Résultants : des matrices pour l'élimination

Laurent Busé

Résultants: des matrices pour l'élimination

Laurent Busé,
INRIA Sophia-Antipolis Méditerrannée,
Laurent.Buse@sophia.inria.fr

Notes de cours pour les Journées Nationales du Calcul Formel 2008
20-24 octobre 2008

Table des matières

Introduction

Ce cours est divisé en trois parties. La première partie traite du résultant bien connu de deux polynômes univariés, très souvent appelé résultant de Sylvester. L'objectif principal est ici d'illustrer le contenu géométrique du résultant au travers d'applications concrètes en géométrie et modélisation algébrique : théorème de Bézout, problèmes d'inversion et d'implicitation d'une courbe plane rationelle. Notamment, l'accent sera mis sur deux propriétés fondamentales du résultant qui le distinguent des autres techniques d'élimination : son caractère universel et ses représentations matricielles.

La deuxième partie est consacrée à la généralisation du résultant de Sylvester au cas de n polynômes homogènes en n variables, souvent appelé résultant de Macaulay. Après une brève introduction sur le théorème de l'élimination, l'existence et les principales propriétés de ce résultant seront présentées sous l'angle le plus adapté au calcul : les formes d'inerties. Pour finir, on présentera la formule de Poisson que l'on illustrera par quelques applications géométriques.

La dernière partie propose une discussion plus avancée sur l'existence générale des résultants. On montrera qu'il est (presque) toujours possible de donner une définition géométrique pour le résultant d'un système algébrique bien dimensionné. En revanche, il est plus délicat de pouvoir le "calculer", c'est-à-dire d'en trouver une représentation matricielle. En fait, ce calcul nécessite une étude approfondie qui doit bien souvent être menée au cas par cas. Nous l'illustrerons au travers d'un exemple concret.

Dans la suite, tous les anneaux seront supposés commutatifs et unitaires.

Chapitre 1

Le cas d'une variable

Dans cette première partie, le résultant de deux polynômes univariés est introduit puis illustré dans deux contextes. Tout d'abord le calcul le l'intersection de deux courbes planes puis les deux problèmes d'implicitation et d'inversion d'une paramétrisation d'une courbe algébrique plane. L'objectif est ici de souligner que la représentation matricielle et le caractère universel du résultant sont deux propriétés fortes du résultant comme outil pour l'élimination.

1.1 Définition et propriétés élémentaires

Soit A un anneau commutatif unitaire. Considérons les deux polynômes de $A[X]$

$$\left\{ \begin{array}{rcl} f(X) & := & a_0X^m + a_1X^{m-1} + \cdots + a_m \\ g(X) & := & b_0X^n + b_1X^{n-1} + \cdots + b_n \end{array} \right. \tag{1.1}$$

où m et n sont deux entiers positifs tels que $(m,n) \neq (0,0)$. On leur associe la matrice suivante, dite matrice de Sylvester,

$$S_{m,n}(f,g) := \begin{pmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & 0 \\ a_1 & a_0 & & \vdots & b_1 & \ddots & 0 \\ \vdots & & \ddots & 0 & \vdots & & b_0 \\ a_m & & & a_0 & b_{n-1} & & b_1 \\ 0 & a_m & & a_1 & b_n & & \vdots \\ \vdots & & \ddots & \vdots & 0 & \ddots & b_{n-1} \\ 0 & \cdots & 0 & a_m & 0 & 0 & b_n \end{pmatrix}.$$

C'est une matrice carrée de taille $(m+n) \times (m+n)$; ses n premières colonnes ne dépendent que des coefficients du polynôme f et ses m dernières colonnes que des coefficients du polynôme g.

Définition 1.1.1 *On définit le résultant des polynômes $f(X)$ et $g(X)$ en degré (m,n), et nous le noterons $\mathrm{Res}_{m,n}(f,g)$, comme le déterminant de la matrice de Sylvester $S_{m,n}(f,g)$.*

De cette définition, on tire facilement que si $m > 0$ (resp. $n > 0$) alors $\mathrm{Res}_{m,0}(f,b_0) = b_0^m$ (resp. $\mathrm{Res}_{0,n}(a_0,g) = a_0^n$). Il faut aussi remarquer l'impact du choix des entiers (m,n) : par exemple, si $b_0 = 0$, c'est-à-dire si g est en fait un polynôme de degré $n-1$ et non n, alors

$$\mathrm{Res}_{m,n}(f,g) = a_0\mathrm{Res}_{m,n-1}(f,g).$$

Plus généralement, si $\deg(f) = m$ et $n \geq \deg(g)$ alors

$$\mathrm{Res}_{m,n}(f,g) = a_0^{n-\deg(g)}\mathrm{Res}_{m,n-\deg(g)}(f,g),$$

ce qui se voit en développant le déterminant de la matrice de Sylvester suivant la première ligne itérativement.

Exemple 1.1.1 *Si* $f := aX^2 + bX + c$ *et* $g = \partial_X f = 2aX + b$ *alors*

$$\mathrm{Res}_{2,1}(f,g) = \begin{vmatrix} a & 2a & 0 \\ b & b & 2a \\ c & 0 & b \end{vmatrix} = (-a)(b^2 - 4ac).$$

Exemple 1.1.2 *Si* $f = a_0X^m + \cdots + a_m$ *et* $g = X - b$ *alors*

$$\mathrm{Res}_{m,1}(f,g) = \begin{vmatrix} a_0 & 1 & 0 & \cdots & 0 \\ a_1 & -b & 1 & & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & -b & 1 \\ a_m & 0 & \cdots & 0 & -b \end{vmatrix} = (-1)^m f(b)$$

(développer ce déterminant suivant la première colonne).

Proposition 1.1.2 *Soient* $f, g \in A[X]$ *définis par* (1.1). *Alors* $\mathrm{Res}_{m,n}(f,g) = (-1)^{mn}\mathrm{Res}_{n,m}(g,f)$.

Preuve. On passe de la matrice $S_{m,n}(f,g)$ à la matrice $S_{n,m}(g,f)$ par mn transpositions de colonnes. □

Dans la suite, nous noterons classiquement $A[X]_{<n}$ l'ensemble des polynômes de $A[X]$ de degré strictement plus petit que n et $A[X]_{\leq n}$ l'ensemble des polynômes de $A[X]$ de degré plus petit ou égal à n.

Proposition 1.1.3 *Soient* $f, g \in A[X]$ *définis par* (1.1). *Alors il existe deux autres polynômes* $U \in A[X]_{<n}$ *et* $V \in A[X]_{<m}$ *tels que l'on ait l'égalité*

$$\mathrm{Res}_{m,n}(f,g) = Uf + Vg$$

dans $A[X]$. *En particulier,* $\mathrm{Res}_{m,n}(f,g) \in (f,g) \subset A[X]$.

Preuve. Il est immédiat de constater que l'on a l'égalité

$${}^tS_{m,n}(f,g) \begin{pmatrix} X^{m+n-1} \\ X^{m+n-2} \\ \vdots \\ X \\ 1 \end{pmatrix} = \begin{pmatrix} X^{n-1}f \\ \vdots \\ Xf \\ f \\ X^{m-1}g \\ \vdots \\ Xg \\ g \end{pmatrix} \tag{1.2}$$

dans $A[X]$. Par conséquent, les régles de Cramer montrent que

$$\det(S_{m,n}(f,g)).1 = \det \begin{pmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & 0 \\ a_1 & a_0 & & \vdots & b_1 & \ddots & 0 \\ \vdots & & \ddots & 0 & \vdots & & b_0 \\ a_m & & & a_0 & b_{n-1} & & b_1 \\ 0 & a_m & & a_1 & b_n & & \vdots \\ \vdots & & \ddots & \vdots & 0 & \ddots & b_{n-1} \\ X^{n-1}f & \cdots & Xf & f & X^{m-1}g & \cdots & g \end{pmatrix},$$

d'où le résultat annoncé en développant ce dernier déterminant suivant sa dernière ligne. Noter que l'on peut voir ce même résultat en utilisant l'invariance du déterminant lorsque l'on ajoute à la dernière ligne

de la matrice $S_{m,n}(f,g)$ la $i^{\text{ème}}$ ligne multipliée par X^{m+n-i}, cela pour tout $i = 1, \ldots, m+n-1$. □

L'égalité (1.2) peut s'interpréter comme suit : les polynômes f et g définissent un morphisme de $A[X]$-modules libres

$$A[X] \oplus A[X] \to A[X] : u \oplus v \mapsto uf + vg$$

qui induit, en bornant judicieusement les degrés des polynômes u et v, un morphisme de A-modules libres

$$\phi : A[X]_{<n} \times A[X]_{<m} \to A[X]_{<m+n} : (u,v) \mapsto uf + vg.$$

On constate alors que la matrice de l'application A-linéaire ϕ dans les bases

$$\{(X^{n-1},0),(X^{n-2},0),\ldots,(X,0),(1,0),(0,X^{m-1}),\ldots,(0,X),(0,1)\} \text{ et } \{X^{m+n-1},\ldots,X,1\} \quad (1.3)$$

n'est autre que la matrice de Sylvester $S_{m,n}(f,g)$. La proposition 1.1.3 revient donc à dire que $\mathrm{Res}_{m,n}(f,g)$ appartient à l'image de ϕ, ce que l'on voit facilement en multipliant l'égalité classique ($\mathrm{cof}(-)$ désigne ici la matrice des cofacteurs)

$$S_{m,n}(f,g).{}^t\mathrm{cof}(S_{m,n}(f,g)) = \mathrm{Res}_{m,n}(f,g).\mathrm{Id}_{m+n}$$

par le vecteur colonne ${}^t(0 \cdots 0\,1)$ de taille $m+n$; le résultant est alors obtenu comme l'image par ϕ de l'élément

$${}^t\mathrm{cof}(\mathrm{S_{m,n}(f,g)}) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \in A[X]_{<n} \times A[X]_{<m}.$$

Proposition 1.1.4 *Supposons que A soit un anneau intègre et notons $K := \mathrm{Frac}(A)$ son corps des fractions. Soient f et g deux polynômes de $A[X]$ définis par* (1.1) *et tels que $a_0 \neq 0$. Alors, les assertions suivantes sont équivalentes :*

(i) *ϕ est injective,*
(ii) *$\mathrm{Res}_{m,n}(f,g) \neq 0$,*
(iii) *$f(X)$ et $g(X)$ sont premiers entre eux dans $K[X]$.*

Preuve. L'équivalence entre les points (i) et (ii) résulte de la propriété plus générale suivante : soit $\varphi : A^r \to A^r$ un morphisme de A-modules, B et B' deux bases de A^r et M la matrice de φ dans ces bases. Alors φ est injective si et seulement si $\det(M) \neq 0$. Montrons-le. Soit $x \in A^r$ tel que $\varphi(x) = 0$. L'égalité dans A

$${}^t\mathrm{cof}(M).M = \det(M)\mathrm{Id}$$

implique alors que $\det(M)x = 0$ et donc $x = 0$ si $\det(M) \neq 0$ puisque A est intègre. Inversement, supposons maintenant que $\det(M) = 0$ et voyons M comme une matrice à coefficients dans le corps K. Il existe alors un vecteur non nul y tel que $My = 0$. Soit b le produit des dénominateurs des entrées de y, alors $M.(by) = 0$ et by est un vecteur non nul à entrées dans A. Il s'en suit que φ n'est pas injective.

Montrons à présent que (i) est équivalent à (iii). Supposons que f et g soient premiers entre eux dans $K[X]$ et soit $(u,v) \in A[X]_{<n} \times A[X]_{<m}$ tel que $\phi(u,v) = uf + vg = 0$. Alors $uf = -vg$ d'où l'on déduit que g divise u et f divise v. Vus les degrés de ces polynômes, on déduit que $u = v = 0$. Maintenant, si f et g ne sont pas premiers entre eux dans $K[X]$ alors il existe $h \in K[X]$ de degré strictement positif tel que $f = hf_1$ et $g = hg_1$. Si d désigne le produit des dénominateurs des coefficients des polynômes f_1 et g_1 on vérifie alors que $d(gf - fg) = h(dg_1 f - df_1 g) = 0$ qui montre que ϕ n'est pas injective puisque $\phi(dg_1, -df_1) = 0$. □

Corollaire 1.1.5 *Supposons que A soit un anneau intègre et que $f, g \in A[X]$ soient définis par* (1.1). *Alors $\mathrm{Res}_{m,n}(f,g) = 0$ si et seulement si f et g possèdent une racine commune dans une extension*[1] *du corps K des fractions de A, ou bien $a_0 = b_0 = 0$.*

[1] Une extension L du corps K est une K-algèbre qui est un corps. Autrement dit, L est un corps et K est un sous-corps de L.

Preuve. Il résulte de la définition du résultant que celui-ci reste inchangé si l'on voit les polynômes f et g dans $A[X]$, $K[X]$ ou bien $L[X]$ où L est une extension quelconque de K. Prenant pour L une extension de K pour laquelle f et g se scindent (par exemple la clotûre algébrique de K), les propositions 1.1.2 et 1.1.4 nous donnent ce corollaire si $a_0 \neq 0$ ou $b_0 \neq 0$. Si $a_0 = b_0 = 0$ il est clair que le résultant est nul. □

Exercice 1.1.1 *Soient $f(X)$ et $g(X)$ définis par (1.1). Si A est un corps et si $(a_0, b_0) \neq (0, 0)$ alors montrer que $\dim_A \ker S_{m,n}(f, g) = \deg \operatorname{pgcd}(f, g)$.*

Exercice 1.1.2 *Soit K un corps infini. Montrer que la propriété d'être premier entre eux pour deux polynômes $f, g \in K[X]$ est une propriété ouverte dans l'espace des coefficients de ces polynômes. En particulier, si $f, g \in K[X]$ sont premiers entre eux alors une "petite" perturbation de leurs coefficients les conserve premiers entre eux.*

Le cadre homogène : Soient f et g définis par (1.1). Introduisant un nouvelle indéterminée Y, on définit les polynômes *homogènes* associés à f et à g de degré m et n respectivement comme

$$\begin{cases} F(X,Y) & := & a_0X^m + a_1X^{m-1}Y + \cdots + a_mY^m \\ G(X,Y) & := & b_0X^n + b_1X^{n-1}Y + \cdots + b_nY^n \end{cases} \tag{1.4}$$

Leur résultant, noté $\operatorname{Res}(F, G)$, est défini comme $\operatorname{Res}_{m,n}(f, g)$. Noter qu'il n'y a plus d'ambiguité sur les degrés pour définir les résultant de deux polynômes homogènes en deux variables puisque leur degré ne varie pas suivant les valeurs que l'on donne aux coefficients a_i et b_j (contrairement au degré de f et de g). Le corollaire 1.1.5 peut maintenant s'énoncer comme

$$\operatorname{Res}(F, G) = 0 \Longleftrightarrow F \text{ et } G \text{ possèdent une racine commune dans } \mathbb{P}^1_L$$

où L désigne la clotûre algébrique du corps K des fractions de A.

Le caractère universel du résultant : Une des propriétés fondamentale du résultant est que cet objet est *universel*, ce qui découle immédiatement de sa définition. Plus précisemment, considérant les coefficients des polynômes f et g définis par (1.1) comme des variables, on peut construire une application, dite de spécialisation,

$$\rho : \mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_n] \to A : a_i \mapsto a_i, b_j \mapsto b_j,$$

qui envoie les *variables* a_i et b_j de l'anneau $\mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_n]$ appelé anneau universel des coefficients de f et g, sur les *coefficients* correspondants a_i et b_j qui sont des éléments dans l'anneau commutatif A (rappelons qu'il existe toujours un morphisme d'anneaux de $\mathbb{Z}$ dans A et qu'il est unique). Ainsi $\operatorname{Res}_{m,n}(f, g) \in A$ est l'image par ρ du résultant de f et de g vu comme polynômes dans l'anneau $\mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_n][X]$, i.e. du résultant $\operatorname{Res}_{m,n}(f, g) \in \mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_n][X]$. On résume cette propriété en disant que le résultant est un polynôme universel. On peut ainsi considérer le résultant comme une "fonction" des variables $a_0, \ldots, a_m, b_0, \ldots, b_n$, ce qui justifie la notation $\operatorname{Res}_{m,n}(f, g)$ puisque les polynômes f et g fournissent des instances de ces variables. Une conséquence importante du caractère universel du résultant est qu'il suffit bien souvent de montrer une propriété ou une formule dans le cadre universel, c'est-à-dire en supposant que A est l'anneau $\mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_n]$ (l'intérêt étant que ce dernier est alors un anneau factoriel), pour l'obtenir immédiatement sur n'importe quel anneau commutatif par spécialisation, c'est-à-dire en transportant cette propriété ou cette formule par la spécialisation ρ. On commencera donc souvent les preuves dans ce qui suit par une phrase du type : "Par spécialisation, on se ramène au cas où A est l'anneau universel des coefficients de f et de g".

Pour un traitement complet et détaillé de la théorie du résultant de deux polynômes univariés nous renvoyons le lecteur au livre [AJ06].

1.2 Quelques propriétés formelles

"L'expérience prouve qu'il ne sert à rien de connaître le résultant si l'on ne possède pas suffisamment de règles de calcul ..." (Nicolas Bourbaki).

Ci-après, A désigne toujours un anneau commutatif unitaire et f, g les polynômes définis par (1.1).

1.2.1 Homogénéité

Pour tout $a \in A$ on a $\mathrm{Res}_{m,n}(af, g) = a^n \mathrm{Res}_{m,n}(f, g)$ *et* $\mathrm{Res}_{m,n}(f, ag) = a^m \mathrm{Res}_{m,n}(f, g)$.

Preuve. C'est immédiat à partir de la définition du résultant comme déterminant de la matrice de Sylvester. □

Prenant pour anneau de base A l'anneau universel des coefficients de f et de g, c'est-à-dire $A := \mathbb{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m]$, alors $\mathrm{Res}_{m,n}(f, g)$ est homogène de degré n en les variables $a_0, \ldots, a_m$ (toutes affectées du poids 1) et de degré m en les variables $b_0, \ldots, b_n$ (toutes affectées du poids 1). Cela peut également se traduire par les égalités

$$\sum_{i=0}^{m} a_i \frac{\partial \mathrm{Res}_{m,n}(f,g)}{\partial a_i} = m\mathrm{Res}_{m,n}(f,g) \quad \text{et} \quad \sum_{i=0}^{n} b_i \frac{\partial \mathrm{Res}_{m,n}(f,g)}{\partial b_i} = n\mathrm{Res}_{m,n}(f,g).$$

1.2.2 Formule de Poisson

Supposons que a_0 soit inversible dans A et considérons le morphisme de multiplication par g dans l'anneau quotient[2] $A[X]/(f)$

$$\psi : A[X]/(f) \to A[X]/(f) : \overline{u} \mapsto \overline{ug}.$$

Alors le déterminant de la matrice de ψ est égal à $a_0^{-n}\mathrm{Res}_{m,n}(f, g)$.

Preuve. Considérons les deux morphismes de A-modules suivants :

$$\phi : A[X]_{<n} \times A[X]_{<m} \to A[X]_{<m+n} : (u, v) \mapsto uf + vg$$

et

$$\theta : A[X]_{<m+n} \to A[X]_{<n} \times A[X]_{<m} : P \mapsto (Q, R)$$

où (Q, R) correspondent respectivement au quotient et au reste de la division euclidienne de P par f, i.e. $P = Qf + R$. Choisissant les bases (1.3) pour $A[X]_{<n} \times A[X]_{<m}$ et $A[X]_{<m+n}$, les matrices M_ϕ, M_θ et $M_{\theta\circ\phi}$ des applications respectives ϕ, θ et $\theta \circ \phi$ dans ces bases vérifient

$$\det(M_\phi)\det(M_\theta) = \det(M_{\theta\circ\phi}). \tag{1.5}$$

Puisque $M_\phi = S_{m,n}(f, g)$, il vient $\det(M_\phi) = \mathrm{Res}_{m,n}(f, g)$. De plus, on voit que les matrices M_θ et $M_{\theta\circ\phi}$ sont de la forme

$$M_\theta = \left(\begin{array}{ccc|ccc} a_0^{-1} & 0 & 0 & & & \\ & \ddots & 0 & & 0 & \\ & & a_0^{-1} & & & \\ \hline & & & 1 & 0 & 0 \\ & & & 0 & \ddots & 0 \\ & & & 0 & 0 & 1 \end{array}\right) \quad \text{et} \quad M_{\theta\circ\phi} = \left(\begin{array}{ccc|c} 1 & 0 & 0 & \\ 0 & \ddots & 0 & \\ 0 & 0 & 1 & \\ \hline 0 & \ldots & 0 & \\ \vdots & 0 & \vdots & M_\psi \\ 0 & \ldots & 0 & \end{array}\right).$$

Par conséquent, (1.5) donne la formule annoncée : $a_0^{-n}\mathrm{Res}_{m,n}(f, g) = \det(M_\psi)$. □

1.2.3 Multiplicativité

Soit $f(X) = a_0X^n + \cdots + a_n \in A[X]$ et supposons donnés deux polynômes $g_1(X)$ et $g_2(X)$ dans $A[X]$ tels que $\deg(g_1) \leq n_1$ *et* $\deg(g_2) \leq n_2$. *Alors on a l'égalité suivante dans A :*

$$\mathrm{Res}_{m,n_1+n_2}(f, g_1g_2) = \mathrm{Res}_{m,n_1}(f, g_1)\mathrm{Res}_{m,n_2}(f, g_2).$$

[2] Rappelons que puisque a_0 est inversible l'anneau quotient $A[X]/(f)$ est un A-module libre de base $\{\overline{X}^{m-1}, \ldots, \overline{1}\}$ par simple division euclidienne : tout polynôme $u(X) \in A[X]$ s'écrit de manière unique comme $u(X) = q(X)f(X) + r(X)$ avec $\deg(r(X)) < m$, et on a $\overline{u} = r(\overline{X})$.

Preuve. Par spécialisation, on se ramène à démontrer cette propriété dans le cas universel où

$$A := \mathbb{Z}[\mathrm{coeff}(f), \mathrm{coeff}(g_1), \mathrm{coeff}(g_2)]$$

On regarde les polynômes f, g_1 et g_2 dans l'anneau $A_{a_0}[X]$ où l'élément a_0 est inversible (on a une application canonique $A \to A_{a_0} : a \mapsto a/1$ qui est *injective* puisque A est sans torsion). Le diagramme suivant étant commutatif

$$\begin{array}{ccc} A_{a_0}[X]/(f) & \xrightarrow{\times g_1 g_2} & A_{a_0}[X]/(f) \\ & {\scriptstyle \times g_1} \searrow \quad \nearrow {\scriptstyle \times g_2} & \\ & A_{a_0}[X]/(f) & \end{array}$$

On déduit de la formule de Poisson 1.2.2, choisissant la base sur A appropriée pour $A[X]/(f)$, l'égalité

$$a_0^{-n_1-n_2}\mathrm{Res}_{m,n_1+n_2}(f, g_1g_2) = a_0^{-n_1}\mathrm{Res}_{m,n_1}(f, g_1)a_0^{-n_2}\mathrm{Res}_{m,n_2}(f, g_2).$$

L'élément a_0 n'étant pas diviseur de zéro dans A, l'égalité ci-dessus devient une égalité dans A après simplification par a_0, et fournit alors le résultat annoncé. □

1.2.4 Transformations élémentaires

Si $n \geq m$ (resp. $m \geq n$), alors pour tout polynôme $h \in A[X]_{\leq n-m}$ (resp. $h \in A[X]_{\leq m-n}$), on a l'égalité dans A

$$\mathrm{Res}_{m,n}(f, g + hf) = \mathrm{Res}_{m,n}(f, g) \quad (\text{resp. } \mathrm{Res}_{m,n}(f + hg, g) = \mathrm{Res}_{m,n}(f, g)).$$

Preuve. Traitons le cas où $n \geq m$, l'autre cas étant une conséquence de la proposition 1.1.2. Notant $h(X) := c_0X^{n-m} + \cdots + c_{n-m}$, pour tout $i \in \{0, \ldots, m-1\}$ on a

$$X^i(g + hf) = X^ig + c_0X^{n-(m-i)}f + \cdots + c_{n-m}X^{n-(n-i)}f.$$

Il est alors clair que la matrice $S_{m,n}(f, g + hf)$ est obtenue à partir de la matrice $S_{m,n}(f, g)$ par les opérations

$$\mathrm{Col}_{m+n-i} \leftarrow \mathrm{Col}_{m+n-i} + c_0\mathrm{Col}_{m-i} + \cdots + c_{n-m}C_{n-i}$$

pour tout $i \in \{0, \ldots, m-1\}$, où Col_j désigne la j^{th} colonne de la matrice $S_{m,n}(f, g)$. L'invariance du déterminant par de telles opérations donne la formule annoncée. □

1.2.5 Covariance

Supposons que $n = m$. Pour toute matrice $\varphi = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients dans l'anneau A, on a l'égalité suivante dans A :

$$\mathrm{Res}_{m,m}(af + bg, cf + dg) = \det(\varphi)^m\mathrm{Res}_{m,m}(f, g)$$

Preuve. Par spécialisation, on se ramène au cas générique où $A := \mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_n, a, b, c, d]$. Puisque pour tout $i \in \{0, \ldots, m-1\}$ on a trivialement $X^i(af + bg) = aX^if + bX^ig$ pour tout $a, b \in A$, on vérifie aisément que

$$S_{m,m}(af + bg, cf + dg) = S_{m,m}(f, g)\begin{pmatrix} a \times \mathrm{Id} & c \times \mathrm{Id} \\ b \times \mathrm{Id} & d \times \mathrm{Id} \end{pmatrix}$$

où Id désigne la matrice identité de taille $m \times m$. Le résultat découle alors des propriétés classiques du déterminant. En effet, on a

$$\det\begin{pmatrix} ab \times \mathrm{Id} & bc \times \mathrm{Id} \\ ab \times \mathrm{Id} & ad \times \mathrm{Id} \end{pmatrix} = a^mb^m \det\begin{pmatrix} a \times \mathrm{Id} & c \times \mathrm{Id} \\ b \times \mathrm{Id} & d \times \mathrm{Id} \end{pmatrix}$$

et

$$\det\begin{pmatrix} ab\times \mathrm{Id} & bc\times \mathrm{Id} \\ ab\times \mathrm{Id} & ad\times \mathrm{Id}\end{pmatrix} = \det\begin{pmatrix} ab\times \mathrm{Id} & bc\times \mathrm{Id} \\ 0 & (ad-bc)\times \mathrm{Id}\end{pmatrix} = a^m b^m (ad-bc)^m = a^m b^m \det(\varphi)^m.$$

On conclut alors en notant que a et b ne sont pas des diviseurs de zéro dans A. □

1.2.6 Invariance et changement de base

Supposons donnés deux polynômes $u(X)$ et $v(X)$ dans $A[X]$ de degré inférieur ou égal à un entier $d \geq 1$. Notant F et G les polynômes homogènes de degré respectifs m et n associés à f et à g, on a l'égalité dans A :

$$\mathrm{Res}_{md,nd}(F(u,v),G(u,v)) = \mathrm{Res}_{d,d}(u,v)^{mn}\mathrm{Res}_{m,n}(f,g)^d.$$

Le cas particulier $d=1$ donne la propriété dite d'*invariance* du résultant :

$$\mathrm{Res}_{m,n}(F(aX+b,cX+d),G(aX+b,cX+d)) = (ad-bc)^{mn}\mathrm{Res}_{m,n}(f,g) \tag{1.6}$$

pour tout a,b,c,d dans A.

Preuve. Par spécialisation, on se ramène à montrer le résultat dans le cas universel, c'est-à-dire dans le cas où $A := \mathbb{Z}[a_0,\dots,a_m,b_0,\dots,b_n,\mathrm{coeff}(u),\mathrm{coeff}(v)]$. On peut également supposer que $m \geq n$ en vertu de 1.1.2.

Nous procédons par récurrence sur $m+n$: les cas où $m=0$ ou $n=0$ se vérifient facilement et le cas $m=n=1$ n'est autre que la propriété de covariance 1.2.5. On suppose donc que $m \geq 1$, $n \geq 1$ et $m+n \geq 3$ (donc $m \geq 2$). Il existe alors un polynôme homogène $H(X,Y)$ de degré $m-1$ tel que

$$b_0F(X,Y) - a_0X^{m-n}G(X,Y) = YH(X,Y). \tag{1.7}$$

D'où le calcul

$$\begin{aligned}
\mathrm{Res}_{md,nd}(b_0F(u,v),G(u,v)) &= \mathrm{Res}_{md,nd}(vH(u,v),G(u,v)) && \text{par 1.2.4}\\
&= \mathrm{Res}_{d,nd}(v,G(u,v))\mathrm{Res}_{(m-1)d,nd}(H(u,v),G(u,v)) && \text{par 1.2.3}\\
&= \mathrm{Res}_{d,nd}(v,b_0u^n)\mathrm{Res}_{(m-1)d,nd}(H(u,v),G(u,v)) && \text{par 1.2.4}\\
&= b_0^d\mathrm{Res}_{d,d}(v,u)^n\mathrm{Res}_{(m-1)d,nd}(H(u,v),G(u,v)) && \text{par 1.2.1 et 1.2.4}\\
&= b_0^d\mathrm{Res}_{d,d}(v,u)^n\mathrm{Res}_{d,d}(u,v)^{(m-1)n}\mathrm{Res}(H,G)^d && \text{par récurrence}\\
&= (-1)^{nd^2}b_0^d\mathrm{Res}(H,G)^d\mathrm{Res}_{d,d}(u,v)^{mn} && \text{par prop. 1.1.2}\\
&= (-1)^{nd(d+1)}\mathrm{Res}(Y,G)^d\mathrm{Res}(H,G)^d\mathrm{Res}_{d,d}(u,v)^{mn} &&\\
&= \mathrm{Res}(YH,G)^d\mathrm{Res}_{d,d}(u,v)^{mn} && \text{par 1.2.3}\\
&= \mathrm{Res}(b_0F,G)^d\mathrm{Res}_{d,d}(u,v)^{mn} && \text{par 1.2.4 et (1.7).}
\end{aligned}$$

On conclut alors en notant que b_0 ne divise par zéro dans A, que

$$\mathrm{Res}_{md,nd}(b_0F(u,v),G(u,v)) = b_0^{nd}\mathrm{Res}_{md,nd}(F(u,v),G(u,v))$$

et que $\mathrm{Res}(b_0F,G)^d = b_0^{nd}\mathrm{Res}(F,G)$ en utilisant la propriété d'homogénéité 1.2.1. □

1.2.7 Expression en les racines

Supposons que f et g soient complètement scindés sur A, c'est-à-dire que l'on puisse écrire

$$f(x) := a_0\prod_{i=1}^{m}(X-\alpha_i) \quad et \quad g(x) := b_0\prod_{i=1}^{n}(X-\beta_i).$$

Alors, on a les égalités dans A :

$$\mathrm{Res}_{m,n}(f,g) = a_0^n b_0^m \prod_{\substack{1\le i\le m\\ 1\le j\le n}} (\alpha_i - \beta_j) = a_0^n \prod_{i=1}^{m} g(\alpha_i) = (-1)^{mn} b_0^m \prod_{i=1}^{n} f(\beta_i).$$

Preuve. La première et la troisième formules s'obtiennent comme suit :

$$\begin{aligned}
\mathrm{Res}_{m,n}(f,g) &= \mathrm{Res}_{m,n}(f, b_0 \prod_{i=1}^{n}(X-\beta_i)) \\
&= b_0^m \mathrm{Res}_{m,n}(f, \prod_{i=1}^{n}(X-\beta_i)) && \text{par 1.2.1} \\
&= b_0^m \prod_{i=1}^{n} \mathrm{Res}_{m,n}(f, X-\beta_i) && \text{par 1.2.3} \\
&= b_0^m \prod_{i=1}^{n} (-1)^m f(\beta_i) && \text{par l'exemple 1.1.2} \\
&= a_0^n b_0^m \prod_{j=1}^{n}\prod_{i=1}^{m} (\alpha_i - \beta_j).
\end{aligned}$$

Un calcul similaire en inversant le rôle joué par f et par g permet de montrer la dernière formule. □

1.2.8 Quasi-homogénéité

Dans le cas universel, i.e. $A = \mathbb{Z}[a_0, \dots, a_m, b_0, \dots, b_n]$, on gradue l'anneau A en posant

$$\begin{cases} \deg(p) = 0 & \text{pour tout } p \in \mathbb{Z}, \\ \deg(a_i) = i \quad (\text{resp. } m-i) & \text{pour tout } i = 0, \dots, m, \\ \deg(b_j) = j \quad (\text{resp. } n-j) & \text{pour tout } j = 0, \dots, n. \end{cases}$$

Alors, $\mathrm{Res}_{m,n}(f,g) \in A$ *est quasi-homogène (ou isobare) de degré* mn.

Preuve. C'est une conséquence de la propriété d'invariance (1.6) puisque l'on a

$$\mathrm{Res}(F(tX,Y), G(tX,Y)) = \mathrm{Res}(F(X,tY), G(X,tY)) = t^{mn}\mathrm{Res}_{m,n}(f,g),$$

où $F(X,Y)$ et $G(X,Y)$ sont les polynômes homogènes de degré m et n associés à $f(X)$ et $g(X)$ respectivement, comme définis dans (1.4).

Noter qu'une autre façon de le voir est de constater que d'après 1.2.7, $\mathrm{Res}_{m,n}(f,g)$ est homogène de degré mn en les racines de $f(X)$ et de $g(X)$ (il faut se placer dans une extension bien choisie), puis que les coefficients a_i et b_j sont eux-mêmes homogènes de degré i et j respectivement par rapport à ces mêmes racines. □

Remarquer que ce résultat d'homogénéité peut également se traduire par l'égalité

$$\sum_{i=0}^{m} i a_i \frac{\partial \mathrm{Res}_{m,n}(f,g)}{\partial a_i} + \sum_{j=0}^{n} j b_j \frac{\partial \mathrm{Res}_{m,n}(f,g)}{\partial b_j} = mn \mathrm{Res}_{m,n}(f,g).$$

Noter également que les propriétés d'homogénéités 1.2.1 et de quasi-homogénéités 1.2.8 du résultant implique que

$$\mathrm{Res}_{m,n}(f,g) = \sum_{\substack{i_0+i_1+\cdots+i_m=n\\ j_0+j_1+\cdots+j_n=m\\ i_1+2i_2+\cdots+mi_m+j_1+2j_2+\cdots+nj_n=mn}} c_{i_0,i_1,\dots,i_m,j_0,\dots,j_n} a_0^{i_0} a_1^{i_1} \dots a_m^{i_m} b_0^{j_0} b_1^{j_1} \dots b_n^{j_n}$$

où $c_{i_0,i_1,\dots,i_m,j_0,\dots,j_n} \in \mathbb{Z}$ pour tous les multi-indices $(i_0, i_1, \dots, i_m, j_0, \dots, j_n) \in \mathbb{N}^{m+n+2}$. Noter que la condition de quasi-homogénéité $mi_0 + (m-1)i_1 + \cdots + i_{m-1} + nj_0 + (n-1)j_1 + \cdots + j_{n-1} = mn$ est déjà contenue dans les trois conditions apparaissant dans la somme ci-dessus.

