique que I n'est pas nul et on peut supposer que $1 \notin I$.
1. $\Longrightarrow$ 2. Pour $1 \leq i \leq n$, on a $I \cap K[X_i] \neq \{0\}$de sorte qu'il existe $d_i \geq 1$ et $f_i \in K[X]$ tel que $x^{d_i} = f_i(x_i)$ avec $\deg(f_i) < d_i$. Il en résulte que $(x_1^{k_1} \cdots x_n^{k_n})_{0 \leq k_1 < d_1, \ldots, 0 \leq k_n < d_n}$ est un système générateur du K espace vectoriel $K[X_1, \cdots, X_n]/I$ qui est donc de dimension finie.
2. $\Longrightarrow$ 1. la famille $(\overline{X_i^k})_{k \geq 0}$ est liée dans $K[X_1, \cdots, X_n]/I$ donc il existe une combimaison linéaire non triviale des $(X_i^k)_{k \geq 0}$ qui appartient à I.
2. $\Longleftrightarrow$ 3. Comme on a $\mathrm{lm}_{\preceq}(I) = \mathrm{lm}_{\preceq}(I_{(\Omega)})$, les monômes réduits sont le mêmes pour I et pour $I_{(\Omega)}$; d'après le théorème de Macaulay $K[X_1, \cdots, X_n]/I$ est de dimension finie sur K si et seulement si $\Omega[X_1, \cdots, X_n]/I_{(\Omega)}$ est de dimension finie sur Ω et, dans ce cas, les dimensions sont égales.
1. $\Longrightarrow$ 4. Soit p_i non nul appartenant à $I \cap K[X_i] \neq \{0\}$ pour $1 \leq i \leq n$; on a alors $Z(I) \subset \prod_i Z(p_i)$ qui est fini.
4. $\Longrightarrow$ 3. On a $\mathrm{Z}(I) = \mathrm{Z}(I_{(\Omega)})$ fini. Pour tout $1 \leq i \leq n$, il existe un polynôme $P_i \in \Omega[X_i]$ tel que $\mathrm{Z}(P_i) = \pi_i(\mathrm{Z}(I_{(\Omega)}))$ de sorte que $P_i|_{\mathrm{Z}(I_{(\Omega)})} = 0$. Par le théorème des zéros de Hilbert, il existe $k_i \geq 1$ tel que $f_i = P_i^{k_i} \in I_{(\Omega)} \cap \Omega[X_i]$. Par 1. $\Rightarrow$ 3. le Ω-espace vectoriel $\Omega[X_1, \cdots, X_n]/I_{(\Omega)}$ est de dimension finie.
2. $\Rightarrow$ 5. Comme le nombre de monômes réduits est égal à $\dim_K(K[X_1, \cdots, X_n]/I)$, il n'y a qu'un nombre fini de monômes réduits donc X_i^k n'est pas réduit pour $k >> 0$.
5. $\Rightarrow$ 2 L'ensemble des monômes réduits est fini et on conclut par le th. de Macaulay.
5. $\Rightarrow$ 6. Si X_i^k n'est pas réduit, il existe $g_i \in \mathbf{G}$ tel que $\mathrm{lm}_{\preceq}(g_i) | x_i^k$ de sorte que $\mathrm{lm}_{\preceq}(g_i) = X_i^d$.
6. $\Rightarrow$ 5. Si $\mathrm{lm}_{\preceq}(g_i) = X_i^{d_i}$, X_i^k n'est pas réduit pour $k \geq d_i$. $\triangle$

Corollaire 5
Soit I un idéal de $K[X_1, \cdots, X_n]$ de dimension nulle ; on a :

$$\mathrm{Card}(\mathrm{Z}(I)) \leq \dim_K(K[X_1, \cdots, X_n]/I)$$

11. on a plus précisément $\Omega[X_1, \cdots, X_n]/I_{(\Omega)} \simeq (K[X_1, \cdots, X_n]/I) \otimes_K \Omega$.

