Résultant univarié et courbes algébriques planes

Laurent Busé

Résultant univarié et courbes algébriques planes

Laurent Busé,
INRIA Sophia Antipolis Méditerranée,
Laurent.Buse@inria.fr*

Cours de Master de Mathématiques, 2ième année,
Université de Nice, 2006-2008.

Table des matières

*http://www-sop.inria.fr/members/Laurent.Buse/

1 Le résultant de Sylvester

Dans cette première partie, nous développons quelques éléments de la théorie du résultant de deux polynômes univariés. Ils nous seront utiles dans la suite de ces notes. Pour plus de détails, nous renvoyons le lecteur au monographe [Jou91] et au livre [AJ06].

1.1 Définition et premières propriétés

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

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

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. Comme nous allons jouer avec cette matrice tout au long de ces notes, nous donnons une procédure MAPLE permettant de former cette matrice (`var` ci-dessous désigne la variable à éliminer)

```
Sylv:= proc(f,g,m,n,var)
local i,j,M;
        M:=matrix(m+n,m+n);
        for i from 1 to n do
            for j from 1 to m+n do
                M[j,i]:=coeftayl(var^(n-i)*f,var=0,m+n-j);
            od;
        od;
        for i from 1 to m do
            for j from 1 to m+n do
                M[j,i+n]:=coeftayl(var^(m-i)*g,var=0,m+n-j);
            od;
        od;
RETURN(evalm(M));
end:
```

Définition 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 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 *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 1.2 *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 1.2 *Soient* $f, g \in A[X]$ *définis par* (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 1.3 *Soient* $f, g \in A[X]$ *définis par* (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

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

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 (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

$$\{(X^{n-1},0),(X^{n-2},0),\ldots,(X,0),(1,0),(0,X^{m-1}),\ldots,(0,X),(0,1)\} \text{ et } \{X^{m+n-1},\ldots,X,1\} \qquad (3)$$

n'est autre que la matrice de Sylvester $S_{m,n}(f,g)$. La proposition 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 1.4 *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) *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 1.5 *Supposons que A soit un anneau intègre et que $f, g \in A[X]$ soient définis par* (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 1.2 et 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 *Soient $f(X)$ et $g(X)$ définis par (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 1.2 *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). Introduisant un nouvelle indéterminée Y, on définit les polynômes *homogènes* associés à f et à g de degré m et n respectivement comme

$$\begin{cases} F(X,Y) & := & a_0X^m + a_1X^{m-1}Y + \cdots + a_mY^m \\ G(X,Y) & := & b_0X^n + b_1X^{n-1}Y + \cdots + b_nY^n \end{cases} \tag{4}$$

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 1.5 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) 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 de polynômes $\mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_n]$ 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 $\mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_n][X]$, 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".

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).

1.2.1 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 (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

$$\det(M_\phi)\det(M_\theta) = \det(M_{\theta\circ\phi}). \tag{5}$$

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

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

Par conséquent, (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

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

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 1.2. 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

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

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 :

$$\mathrm{Res}_{m,n}(F(aX+b, cX+d), G(aX+b, cX+d)) = (ad-bc)^{mn} \mathrm{Res}_{m,n}(f,g) \tag{6}$$

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 $A := \mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_n, \mathrm{coeff}(u), \mathrm{coeff}(v)]$. On peut également supposer que $m \geq n$ en vertu de 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

$$b_0 F(X,Y) - a_0 X^{m-n} G(X,Y) = Y H(X,Y). \tag{7}$$

D'où le calcul

$$\begin{aligned}
\mathrm{Res}_{md,nd}(b_0 F(u,v), G(u,v)) &= \mathrm{Res}_{md,nd}(vH(u,v), G(u,v)) && \text{par 1.2.4} \\
&= \mathrm{Res}_{d,nd}(v, G(u,v)) \mathrm{Res}_{(m-1)d,nd}(H(u,v), G(u,v)) && \text{par 1.2.3} \\
&= \mathrm{Res}_{d,nd}(v, b_0 u^n) \mathrm{Res}_{(m-1)d,nd}(H(u,v), G(u,v)) && \text{par 1.2.4} \\
&= b_0^d \mathrm{Res}_{d,d}(v,u)^n \mathrm{Res}_{(m-1)d,nd}(H(u,v), G(u,v)) && \text{par 1.2.1 et 1.2.4} \\
&= b_0^d \mathrm{Res}_{d,d}(v,u)^n \mathrm{Res}_{d,d}(u,v)^{(m-1)n} \mathrm{Res}(H,G)^d && \text{par récurrence} \\
&= (-1)^{nd^2} b_0^d \mathrm{Res}(H,G)^d \mathrm{Res}_{d,d}(u,v)^{mn} && \text{par prop. 1.2} \\
&= (-1)^{nd(d+1)} \mathrm{Res}(Y,G)^d \mathrm{Res}(H,G)^d \mathrm{Res}_{d,d}(u,v)^{mn} && \\
&= \mathrm{Res}(YH,G)^d \mathrm{Res}_{d,d}(u,v)^{mn} && \text{par 1.2.3} \\
&= \mathrm{Res}(b_0 F, G)^d \mathrm{Res}_{d,d}(u,v)^{mn} && \text{par 1.2.4 et (7).}
\end{aligned}$$