1.2.9 Matrice de Bézout

Soit A un anneau commutatif unitaire. Considérons les deux polynômes de $A[X]$

$$\left\{ \begin{array}{lcl} f(X) & := & a_0X^n + a_1X^{n-1} + \cdots + a_n \\ g(X) & := & b_0X^n + b_1X^{n-1} + \cdots + b_n \end{array} \right. \tag{1.8}$$

où n est un entier strictement positif. Nous avons vu que le déterminant de la matrice de Sylvester fournit, par définition, le résultant de f et de g. Nous allons à présent construire une autre matrice à partir des polynômes f et g qui permet également de calculer ce résultant.

Introduisons une nouvelle indéterminée Y. Il est clair que le polynôme $X - Y$ divise le polynôme $f(X)g(Y) - f(Y)g(X)$ de $A[X, Y]$. Plus précisemment, on a

$$f(X)g(Y) - f(Y)g(X) = (X - Y) \sum_{i,j=0}^{n-1} c_{i,j}X^iY^j$$

dans $A[X, Y]$, où les $c_{i,j}$ sont dans A.

Définition 1.2.1 *On appelle matrice de Bézout en degré n associée au couple de polynômes f, g de $A[X]_{\leq n}$ défini par* (1.8) *la matrice $n \times n$ à coefficients dans A*

$$\mathrm{Bez}_n(f, g) = \begin{pmatrix} c_{n-1,n-1} & c_{n-1,n-2} & \cdots & c_{n-1,1} & c_{n-1,0} \\ c_{n-2,n-1} & c_{n-2,n-2} & \cdots & c_{n-2,1} & c_{n-2,0} \\ \vdots & \vdots & & \vdots & \vdots \\ c_{1,n-1} & c_{1,n-2} & \cdots & c_{1,1} & c_{1,0} \\ c_{0,n-1} & c_{0,n-2} & \cdots & c_{0,1} & c_{0,0} \end{pmatrix}.$$

Voici une petite procédure Maple qui permet de former cette matrice (`var` ci-dessous désigne la variable à éliminer) :

```
Bez:= proc(f,g,n,var)
        local i,j,b,M;
        M:=matrix(n,n);
        b:=simplify((fsubs(var=_var,g)-gsubs(var=_var,f))/(var-_var));
        for i from 1 to n do
                for j from 1 to n do
                M[i,j]:=coeftayl(b,[var,_var]=[0,0],[n-i,n-j]);
                od;
        od;
RETURN(evalm(M));
end:
```

Par définition de la matrice de Bézout, on a les égalités dans $A[X, Y]$

$$\begin{pmatrix} X^{n-1} & \cdots & X & 1 \end{pmatrix} \mathrm{Bez}_n(f, g) \begin{pmatrix} Y^{n-1} \\ \vdots \\ Y \\ 1 \end{pmatrix} = \frac{f(X)g(Y) - f(Y)g(X)}{X - Y} = \sum_{i,j=0}^{n-1} c_{i,j}X^iY^j. \tag{1.9}$$

Proposition 1.2.2 *Soient f, g définis par* (1.8)*. Alors, la matrice* $\mathrm{Bez}_n(f, g)$ *est symétrique et est une fonction linéaire alternée de f et g, c'est-à-dire que l'on a les égalités*

$$\mathrm{Bez}_n(f, f) = 0,\ {}^t\mathrm{Bez}_n(f, g) = \mathrm{Bez}_n(f, g),\ \mathrm{Bez}_n(f, g) = -\mathrm{Bez}_n(g, f),$$

$$\mathrm{Bez}_n(af_1 + f_2, g) = a\mathrm{Bez}_n(f_1, g) + \mathrm{Bez}_n(f_2, g) \quad \textit{pour tout } a \in A.$$

Preuve. C'est immédiat sur la définition. □

Proposition 1.2.3 *Soient f, g définis par* (1.8)*. On a l'égalité dans A :*

$$\det(\mathrm{Bez}_n(f,g)) = (-1)^{\frac{n(n-1)}{2}} \mathrm{Res}_{n,n}(f,g).$$

Preuve. Par spécialisation, on se ramène à montrer le résultat dans le cas universel.

Notant J_n la matrice $n \times n$ dont les seules entrées non nulles sont les entrées de l'anti-diagonale qui valent 1, on a l'égalité matricielle :

$$S_{n,n}(f,g) \left(\begin{array}{c|c} 0 & J_n \\ \hline -J_n & 0 \end{array}\right) {}^t S_{n,n}(f,g) = \left(\begin{array}{c|c} 0 & \mathrm{Bez}_n(f,g) \\ \hline -\mathrm{Bez}_n(f,g) & 0 \end{array}\right). \tag{1.10}$$

Pour la vérifier, il suffit de multiplier les deux membres de cette égalité par $(X^{2n-1} \ \cdots \ X \ 1)$ à gauche et ${}^t(Y^{2n-1} \ \cdots \ Y \ 1)$ à droite ; on trouve alors dans les deux cas

$$(X^{n-1} + X^{n-1}Y + \cdots + Y^{n-1})(f(X)g(Y) - f(Y)g(X)) = \frac{X^n - Y^n}{X - Y}(f(X)g(Y) - f(Y)g(X)).$$

De la formule (1.10), on déduit immédiatement que $\mathrm{Res}_{n,n}(f,g)^2 = \det(\mathrm{Bez}_n(f,g))^2$, donc que $\mathrm{Res}_{n,n}(f,g)$ et $\det(\mathrm{Bez}_n(f,g))$ sont égaux au signe près. Pour déterminer ce signe on utilise la spécialisation $f \mapsto X^n, g \mapsto 1$: on a $\mathrm{Res}_{n,n}(X^n, 1) = 1$ et $\det(\mathrm{Bez}_n(X^n, 1)) = \det(\mathrm{J_n}) = (-1)^{\frac{n(n-1)}{2}}$. □

Remarque 1.2.4 *La conjonction des propositions 1.2.2 et 1.2.3 donnent directement la propriété de covariance 1.2.5 du résultant.*

Exercice 1.2.1 *Soient $f(X)$ et $g(X)$ définis par* (1.8) *tels que A soit un corps et $(f,g) \neq (0,0)$. Alors* $\dim_A(\ker \mathrm{Bez}_n(f,g)) = \deg(\mathrm{pgcd}(f,g))$.

1.3 Intersection de deux courbes algébriques planes

Étant donnés deux polynômes $f(x,y)$ et $g(x,y)$ dans $\mathbb{K}[x,y]$ où $\mathbb{K}$ est un corps algébriquement clos, on souhaite étudier et calculer leurs zéros communs. Ce problème s'interprète géométriquement : les polynômes f et g définissent deux courbes algébriques $\mathcal{C}_f := V(f)$ et $\mathcal{C}_g := V(g)$ dans le plan affine $\mathbb{A}^2$ (de coordonnées (x,y)) et l'on souhaite étudier leur intersection. Nous ne nous intéresserons qu'au cas où $f(x,y) = g(x,y) = 0$ possède un nombre fini de solutions, c'est-à-dire que les courbes $\mathcal{C}_f$ et $\mathcal{C}_g$ n'ont pas de composante courbe commune. Cette condition n'est pas vraiment restrictive puisqu'elle revient à demander que $f(x,y)$ et $g(x,y)$ soient des polynômes premiers entre eux dans $\mathbb{K}[x,y]$; noter que le plus grand diviseur commun à f et à g fournit toute la composante courbe commune à $\mathcal{C}_f$ et $\mathcal{C}_g$.

Un cas particulier. Le cas où l'une des deux courbes est une droite, c'est-à-dire où l'un des polynômes est de degré 1, se réduit à la résolution d'un polynôme univarié. En effet, on peut supposer que $g(x,y) = y$ et ainsi se ramener à un polynôme univarié $f(x,0) \neq 0 \in \mathbb{K}[x]$. On peut écrire

$$f(x,0) = c(x - z_1)^{\mu_1}(x - z_2)^{\mu_2} \cdots (x - z_s)^{\mu_s},$$

où les z_i sont les racines distinctes et $c \in \mathbb{K} \setminus \{0\}$. L'entier μ_i, pour $i = 1, \ldots, s$, qui est classiquement appelé la multiplicité de la racine z_i du polynôme $f(x,0) \in \mathbb{K}[x]$, est également appelé la *multiplicité d'intersection* entre les courbes $\mathcal{C}_f$ et $\mathcal{C}_g$ au point d'intersection de coordonnées $(z_i, 0) \in \mathbb{A}^2$. On a $\sum_{i=1}^s \mu_i = \deg_x(f(x,y))$ et on vérifie aisément que $\sum_{i=1}^s \mu_i = \deg(f(x,y))$ (degré en tant que polynôme en les deux variables x et y) si $f(x,y)$ ne s'annule pas au point à l'infini de l'axe des x, ou bien encore, de manière équivalente, si la partie homogène de plus haut degré de $f(x,y)$ n'est pas divisible par y. Cette dernière condition peut-être absorbée par la géométrie projective : introduisant une nouvelle variable t et notant $F(x,y,t)$ le polynôme homogénéisé de $f(x,y)$, on a alors

$$F(x,0,t) = c(x - z_1 t)^{\mu_1}(x - z_2 t)^{\mu_2} \cdots (x - z_s t)^{\mu_s} t^{\mu_\infty}, \tag{1.11}$$

où μ_∞ est un entier correspondant à la multiplicité de la racine à l'infini. Ainsi, on a toujours la relation

$$\mu_\infty + \sum_{i=1}^{s} \mu_i = \deg(F(x,y,t)) = \deg(f(x,y)). \tag{1.12}$$

Il est également possible de calculer les racines $z_1, \ldots, z_s$ ainsi que leur multiplicité par des calculs de valeurs et vecteurs propres. En effet, écrivant

$$f(x,0) = f_d x^d + f_{d-1} x^{d-1} + \cdots + f_1 x + f_0 \in \mathbb{K}[x]$$

(noter que $d := \deg(f(x,0)) = \sum_{i=1}^{s} \mu_i$ n'est pas forcément égal à $\deg(f(x,y))$ d'après la discussion précédente) et notant I l'idéal principal de $\mathbb{K}[x]$ engendré par ce polynôme $f(x,0)$, nous avons déjà rappelé que l'algèbre quotient $\mathbb{K}[x]/I$ est un espace vectoriel sur $\mathbb{K}$ de dimension d ayant pour base canonique $\{1, x, \ldots, x^{d-1}\}$. Considérons l'endomorphisme $M_x : \mathbb{K}[x]/I \xrightarrow{\times x} \mathbb{K}[x]/I$ de multiplication par x dans $\mathbb{K}[x]/I$. Il est immédiat de constater que sa matice dans la base canonique est

$$\begin{bmatrix} 0 & \cdots & 0 & -f_0/f_d \\ 1 & \ddots & & \vdots \\ \vdots & & 0 & \vdots \\ 0 & & 1 & -f_{d-1}/f_d \end{bmatrix},$$

(la colonne la plus à droite correspond à la division euclidienne de x^d par $f(x,0)$) et donc que le polynôme caractéristique de M_x est exactement $\frac{(-1)^d}{f_d} f(x)$. Les racines du polynôme $f(x,0)$ avec multiplicité correspondent donc aux valeurs propres avec multiplicité de l'endomorphisme M_x.

Dans ce qui suit, nous allons généraliser ces calculs au cas où $f(x,y)$ et $g(x,y)$ ont des degrés arbitraires.

1.3.1 Le théorème de Bézout

Dans tout ce paragraphe, $\mathbb{K}$ désigne un corps algébriquement clos et on suppose donnés deux polynômes non constants $f(x,y)$ et $g(x,y)$ de $\mathbb{K}[x,y]$. Introduisant une nouvelle indéterminée z, on note $F(x,y,z)$, respectivement $G(x,y,z)$, le polynôme homogénéisé de $f(x,y)$, respectivement de $g(x,y)$, de même degré.

Théorème 1.3.1 (Bézout homogène) *Si les polynômes $F(x,y,z)$ et $G(x,y,z)$ sont premiers entre eux dans $\mathbb{K}[x,y,z]$ alors les courbes algébriques $V(F)$ et $V(G)$ se coupent en un nombre fini de points, plus précisément en $\deg(F)\deg(G)$ points comptés avec une multiplicité appropriée.*

Preuve. Considérons les polynômes F et G comme des polynômes en y à coefficients (homogènes) dans $\mathbb{K}[x,z]$:

$$\begin{cases} F(x,y,z) &= a_0(x,z)y^m + a_1(x,z)y^{m-1} + \cdots + a_{m-1}(x,z)y + a_m(x,z) \\ G(x,y,z) &= b_0(x,z)y^n + b_1(x,z)y^{n-1} + \cdots + b_{n-1}(x,z)y + b_n(x,z) \end{cases} \tag{1.13}$$

où $a_i(x,z) \in \mathbb{K}[x,z]$ est homogène pour $i = 0, \ldots, m$ avec $a_0(x,z) \neq 0$, et $b_j(x,z) \in \mathbb{K}[x,z]$ est homogène pour $j = 0, \ldots, n$ avec $b_0(x,z) \neq 0$. Par changement de coordonnées projective (changement qui laisse invariant la propriété de finitude ou non de $V(F) \cap V(G)$) suffisamment général (rappelons que $\mathbb{K}$ est infini car algébriquement clos) on peut supposer que

($\star$) le point $\infty_y := (0:1:0)$ n'appartient pas à $V(F) \cup V(G) \subset \mathbb{P}^2$.

Cela implique que $a_0(0,0)$ $b_0(0,0)$ sont tous les deux non nuls et donc que $a_0(x,z)$ et $b_0(x,z)$ sont des *constantes non nulles*. Ainsi, puisque F et G sont premiers entre eux, le résultant $\mathrm{Res}_{m,n}(F,G) \in \mathbb{K}[x,z]$ est un polynôme homogène *non nul* par la proposition[3] 1.1.4. Maintenant, si $(x_0 : y_0 : z_0)$ est un point

[3] Il faut ici utiliser un corollaire très classique du lemme de Gauss (voir, par exemple, [Lan02, chap. IV, §2]), que nous rappelons rapidement.

Soit A un anneau factoriel et $K := \mathrm{Frac(A)}$ son corps des fractions. Tout polynôme $f(X) \in K[X]$ peut s'écrire $cf_1(X)$ où $c \in K$ et $f_1(X) \in A[X]$ est primitif (i.e. le pgcd de ses coefficients vaut 1), et on a le résultat suivant : si un polynôme $f(X) \in A[X]$ admet une factorisation $g(X)h(X)$ dans $K[X]$, alors $f(X) = af_1(X)g_1(X)$ où $a \in K$.

de $V(F) \cap V(G)$ alors $(x_0 : z_0)$ est une racine de $\mathrm{Res}_{m,n}(F,G)$ d'après le corollaire 1.1.5 ; puisque ce résultant n'admet qu'un nombre fini de racines, il ne peut donc y avoir qu'un nombre fini de points dans $V(F) \cap V(G)$.

Comptons à présent le nombre de points dans $V(F) \cap V(G)$. Pour cela, on peut supposer par changement de coordonnées projectives suffisamment général que $(\star)$ est vérifiée mais également que tous les points $P := (x_P : y_P : z_P) \in V(F) \cap V(G)$ sont tels que les "abscisses" $(x_P : z_P)_{P \in V(F) \cap V(G)}$ sont disctinctes deux à deux (le vérifier et l'écrire complètement). Noter que les degrés de F et de G sont invariants par changement de coordonnées. Aussi, $(\star)$ implique comme nous l'avons déjà vu que a_0 et b_0 sont des constantes, mais aussi du même coup que $a_i(x,z)$, resp. $b_j(x,j)$, est un polynôme homogène de degré i,resp. j, dans $\mathbb{K}[x,z]$ pour tout $i = 0, \ldots, m$, resp. $j = 0, \ldots, n$). La propriété de quasi-homogénéité 1.2.8 du résultant montre alors que $\mathrm{Res}_{m,n}(F,G)$ est un polynôme homogène de degré $mn = \deg(F)\deg(G)$. De plus notant $\{P_1, \ldots, P_r\} = V(F) \cap V(G)$, ce résultant s'ecrit, d'après le corollaire 1.1.5,

$$\mathrm{Res}_{m,n}(f,g) = c.(z_{P_1}x - x_{P_1}z)^{m_1}(z_{P_2}x - x_{P_2}z)^{m_2} \cdots (z_{P_r}x - x_{P_r}x)^{m_r} \tag{1.14}$$

où $c \in \mathbb{K}$ est une constante non nulle et où $\sum_{i=1}^{r} m_i = mn = \deg(F)\deg(G)$. Définissant la multiplicité du point $P_i \in V(F) \cap V(G)$ par l'entier m_i, le théorème est démontré. □

Corollaire 1.3.2 (Bézout affine) *Si $f(x,y)$ et $g(x,y)$ ne possèdent pas de zéro commun à l'infini (i.e. si $F(x,y,0)$ et $G(x,y,0)$ n'ont pas de zéro commun) alors $V(f) \cap V(g) \subset \mathbb{A}^2$ est constitué d'exactement $\deg(f)\deg(g)$ points comptés avec une multiplicité appropriée.*

Exercice 1.3.1 *Montrer que l'intersection de deux "cercles" d'équations respectives*

$$\alpha_0(x^2+y^2) + \alpha_1 x + \alpha_2 y + \alpha_3 = 0, \quad \beta_0(x^2+y^2) + \beta_1 x + \beta_2 y + \beta_3 = 0,$$

où $\alpha_0 \neq 0$ et $\beta_0 \neq 0$, est consistuée de 2 points à distance finie et 2 points distincts à l'infini.

Comme nous l'avons introduite dans la preuve précédente, la "multiplicité d'intersection" de f et de g en un point P n'apparait pas clairement comme un invariant local associé au point P. Dans le paragraphe suivant nous donnons une définition plus rigoureuse de cette multiplicité d'intersection puis nous montrons qu'elle correspond bien à celle qui apparaît dans la preuve du théorème de Bézout que nous avons donnée.

1.3.2 Multiplicité d'un point d'intersection

1.3.2.1 Un résultat d'algèbre

Nous commençons par rappeler un résultat (très important) d'algèbre qui est une conséquence du fameux théorème des zéros de Hilbert. Dans la suite, $\mathbb{K}$ désigne un corps algébriquement clos.

Proposition 1.3.3 *Soit I un idéal de l'anneau de polynômes $\mathbb{K}[X_1, \ldots, X_n]$, avec n un entier strictement positif. Notant classiquement*

$$V(I) := \{\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{K} \mid f(\mathbf{x}) = 0 \text{ pour tout } f(X_1, \ldots, X_n) \in I\},$$

on a les deux équivalences suivantes :

$$V(I) = \emptyset \Leftrightarrow I = (1),$$

$$V(I) \text{ est fini } \Leftrightarrow \dim_{\mathbb{K}} \mathbb{K}[X_1, \ldots, X_n]/I < \infty.$$

Preuve. La première équivalence est une conséquence directe du théorème des zéros (elle porte d'ailleurs souvent le nom de version "faible" du théorème des zéros). Supposons que $V(I)$ soit un ensemble fini de points, disons $P_1, \ldots, P_r$. Si $\mathfrak{m}_{P_i}$ désigne l'idéal maximal associé au point P_i, pour $i = 1, \ldots, r$, alors le théorème des zéros nous dit que $\sqrt{I} = \prod_{i=1}^{r} \mathfrak{m}_{P_i}$, et donc que I contient une certaine puissance de l'idéal $\prod_{i=1}^{r} \mathfrak{m}_{P_i}$. On en déduit l'existence, pour tout $i = 1, \ldots, n$, de polynômes $U_i(X_i)$ de degré u_i appartenant à l'idéal I. En effectuant, pour tout polynôme $Q \in \mathbb{K}[X_1, \ldots, X_n]$ des divisions euclidiennes

successives par $U_1(X_1), \ldots, U_n(X_n)$, on montre que $\mathbb{K}[X_1, \ldots, X_n]/I$ est engendré par les classes des monômes $X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}$ avec $0 \leq i_j < u_j$ pour tout $j = 1, \ldots, n$. C'est donc bien un $\mathbb{K}$-espace vectoriel de dimension finie. Inversement, Si $\mathbb{K}[X_1, \ldots, X_n]/I$ est un $\mathbb{K}$-espace vectoriel de dimension finie d, pour tout $i = 1, \ldots, n$, les classes des monômes $1, X_i, X_i^2, \ldots, X_i^d$ sont liées. Il existe donc, pour tout $i = 1, \ldots, n$, un polynôme non nul $U_i(X_i)$ appartenant à l'idéal I. Mais alors $V(I) \subset V(U_1, \ldots, U_n)$ et ce dernier est forcément fini. □

Rappelons à présent qu'un anneau est dit *artinien* s'il satisfait une condition duale de la condition noethérienne, à savoir : toute chaîne décroissante d'idéaux de R est finie. On peut alors montrer (voir par exemple [Eis95, §2.4]), entres autres, que

- R est noethérien et tous ses idéaux premiers sont maximaux,
- R ne possède qu'un nombre fini d'idéaux maximaux,
- R est isomorphe à la somme directe de ses localisés. Plus précisemment, le morphisme canonique $R \to \oplus_{\mathfrak{p}} R_{\mathfrak{p}}$, où la somme est prise sur tous les idéaux maximaux de R, est un isomorphisme.

L'intérêt de ces considérations est que l'on peut compléter la proposition 1.3.3 en ajoutant[4] :

$$V(I) \text{ est fini } \Leftrightarrow \dim_{\mathbb{K}} \mathbb{K}[X_1, \ldots, X_n]/I < \infty \Leftrightarrow \mathbb{K}[X_1, \ldots, X_n]/I \text{ est un anneau artinien.}$$

Ainsi, si $V(I)$ est fini alors $\mathbb{K}[X_1, \ldots, X_n]/I \simeq \bigoplus_{\mathfrak{p} \in \mathrm{Spec}(\mathbb{K}[X_1, \ldots, X_n]/I)} \mathbb{K}[X_1, \ldots, X_n]_{\mathfrak{p}}/I_{\mathfrak{p}}$ et donc

$$\dim_{\mathbb{K}} \mathbb{K}[X_1, \ldots, X_n]/I = \sum_{\mathfrak{p} \in \mathrm{Spec}(\mathbb{K}[X_1, \ldots, X_n]/I)} \dim_{\mathbb{K}} \mathbb{K}[X_1, \ldots, X_n]_{\mathfrak{p}}/I_{\mathfrak{p}}.$$

Cette formule montre que l'on peut "distribuer" une quantité associée à l'idéal I sur les points de $V(I)$ qui sont en correspondance avec les idéaux maximaux de $\mathbb{K}[X_1, \ldots, X_n]/I$. La tentation est donc grande de définir la multiplicité du point $V(\mathfrak{p})$ de $V(I)$ comme l'entier $\dim_{\mathbb{K}} \mathbb{K}[X_1, \ldots, X_n]_{\mathfrak{p}}/I_{\mathfrak{p}}$.

1.3.2.2 Multiplicité d'intersection

Commençons par énoncer un corollaire des considérations du paragraphe 1.3.2.1 précédent.

Corollaire 1.3.4 *Soient $\mathbb{K}$ un corps algébriquement clos et $f(x, y), g(x, y)$ deux polynômes de $\mathbb{K}[x, y]$. Les propositions suivantes sont équivalentes :*

(i) *$V(f) \cap V(g)$ est un nombre fini de points,*
(ii) *$\dim_{\mathbb{K}} \mathbb{K}[x, y]/(f, g)$ est un $\mathbb{K}$-espace vectoriel de dimension finie,*
(iii) *f et g sont premiers entre eux dans $\mathbb{K}[x, y]$.*

De plus, lorsque ces assertions sont réalisées, on a

$$\dim_{\mathbb{K}} \mathbb{K}[x, y]/(f, g) = \sum_{\mathfrak{p} \in \mathrm{Spec}(\mathbb{K}[x,y]/(f,g))} \dim_{\mathbb{K}} \mathbb{K}[x, y]_{\mathfrak{p}}/(f, g)_{\mathfrak{p}}$$

où la somme est prise sur tous les idéaux premiers, qui sont en fait maximaux et en nombre fini, de l'anneau quotient $\mathbb{K}[x, y]/(f, g)$.

Preuve. L'équivalence entre (i) et (ii) est une conséquence de la proposition 1.3.3. Le fait que (i) implique (iii) se voit facilement par contraposée. On a déjà vu que (iii) implique (i) au début de la preuve du théorème 1.3.1. □

Définition 1.3.5 *Soit $\mathbb{K}$ un corps algébriquement clos et soient $f(x, y)$ et $g(x, y)$ deux polynômes dans $\mathbb{K}[x, y]$ supposés premiers entre eux. La multiplicité d'intersection de f et de g au point $P \in \mathbb{A}^2$ est l'entier*

$$i(f, g; P) := \dim_{\mathbb{K}} \mathbb{K}[x, y]_{\mathfrak{p}}/(f, g)_{\mathfrak{p}}$$

où $\mathfrak{p}$ est l'idéal maximal de $k[x, y]$ correspondant au point $P \in \mathbb{A}^2$.

[4] En effet, si $R := \mathbb{K}[X_1, \ldots, X_n]/I$ est un $\mathbb{K}$-espace vectoriel de dimension finie, alors toute chaîne décroissante de sous-espaces vectoriels est finie et donc toute chaîne décroissante d'idéaux de R est nécessairement finie. Inversement, si R est artinien alors tous ses idéaux premiers sont maximaux et il ne possède qu'un nombre fini de tels idéaux ; en d'autres termes, $V(I)$ est fini.

Noter que la multiplicité d'intersection est *invariante par changement linéaire de coordonnées* dans $\mathbb{A}^2$ et que l'on a l'égalité

$$\dim_{\mathbb{K}} \mathbb{K}[x,y]/(f,g) = \sum_{P \in V(f)\cap V(g)} i(f,g;P)$$

où la somme est finie puisque $V(f)\cap V(g)$ est un nombre fini de points par le corollaire 1.3.4, points qui sont, rappelons-le, en correspondance avec les idéaux maximaux de $\mathbb{K}[x,y]/(f,g)$.

Maintenant que nous avons une définition de la multiplicité d'intersection, nous en donnons une caractérisation similaire à (1.11) et à (1.14) qui permet de la calculer à l'aide d'un résultant. Pour cela, nous voyons $f(x,y)$ et $g(x,y)$ comme des polynômes univariés en la variable y dont les coefficients sont dans $\mathbb{K}[x]$; on écrit, comme dans (1.13),

$$\left\{ \begin{array}{rcl} f(x,y) & = & a_0(x)y^m + a_1(x)y^{m-1} + \cdots + a_{m-1}(x)y + a_m(x) \\ g(x,y) & = & b_0(x)y^n + b_1(x)y^{n-1} + \cdots + b_{n-1}(x)y + b_n(x) \end{array} \right. \tag{1.15}$$

où $a_i(x) \in \mathbb{K}[x]$ pour $i = 0,\ldots,m$ et $b_j(x) \in \mathbb{K}[x]$ pour $j = 0,\ldots,n$. La proposition 1.1.4 nous montre que $\mathrm{Res}_{m,n}(f,g)$ est un polynôme *non nul* de $\mathbb{K}[x]$ si f et g sont supposés premiers entre eux (cf. preuve du théorème 1.3.1).

Pour tout polynôme $R(x) \in \mathbb{K}[x]$ et tout point $x_0 \in \mathbb{K}$ nous noterons $\mathrm{val}_{x_0}(R)$ la valuation de R en x_0, c'est-à-dire le plus grand entier s tel que $(x-x_0)^s$ divise $R(x)$; si $x-x_0$ ne divise pas R alors $\mathrm{val}_{x_0}(R) = 0$. Aussi, pour tout point $P \in \mathbb{A}^2$ nous noterons x_P, respectivement y_P, son abscisse, respectivement son ordonnée.

Proposition 1.3.6 *Soient $f(x,y)$ et $g(x,y)$ deux polynômes premiers entre eux. Avec les notations de* (1.13)*, supposons donné $x_0 \in \mathbb{K}$ tel que $a_0(x_0) \neq 0$ ou $b_0(x_0) \neq 0$. Alors*

$$\mathrm{val}_{x_0}(\mathrm{Res}_{m,n}(f,g)) = \sum_{P \in \mathbb{A}^2 \,:\, x_P = x_0} i(f,g;P).$$

En particulier, si $P \in \mathbb{A}^2$ est le seul point de $V(f)\cap V(g)$ d'abscisse[5] *x_P, alors la multiplicité d'intersection de f et de g au point P est exactement* $\mathrm{val}_{x_P}(\mathrm{Res}_{m,n}(f,g))$.

Preuve. Sans perdre en généralité, nous pouvons supposer que $x_0 = 0$ et que $a_0(0) \neq 0$. Notons A l'anneau local de l'axe des x à l'origine, c'est-à-dire $A := \mathbb{K}[x]_{(x)}$ (qui est isomorphe à $(\mathbb{K}[x,y]/(y))_{(x,y)}$). Puisque $a_0(0) \neq 0$, le polynôme $a_0(x)$ est inversible dans A et la formule de Poisson 1.2.2 fournit l'égalité

$$\det{}_{\mathcal{B}}(A[Y]/(f) \xrightarrow{\times g} A[Y]/(f)) = a_0(x)^{-n}\mathrm{Res}_{m,n}(f,g) \in A$$

où le membre de gauche est le déterminant de la matrice de multiplication par g dans $A[Y]/(f)$ exprimée dans la base canonique $\mathcal{B} := \{\overline{Y}^{m-1},\ldots,\overline{1}\}$, matrice de taille $m \times m$ à entrées dans A.

Soit $Q(x) \in \mathbb{K}[x]$, alors il est immédiat de constater que $\mathrm{val}_0(Q) = \dim_{\mathbb{K}} A/(Q)$, autrement dit que la suite exacte $0 \to A \xrightarrow{\times Q} A \to A/(Q) \to 0$ donne la relation

$$\mathrm{val}_0\left(\det(A \xrightarrow{\times Q} A)\right) = \dim_{\mathbb{K}} A/(Q) = \dim_{\mathbb{K}} \mathrm{coker}(\mathrm{A} \xrightarrow{\times \mathrm{Q}} \mathrm{A}).$$

Par somme directe, on en déduit que cette propriété reste vraie pour une matrice diagonale, c'est-à-dire que si $Q_1(x),\ldots,Q_s(x)$ sont des polynômes de $\mathbb{K}[x]$, alors on a une suite exacte

$$0 \to A^s \xrightarrow{M := \begin{pmatrix} Q_1 & & 0 \\ & \ddots & \\ 0 & & Q_s \end{pmatrix}} A^s \to A/(Q_1)\oplus\cdots\oplus A/(Q_s) \to 0$$

et la formule

$$\mathrm{val}_0(\det(M)) = \mathrm{val}_0(Q_1(x)\ldots Q_s(x)) = \dim_{\mathbb{K}} \oplus_{i=1}^s A/(Q_i) = \dim_{\mathbb{K}} \mathrm{coker}(\mathrm{A}^{\mathrm{s}} \xrightarrow{\mathrm{M}} \mathrm{A}^{\mathrm{s}}).$$

[5] Les points d'abscisse $x_0 \in \mathbb{K}$ sont tous les points de $\mathbb{P}^2$ qui sont sur la droite projective $x - x_0 z$.

Or, A est un anneau principal, donc le théorème des facteurs invariants[6] implique qu'il existe des bases de $A[Y]/(f)$ dans lesquelles la matrice de multiplication par g est diagonale. En conséquence, on obtient

$$\mathrm{val}_0(\mathrm{Res}_{m,n}(f,g)) = \mathrm{val}_0(\det(A^m \simeq A[y]/(f) \xrightarrow{\times g} A^m)) = \dim_{\mathbb{K}} \mathrm{coker}(\times \mathrm{g}) = \dim_{\mathbb{K}} A[y]/(f,g).$$

Pour achever la démonstration de cette proposition, il nous reste donc à montrer l'égalité

$$\dim_{\mathbb{K}} A[y]/(f,g) = \sum_{P \in \mathbb{A}^2 \,:\, x_P = x_0} i(f,g;P).$$

Nous savons que l'anneau quotient $\mathbb{K}[x,y]/(f,g)$ est artinien. En particulier, tous ses idéaux premiers sont maximaux et en nombre fini ; on les note $J_1 = (x - x_1, y - y_1), \ldots, J_r = (x - x_r, y - y_r)$ (rappelons qu'ils sont en correspondances avec les points de $\mathbb{A}^2$ $P_1 = (x_1, y_1), \ldots, P_r = (x_r, y_r)$ qui sont solutions du système $f(x,y) = g(x,y) = 0$).

Considérons à présent le morphisme canonique d'anneaux

$$\mathbb{K}[x,y]/(f,g) \xrightarrow{\phi} A[y]/(f,g) = \mathbb{K}[x]_{(x)}[y]/(f,g)$$

induit par le morphisme de localisation $\mathbb{K}[x] \to A : x \to x/1$. Puisque ϕ est un morphisme d'anneaux, tout idéal premier (donc propre) K de $A[y]/(f,g)$ fournit un idéal premier (donc propre) de $\mathbb{K}[x,y]/(f,g)$, à savoir l'idéal $\phi^{-1}(K) = \{a \in \mathbb{K}[x,y]/(f,g) \text{ tel que } \phi(a) \in K\}$. Cet idéal est donc l'un des idéaux maximaux J_i, avec $i \in \{1, \ldots, r\}$, tel que $x_i = 0$ (car sinon K ne serait pas un idéal propre). Inversement, à tout idéal J_i de $\mathbb{K}[x,y]/(f,g)$ tel que $x_i = 0$ on peut associer l'idéal $\phi(J_i).A[y]/(f,g) = (x/1, y - y_i)$ qui est un idéal premier (on a $(f,g) \subset J_i = (x, y - y_i) \subset \mathbb{K}[x,y]$ ce qui donne $(A[y]/(f,g))/(x/1, y - y_i) \simeq A[y]/(x/1, y - y_i) \simeq \mathbb{K}$ intègre). On a donc la correspondance bijective :

$$\text{idéaux } J_i \text{ maximaux de } \mathbb{K}[x,y]/(f,g) \text{ tels que } x_i = 0 \;\leftrightarrow\; \text{idéaux premiers de } A[y]/(f,g).$$

Cela montre que les idéaux premiers de $A[y]/(f,g)$ sont maximaux et en nombre fini. Il s'en suit que $A[y]/(f,g)$ est artinien et donc que

$$A[y]/(f,g) \simeq \bigoplus_{\mathfrak{p} \in \mathrm{Spec}(A[y]/(f,g))} A[y]_{\mathfrak{p}}/(f,g)_{\mathfrak{p}} \simeq \bigoplus_{J_i \text{ tel que } x_i = 0} \mathbb{K}[x,y]_{J_i}/(f,g)_{J_i}.$$

Par conséquent $\dim_{\mathbb{K}} A[y]/(f,g) = \sum_{P_i \in \mathbb{A}^2 \,:\, x_p = 0} i(f,g;P_i)$.