$\triangledown$ Soit $(t_1, \cdots, t_N) \in \Omega^N$; pour $1 \leq i \leq N$ on pose :

$$L^i_{(t_1,\cdots,t_N)} = \frac{\prod\limits_{\substack{1\leq j\leq N \\ t_j \neq t_i}} (T - t_j)}{\prod\limits_{\substack{1\leq j\leq N \\ t_j \neq t_i}} (t_i - t_j)} \in \Omega[T]$$

On a $L^i_{(t_1,\cdots,t_N)}(t_i) = 1$ tandis que pour $1 \leq j \leq N$, $t_j \neq t_i$ on a $L^i_{(t_1,\cdots,t_N)}(t_j) = 0$.
Considérons $\mathrm{Z}(I) = \{x_1, \cdots, x_N\}$. Pour tout $1 \leq i \leq N$ posons

$$L^i_{Z(I)} = \prod_{k=1}^{n} L^i_{((x_1)_k,\cdots,(x_N)_k)}(X_k) \in \Omega[X_1, \cdots, X_n]$$

On a alors pour $1 \leq i \leq N$:

$$L^i_{Z(I)}(x_i) = \prod_{k=1}^{n} L^i_{((x_1)_k,\cdots,(x_N)_k)}((x_i)_k) = 1$$

tandis que pour $1 \leq j \leq N$ et $j \neq i$ on a :

$$L^i_{Z(I)}(x_j) = \prod_{k=1}^{n} L^i_{((x_1)_k,\cdots,(x_N)_k)}((x_j)_k) = 0$$

puisque $x_j \neq x_i$, il existe l, $1 \leq l \leq n$, tel que $(x_j)_l \neq (x_i)_l$ de sorte que $L^i_{((x_1)_l,\cdots,(x_N)_l)}((x_j)_l) = 0$.
Alors $(\overline{L^i_{Z(I)}})_{1\leq i\leq N}$ est libre dans $\Omega[X_1, \cdots, X_n]/I_{(\Omega)}$: la relation $a_1\overline{L^1_{Z(I)}} + \cdots + a_N\overline{L^N_{Z(I)}} = \overline{0}$ donne $a_1L^1_{Z(I)} + \cdots + a_NL^N_{Z(I)} \in I_{(\Omega)}$ et en prenant la valeur sur x_i on a $a_i = 0$. On a donc :

$$N \leq \dim_\Omega(\Omega[X_1, \cdots, X_n]/I_{(\Omega)}$$

$\triangle$

Lemme 5

1. *Soit I un idéal de $K[X_1, \cdots, X_n]$, si $I_{(\Omega)}$ est radiciel, alors I est radiciel.*
2. *Tout idéal maximal $\mathfrak{m}$ de $K[X_1, \cdots, X_n]$ est radiciel.*
3. *Soit $(I_\lambda)_{\lambda\in\Lambda}$ une famille d'idéaux radiciels de $K[X_1, \cdots, X_n]$, alors si $\bigcap\limits_{\lambda\in\Lambda} I_\lambda$ est radiciel.*

$\triangledown$ 1. Soit $f \in K[X_1, \cdots, X_n]$ tel que $f^k \in I$ avec $k \geq 1$; on a $f \in I_{(\Omega)} \cap K[X_1, \cdots, X_n] = I$.
2. On a $\mathfrak{m} \subset \mathrm{rac}(\mathfrak{m}) \subsetneq K[X_1, \cdots, X_n]$ de sorte que $\mathfrak{m} = \mathrm{rac}(\mathfrak{m})$.
3. Supposons que $f^k \in \bigcap\limits_{\lambda\in\Lambda} I_\lambda$ avec $k \geq 1$; on a donc $f^k \in I_{(\lambda)}$ donc $f \in I_\lambda$ pour tout $\lambda \in \Lambda$. $\triangle$