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

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

et que $\mathrm{Res}(b_0 F, G)^d = b_0^{nd} \mathrm{Res}(F,G)$ 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 :

$$\begin{aligned}
\mathrm{Res}_{m,n}(f,g) &= \mathrm{Res}_{m,n}(f, b_0 \prod_{i=1}^{n}(X-\beta_i)) \\
&= b_0^m \mathrm{Res}_{m,n}(f, \prod_{i=1}^{n}(X-\beta_i)) && \text{par 1.2.1} \\
&= b_0^m \prod_{i=1}^{n} \mathrm{Res}_{m,n}(f, X-\beta_i) && \text{par 1.2.3} \\
&= b_0^m \prod_{i=1}^{n} (-1)^m f(\beta_i) && \text{par l'exemple 1.2} \\
&= a_0^n b_0^m \prod_{j=1}^{n}\prod_{i=1}^{m}(\alpha_i - \beta_j).
\end{aligned}$$

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. $A = \mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_n]$, on gradue l'anneau A en posant

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

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 (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 (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

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

oú $c_{i_0,i_1,\ldots,i_m,j_0,\ldots,j_n} \in \mathbb{Z}$ pour tous les multi-indices $(i_0,i_1,\ldots,i_m,j_0,\ldots,j_n) \in \mathbb{N}^{m+n+2}$. 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.

1.3 La matrice de Bézout

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

$$\left\{ \begin{array}{lcl} f(X) & := & a_0X^n + a_1X^{n-1} + \cdots + a_n \\ g(X) & := & b_0X^n + b_1X^{n-1} + \cdots + b_n \end{array} \right. \tag{8}$$

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 1.6 *On appelle matrice de Bézout en degré n associée au couple de polynômes f,g de $A[X]_{\leq n}$ défini par* (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((f*subs(var=_var,g)-g*subs(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 $A[X,Y]$

$$\begin{pmatrix} X^{n-1} & \cdots & X & 1 \end{pmatrix} \mathrm{Bez}_n(f,g) \begin{pmatrix} Y^{n-1} \\ \vdots \\ Y \\ 1 \end{pmatrix} = \frac{f(X)g(Y)-f(Y)g(X)}{X-Y} = \sum_{i,j=0}^{n-1} c_{i,j}X^iY^j. \tag{9}$$

Proposition 1.7 *Soient f, g définis par* (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 1.8 *Soient f, g définis par* (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 :

$$S_{n,n}(f,g)\left(\begin{array}{c|c} 0 & J_n \\ \hline -J_n & 0 \end{array}\right){}^tS_{n,n}(f,g) = \left(\begin{array}{c|c} 0 & \mathrm{Bez}_n(f,g) \\ \hline -\mathrm{Bez}_n(f,g) & 0 \end{array}\right). \tag{10}$$

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 (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 1.9 *La conjonction des propositions 1.7 et 1.8 donnent directement la propriété de covariance 1.2.5 du résultant.*

Exercice 1.3 *Soient $f(X)$ et $g(X)$ définis par* (8) *tels que A soit un corps et $(f,g) \neq (0,0)$. Alors* $\dim_A(\ker \mathrm{Bez}_n(f,g)) = \deg(\mathrm{pgcd}(f,g))$.

1.4 Le discriminant

Soit A un anneau commutatif et supposons donné un polynôme dans $A[X]$

$$f(X) := a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \tag{11}$$

où n est entier supérieur ou égal à 2. Sa dérivée par rapport à X est le polynôme

$$\frac{\partial f}{\partial X}(X) = na_0X^{n-1} + (n-1)a_1X^{n-2} + \cdots + a_{n-1}$$

(il faut noter que l'on n'a pas forcément l'égalité $\deg(\frac{\partial f}{\partial X}) = \deg(f) - 1$). Introduisant une nouvelle indéterminée Y, nous noterons

$$F(X,Y) := a_0X^n + a_1X^{n-1}Y + \cdots + a_{n-1}XY^{n-1} + a_nY^n \tag{12}$$

le polynôme homogène de degré n associé à f. C'est un polynôme de $A[X,Y]$; ses dérivées partielles sont

$$\frac{\partial F}{\partial X}(X,Y) = na_0X^{n-1} + (n-1)a_1X^{n-2}Y + \cdots + 2a_{n-2}XY^{n-2} + a_{n-1}Y^{n-1},$$
$$\frac{\partial F}{\partial Y}(X,Y) = a_1X^{n-1} + 2a_2X^{n-2}Y + \cdots + (n-1)a_{n-1}XY^{n-2} + na_nY^{n-1}.$$

Proposition 1.10 *Supposons que A soit l'anneau universel des coefficients de F, c'est-à-dire $A = \mathbb{Z}[a_0, \ldots, a_n]$, alors on a l'égalité suivante dans A :*

$$a_0 \mathrm{Res}(F, \frac{\partial F}{\partial Y}) = a_n \mathrm{Res}(F, \frac{\partial F}{\partial X}).$$