□

Finissons ce paragraphe en donnant quelques propriétés de la multiplicité d'intersection qui découlent (presque) directement de ce qui précède et des propriétés du résultant :

- $i(f,g;P) = 0$ si et seulement si $P \notin V(f) \cap V(g)$,
- $i(f,g;P)$ ne dépend que des composantes de $V(f)$ et de $V(g)$ qui passent par P,
- $i(f,g;P) = i(g,f;P)$,
- $i(f_1 f_2, g; P) = i(f_1, g; P) + i(f_2, g; P)$,
- Pour tout polynôme $h \in \mathbb{K}[x,y]$ on a $i(f,g;P) = i(f, g + hf; P)$.

1.3.3 Calcul des points d'intersection par valeurs et vecteurs propres

Dans ce paragraphe, nous montrons comment il est possible de retrouver explicitement les points d'intersection de deux courbes algébriques représentées par des équations implicites $f(x,y) = 0$ et $g(x,y) = 0$ à l'aide des représentations matricielles du résultant que sont les matrices de Sylvester et de Bézout.

[6] Soit R un anneau *principal*, M et N deux R-modules libres de type fini et f un morphisme de M dans N. Le théorème des facteurs invariants dit qu'il existe alors une base de M et une base de N telles que, dans ces bases, la matrice de f est de la forme $\begin{pmatrix} d_1 & 0 & \ldots & 0 \\ 0 & d_2 & 0 & \vdots \\ \vdots & 0 & \ddots & 0 \\ 0 & \ldots & 0 & d_{\min(m,n)} \end{pmatrix}$, éventuellement complétée par des lignes ou des colonnes de zéros si les rangs de M et N diffèrent. En outre, on peut supposer que d_i divise d_{i+1} (rappelons qu'un anneau principal est factoriel). Pour plus de détails, voir [Bou81, chapitre VII, §4, numéro 6].

1.3.3.1 Valeurs et vecteurs propres généralisés

Définition 1.3.7 *Soient A et B deux matrices carrées de taille $n \times n$. Une* valeur propre généralisée *de A et B est un élément de l'ensemble*

$$\lambda(A, B) := \{\lambda \in \mathbb{C} : \det(A - \lambda B) = 0\}.$$

Un vecteur $x \neq 0$ est appelé un vecteur propre généralisé *associé à la valeur propre $\lambda \in \lambda(A, B)$ si $Ax = \lambda Bx$.*

Les matrices A et B ont n valeurs propres généralisées si et seulement si $\text{rang}(B) = n$. Si $\text{rang}(B) < n$ alors $\lambda(A, B)$ peut-être un ensemble fini, vide, ou bien infini. Notons que si $0 \neq \mu \in \lambda(A, B)$ alors $1/\mu \in \lambda(B, A)$. De plus, si B est inversible alors $\lambda(A, B) = \lambda(B^{-1}A, I)$ qui n'est autre que le spectre classique de la matrice $B^{-1}A$.

Étant donnée une matrice $T(x)$ de taille $n \times n$ dont les entrées sont des polynômes dans l'anneau $\mathbb{C}[x]$, nous pouvons lui associer un polynôme en la variable x dont les coefficients sont des matrices $n \times n$ à coefficients dans $\mathbb{C}$: si $d = \max_{i,j}\{\deg(T_{ij}(x))\}$, on obtient $T(x) = T_d x^d + T_{d-1}x^{d-1} + \cdots + T_0$, où T_i est une matrice $n \times n$ à coefficients dans $\mathbb{C}$. Bien sûr, cette opération est réversible.

Définition 1.3.8 *Avec les notations précédentes et désignant par Id_n la matrice identité de taille $n \times n$, on appelle matrices compagnons de $T(x)$ les deux matrices A et B définies par*

$$A = \begin{pmatrix} 0 & Id_n & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & Id_n \\ {}^tT_0 & {}^tT_1 & \cdots & {}^tT_{d-1} \end{pmatrix}, B = \begin{pmatrix} Id_n & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & Id_n & 0 \\ 0 & \cdots & 0 & -{}^tT_d \end{pmatrix}.$$

Nous avons alors la propriété intéressante suivante qui montre que l'on peut remplacer le calcul des valeurs singulières de $T(x)$ (c'est-à-dire le calcul des $x \in \mathbb{C}$ tels que $\det(T(x)) = 0$) et des noyaux correspondants par un problème de calcul de valeurs et vecteurs propres généralisés.

Proposition 1.3.9 *Avec les notations précédentes, pour tout vecteur $v \in \mathbb{C}^n$ et tout $x \in \mathbb{C}$, on a :*

$${}^tT(x)v = 0 \Leftrightarrow (A - xB) \begin{pmatrix} v \\ xv \\ \vdots \\ x^{d-1}v \end{pmatrix} = 0.$$

Preuve. En effet, si ${}^tT(x)v = 0$ alors

$$A \begin{pmatrix} v \\ xv \\ \vdots \\ x^{d-1}v \end{pmatrix} = \begin{pmatrix} xv \\ x^2v \\ \vdots \\ x^{d-1}v \\ ({}^tT_0 + \cdots + {}^tT_{d-1}x^{d-1})v \end{pmatrix} = \begin{pmatrix} xv \\ x^2v \\ \vdots \\ x^{d-1}v \\ -{}^tT_d x^d v \end{pmatrix} = xB \begin{pmatrix} v \\ xv \\ \vdots \\ x^{d-1}v \end{pmatrix}.$$

Inversement, si

$$(A - xB) \begin{pmatrix} v \\ xv \\ \vdots \\ x^{d-1}v \end{pmatrix} = 0$$

alors la dernière ligne montre que ${}^tT(x)v = 0$. □

1.3.3.2 Le résultat principal

On suppose donnés deux polynômes $f(x,y)$ et $g(x,y)$ dans $\mathbb{C}[x,y]$ que l'on écrit sous la forme

$$\left\{ \begin{array}{rcl} f(x,y) & = & a_0(x)y^m + a_1(x)y^{m-1} + \cdots + a_{m-1}(x)y + a_m(x) \\ g(x,y) & = & b_0(x)y^n + b_1(x)y^{n-1} + \cdots + b_{n-1}(x)y + b_n(x) \end{array} \right. \tag{1.16}$$

où $a_i(x) \in \mathbb{C}[x]$ pour $i = 0, \ldots, m$ et $b_j(x) \in \mathbb{C}[x]$ pour $j = 0, \ldots, n$. Nous supposons en outre que $n \geq 1$, $m \geq 1$ (dans le cas contraire la résolution du système $f(x,y) = g(x,y) = 0$ se ramène à la résolution d'un polynôme univarié) et que ces deux polynômes sont premiers entre eux, de telle sorte qu'ils définissent un nombre fini de points dans l'espace affine $\mathbb{A}^2$ et que le résultant $\mathrm{Res}_{m,n}(f,g)$ éliminant la variable y soit non nul (voir corollaire 1.3.4). Nous avons vu que $\mathrm{Res}_{m,n}(f,g) \in \mathbb{C}[x]$ s'annule en $x_0 \in \mathbb{C}$ si et seulement s'il existe un $y_0 \in \mathbb{C}$ tel que $f(x_0,y_0) = g(x_0,y_0) = 0$ ou bien $a_0(x_0) = b_0(x_0) = 0$ (cas où la solution se trouve à l'infini). Par conséquent, on peut se poser la question suivante :

Étant donné un point x_0 tel que $\mathrm{Res}_{m,n}(f,g)(x_0) = 0$ et tel que $a_0(x_0) \neq 0$ ou bien $b_0(x_0) \neq 0$, expliquer comment on peut calculer tous les $y_0 \in \mathbb{C}$ tels que $f(x_0,y_0) = g(x_0,y_0) = 0$, c'est-à-dire comment trouver tous les points d'intersection des deux courbes $V(f)$ et $V(g)$ qui ont x_0 pour abscisse ?
Rappelons qu'il est possible, comme nous l'avons montré dans la preuve de théorème de Bézout, de se ramener au cas où $a_0(x)$ et $b_0(x)$ sont des constantes non nulles par simple changement de coordonnées suffisamment général.

Supposons donc donné un tel point x_0. Puisque $\mathrm{Res}_{m,n}(f,g) \in \mathbb{C}[x]$ n'est autre que le déterminant de la matrice de Sylvester $S(x) := S_{m,n}(f,g) \in \mathrm{Mat}_{m+n}(\mathbb{C}[x])$, nous déduisons que la matrice $S(x_0)$ (où l'on a spécialisé la variable x en x_0) est singulière, c'est-à-dire possède un noyau non nul. Si $\ker({}^tS(x_0))$ est de dimension 1, alors il est aisé de montrer qu'il n'y a qu'un seul y_0 tel que $f(x_0,y_0) = g(x_0,y_0) = 0$, puisque le vecteur $[y_0^{m+n-1}, \cdots, y_0, 1]$ appartient clairement à $\ker({}^tS(x_0))$. De plus, à partir de n'importe quel vecteur $v := [v_{m+n-1}, \cdots, v_1, v_0] \in \ker({}^tS(x_0))$, on peut retrouver y_0 par la formule $v_0 y_0 = v_1$. Ainsi, dans ce cas, calculer y_0 revient à calculer un élement non nul dans $\ker(S(x_0)^t)$. Dans ce qui suit, nous allons montrer que cette approche se généralise.

Notations : Partant du système (1.16), avec les hypothèses précédentes, on suppose donné un point $x_0 \in \mathbb{C}$ tel que $\det(S(x_0)) = \mathrm{Res}_{m,n}(f,g)(x_0) = 0$ et $a_0(x_0) \neq 0$ (ou bien $b_0(x_0) \neq 0$).

Soient $\Lambda_1, \cdots, \Lambda_d$ des vecteurs de $\mathbb{C}^{m+n}$ formant une base du noyau de la matrice ${}^tS(x_0)$. On note $\mathbf{\Lambda}$ la matrice de taille $d \times (m+n)$ à coefficients dans $\mathbb{C}$ dont la $i^{\text{ième}}$ ligne est le vecteur Λ_i :

$$\mathbf{\Lambda} := \begin{pmatrix} \Lambda_1 \\ \Lambda_2 \\ \vdots \\ \Lambda_d \end{pmatrix} = \begin{pmatrix} \Lambda_{1,0} & \Lambda_{1,1} & \cdots & \Lambda_{1,m+n-1} \\ \Lambda_{2,0} & \Lambda_{2,1} & \cdots & \Lambda_{2,m+n-1} \\ \vdots & \vdots & & \vdots \\ \Lambda_{d,0} & \Lambda_{d,1} & \cdots & \Lambda_{d,m+n-1} \end{pmatrix}$$

(où l'on a posé $\Lambda_i := [\Lambda_{i,0}, \Lambda_{i,1}, \cdots, \Lambda_{i,m+n-1}]$ pour tout $i = 1, \ldots, d$). On définit également la matrice Δ_0, resp. Δ_1, comme la sous-matrice de taille $d \times d$ formée des d dernières colonnes, resp. des colonnes m+n-d-1,m+n-d,...,m+n-2, de la matrice $\mathbf{\Lambda}$:

$$\Delta_0 := \begin{pmatrix} \Lambda_{1,m+n-d} & \Lambda_{1,m+n-d+1} & \cdots & \Lambda_{1,m+n-1} \\ \Lambda_{2,m+n-d} & \Lambda_{2,m+n-d+1} & \cdots & \Lambda_{2,m+n-1} \\ \vdots & \vdots & & \vdots \\ \Lambda_{d,m+n-d} & \Lambda_{d,m+n-d+1} & \cdots & \Lambda_{d,m+n-1} \end{pmatrix},$$

$$\Delta_1 := \begin{pmatrix} \Lambda_{1,m+n-d-1} & \Lambda_{1,m+n-d} & \cdots & \Lambda_{1,m+n-2} \\ \Lambda_{2,m+n-d-1} & \Lambda_{2,m+n-d} & \cdots & \Lambda_{2,m+n-2} \\ \vdots & \vdots & & \vdots \\ \Lambda_{d,m+n-d-1} & \Lambda_{d,m+n-d} & \cdots & \Lambda_{d,m+n-2} \end{pmatrix}.$$

Il faut noter que les matrices Δ_0 et Δ_1 sont bien toujours définies, c'est-à-dire que la matrice $\mathbf{\Lambda}$ a toujours au moins $d+1$ colonnes. Cela provient du fait que nous avons supposé que les polynômes f et g dépendent tous les deux de la variable y ; $m+n$, le nombre de ligne de la matrice $S(x_0)$, est alors toujours strictement plus grand que le $\max(m,n) \geq \deg(\gcd(f(x_0,y), f(x_0,y))) = \dim_{\mathbb{C}} \ker({}^tS(x_0))$ (voir exercice 1.1.1 pour cette dernière égalité).

Proposition 1.3.10 *Avec les notations précédentes, $\lambda(\Delta_1, \Delta_0)$ est l'ensemble de toutes les racines dans $\mathbb{C}$ du système $f(x_0, y) = g(x_0, y) = 0$, c'est-à-dire l'ensemble des ordonnées des points d'intersection des courbes $V(f)$ et $V(g)$ d'abscisse x_0.*

Preuve. On commence par rappeler que la matrice de l'application

$$\phi_{x_0} : \mathbb{C}[y]_{<n} \times \mathbb{C}[y]_{<m} \to \mathbb{C}[y]_{<m+n} : (u, v) \mapsto uf + vg$$

dans les bases monomiales canoniques est $S(x_0) := S_{m,n}(f, g)(x_0)$. Considérons à présent le polynôme

$$h(y) := \mathrm{pgcd}(f(x_0, y), g(x_0, y)).$$

C'est un polynôme unitaire de $\mathbb{C}[y]$ dont le degré est égale à la dimension du noyau de $S(x_0)$ (voir exercice 1.1.1). On a donc $\deg(h(y)) = \dim_{\mathbb{C}}(\ker({}^tS(x_0)) = d$, où d est le nombre de lignes de la matrice $\mathbf{\Lambda}$ introduite précédemment.

Considérons l'application

$$\psi_{x_0} : \mathbb{C}[y]_{<m+n} \to \mathbb{C}[y]_{<d} : p(y) \mapsto r(y),$$

où $r(y)$ est le reste de la division euclidienne de $p(y)$ par $h(y) : p(y) = q(y)h(y) + r(y)$. Sa matrice Δ, de taille $d \times (m+n)$, dans les bases monomiales canoniques $\{y^{m+n-1}, \ldots, y, 1\}$ et $\{y^{d-1}, \ldots, y, 1\}$ est de la forme

$$\Delta := \left(\begin{array}{c|ccc} & 1 & & 0 \\ \star & & \ddots & \\ & 0 & & 1 \end{array}\right)$$

où la bloc de droite est la matrice identité de taille $d \times d$. Puisque l'on vérifie sans peine que $\psi_{x_0} \circ \phi_{x_0} = 0$, on en déduit que les lignes de Δ sont d vecteurs de $\mathbb{C}^{m+n}$ qui forment une base de $\ker({}^tS(x_0))$. De plus, si l'on note $\mathtt{M}_y$ la matrice, dans la base monomiale canonique $\{y^{d-1}, \ldots, y, 1\}$, de multiplication par y dans l'anneau quotient $\mathbb{C}[y]/(h(y)) \simeq \mathbb{C}[y]_{<d}$, on s'aperçoit que la multiplication à gauche par $\mathtt{M}_y$ d'une colonne de Δ fournit la colonne voisine à gauche, si cette dernière existe. En effet, il est immédiat de constater que pour tout $i = 0, \ldots, m+n-2$ on a $\psi_{x_0}(y^{i+1}) = \psi_{x_0}(y\,\psi_{x_0}(y^i))$, propriété élémentaire de la division euclidienne (qui est même vraie plus généralement pour un produit de deux polynômes quelconques), et que par conséquent l'on a $\psi_{x_0}(y^{i+1}) = \mathtt{M}_y\psi_{x_0}(y^i)$. Ainsi, définissant les matrices Δ_0 et Δ_1 à partir de la matrice $\mathbf{\Lambda} := \Delta$, on obtient $\Delta_1 = \mathtt{M}_y\Delta_0 = \mathtt{M}_y$ (puisque Δ_0 est la matrice identité) et les éléments de $\lambda(\Delta_1, \Delta_0)$ sont les valeurs propres de $\mathtt{M}_y$, c'est-à-dire toutes les racines du polynôme $h(y)$, donc toutes les solutions du système $f(x_0, y) = g(x_0, y) = 0$. L'énoncé général de la proposition s'obtient alors par un simple changement de base. □

Utilisation de la matrice de Bézout : Dans ce résultat, nous avons utilisé la matrice de Sylvester pour "représenter" le résultant de f et de g en la variable y. Cependant, il est possible de remplacer cette matrice par la matrice de Bézout (noter qu'il faut alors considérer f et g comme des polynômes en y de degré le plus grand des degrés de f et de g en y) qui possède toutes les propriétés requises exceptées une : cette matrice étant plus petite que la matrice de Sylvester, les matrices Δ_0 et Δ_1 ne sont pas toujours bien définies (alors qu'elles le sont avec la matrice de Sylvester, comme nous l'avons déjà remarqué plus haut). Plus précisemment, pour pouvoir utiliser la matrice de Bézout nous avons besoin de vérifier l'inégalité

$$\max(\deg(f(x_0, y), \deg(g(x_0, y)) > \deg(\gcd(f(x_0, y), g(x_0, y)).$$

L'exemple suivant, où l'on prend $x_0 = -1$, montre qu'elle ne l'est pas toujours :

$$\left\{\begin{array}{l} p(x, y) = x^2y^2 - 2y^2 + xy - y + x + 1 \\ q(x, y) = y + xy \end{array}\right.$$

1.3.3.3 L'algorithme

Nous avons maintenant réuni tous les ingrédients pour énoncer un algorithme de résolution d'un système de la forme $f(x,y) = g(x,y) = 0$ basé sur les résultants. La matrice de Bézout donne, en pratique, un algorithme plus rapide du fait qu'elle est plus compacte que la matrice de Sylvester (bien que son calcul prenne plus de temps) ; nous l'avons donc incorporée à l'algorithme. Utilisant la proposition 1.3.9, nous avons remplacé le calcul du résultant, de ses zéros et des noyaux des matrices ${}^tS(x_0)$ par le calcul de valeurs et vecteurs propres généralisés des matrices compagnons associées. Ce calcul peut s'effectuer à l'aide d'un algorithme bien connu d'algèbre linéaire dit "QZ" (voir par exemple [GVL96]).

Algorithme pour l'intersection de deux courbes algébriques planes :
Input : Deux polynômes $f(x,y)$ et $g(x,y)$ dans $\mathbb{C}[x,y]$ premiers entre eux, dépendants tous les deux de la variable y et sans solution commune à l'infini.
Output : Tous les points d'intersection des courbes $V(f)$ et $V(g)$ dans $\mathbb{A}^2$, ainsi que la somme des multiplicités par abscisse.

1. Former la matrice de Bézout $B(x)$ de f et g.
2. Former les matrices compagnons A et B associés (voir proposition 1.3.9).
3. Calculer les valeurs et vecteurs propres généralisés de (A,B). Les valeurs propres fournissent les abscisses des points d'intersection des courbes $V(f)$ de $V(g)$ (ce sont les points notés x_0 plus haut), et leur multiplicité donne la somme des multiplicité d'intersection des points d'intersection ayant même abscisse (voir la proposition 1.3.6). Les espaces propres fournissent des bases pour $\ker(B(x_0))$, bases notées $\mathbf{\Lambda}$ dans la proposition 1.3.10 ; leur dimension donne le degré du pgcd de $f(x_0,y)$ et $g(x_0,y)$.
4. Pour chaque point x_0,
   (a) si le nombre de vecteurs propres associés est au moins $\max(\deg(f(x_0,y)),\deg(g(x_0,y)))$, qui est la taille de la matrice $B(x_0)$, alors calculer Δ_0 et Δ_1 en utilisant une base de $\ker(S(x_0)^t)$,
   (b) sinon, calculer Δ_0 et Δ_1 en utilisant les vecteurs propres associés à la valeur propre x_0.
5. Calculer les valeurs propres de (Δ_1,Δ_0) qui fournissent les ordonnées des points d'intersection ayant pour abscisse x_0 (voir la proposition 1.3.10).

1.4 Implicitation et inversion d'une courbe algébrique plane rationnelle

1.4.1 Degré d'une courbe.

Soit $\mathcal{C}$ une courbe algébrique de $\mathbb{A}^2_{\mathbb{K}}$. On peut lui associer l'idéal $I_{\mathcal{C}}$ de $\mathbb{K}[x,y]$ constitué des polynômes $P(x,y)$ qui s'annulent sur $\mathcal{C}$. Rappelons que la courbe $\mathcal{C}$ est irréductible si et seulement si l'idéal $I_{\mathcal{C}}$ est premier.

Lemme 1.4.1 *Soit $\mathcal{C}$ une courbe algébrique de $\mathbb{A}^2_{\mathbb{K}}$, alors l'idéal $I_{\mathcal{C}}$ est un idéal principal de $\mathbb{K}[x,y]$.*

Preuve. En opérant une décomposition en composante irréductible sur $\mathcal{C}$, on se ramène à montrer cette propriété lorsque $\mathcal{C}$ est une courbe irréductible, c'est-à-dire lorsque $I_{\mathcal{C}}$ est un idéal premier. Si $I_{\mathcal{C}} = (g_1, g_2, \ldots)$ alors, par primalité, on peut supposer que g_1 est premier. Et puisque $(g_1) \subset I_{\mathcal{C}}$, il s'en suit que $\mathcal{C} \subset V(g_1)$ où $V(g_1)$ est une courbe irréductible (car g_1 est premier), tout comme $\mathcal{C}$; ainsi $\mathcal{C} = V(g_1)$ et $I_{\mathcal{C}} = (g_1)$. □

Définition 1.4.2 *Un générateur de $I_{\mathcal{C}}$ est appelé une équation implicite de la courbe $\mathcal{C}$, et son degré (qui est indépendant de son choix) le degré de la courbe $\mathcal{C}$ que l'on note* $\deg(\mathcal{C})$.

Proposition 1.4.3 *Soit $\mathbb{K}$ un corps algébriquement clos et supposons données une courbe algébrique $\mathcal{C}$ de $\mathbb{P}^2_{\mathbb{K}}$ et une droite H de $\mathbb{P}^2$ non contenue dans $\mathcal{C}$. Alors $\mathcal{C}$ et H se rencontrent en* $\deg(\mathcal{C})$ *points, comptés avec multiplicité.*

Preuve. C'est un corollaire du théorème de Bézout puisque $\deg(H) = 1$ et que $\deg(\mathcal{C}).1 = \deg(\mathcal{C})$. □

Il faut noter que cette proposition est souvent utilisée pour donner une définition géométrique du degré d'une courbe, et même d'une variété algébrique : on intersecte la variété avec un espace linéaire de dimension complémentaire de telle sorte que le résultat de cette intersection soit un nombre fini de points ; le degré est alors défini comme ce nombre de points (comptés avec multiplicité).

1.4.2 Courbes planes rationnelles

Ci-après, $\mathbb{K}$ désigne un corps.

Définition 1.4.4 *On dit qu'une courbe $\mathcal{C}$ de $\mathbb{A}^2$ (resp. $\mathbb{P}^2$) est* rationnelle *si elle admet une paramétrisation par une application rationnelle de $\mathbb{A}^1 \to \mathbb{A}^2$ (resp. $\mathbb{P}^1 \to \mathbb{P}^2$).*

Ainsi, une courbe $\mathcal{C}$ de $\mathbb{A}^2$ est rationnelle s'il existe deux fractions rationnelles $p, q \in \mathbb{K}(t)$, non toutes les deux constantes, telles que l'image de l'application

$$\phi : \mathbb{A}^1 \to \mathbb{A}^2 : t \mapsto (p(t), q(t)) \tag{1.17}$$

soit dense (pour la topologie de Zariski) dans cette courbe (qui est alors l'adhérence de cette image) ; autrement dit, $\mathcal{C}$ est la plus petite courbe algébrique contenant l'image ensembliste de ϕ. Cette image décrit donc, en général, toute la courbe excepté un nombre fini de points. Ce phénomène provient du fait qu'il existe des valeurs du paramètre t pour lesquelles $p(t)$ ou bien $q(t)$ n'est pas défini.

On peut homogénéiser cette paramétrisation. Ainsi, une courbe $\mathcal{C}$ de $\mathbb{P}^2$ est rationnelle s'il existe trois polynômes homogènes de même degré $P, Q, R \in \mathbb{K}[t, u]$, non tous les trois associés, telles que l'image de l'application

$$\phi : \mathbb{P}^1 \to \mathbb{P}^2 : (t : u) \mapsto (P(t, u) : Q(t, u) : R(t, u))$$

décrive la courbe, excepté peut-être en un nombre fini de points. (qui correspondent aux valeurs du paramètre $V(P, Q, R) \subset \mathbb{P}^1$).

Lemme 1.4.5 *Une courbe rationnelle est irréductible.*

Preuve. Soit $\mathcal{C}$ une courbe rationnelle paramétrée par (1.17). Considérant le morphisme d'anneaux

$$\psi : \mathbb{K}[x, y] \to \mathbb{K}(t) : f(x, y) \mapsto f(p(t), q(t))$$

on déduit une injection $\mathbb{K}[x, y]/(\ker(\psi)) \hookrightarrow \mathbb{K}(t)$ qui montre que $\ker(\psi)$ est un idéal premier puisque $\mathbb{K}(t)$ est intègre. Ainsi, $V(\ker(\psi))$ est irréductible. Or, l'image de ϕ est contenue dans $V(\ker(\psi))$ et $\mathcal{C}$ est l'adhérence de cette image, c'est-à-dire le plus petit fermé que l'a contient. Il s'en suit que $\mathcal{C} = V(\ker(\psi))$. □

IL est bien connu que toutes les courbes algébriques planes, même irréductibles, ne sont pas forcément rationnelles. En fait, les courbes rationnelles sont les courbes dont le nombre de points singuliers, comptés avec leur multiplicité respective, est maximum ; autrement dit les courbes de "genre géométrique" nul.

1.4.3 Degré d'une paramétrisation

Commençons par un rappeler le résultat suivant. Soit $\mathbb{K}$ un corps et X une indéterminée. Par définition, pour tout $\eta \in \mathbb{K}(X)$ il existe deux polynômes $f, g \in \mathbb{K}[X]$, avec $g \neq 0$ et $\mathrm{pgcd}(f, g) = 1$, tels que $\eta = f(X)/g(X) \in \mathbb{K}(X)$. On définit alors le *degré* de η par

$$\deg(\eta) := \max(\deg(f), \deg(g))$$

Proposition 1.4.6 *Soit $\eta \in \mathbb{K}(X) \setminus \mathbb{K}$. Alors,*
(i) *$\mathbb{K}(X)$ est une extension algébrique sur $\mathbb{K}(\eta)$,*
(ii) *η est transcendant sur $\mathbb{K}$,*
(iii) *$\deg(\eta) = [\mathbb{K}(X) : \mathbb{K}(\eta)]$.*

Supposons à présent donnée une courbe rationnelle $\mathcal{C}$ paramétrée par

$$\phi : \mathbb{A}^1_{\mathbb{K}} \to \mathbb{A}^2_{\mathbb{K}} : t \mapsto (p(t), q(t)) \tag{1.18}$$

où $\mathbb{K}$ est un corps et $p(t), q(t)$ deux fractions rationnelles de $\mathbb{K}(t)$, non toutes les deux constantes (c'est-à-dire dont l'image n'est pas réduite à un point).

Définition 1.4.7 *Avec les notations précédentes, on appelle degré de la paramétrisation ϕ l'entier*

$$\deg(\phi) := [\mathbb{K}(t) : \mathbb{K}(p(t), q(t))].$$

Noter que d'après ce qui précède, $\mathbb{K}(t)$ est bien une extension algébrique sur $\mathbb{K}(p(t), q(t))$, donc que $\deg(\phi)$ est bien défini. On montre que si $\mathbb{K}$ est algébriquement clos, ce degré est le nombre de points distincts dans une fibre générique de la co-restriction de ϕ à la courbe $\mathcal{C}$, autrement dit le nombre d'antécédents d'un point générique pris sur la courbe $\mathcal{C}$, autrement dit le nombre de points dans une fibre générique de $\phi_{|\mathcal{C}} : \mathbb{A}^1_{\mathbb{K}} \xrightarrow{\phi} \mathcal{C} \subset \mathbb{A}^2_{\mathbb{K}}$.

Précisons que l'égalité $\deg(\phi) = 1$ n'implique pas que ϕ est une application injective, mais seulement génériquement injective, comme on peut le voir sur la paramétrisation

$$\mathbb{C} \mapsto \mathbb{C}^2 : t \mapsto (t^2 - 1, t(t^2 - 1))$$

de la courbe $V(Y^2 - X^2(X+1))$. En effet, on vérifie aisément que ϕ n'est injective que sur $\mathbb{C} \setminus \{-1, +1\}$; les paramétres -1 et $+1$ étant tous les deux envoyés sur l'origine $(0, 0)$.

1.4.4 Reparamétrisation propre d'une courbe rationnelle

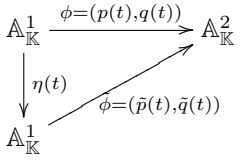
Soit $\eta = f(X)/g(X) \in \mathbb{K}(X)$ tel que $\mathbb{K} \subsetneq \mathbb{K}(\eta) \subset \mathbb{K}(X)$, où f et g sont des polynômes premiers entre eux dans $\mathbb{K}[X]$ avec $g \neq 0$. Nous avons vu que $\mathbb{K}(X)$ est une extension algébrique sur $\mathbb{K}(\eta)$, qui est elle-même transcendante sur $\mathbb{K}$. De plus, $\deg(\eta) = [\mathbb{K}(X) : \mathbb{K}(\eta)]$ qui ne dépend donc que de $\mathbb{K}(\eta)$ et de $\mathbb{K}(X)$; par conséquent on en déduit que

$$\mathbb{K}(X) = \mathbb{K}(\eta) \Leftrightarrow \deg(\eta) = 1.$$

En d'autres termes, les $\mathbb{K}$-automorphismes de $\mathbb{K}(X)$ sont les homographies $X \mapsto \frac{aX+b}{cX+d}$, où $ad - bc \neq 0$.

Théorème 1.4.8 (Lurôth) *Soit $\mathbb{L}$ un corps tel que $\mathbb{K} \subsetneq \mathbb{L} \subseteq \mathbb{K}(X)$. Alors il existe $\eta \in \mathbb{K}(X) \setminus \mathbb{K}$ tel que $\mathbb{L} = \mathbb{K}(\eta)$.*

Un corollaire immédiat du théorème de Lurôth est que toute courbe rationnelle admet une paramétrisation propre (ou birationnelle), c'est-à-dire une paramétrisation de degré 1. En effet, d'après Lurôth, il existe $\eta(t) \in \mathbb{K}(t)$ tel que $\mathbb{K}(\eta(t)) = \mathbb{K}(p(t), q(t))$, et donc $p(t) = \tilde{p}(\eta(t))$ et $q(t) = \tilde{q}(\eta(t))$ où $\tilde{p}(t)$ et $\tilde{q}(t)$ sont des fractions rationnelles de $\mathbb{K}(t)$. On a donc un diagramme commutatif



où l'on montre que $\deg(\tilde{\phi}) = 1$ puisque

$$\begin{aligned}\deg(\phi) = [\mathbb{K}(t) : \mathbb{K}(p, q)] &= [\mathbb{K}(t) : \mathbb{K}(\eta)][\mathbb{K}(\eta) : \mathbb{K}(p, q)] \\ &= [\mathbb{K}(t) : \mathbb{K}(\eta)][\mathbb{K}(t) : \mathbb{K}(\tilde{p}, \tilde{q})] \\ &= \deg(\eta)\deg(\tilde{\phi}) = \deg(\phi)\deg(\tilde{\phi}).\end{aligned}$$

1.4.5 Implicitation d'une courbe rationnelle

On suppose donnée une courbe rationnelle (donc irréductible) $\mathcal{C}$ représentée par une paramétrisation, comme dans (1.17),

$$\phi : \mathbb{A}^1_{\mathbb{K}} \to \mathbb{A}^2_{\mathbb{K}} : t \mapsto (p(t), q(t))$$

où $\mathbb{K}$ est un corps et p, q sont deux fractions rationnelles de $\mathbb{K}(t)$ non toutes les deux constantes (sinon ϕ décrit un point et non une courbe). En outre, on note $p(t) = p_1(t)/p_2(t)$, $m := \deg(p)$ et $q(t) = q_1(t)/q_2(t)$, $n = \deg(q)$ où p_1, p_2, q_1, q_2 sont des polynômes de $\mathbb{K}[t]$ tels que $p_2 \neq 0$, $q_2 \neq 0$ et $\mathrm{pgcd}(p_1, p_2) = \mathrm{pgcd}(q_1, q_2) = 1$. Rappelons que l'idéal $I_{\mathcal{C}}$ n'est autre que le noyau de l'application (voir le lemme 1.4.5)

$$\psi : \mathbb{K}[x, y] \to \mathbb{K}(t) : f(x, y) \mapsto f(p(t), q(t)).$$

Théorème 1.4.9 *Avec les notations précédentes, on a l'égalité entre idéaux de* $\mathbb{K}[x, y]$

$$I_{\mathcal{C}}^{\deg(\phi)} = (\mathrm{Res}_{m,n}(p_1(t) - xp_2(t), q_1(t) - yq_2(t))).$$

En d'autres termes, ce résultant fournit une équation implicite de $\mathcal{C}$ *élevée à la puissance* $\deg(\phi)$.

Preuve. Pour simplifier les notations, on pose

$$f(t) := p_1(t) - xp_2(t) \quad \text{et} \quad g(t) := q_1(t) - yq_2(t).$$

Ce sont des polynômes en la variable t, de degré m et n respectivement, à coefficients dans $\mathbb{K}[x, y]$.

Nous supposons tout d'abord que $\deg(\phi) = 1$, c'est-à-dire que la paramétrisation ϕ est birationnelle de $\mathbb{A}^1_{\mathbb{K}}$ sur $\mathcal{C}$, et on veut montrer que $I_{\mathcal{C}} = (\mathrm{Res}_{m,n}(f, g))$. D'après la proposition 1.1.3, ce dernier résultant appartient à l'idéal (f, g). Or, f et g sont clairement dans le noyau de ψ si l'on étend cette application à $\mathbb{K}[x, y, t]$ (où l'on envoit t sur t). On a donc l'inclusion $(\mathrm{Res}_{m,n}(f, g)) \subset I_{\mathcal{C}}$. Remarquons également que $f(t)$ et $g(t)$ sont premiers entre eux dans $\mathbb{K}(x, y)[t]$ (on le voit dans $\mathbb{K}[x, y][t]$ puis on invoque le lemme de Gauss), ce qui montre que $\mathrm{Res}_{m,n}(f, g) \neq 0$ dans $\mathbb{K}[x, y]$ d'après la proposition 1.1.4. Pour montrer l'autre inclusion, c'est-à-dire $I_{\mathcal{C}} \subset (\mathrm{Res}_{m,n}(f, g))$, on va s'intéresser au degré de ce résultant. Rappelons que tout générateur de $I_{\mathcal{C}}$ est de degré $\deg(\mathcal{C})$ par la définition 1.4.2.