Lemme 6
Soient I un idéal de $K[X_1, \cdots, X_n]$, $g_1, \cdots, g_r \in K[X_1]$ des polynômes, deux à deux premiers entre eux dans $K[X_1]$. Posons $f = g_1 \ldots g_r \in K[X_1]$; on a alors :

$$I + K[X_1, \cdots, X_n]f = \bigcap_{j=1}^{r} (I + K[X_1, \cdots, X_n]g_j)$$

$\triangledown$ On a évidemment $I + K[X_1, \cdots, X_n]f \subset \bigcap_{j=1}^{r} (I + K[X_1, \cdots, X_n]g_j)$.
Posons $f = g_j h_j$ avec $h_j = \prod_{k \neq j} g_k$. Ainsi $h_1, \cdots, h_r$ sont premiers entre eux dans $K[X_1]$ de sorte que $\sum_{j=1}^{r} u_j h_j = 1$ avec $u_j \in K[X_1]$ d'après la formule de Bezout. Soit $h \in \bigcap_{j=1}^{r} (I + K[X_1, \cdots, X_n]g_j)$; on a donc, pour $1 \leq j \leq r$, $h = b_j + a_j g_j$ avec $b_j \in I$ et $a_j \in K[X_1, \cdots, X_n]$. On a donc :

$$h = \sum_{j=1}^{r} u_j h_j \, h = \sum_{j=1}^{r} u_j h_j b_j + (\sum_{j=1}^{r} u_j a_j) f \in I + K[X_1, \cdots, X_n]f$$

$\triangle$

Proposition 4 (Lemme de Seidenberg)
Soit I un idéal de dimension nulle de $K[X_1, \cdots, X_n]$ tel que pour tout i, $1 \leq i \leq n$, il existe un polynôme unitaire $f_i \in K[X_i] \cap I$ tel que $\text{pgcd}(f_i, f_i') = 1$ *; alors l'idéal I est radiciel.*

$\triangledown$ Montrons par récurrence sur n que I est l'intersection d'un nombre fini d'idéaux maximaux de $K[X_1, \cdots, X_n]$..
Dans le cas $n = 1$ on a $I = \langle f \rangle$ avec $f | f_1$ de sorte que $f_1 = g_1 \ldots g_r$ avec $g_1, \cdots, g_r \in K[X_1]$ unitaires, irréductibles et deux à deux distincts et l'on a $I = \bigcap_{j=1}^{r} \langle g_j \rangle$ et les idéaux $\langle g_j \rangle$ sont maximaux.
La propriété étant supposée vérifiée dan le cas de $n-1$ indéterminées, considérons un idéal I de $K[X_1, \cdots, X_n]$. On a encore $f_1 = g_1 \ldots g_r$ avec $g_1, \cdots, g_r \in K[X_1]$ unitaires, irréductibles et deux à deux distincts de sorte que l'on a :

$$I = I + K[X_1, \cdots, X_n]f_1 = \bigcap_{j=1}^{r} (I + K[X_1, \cdots, X_n]g_j)$$

Il suffit alors de montrer que les idéaux $I + K[X_1, \cdots, X_n]g_j$, $1 \leq j \leq r$ sont intersections d'un nombre fini d'idéaux maximaux. Comme ces idéaux vérifient les hypothèses de la proposition on peut supposer que f_1 est *irréductible*.
Dans ces conditions $L = K[X_1]/\langle f_1 \rangle = K[x_1]$ est une K-extension de degré fini et l'on a un K-morphisme *surjectif* de noyau $K[X_1, \cdots, X_n]f_1$:

$$\begin{array}{rccc} \psi : & K[X_1, X_2, \cdots, X_n] & \longrightarrow & L[X_2, \cdots, X_n] \\ H = & \sum_{\beta=(\beta_2, \cdots, \beta_n)} h_\beta(X_1) X_2^{\beta_2} \cdots X_n^{\beta_n} & \longrightarrow & \sum_{\beta=(\beta_2, \cdots, \beta_n)} h_\beta(x_1) X_2^{\beta_2} \cdots X_n^{\beta_n} \end{array}$$

L'idéal $J = \psi(I)$ et les polynômes $\psi(f_i)$ pour $2 \leq i \leq n$ vérifient les conditions de la propriété de sorte que $J = \bigcap_{j=1}^{s} \mathfrak{n}_j$ avec $\mathfrak{n}_j$, $1 \leq j \leq s$, idéaux maximaux de $L[X_2, \cdots, X_n]$. On a alors [12] $I = \psi^{-1}(J) = \bigcap_{j=1}^{s} \psi^{-1}(\mathfrak{n}_j)$; mais $\mathfrak{m} = \psi^{-1}(\mathfrak{n})$ est un idéal maximal de $K[X_1, X_2, \cdots, X_n]$ pour tout idéal maximal [13] $\mathfrak{n}$ de $L[X_2, \cdots, X_n]$ contenant J.