Preuve. L'identité d'Euler $nF = X\frac{\partial F}{\partial X} + Y\frac{\partial F}{\partial Y}$ montre que

$$\mathrm{Res}(F, X\frac{\partial F}{\partial X}) = \mathrm{Res}(F, nF - Y\frac{\partial F}{\partial Y}) = \mathrm{Res}(F, -Y\frac{\partial F}{\partial Y})$$

où la dernière égalité provient de la formule des transformations élémentaires 1.2.4. Utilisant la multiplicativité 1.2.3 du résultant on en tire

$$\mathrm{Res}(F, X)\mathrm{Res}(F, \frac{\partial F}{\partial X}) = \mathrm{Res}(F, -Y)\mathrm{Res}(F, \frac{\partial F}{\partial Y}).$$

On conclut alors en notant que

$$\begin{aligned}
&\mathrm{Res}(F, X) = \mathrm{Res}(a_n Y^n, X) = a_n \mathrm{Res}(Y, X)^n = (-1)^n a_n, \\
&\mathrm{Res}(F, -Y) = (-1)^n \mathrm{Res}(F, Y) = (-1)^n \mathrm{Res}(a_0 X^n, Y) = (-1)^n a_0 \mathrm{Res}(X, Y)^n = (-1)^n a_0.
\end{aligned}$$

□

Cette proposition nous montre que, dans le cas où A est l'anneau universel des coefficients de f (ou de F qui a exactement les mêmes coefficients) le polynôme $\mathrm{Res}(F, \frac{\partial F}{\partial X})$ est divisible par a_0. Le quotient est par définition le *discriminant* :

Définition 1.11 *Supposons que A soit l'anneau universel $\mathbb{Z}[a_0, \ldots, a_n]$ des coefficients de f. On définit le discriminant (universel) de f en degré n, aussi appelé le discriminant (universel) de F, comme le quotient*

$$\mathrm{Disc}_n(f) = \mathrm{Disc}(F) := \frac{\mathrm{Res}(F, \frac{\partial F}{\partial X})}{a_0} = \frac{\mathrm{Res}(F, \frac{\partial F}{\partial Y})}{a_m} \in A.$$

Lorsque A est un anneau commutatif quelconque, on définit $\mathrm{Disc}_n(f) = \mathrm{Disc}(F)$ comme l'image du discriminant universel par la spécialisation

$$\mathbb{Z}[a_0, \ldots, a_n] \to A : a_i \mapsto a_i.$$

Sans entrer dans les détails, nous donnons à présent quelques formules, notamment une qui précise la dépendance de n du discriminant.

Proposition 1.12 *Soit A un anneau commutatif. Supposons donné le polynôme $f \in A[X]$ défini par* (11)*, et notons F sont homogénéisé* (12) *en degré n. On a les égalités dans A suivantes :*

$$\begin{aligned}
\mathrm{Res}(F, \frac{\partial F}{\partial X}) &= \mathrm{Res}(\frac{\partial F}{\partial X}, F) = a_0 \mathrm{Disc}(F), \\
\mathrm{Res}(F, \frac{\partial F}{\partial Y}) &= \mathrm{Res}(\frac{\partial F}{\partial Y}, F) = a_n \mathrm{Disc}(F), \\
\mathrm{Res}(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}) &= n^{n-2} \mathrm{Disc}(F), \\
\mathrm{Res}_{n,n-1}(f, \frac{\partial f}{\partial x}) &= \mathrm{Res}_{n-1,n}(\frac{\partial f}{\partial x}, f) = a_0 \mathrm{Disc}_n(f).
\end{aligned}$$

De plus, on a

$$\mathrm{Disc}_{n+1}(f) = (-1)^n a_0^2 \mathrm{Disc}_n(f),$$

et pour tout entier $n' \geq n+2$ on a $\mathrm{Disc}_{n'}(f) = 0$.

Preuve. Par spécialisation, on se ramène à montrer ces formules dans le cas universel, i.e. $A = \mathbb{Z}[a_0, \ldots, a_n]$. Les deux premières formules ont déjà été démontrées ; le fait que l'on puisse permuter les polynômes dont on prend le résultant provient de ce que $n(n-1)$ est toujours un nombre pair (cf. proposition 1.2). La quatrième formule est une déclinaison de la première formule.

La troisième formule s'obtient en calculant de deux façons le résultant de $X\frac{\partial F}{\partial X}$ et $\frac{\partial F}{\partial Y}$. D'une part nous avons

$$\mathrm{Res}(X\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}) = \mathrm{Res}(X, \frac{\partial F}{\partial Y})\mathrm{Res}(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}) = \mathrm{Res}(X, na_nY^{n-1})\mathrm{Res}(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}) = na_n\mathrm{Res}(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}),$$

et d'autre part, en utilisant la formule d'Euler,

$$\mathrm{Res}(X\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}) = \mathrm{Res}(nF - Y\frac{\partial F}{\partial Y}, \frac{\partial F}{\partial Y}) = \mathrm{Res}(nF, \frac{\partial F}{\partial Y}) = n^{n-1}\mathrm{Res}(F, \frac{\partial F}{\partial Y}) = n^{n-1}a_n\mathrm{Disc}(F).$$