Plongeons-nous dans la clotûre algébrique de $\mathbb{K}$ (qui est un corps infini), ce qui ne change pas $\deg(\mathcal{C})$. L'intersection de $\mathcal{C}$ et de la droite a l'infini étant fini et les points singuliers de $\mathcal{C}$ étant également en nombre fini, on déduit de la proposition 1.4.3 que toute droite, d'équation $ax + by + c = 0$, suffisamment générique coupe la courbe $\mathcal{C}$ en $\deg(\mathcal{C})$ points simples (il s'agit de choisir a, b, c de telle sorte que la droite $ax + by + c = 0$ évite les points singuliers et à l'infini de $\mathcal{C}$) appartenant à l'image de ϕ et n'ayant qu'un seul antécédent (là encore, il faut éviter un nombre fini de points de $\mathcal{C}$). L'intersection entre $\mathcal{C}$ et cette droite correspond, dans l'espace des paramétres, à l'équation polynomiale

$$\frac{ap_1(t)q_2(t) + bq_1(t)p_2(t) + cp_2(t)q_2(t)}{\mathrm{pgcd}(p_2(t), q_2(t))} = 0 \tag{1.19}$$

qui est donc de degré $d := \deg(\mathcal{C})$.

Notant $r(t) := \mathrm{pgcd}(p_2(t), q_2(t))$, la multiplicativité 1.2.3 du résultant montre que

$$\mathrm{Res}_{d,d}(\frac{q_2(t)}{r(t)}f(t), \frac{p_2(t)}{r(t)}g(t)) = \mathrm{Res}(\frac{q_2(t)}{r(t)}, \frac{p_2(t)}{r(t)})\mathrm{Res}(\frac{q_2(t)}{r(t)}, g(t))\mathrm{Res}(f(t), \frac{p_2(t)}{r(t)})\mathrm{Res}_{m,n}(f(t), g(t))$$

(on laisse le soin au lecteur de compléter les degrés manquant en indice), c'est-à-dire que

$$\mathrm{Res}_{d,d}(\frac{q_2(t)}{r(t)}f(t), \frac{p_2(t)}{r(t)}g(t)) = c\mathrm{Res}_{m,n}(f(t), g(t))$$

où $c \in \mathbb{K} \setminus \{0\}$ (les trois autres résultants de la formule précédente sont des constantes non nulles dans $\mathbb{K}$; le vérifier en exercice). Or, il est immédiat de remarquer que ce dernier résultant est un polynôme dans $\mathbb{K}[x, y]$ de degré au plus $d = \deg(\mathcal{C})$ en regardant sa matrice de Sylvester associée puisque x et y ont le même coefficient : $p_2(t)q_2(t)/r(t)$ (c'est une conséquence directe de la multilinéarité du résultant). Mais nous avons vu que $\mathrm{Res}_{m,n}(f, g) \in I_{\mathcal{C}}$ et qu'il est non nul ; il s'en suit $Res_{m,n}(f, g)$ est de degré $d = \deg(\mathcal{C})$ et que c'est un générateur de $I_{\mathcal{C}}$.

Il nous reste à examiner le cas où $\deg(\phi)$ est quelconque. Pour cela, nous allons reparamétrer notre courbe rationnelle. Comme décrit en 1.4.4, nous pouvons trouver des fractions rationnelles $\eta(t)$, $\tilde{p}(t)$ et $\tilde{q}(t)$ telles que $p(t) = \tilde{p}(\eta(t))$, $q(t) = \tilde{q}(\eta(t))$ et

$$\tilde{\phi} : \mathbb{A}^1_{\mathbb{K}} \to \mathbb{A}^2_{\mathbb{K}} : t \mapsto (\tilde{p}(t), \tilde{q}(t)),$$

soit une paramétrisation de $\mathcal{C}$ de degré 1. De ce que nous venons de voir, nous déduisons, avec des notations évidentes, que

$$I_{\mathcal{C}} = \left(\mathrm{Res}_{\frac{m}{deg(\phi)}, \frac{n}{\deg(\phi)}}(\tilde{p}_1(t) - x\tilde{p}_2(t), \tilde{q}_1(t) - x\tilde{q}_2(t))\right) \in \mathbb{K}[x, y].$$

Or la formule de changement de base 1.2.6 pour le résultant montre que

$$\begin{aligned} \mathrm{Res}_{m.n}(f, g) &= \mathrm{Res}_{m,n}(\tilde{p}_1(\eta(t)) - x\tilde{p}_2(\eta(t)), \tilde{q}_1(\eta(t)) - y\tilde{q}_2(\eta(t)))) && (1.20) \\ &= c' \,\mathrm{Res}_{\frac{m}{deg(\phi)}, \frac{n}{\deg(\phi)}}(\tilde{p}_1(t) - x\tilde{p}_2(t), \tilde{q}_1(t) - x\tilde{q}_2(t))^{\deg(\phi)} \in \mathbb{K}[x, y] && (1.21) \end{aligned}$$

où $c' \in \mathbb{K} \setminus \{0\}$, ce qui achève la preuve de ce théorème. □

Un corollaire de cette preuve est qu'il est possible de prévoir le degré de $\mathcal{C}$ à partir de sa paramétrisation (c'est l'entier d dans la preuve ci-dessus). Pour énoncer ce résultat de manière simple et confortable, il faut se placer dans le contexte projectif. On suppose donc donnée une courbe projective irréductible $\mathcal{C}$ paramétrée par

$$\phi : \mathbb{P}^1_{\mathbb{K}} \to \mathbb{P}^2_{\mathbb{K}} : (s : t) \mapsto (p(s, t) : q(s, t) : r(s, t)),$$

où $\mathbb{K}$ est un corps et $p, q, r(s, t)$ des polynômes homogènes dans $\mathbb{K}[s, t]$ de même degré (forcément) $D \geq 1$. Comme nous l'avons déjà montré dans le lemme 1.4.5, l'idéal homogène et premier $I_{\mathcal{C}}$ est alors le noyau de l'application

$$\psi : \mathbb{K}[x, y, z] \to \mathbb{K}[s, t] : f(x, y, z) \mapsto f(p(s, t), q(s, t), r(s, t)).$$

Ainsi, on a un isomorphisme gradué $I_{\mathcal{C}} \simeq \mathbb{K}[x, y, z](-\deg(\mathcal{C}))$ qui est donné par une équation implicite de la courbe $\mathcal{C}$.

Proposition 1.4.10 *Avec les notations précédentes,* $D - \deg(\mathrm{pgcd}(p, q, r)) = \deg(\phi)\deg(\mathcal{C})$.

Preuve. C'est une conséquence de la preuve du théorème 1.4.9 qui s'obtient á l'aide de l'équation polynomiale (1.19) dont on sait qu'elle est de degré $\deg(\phi)\deg(\mathcal{C})$. □

Intersection de deux courbes dont une est rationnelle. Les courbes utilisées en CAO (Conception assistée par ordinateur) sont souvent des courbes rationnelles représentées par des paramétrisations. Prenons par exemple deux telles courbes

$$\phi_1 : \mathbb{A}^1_{\mathbb{K}} \to \mathbb{A}^2_{\mathbb{K}} : t \mapsto (p(t), q(t)),$$

$$\phi_2 : \mathbb{A}^1_{\mathbb{K}} \to \mathbb{A}^2_{\mathbb{K}} : s \mapsto (u(s), v(s)).$$

Ces deux courbes sont bien souvent utilisées pour décrire le bord de certains objets (Boundary Representation) et il est indispensable de savoir "calculer l'intersection" entre deux objets, c'est-à-dire décrire l'intersection de deux courbes paramétrées.

Pour résoudre ce problème, on peut écrire un système polynomial en les variables s et t puis le résoudre. Mais le paragraphe précédent nous montre que l'on peut faire mieux : si l'on calcul une équation implicite, disons de la courbe paramétrée par ϕ_1, et que l'on substitue la paramétrisation de ϕ_2 dans cette équation, on obtient alors une équation en une seule variable, ici s, dont les solutions correspondent à des valeurs du paramètre de la deuxième courbe dont l'image est un point d'intersection des deux courbes. Il faut également noter que puisqu'une équation implicite peut-être obtenue par un calcul de résultant, elle peut-être décrite comme le déterminant d'une matrice (généralement de Sylvester ou de Bézout) à entrées dans $\mathbb{K}[x, y]$. Si l'on substitue alors la paramétrisation de la deuxième courbe dans cette matrice (et non pas dans son déterminant), on ramène le problème de résolution d'un polynôme univarié à un problème de valeurs propres, comme nous l'avons brièvement décrit au paragraphe 1.3.3.3 ; c'est un des avantages indéniables des résultants comme outil pour l'élimination.

1.4.6 Inversion d'une courbe rationnelle

Dans ce paragraphe, étant donnée une courbe rationnelle représentée par une paramétrisation (1.17), nous nous intéressons aux deux problèmes suivants :

- Tester si la paramétrisaton est birationnelle, i.e. de degré 1,
- Si $\deg(\phi) = 1$, calculer un inverse de ϕ, c'est-à-dire une application rationnelle

$$\rho : \mathbb{A}^2_{\mathbb{K}} \to \mathbb{A}^1_{\mathbb{K}} : (x, y) \mapsto \rho(x, y)$$

telle que $\rho \circ \phi(t) = t$ pour tout $t \in \mathbb{A}^1_{\mathbb{K}}$, excepté peut-être pour un nombre fini de valeurs de t.

Supposons donnée une courbe rationnelle $\mathcal{C}$ paramétrée par (1.17)

$$\phi : \mathbb{A}^1_{\mathbb{K}} \to \mathbb{A}^2_{\mathbb{K}} : t \mapsto \left(p(t) = \frac{p_1(t)}{p_2(t)}, \frac{q_1(t)}{q_2(t)} \right),$$

où $\operatorname{pgcd}(p_1, p_2) = \operatorname{pgcd}(q_1, q_2) = 1$. On suppose en outre que $\mathcal{C}$ n'est pas une droite (auquel cas le test de birationnalité et l'inversion sont triviaux), ce qui entraîne que les entiers $m := \deg(p)$ et $n := \deg(q)$ sont tous les deux plus grands que 1. Nous avons vu dans ce qui précède que

$$\operatorname{Res}_{m,n}(p_1(t) - xp_2(t), q_1(t) - yq_2(t)) = C(x, y)^{\deg(\phi)}$$

où $C(x, y)$ est une équation implicite de la courbe $\mathcal{C}$. De plus, nous savons que la matrice de Sylvester associée à ce résultant vérifie (voir (1.2))

$$ {}^tS_{m,n}(p_1(t) - xp_2(t), q_1(t) - yq_2(t)) \begin{pmatrix} t^{m+n-1} \\ t^{m+n-2} \\ \vdots \\ t \\ 1 \end{pmatrix} = \begin{pmatrix} t^{n-1}(p_1(t) - xp_2(t)) \\ \vdots \\ t(p_1(t) - xp_2(t)) \\ p_1(t) - xp_2(t) \\ t^{m-1}(q_1(t) - yq_2(t)) \\ \vdots \\ t(q_1(t) - yq_2(t)) \\ q_1(t) - yq_2(t) \end{pmatrix}. \tag{1.22}$$

Dans ce qui suit, nous noterons par $\mathbb{M}$ la sous-matrice de la matrice de Sylvester $S_{m,n}(p_1(t) - xp_2(t), q_1(t) - yq_2(t))$ obtenue en effaçant sa dernière colonne. Pour $i = 1, \ldots, m + n$, on note également Δ_i le déterminant signé de $\mathbb{M}$ obtenu en effaçant la $i^{\text{ième}}$ ligne. Ainsi,

$$\operatorname{Res}_{m,n}(p_1(t) - xp_2(t), q_1(t) - yq_2(t)) = \sum_{i=1}^{m+n} c_i \Delta_i, \tag{1.23}$$

où les $c_i \in \mathbb{K}[y]$ sont les entrées de la dernière colonne de la matrice de Sylvester (celle que l'on a effacée pour définir $\mathbb{M}$), i.e. $q_1(t) - yq_2(t) = \sum_{i=0}^{m+n-1} c_i t^{m+n-1-i}$.

Proposition 1.4.11 *Avec les notations précédentes, on a*

$$\deg(\phi) = 1 \Leftrightarrow \operatorname{pgcd}(\Delta_1, \ldots, \Delta_{m+n}) \in \mathbb{K} \setminus \{0\}.$$

De plus, si $\deg(\phi) = 1$ *alors pour tout* $i = 1, \ldots, m + n - 1$ *l'application rationnelle*

$$\mathbb{A}^2_{\mathbb{K}} \to \mathbb{A}^1_{\mathbb{K}} : (x, y) \mapsto \frac{\Delta_i}{\Delta_{i+1}}$$

est une inversion de ϕ.

Preuve. Supposons que $\deg(\phi) = 1$. Alors (1.23) montre que $\operatorname{pgcd}(\Delta_1, \ldots, \Delta_{m+n})$ ne peut être qu'une constante non nulle car le résultant y est irréductible et au moins un des c_i dépend de y.

Supposons maintenant que $\text{pgcd}(\Delta_1, \cdots, \Delta_{m+n}) \in \mathbb{K} \setminus \{0\}$. On en déduit qu'il existe un entier $i \in \{1, \cdots, m+n\}$ tel que $\Delta_i \neq 0$ dans $\mathbb{K}[x,y]$ et surtout tel que Δ_i ne s'annule pas identiquement sur $\mathcal{C}$, i.e $\Delta_i \notin I_{\mathcal{C}}$. Rappelons que l'idéal premier $I_{\mathcal{C}}$ associé à la courbe $\mathcal{C}$ est le noyau de l'application

$$\psi : \mathbb{K}[x,y] \to \mathbb{K}(t) : f(x,y) \mapsto f(p(t), q(t))$$

et que montrer que $\deg(\phi) = 1$ revient à montrer que $\mathbb{K}(p(t), q(t)) = \mathbb{K}(t)$, c'est-à-dire que $t \in \mathbb{K}(p(t), q(t))$. En fait, il s'agit de voir que l'application injective entre corps

$$\overline{\psi} : \text{Frac}(\mathbb{K}[x,y]/I_{\mathcal{C}}) \hookrightarrow \mathbb{K}(t) : f(x,y)/g(x,y) \mapsto f(p(t),q(t))/g(p(t),q(t)),$$

dont l'image est $\mathbb{K}(p(t), q(t))$, est surjective (noter que $\deg(\phi) = [\mathbb{K}(t) : \text{Frac}(\mathbb{K}[x,y]/I_{\mathcal{C}})]$). Pour le montrer, il faut tout d'abord observer que la matrice $\mathbb{M} \otimes_{\mathbb{K}[x,y]} \text{Frac}(\mathbb{K}[x,y]/I_{\mathcal{C}})$, c'est-à-dire la matrice $\mathbb{M}$ vue comme matrice à coefficients dans $\text{Frac}(\mathbb{K}[x,y]/I_{\mathcal{C}})$, est de rang $m+n-1$ puisque que l'on a un $\Delta_i \notin I_{\mathcal{C}}$, et donc ${}^t\mathbb{M}$ a un noyau de rang 1 qui est engendré par le vecteur colonne non nul

$${}^t(\Delta_1, \ldots, \Delta_{m+n-1}, \Delta_{m+n}).$$

Mais alors, $\overline{\psi}({}^t\mathbb{M})$ est une matrice (à coefficients dans $\mathbb{K}(t)$) de rang $m+n-1$ (puisque $\overline{\psi}$ est injective) dont on voit, grâce à (1.22), que le noyau est engendré par le vecteur colonne

$${}^t(t^{m+n-1}, \ldots, t, 1).$$

On en déduit donc que

$$(\psi(\Delta_1), \ldots, \psi(\Delta_{m+n})) = \overline{\psi}\left((\Delta_1, \ldots, \Delta_{m+n-1}, \Delta_{m+n})\right) = r(t)(t^{m+n-1}, \ldots, t, 1),$$

où $r(t) \in \mathbb{K}(t) \setminus \{0\}$, et donc que

$$\frac{\psi(\Delta_1)}{\psi(\Delta_2)} = \frac{\psi(\Delta_2)}{\psi(\Delta_3)} = \cdots = \frac{\psi(\Delta_{m+n-1})}{\psi(\Delta_{m+n})} = t \in \mathbb{K}(t).$$

Il s'en suit que $\overline{\psi}$ est bien surjective (puisque $\overline{\psi}(\frac{\Delta_i}{\Delta_{i+1}}) = \frac{\psi(\Delta_i)}{\psi(\Delta_{i+1})}$) et que les applications rationnelles, pour $i = 1, \ldots, m+n-1$,

$$\mathbb{A}^2 \to \mathbb{A}^1 : (x,y) \mapsto \Delta_i/\Delta_{i+1}$$

donnent des inverses de la paramétrisation ϕ de la courbe $\mathcal{C}$. □

Noter qu'il est tout à fait possible de transposer ces deux dernières propositions au cas où l'on substitue la matrice de Bézout à la matrice de Sylvester comme représentation matricielle du résultant.

Exemple 1.4.1 *On considère l'exemple très simple du cercle unité que l'on paramètre classiquement par*

$$\phi : \mathbb{A}^1_{\mathbb{K}} \to \mathbb{A}^2_{\mathbb{K}} : t \mapsto \left(\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right).$$

La matrice de Sylvester associée est donc

$$S_{2,2}(2t - x(1+t^2), 1 - t^2 - y(1+t^2)) = \begin{pmatrix} -x & 0 & -1-y & 0 \\ 2 & -x & 0 & -1-y \\ -x & 2 & 1-y & 0 \\ 0 & -x & 0 & 1-y \end{pmatrix}.$$

À ce stade, on peut utiliser le théorème 1.4.9 : le déterminant de cette matrice de Sylvester vaut $4(x^2 + y^2 - 1)$*, ce qui montre que* ϕ *est de degré 1 et qu'une équation implicite du cercle est, comme attendu,* $x^2 + y^2 - 1 = 0$.

Afin d'illustrer la proposition 1.4.11, introduisons à présent la matrice

$$\mathbb{M} = \begin{pmatrix} -x & 0 & -1-y \\ 2 & -x & 0 \\ -x & 2 & 1-y \\ 0 & -x & 0 \end{pmatrix}.$$

Ses mineurs maximaux sont

$$\Delta_1 = 2x(y-1),\ \Delta_2 = -2x^2,\ \Delta_3 = -2x(y+1),\ \Delta_4 = 2x^2 - 4(y+1).$$

Le pgcd de ces quatres déterminants vaut 2, donc ϕ est propre dès que $2 \neq 0$ dans $\mathbb{K}$ (noter que si $2 = 0$ dans $\mathbb{K}$, alors ϕ ne décrit pas une courbe, mais un point, le point $(0,1)$), et l'on vérifie alors que

$$\frac{\Delta_1}{\Delta_2} = \frac{\Delta_2}{\Delta_3} = \frac{\Delta_3}{\Delta_4} \in \mathrm{Frac}(\mathbb{K}[x,y]/I_{\mathcal{C}}),$$

par exemple

$$\frac{\Delta_1}{\Delta_2} - \frac{\Delta_2}{\Delta_3} = \frac{2x(y-1)}{-2x^2} - \frac{-2x^2}{-2x(y+1)} = -\frac{x^2+y^2-1}{x(y+1)} = 0,$$

et que l'on a les formules d'inversion

$$\frac{\psi(\Delta_1)}{\psi(\Delta_2)} = \frac{\psi(\Delta_2)}{\psi(\Delta_3)} = \frac{\psi(\Delta_3)}{\psi(\Delta_4)} = t \in \mathbb{K}(t),$$

par exemple,

$$\frac{\psi(\Delta_1)}{\psi(\Delta_2)} = \overline{\psi}\left(\frac{1-y}{x}\right) = \left(\frac{1+t^2}{2t}\right)\left(1 - \frac{1-t^2}{1+t^2}\right) = t.$$

1.5 Et l'implicitation d'une surface rationnelle ?

Supposons donnée une surface rationnelle paramétrée par

$$\phi : \mathbb{A}^2_{\mathbb{K}} \to \mathbb{A}^3_{\mathbb{K}} : (s,t) \mapsto \left(\frac{p_1(s,t)}{p_2(s,t)}, \frac{q_1(s,t)}{q_2(s,t)}, \frac{r_1(s,t)}{r_2(s,t)}\right)$$

Notons X, Y, Z les coordonnées dans $\mathbb{A}^3_{\mathbb{K}}$. Impliciter cette surface rationnelle revient à éliminer les variables s et t du système algébriques

$$\begin{cases} Xp_2(s,t) - p_1(s,t) &= 0 \\ Yq_2(s,t) - q_1(s,t) &= 0 \\ Zr_2(s,t) - r_1(s,t) &= 0 \end{cases}$$

La tentation est donc grande d'éliminer tout d'abord une variable, disons t, en calculant deux résultants de deux équations, par exemple :

$$R_1 := \mathrm{Res}_t(Xp_2(s,t) - p_1(s,t), Yq_2(s,t) - q_1(s,t)) \in \mathbb{K}[X,Y,s] \tag{1.24}$$
$$R_2 := \mathrm{Res}_t(Xp_2(s,t) - p_1(s,t), Zr_2(s,t) - r_1(s,t)) \in \mathbb{K}[X,Z,s] \tag{1.25}$$

puis finalement d'éliminer s dans ces deux équations R_1 et R_2. Notons $H(X,Y,Z) \in \mathbb{K}[X,Y,Z]$ le résultat de ce processus. On montre alors facilement que l'équation implicite est un facteur irréductible de H. Et malheureusement, on se convainc très vite à l'aide d'un raisonnement géométrique que H n'est généralement par une l'équation implicite recherchée.

Exemple 1.5.1 *Considérons la paramétrisation suivante :*

$$\phi : \mathbb{A}^2_{\mathbb{K}} \to \mathbb{A}^3_{\mathbb{K}} : (s,t) \mapsto \left(1 - 2s^2 - st - 3s - 3t^2 - t, -2 + s^2 - 2st - 2s - 2t^2 - t, -3 + 3st - 2s - 3t^2 + t\right)$$

On trouve alors

$$R_1 = 61 - 15s - 31X + 47Y - 117s^2 - 12XY + 4X^2 - 5sY + 36Xs^2 - 46Ys^2 + 9Y^2 + 6Xs + 69s^4 + 33s^3$$

puis

$$R_2 = 156 - 18s - 66X + 78Z + 3s^2 + 9X^2 + 72Xs^2 + 48Xs + 108s^4 + 228s^3 + 9Z^2 - 24Zs^2 - 18XZ$$

Ensuite, le calcul du résultant de R_1 et R_2 éliminant s donne $243 \times P \times Q$ où

$$\begin{aligned} P = (&41099+232192X-416669Y+506391Z+309919XY-126913X^2-87283Y^2+198609Z^2-162444XZ \\ &+ 2496ZXY + 3249ZX^2 + 25389ZY + 26955Z^3 + 243X^4 + 1587Z^4 + 3888Y^4 + 15957X^3 + 13104Y^3 \\ &- 55152X^2Y + 39996XY^2 + 23920Z^2Y - 50385XZ^2 + 1458X^2Z^2 + 1620X^3Z - 1944X^2Y^2 - 4140Z^3X \\ &+ 4968Z^2Y^2 - 6480XZY^2 + 4452ZY^2) \end{aligned}$$

et

$$\begin{aligned} Q = (&-33294794X - 5118385Y + 49487931Z + 7821955XY + 4867599X^2 - 7608105Y^2 + 14309649Z^2 \\ &+ 2682720Z^2XY - 24208020XZ + 3700848ZXY + 3047661ZX^2 + 3758145ZY + 3096063Z^3 + 169X^4 \\ &+ 385641Z^4 + 944784Y^4 - 1195104X^2ZY - 527X^3 - 3593808Y^3 - 2066440X^2Y + 513036XY^2 \\ &- 4599720Z^2Y - 6109533XZ^2 + 672246X^2Z^2 - 21060X^3Z + 18720X^3Y + 543672X^2Y^2 - 1006020Z^3X \\ &+2426040Z^2Y^2-1371168Z^3Y+1399680XY^3-2146176Y^3Z-3164400XZY^2+6324372ZY^2+57646951) \end{aligned}$$

On peut alors vérifier que P est une équation implicite pour notre surface paramétrée.

Cette situation pose donc deux problèmes : comment calculer directement l'équation implicite de cette surface paramétrée ? Enfin, quel est ce facteur "parasite", peut-on le calculer ?

Chapitre 2

Le résultant multivarié

Cette partie est consacrée à l'étude du résultant dit de Macaulay qui permet d'éliminer n variables de n équations homogènes en ces variables. Après avoir rappelé le célèbre théorème de l'élimination, l'existence de ce résultant est montrée à l'aide des formes d'inerties. Cette approche du résultant permet à la fois d'obtenir des preuves relativement élémentaires, mais également de fournir des outils essentiels pour son calcul ou sa représentation. On termine par un bref rappel de la formule de Poisson et quelques-unes de ces applications.

2.1 Théorème de l'élimination

Le théorème de l'élimination est un résultat assez ancien qui est devenu un résultat élémentaire de la théorie des schémas (voir par exemple [Har77, chapter II, theorem 4.9]). Des énoncés et des preuves plus standards se trouvent dans de nombreux livres de géométrie algébrique classique, par exemple [Har92]. Pour ce qui nous concerne, nous énoncerons ce théorème dans un cadre algébrique, cadre qui est le plus adapté au calcul. Pour cela, nous nous inspirerons fortement de [CT78] (voir aussi [Bou69]).

Rappelons qu'un anneau R est dit gradué (plus précisemment $\mathbb{N}$-gradué) s'il peut être décomposé, comme groupe abélien, en une somme directe

$$R := R_0 \oplus R_1 \oplus \cdots \oplus R_n \oplus \cdots$$

et si on a, pour tout couple (m, n) d'entiers, la relation $R_n R_m \subset R_{n+m}$. Le groupe R_i est alors appelé la partie homogène de degré i de R.

Un idéal I d'un anneau gradué R est dit gradué s'il peut être engendré par des éléments homogènes (i.e. des éléments appartenant à des parties homomgènes de R) ou bien, de manière équivalente, si l'on a l'égalité $I = \oplus_{i\in\mathbb{N}} I \cap R_i$.

2.1.1 Zéros d'un idéal

Soit A un anneau, n un entier strictement positif et I un idéal de l'anneau des polynômes $A[X_1, \ldots, X_n]$. Si B est un anneau et $h : A \to B$ un morphisme d'anneaux, pour tout $P \in A[X_1, \ldots, X_n]$ nous noterons h_P l'élément de $B[X_1, \ldots, X_n]$ image de P par l'extension canonique de h aux anneaux de polynômes.

Un élément $b = (b_1, \ldots, b_n) \in B^n$ sera appelé un *zéro de I dans B^n* si $h_P(b_1, \ldots, b_n) = 0$ pour tout $P \in I$. Aussi, si l'idéal I est engendré par les polynômes $P_1, \ldots, P_r$ on parle également d'un *zéro commun aux polynômes $P_1, \ldots, P_r$ dans B^n*. Si I est un idéal gradué et si $h(I \cap A) = 0$, il est clair que $(0, \ldots, 0) \in B^n$ est un zéro de I ; on l'appelle le *zéro trivial*.

Théorème 2.1.1 (des zéros de Hilbert) *Soit $\mathbb{K}$ un corps et $\overline{\mathbb{K}}$ une clotûre algébrique de $\mathbb{K}$. On a les propriétés suivantes :*

(i) *Tout idéal I de $\mathbb{K}[X_1, \ldots, X_n]$ ne contenant pas 1 admet au moins un zéro dans $\overline{\mathbb{K}}^n$.*

(ii) *Pour qu'un idéal I de $\mathbb{K}[X_1, \ldots, X_n]$ soit maximal, il faut et il suffit qu'il existe un élément $x = (x_1, \ldots, x_n) \in \overline{\mathbb{K}}^n$ tel que I soit l'ensemble des polynômes de $\mathbb{K}[X_1, \ldots, X_n]$ nuls en x.*

(iii) *Pour qu'un polynôme P de $\mathbb{K}[X_1,\ldots,X_n]$ soit nul dans l'ensemble des zéros dans $\overline{\mathbb{K}}^n$ d'un idéal I de $\mathbb{K}[X_1,\ldots,X_n]$, il faut et il suffit qu'il existe un entier $m>0$ tel que $P^m \in I$, c'est-à-dire que $P \in \sqrt{I}$.*

Preuve. Ce théorème se trouve dans la plupart des livres traitant de géométrie algébrique élémentaire. Cet énoncé est tiré de [Bou85, Chapitre 5, §3, numéro 3]. □

Corollaire 2.1.2 *Si $\mathbb{K}$ est un corps, $\overline{\mathbb{K}}$ une clotûre algébrique de $\mathbb{K}$ et I un idéal gradué de l'anneau des polynômes $\mathbb{K}[X_1,\ldots,X_n]$, les conditions suivantes sont équivalentes :*
(i) *I possède un zéro non trivial dans $\overline{\mathbb{K}}^n$,*
(ii) *il existe une extension $\mathbb{L}$ de k telle que I possède un zéro non trivial dans $\mathbb{L}^n$.*

Preuve. Il est clair que (i) entraîne (ii). Supposons (ii) et notons $\xi=(\xi_1,\ldots,\xi_n)$ un zéro non trivial de I dans $\mathbb{L}^n$. Puisqu'il existe un i tel que $\xi_i\neq 0$, on a $X_i^m \notin I$ pour ce même i et pour tout entier m. Le théorème des zéros 2.1.1, propriété (iii), montre alors qu'il existe un zéro $\eta=(\eta_1,\ldots,\eta_n)$ de I dans $\overline{\mathbb{K}}^n$ tel que $X_i(\eta)=\eta_i\neq 0$, ce qui montre (i). □

2.1.2 Idéaux éliminants

Définition 2.1.3 *Soit A un anneau et I un idéal gradué de l'anneau des polynômes $A[X_1,\ldots,X_n]$. On appelle* idéal éliminant *de I l'idéal de A*

$$\mathfrak{A} := \cup_{n\in\mathbb{N}}(I:\mathfrak{m}^n)\cap A = \{a\in A \text{ tel que } \exists m\in\mathbb{N} : aX_i^m \in I \text{ pour tout } i=1,\ldots,n\}$$

où $\mathfrak{m}$ désigne l'idéal $(X_1,\ldots,X_n)$ de $A[X_1,\ldots,X_n]$.

Théorème 2.1.4 (de l'élimination) *Soit A un anneau, I un idéal gradué de l'anneau $A[X_1,\ldots,X_n]$, $\mathfrak{A}$ son idéal éliminant et $\rho : A\to k$ un morphism de A dans un corps k. Les conditions suivantes sont équivalentes :*
(i) *$\rho(\mathfrak{A})=0$,*
(ii) *il existe une extension $\mathbb{L}$ de k et un zéro non-trivial de I dans $\mathbb{L}^n$.*

Pour démontrer ce théorème, nous aurons besoin du

Lemme 2.1.5 *Soient A un anneau, M un A-module de type fini et $\rho : A\to k$ un morphisme de A dans un corps k. Pour que $M\otimes_A k\neq 0$ il faut et il suffit que $\rho(\mathrm{ann}_A(M))=0$.*

Preuve. Il est clair que tout élément de $\rho(\mathrm{ann}_A(M))\subset k$ annule le k-espace vectoriel $M\otimes_A k$, donc si $M\otimes_A k\neq 0$ alors il est nécessaire que $\rho(\mathrm{ann}_A(M))=0$. Inversement, supposons que $M\otimes_A k=0$ et montrons que $\rho(\mathrm{ann}_A(M))\neq 0$.

Puisque M est de type fini, il existe une suite exacte courte de A-modules

$$0\to \mathrm{Ker}(f)\xrightarrow{i} A^p \xrightarrow{\pi} M\to 0.$$

Par tensorisation, on obtient la suite exacte de k-espaces vectoriels

$$\mathrm{Ker}(f)\otimes_A k \xrightarrow{i\otimes_A k} k^p \xrightarrow{\pi\otimes_A k} M\otimes_A k\to 0$$

qui montre que $\mathrm{Ker}(f)\otimes_A k$ est surjective puisque nous avons supposé que $M\otimes_A k=0$. Il s'en suit que l'on peut trouver p éléments $n_1,\ldots,n_p\in\mathrm{Ker}(f)$ tels que la famille $(i(n_i)\otimes_A k)_{i=1,\ldots,p}$ soit une base de k^p. Notant M la matrice de taille $p\times p$ de l'application $A^p \xrightarrow{(n_1,\ldots,n_p)} A^p$ dans la base canonique, on déduit que $\rho(M)$ est une matrice inversible, i.e $\rho(\det(M))\neq 0$. Les formules de Cramer montrent alors que $\det(M)A^p\subset\mathrm{Ker}(f)$ et donc que $d\in\mathrm{ann}_A(M)$ qui montre que $\rho(\mathrm{ann}_A(M))\neq 0$. □

Preuve du théorème 2.1.4 Supposons (ii) ; soit $\xi\in\mathbb{L}^n$ est un zéro non trivial de I. Notant i l'injection de k dans son extension $\mathbb{L}$, on a $i\circ\rho(P)(\xi)=0$ pour tout $P\in I$. Si $a\in\mathfrak{A}$ alors il existe $m\in\mathbb{N}$ tel que $aX_i^m\in I$ pour $i=1,\ldots,n$ et donc

$$i\circ\rho(aX_i^m)(\xi)=(i\circ\rho(a)X_i^m)(\xi)=i\circ\rho(a)\xi_i^m=0.$$

Or, puisque ξ est un zéro non trivial, un des ξ_i est non nul et donc $i \circ \rho(a) = 0$, c'est-à-dire $\rho(a) = 0$, ce qui montre (i).

Supposons à présent que $\rho(\mathfrak{A}) = 0$ et considérons l'anneau gradué $B := A[X_1, \ldots, X_n]/I$. Nous noterons B_m, pour $m \in \mathbb{N}$, l'ensemble des éléments homogènes de degré m de B ; c'est un A-module, et même un $B_0 = A/I \cap A$-module. Puisque B_1 est un A-module de type fini et que $B_0 \cup B_1$ engendre B, nous en déduisons que pour tout m le B_0-module B_m est de type fini et que la multiplication

$$B_1 \otimes_{B_0} B_m \to B_{m+1} : x \otimes y \mapsto xy$$

est surjective. Pour tout $m \in \mathbb{N}$, il est clair que $\mathrm{ann}_{B_0}(B_m) \subset \mathfrak{A}$, donc que $\rho(\mathrm{ann}_{B_0}(B_m)) = 0$ ce qui entraîne, par le lemme 2.1.5, que $B_m \otimes_{B_0} k \neq 0$. Précisons ici que $\rho : A \to k$ se factorise en un morphisme $\overline{\rho} : B_0 \to k$ (puisque $\rho(I \cap A) = 0$) qui donne à k une structure de B_0-module.