Corollaire 6
Soit I un idéal de $K[X_1, \cdots, X_n]$ de dimension nulle ; on désigne par p_i le générateur unitaire

12. puisque $\text{Ker}(\psi) \subset I$
13. contenant I

de l'idéal $I \cap K[X_i]$ *pour* $1 \leq i \leq n$ *; on a alors :*

$$\mathrm{rac}(I) = I + \sum_{i=1}^{n} K[X_1, \cdots, X_n]\widetilde{p_i} \quad \text{et} \quad \mathrm{rac}(I_{(\Omega)}) = \mathrm{rac}(I)_{(\Omega)}$$

où $\widetilde{p_i}$ *désigne la partie sans facteur multiple de* p_i*. En particulier* I *est radiciel si et seulement si* $I_{(\Omega)}$ *est radiciel.*

$\triangledown$ On a $\widetilde{p_i} \in \mathrm{rac}(I)$ pour $1 \leq i \leq n$ de sorte que l'on a :

$$I \subset \underbrace{I + \sum_{i=1}^{n} K[X_1, \cdots, X_n]\widetilde{p_i}}_{=J} \subset \mathrm{rac}(I) \subsetneq K[X_1, \cdots, X_n]$$

Mais l'idéal :

$$J = I + \sum_{i=1}^{n} K[X_1, \cdots, X_n]\widetilde{p_i}$$

est *radiciel* et il en est de même de l'idéal :

$$J_{(\Omega)} = I_{(\Omega)} + \sum_{i=1}^{n} \Omega[X_1, \cdots, X_n]\widetilde{p_i} = \mathrm{rac}(I_{(\Omega)})$$

$\triangle$

Corollaire 7
Soit I *un idéal de* $K[X_1, \cdots, X_n]$ *de dimension nulle ; on a :*

$$\mathrm{Card}(\mathrm{Z}(I)) = \dim_K(K[X_1, \cdots, X_n]/\mathrm{rac}(I))$$

$\triangledown$ Posons $\mathrm{Z}(I) = \{x_1, \cdots, x_N\}$. Pour tout $1 \leq i \leq N$, considérons $L^i_{Z(I)} \in\in \Omega[X_1, \cdots, X_n]$; on a $L^i_{Z(I)}(x_i) = 1$ tandis que pour $1 \leq j \leq N$, $j \neq i$ on a $L^i_{Z(I)}(x_j) = 0$.
Alors $(\overline{L^i_{Z(I)}})_{1 \leq i \leq N}$ est libre dans $\Omega[X_1, \cdots, X_n]/\mathrm{rac}(I_{(\Omega)}$; de plus c'est une famille génératrice : pour tout $f \in \Omega[X_1, \cdots, X_n]$ on a $f - \sum_{i=1}^{N} f(x_i)L^i_{Z(I)} \in \mathrm{rac}(I_{(\Omega)})$. Ainsi on a :

$$N = \dim_\Omega(\Omega[X_1, \cdots, X_n]/\mathrm{rac}(I_{(\Omega)})$$

$\triangle$

5 Courbes algébriques

Une *courbe algébrique plane affine* est un ensemble de la forme $\mathcal{C} = Z(f)$ où $f \in \Omega[X, Y]$ est *non constant et sans facteurs multiples.*

Lemme 7
Soit $\mathcal{C}$ *une courbe algébrique ; alors* $\mathcal{C}$ *est infinie.*

$\triangledown$ On a $\mathcal{C} = Z(f)$. En particulier f n'est pas constant, on peut écrire (par exemple) $f = c_d Y^d + c_{d-1}Y^{d-1} + \cdots + c_0$ avec $c_d \neq 0$ et $c_0, \cdots, c_d \in \mathbb{C}[X]$.
Pour tout $x \in \mathbb{C} \setminus \{x_1, \cdots, x_s\}$ on a $c_d(x) \neq 0$.
Le polynôme $F = f(x, Y) \in \mathbb{C}[Y]$ n'est pas constant et possède une racine y dans $\mathbb{C}$. $\triangle$

Lemme 8
Soient $f, g \in K[X_1, \cdots, X_n]$ des polynômes non constants et sans facteurs multiples tels que $Z(f) = Z(g)$; on a $g = c\,f$ avec $c \in K^\star$.