Pour montrer la cinquième formule, il faut noter que l'homogénéisé de f en degré $n+1$ est le polynôme $YF(X,Y)$, et on a alors

$$\begin{aligned} a_n\mathrm{Disc}_{n+1}(f) &= a_n\mathrm{Disc}(YF) \\ &= \mathrm{Res}(YF, \frac{\partial(YF)}{\partial Y}) = \mathrm{Res}(YF, F + Y\frac{\partial F}{\partial Y}) \\ &= \mathrm{Res}(Y, F)\mathrm{Res}(F, Y\frac{\partial F}{\partial Y}) \\ &= \mathrm{Res}(Y, F)\mathrm{Res}(F, Y)\mathrm{Res}(F, \frac{\partial F}{\partial Y}) \\ &= (-1)^n\mathrm{Res}(F, Y)^2a_n\mathrm{Disc}(F) = (-1)^n a_0^2 a_n\mathrm{Disc}_n(f), \end{aligned} \tag{13}$$

d'où la formule annoncée en simplifiant par a_n.

Enfin, la dernière formule provient du fait que, $Y^{n'-n}F$ étant l'homgénéisé de f en degré n',

$$\frac{\partial Y^{n'-n}F}{\partial Y} = Y^{n'-n-1}\frac{\partial F}{\partial Y} + Y^{n'-n}\frac{\partial F}{\partial Y}$$

montrant que si $n' - n \geq 2$ alors $Y^{n'-n}F$ et $\frac{\partial Y^{n'-n}F}{\partial Y}$ son tous deux divisible par Y. Cela entraîne, par la proposition 1.4 par exemple, que

$$0 = \mathrm{Res}(Y^{n'-n}F, \frac{\partial Y^{n'-n}F}{\partial Y}) = a_n\mathrm{Disc}(Y^{n'-n}F) = a_n\mathrm{Disc}_{n'}(f).$$

□

Proposition 1.13 *Supposons que A soit un anneau intégre et notons K son corps des fractions. Si $f(X)$ est le polynôme défini par* (11) *tel que $a_0 = 1$, alors les assertions suivantes sont equivalentes :*

(i) $\mathrm{Disc}_n(f) \neq 0$,
(ii) *f et $\frac{\partial f}{\partial X}$ sont premiers entre eux dans $K[X]$,*
(iii) *f n'a pas de racine multiple dans toute extension L de K,*
(iv) *f est sans facteur multiple dans sa décomposition en irréductible dans $K[X]$.*

Preuve. Nous avons $\mathrm{Disc}_n(f) = \mathrm{Res}_{n,n-1}(f, \frac{\partial f}{\partial X})$ et cette proposition découle alors de la proposition 1.4 et de son corollaire 1.5. □

Proposition 1.14 *Supposons que le polynôme f défini par* (11) *dans l'anneau commutatif A soit scindé dans A, c'est-à-dire que $f(X) = a_0\prod_{i=1}^n(X - \alpha_i)$, alors on a*

$$\mathrm{Disc}_n(f) = a_0^{n-2}\prod_{i=1}^n\frac{\partial f}{\partial X}(\alpha_i) = (-1)^{\frac{n(n-1)}{2}}a_0^{2n-2}\prod_{1\leq i<j\leq n}(\alpha_i - \alpha_j)^2.$$

Preuve. Par spécialisation, on se ramène à montrer ces égalités dans le cas universel ; elles des conséquences des formules correspondantes pour le résultant qui ont été vues en 1.2.7. En effet, la première égalité vient de ce que

$$a_0\mathrm{Disc}_n(f) = \mathrm{Res}_{n,n-1}(f, \frac{\partial f}{\partial X}) = a_0^{n-1}\prod_{i=1}^{n}\frac{\partial f}{\partial X}(\alpha_i).$$

Pour la deuxième, il faut noter que $\frac{\partial f}{\partial X} = \sum_{i=1}^{n}\prod_{j\neq i, j=1}^{n}(X-\alpha_j)$, et on obtient alors

$$a_0\mathrm{Disc}_n(f) = a_0^{n-1}\prod_{i=1}^{n}\frac{\partial f}{\partial X}(\alpha_i) = a_0^{n-1}\prod_{i=1}^{n}\prod_{\substack{j=1\\ j\neq i}}^{n}(\alpha_i-\alpha_j) = (-1)^{\frac{n(n-1)}{2}}\prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)^2.$$

□

2 Intersection de deux courbes algébriques planes

Dans cette partie, étant donnés deux polynômes $f(x,y)$ et $g(x,y)$ dans $\mathbb{K}[x,y]$ où $\mathbb{K}$ est un corps algébriquement clos, nous nous intéressons à l'étude et au calcul de 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 $\mathcal{C}_g$.

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

$$F(x,0,t) = c(x-z_1t)^{\mu_1}(x-z_2t)^{\mu_2}\cdots(x-z_st)^{\mu_s}t^{\mu_\infty}, \tag{14}$$

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

$$\mu_\infty + \sum_{i=1}^{s}\mu_i = \deg(F(x,y,t)) = \deg(f(x,y)). \tag{15}$$

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

$$f(x,0) = f_dx^d + f_{d-1}x^{d-1} + \cdots + f_1x + f_0 \in \mathbb{K}[x]$$

(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.