L'anneau gradué $E := B \otimes_{B_0} k$ est donc tel que $E_0 = k$ et $E_m \neq 0$ pour tout $m \in \mathbb{N}$. Nous savons que E_1 est engendré par $\overline{X}_1, \ldots . \overline{X}_n$ et que la multiplication $E_1 \otimes E_m \to E_{m+1}$ est surjective ; ainsi, s'il existe un entier N tel que $\overline{X}_i^N = 0$ pour $i = 1, \ldots, n$ alors $E^m = 0$ pour tout $m \geq n(N-1)+1$. On en déduit donc qu'il existe un élément $\xi \in E_1$ tel que $\xi^m \neq 0$ pour tout $m \in \mathbb{N}$. De plus, l'élément $1 - \xi$ de E n'est pas inversible : si $(1-\xi)u = 1$ avec $u = u_0 + u_1 + \cdots + u_m \in E$, alors le développement

$$(1-\xi)u = (u_0) + (u_1 - \xi u_0) + (u_2 - \xi u_1) + \cdots + (u_m - \xi u_{m-1}) + (-\xi u_m) = 1$$

montre que $u_0 = 1, u_1 = \xi, u_2 = \xi^2, \ldots, u_m = \xi^m$ et finalement $\xi^{m+1} = 0$. Par conséquent, il existe un idéal maximal (donc propre) $\mathfrak{m}$ de E contenant l'élément $1 - \xi$. Soient $\mathbb{L}$ le corps $E/\mathfrak{m}$, $\overline{h} : E \to \mathbb{L}$ et $i : k \hookrightarrow \mathbb{L}$ les morphismes canoniques, on a $\overline{h}_{|E_0} = i$ et $f(\xi) = 1$.

Le morphisme $\overline{h} : E = B \otimes_{B_0} k \to \mathbb{L}$ s'étend canoniquement en un morphisme $h : B \to \mathbb{L}$ que l'on obtient par la composition

$$\begin{array}{ccccc} B & \to & E = B \otimes_{B_0} k & \stackrel{\overline{h}}{\to} & \mathbb{L} \\ b & \mapsto & b \otimes 1_k & & \end{array}$$

et qui est tel que $h_{|B_0} = \overline{\rho} : B_0 \to \mathbb{K} \hookrightarrow \mathbb{L}$ et $h(B_1) \neq 0$ (rappelons que B_1 est engendré par $\overline{X}_1, \ldots, \overline{X}_n$).

Soit $\pi : A[X_1, \ldots, X_n] \to B$. Le morphisme composé $h \circ \pi : A[X_1, \ldots, X_n] \to \mathbb{L}$ envoie tout polynôme $P \in A[X_1, \ldots, X_n]$ sur $P(\xi_1, \ldots, \xi_n) \in \mathbb{L}$ où $\xi_i := \overline{h}(\overline{X}_i) \in \mathbb{L}$. Par conséquent, $(\xi_1, \ldots, \xi_n) \in \mathbb{L}^n$ est un zéro non trivial de I, ce qui montre (ii). □

2.1.3 Interprétation géométrique

Dans la littérature, on appelle très souvent théorème de l'élimination le corollaire suivant du théorème 2.1.4 :

Corollaire 2.1.6 *Soient k un corps algébriquement clos et W une sous-variété algébrique de $\mathbb{A}_k^m \times \mathbb{P}_k^n$. Si π désigne la projection canonique de $\mathbb{A}_k^m \times \mathbb{P}_k^n$ sur $\mathbb{P}_k^n$, alors $\pi(W)$ est une sous-variété algébrique de $\mathbb{P}_k^n$.*

Le théorème 2.1.4 est plus général que le corollaire ci-dessus car il permet de remplacer $\mathbb{A}_k^n$ par une de ses sous-variétés algébriques, et même par un de ses sous-schémas. Pour être complet, on peut d'ailleurs préciser la géométrie du théorème 2.1.4 :

Soient A un anneau et I un idéal gradué de l'anneau des polynômes $A[X_1, \ldots, X_n]$. L'idéal éliminant $\mathfrak{A}$ associé est alors l'idéal de définition dans le schéma affine $\mathrm{Spec}(A)$ de la projection canonique de $\mathrm{Proj}(A[X_1, \ldots, X_n]/I)$ sur $\mathrm{Spec}(A)$ qui est donc un sous-schéma *fermé* de $\mathrm{Spec}(A)$. Rappelons que cette projection correspond à l'injection canonique

$$A \hookrightarrow B := A[X_1, \ldots, X_n]/I,$$

et le calcul suivant précise ce qui précède :

$$\begin{array}{rcl} \mathrm{Ker}\left(A = \Gamma(\mathrm{Spec}(A), \mathcal{O}_{\mathrm{Spec}(A)}) \stackrel{can}{\longrightarrow} \Gamma(\mathrm{Proj}(B), \mathcal{O}_{\mathrm{Proj}(B)})\right) & = & \mathrm{Ker}\left(A \to \prod_{i=1}^{n} B_{(X_i)}\right) \\ & = & (I :_{A[\mathbf{X}]} \mathfrak{m}^\infty) \cap A = \mathfrak{A} \end{array}$$

(la première égalité provient du fait qu'une section $s \in \Gamma(\mathrm{Proj}(B), \mathcal{O}_{\mathrm{Proj}(B)})$ est uniquement déterminée par ses restrictions aux ouverts $D^+(X_i)$, $i = 1, \ldots, n$).

2.1.4 Interprétation en termes d'annulateur

On note pour la suite

$$H^0_{\mathfrak{m}}(B) := \bigcup_{n\in\mathbb{N}} (0 :_B \mathfrak{m}^n) = \{P \in B \ \exists n \in \mathbb{N} \text{ such that } \mathfrak{m}^n P = 0\}.$$

Pour tout couple d'entiers $(\nu, t) \in \mathbb{N}^2$, définissant l'application A-linéaire

$$\Theta_{\nu,t} : B_\nu \to \mathrm{Hom}_A(B_t, B_{t+\nu}) : b \mapsto (c \mapsto b.c).$$

on déduit immédiatement que pour tout $\nu \in \mathbb{N}$

$$H^0_{\mathfrak{m}}(B)_\nu = \bigcup_{t\in\mathbb{N}} \mathrm{Ker}(\Theta_{\nu,t}). \tag{2.1}$$

De plus, pour tout couple $(\nu, t) \in \mathbb{N}^2$ on a $\mathrm{Ker}(\Theta_{\nu,t}) \subset \mathrm{Ker}(\Theta_{\nu,t+1})$. En effet, la multiplication $B_1 \otimes B_n \to B_{n+1}$ étant surjective, si $b \in \mathrm{Ker}(\Theta_{\nu,t})$ alors $b.c = 0$ pour tout $c \in B_{t+1+\nu}$ puisque $c = c_1 \otimes c_n$ et $bc_n = 0$ par hypothèse.

Par conséquent, remarquant que $\mathrm{ann}_A(B_t) = \mathrm{Ker}(\Theta_{0,t})$ pour tout $t \in \mathbb{N}$ (rappelons que $A \cap I = 0$, ce qui implique que $B_0 = A$), on obtient

$$\mathfrak{A} := H^0_{\mathfrak{m}}(B)_0 = \bigcup_{t\geq 0} \mathrm{ann}_A(B_t). \tag{2.2}$$

où $\mathrm{ann}_A(B_t) \subset \mathrm{ann}_A(B_{t+1})$ pour tout $t \in \mathbb{N}$. Ainsi, il serait très utile de savoir si cette chaîne ascendante d'annulateurs s'arrête (ce qui est clair si A est noetherien) et surtout à partir de quand elle s'arrête.

Proposition 2.1.7 *Soit un entier $\eta \in \mathbb{N}$ tel que $H^0_{\mathfrak{m}}(B)_\eta = 0$. Alors, pour tout entier $t \geq 0$ on a*

$$\mathrm{ann}_A(B_\eta) = \mathrm{ann}_A(B_{\eta+t}) = H^0_{\mathfrak{m}}(B)_0 =: \mathfrak{A}.$$

Preuve. Soit $(\nu, t) \in \mathbb{N}^2$. Il est aisé de vérifier que si $a \in \mathrm{ann}_A(B_{\nu+t})$ alors $aB_\nu \subset \mathrm{Ker}(\Theta_{\nu,t})$. En particulier, puisque l'on sait que $\mathrm{ann}_A(B_\nu) \subset \mathrm{ann}_A(B_{\nu+t})$, l'égalité $\mathrm{Ker}(\Theta_{\nu,t}) = 0$ montre que $\mathrm{ann}_A(B_\nu) = \mathrm{ann}_A(B_{\nu+t})$. Mais par hypothèse $H^0_{\mathfrak{m}}(B)_\eta = 0$. Par conséquent $\mathrm{Ker}(\Theta_{\eta,t}) = 0$ pour tout $t \in \mathbb{N}$ par (2.1), et l'on conclut par (2.2). □

Cette proposition montre qu'une fois le plus petit entier η tel que $H^0_{\mathfrak{m}}(B)_\eta = 0$ calculé (un tel entier est appelé indice de saturation de B), alors l'idéal éliminant $\mathfrak{A}$ n'est rien d'autre que $\mathrm{ann}_A(B_\eta)$. Lorsque ce dernier est un idéal principal, alors cette approche permet de faire un lien avec les idéaux de Fitting et les invariants de MacRae que l'on sait calculer.

2.2 Préliminaires : suites régulières et complexe de Koszul

Soit A un anneau commutatif unitaire. Pour tout élément $x \in A$ on définit son *complexe de Koszul homologique* comme le complexe

$$K_\bullet(x) := 0 \to K_1(x; A) = A \xrightarrow{(x)} K_0(x; A) = A \to 0,$$

où la seule application non nulle est la multiplication par x dans A.

Etant donnée une suite $\mathbf{x} := (x_1, \ldots, x_n)$ de n éléments, son complexe de Koszul homologique est défini comme

$$K_\bullet(\mathbf{x}) := K_\bullet(x_1) \otimes \cdots \otimes K_\bullet(x_n).$$

On peut cependant donner une définition plus "explicite" de ce complexe de Koszul comme suit. Le module $K_i(\mathbf{x})$ est la puissance extérieure $\wedge^i(A^n)$. Ainsi, si $\{e_1, \ldots, e_n\}$ est une base de A^n, on obtient $K_0(\mathbf{x}) = A$ et pour tout $p \in \mathbb{N}^*$

$$K_p(\mathbf{x}) = \bigoplus_{1\leq i_1<\cdots<i_p\leq n} Ae_{i_1} \wedge \cdots \wedge e_{i_p}.$$

De plus, l'application $d_p : K_p(\mathbf{x}) \to K_{p-1}(\mathbf{x})$ est l'application qui envoie $e_{i_1} \wedge \cdots \wedge e_{i_p}$ sur

$$d_p(e_{i_1} \wedge \cdots \wedge e_{i_p}) := \sum_{k=1}^{p} (-1)^{k+1} x_{i_k} e_{i_1} \wedge \cdots \wedge \widehat{e_{i_k}} \wedge \cdots \wedge e_{i_p}.$$

Il est immédiat de constater que l'on définit bien un complexe, c'est-à-dire que $d_{p-1} \circ d_p = 0$ pour tout p.

SI M est un A-module, le complexe de Koszul homologique de la suite $\mathbf{x}$ sur M est défini comme $K_\bullet(\mathbf{x}; M) := K_\bullet(\mathbf{x}) \otimes_A M = K_\bullet(\mathbf{x}; A) \otimes_A M$. Pour tout entier p, on note $H_p(\mathbf{x}; M)$ le p$^{\text{ième}}$ A-module d'homologie du complexe de Koszul $K_\bullet(\mathbf{x}; M)$.

Proposition 2.2.1 *Avec les notations précédentes,*

(i) *les idéaux* $\mathrm{ann}_A(M)$ *et* $(\mathbf{x})$ *de A annulent tous les modules d'homologie du complexe de Koszul* $K_\bullet(\mathbf{x}; M)$.

(ii) *si* $\mathbf{x}$ *est une suite M-régulière*[1]*, alors* $H_p(\mathbf{x}; M) = 0$ *pour tout* $p \geq 1$.

Preuve. Pour voir le premier point il suffit de vérifier que pour tout entier $p \geq 0$, tout entier $j = 1, \ldots, n$ et tout $x \in K_p(\mathbf{x}; M)$

$$d_{p+1}\sigma_p^j(x) + \sigma_{p_1}^j d_p(x) = x_j x,$$

où l'application $\sigma_p^j : K_p(\mathbf{x}; M) \to K_{p+1}(\mathbf{x}; M)$ envoie $e_{i_1} \wedge \cdots \wedge e_{i_p}$ sur $e_j \wedge e_{i_1} \wedge \cdots \wedge e_{i_p}$.

La preuve du deuxième point se fait par récurrence sur l'entier n. Si $n = 1$ alors $H_1(x_1; M) = \mathrm{Ker}(M \xrightarrow{\times x_1} M) = 0$. Supposons donc que (ii) est vraie pour tout entier $1, \ldots, t-1$ et posons $\mathbf{x}' := (x_1, \ldots, x_{n-1})$. On vérifie facilement que l'on a la suite exacte de complexes :

$$0 \to K_\bullet(\mathbf{x}'; M) \hookrightarrow K_\bullet(\mathbf{x}; M) \xrightarrow{\pi} K_\bullet(\mathbf{x}'; M)[-1] \to 0$$

où la notation $K_\bullet[-1]$ désigne le "décalage à gauche" de $K_\bullet$ (i.e. $K_p[-1] := K_{p-1}$ et $d_p[-1] := d_{p-1}$) et l'application A-linéaire π envoie $e_{i_1} \wedge \cdots \wedge e_{i_p}$ sur $e_{i_1} \wedge \cdots \wedge e_{i_{p-1}}$ si $i_p = n$, ou sur 0 sinon. Cette suite exacte permet d'écrire une suite exacte longue d'homologie (le soin est laissé au lecteur de décrire explicitement le morphisme de connection)

$$\cdots \to H_p(\mathbf{x}'; M) \xrightarrow{\times(-1)^p x_n} H_p(\mathbf{x}'; M) \to H_p(\mathbf{x}; M) \to H_{p-1}(\mathbf{x}; M) \to \cdots$$

qui montre immédiatement, à l'aide de l'hypothèse de récurrence, que $H_p(\mathbf{x}; M) = 0$ pour tout $p > 1$. Enfin, nous avons

$$0 = H_1(\mathbf{x}'; M) \to H_1(\mathbf{x}; M) \to H_0(\mathbf{x}'; M) \xrightarrow{\times x_n} H_0(\mathbf{x}'; M) \to \cdots$$

et puisque $\mathbf{x}$ est une suite M-régulière, l'application la plus à droite est injective, d'où l'on conclut que $H_1(\mathbf{x}; M) = 0$. □

Remarque 2.2.2 *Le point (ii) devient une équivalence dans le cas local et dans le cas gradué. Plus précisément, si l'une des deux conditions suivantes est réalisée*

- *A est un anneau gradué, M est un A-module gradué de type fini et les éléments x_i sont homogènes de degré positif*
- *A est un anneau local noethérien $(A, \mathfrak{m})$ et pour tout $i = 1, \ldots, n$ on a $x_i \in \mathfrak{m}$*

alors $\mathbf{x}$ *est une suite M-régulière si et seulement si* $H_p(\mathbf{x}; M) = 0$ *pour tout* $p \geq 1$*, si et seulement si* $H_1(\mathbf{x}; M) = 0$*. Comme corollaire, on obtient sous la même condition que* $\mathbf{x}$ *est une suite régulière indépendamment de l'ordre de ses éléments.*

Notons que si A est un anneau gradué alors le complexe de Koszul $K_\bullet(\mathbf{x}; M)$ hérite de cette graduation. Par exemple, si A est un anneau $\mathbb{Z}$-gradué et que les éléments $x_1, \ldots, x_n$ sont homogènes de degré $d_1, \ldots, d_n$ respectivement, alors le complexe de Koszul est gradué comme suit : $K_0(\mathbf{x}; A) = A(0)$ et pour tout $p \geq 1$,

$$K_p(\mathbf{x}; A) = \bigoplus_{1 \leq i_1 < \cdots < i_p \leq n} A(-d_{i_1} - \cdots - d_{i_p}).$$

La notation $A(\nu)$ désigne le "twist" de A par ν, i.e. $A(\nu)_t = A_{\nu+t}$ pour tout couple $(\nu, t) \in \mathbb{Z}^2$.

[1] ce qui signifie que pour tout $i = 1, \ldots, n$ l'élément x_i n'est pas diviseur de zéro dans $M/(x_1, \ldots, x_{i-1})M$.

Polynômes génériques. Soit k un anneau et $P_1, \ldots, P_s$ les polynômes homogènes génériques de degré $d_1, \ldots, d_s$ respectivement, dans les variables homogènes $X_1, \ldots, X_n$:

$$P_i(X_1, \ldots, X_n) := \sum_{|\alpha|=d_i} U_{i,\alpha} X^\alpha \in C := k[U_{i,\alpha} : i = 1, \ldots, s, |\alpha| = d_i][X_1, \ldots, X_n].$$

Lemme 2.2.3 *Si $s \leq n$ alors $P_1, \ldots, P_s$ est une suite régulière dans l'anneau C.*

Preuve. Pour tout $i = 1, \ldots, s$ on distingue le coefficient $\mathcal{E}_i := U_{i,(0,\ldots,0,d_i,0,\ldots,0)}$ du monôme $X_i^{d_i}$ du polynôme P_i. Tous les coefficients restant $U_{i,\alpha}$ forment une suite régulière et $P_i \equiv \mathcal{E}_i X_i^{d_i}$ dans l'anneau quotient $k[\mathcal{E}_1, \ldots, \mathcal{E}_n][X_1, \ldots, X_n]$. Maintenant, dans ce quotient il est aisé de constater que les polynômes $F_i = X_i - \mathcal{E}_i$, $i = 1, \ldots, s$ forment une suite régulière. A nouveau, l'anneau quotient correspondant est isomorphe à $k[X_1, \ldots, X_n]$ et $P_i \equiv X_i^{d_i+1}$, $i = 1, \ldots, s$. Ces derniers constituent trivialement une suite régulière.

On conclut grâce à la remarque 2.2.2 qui affirme que la propriété d'être une suite régulière pour une suite d'éléments homogènes dans un anneau gradué ne dépend pas de l'ordre de ses éléments. □

Corollaire 2.2.4 *Graduant l'anneau C en posant $\deg(U_{i,\alpha}) = 0$ et $\deg(X_j) = 1$, le complexe de Koszul $K_\bullet(P_1, \ldots, P_s; C)$ fournit, pour tout $s \leq n$, une résolution libre finie du quotient $C/(P_1, \ldots, P_s)$.*

Autrement dit, nous avons la suite exacte

$$0 \to C(-d_1 - \cdots - d_s) \xrightarrow{d_s} \cdots \xrightarrow{d_3} \bigoplus_{1 \leq i < j \leq s} C(-d_i - d_j) \xrightarrow{d_2} \bigoplus_{i=1}^{s} C(-d_i) \xrightarrow{d_1} C \to \frac{C}{(P_1, \ldots, P_s)} \to 0.$$

En particulier, le noyau de d_1 est égal à l'image de d_2 ; par conséquent $(h_1, \ldots, h_s) \in \mathrm{Ker}(d_1)$ si et seulement s'il existe $(\ldots, F_{i,j}, \ldots) \in \bigoplus_{1 \leq i < j \leq s} C(-d_i - d_j)$ tel que $d_2(\ldots, F_{i,j}, \ldots) = (h_1, \ldots, h_s)$, c'est-à-dire si et seulement si

$$M \begin{pmatrix} P_1 \\ \vdots \\ P_s \end{pmatrix} = \begin{pmatrix} h_1 & \cdots & h_s \end{pmatrix}$$

où M est une matrice antisymétrique (i.e. ${}^tM = -M$), à savoir $M := (F_{i,j})_{1 \leq i,j \leq s}$ (cette dernière équivalence découle du fait que $d_2(F_{i,j} e_i \wedge e_j) = F_{i,j} f_j e_i - F_{i,j} f_i e_j$).

2.3 Définition du résultant de Macaulay

On suppose donnés $r \geq 1$ polynômes homogènes en les variables $X_1, \ldots, X_n$ (toutes supposées de poids 1) de degré strictement positifs $d_1, \ldots, d_r$ respectivement,

$$f_i(X_1, \ldots, X_n) = \sum_{|\alpha|=d_i} U_{i,\alpha} X^\alpha, \quad i = 1, \ldots, r.$$

En outre, on pose $A := k[U_{i,\alpha} : i = 1, \ldots, r, |\alpha| = d_i]$ où k désigne un *anneau factoriel*. Ainsi, $f_i \in C := A[X_1, \ldots, X_n]$ pour tout $i = 1, \ldots, r$. On s'intéresse à l'idéal $I := (f_1, \ldots, f_r) \subset C$ et à l'anneau quotient gradué $B := C/I$. On note $\mathfrak{A} = H^0_{\mathfrak{m}}(B)_0$ l'idéal éliminant. Dans ce qui suit, nous démontrerons le

Théorème 2.3.1 *Si $r = n$ alors l'idéal $\mathfrak{A}$ est un idéal premier et principal de A. De plus, il possède un unique générateur, noté* $\mathrm{Res}(f_1, \ldots, f_n)$ *et appelé le* résultant *de $f_1, \ldots, f_n$, tel que*

$$\mathrm{Res}(X_1^{d_1}, \ldots, X_n^{d_n}) = 1 \in k.$$

Nous suivrons de près la "preuve élémentaire" donnée par Jean-Pierre Jouanolou dans le monographe [Jou91a]. Avant de continuer, signalons ici que ce théorème reste vrai sans hypothèse sur l'anneau k (sauf pour l'unicité du générateur qui nécessite que k soit un anneau réduit) ; nous renvoyons le lecteur intéressé à [Jou91a] pour plus de détails.

Hurwitz fût sans doute le premier à introduire le concept de *formes d'inertie* dans le cadre de la théorie de l'élimination. Ce concept s'est révélé être un outil très puissant pour l'étude des idéaux éliminants, notamment dans le cas $r = n$. Rappelons que $\mathfrak{m} := (X_1, \ldots, X_n) \subset C$ et que r et n sont deux entiers *a priori* distincts.

Définition 2.3.2 *L'idéal des formes d'inerties de I par rapport à l'idéal $\mathfrak{m}$ est l'idéal*

$$\mathrm{TF}_{\mathfrak{m}}(I) := \bigcup_{t\geq 0}(I :_C \mathfrak{m}^t) = \{f \in C : \exists \nu \in \mathbb{N}\ \mathfrak{m}^\nu f \subset I\} = \pi^{-1}(H^0_{\mathfrak{m}}(B)) \subset C,$$

où π désigne la projection canonique $C \to B = C/I \to 0$. C'est un idéal homogène de C et $\mathfrak{A} = \mathrm{TF}_{\mathfrak{m}}(I)_0 \subset A$.

Lemme 2.3.3 *Pour tout entier $j \in \{1, \ldots, n\}$ on a*

$$\mathrm{TF}_{\mathfrak{m}}(I) = \bigcup_{t\geq 0}(I :_C X_j^t) = \{f \in C : \exists \nu \in \mathbb{N}\ X_j^\nu f \subset I\} = \mathrm{Ker}(C \to B_{X_j}). \tag{2.3}$$

De plus, $\mathrm{TF}_{\mathfrak{m}}(I)$ est un idéal premier de C (et par conséquent $\mathfrak{A}$ est un idéal premier de A).

Preuve. Soit un entier $j \in \{1, \ldots, n\}$. Pour tout $i = 1, \ldots, r$ on distingue le coefficient

$$\mathcal{E}_i := U_{i,(0,\ldots,0,d_i,0,\ldots,0)}$$

du polynôme f_i qui prend la forme suivante dans $C[X_j^{-1}]$:

$$f_i = X_j^{d_i}(\mathcal{E}_i + \sum_{\alpha\neq(0,\ldots,0,d_i,0,\ldots,0)} U_{i,\alpha}X^\alpha X_j^{-d_i}).$$

On obtient ainsi un isomorphisme de k-algebras

$$\begin{array}{rcl} B_{X_j} & \xrightarrow{\sim} & k[U_{l,\alpha} : U_{l,\alpha} \neq \mathcal{E}_i][X_1, \ldots, X_n][X_j^{-1}] \\ \mathcal{E}_i & \mapsto & \mathcal{E}_i - \dfrac{f_i}{X_j^{d_i}} = -\displaystyle\sum_{\alpha\neq(0,\ldots,0,d_i,0,\ldots,0)} U_{i,\alpha}X^\alpha X_j^{-d_i} \end{array} \tag{2.4}$$

qui montre que X_i n'est pas un diviseur de zéro dans B_{X_j} pour tout couple $(i, j) \in \{1, \ldots, n\}^2$. Par suite, on obtient successivement, pour tout couple $(i, j) \in \{1, \ldots, n\}^2$, les égalités

$$\mathrm{Ker}(C \to B_{X_i}) = \mathrm{Ker}(C \to B_{X_iX_j}) = \mathrm{Ker}(C \to B_{X_jX_i}) = \mathrm{Ker}(C \to B_{X_j})$$

qui prouvent la description annoncée pour $\mathrm{TF}_{\mathfrak{m}}(I)$. De plus, puisque k est intègre, B_{X_j} l'est également pour tout i. Par conséquent $\mathrm{TF}_{\mathfrak{m}}(I)$ est un idéal premier de C. □

Avant d'aller plus loin, et notamment de montrer le résultat clé de Hurwitz, donnons deux exemples connus de formes d'inerties.

Le Jacobien. Le déterminant de la matrice Jacobienne

$$\mathrm{Jac}(f_1, \ldots, f_n) = \begin{pmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_n}{\partial X_1} \\ \vdots & & \vdots \\ \frac{\partial f_1}{\partial X_n} & \cdots & \frac{\partial f_n}{\partial X_n} \end{pmatrix}$$

est une forme d'inertie. En effet, par opérations élémentaires sur les lignes de cette matrice, le formule d'Euler montre que $X_n\mathrm{det}(\mathrm{Jac}(f_1, \ldots, f_n)) \in (f_1, \ldots, f_n)$.

Les matrices de Macaulay. Montrons l'existence de formes d'inerties de degré 0, c'est-à-dire d'éléments non nuls dans $\mathfrak{A}$: les déterminants de Macaulay [Mac02]. Posons $\mathrm{Mon}(t) := \{X^\alpha : |\alpha| = t\}$, l'ensemble des monômes homogènes de degré t. On voit facilement que si $t \geq \sum_{i=1}^n (d_i - 1) + 1$ alors tout monôme $X^\alpha \in \mathrm{Mon}(t)$ est divisible par au moins l'une des puissances pures $X_1^{d_1}, X_2^{d_2}, \ldots, X_n^{d_n}$. On peut donc définir l'indice $i(\alpha) := \min\{i : \alpha_i \geq d_i\}$.

Choisissant un ordre pour $\mathrm{Mon}(n,t)$, on construit la matrice

$$\mathbb{M}(f_1, \ldots, f_n; t) = [m_{\alpha,\beta}] : \mathrm{Mon}(n,t) \times \mathrm{Mon}(n,t) \to A$$

telle que pour tout $X^\beta \in \mathrm{Mon}(t)$

$$\frac{X^\beta}{X_{i(\beta)}^{d_{i(\beta)}}} f_{i(\beta)} = \sum_{|\alpha|=t} m_{\alpha,\beta} X^\alpha$$

(remarquer que si $n = 2$ la matrice $\mathbb{M}(f_1, f_2; d_1 + d_2 - 1)$ est la matrice de Sylvester, à l'ordre près des lignes et des colonnes) On voit facilement, en faisant des opérations sur les lignes de la matrice de Macaulay que, par exemple, $X_1^t \det(\mathbb{M}(f_1, \ldots, f_n; t)) \in (f_1, \ldots, f_n)$ et donc que $\det(\mathbb{M}(f_1, \ldots, f_n; t))$ est une forme d'inertie (de degré 0). Maintenant, il est clair par spécialisation que la matrice de Macaulay de $X_1^{d_1}, \ldots, X_n^{d_n}$ est l'identité et donc que $\det(\mathbb{M}(f_1, \ldots, f_n; t))$ est une forme d'inertie non nulle.

Par propriété du déterminant, on observe que $\det(\mathbb{M}(f_1, \ldots, f_n; t))$ est homogène en les coefficients de chacun des polynômes $f_1, \ldots, f_n$. De plus, on a

$$\deg_{f_n}(\det(\mathbb{M}(f_1, \ldots, f_n; t))) = d_1 \ldots d_{n-1}$$

où $\deg_{f_n}(-)$ désigne le degré par rapport aux coefficients de f_n. En effet, il est clair que

$$\deg_{f_i}(\det(\mathbb{M}(f_1, \ldots, f_n; t))) = \sharp\{\alpha \text{ tel que } |\alpha| = t \text{ et } i(\alpha) = i\}$$

et de plus, $i(\alpha) = n$ si et seulement si $0 \leq \alpha \leq d_i - 1$ pour $i = 0, \ldots, n-1$. Enfin, par permutation des polynômes $f_1, \ldots, f_n$, on déduit que pour tout $i = 1, \ldots, n$ il existe une forme d'inertie non nulle dans $\mathfrak{A}$ dont le degré par rapport aux coefficients du polynôme f_i est $\leq d_1 \ldots d_n / d_i$.

Proposition 2.3.4 (Hurwitz) *Si $r < n$ alors $\mathrm{TF}_{\mathfrak{m}}(I) = I$.*

Preuve. Il suffit de montrer $\mathrm{TF}_{\mathfrak{m}}(I) \subset I$ puisque l'autre inclusion est évidente. Par le lemme 2.3.3 précédent, il nous faut montrer que pour tout $f \in C$ tel qu'il existe $s \in \mathbb{N}$ tel que $X_n^s f \in I$ alors $f \in I$. C'est clair si $s = 0$ et un raisonnement inductif élémentaire montre qu'il suffit d'établir la propriété annoncée dans le cas $s = 1$ pour qu'elle soit vraie pour tout $s \in \mathbb{N}$ (utiliser $X_n^k f = X_n(X_n^{k-1} f)$).

Soit donc $f \in C$ tel que $X_n f = h_1 f_1 + \cdots + h_r f_r \in I \subset C$. En spécialisant X_n à 0 on déduit que $\overline{h}_1 \overline{f}_1 + \cdots + \overline{h}_r \overline{f}_r = 0$, où les polynômes $\overline{f}_i$ sont des polynômes homogènes génériques en $n-1$ variables. Par conséquent, on déduit du lemme 2.2.3 qu'ils forment une suite régulière dans $A[X_1, \ldots, X_{n-1}]$, et par le corollaire 2.2.4, que le complexe de Koszul $K_\bullet(\overline{f}_1, \ldots, \overline{f}_r; A[X_1, \ldots, X_{n-1}])$ est acyclique. D'après la remarque suivant le corollaire 2.2.4 il existe une matrice antisymétrique M (i.e. ${}^tM = -M$), telle que

$$\begin{pmatrix} \overline{h}_1 & \overline{h}_2 & \cdots & \overline{h}_r \end{pmatrix} = M \begin{pmatrix} \overline{f}_1 \\ \vdots \\ \overline{f}_r \end{pmatrix}.$$

On définit ainsi les polynômes $g_1, \ldots, g_r \in A[X_1, \ldots, X_n]$ de telle sorte que

$$\begin{pmatrix} g_1 & g_2 & \cdots & g_r \end{pmatrix} = M \begin{pmatrix} f_1 \\ \vdots \\ f_r \end{pmatrix}.$$

Puisque M est antisymétrique, on voit facilement que $\sum_{i=1}^n g_i f_i = 0$. De plus, pour tout $i = 1, \ldots, r$ on a $\overline{g}_i = \overline{h}_i$ et donc l'existence d'un polynôme l_i tel que $h_i - g_i = X_n l_i$. Il s'en suit que

$$X_n f = (g_1 + X_n l_1) f_1 + \cdots + (g_r + X_n l_r) f_r = \sum_{i=1}^n g_i f_i + X_n \sum_{i=1}^n l_i f_i$$

ce qui montre que $f = \sum_{i=1}^n l_i f_i \in A[X_1, \ldots, X_n]$ (car X_n n'est pas un diviseur de zéro), i.e. $f \in I$. □

Corollaire 2.3.5 *Supposons $r = n$ et soit $f \in \mathrm{TF}_{\mathfrak{m}}(I) \subset A[X_1, \ldots, X_n]$. Alors, ou bien $f \in I = (f_1, \ldots, f_n)$ ou bien f dépend de tous les coefficients de chacun des polynômes $f_1, \ldots, f_n$.*

Preuve. Soit $U := U_{i,\alpha}$ un coefficient d'un polynôme f_i pour un $i \in \{1, \ldots, n\}$; on pose $g_i = f_i - UX^\alpha$. Supposons qu'il existe $f \in \mathrm{TF}_{\mathfrak{m}}(I)$ qui ne dépend pas de U ; nous allons montrer qu'alors $f \in I$.

Puisque $f \in \mathrm{TF}_{\mathfrak{m}}(I)$, nous savons que $X_n^l f = \sum_{i=1}^n h_i f_i \in A[X_1, \ldots, X_n]$ pour un $l \in \mathbb{N}$. Considérons le morphisme de k-algèbres

$$\begin{array}{rcl} A[X_1, \ldots, X_n] & \xrightarrow{\varphi} & A[X_1, \ldots, X_n]_{X_1 X_2 \ldots X_n} \\ U & \mapsto & -g_i/X^\alpha \\ U_{j,\beta} & \mapsto & U_{j,\beta} \text{ if } (j,\beta) \neq (i,\alpha) \\ X_j & \mapsto & X_j. \end{array}$$

Puisque $\varphi(f_i) = 0$, on a

$$\varphi(X_n^l f) = H_1 f_1 + \cdots + H_{i-1} f_{i-1} + H_{i+1} f_{i+1} + \cdots + H_n f_n \in A[X_1, \ldots, X_n]_{X_1 \ldots X_n}.$$

Mais $X_1 \ldots X_n$ n'est pas diviseur de zéro dans $A[X_1, \ldots, X_n]_{X_1 \ldots X_n}$ et $\varphi(X_n^l f) = X_n^l f$, donc il existe un monôme X^β tel que

$$X^\beta \varphi(X_n^l f) = X^\beta X_n^l f = G_1 f_1 + \cdots + G_{i-1} f_{i-1} + G_{i+1} f_{i+1} + \cdots + G_n f_n \in A[X_1, \ldots, X_n],$$

c'est-à-dire $f \in \mathrm{TF}_{\mathfrak{m}}(f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_n)$ (modulo une extension appropriée de l'anneau des coefficients). On conclut que $f \in I$ d'après la proposition 2.3.4. □

Preuve de théorème 2.3.1. Tout d'abord remarquons $\mathfrak{A} \neq 0$ puisque

$$\mathrm{Proj}(k[X_1, \ldots, X_n]/(X_1^{d_1}, \ldots, X_n^{d_n})) = \emptyset$$

(on peut aussi remarquer l'existence des matrices de Macaulay ici). A présent, choisissons un coefficient $U := U_{i,\alpha}$ et définissons l'anneau de polynômes A' tel que $A = A'[U]$ (A' est aussi un anneau factoriel). Puisque $I \cap A = 0$, le corollaire 2.3.5 entraîne que tout $0 \neq f \in \mathfrak{A}$ possède un degré strictement positif comme polynôme en U, i.e. $\deg_U(f) \geq 1$. Soit $s \geq 1$ le minimum de ces degrés parmi tous les $0 \neq f \in \mathfrak{A}$.