$\triangledown$ Soient $f \in K[X_1, \cdots, X_n]$ et $\widetilde{f}$ la partie sans facteur multiple de f. Comme il existe $k \geq 1$ tel que $f|\widetilde{f}^k$ on a $\widetilde{f} \in \mathrm{rac}(\langle f \rangle)$. Réciproquement si $g \in \mathrm{rac}(\langle f \rangle)$ il existe $k \geq 1$ tel que $f|g^k$ de sorte que tout facteur irréductible h de f divise g et l'on a $\widetilde{f}|g$. On a ainsi :

$$\mathrm{rac}(\langle f \rangle) = \langle \widetilde{f} \rangle$$

Par le théorème des zéros de Hilbert, on a donc $\mathcal{I}(Z(f)) = \langle \widetilde{f} \rangle$. $\triangle$
On dit alors que f est une *équation* de $\mathcal{C} = Z(f)$. Le degré d'une équation f est le *degré* $\deg(\mathcal{C})$ de la courbe $\mathcal{C}$. Si $f \in K[X, Y]$ on dit que $\mathcal{C}$ est *définie sur* K.
Lorsque f est irréductible [14] dans $\Omega[X, Y]$ on dit que la courbe $\mathcal{C}$ est *irréductible*. Sinon on a la décomposition en facteurs irréductibles $f = f_1 \cdots f_r$ de f dans $\Omega[X, Y]$ avec les $f_i \in \Omega[X, Y]$ irréductibles et deux à deux non associés. Les courbes $\mathcal{C}_i$ sont appelées les *composantes irréductibles* de $\mathcal{C}$, sont irréductibles et l'on a $\mathcal{C} = \bigcup_{i=1}^{r} \mathcal{C}_i$.
Considérons une courbe plane affine $\mathcal{C}$ d'équation $f \in \Omega[X, Y]$; un point $(x, y) \in \mathcal{C}$ (i.e. tel que $f(x, y) = 0$) est un point *singulier* si et seulement si on a $\dfrac{\partial f}{\partial X}(x, y) = \dfrac{\partial f}{\partial Y}(x, y) = 0$ sinon le point est *régulier*.

Lemme 9
Tout polynôme homogène $F \in \Omega[X, Y]$ de degré d est de la forme $F = c\prod_{i=1}^{p}(a_i X + b_i Y)^{r_i}$ avec $\sum_{i=1}^{p} r_i = d$.

$\triangledown$ Considérons l'application linéaire :

$$\begin{array}{rcl} \mathcal{H}_d : \Omega[X]_{\leq d} & \longrightarrow & \Omega[X, Y]^d \\ f & \longrightarrow & Y^d f(\dfrac{X}{Y}) \end{array}$$

de l'espace vectoriel $\Omega[X]_{\leq d}$ des polynômes nul ou de degré $\leq d$ dans l'espace vectoriel $\Omega[X, Y]^d$ des polynômes nul ou homogènes de degré d. On a $f = \mathcal{H}_d(f)_{Y \to 1}$ pour tout $f \in \Omega[X]_{\leq d}$ et $F = \mathcal{H}_d(F_{Y \to 1})$ pour tout $F \in \Omega[X, Y]^d$ de sorte que $\mathcal{H}_d$ est bijective.
Soit $F \in \Omega[X, Y]^d$; on a $F = \mathcal{H}_d(f)$ avec $f \in \Omega[X]_{\leq d}$ d'où $f = c\prod_{i=1}^{q}(X - x_i)^{r_i}$ de sorte que $F = cY^{d-\deg(f)}\prod_{i=1}^{q}(X - x_i Y)^{r_i}$ On a donc $p = q + 1$, $r_q = d - \deg(f)$, $a_i = 1$ et $b_i = -x_i$ pour $1 \leq i \leq q$, $a_q = 0$ et $b_q = 1$. $\triangle$

Soit (x, y) un point d'une courbe algébrique $\mathcal{C}$ irréductible ; le *cône tangent* $\mathcal{T}_{(x,y)}(\mathcal{C})$ à la courbe $\mathcal{C}$ au point (x, y) est la *partie principale* du développement de Taylor de f au point (x, y). C'est un polynôme *homogène* de degré m en $X - x$ et $Y - y$: m est la *multiplicité* de $\mathcal{C}$ en (x, y).