2.1 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 2.1 (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 $\mathbb{K}[x,z]$:

$$\left\{ \begin{array}{rcl} F(x,y,z) & = & a_0(x,z)y^m + a_1(x,z)y^{m-1} + \cdots + a_{m-1}(x,z)y + a_m(x,z) \\ G(x,y,z) & = & b_0(x,z)y^n + b_1(x,z)y^{n-1} + \cdots + b_{n-1}(x,z)y + b_n(x,z) \end{array} \right. \tag{16}$$

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] 1.4. Maintenant, si $(x_0 : y_0 : z_0)$ est un point 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 1.5 ; 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

[3] Il faut ici utiliser un corollaire très classique du lemme de Gauss (voir, par exemple, [Lan84, chap. IV, §2]), que nous rappelons rapidement.

Soit A un anneau factoriel et $K :=$ 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 $a \in K$.

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 $\{P_1,\dots,P_r\} = V(F)\cap V(G)$, ce résultant s'ecrit, d'après le corollaire 1.5,

$$\mathrm{Res}_{m,n}(f,g) = c.(z_{P_1}x - x_{P_1}z)^{m_1}(z_{P_2}x - x_{P_2}z)^{m_2}\cdots(z_{P_r}x - x_{P_r}x)^{m_r} \tag{17}$$

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 2.2 (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 2.1 *Montrer que l'intersection de deux "cercles" d'équations respectives*

$$\alpha_0(x^2+y^2)+\alpha_1x+\alpha_2y+\alpha_3=0,\quad \beta_0(x^2+y^2)+\beta_1x+\beta_2y+\beta_3=0,$$

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.

2.2 Multiplicité d'un point d'intersection

2.2.1 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 2.3 *Soit I un idéal de l'anneau de polynômes $\mathbb{K}[X_1,\dots,X_n]$, avec n un entier strictement positif. Notant classiquement*

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

on a les deux équivalences suivantes :

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

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

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 $P_1,\dots,P_r$. Si $\mathfrak{m}_{P_i}$ désigne l'idéal maximal associé au point P_i, pour $i=1,\dots,r$, 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 $i=1,\dots,n$, de polynômes $U_i(X_i)$ de degré u_i appartenant à l'idéal I. En effectuant, pour tout polynôme $Q\in\mathbb{K}[X_1,\dots,X_n]$ des divisions euclidiennes successives par $U_1(X_1),\dots,U_n(X_n)$, on montre que $\mathbb{K}[X_1,\dots,X_n]/I$ est engendré par les classes des monômes $X_1^{i_1}X_2^{i_2}\dots X_n^{i_n}$ avec $0\le i_j<u_j$ pour tout $j=1,\dots,n$. C'est donc bien un $\mathbb{K}$-espace vectoriel de dimension finie. Inversement, Si $\mathbb{K}[X_1,\dots,X_n]/I$ est un $\mathbb{K}$-espace vectoriel de dimension finie d, pour tout $i=1,\dots,n$, les classes des monômes $1,X_i,X_i^2,\dots,X_i^d$ sont liées. Il existe donc, pour tout $i=1,\dots,n$, un polynôme non nul $U_i(X_i)$ appartenant à l'idéal I. Mais alors $V(I)\subset V(U_1,\dots,U_n)$ 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 2.3 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 $\dim_{\mathbb{K}} \mathbb{K}[X_1, \ldots, X_n]_{\mathfrak{p}}/I_{\mathfrak{p}}$.

2.2.2 Multiplicité d'intersection

Commençons par énoncer un corollaire des considérations du paragraphe 2.2.1 précédent.

Corollaire 2.4 *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 2.3. 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 2.1. □

Définition 2.5 *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 $P \in \mathbb{A}^2$.

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 2.4, points qui sont, rappelons-le, en correspondance avec les idéaux maximaux de $\mathbb{K}[x,y]/(f,g)$.

[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.

Maintenant que nous avons une définition de la multiplicité d'intersection, nous en donnons une caractérisation similaire à (14) et à (17) 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 (16),

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

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 1.4 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 2.1).

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 2.6 *Soient $f(x,y)$ et $g(x,y)$ deux polynômes premiers entre eux. Avec les notations de (16), 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

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

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

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

[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].

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 $i(f,g;P) = i(f, g + hf; P)$.

2.3 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 matrices de Sylvester et de Bézout.

2.3.1 Valeurs et vecteurs propres généralisés

Définition 2.7 *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 2.8 *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 2.9 *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 ${}^tT(x)v = 0$. □

2.3.2 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

$$\left\{ \begin{array}{rcl} f(x,y) & = & a_0(x)y^m + a_1(x)y^{m-1} + \cdots + a_{m-1}(x)y + a_m(x) \\ g(x,y) & = & b_0(x)y^n + b_1(x)y^{n-1} + \cdots + b_{n-1}(x)y + b_n(x) \end{array} \right. \quad (18)$$

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 2.4). 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 (18), 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 pour cette dernière égalité).

Proposition 2.10 *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). 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 :

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

2.3.3 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 2.9, 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 2.9).
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 2.6). Les espaces propres fournissent des bases pour $\ker(B(x_0))$, bases notées $\mathbf{\Lambda}$ dans la proposition 2.10 ; 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 2.10).