On montre qu'il existe un élément *premier* $R \in \mathfrak{A}$ tel que $\deg_U(R) = s$. En effet, soit $0 \neq f \in \mathfrak{A}$ tel que $\deg_U(f) = s$. Puisque A' est un anneau factoriel, il existe une décomposition $f = q_1 \ldots q_t$ où chaque q_j est un élément premier dans $A'[U]$. Mais comme $\mathfrak{A}$ est un idéal premier le lemme 2.3.3, on déduit qu'il existe un entier $j \in \{1, \ldots, t\}$ tel que $q_j \in \mathfrak{A}$. De plus, nous avons $1 \leq \deg_U(q_j) \leq \deg_U(f) = s$ et par définition de l'entier s on obtient que $\deg_U(q_j) = s$, ce qui entraîne la propriété annoncée de l'élément $R := q_j$.

Montrons à présent que l'élément R engendre $\mathfrak{A}$. Du fait que A' n'a pas de diviseur de zéro on déduit que pour tout $g \in \mathfrak{A}$

$$\lambda g = uR + v \text{ with } \lambda \in A' \text{ and } \left\{ \begin{array}{l} v = 0 \\ \text{or} \\ \deg_U(v) < s. \end{array} \right.$$

Il s'en suit que $v = \lambda g - uR \in \mathfrak{A}$. Si $v \neq 0$ alors $\deg_U(v) \geq 1$ par la proposition 2.3.5, et donc $\deg_U(v) \geq s$ par définition de l'entier s ; une contradiction. Par conséquent $\lambda g = uR$. De plus, $\lambda \in A'$ et $U \notin A'$, donc forcément R divise g.

Finalement, R est unique à multiplication près par un élément inversible de A', donc de k. Cet élément est forcé d'être l'élément $1 \in k$ par la normalisation donnée dans l'énoncé de ce théorème. □

Pour définir le résultant de n polynômes homogènes en les variables $X_1, \ldots, X_n$ on procède comme suit. Soit $\mathbb{S}$ un anneau commutatif. Pour tout entier $i \in \{1, \ldots, n\}$, supposons donné un polynôme homogène de degré d_i dans les variables $X_1, \ldots, X_n$

$$g_i = \sum_{|\alpha| = d_i} u_{i,\alpha} X^\alpha \in \mathbb{S}[X_1, \ldots, X_n]_{d_i}$$

et considérons le morphisme $\theta : A \to \mathbb{S} : U_{j,\alpha} \mapsto u_{j,\alpha}$ correspondant à la *spécialisation* de chaque polynôme f_i en le polynôme g_i. Alors, pour toute forme d'inertie $a \in \mathrm{TF}_{\mathfrak{m}}(f_1, \ldots, f_n)$ on pose $a(g_1, \ldots, g_n) := \theta(a)$. En particulier, le résultant de $g_1, \ldots, g_n$ est par définition

$$\mathrm{Res}(g_1, \ldots, g_n) := \theta(\mathrm{Res}(f_1, \ldots, f_n)).$$

Ainsi, si $\mathbb{S} = A$ et θ est le morphisme identité (i.e. $g_i = f_i$ pour tout i), alors on obtient $a = a(f_1, \ldots, f_n)$, ce qui clarifie la notation $\mathrm{Res}(f_1, \ldots, f_n)$ pour la forme d'inertie $\mathrm{Res} \in A$.

2.4 Quelques propriétés formelles

Le résultant que nous venons de construire possède de très nombreuses propriétés formelles qui permettent de le calculer, sinon de bien l'appréhender. Nous en rappelons ici quelques unes et renvoyons le lecteur au monographe [Jou91b, §5] pour plus de détails, notamment les preuves. Au passage, on montre comment l'utilisation des formes d'inerties permet de simplifier l'établissement de ces propriétés.

Formes linéaires. Si $d_1 = d_2 = \cdots = d_n = 1$ et $f_i = \sum_{j=1}^n U_{i,j} X_j$, $i = 1, \ldots, n$, alors

$$\mathrm{Res}(f_1, \ldots, f_n) = \det (U_{i,j})_{\substack{1 \le i \le n \\ 1 \le j \le n}}$$

En effet, dans la situation générique, on vérifie aisément que ce déterminant est une forme d'inertie et donc que c'est un multiple du résultant. Puisque le degré du résultant par rapport à chaque f_i est exactement 1 (au moins 1 par les matrices de Macaulay et au plus 1 par la proposition 2.3.5), on en déduit que ce déterminant et le résultant ne diffèrent que par une constante multiplicative entière. Finalement cette constante vaut 1 par spécialisation $f_i \mapsto X_i$ pour tout $i = 1, \ldots, n$.

Divisibilité. Si $g_1, \ldots, g_n$ sont des polynômes homogènes dans $\mathbb{S}[X]$ tels que pour tout $i = 1, \ldots, n$ on ait $f_i \in (g_1, \ldots, g_n)^{\mu_i}$, alors $\mathrm{Res}(g_1, \ldots, g_n)$ divise $\mathrm{Res}(f_1, \ldots, f_n)$ dans $\mathbb{S}$.

En effet, par hypothèse on a $g_i = \sum_{j=1}^n h_{i,j} f_j$ pour tout $i = 1, \ldots, n$. Par spécialisation, on se ramène donc à la situation générique (c'est-à-dire on suppose que les coefficients des f_j et $h_{i,j}$ sont des indéterminées). On a alors, par définition puis par hypothèse,

$$X_n^N \mathrm{Res}(g_1, \ldots, g_n) \in (g_1, \ldots, g_n) \subset (f_1, \ldots, f_n)$$

où $N \in \mathbb{N}$, ce qui montre que $\mathrm{Res}(g_1, \ldots, g_n)$ est une forme d'inertie de $(f_1, \ldots, f_n)$, donc un multiple de $\mathrm{Res}(f_1, \ldots, f_n)$.

En fait, on peut montrer une version plus fine de ce résultat, à savoir : si $g_1, \ldots, g_n$ sont des polynômes homogènes dans $\mathbb{S}[X]$ tels que pour tout $i = 1, \ldots, n$ il existe un entier μ_i satisfaisant $f_i \in (g_1, \ldots, g_n)^{\mu_i}$, alors $\mathrm{Res}(g_1, \ldots, g_n)^{\mu_1 \cdots \mu_n}$ divise $\mathrm{Res}(f_1, \ldots, f_n)$ dans $\mathbb{S}$.

Multi-homogénéité. Pour tout $i = 1, \ldots, n$, $\mathrm{Res}(f_1, \ldots, f_n)$ est homogène par rapport aux coefficients du polynôme f_i de degré $d_1 \ldots d_n / d_i$.

En effet, es déterminants de Macaulay montrent déjà que $\deg_{f_i}(Res) \le d_1 \ldots d_n / d_i$ pour tout $i = 1, \ldots, n$. Pour montrer l'inégalité dans l'autre sens, on spécialise chaque polynôme f_i en un produit de formes linéaires génériques $g_i := \prod_{j=1}^{d_i} l_{i,j}(X_1, \ldots, X_n)$. Alors, par divisibilité $\mathrm{Res}(g_1, \ldots, g_n)$ est divisible par

$$\prod_{\substack{j_k = 1, \ldots, d_k \\ k = 1, \ldots, n}} \mathrm{Res}(l_{1,j_1}, \ldots, l_{n,j_n})$$

Mais alors, $\deg_{f_i}(\mathrm{Res}(l_{1,j_1}, \ldots, l_{n,j_n})) = 1$ (car c'est un résultant de formes linéaires génériques) et donc

$$\deg_{f_i}(\mathrm{Res}(g_1, \ldots, g_n)) \ge \frac{d_1 \ldots d_n}{d_i}$$

d'où le résultat.

Multiplicativité. Supposons que, pour un $i \in \{1, \ldots, n\}$ il existe deux polynômes homogènes f_i' et f_i" tels que $f_i = f_i' f_i$" dans $\mathbb{S}[X_1, \ldots, X_n]$. Alors

$$\mathrm{Res}(f_1, \ldots, f_i' f_i'', \ldots, f_n) = \mathrm{Res}(f_1, \ldots, f_i', \ldots, f_n)\mathrm{Res}(f_1, \ldots, f_i'', \ldots, f_n)$$

dans $\mathbb{S}$.

Par spécialisation, on se place dans la situation générique, i.e. les coefficients des polynômes

$$f_1, \ldots, f_{i-1}, f_i', f_i", f_{i+1}, \ldots, f_n$$

sont des indéterminées. On utilise la divisibilité et la primalité du résultant pour montrer que le produit des deux résultants ci-dessus divise $\mathrm{Res}(f_1, \ldots, f_i' f_i'', \ldots, f_n)$. Ensuite, on conclut à l'égalité grâce à des considérations de degré (d'où une égalité à multiplicatio près par un entier) puis par spécialisation aux puissance pures $f_j \mapsto X_j^{d_j}$.

Permutation des variables. Pour toute permutation σ de l'ensemble $\{1, \ldots, n\}$ on a

$$\mathrm{Res}(f_{\sigma(1)}, \ldots, f_{\sigma(n)}) = (\mathcal{E}(\sigma))^{d_1 \cdots d_n}\mathrm{Res}(f_1, \ldots, f_n)$$

où $\mathcal{E}(\sigma)$ désigne la signature de la permutation σ.

En effet, par homogénéité dans le cadre générique, on obtient l'égalité au signe près. La détermination de ce signe se fait par spécialisation $f_i \mapsto X_i^{d_i}$ puis utilisation de la multiplicativité et enfin du fait que $\mathrm{Res}(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = \mathcal{E}(\sigma)$ (résultant de formes linéaires).

Transformations élémentaires.

$$\mathrm{Res}(f_1, \ldots, f_i + \sum_{i \neq j} h_j f_j, \ldots, f_n) = \mathrm{Res}(f_1, \ldots, f_n)$$

En effet, en se plaçant dans le cadre générique, il est clair que l'un divise l'autre comme forme d'inertie, puis que les deux sont égaux à multiplication près par une constante dans $\mathbb{Z}$ par des considérations de degré. La spécialisation $h_j \mapsto 0$ pour tout j permet de conclure.

Homogénéité tordue. $\mathrm{Res}(f_1, \ldots, f_n)$ est isobare de degré $d_1 \ldots d_n$ si chaque coefficient des polynômes $f_1, \ldots, f_n$ est de poids la puissance de la variable X_n de son monôme correspondant.

Changement de base. Si $g_1, \ldots, g_n$ sont des polynômes homogènes dans $\mathbb{S}[X_1, \ldots, X_n]$ de même degré d, alors

$$\mathrm{Res}(f_1(g_1, \ldots, g_n), \ldots, f_n(g_1, \ldots, g_n)) = \mathrm{Res}(g_1, \ldots, g_n)^{d_1 \cdots d_n}\mathrm{Res}(f_1, \ldots, f_n)^{d^{n-1}}$$

2.5 Retour sur l'implicitation d'une surface rationnelle

Revenons un instant sur le calcul que nous avons fait en 1.5 afin de comprendre d'où vient ce facteur parasite. Pour cela, on établit un lien entre un résultant univarié de deux résultants univariés et un résultant multivarié (voir [BM07] pour ce résultat et d'autres du même genre).

Supposons donnés quatre entiers strictement positifs d_1, d_2, d_3, d_4 et quatre polynômes homogènes génériques

$$P_k(X_1, X_2, X_3) = \sum_{0 \leq i,j; i+j \leq d_k} U_{i,j}^{(k)} X_1^i X_2^j X_3^{d_k - i - j} \in \mathbb{U}[X_1, X_2, X_3], k = 1, \ldots, 4,$$

où $\mathbb{U}$ désigne l'anneau universel des coefficients

$$\mathbb{U} := \mathbb{Z}[U_{i,j}^{(k)}; 0 \leq i, j; i + j \leq d_k, k = 1, \ldots, 4].$$

On note X_4 une nouvelle indéterminée.

Proposition 2.5.1 *Posant*

$$\begin{aligned} R_{12} &:= \mathrm{Res}_{X_3}(P_1(1,X_2,X_3),P_2(1,X_2,X_3)) \in \mathbb{U}[X_2], \\ R_{34} &:= \mathrm{Res}_{X_3}(P_3(1,X_2,X_3),P_4(1,X_2,X_3)) \in \mathbb{U}[X_2], \end{aligned}$$

il vient l'égalité dans $\mathbb{U}$ *:*

$$\mathrm{Res}_{X_2}(R_{12},R_{34}) = \mathrm{Res}_{X_1:\cdots:X_4}(P_1(X_1,X_2,X_3),P_2(X_1,X_2,X_3),P_3(X_1,X_2,X_4),P_4(X_1,X_2,X_4)).$$

De plus, cette quantité est non nulle, irréductible et multi-homogène par rapport aux ensembles de coefficients $(U^{(1)}_{i,j})_{i,j}$, $(U^{(2)}_{i,j})_{i,j}$, $(U^{(3)}_{i,j})_{i,j}$, $(U^{(4)}_{i,j})_{i,j}$ *de multi-degré* $(d_2d_3d_4, d_1d_3d_4, d_1d_2d_4, d_1d_2d_3)$.

Preuve. First of all, we observe that the iterated resultant $\mathrm{Res}_{X_2}(R_{12},R_{34})$ and the resultant

$$\mathcal{R} := \mathrm{Res}(P_1(X_1,X_2,X_3),P_2(X_1,X_2,X_3),P_3(X_1,X_2,X_4),P_4(X_1,X_2,X_4))$$

are both non-zero polynomials, for they both specialize to the quantity $(-1)^{d_1d_2d_3d_4}$ if the polynomials $P_i(X_1,X_2,X_3), i=1,\ldots,4$, are specialized to $X_1^{d_1}$, $X_3^{d_2}$, $X_2^{d_3}$ and $X_3^{d_4}$ respectively. Note also that the statement about the multi-degree of $\mathcal{R}$ follows from the homogeneity property of resultants.

To prove the irreducibility of $\mathcal{R}$, we proceed by induction on the positive integer $d := d_1+d_2+d_3+d_4 \geq 4$. For $d=4$, $\mathcal{R}$ equals the determinant

$$\begin{vmatrix} U^{(1)}_{1,0} & U^{(2)}_{1,0} & U^{(3)}_{1,0} & U^{(4)}_{1,0} \\ U^{(1)}_{0,1} & U^{(2)}_{0,1} & 0 & 0 \\ U^{(1)}_{0,0} & U^{(2)}_{0,0} & U^{(3)}_{0,0} & U^{(4)}_{0,0} \\ 0 & 0 & U^{(3)}_{0,1} & U^{(4)}_{0,1} \end{vmatrix} \in \mathbb{U}$$

which is checked to be irreducible. Thus, we assume that $\mathcal{R}$ is irreducible up to a given integer $p \geq 4$ and we will prove that $\mathcal{R}$ is irreducible if $d = p+1$. To do this, first observe that one of the integers d_1,d_2,d_3,d_4 must be greater or equal to 2. We can assume that $d_1 \geq 2$ without loss of generality. Consider the specialization ϕ leaving invariant the polynomials P_2, P_3 and P_4 and sending the polynomial P_1 to the product L_1Q_1 where L_1 and Q_1 are both generic forms of respective degree 1 and $d_1-1 \geq 1$. Then, by multiplicativity of resultants we have the equality

$$\phi(\mathcal{R}) = \mathrm{Res}(L_1,P_2,P_3,P_4)\mathrm{Res}(Q_1,P_2,P_3,P_4),$$

whose right hand side is a product of two irreducible polynomials by our induction hypothesis. As the specialization ϕ is homogeneous (in terms of the coefficients of the P_i's, L_1 and Q_1), the number of irreducible factors of $\mathcal{R}$ can not decrease under the specialization ϕ and we deduce that $\mathcal{R}$ is the product of two irreducible polynomials $\mathcal{R}_1$ and $\mathcal{R}_2$. But then, one of these two factors must depend on the coefficients of P_1, say $\mathcal{R}_1$, and therefore $\phi(\mathcal{R}_1)$ must depend on the coefficients of L_1 and Q_1. This implies that $\mathcal{R}_2$ is an invertible element in $\mathbb{Z}$ and consequently that $\mathcal{R}$ is irreducible.

It remains to prove the claimed equality. To do this, we rewrite $P_k(1,X_2,X_3)$, for all $k=1,\ldots,4$, as

$$P_k(1,X_2,X_3) = \sum_{i=0}^{d_k} \left(\sum_{j=0}^{d_k-i} U^{(k)}_{i,j} X_2^j \right) X_3^i \in \mathbb{U}[X_2,X_3],$$

and we then easily see from well-known properties of the Sylvester resultant that

- R_{12} is bi-homogeneous in the set of coefficients $(U^{(1)}_{i,j})$ and $(U^{(2)}_{i,j})$ of bi-degree (d_2,d_1),
- R_{12} is a polynomial in $\mathbb{U}[X_2]$ of degree d_1d_2,
- $R_{12} \in (P_1(1,X_2,X_3),P_2(1,X_2,X_3)) \subset \mathbb{U}[X_2,X_3]$.

Of course, completely analogous results hold for R_{34}, in particular

$$R_{34} \in (P_3(1,X_2,X_4),P_4(1,X_2,X_4)) \subset \mathbb{U}[X_2,X_4].$$

Again, $\mathrm{Res}_{X_2}(R_{12}, R_{34}) \in (R_{12}, R_{34}) \subset \mathbb{U}[X_2]$ and we deduce that

$$\mathrm{Res}_{X_2}(R_{12}, R_{34}) \in \\ (P_1(1, X_2, X_3), P_2(1, X_2, X_3), P_3(1, X_2, X_4), P_4(1, X_2, X_4)) \subset \mathbb{U}[X_2, X_3, X_4].$$

After homogenization with the variable X_1, it follows that there exists an integer N such that

$$X_1^N \mathrm{Res}_{X_2}(R_{12}, R_{34}) \in \\ (P_1(X_1, X_2, X_3), P_2(X_1, X_2, X_3), P_3(X_1, X_2, X_4), P_4(X_1, X_2, X_4))$$

in $\mathbb{U}[X_1, X_2, X_3, X_4]$ (notice that this does not imply directly that $\mathrm{Res}_{X_2}(R_{12}, R_{34})$ is an inertia form because $P_1(X_1, X_2, X_3)$, $P_2(X_1, X_2, X_3)$, $P_3(X_1, X_2, X_4)$ and $P_4(X_1, X_2, X_4)$ are not generic polynomials). It implies by the divisibility property of resultants, that $\mathcal{R} = \mathrm{Res}(P_1(X_3), P_2(X_3), P_3(X_4), P_4(X_4))$ divides the quantity

$$\mathrm{Res}(X_1^N \mathrm{Res}_{X_2}(R_{12}, R_{34}), P_1(X_1, X_2, X_3), P_2(X_1, X_2, X_3), P_3(X_1, X_2, X_4)) = \\ \mathrm{Res}_{X_2}(R_{12}, R_{34})^{d_1 d_2 d_3} \mathrm{Res}(X_1, P_1(X_3), P_2(X_3), P_3(X_4))^N.$$

Since $\mathcal{R}$ is irreducible and since the second term in the right hand side of the above product does not depend on the coefficients of P_4, we deduce that $\mathcal{R}$ divides $\mathrm{Res}_{X_2}(R_{12}, R_{34})$. Now, from the degree properties of R_{12} and R_{13} we deduce that $\mathrm{Res}_{X_2}(R_{12}, R_{34})$ is, similarly to $\mathcal{R}$, multi-homogeneous with respect to the set of coefficients $(U_{i,j}^{(1)})_{i,j}, (U_{i,j}^{(2)})_{i,j}, (U_{i,j}^{(3)})_{i,j}$, $(U_{i,j}^{(4)})_{i,j}$ of multi-degree

$$(d_2 d_3 d_4, d_1 d_3 d_4, d_1 d_2 d_4, d_1 d_2 d_3).$$

This shows that $\mathrm{Res}_{X_2}(R_{12}, R_{34})$ and $\mathcal{R}$ are equal up to multiplication by an invertible element in $\mathbb{Z}$. To determine this invertible element, we take again the specialization sending P_1 to $X_1^{d_1}$, P_2 to $X_3^{d_2}$, P_3 to $X_2^{d_3}$, P_4 to $X_3^{d_4}$, and check that $\mathcal{R}$ specializes to $(-1)^{d_1 d_2 d_3 d_4}$, as well as $\mathrm{Res}_{X_2}(R_{12}, R_{34})$. □

En spécialisant la formule que nous venons de montrer, on obtient la factorisation suivante d'un résultant itéré particulier.

Corollaire 2.5.2 *Supposons que $d_1 \geq 2$ et posons*

$$\begin{aligned} R_{12} &:= \mathrm{Res}_{X_3}(P_1(1, X_2, X_3), P_2(1, X_2, X_3)) \in \mathbb{U}[X_2], \\ R_{13} &:= \mathrm{Res}_{X_3}(P_1(1, X_2, X_3), P_3(1, X_2, X_3)) \in \mathbb{U}[X_2]. \end{aligned}$$

Alors, notant $\delta_{3,4} P_1(X_3, X_4) = \frac{P_1(X_4) - P_1(X_3)}{X_4 - X_3}$, nous avons l'égalité

$$\mathrm{Res}_{X_2}(R_{13}, R_{12}) = \mathrm{Res}_{X_1 : X_2 : X_3}(P_1, P_2, P_3) \times \\ \mathrm{Res}_{X_1 : \cdots : X_4}(P_1(X_3), P_2(X_4), P_3(X_3), \delta_{3,4} P_1(X_3, X_4))$$

où le membre de droite est le produit de deux polynômes irréductibles dans $\mathbb{U}$.

De plus, le résultant itéré $\mathrm{Res}_{X_2}(R_{13}, R_{12})$ est multi-homogène par rapport aux ensembles de coefficients $(U_{i,j}^{(1)})_{i,j}, (U_{i,j}^{(2)})_{i,j}, (U_{i,j}^{(3)})_{i,j}$ de degré $2d_1 d_2 d_3$, $d_1^2 d_3$ et $d_1^2 d_2$ respectivement.

Preuve. The claimed equality is easily obtained using formal properties of resultants by specialization of the formula proved in Theorem 2.5.1 :

$$\begin{aligned} &\mathrm{Res}(P_1(X_3), P_3(X_3), P_1(X_4), P_2(X_4)) \\ &= \mathrm{Res}(P_1(X_3), P_2(X_4), P_3(X_3), P_1(X_4)) \\ &= \mathrm{Res}(P_1(X_3), P_2(X_4), P_3(X_3), P_1(X_4) - P_1(X_3)) \\ &= \mathrm{Res}(P_1(X_3), P_2(X_4), P_3(X_3), (X_4 - X_3)\delta_{3,4}(P_1)) \\ &= \mathrm{Res}(P_1, P_2, P_3)\mathrm{Res}(P_1(X_3), P_2(X_4), P_3(X_3), \delta_{3,4}(P_1)). \end{aligned}$$

The multi-degree computation and the irreducibility of $\mathrm{Res}(P_1, P_2, P_3)$ are known properties of resultants. The only point which requires a proof is the irreducibility of the factor (which is easily seen to be non-zero by a straightforward specialization)

$$\mathcal{D} := \mathrm{Res}(P_1(X_3), P_2(X_4), P_3(X_3), \delta_{3,4}(P_1)(X_3, X_4)).$$

To do this, we proceed similarly to what we did in Theorem 2.5.1, that is, by induction on the integer $d := d_1 + d_2 + d_3 \geq 4$. We can check by hand (or with a computer) that $\mathcal{D}$ is an irreducible polynomial in $\mathbb{U}$ if $(d_1, d_2, d_3) = (2, 1, 1)$. We thus assume that $\mathcal{D}$ is irreducible up to a given integer $p \geq 4$ and we will prove that $\mathcal{D}$ is irreducible if $d = p + 1$. If $d_2 \geq 2$ (resp. $d_3 \geq 2$) then we can specialize P_2 (resp. P_3) as a product of a generic linear form and a generic form of degree $d_2 - 1 \geq 1$ (resp. $d_3 - 1 \geq 1$) and conclude, exactly as we did in Theorem 2.5.1, that $\mathcal{D}$ is then irreducible. Otherwise, then $d_1 \geq 3$ and we specialize P_1 to the product of a generic linear form

$$L_1(X_1, X_2, X_3) := a\, X_1 + b\, X_2 + c\, X_3$$

and a generic form Q_1 of degree $d_1 - 1 \geq 2$. We call ϕ the map corresponding to this specialization. We have

$$\delta_{3,4}(L_1 Q_1)(X_3, X_4) = c\, Q_1(X_3) + L_1(X_4)\, \delta_{3,4}(Q_1)(X_3, X_4)$$

and we deduce after some manipulations on resultants that

$$\begin{aligned}
\phi(\mathcal{D}) &= \mathrm{Res}(L_1(X_3)Q_1(X_3), P_2(X_4), P_3(X_3), cQ_1(X_3) + L_1(X_4)\delta_{3,4}(Q_1)) \\
&= \mathrm{Res}(Q_1(X_3), P_2(X_4), P_3(X_3), L_1(X_4)\delta_{3,4}(Q_1)(X_3, X_4)) \times \\
&\quad \mathrm{Res}(L_1(X_3), P_2(X_4), P_3(X_3), cQ_1(X_3) + L_1(X_4)\delta_{3,4}(Q_1)(X_3, X_4)) \\
&= \mathrm{Res}(Q_1(X_3), P_2(X_4), P_3(X_3), \delta_{3,4}(Q_1)(X_3, X_4)) \times \\
&\quad \mathrm{Res}(Q_1(X_3), P_2(X_4), P_3(X_3), L_1(X_4)) \times \\
&\quad \mathrm{Res}(L_1(X_3), P_2(X_4), P_3(X_3), (L_1(X_4) - L_1(X_3))\delta_{3,4}(Q_1) + cQ_1(X_3)) \\
&= \mathrm{Res}(Q_1(X_3), P_2(X_4), P_3(X_3), \delta_{3,4}(Q_1)(X_3, X_4)) \times \\
&\quad \mathrm{Res}(Q_1(X_3), P_2(X_4), P_3(X_3), L_1(X_4)) \times \\
&\quad \mathrm{Res}(L_1(X_3), P_2(X_4), P_3(X_3), cQ_1(X_4)) \\
&= c^{d_2 d_3}\mathrm{Res}(Q_1(X_3), P_2(X_4), P_3(X_3), \delta_{3,4}(Q_1)(X_3, X_4)) \times \\
&\quad \mathrm{Res}(Q_1(X_3), P_2(X_4), P_3(X_3), L_1(X_4)) \times \\
&\quad \mathrm{Res}(L_1(X_3), P_2(X_4), P_3(X_3), Q_1(X_4)).
\end{aligned}$$

Either by our induction hypothesis or by Theorem 2.5.1, it turns out that the three resultants involved in the right hand side of the above computation are irreducible in $\mathbb{U}$. So if $\mathcal{D}$ were reducible, say $\mathcal{D} = \mathcal{D}_1\mathcal{D}_2$, then each factor should be homogeneous in the coefficients $(U^{(1)}_{i,j})_{i,j}$ and hence $\phi(\mathcal{D}_1)$ and $\phi(\mathcal{D}_2)$ should be homogeneous in the coefficients of Q_1 and L_1 of the same degree. But

$$\begin{aligned}
\deg_{L_1,Q_1}(c) &= (1, 0), \\
\deg_{L_1,Q_1}(\mathrm{Res}(L_1(X_3), P_2(X_4), P_3(X_3), Q_1(X_4))) &= ((d_1 - 1)d_2d_3, d_2d_3), \\
\deg_{L_1,Q_1}(\mathrm{Res}(Q_1(X_3), P_2(X_4), P_3(X_3), L_1(X_4))) &= ((d_1 - 1)d_2d_3, d_2d_3), \\
\deg_{L_1,Q_1}(\mathrm{Res}(Q_1(X_3), P_2(X_4), P_3(X_3), \delta_{3,4}(Q_1)(X_3, X_4))) &= (0, 2d_1d_2d_3 - 3d_2d_3),
\end{aligned}$$

which implies that either $\mathcal{D}_1$ or $\mathcal{D}_2$ is an invertible element in $\mathbb{Z}$. □

On est maintenant en mesure de comprendre le facteur parasite que nous avions obtenu lors du calcul de l'équation implicite d'une surface rationnelle.

Corollaire 2.5.3 *Etant donnés trois polynômes $f_k(\boldsymbol{x}, y, z), k = 1, \ldots, 3$ de la forme*

$$f_k(\boldsymbol{x}, y, z) = \sum_{|\alpha|+i+j \leqslant d_k} a^{(k)}_{\alpha,i,j} \boldsymbol{x}^\alpha y^i z^j \in \mathbb{S}[\boldsymbol{x}][y, z],$$

où $\boldsymbol{x}$ désigne la collection de variables $(x_1, \ldots, x_n)$ pour un entier $n \geq 1$ et $\mathbb{S}$ un anneau commutatif, alors le résultant itéré $\mathrm{Res}_y(\mathrm{Res}_z(f_1, f_2), \mathrm{Res}_z(f_1, f_3)) \in \mathbb{S}[\boldsymbol{x}]$ est de degré au plus $d_1^2 d_2 d_3$ en les variables $\boldsymbol{x}$ et on a

$$\begin{aligned}\mathrm{Res}_y(\mathrm{Res}_z(f_1, f_2), \mathrm{Res}_z(f_1, f_3)) = (-1)^{d_1 d_2 d_3} \times \\ \mathrm{Res}_{y,z}(f_1(\boldsymbol{x}, y, z), f_2(\boldsymbol{x}, y, z), f_3(\boldsymbol{x}, y, z)) \times \\ \mathrm{Res}_{y,z,z'}(f_1(\boldsymbol{x}, y, z), f_2(\boldsymbol{x}, y, z), f_3(\boldsymbol{x}, y, z'), \delta_{z,z'}(f_1)).\end{aligned}$$

De plus, si les polynômes f_1, f_2, f_3 sont suffisamment génériques et $n > 1$ alors ce résultant itéré est de degré exactement $d_1^2 d_2 d_3$ en $\boldsymbol{x}$ et les deux résultants multivariés ci-dessus sont distincts et irréductibles.

Ce corollaire peut s'interpréter géométriquement comme suit. Pour simplifier, supposons que $\boldsymbol{x}$ est une unique variable x et que f_1, f_2 et f_3 sont trois polynômes en x, y, z. Le résultant $R_{12} := \mathrm{Res}_z(f_1, f_2)$ définit la projection de la courbe intersection des deux surfaces $\{f_1 = 0\}$ et $\{f_2 = 0\}$. De la même façon, $R_{13} := \mathrm{Res}_z(f_1, f_3)$ définit la projection de la courbe intersection des deux surfaces $\{f_1 = 0\}$ et $\{f_3 = 0\}$. Ainsi, les racines de $\mathrm{Res}_y(R_{12}, R_{13})$ peuvent être séparées en deux ensembles distincts : l'ensemble des racines x_0 tel qu'il existe y_0 et z_0 satisfaisant $f_1(x_0, y_0, z_0) = f_2(x_0, y_0, z_0) = f_3(x_0, y_0, z_0)$, et l'ensemble des racines x_1 tel qu'il existe deux points distincts (x_1, y_1, z_1) et (x_1, y_1', z_1') satisfaisant $f_1(x_1, y_1, z_1) = f_2(x_1, y_1, z_1)$ et $f_1(x_1, y_1', z_1') = f_3(x_1, y_1', z_1')$. Le premier ensemble fournit le terme $\mathrm{Res}_{x,y,z}(f_1, f_2, f_3)$ dans la factorisation du résultant itéré $\mathrm{Res}_y(\mathrm{Res}_{12}, \mathrm{Res}_{13})$, et le second ensemble fournit l'autre facteur.

2.6 Formes d'inerties et représentations matricielles

Les formes d'inerties fournissent, nous l'avons vu, un outil efficace pour établir des propriétés formelles du résultant. Nous allons maintenant montrer qu'elles permettent également de construire des matrices d'élimination de manière systématique. D'ailleurs, la grande majorité des matrices connues qui permettent de "calculer" le résultant sont obtenues de cette façon (voir par exemple [Mac02], [Jou97], [GKZ94a], [CLO98] et leurs références).

Matrices de formes d'inerties. Rappelons qu'une forme d'inertie de degré 0 est toujours un multiple du résultant. De manière générale, on peut construire des formes d'inerties de degré 0 comme des déterminants de matrices obtenues à l'aide de formes d'inerties de degré supérieur.

Lemme 2.6.1 *Supposons donnés un entier $\nu \geq 1$ et $\sharp\mathrm{Mon}(n; \nu)$ formes d'inerties ϕ_α, $|\alpha| = \nu$, pour l'idéal $(f_1, \ldots, f_n)$ de degré ν. Le déterminant de la matrice*

$$\Phi : \mathrm{Mon}(n; \nu) \times \mathrm{Mon}(n; \nu) \to A$$

telle que pour tout $|\alpha| = \nu$ on ait

$$\sum_{|\beta|=\nu} \Phi(X^\alpha, X^\beta) X^\beta = \phi_\alpha \in A[X_1, \ldots, X_n]$$

est une forme d'inertie de degré 0, c'est-à-dire un élément de $\mathfrak{A}$.

Preuve. Par construction, on a l'égalité matricielle

$$\Phi \begin{pmatrix} \vdots \\ X^\beta \\ \vdots \end{pmatrix} = \begin{pmatrix} \vdots \\ \phi_\alpha \\ \vdots \end{pmatrix}$$

dont on déduit par multiplication à gauche par le matrice $\tilde{\Phi}$ des cofacteurs de Φ que

$$\det(\Phi) \begin{pmatrix} \vdots \\ X^\beta \\ \vdots \end{pmatrix} = \tilde{\Phi} \begin{pmatrix} \vdots \\ \phi_\alpha \\ \vdots \end{pmatrix}$$

Les formules de Cramer montrent alors que $X^\beta \det(\Phi) \in (\ldots, \phi_\alpha, \ldots)$ pour tout β tel que $|\beta| = \nu$. On conclut alors en utilisant le fait que les ϕ_α sont des formes d'inerties de $(f_1, \ldots, f_n)$. □

Ce procédé permet de construire des matrices d'élimination personnalisées en utilisant diverses formes d'inerties. Pour aboutir exactement au résultant il faut alors réussir à montrer que le déterminant construit est non nul (on peut pour cela procédé par spécialisation) et qu'il a le bon degré par rapport aux coefficients de chacun des polynômes $f_1, \ldots, f_n$.