Lemme 10

1. *(x, y) est un point régulier de $\mathcal{C}$ si est seulement s'il est de multiplicité $m = 1$; $\mathcal{T}_{(x,y)}(\mathcal{C})$ est alors la droite affine d'équation $\dfrac{\partial f}{\partial X}(x, y)(X - x) + \dfrac{\partial f}{\partial Y}(x, y)(Y - y)$ (i.e. la tangente à $\mathcal{C}$ en (x, y).*

14. on dit *absolument irréductible* pour distinguer d'irréductible dans $K[X, Y]$

2. *Lorsque $m \geq 2$ (i.e. (x,y)) point singulier de $\mathcal{C}$), on a :*

$$\mathcal{T}_{(x,y)}(\mathcal{C}) = c\prod_{i=1}^{p}(a_iX + b_iY + c_i)^{r_i}$$

les droites affines d'équations $a_iX + b_iY + c_i$, $1 \leq i \leq p$, étant deux à deux distinctes et concourantes en (x,y).

$\triangledown$ Notons P la partie principale du développement de Taylor.
Si (x,y) est un point régulier de $\mathcal{C}$ on a $\mathrm{P}_{(x,y)}(f) = \dfrac{\partial f}{\partial X}(x,y)(X-x) + \dfrac{\partial f}{\partial Y}(x,y)(Y-y)$.
Pour un point singulier, on a $m \geq 2$ mais $\mathrm{P}_{(x,y)}(f)$ est un polynôme *homogène* de degré m de $\Omega[X-x, Y-y]$ de sorte que l'on a la factorisation $\mathrm{P}_{(x,y)}(f) = c\prod_{i=1}^{p}(a_iX + b_iY + c_i)^{r_i}$ $\triangle$

La multiplicité $m = \mathrm{mult}_{(x,y)}(\mathcal{C})$ et les exposants $(r_i)_{1\leq i\leq p}$ caractérisent le type de la singularité du point (x,y) de la courbe $\mathcal{C}$. La singularité est ordinaire si l'on a $r_i = 1$ pour $1 \leq i \leq p$. Pour un point double ($\mathrm{mult}_{(x,y)}(\mathcal{C}) = 2$), on a $p = 2$ et $r_1 = r_2 = 1$ (point double ordinaire ou *node*) ou bien $p = 1$ et $r_1 = 2$ (point de rebroussement ou *cusp*).

Proposition 5
Soient $f, g \in A[X_1, \cdots, X_r, Y]$ avec $m = \deg(f)$ et $n = \deg(g)$; on a

$$R_Y(f,g) \in A[X_1, \cdots, X_r] \text{ et } \deg(R_Y(f,g)) \leq m\,n$$

$\triangledown$ On a $f = \sum_{i=0}^{m} f_iY^i$ et $g = \sum_{j=0}^{n} g_jY^j$ avec $f_i, g_j \in A[X_1, \cdots, X_r]$ et

$$\deg(f_i) \leq m - i \text{ pour } 0 \leq i \leq m \text{ et } \deg(g_j) \leq n - j \text{ pour } 0 \leq j \leq n$$

Le résultant

$$R_X(f,g) = \det(S_X^{m,n}(f,g))$$

est le déterminant de la matrice de Sylvester $S_X^{m,n}(f,g) = (S_{i,j})_{1\leq i,j\leq m+n}$:

- $\star$ pour $1 \leq j \leq n$:
  $\begin{cases} S_{j+i,j} = f_{m-i} \text{ pour } 0 \leq i \leq m \\ S_{k,j} = 0 \text{ pour } k \notin [j, m+j] \end{cases}$
- $\star$ pour $1 \leq i \leq m$:
  $\begin{cases} S_{i+j,n+i} = g_{n-j} \text{ pour } 0 \leq j \leq n \\ S_{k,n+i} = 0 \text{ pour } k \notin [i, n+i] \end{cases}$

On a ainsi :

$$S_X^{m,n}(f,g) = \begin{pmatrix} f_m & 0 & 0 & \cdots & 0 & g_n & 0 & \cdots & 0 \\ f_{m-1} & f_m & \vdots & & & g_{n-1} & g_n & & \vdots \\ \vdots & f_{m-1} & f_m & & & & g_{n-1} & & 0 \\ & \vdots & f_{m-1} & & 0 & \vdots & & & g_n \\ f_0 & & \vdots & & f_m & & \vdots & & g_{n-1} \\ 0 & f_0 & & \ddots & f_{m-1} & g_0 & & \ddots & \\ \vdots & 0 & f_0 & & \vdots & 0 & g_0 & & \vdots \\ & & 0 & & & \vdots & 0 & & \\ 0 & & & & f_0 & 0 & & & g_0 \end{pmatrix}$$

On a alors, en utilisant la *formule de Leibniz* :

$$R_Y(f,g) = \sum_{\sigma\in\mathfrak{S}_{m+n}} S_{\sigma(1),1}\cdots S_{\sigma(j),j}\cdots S_{\sigma(n),n}S_{\sigma(n+1),n+1}\cdots S_{\sigma(n+i),i}\cdots S_{\sigma(m+n),m+n}$$

Considérons alors un *terme non-nul* de cette somme :

$$\mathcal{T} = S_{\sigma(1),1}\cdots S_{\sigma(j),j}\cdots S_{\sigma(n),n}S_{\sigma(n+1),n+1}\cdots S_{\sigma(n+i),i}\cdots S_{\sigma(m+n),m+n}$$

La permutation $\sigma\in\mathfrak{S}_{m+n}$ vérifie nécessairement :

$$\left\{\begin{array}{l} j\leq\sigma(j)\leq m+j \text{ pour } 1\leq j\leq n \\ i\leq\sigma(n+i)\leq n+i \text{ pour } 1\leq i\leq m\end{array}\right.$$

de sorte que l'on a :

$$\left\{\begin{array}{l} S_{\sigma(j),j} = f_{m-\sigma(j)+j} \text{ pour } 1\leq j\leq n \\ S_{\sigma(n+i),i} = g_{n-\sigma(n+i)+i} \text{ pour } 1\leq i\leq m\end{array}\right.$$

Puisque $\mathcal{T}\neq 0$ on a :

$$\begin{array}{rcl}
\deg(\mathcal{T}) & = & \displaystyle\sum_{j=1}^{n}\deg(f_{m-\sigma(j)+j}) + \sum_{i=1}^{m}\deg(g_{n-\sigma(n+i)+i}) \\
& \leq & \displaystyle\sum_{j=1}^{n}(\sigma(j)-j) + \sum_{i=1}^{m}(\sigma(n+i)-i) \\
& = & \displaystyle\left(\sum_{j=1}^{n}\sigma(j) + \sum_{i=1}^{m}\sigma(n+i)\right) - \left(\sum_{j=1}^{n}j + \sum_{i=1}^{m}i\right) \\
& = & \displaystyle\sum_{k=1}^{m+n}k - \left(\sum_{j=1}^{n}j + \sum_{i=1}^{m}i\right) \\
& = & \displaystyle\frac{(m+n)(m+n-1)}{2} - \frac{n(n-1)}{2} - \frac{m(m-1)}{2} \\
& = & m\,n
\end{array}$$

$\triangle$

Remarque : Si les polynômes f et g sont *homogènes* de degrés respectifs m et n , le polynôme $R_Y(f,g)$ est *homogène* de degré $m\,n$.