2.4 Points singuliers

Dans ce court paragraphe, nous introduisons et caractérisons brièvement la notion de point singulier sur une courbe. Soit un polynôme non constant $f(x,y) \in \mathbb{K}[x,y]$, où $\mathbb{K}$ est un corps de caractéristique nulle, donc infini, et $\mathcal{C} = V(f)$ la courbe algébrique qu'il représente. Soit M un point de $\mathcal{C}$. Quitte à faire un changement linéaire de coordonnées, on peut supposer que ce point est l'origine $M = (0,0)$.

Proposition 2.11 *Les conditions suivantes sont équivalentes :*
(i) *les polynômes $\frac{\partial f}{\partial x}$ et $\frac{\partial f}{\partial y}$ ne s'annulent pas simultanément au point $M = (0,0)$,*
(ii) *$f(x,y)$ est d'ordre 1 au point M,*
(iii) *dans le pinceau de droites de sommet M, toutes, sauf un nombre fini, ont une multiplicité d'intersection en M avec $\mathcal{C}$ égale à 1.*

Preuve. L'équivalence entre (i) et (ii) provient du fait que le polynôme $f(x,y)$ s'écrit

$$f(x,y) = \frac{\partial f}{\partial x}(0,0)x + \frac{\partial f}{\partial y}(0,0)y + r(x,y) \tag{19}$$

où $r(x,y)$ est d'ordre au moins 2 en $(0,0)$. Montrons à présent que (ii) est équivalent à (iii).

Supposons que f soit d'ordre 1. Alors il existe un couple $(a,b) \neq (0,0) \in \mathbb{K}^2$ et $r(x,y)$ d'ordre au moins 2 tels que $f(x,y) = ax + by + r(x,y)$. Les couples projectifs $(\lambda:\mu) \in \mathbb{P}^1_{\mathbb{K}}$ paramètrent le faisceau des droites $\Delta_{\lambda:\mu} = V(\lambda x + \mu y)$ de sommet M. On peut alors calculer la multiplicité d'intersection $i(f,\Delta_{\lambda:\mu};M)$ par un simple calcul de résultant. En effet, si $\mu \neq 0$ la proposition 2.6 implique que

$$i(f,\Delta_{\lambda:\mu};M) = \mathrm{val}_0(\mathrm{Res}_{d,1}(f,\lambda x + \mu y))$$

où d désigne le degré de f en tant que polynôme en la variable y. En vertu des formules 1.2.7 pour le résultant, on a

$$\mathrm{Res}_{d,1}(f,\lambda x+\mu y) = (-1)^d\mu^d f(-\frac{\lambda}{\mu}x) = (-1)^d\mu^d\left(x(a-\frac{\lambda}{\mu}b) + r(x,-\frac{\lambda}{\mu}x)\right)$$

où $\mathrm{val}_0(r(x,-\frac{\lambda}{\mu}x)) \geq 2$ (ou bien $r(x,-\frac{\lambda}{\mu}x) = 0$). On en déduit que si $\mu \neq 0$, alors

$$i(f,\Delta_{\lambda:\mu};M) = 1 \Leftrightarrow (\lambda:\mu) \neq (a:b). \tag{20}$$

Si $\mu = 0$ on montre de la même manière que (20) est vraie en intervertissant le rôle de x et de y (ce qui revient à faire un changement de variable). Ainsi, (20) montre que toute droite de sommet M, exceptée la tangente à $\mathcal{C}$ en M, a une multiplicité d'intersection avec $\mathcal{C}$ égale à 1, et montre donc que (ii) implique (iii).

Inversement, si $\Delta_{\lambda:\mu}$ a une multiplicité d'intersection avec $\mathcal{C}$ égale à 1, alors le calcul de résultant précédent montre que le couple $(a, b) := (\frac{\partial f}{\partial x}(0,0), \frac{\partial f}{\partial y}(0,0))$ est différent du couple nul $(0, 0)$, et donc que (iii) implique (ii). □

Définition 2.12 *Si M vérifie les conditions de la proposition 2.11 ci-dessus, on dit que M est un point* régulier *de $\mathcal{C}$. Sinon, on dit que M est un point* singulier *de $\mathcal{C}$.*

Proposition 2.13 *Soit $f(x, y) \in \mathbb{K}[x, y]$ un polynôme non constant sans facteur multiple (on dit que la courbe $\mathcal{C} = V(f)$ est réduite), alors l'ensemble* $\mathrm{Sing}(\mathcal{C})$ *des points singuliers de $\mathcal{C} = V(f)$ est fini.*

Preuve. Puisque f est non constant, il dépend de x ou de y, disons x. Alors, par le théorème de Bézout et la proposition 1.13, l'ensemble $\mathcal{C} \cap V(\partial f/\partial x)$ est fini[7] dans la clotûre algébrique de $\mathbb{K}$, donc dans $\mathbb{K}$. Puisque $\mathrm{Sing}(\mathcal{C})$ est inclu dans cet ensemble, il est également fini. □

Comme conséquence, on voit que le calcul des points singuliers d'une courbe réduite définie par un polynôme $f(x, y)$ peut se faire en appliquant l'algorithme du paragraphe 2.3.3 aux polynômes f et $\partial f/\partial x$ puis en excluant éventuellement certains points pour lesquels $\partial f/\partial y$ serait non nul.