C'est par exemple comme cela que l'on construit les matrices de Macaulay, en utilisant les formes d'inertie les plus simples : des multiples des polynômes $f_1, \ldots, f_n$.

Formule de Macaulay. Nous avons déjà construit les matrices de Macaulay et vu que leur déterminant fournissait un multiple du résultant. Il est en fait possible d'en extirper exactement le résultant : c'est la formule de Macaulay [Mac02].

Reprenant les notations précédentes, nous avons montré que $\det(\mathbb{M}(f_1, \ldots, f_n; t))$ est une forme d'inertie, et donc un multiple de $\mathrm{Res}(f_1, \ldots, f_n)$. Il existe donc un polynôme $H \in \mathbb{S}[X_1, \ldots, X_n]$ tel que

$$\det(\mathbb{M}(f_1, \ldots, f_n; t)) = \mathrm{Res}(f_1, \ldots, f_n) H(f_1, \ldots, f_{n-1}; t)$$

(noter que nous avons montré que H ne dépend pas des coefficients du polynôme f_n).

La formule de Macaulay permet de calculer ce polynôme $H(f_1, \ldots, f_{n-1}; t)$: pour tout entier $t \geq \sum_{i=1}^n (d_i - 1) + 1$, on a

$$H(f_1, \ldots, f_{n-1}; t) = \det(\Delta(f_1, \ldots, f_{n-1}; t))$$

où $\Delta(f_1, \ldots, f_{n-1}; t)$ est la sous-matrice de $\mathbb{M}(f_1, \ldots, f_n; t)$ indexée par

$$\mathrm{Dod}(n, t) \times \mathrm{Dod}(n, t) \subset \mathrm{Mon}(n, t) \times \mathrm{Mon}(n, t)$$

avec $\mathrm{Dod}(n, t) := \{X^\alpha : \exists i \neq j \ \alpha_i \geq d_i, \alpha_j \geq d_j\}$. Nous renvoyons le lecteur à [Jou97] pour la preuve de cette formule.

Représentation matricielle. On ne connaît pas de matrice carrée non triviale dont le déterminant soit le résultant en toute généralité. Il existe bien une liste de cas pour lesquels une telle formulation est connue (voir par exemple [Jou97]), mais elle est relativement limitée.

Par contre, on sait toujours "représenter" le résultant à l'aide d'une matrice non carrée. En effet, nous avons vu au début de ce chapitre que l'idéal éliminant $\mathfrak{A}$ est égal à l'annulateur du quotient B en degré suffisamment grand. En fait, on peut montrer que cette propriété est vraie à partir du degré $\sum_{i=1}^n (d_i - 1) + 1 =: \delta + 1$. Ainsi, toute présentation de $B_{\delta+1}$ fournit une représentation du résultant, c'est-à-dire fournit une matrice à coefficient dans A telle que

- la matrice est de génériquement de rang maximal
- le PGCD des mineurs maximaux est égal au résultant
- le rang de cette matrice chute exactement là où le résultant s'annule

C'est surtout la dernière propriété qui permet de parler de représentation du résultant. Pour être plus concret, la matrice de l'application (dans les bases canoniques par exemple)

$$\bigoplus_{i=1}^n A[X_1, \ldots, X_n]_{\delta+1-d_i} \to A[X_1, \ldots, X_n]_{\delta+1} : (g_1, \ldots, g_n) \mapsto \sum_{i=1}^n g_i f_i$$

est une représentation du résultant. Notez que les matrices de Macaulay sont des mineurs maximaux de cette matrice.

Ce genre de résultat suggère fortement que le calcul formel s'intéresse à la manipulation de représentation matricielle des objets, et pas seulement polynomiale. Ce point de vue pourrait permettre dans bien des cas d'améliorer de nombreux algorithmes, notamment en renforçant le l'utilisation d'outils de l'algèbre linéaire numérique.

2.7 La formule de Poisson

Il n'est pas possible de clore ce chapitre sans brièvement donner la célèbre formule de Poisson [Poi02]. Pour un énoncé en toute généralité, on renvoie le lecteur à [Jou97].

Soit k un corps algébriquement clos et soient $f_1, \ldots, f_{n-1} \in k[X_1, \ldots, X_n]$ des polynômes homogènes de degré $d_1, \ldots, d_n \geq 1$ respectivement. On suppose en outre que la variété projective

$$X = V(f_1, \ldots, f_{n-1}) \subset \mathbb{P}_k^{n-1}$$

définit un nombre fini de points à distance finie (donc qu'elle définit $d_1 \ldots d_{n-1}$ points comptés avec multiplicité à distance finie), l'infini correspondant à la droite $V(X_n)$. Pour tout polynôme homogènes $f \in k[X_1, \ldots, X_n]$ de degré $d \geq 1$ on a

$$\frac{\mathrm{Res}(f_1, \ldots, f_{n-1}, f)}{\mathrm{Res}(\overline{f}_1, \ldots, \overline{f}_{n-1})} = \prod_{\xi=(\xi_1:\cdots:\xi_{n-1}:1)\in X} f(\xi)^{\mu(\xi)}$$

où $\mu(\xi)$ désigne la multiplicité de $\xi \in X$ et où $\overline{f}_i := f_i(X_1, \ldots, X_{n-1}, 0) \in k[X_1, \ldots, X_{n-1}]$ pour tout $i = 1, \ldots, n-1$.

Cet énoncé montre clairement le lien que l'on peut faire entre résultant et résolution de systèmes polynomiaux zéro-dimensionnels. Pour en savoir plus, on renvoie le lecteur à [EM07, Chapitre 6], ou encore à [CLO98, Chapitre 3].

Pour finir, mentionnons une autre forme de la formule de Poisson qui se déduit directement de la précédente et qui permet notamment de montrer des résultats non triviaux de géométrie plane (exposés de Jouanolou au CIRM, janvier 1983).

Soient f et g deux polynômes homogènes de degré $d \geq 1$ tels que $V(f_1, \ldots, f_{n-1}, g) = \emptyset$ dans $\mathbb{P}_k^{n-1}$. Alors

$$\frac{\mathrm{Res}(f_1, \ldots, f_{n-1}, f)}{\mathrm{Res}(f_1, \ldots, f_{n-1}, g)} = \prod_{\xi=(\xi_1:\cdots:\xi_{n-1}:1)\in X} \left(\frac{f(\xi)}{g(\xi)}\right)^{\mu(\xi)}$$

(noter que $g = X_n^d$ redonne la formule précédente).

Chapitre 3

Vers une théorie générale du résultant

Bien que de nombreux types de résultants soient connus (Macaulay, toriques, anisotropes, ...), il est fort possible qu'aucun d'entres eux ne permette de traiter un système lié à une situation géométrique spécifique. Le but de ce qui suit est d'illustrer comment il est possible de construire un "résultant" adapté à une telle situation. En filigrane, on illustre le lien entre géométrie et relations algébriques (syzygies). La dernière partie est extraite de [BEM03] où l'on peut également trouver plusieurs applications à la modélisation géométrique.

3.1 Le cas de trois courbes dans le plan

Dans ce qui suit, on se placera toujours dans le plan projectif $\mathbb{P}^2$ dont $R = k[x, y, z]$ désigne l'anneau des coordonnées, k étant un corps algébriquement clos.

Soient f_0, f_1, f_2 trois polynômes homogènes dans $\mathbb{P}^2$ de degré d_0, d_1, d_2 respectivement. On note I l'idéal (f_0, f_1, f_2). Pour un choix suffisamment générique de f_0, f_1, f_2, on a $\sqrt{I} = R$ c'est-à-dire que f_0, f_1, f_2 non pas de racine commune dans $\mathbb{P}^2$. En fait, l'existence d'une racine commune se traduit en termes de non-exactitude du complexe de Koszul associé aux polynôme f_0, f_1, f_2 dans R. On notera ce complexe $K_\bullet(f_0, f_1, f_2)$; il est de la forme

$$R(-d_0 - d_1 - d_2) \xrightarrow{\partial_3} \bigoplus_{0 \le i < j \le 2} R(-d_i - d_j) \xrightarrow{\partial_2} \oplus_{i=0}^{2} R(-d_i) \xrightarrow{\partial_1} R,$$

où

$$\partial_1 = \begin{pmatrix} f_0 & f_1 & f_2 \end{pmatrix}, \partial_2 = \begin{pmatrix} f_1 & f_2 & 0 \\ -f_0 & 0 & f_2 \\ 0 & -f_0 & -f_1 \end{pmatrix}, \partial_3 = \begin{pmatrix} f_2 \\ -f_1 \\ f_0 \end{pmatrix}.$$

Il faut remarquer que ce complexe est construit à partir des relations *triviales* des polynômes f_0, f_1, f_2, c'est-à-dire des relations qui sont toujours vraies quelques soient f_0, f_1, f_2. Elles sont de la forme $f_2 f_1 - f_1 f_2$, $f_1 f_0 - f_0 f_1$, etc .... Les premières relations triviales sont au nombre de trois : les 2×2-mineurs (identiquement nuls) de la matrice

$$\begin{pmatrix} f_0 & f_1 & f_2 \\ f_0 & f_1 & f_2 \end{pmatrix},$$

et la troisième relation (il n'y en a qu'une seule) correspond au déterminant de la matrice

$$\begin{pmatrix} f_0 & f_1 & f_2 \\ f_0 & f_1 & f_2 \\ f_0 & f_1 & f_2 \end{pmatrix}.$$

Proposition 3.1.1 *Les propriétés suivantes sont équivalentes :*
- f_0, f_1, f_2 *n'ont pas de racine commune dans* $\mathbb{P}^2$
- $\sqrt{I} = R$

- $I^{sat} := (I : (x, y, z)^\infty) = R$
- $\mathrm{codim}(I) = 3$
- $K_\bullet(f_0, f_1, f_2)$ *est acyclique*
- I *n'a que des relations triviales*

Preuve. Ces résultats sont classiques. Voir par exemple [Eis95]. □

Remarque 3.1.2 *Les résultats du chapitre précédant montrent que l'on aurait pu ajouter la condition* $\mathrm{Res}(f_0, f_1, f_2) = 0$ *à cette proposition.*

Si notre idéal I possède seulement des relations triviales, son complexe de Koszul associé $K_\bullet(f_0, f_1, f_2)$ fournit alors une résolution libre de R-modules de R/I. On peut alors montrer que I est $(d_0+d_1+d_2-2)$-régulier (au sens de Castelnuovo-Mumford), et donc que I est $(d_0+d_1+d_2-2)$-saturé (voir par exemple [Eis05] pour cette notion de régularité). On déduit la propriété suivante :

Corollaire 3.1.3 *Soit* ν *un entier tel que* $\nu \geq d_0 + d_1 + d_2 - 2$*, alors les polynômes* f_0, f_1, f_2 *ont une racine commune dans* $\mathbb{P}^2$ *si et seulement si l'application* $\partial_{1\nu}$ *n'est pas de rang maximal* $\binom{\nu+2}{2}$*.*

Preuve. Pour tout entier ν nous avons une suite exacte d'espaces vectoriels

$$R_{\nu-d_0-d_1} \oplus R_{\nu-d_0-d_2} \oplus R_{\nu-d_1-d_2} \xrightarrow{\partial_{1\nu}} R_\nu \to R_\nu/I_\nu.$$

Il est clair que si f_0, f_1, f_2 ont une racine commune, alors $\dim(R_\nu/I_\nu) \geq 1$ pour tout entier ν, et donc $\partial_{1\nu}$ n'est pas surjective.

Maintenant, si f_0, f_1, f_2 n'ont pas de racine commune alors $K_\bullet(f_0, f_1, f_2)$ est une résolution libre de R-modules de I et donc I ν-saturé pour tout $\nu \geq d_0 + d_1 + d_2 - 2$. Puisque $I^{sat} = R$, on en déduit que $R_\nu/I_\nu = 0$ pour tout $\nu \geq d_0 + d_1 + d_2 - 2$, et donc que $\partial_{1\nu}$ est surjective. □

Remarque 3.1.4 *La corollaire précédent est une généralisation directe du résultant de Sylvester. Le seule différence notable est qu'ici la représentation matricielle n'est pas carrée en général, alors qu'elle l'est pour Sylvester pour* $\nu = d_1 + d_2 - 1$ *(ensuite elle ne l'est plus).*

Il est intéressant de spécialiser ce corollaire au cas où f_0, f_1, f_2 *sont des formes linéaires et l'entier* ν *est le plus petit possible.*

Considérons à présent l'exemple de l'intersection de trois cercles dans $\mathbb{P}^2$:

$$\begin{cases} f_0 = a_0z^2 + a_1xz + a_2yz + a_3(x^2+y^2) \\ f_1 = b_0z^2 + b_1xz + b_2yz + b_3(x^2+y^2) \\ f_2 = c_0z^2 + c_1xz + c_2yz + c_3(x^2+y^2) \end{cases} \tag{3.1}$$

où les a_i, b_j et c_k sont des éléments de k. Nous voudrions savoir si ces trois cercles se coupent en un même point dans $\mathbb{P}^2$, ce qui dépend évidemment des paramètres a_i, b_j et c_k. Mais ces trois cercles se coupent *toujours* à l'infini en les deux points $P_1 = (1 : i : 0)$ et $P_2 = (1 : -i : 0)$; ces deux points sont définis par l'idéal $(z, x^2 + y^2)$. Par conséquent, le complexe de Koszul $K_\bullet(f_0, f_1, f_2)$ ne sera jamais acyclique dans ce cas. De plus, le résultant de Macaulay de nos trois équations sera toujours identiquement nul (et il en est de même pour le résultant torique que nous n'avons pas eu le temps d'aborder dans ces notes).

Puisque les points P_1 et P_2 sont toujours dans l'intersection de nos trois cercles, on peut reformuler notre problématique ainsi : est-ce que nos trois cercles se coupent en dehors des points P_1 et P_2 ? Cette question conduit naturellement à la recherche d'un résultant généralisé. Nous allons voir comment l'on peut répondre à cette question, toujours à l'aide des relations "triviales".

Soit $G = (g_1, \ldots, g_n)$ un idéal homogène de R, les g_i étant des polynômes homogènes. On note $k_1 \geq \ldots \geq k_n$ respectivement, le degré des polynômes $g_1, \ldots, g_n$. On considère alors trois polynômes homogènes f_0, f_1, f_2 de degré $d_0 \geq d_1 \geq d_2 \geq k_1$ respectivement, dans l'idéal G, c'est-à-dire que nous pouvons écrire :

$$\begin{cases} f_0(x) &= \sum_{i=1}^n h_{i,0}(x)\, g_i(x) \\ f_1(x) &= \sum_{i=1}^n h_{i,1}(x)\, g_i(x) \\ f_2(x) &= \sum_{i=1}^n h_{i,2}(x)\, g_i(x) \end{cases}$$

ou de manière équivalente

$$\begin{pmatrix} f_0 & f_1 & f_2 \end{pmatrix} = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \end{pmatrix} \begin{pmatrix} h_{1,0} & h_{1,1} & h_{1,2} \\ h_{2,0} & h_{2,1} & h_{2,2} \\ \vdots & \vdots & \vdots \\ h_{n,0} & h_{n,1} & h_{n,2} \end{pmatrix} \tag{3.2}$$

où $h_{i,j} = \sum_{\alpha_1+\alpha_2+\alpha_3=d_j-k_i} c_\alpha^{i,j}\, x^{\alpha_1} y^{\alpha_2} z^{\alpha_3}$ sont des polynômes homogènes de degré $d_j - k_i$.

La situation géométrique s'interprète comme suit : l'idéal G définit un sous-schéma fermé de $\mathbb{P}^2 := \mathrm{Proj}(R/G)$; on note $\mathcal{G}$ son faisceau d'idéaux associé. Le polynômes f_0, f_1, f_2 sont des sections globales de $\mathcal{G}(d_0), \mathcal{G}(d_1), \mathcal{G}(d_2)$ respectivement (et donc s'annulent le long de $\mathrm{Proj}(R/G)$) et nous voudrions savoir s'ils possèdent une racine commune "en dehors" du sous-schéma défini par $\mathcal{G}$. Désignant par $\mathcal{I}$ le faisceau d'idéaux associé à l'idéal $I = (f_0, f_1, f_2)$, on donne un sens au terme "en dehors" en demandant que le sous-schéma défini par $\mathcal{I}$ soit strictement plus gros que le sous-schéma défini par $\mathcal{G}$. C'est équivalent à demander que $(\mathcal{I} : \mathcal{G}) \subsetneq \mathcal{O}_{\mathbb{P}^2}$, ou bien $V(I : G) \neq \emptyset$, ou bien encore $I^{sat} \subsetneq G^{sat}$, où l'exposant *sat* désigne la saturation par l'idéal maximal (x, y, z) de R. Notre objectif est ici de construire un complexe de relations triviales pour les idéaux de la forme $(I : G)$ où G est fixé ; un tel idéal est souvent appelé une *intersection résiduelle*.

A partir de maintenant, nous supposerons que l'idéal $G = (g_1, \ldots, g_n)$ est fixé et qu'il est *saturé de codimension 2*. Ainsi, nous avons la

Proposition 3.1.5 (Hilbert-Burch) *Toute résolution minimale libre graduée de R-modules de l'idéal G est de la forme :*

$$0 \to \bigoplus_{i=1}^{n-1} R(-l_i) \xrightarrow{\psi} \bigoplus_{i=1}^{n} R(-k_i) \xrightarrow{\gamma=(g_1,\ldots,g_n)} G \to 0,$$

où $\sum_{i=1}^{n-1} l_i = \sum_{i=1}^{n} k_i$ et $aI_{n-1}(\psi) = \gamma$, avec $a \in k \setminus \{0\}$.

Preuve. Ce résultat est classique, voir par exemple [Eis95, Theorem 20.15]. Noter que ce théorème est vrai dans un contexte plus général : tout idéal Q d'un anneau commutatif A de codimension 2 tel que A/Q est Cohen-Macaulay est de dimension projective 1. □

De la résolution de G, on peut déjà savoir combien de points nous essayons de soustraire de l'intersection des polynômes f_0, f_1, f_2.

Corollaire 3.1.6 *L'idéal G de la proposition 3.1.5 définit exactement*

$$\frac{\sum_{i=1}^{n-1} l_i^2 - \sum_{i=1}^{n} k_i^2}{2}$$

points (comptés avec multiplicité).

Preuve. Puisque G définit des points isolés, il suffit de calculer la caractéristique d'Euler d'une partie graduée, disons t, de sa résolution libre. Ainsi, le nombre de points est donnés par la formule (forcément indépendante de t) :

$$N = \binom{t+2}{2} - \sum_{i=1}^{n} \binom{t-k_i+2}{2} + \sum_{i=1}^{n-1} \binom{t-l_i+2}{2}.$$

Un calcul direct donne alors le résultat annoncé. □

Exemple 3.1.1 *Dans le cas où G est une intersection complète, i.e. $G = (g_1, g_2)$, on retrouve bien le nombre de Bézout attendu.*

De la proposition 3.1.5 on déduit la présentation graduée de R-modules de l'idéal G/I (rappelons que $I \subset G$) suivante :

$$\bigoplus_{i=1}^{n-1} R(-l_i) \bigoplus_{i=0}^{2} R(-d_i) \xrightarrow{\psi\oplus\phi} \bigoplus_{i=1}^{n} R(-k_i) \xrightarrow{\gamma} G/I \to 0, \tag{3.3}$$

où ϕ est la $n \times 2$-matrice $(h_{i,j})_{1\leq i\leq n, 0\leq j\leq 2}$ qui apparait dans (3.2). Noter que notre intérêt pour l'idéal G/I est du à l'égalité, facile à vérifier,

$$\mathrm{ann}_R(\mathrm{coker}(\psi \oplus \phi)) = \mathrm{ann}_R(G/I) = (I : G)$$

Cette égalité nous conduit à un théorème de Buchsbaum et Eisenbud (voir [BE77]) :

Proposition 3.1.7 *Soit S un anneau noetherien et $\alpha : S^m \to S^n$ un morphisme tel que $m \geq n$. Alors*

$$\mathrm{ann}_S(coker(\alpha))^n \subseteq I_n(\alpha) \subseteq \mathrm{ann}_S(coker(\alpha)),$$

où $I_n(\alpha)$ désigne l'idéal engendré par les $n \times n$-mineurs de la matrice α. De plus, si $\mathrm{depth}(I_n(\alpha)) = m - n + 1$, alors $I_n(\alpha) = \mathrm{ann}_S(coker(\alpha))$.

Dans notre contexte, cette proposition montre que si $I_n(\psi \oplus \phi)$ est de codimension attendue $(n + 2) - n + 1 = 3$, alors il est égal à l'idéal $(I : G)$. De plus, si tel est le cas, nous connaissons un résolution libre de $(I : G)$:

Proposition 3.1.8 *Soit S un anneau noethérien et $\alpha : S^m \to S^n$ tel que $m \geq n$. Le complexe d'Eagon-Northcott $\mathrm{EN}(\alpha)$ de l'application α est exact (et donc fournit une résolution libre de $S/I_n(\alpha)$) si et seulement si $\mathrm{depth}(I_n(\alpha)) = m - n + 1$, la profondeur attendue.*

Arrêtons-nous un instant sur ce complexe. Noter tout d'abord que si $n = 1$, ce complexe est simplement le complexe de Koszul associé à la suite formée des éléments de la matrice-ligne $S^m \to S$. En fait, comme le complexe de Koszul, le complexe d'Eagon-Northcott d'une application α donnée est construit à partir des relations *triviales* de α. Pour l'illustrer, supposons que α est la $n \times (n + 1)$-matrice

$$\alpha = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n+1} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n+1} \end{pmatrix}.$$

La première application de $\mathrm{EN}(\alpha)$ est $\wedge^n\alpha : \wedge^n(S^{n+1}) \to \wedge^n(S^n)$ qui, en termes de base, envoie l'élément $e_{i_1} \wedge \ldots \wedge e_{i_n}$ sur le déterminant $\Delta_{i_1,\ldots,i_n}$ de la sous-matrice de α correspondant aux colonnes $i_1, \ldots, i_n$. Maintenant, si l'on regarde les relations triviales de ces n déterminants, on doit choisir une ligne de α (il y a n possibilités), disons la ligne numéro i, et écrire que le déterminant de la matrice (qui est α plus la ligne i)

$$\begin{vmatrix} a_{i,1} & \cdots & a_{i,n+1} \\ a_{1,1} & \cdots & a_{1,n+1} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n+1} \end{vmatrix} = a_{i,1}\Delta_{2,\ldots,n+1} - a_{i,2}\Delta_{1,3,\ldots,n+1} + \ldots = 0.$$

De cette facon, on obtient n relations triviales sur les déterminants Δ et donc une application $S_1(S^{n*}) \to \wedge^n(S^{n+1})$ correspondant à choisir une ligne dans α (ce qui explique le dual "*") et lui associer la relation triviale que l'on vient de décrire. Si l'on respecte les règles de signe sur les déterminants, alors il est facile de constater que la dernière application n'est rien d'autre que la transposée de α. Nous avons ainsi construit le complexe d'Eagon-Northcott, qui est souvent appelé le complexe d'Hilbert-Burch dans ce cas.

Si maintenant l'on suppose que α est de taille $n \times (n + 2)$, nous devons alors ajouter une ligne à α (donc on a $S_1(S^{n*})$) et choisir $n+1$ colonnes dans la nouvelle matrice obtenue à partir de α en ajoutant cette ligne, qui est de taille $n \times (n + 1)$ (cela donne $\wedge^{n+1}(S^{n+2})$). Nous obtenons ainsi le complexe

$$S_1(S^{n*}) \otimes \wedge^{n+1}(S^{n+2}) \to \wedge^n(S^{n+2}) \xrightarrow{\wedge^n\alpha} \wedge^n(S^n).$$

La dernière étape est d'ajouter une nouvelle ligne de α à cette dernière matrice, ce qui correspond à un choix dans $S_2(S^{n*})$. Finalement, le complexe d'Eagon-Northcott est donné par :

$$0 \to S_2(S^{n*}) \to S_1(S^{n*}) \otimes \wedge^{n+1}(S^{n+2}) \to \wedge^n(S^{n+2}) \xrightarrow{\wedge^n\alpha} \wedge^n(S^n).$$

Revenons à notre situation.

Théorème 3.1.9 *Les propriétés suivantes sont équivalentes :*
- $\sqrt{(I:G)} = R$
- $I^{sat} = G^{sat}$ *(c'est-à-dire* $\mathcal{I} = \mathcal{G}$*)*
- $\operatorname{codim}((I:G)) = 3$
- $\mathrm{EN}(\psi \oplus \phi)$ *est acyclique*
- $(I:G)$ *n'a que des relations triviales*

Nous avons ainsi que $\mathrm{EN}(\psi \oplus \phi)$ n'est pas acyclique si et seulement si $\mathcal{I} \subsetneq \mathcal{G}$, c'est-à-dire que les polynômes f_0, f_1, f_2 définissent un point qui n'est pas défini par $\mathcal{G}$, au sens des schémas.

Supposons que nous ayons un idéal I tel que $\operatorname{codim}(I:G) = 3$. Par le théorème précédent, $\mathrm{EN}(\psi \oplus \phi)$ fournit une résolution libre graduée de R-modules de $R/(I:G)$. Il s'en suit que nous pouvons borner sa régularité (au sens de Castelnuovo), et donc l'indice de saturation, de $(I:G)$:

Corollaire 3.1.10 *Supposons que* $\operatorname{codim}(I:G) = 3$*, alors* $(I:G)$ *est* ν*-regulier pour tout* $\nu \geq d_0 + d_1 + d_2 - 2(k_n + 1)$ *(rappelons que* $k_n = \min k_i$*).*

Preuve. Nous avons juste à écrire les "shifts" sur les degrés du complexe d'Eagon-Northcott $\mathrm{EN}(\psi \oplus \phi)$. L'application à considérer est

$$\psi \oplus \phi : E := \bigoplus_{i=1}^{n-1} R(-l_i) \bigoplus_{i=0}^{2} R(-d_i) \longrightarrow F := \bigoplus_{i=1}^{n} R(-k_i),$$

et $\mathrm{EN}(\psi \oplus \phi)$ est le complexe :

$$0 \to \wedge^{n+2} E \otimes S_2(F^*) \otimes \wedge^n F^* \to \wedge^{n+1} E \otimes S_1(F^*) \otimes \wedge^n F^*$$

$$\to \wedge^n E \otimes S_0(F^*) \otimes \wedge^n F^* \to R \to R/(I:G) \to 0.$$

Le terme le plus à gauche à un "shift" de $-d_0 - d_1 - d_2 - \sum l_i$ provenant de $\wedge^{n+2} E$, $\sum k_i$ provenant de $\wedge^n F^*$, et aussi $k_i k_j$ provenant de $S_2(F^*)$. Il vient alors que $R/(I:G)$ est $(d_0+d_1+d_2-2k_n-3)$-régulier. □

Nous sommes maintenant en mesure d'énoncer une généralisation du corollaire 3.1.3 :

Corollaire 3.1.11 *Soit* ν *un entier tel que* $\nu \geq d_0 + d_1 + d_2 - 2(k_n + 1)$*, alors* $\operatorname{codim}(I:G) \leq 2$ *si et seulement si l'application* $\wedge^n (\psi \oplus \phi)_\nu$ *n'est pas surjective, c'est-dire n'est pas de rang maximal* $\binom{\nu+2}{2}$*.*

Preuve. Similaire à la preuve du corollaire 3.1.3. □

Remarque 3.1.12 *Ce corollaire généralise le corollaire 3.1.3 puisqu'on obtient ce dernier en prenant* $G = R$ *(et donc* $k_n = 0$*).*

Ce corollaire est le point de départ de la définition et du calcul d'une représentation matricielle d'un résultant avec point bases fixés dans le plan. Nous y reviendrons à la fin du chapitre.

Pour terminer, nous finissons avec l'exemple (3.1) des trois cercles :

$$\begin{cases} f_0 = a_0 z^2 + a_1 xz + a_2 yz + a_3(x^2 + y^2) \\ f_1 = b_0 z^2 + b_1 xz + b_2 yz + b_3(x^2 + y^2) \\ f_2 = c_0 z^2 + c_1 xz + c_2 yz + c_3(x^2 + y^2) \end{cases}$$

L'idéal G est ici $G = (z, x^2 + y^2)$, deux points en intersection complète. La résolution de G est donnée par le complexe de Koszul et donc $\psi = \begin{pmatrix} x^2 + y^2 \\ -z \end{pmatrix}$. La matrice $\psi \oplus \phi$ est donc

$$\begin{pmatrix} x^2 + y^2 & a_0 z + a_1 x + a_2 y & b_0 z + b_1 x + b_2 y & c_0 z + c_1 x + c_2 y \\ -z & a_3 & b_3 & c_3 \end{pmatrix}$$

La borne de régularité, donc de l'indice de saturation, est ici $6-4=2$. et doc la matrice $\wedge^2(\psi\oplus\phi)_2$ est de taille 6×12 et est de la forme :

$$\begin{pmatrix} a_0 & b_0 & c_0 & 0 & 0 & 0 & \\ 0 & 0 & 0 & -b_1c_3+c_1b_3 & -b_2c_3+c_2b_3 & -c_1a_3+a_1c_3 & \cdots \\ a_1 & b_1 & c_1 & 0 & -c_3b_0+b_3c_0 & 0 & \\ c_2 & b_2 & c_2 & -c_3b_0+b_3c_0 & 0 & a_0c_3-c_0a_3 & \cdots \\ a_3 & b_3 & c_3 & 0 & -b_1c_3+c_1b_3 & 0 & \\ a_3 & b_3 & c_3 & -b_2c_3+c_2b_3 & 0 & -c_2a_3+a_2c_3 & \end{pmatrix}.$$

3.2 Résultant général d'un système polynomial

The theory of resultant is devoted to the study of conditions on the coefficients of an overdetermined system to have a solution in a fixed variety. The typical situation is the case of a system of $n+1$ equations in a projective variety X of dimension n, of the form :

$$\mathbf{f_c} := \begin{cases} f_0(x) &= \sum_{j=0}^{k_0} c_{0,j}\,\psi_{0,j}(x) \\ &\vdots \\ f_n(x) &= \sum_{j=0}^{k_n} c_{n,j}\,\psi_{n,j}(x) \end{cases}$$

where $\mathbf{c}=(c_{i,j})$ are parameters, x is a point of X, and such that for all $i=0,\ldots,n$ we have a regular map (independent of $\mathbf{c}$)

$$\phi_i : x\in X \mapsto (\psi_{i,0}(x):\ldots:\psi_{i,k_i}(x))\in\mathbb{P}^{k_i}\ .$$

In the language of modern algebraic geometry, to each map ϕ_i is associated an invertible sheaf $\mathcal{L}_i=\phi^*(\mathcal{O}_{\mathbb{P}^{k_i}}(1))$, and a vector subspace $V_i=\langle\psi_{i,0},\ldots,\psi_{i,k_i}\rangle$ of its global sections $\Gamma(X,\mathcal{L}_i)$ (see [Har77], II.7). In this way, the $\mathbb{K}$-vector space V_i parameterizes all the polynomials f_i that we can obtain by specializing the coefficients $(c_{i,j})_{j=0,\ldots,k_i}$ in $\mathbb{K}$. As two polynomials f_i and g_i such that $f_i=\lambda g_i$ with $\lambda\in\mathbb{K}^*$ define the same zero locus, it is convenient to identify them, and hence to parameterize polynomials f_i by the projective space $\mathbb{P}(V_i)\simeq\mathbb{P}^{k_i}$.

The projection (or elimination) problem consists, in this case, in finding necessary (and sufficient) conditions on $\mathbf{c}$ such that the system $\mathbf{f_c}=0$ has a solution in X. Considering a geometric point of view, we look for the values of parameters $\mathbf{c}=(c_{i,j})\in\mathbb{P}^{k_0}\times\cdots\times\mathbb{P}^{k_n}$ such that there exists $x\in X$ with $f_i(x)=\sum_{j=0}^{k_i}c_{i,j}\psi_{i,j}(x)=0$ for $i=0,\ldots,n$. In other words, $\mathbf{c}$ is the first projection of the point $(\mathbf{c},x)$ in the *incidence variety*

$$W_X=\{(\mathbf{c},x)\in\mathbb{P}^{k_0}\times\cdots\times\mathbb{P}^{k_n}\times X : f_i(x)=0, i=0,\ldots,n\}.$$

We denote by $\pi_1 : W_X\to\mathbb{P}^{k_0}\times\cdots\times\mathbb{P}^{k_n}$ and $\pi_2 : W_X\to X$ the first and second projections. The image by π_2 of a point of W_X is a solution in X of the associated system, and the image of W_X by π_1 is precisely the set of values of parameters $\mathbf{c}$ for which the system has a root in X. We define the resultant of $f_0,\ldots,f_n$ when $\pi_1(W_X)$ is an irreducible hypersurface, and we denote $\mathrm{Res}_{V_0,\ldots,V_n}$ its equation (unique up to a non-zero multiple in $\mathbb{K}$).

Définition 3.2.1 *Let $\mathcal{L}$ be an invertible sheaf on X and V be a vector subspace of the vector space of its global sections $H^0(X,\mathcal{L})$.*

- *The base points of V are the points $x\in X$ such that $f(x)=0$ for all $f\in V$.*
- *V is said to be very ample if the canonical map*

$$x\in X\mapsto\{f\in V : f(x)=0\}\in\mathbb{P}(V)$$

is an embedding, or equivalently, if V separates the points and the tangent vectors in X (see [GH94] p.180).

- *V is said to be very ample almost everywhere if there exists a dense open subset U of X such that the restricted map*

$$x\in U\mapsto\{f\in V : f(x)=0\}\in\mathbb{P}(V)$$

is an embedding.

Théorème 3.2.2 ([BEM01] proposition 1) *Suppose that each V_i is very ample almost everywhere and has no base points, then $\pi_1(W_X)$ is a hypersurface of $\prod_{i=0}^n \mathbb{P}^{k_i}$. Its degree in the coefficients of f_i (that is w.r.t. to $\mathbb{P}^{k_i}$) is $\int_X \prod_{j\neq i} c_1(\mathcal{L}_j)$, where $c_1(\mathcal{L}_j)$ denotes the first Chern class of the invertible sheaf $\mathcal{L}_j$.*

Remarque 3.2.3 *It is clear that if V_i is very ample then V_i has no base points and V_i is very ample almost everywhere. Consequently the mixed resultant of [GKZ94b] is contained in this theorem.*

If the system $\mathbf{f_c}$ satisfies the hypothesis of theorem 3.2.2, $\mathrm{Res}_{V_0,\dots,V_n}$ is a function on $\prod_{i=0}^n \mathbb{P}^{k_i}$ satisfying the property

$$\mathrm{Res}_{V_0,\dots,V_n}(f_0,\dots,f_n)=0 \Leftrightarrow \exists\, x\in X : f_0(x)=\cdots=f_n(x)=0.$$

By construction $\mathrm{Res}_{V_0,\dots,V_n}$ is multihomogeneous, its degree in the coefficients of f_i is given by the "explicit formula" $\int_X \prod_{j\neq i} c_1(\mathcal{L}_j)$. This number can be seen as the number of solutions of a generic system $\{x\in X : f_j(x)=0 : j=0,\dots,n, j\neq i\}$.