$\triangledown$ On a $\deg(f_i) = m-i$ pour $0\leq i\leq m$ et $\deg(g_j) = n-j$ pour $0\leq j\leq n$ Il en résulte que pour tout *terme non-nul* $\mathcal{T} = S_{\sigma(1),1}\cdots S_{\sigma(j),j}\cdots S_{\sigma(n),n}S_{\sigma(n+1),n+1}\cdots S_{\sigma(n+i),i}\cdots S_{\sigma(m+n),m+n}$ dans la formule de Leibniz on a $\deg(\mathcal{T}) = m\,n$ $\triangle$

Proposition 6 (forme faible du théorème de Bezout)
Soient $\mathcal{C}$ et $\mathcal{D}$ deux courbes algébriques planes affines irréductibles distinctes ; alors $\mathcal{C}\cap\mathcal{D}$ est un ensemble fini et l'on a :

$$\mathrm{Card}(\mathcal{C}\cap\mathcal{D}) \leq \deg(\mathcal{C})\deg(\mathcal{D})$$

$\triangledown$ On a $\mathcal{C} = Z(f)$ et $\mathcal{D} = Z(g)$ avec $f,g\in K[X]$ *non associés* et *irréductibles* dans $\mathbb{C}[X,Y]$. Quitte à appliquer une transformation du type φ_c on peut supposer que [15]

$$f = a_m\,Y^m + a_{m-1}(X)Y^{m-1} + \cdots + a_0(X)$$

15. puisque $\widetilde{\varphi_c}^{-1}(Z(f)\cap Z(g)) = Z(\varphi_c(f),\varphi_c(g))$.

$$g = b_n\, Y^n + b_{n-1}(X)Y^{n-1} + \cdots + b_0(X)$$

avec $a_m, b_n \in \mathbb{C}^*$ et $a_0(X), \cdots, a_{m-1}(X), b_0(X), \cdots, b_{n-1}(X) \in \mathbb{C}[X]$ avec $m, n \geq 1$.
Par ailleurs [16] les racines x du résultant $R = R_Y(f, g)$ sont les abscisses des points d'intersection $(x, y) \in \mathcal{C} \cap \mathcal{D}$ et pour un tel x, les ordonnées de ces points d'intersection sont les racines du polynôme $\text{pgcd}(f(x, Y), g(x, Y)) \in \mathbb{C}[Y]$ de sorte que $\mathcal{C} \cap \mathcal{D}$ est un ensemble fini [17]. On a ainsi :

$$\mathcal{C} \cap \mathcal{D} = \{(x_i, y_i) \,/\, 1 \leq i \leq N\}$$

Soit $c \in \mathbb{C}^\star$; on a :

$$\widetilde{\varphi_c}^{-1}(\mathcal{C} \cap \mathcal{D}) = \{(x_i + c\, y_i, y_i) \,/\, 1 \leq i \leq N\} = Z(\varphi_c(f), \varphi_c(g))$$

et on peut choisir c de sorte que les polynômes $\varphi_c(f)$ et $\varphi_c(g)$ soient quasi-unitaires en Y et les $x_i + c\, y_i$ pour $1 \leq i \leq N$ deux à deux distincts. Si $x_i = x_j$ on a $y_i \neq y_j$ de sorte que $x_i + c\, y_i \neq x_j + c\, y_j$ pour tout $c \neq 0$. Si $x_i \neq x_j$ et $y_i = y_j$ on a encore $x_i + c\, y_i \neq x_j + c\, y_j$ pour tout $c \neq 0$. Il suffit alors de prendre c distinct des $-\dfrac{y_j - y_i}{x_j - x - i}$ et tel que les polynômes $\varphi_c(f)$ et $\varphi_c(g)$ soient quasi-unitaires en Y. On a alors :

$$N = \text{Card}(\mathcal{C} \cap \mathcal{D}) = \deg(R_Y(\varphi_c(f), \varphi_c(g))) \leq \deg(\varphi_c(f))\deg(\varphi_c(g)) = \deg(f)\deg(g)$$

$\triangle$

16. *cf.* le théorème d'élimination de Kronecker
17. on a $R \in \langle f, g\rangle \cap K[X]$ et de même $R_X(f, g) \in \langle f, g\rangle \cap K[Y]$ de sorte que $\mathcal{C} \cap \mathcal{D} = Z(f, g)$ est fini.