3 Manipulation des courbes algébriques planes rationnelles

3.1 Courbes planes rationnelles

3.1.1 Définition

Jusqu'ici nous avons représenté les courbes planes comme le lieu des zéros d'un polynôme, c'est-à-dire comme $V(f(x, y)) \subset \mathbb{A}^2$, ou même $V(F(x, y, z)) \subset \mathbb{P}^2$. Il existe cependant une autre façon, bien connue de tous, de représenter les courbes : les paramétrisations. Par exemple, la droite $V(x - y)$ peut être représentée par la paramétrisation $t \in \mathbb{K} \mapsto (t, t) \in \mathbb{K}^2$. Ci-après, $\mathbb{K}$ désigne un corps.

Définition 3.1 *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

$$\phi : \mathbb{A}^1 \to \mathbb{A}^2 : t \mapsto (p(t), q(t)) \tag{21}$$

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 3.2 *Une courbe rationnelle est irréductible.*

[7] noter que l'on utilise ici le fait que la caractéristique de $\mathbb{K}$ est nulle pour déduire que le polynôme $\partial f/\partial x$ est non identiquement nul.

Preuve. Soit $\mathcal{C}$ une courbe rationnelle paramétrée par (21). 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 $\mathcal{C} = V(\ker(\psi))$. □

Exercice 3.1 *Compléter la preuve précédente pour le cas d'une courbe rationnelle projective.*

La première question naturelle est de savoir quelles sont, parmi toutes les courbes algébriques irréductibles, celles qui sont rationnelles. La réponse est "simple" : 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. Nous ne développerons pas ici cette propriété qui relève d'un cours de géométrie algébrique (voir cependant l'exercice 4.5). Mentionnons cependant qu'il existe des algorithmes pour décider si une courbe est rationnelle, et le cas échéant en trouver une paramétrisation.

Cela dit, dans beaucoup de domaines applicatifs, notamment la conception assistée par ordinateur, les courbes que l'on manipule sont toujours rationnelles car toujours représentées sous une forme paramétrée ; cette représentation est en effet plus "souple" que la représentation implicite, bien qu'elle ne soit pas unique (une même courbe peut posséder de nombreuses paramétrisations différentes).

3.1.2 Degré d'une paramétrisation

Supposons donnée un courbe rationnelle $\mathcal{C}$ représentée par une paramétrisation, disons (21). Un invariant important attaché à une telle paramétrisation est son *degré* ; on le note $\deg(\phi)$. 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 $\mathcal{C}$. Afin de poser une définition précise du degré de ϕ, nous aurons besoin de quelques résultats de la théorie des corps, notamment du théorème de Lurröth.

Le théorème de Lurröth. Soit $\mathbb{K}$ un corps et $\mathbb{K}(\xi)$ une extension transcendante simple de $\mathbb{K}$. Par définition, pour tout $\eta \in \mathbb{K}(\xi)$ il existe deux polynômes $f, g \in \mathbb{K}[X]$, avec $g \neq 0$ et $\text{pgcd}(f, g) = 1$, tels que $\eta = f(\xi)/g(\xi) \in \mathbb{K}(\xi)$. On définit alors le *degré* de η par

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

Exercice 3.2 *Montrer que l'entier* $\deg(\eta)$ *ci-dessus est bien défini.*

Lemme 3.3 *Avec les notations précédentes, on a*
(i) $P(X, Y) = g(X)Y - f(X) \in \mathbb{K}[X, Y]$ *est irréductible,*
(ii) $Q(X, Y) := g(X)f(Y) - f(X)g(Y) \in \mathbb{K}[X, Y]$ *n'a de facteurs ni dans* $\mathbb{K}[X]$*, ni dans* $\mathbb{K}[Y]$.

Preuve. (i) : si P était réductible, il devrait alors posséder un facteur linéaire en Y et un facteur dans $\mathbb{K}[X]$. Or cela est impossible puisque l'on a supposé que $\text{pgcd}(f, g) = 1$.

(ii) : puisque P n'a pas de facteur dans $\mathbb{K}[X]$, cela reste vrai pour Q qui n'est autre que $P(X, Y)$ où l'on a substitué Y par $f(Y)/g(Y)$ puis que l'on a multiplié par $g(Y)$ à la puissance le degré de P en Y. On conclut par le fait que $Q(X, Y)$ est symétrique en X et Y. □

Proposition 3.4 *Soit* $\eta \in \mathbb{K}(\xi) \setminus \mathbb{K}$. *Alors,*
(i) $\mathbb{K}(\xi)$ *est une extension algébrique sur* $\mathbb{K}(\eta)$*,*
(ii) η *est transcendant sur* $\mathbb{K}$*,*
(iii) $\deg(\eta) = [\mathbb{K}(\xi) : \mathbb{K}(\eta)]$.