As we will see in the next section, a lot of known resultants as classical resultants, toric resultants or anisotropic resultants are obtained from theorem 3.2.2 by choosing X and $V_0,\dots,V_n$ adequately. However this construction of resultant degenerates if the system $\mathbf{f_c}$ has base points (i.e. $\pi_1(W_X)=\prod_{i=0}^n \mathbb{P}^{k_i}$). Such systems with base points arise very often in practice, so we now generalize the preceding construction of resultants, taking into account the possible presence of base points.

From now on, we only suppose that the maps ϕ_i are rational and not necessarely regular (i.e. possibly with base points), each vector space V_i being a subvector space of the global sections of a given invertible sheaf $\mathcal{L}_i$. We will use a standard tool in algebraic geometry to "erase" base points, called the blowing-up. The basic idea is to blow-up X along the base points locus of the system $\mathbf{f_c}$, then obtain a new projective variety $\tilde{X}$ of the same dimension where the pull-back of our system $\mathbf{f_c}$ can be seen without base points, and finally apply theorem 3.2.2. Roughly speaking we blow-up the ideal of X associated to the union of base points of each V_i, for $i=0,\dots,n$. More precisely, we blow-up the ideal sheaf $\mathcal{I}$ on X obtained as the image of the morphism of sheaves $(\oplus_{i=0}^n V_i)\otimes_{\mathbb{K}}(\oplus_{i=0}^n \mathcal{L}_i^*)\to\mathcal{O}_X$, induced by the canonical morphism $\oplus_{i=0}^n V_i\otimes_{\mathbb{K}}\mathcal{O}_X\to\oplus_{i=0}^n\mathcal{L}_i$. We denote the blow-up of X along $\mathcal{I}$ by $\pi:\tilde{X}\to X$. The new incidence variety is

$$W_{\tilde{X}}=\{(\mathbf{c},x)\in\mathbb{P}^{k_0}\times\cdots\times\mathbb{P}^{k_n}\times\tilde{X} : \tilde{f}_i(x)=0, i=0,\dots,n\},$$

where $\tilde{f}_i$ denotes the virtual transform of f_i by π, that is the pull-back $\pi^*(f_i)$ of f_i seen as a section of $\pi^*(\mathcal{L}_i)\otimes\pi^{-1}\mathcal{I}.\mathcal{O}_{\tilde{X}}$. Denoting by $\tilde{\pi}_1 : W_{\tilde{X}}\to\mathbb{P}^{k_0}\times\cdots\times\mathbb{P}^{k_n}$ and $\pi_2 : W_{\tilde{X}}\to\tilde{X}$ the two natural projections, we obtain the following corollary of theorem 3.2.2.

Corollaire 3.2.4 ([Bus01a] proposition 2.2.4) *Suppose that each V_i is very ample almost everywhere, then $\tilde{\pi}_1(W_{\tilde{X}})$ is a hypersurface of $\prod_{i=0}^n\mathbb{P}^{k_i}$. Its degree in the coefficients of f_i (that is w.r.t. to $\mathbb{P}^{k_i}$) is given by $\int_X\prod_{j\neq i}c_1(\mathcal{L}_j)\otimes\pi^{-1}\mathcal{I}.\mathcal{O}_{\tilde{X}}$.*

Moreover if there is no base points, then the ideal sheaf $\mathcal{I}$ is exactly $\mathcal{O}_X$, and π is the identity $X\to X$ so that we recover the construction of resultants of theorem 3.2.2. Consequently, as soon as the V_i's are very ample almost everywhere, we construct a resultant for the system $\mathbf{f_c}$ denoted by $\mathrm{Res}_{V_0,\dots,V_n}$ and defined as the equation of the hypersurface $\tilde{\pi}_1(W_{\tilde{X}})$. It is, as usual, multihomogeneous and satisfies

$$\mathrm{Res}_{V_0,\dots,V_n}(f_0,\dots,f_n)=0\Leftrightarrow\exists\, x\in\tilde{X} : \tilde{f}_0(x)=\cdots=\tilde{f}_n(x)=0.$$

Notice that this resultant depend only on the birational equivalent class of X and the vector spaces $V_0,\dots,V_n$ (and not on the $\mathcal{L}_i$'s ; see [Bus01a] chapter 2 for more details).

We have thus constructed a general resultant which is valid for a very large range of systems $\mathbf{f_c}$, but it remains to compute it !

3.3 Exemples de résultants particuliers

In this section we give several examples of resultants as particular cases of the previous construction and show how to compute them.

3.3.1 Macaulay resultant

The classical case studied in [Mac02], [VdW48], is the case where X is the projective space $\mathbb{P}^n$ and V_i, for $i = 0, \ldots, n$, is the vector of all monomials of a fixed degree d_i. Clearly, when $d_i \geq 1$ each $\mathcal{L}_i = \mathcal{O}_X(d_i)$ separates the points and the tangent vectors and thus $\mathrm{Res}_{V_0,\ldots,V_n}$ is well defined. It is traditionally denoted $\mathrm{Res}_{\mathbb{P}^n}$. By theorem 3.2.2 (or Bézout theorem), its degree with respect to V_i is $\prod_{j\neq i} d_j$.

The necessary and sufficient condition on $\mathbf{c}$ such that $f_0, \ldots, f_n$ have a common root in $\mathbb{P}^n$ is $\mathrm{Res}_{\mathbb{P}^n}(\mathbf{f_c}) = 0$. Macaulay's construction [Mac02] of the classical resultant can be seen as an extension of Sylvester's method to the multivariate case. We describe it in the affine setting by substituting $x_0 = 1$, $x_1 = t_1, \ldots, x_n = t_n$.

Let $\nu = \sum_{i=0}^{n} d_i - n$ and $\mathbf{t}^F$ be the set of all monomials in $\mathbf{t}$ of degree $\leq \nu$. It contains $\binom{\nu+n}{n}$ elements. Let $t_n^{d_n}\mathbf{t}^{E_n}$ be the set of all monomials of $\mathbf{t}^F$ which are divisible by $t_n^{d_n}$. For $i = n-1, \ldots, 1$, we define by induction $t_i^{d_i}\mathbf{t}^{E_i}$ to be the set of all monomials of $\mathbf{t}^F \setminus (t_n^{d_n}\mathbf{t}^{E_n} \cup \ldots \cup t_{i+1}^{d_{i+1}}\mathbf{t}^{E_{i+1}})$ which are divisible by $t_i^{d_i}$. The set $\mathbf{t}^F \setminus (t_n^{d_n}\mathbf{t}^{E_n} \cup \ldots \cup t_1^{d_1}\mathbf{t}^{E_1})$ is denoted by $\mathbf{t}^{E_0}$ and is equal to

$$\mathbf{t}^{E_0} = \{t_1^{\alpha_1} \cdots t_n^{\alpha_n} : 0 \leq \alpha_i \leq d_i - 1\}.$$

It has $d_1 \cdots d_n$ monomials.

If $E \subset \mathbb{N}^n$, $\langle \mathbf{t}^E \rangle$ denotes the vector subspace generated by the set $\mathbf{t}^E$.

The resultant matrix $\mathtt{S}$ is the matrix in monomial bases of the linear map :

$$\begin{array}{rcl} \mathcal{S} : \langle \mathbf{t}^{E_0} \rangle \times \cdots \times \langle \mathbf{t}^{E_n} \rangle & \to & \langle \mathbf{t}^F \rangle \\ (q_0, \ldots, q_n) & \mapsto & \displaystyle\sum_{i=0}^{n} q_i f_i. \end{array} \tag{3.4}$$

The determinant of $\mathtt{S}$ is generically not 0 (for it does not vanish when we specialize f_i to $t_i^{d_i}$) and has the same degree $\prod_{i=1}^{n} d_i$ as the resultant with respect to V_0. Therefore

$$\det(\mathtt{S}) = \mathrm{Res}_{\mathbb{P}^n}(\mathbf{f_c})\ \Delta(f_1, \ldots, f_n),$$

where $\Delta(f_1, \ldots, f_n)$ is a subminor of $\mathtt{S}$ depending only on the coefficients of $f_1, \ldots, f_n$ [Mac02].

We remark that, if $R = \mathbb{K}[t_1, \ldots, t_n]$, the map (3.4) is in fact connected to the first map of the Koszul complex of the sequence $f_0, \ldots, f_n$,

$$0 \to \wedge^n R^n \xrightarrow{d_n} \wedge^{n-1} R^n \longrightarrow \cdots \longrightarrow R^n \xrightarrow{d_1} R,$$

in degree ν, where $d_l(e_{i_1} \wedge \cdots \wedge e_{i_l}) = \sum_{j=1}^{l} (-1)^j f_{i_j} e_{i_1} \wedge \cdots \widehat{e_{i_1}} \cdots \wedge e_{i_l}$. Indeed as shown in [Dem84], [Cha] the determinant of the Koszul complex is the classical resultant of $f_0, \ldots, f_n$. For other constructions, also related to the Koszul complex and its dual which also yield the classical resultant sometimes in a more compact way, we refer to [Jou97], [WZ94], [DD01].

This resultant has been widely studied, and has a lot of properties ; a quasi-complete list can be found in [Jou91b]. We recall two of them that we will use later, a weight invariance property and the so-called Poisson's formula.

For $i = 0 \ldots n$, let $f_i = \sum_{|\alpha|=d_i} c_{\alpha,i}\mathbf{x}^\alpha$ be the generic homogeneous polynomial of degree d_i. The coefficients $c_{\alpha,i}$ are considered as indeterminates, that is $f_i \in A[\mathbf{x}]$ where A denotes the coefficient ring $\mathbb{Z}[c_{\alpha,i}, |\alpha| = d_i]$.

Lemme 3.3.1 ([Jou91b] 5.13.2) *Let m be a fixed integer in $\{0, 1, \ldots, n\}$. We graduate the ring A by setting $\deg(c_{\alpha,i}) = \alpha_m$. Then $\mathrm{Res}_{\mathbb{P}^n}(f_0, \ldots, f_n) \in \mathbb{Z}[c_{\alpha,i}, |\alpha| = d_i]$ is isobar (i.e. homogeneous for this graduation) of weight $\prod_{i=0}^{n} d_i$ in A.*

This lemma is a corollary of a more general formula called the "changing basis formula" (see [Jou91b] 5.12). We end this section with the well-known Poisson's formula. For all $i = 0, \ldots, n$, let $\tilde{f}_i(x_1, \ldots, x_n) := f_i(1, x_1, \ldots, x_n)$ and $\overline{f}_i(x_0, \ldots, x_{n-1}) := f_i(0, x_1, \ldots, x_n)$.

Lemme 3.3.2 ([Jou91b] 2.7, [CLO98] III.3.5) *Let $\rho = \mathrm{Res}_{\mathbb{P}^{n-1}}(\overline{f}_1, \ldots, \overline{f}_n) \in A$. We have*

$$\mathrm{Res}_{\mathbb{P}^n}(f_0, \ldots, f_n) = \det(\mathrm{M}(\tilde{f}_0))\ \mathrm{Res}_{\mathbb{P}^{n-1}}(\overline{f}_1, \ldots, \overline{f}_n)^{d_0},$$

where $\mathrm{M}(\tilde{f}_0)$ is the multiplication by $\tilde{f}_0$ in $A_\rho[x_1, \ldots, x_n]/(\tilde{f}_1, \ldots, \tilde{f}_{n-1})$.

3.3.2 Anisotropic resultant

This resultant was introduced and studied by Jouanolou in [Jou91b] and [Jou96]. It is a generalization of the classical resultant, taking into account the possible combinatorial properties of a polynomial system and giving a more "reduced" eliminant polynomial. Instead of considering all the variables $x_0, \ldots, x_n$ of the same degree 1, we consider them with different weights.

Let $m_0, m_1, \ldots, m_n$ in $\mathbb{N}^*$. Set $\mu = \mathrm{lcm}(m_0, \ldots, m_n)$, $\delta = \gcd(m_0, \ldots, m_n)$, and $\Delta = \dfrac{m_0 m_1 \ldots m_n}{\delta} \in \mathbb{N}$. We denote by C the polynomial ring $\mathbb{K}[x_0, \ldots, x_n]$ with $\deg(x_i) = 1$, and by ${}^aC$ the same polynomial ring but with $\deg(x_i) = m_i$ (the exponent a stands for *a*nisotropic). Usually we consider the projective space $\mathbb{P}^n = \mathrm{Proj}(C)$, but here we work on ${}^a\mathbb{P}^n = \mathrm{Proj}({}^aC)$, that is the anisotropic projective space with weights $(m_0, \ldots, m_n)$. Notice that from a geometrical point of view we have the canonical morphism

$$(x_0 : \cdots : x_n) \in \mathbb{P}^n \mapsto (x_0^{m_0} : \cdots : x_n^{m_n}) \in {}^a\mathbb{P}^n.$$

Let $X = {}^a\mathbb{P}^n$ and V_i, for all $i = 0, \ldots, n$, be the set of all isobar (i.e. homogeneous in the weighted variables) monomials of degree d_i in ${}^aC$, that is V_i is the vector space of global sections of the invertible sheaf $\mathcal{L}_i = \mathcal{O}_{{}^a\mathbb{P}^n_{\mathbb{K}}}(d_i)$. In section 3.3.1, we required that $d_i \geq 1$ to fulfill the very ampleness condition for the existence of the resultant. Here we have a similar hypothesis by assuming that $\mu | d_i$ for all $i = 0, \ldots, n$. In this way the resultant $\mathrm{Res}_{V_0,\ldots,V_n}$, denoted ${}^a\mathrm{Res}_{\mathbb{P}^n}$, is well defined. It is also multi-homogeneous, and its degree with respect to the coefficients of the polynomial f_i is $\dfrac{\prod_{j \neq i} d_j}{\Delta}$ (see [Jou91b] 6.3.5(A)).

As for the classical resultant, there are different ways to compute it, the more commonly one is the anisotropic Macaulay's matrices, coming from the anisotropic Koszul complex (see [Jou96]). Anisotropic resultant and classical resultant are closely related, and almost all the classical resultant properties (as Poisson's formula) can be extended to the anisotropic situation. We give the following result which shows how the anisotropic situation reduces to the classical one.

Lemme 3.3.3 ([Jou91b] 6.3.5(B)) *Let $f_0, \ldots, f_n$ be isobar polynomials in ${}^aC$ of respective degree d_i, and let $f_i^\sharp(x_0, \ldots, x_n) = f_i(x_0^{m_0}, \ldots, x_n^{m_n}) \in C$. We have*

$$\mathrm{Res}_{\mathbb{P}^n}(f_0^\sharp, \ldots, f_n^\sharp) = {}^a\mathrm{Res}_{\mathbb{P}^n}(f_0, \ldots, f_n)^\Delta.$$

3.3.3 Toric resultant

The toric (or sparse) resultant has been introduced in [KSZ92], then developed in [GKZ94b]. It takes into account the monomial support of the input polynomials. Thus it is possible to work with polynomials having negative exponents, that is *Laurent polynomials*. Let $f_i(\mathbf{t}) = \sum_{\alpha \in A_i} \mathbf{c}_{\alpha,i}\, \mathbf{t}^\alpha$, $i = 0 \ldots n$, be $n+1$ Laurent polynomials (where $\mathbf{t} = (t_1, \ldots, t_n)$) with supports into fixed sets $A_i \subset \mathbb{Z}^n$. To each finite set $A_i \subset \mathbb{Z}^n$ we can associate a projective toric variety X_{A_i} (not necessary normal, see [GKZ94b] chapter 5) which can be defined as the algebraic closure of the image of the map

$$\sigma_i : \mathbf{t} \in (\mathbb{K}^*)^n \mapsto (\mathbf{t}^\alpha)_{\alpha \in A_i} \in \mathbb{P}^{N_i}$$

where $N_i = |A_i| - 1$. Each $f_i(\mathbf{t})$ can thus be extended globally (by "homogenization") as a linear form on X_{A_i}. In order to apply the previous resultant theory, we consider the projective variety X obtained as the algebraic closure of the image of the map

$$\begin{array}{rcl} \sigma : (\mathbb{K}^*)^n & \to & X_{A_0} \times \ldots \times X_{A_n} \\ \mathbf{t} & \mapsto & (\mathbf{t}^\alpha)_{\alpha \in A_0} \times \ldots \times (\mathbf{t}^\alpha)_{\alpha \in A_n}. \end{array}$$

Denoting by $\mathbb{K}^{A_i}$ the subspace of polynomials with support in A_i, by construction, $X \subset X_{A_0} \times \ldots \times X_{A_n} \subset \mathbb{P}(\mathbb{K}^{A_0 *}) \times \ldots \times \mathbb{P}(\mathbb{K}^{A_n *})$. We then define an invertible sheaf $\mathcal{L}_i$ on X as the inverse image of the sheaf $\mathcal{O}(1)$ from the factor $\mathbb{P}(\mathbb{K}^{A_i *})$, and set $V_i = H^0(X, \mathcal{L}_i)$. If we suppose that each A_i generates $\mathbb{R}^n$ as an affine space and that all A_i together generate $\mathbb{Z}^n$ as an affine lattice, then the resultant $\mathrm{Res}_{V_0,\ldots,V_n}$ is well defined (see [GKZ94b] VIII.1). Its degree with respect to each f_i is the generic number of solutions of the system $\{f_0 = 0, \ldots, f_{i-1} = 0, f_{i+1} = 0, \ldots, f_n = 0\}$. By the BKK theorem [Ber75], this is the *mixed volume* of $\{A_j\}_{j \neq i}$, that is the coefficient of $\prod_{j \neq i} \lambda_j$ in $\mathrm{Vol}\big(\sum_{j \neq i} \lambda_i\, A_i\big) = \mathrm{MV}(\{A_j\}_{j \neq i}) \prod_{j \neq i} \lambda_j + \cdots$ where Vol denotes the usual Euclidean volume.

The methods for constructing a Sylvester-type matrix are based on geometric properties of the supports A_i ([CP93], [CE93], see also the recent papers [D'A02], [Khe03]).

3.3.4 Residual resultant

In many situations coming from practical problems, the polynomial system has commons zeroes which are independent of the parameters, and which we are not interested in. We are going to present here how to compute the resultant in such a situation, under suitable assumptions.

Let $g_1, \ldots, g_r$ be r homogeneous polynomials of degree $k_1 \geq \ldots \geq k_r \geq 1$ in $S = \mathbb{K}[x_0, \ldots, x_n]$, and denote by G the ideal they generate. Being given $n+1$ integers $d_0 \geq \ldots \geq d_n$ greater or equal to k_1, we would like to compute the resultant associated to the system

$$\mathbf{f_c} := \left\{ \begin{array}{rcl} f_0(\mathbf{x}) & = & \sum_{i=1}^{r} h_{i,0}(\mathbf{x})\, g_i(\mathbf{x}) \\ \vdots & & \\ f_n(\mathbf{x}) & = & \sum_{i=1}^{r} h_{i,n}(\mathbf{x})\, g_i(\mathbf{x}) \end{array} \right. \tag{3.5}$$

where $h_{i,j}(\mathbf{x}) = \sum_{|\alpha|=d_j-k_i} c_\alpha^{i,j}\, \mathbf{x}^\alpha$ is a homogeneous polynomial of degree $d_j - k_i$. For this we set $X = \mathbb{P}^n$, and $V_i = H^0(X, \mathcal{G}(d_i))$ for all $i = 0, \ldots, n$, where $\mathcal{G}$ is the coherent ideal sheaf associated to G. The vector space V_i parameterizes all the homogeneous polynomials of degree d_i which are in the saturation of G.

Proposition 3.3.4 ([BEM01]) *Suppose that G is a (projective) local complete intersection, and that $d_n \geq k_r + 1$. Then $\mathrm{Res}_{V_0,\ldots,V_n}$ is well defined and satisfies*

$$\mathrm{Res}_{V_0,\ldots,V_n}(f_0, \ldots, f_n) = 0 \;\Leftrightarrow\; F^{sat} \subsetneq G^{sat} \;\Leftrightarrow\; \mathcal{Z}(F:G) \neq \emptyset.$$

where both ideals F^{sat} and G^{sat} denote respectively the saturations of the ideals $F = (f_0, \ldots, f_n)$ and G.

From a geometrical point of view, the vanishing condition can be stated in the blow-up $\tilde{X}$ of X along the ideal sheaf $\mathcal{G}$, that we denote by $\pi : \tilde{X} \to X$. We have

$$\mathrm{Res}_{V_0,\ldots,V_n}(f_0, \ldots, f_n) = 0 \Leftrightarrow \exists\, x \in \tilde{X} \;:\; \tilde{f}_i(x) = 0 \;\forall i \in \{0, \ldots, n\},$$

where $\tilde{f}_i$ denotes the section $\pi^*(f_i) \in H^0(X, \pi^{-1}\mathcal{G}.\mathcal{O}_{\tilde{X}} \otimes \pi^*(\mathcal{O}_X(d_i)))$, i.e. the virtual transform of f_i by π. In particular, if there exists a point $x \in X \setminus \mathcal{Z}(G)$ such that $f_i(x) = 0$ for all $i = 0, \ldots, n$, then we deduce that $\mathrm{Res}_{V_0,\ldots,V_n}(f_0, \ldots, f_n) = 0$.

The explicit computation of $\mathrm{Res}_{V_0,\ldots,V_n}$ is known in two cases : the case where G is supposed to be a complete intersection [BEM01] (see also [BKM90, CU02, Bus01a]), and the case where G is supposed to be a (projective) local complete intersection codimension 2 arithmetically Cohen-Macaulay (abbreviated ACM) ideal [Bus01a]. Since we are interested in applications to CAGD, we present only the second case which was originally designed for surface implicitization, taking $X = \mathbb{P}^2$ [Bus01b] (point out that a saturated ideal in $\mathbb{P}^2$ of codimension 2 is ACM).

The hypothesis G is ACM of codimension 2 is made to have, using Hilbert-Burch theorem (see [Eis95] theorem 20.15), the following free resolution of G :

$$0 \to \bigoplus_{i=1}^{r-1} S[-l_i] \xrightarrow{\psi} \bigoplus_{i=1}^{r} S[-k_i] \xrightarrow{\gamma=(g_1,\ldots,g_r)} G \to 0, \tag{3.6}$$

with $\sum_{i=1}^{r-1} l_i = \sum_{i=1}^{r} k_i$. It follows that the Eagon-Northcott complex associated to the graded map

$$\bigoplus_{i=1}^{r-1} S[-l_i] \bigoplus_{i=0}^{n} S[-l_i] \xrightarrow{\psi\oplus\phi} \bigoplus_{i=1}^{r} S[-k_i],$$

where ϕ is the matrix $(h_{i,j})_{1\leq i\leq r, 0\leq j\leq n}$ resolves the ideal $(F:G)$, and hence the determinants of some of its graded parts are exactly $\mathrm{Res}_{V_0,\ldots,V_n}$. This result gives a first algorithm to compute $\mathrm{Res}_{V_0,\ldots,V_n}$, and also its multi-degree as an Euler characteristic. A closed formula for all n is difficult to state, but we can do the computation "by hand" in the useful case of $\mathbb{P}^2$, and we obtain that $\mathrm{Res}_{V_0,V_1,V_2}$ is homogeneous in the coefficient of each f_i, $i = 0, 1, 2$, of degree

$$\frac{d_0 d_1 d_2}{d_i} - \frac{\sum_{j=1}^{n-1} l_j^2 - \sum_{j=1}^{n} k_j^2}{2}.$$

Another consequence of this formulation in terms of determinant of complex is the usual "gcd maximal minors" property of resultants :

Théorème 3.3.5 *We denote by $\Delta_{i_1,\ldots,i_r}$ the determinant of the submatrix of the map $\phi\oplus\psi$ corresponding to columns $i_1,\ldots,i_r$, and by $\alpha_{i_1,\ldots,i_r}$ its degree. Then, for any $\nu \geq \sum_{i=0}^{n} d_i - n(k_r+1)$, the morphism*

$$\begin{array}{rccc} \partial_\nu : & \bigoplus_{0\leq i_1<\ldots<i_r\leq n} S_{\nu-\alpha_{i_1,\ldots,i_r}} e_{i_1}\wedge\ldots\wedge e_{i_r} & \longrightarrow & S_\nu \\ & e_{i_1}\wedge\ldots\wedge e_{i_r} & \mapsto & \Delta_{i_1\ldots i_r} \end{array}$$

is surjective if and only if $\mathcal{Z}(F:G)=\emptyset$ (or $F^{sat}=G^{sat}$). In this case, all non-zero maximal minors of size $\dim_{\mathbb{K}}(S_\nu)$ of the matrix ∂_ν is a multiple of $\mathrm{Res}_{V_0,\ldots,V_n}$, and the gcd of all these maximal minors is exactly the residual resultant.

3.4 Bezoutien et calcul du résultant

We have seen that we can compute the resultant in presence of base points (if the base points locus is a complete intersection or a local complete intersection ACM of codimension 2) with similar algorithms to the ones known for the classical resultant.

We have also seen (corollary 3.2.4) that if $X=\mathbb{P}^n$ and $V_0,\ldots,V_n$ are very ample almost everywhere, we can define its resultant $\mathrm{Res}_{V_0,\ldots,V_n}$. Let us see now how to compute a non-zero multiple of it in this general case (see [BEM00] for more details).

Définition 3.4.1 *The Bezoutian $\Theta_{f_0,\ldots,f_n}$ of $f_0,\ldots,f_n\in S$ is the element of $S\otimes_{\mathbb{K}} S$ defined by*

$$\Theta_{f_0,\ldots,f_n}(\mathbf{t},\mathbf{z}) := \begin{vmatrix} f_0(\mathbf{t}) & \theta_1(f_0)(\mathbf{t},\mathbf{z}) & \cdots & \theta_n(f_0)(\mathbf{t},\mathbf{z}) \\ \vdots & \vdots & \vdots & \vdots \\ f_n(\mathbf{t}) & \theta_1(f_n)(\mathbf{t},\mathbf{z}) & \cdots & \theta_n(f_n)(\mathbf{t},\mathbf{z}) \end{vmatrix},$$

where

$$\theta_i(f_j)(\mathbf{t},\mathbf{z}) := \frac{f_j(z_1,\ldots,z_{i-1},t_i,\ldots,t_n) - f_j(z_1,\ldots,z_i,t_{i+1},\ldots,t_n)}{t_i-z_i}.$$

Let $\Theta_{f_0,\ldots,f_n}(\mathbf{t},\mathbf{z}) = \sum \theta_{\alpha\beta}\,\mathbf{t}^\alpha\mathbf{z}^\beta, \theta_{\alpha,\beta}\in\mathbb{K}$. The Bezoutian matrix of $f_0,\ldots,f_n$ is the matrix $B_{f_0,\ldots,f_n} = (\theta_{\alpha\beta})_{\alpha,\beta}$.

The Bezoutian was used by Bézout to construct the resultant of two polynomials in one variable [Béz79]. In the multivariate case, we have the following property.

Théorème 3.4.2 *Assume that each V_i is very ample almost everywhere, then any maximal minor of the Bezoutian matrix $B_{f_0,\ldots,f_n}$ is divisible by the resultant $\mathrm{Res}_{V_0,\ldots,V_m}(f_0,\ldots,f_n)$.*

Remarque 3.4.3 It is possible to use other birational transformations than blowing-up to define the resultant. For instance, in [BEM00] it was proved that this general residual resultant can also be constructed with any birational morphism from a dense open subset of X to a projective space. This point of view generalizes monomial parameterizations used to define the toric resultant to polynomial parameterizations. We refer to [BEM00] for more details and conditions similar to "very ampleness almost everywhere".

Bibliographie

[AJ06] Francois Apéry and Jean-Pierre Jouanolou. *Élimination : le cas d'une variable*. Hermann, collection Méthodes, 2006.

[BE77] David A. Buchsbaum and David Eisenbud. What annihilates a module ? *J. Algebra*, 47(2) :231–243, 1977.

[BEM00] Laurent Busé, Mohamed Elkadi, and Bernard Mourrain. Generalized resultants over unirational algebraic varieties. *J. Symbolic Comput.*, 29(4-5) :515–526, 2000. Symbolic computation in algebra, analysis, and geometry (Berkeley, CA, 1998).

[BEM01] L. Busé, M. Elkadi, and B. Mourrain. Resultant over the residual of a complete intersection. *J. Pure Appl. Algebra*, 164(1-2) :35–57, 2001. Effective methods in algebraic geometry (Bath, 2000).

[BEM03] L. Busé, M. Elkadi, and B. Mourrain. Using projection operators in computer aided geometric design. In *Topics in Algebraic Geometry and Geometric Modeling,*, pages 321–342. Contemporary Mathematics, 2003.

[Ber75] D. N. Bernstein. The number of roots of a system of equations. *Funkcional. Anal. i Prilov zen.*, 9(3) :1–4, 1975.

[Béz79] E. Bézout. *Théorie Générale des Équations Algébriques*. Paris : Ph.-D. Pierres, 1779.

[BKM90] W. Bruns, A. R. Kustin, and M. Miller. The resolution of the generic residual intersection of a complete intersection. *Journal of Algebra*, 128 :214–239, 1990.

[BM07] L. Busé and B. Mourrain. Explicit factors of some iterated resultants and discriminants. To appear in Math. Comp. Preprint at http ://hal.inria.fr/inria-00119287/en/, 2007.

[Bou69] Nicolas Bourbaki. Resultant, Discriminant (état 2). Unpublished appendix of Algebre, Ch. IV, July 1969.

[Bou81] Nicolas Bourbaki. *Éléments de mathématique*. Masson, Paris, 1981. Algèbre. Chapitres 4 à 7. [Algebra. Chapters 4–7], Lecture Notes in Mathematics, 864.

[Bou85] Nicolas Bourbaki. *Éléments de mathématique*. Masson, Paris, 1985. Algèbre commutative. Chapitres 5 à 7. [Commutative algebra. Chapters 5–7], Reprint.

[Bus01a] Laurent Busé. *Étude du résultant sur une variété algébrique*. PhD thesis, Université de Nice Sophia Antipolis, 2001.

[Bus01b] Laurent Busé. Residual resultant over the projective plane and the implicitization problem. In *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation*, pages 48–55 (electronic), New York, 2001. ACM.

[CE93] J. Canny and I. Emiris. An efficient algorithm for the sparse mixed resultant. In G. Cohen, T. Mora, and O. Moreno, editors, *Proc. Intern. Symp. on Applied Algebra, Algebraic Algorithms and Error-Corr. Codes (Puerto Rico)*, volume 673 of *Lect. Notes in Comp. Science*, pages 89–104. Springer, 1993.

[Cha] Marc Chardin. Implicitization using approximation complexes. To appear and math.AC/0503180.

[CLO98] David Cox, John Little, and Donal O'Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1998.

[CP93] J. Canny and P. Pedersen. An algorithm for the Newton resultant. Technical Report 1394, Comp. Science Dept., Cornell University, 1993.

[CT78] P. Cartier and J. Tate. A simple proof of the main theorem of elimination theory in algebraic geometry. *Enseign. Math. (2)*, 24(3-4) :311–317, 1978.

[CU02] Marc Chardin and Bernd Ulrich. Liaison and Castelnuovo-Mumford regularity. *Amer. J. Math.*, 124(6) :1103–1124, 2002.

[D'A02] Carlos D'Andréa. Macaulay style formulas for sparse resultants. *Trans. Amer. Math. Soc.*, 354 :2595–2629, 2002.

[DD01] Carlos D'Andrea and Alicia Dickenstein. Explicit formulas for the multivariate resultant. *J. Pure Appl. Algebra*, 164(1-2) :59–86, 2001. Effective methods in algebraic geometry (Bath, 2000).

[Dem84] Michel Demazure. Une définition constructive du résultant. Preprint of the "Notes Informelles de Calcul Formel", `http://www.gage.polytechnique.fr/notes/1984-1994.html`, may 1984.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[Eis05] David Eisenbud. *The geometry of syzygies*, volume 229 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005. A second course in commutative algebra and algebraic geometry.

[EM07] Mohamed Elkadi and Bernard Mourrain. *Introduction à la résolution des systèmes polynomiaux*, volume 59 of *Mathématiques & Applications (Berlin) [Mathematics & Applications]*. Springer, Berlin, 2007.

[GH94] Phillip Griffiths and Joseph Harris. *Principles of algebraic geometry*. Wiley Classics Library. John Wiley & Sons Inc., New York, 1994. Reprint of the 1978 original.

[GKZ94a] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, resultants, and multidimensional determinants*. Mathematics : Theory & Applications. Birkhäuser Boston Inc., Boston, MA, 1994.

[GKZ94b] I.M. Gelfand, M.M. Kapranov, and A.V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants*. Boston, Birkhäuser, 1994.

[GVL96] Gene H. Golub and Charles F. Van Loan. *Matrix computations*. Johns Hopkins Studies in the Mathematical Sciences. Johns Hopkins University Press, Baltimore, MD, third edition, 1996.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[Har92] Joe Harris. *Algebraic geometry*, volume 133 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. A first course.

[Jou91a] Jean-Pierre Jouanolou. Le formalisme du résultant. *Adv. Math.*, 90(2) :117–263, 1991.

[Jou91b] Jean-Pierre Jouanolou. Le formalisme du résultant. *Adv. Math.*, 90(2) :117–263, 1991.

[Jou96] Jean-Pierre Jouanolou. Résultant anisotrope, compléments et applications. *Electron. J. Combin.*, 3(2) :Research Paper 2, approx. 91 pp. (electronic), 1996. The Foata Festschrift.

[Jou97] Jean-Pierre Jouanolou. Formes d'inertie et résultant : un formulaire. *Adv. Math.*, 126(2) :119–250, 1997.

[Khe03] Amit Khetan. The resultant of an unmixed bivariate system. *J. Symbolic Comput.*, 36(3-4) :425–442, 2003. International Symposium on Symbolic and Algebraic Computation (ISSAC'2002) (Lille).

[KSZ92] M. M. Kapranov, B. Sturmfels, and A. V. Zelevinsky. Chow polytopes and general resultants. *Duke Math. J.*, 67(1) :189–218, 1992.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Mac02] F.S. Macaulay. Some formulae in elimination. *Proc. London Math. Soc.*, 1(33) :3–27, 1902.

[Poi02] Poisson. Mémoire sur l'élimination dans les équations algébriques. *Journal de l'Ecole Polytechnique*, IV :199–203, 1802.

[VdW48] B. L. Van der Waerden. *Modern algebra, Vol. II.* New-York, Frederick Ungar Publishing Co, 1948.

[WZ94] Jerzy Weyman and Andrei Zelevinsky. Determinantal formulas for multigraded resultants. *J. Algebraic Geom.*, 3(4) :569–597, 1994.