Preuve. Soient $f(X) := \sum_{i=0}^{m} a_i X^i$ et $g(X) := \sum_{i=0}^{n} b_i X^i$ deux polynômes de $\mathbb{K}[X]$ tels que $g \neq 0$, $\text{pgcd}(f,g) = 1$ et $\eta = f(\xi)/g(\xi)$. Considérons le polynôme

$$\gamma(X) := g(X)\eta - f(X) = g(X)\frac{f(\xi)}{g(\xi)} - f(X) \in \mathbb{K}(\eta)[X].$$

Il est clair qu'il est non identiquement nul (puisque $g \neq 0$ il existe un $b_j \in \mathbb{K}$ non nul et donc si $\gamma(X) = 0$ on aurait $b_j\eta - a_j = 0$ et donc $\eta = a_j/b_j \in \mathbb{K}$, contraire aux hypothèses) et que $\gamma(\xi) = 0$. On en déduit que ξ est algébrique sur $\mathbb{K}(\eta)$, et donc (i). De plus, si η était algébrique sur $\mathbb{K}$, alors ξ le serait également, ce qui contredirait le fait que $\mathbb{K}(\xi)$ soit une extension transcendante de $\mathbb{K}$, d'où (ii). Enfin, si l'on montre que $\gamma(X)$ est irréductible dans $\mathbb{K}(\eta)[X]$, alors $\gamma(X)$ sera le polynôme minimal de ξ sur $\mathbb{K}(\eta)$ et on en déduira que $\deg(\eta) = \deg_X(\gamma(X)) = [\mathbb{K}(\xi) : \mathbb{K}(\eta)]$.

Pour le voir, on utilise le lemme 3.3 qui montre que le polynôme $g(X)\eta - f(X)$ est irréductible dans $\mathbb{K}[X,\eta] = \mathbb{K}[\eta][X]$, et donc dans $\mathbb{K}(\eta)[X]$ d'après le lemme de Gauss puisque ce polynôme est primitif (il faut ici voir η comme une variable). □

Faisons le point sur les conséquences des résultats précédents dans le cas où ξ est une indéterminée que nous noterons à présent X. Soit donc $\eta = f(X)/g(X) \in \mathbb{K}(X)$ 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 3.5 (Lurőth) *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 $\mathbb{L} = \mathbb{K}(\eta)$.*

Preuve. Pour tout $\rho \in \mathbb{L} \setminus \mathbb{K}$, nous savons que X est algébrique sur $\mathbb{K}(\rho)$; (en choisissant un tel ρ) il s'en suit que X est algébrique sur $\mathbb{L}$. Soit donc $h_1(Y) := \sum_{i=0}^{n} a_i Y^i \in \mathbb{L}[Y] \subset \mathbb{K}(X)[Y]$ le polynôme minimal (donc unitaire) de X sur $\mathbb{L}$ et notons $b_n(X)$ le plus petit commun multiple des dénominateurs de $a_0, \ldots, a_n$. C'est un polynôme de $\mathbb{K}[X]$ tel que

$$b_n(X)h_1(Y) = \sum_{i=0}^{n} b_i(X)Y^i =: H_1(X,Y) \in \mathbb{K}[X,Y]$$

où $\text{pgcd}(b_0(X), b_1(X), \ldots, b_n(X)) = 1$.

Puisque X n'est pas algébrique sur $\mathbb{K}$, il existe un $i \in \{0, \ldots n\}$ pour lequel $a_i(X)$ dépend de X ; on pose alors

$$\eta(X) := a_i(X) = b_i(X)/b_n(X) = f(X)/g(X) \in \mathbb{L} \subset \mathbb{K}(X) \setminus \mathbb{K}$$

où $f, g \in \mathbb{K}[X]$, $g \neq 0$ et $\text{pgcd}(f,g) = 1$.

Le polynôme $\gamma(Y) := g(Y)\eta - f(Y) \in \mathbb{K}(\eta)[Y] \subset \mathbb{K}(X)[Y]$ est non identiquement nul et tel que $\gamma(X) = 0$. On en déduit que $h_1(Y)$ divise $\gamma(Y)$ dans $\mathbb{L}[Y] \subset \mathbb{K}(X)[Y]$, c'est-à-dire qu'il existe $h_2(Y) \in \mathbb{K}(X)[Y]$ tel que

$$\gamma(Y) = g(Y)\frac{f(X)}{g(X)} - f(Y) = h_1(Y)h_2(Y) \in \mathbb{K}(X)[Y].$$

D'après le lemme de Gauss, il existe donc $H_2(X,Y) \in \mathbb{K}[X,Y]$ tel que

$$Q(X,Y) := g(X)f(Y) - g(Y)f(X) = H_1(X,Y)H_2(X,Y) \in \mathbb{K}[X,Y].$$

Or, $\deg_X(H_1) = \max_i(\deg(b_i)) \geq \max(\deg(f), \deg(g)) = \deg_X(Q)$, ce qui montre que $H_2(X,Y)$ ne dépend que de Y et donc, d'après le lemme 3.3, qu'il est constant : $H_2(X,Y) \in \mathbb{K} \setminus \{0\}$.

Ainsi, quitte à multiplier $H_1(X,Y)$ par une constante non nulle dans $\mathbb{K}$, il vient

$$Q(X,Y) = g(X)f(Y) - g(Y)f(X) = H_1(X,Y) = \sum_{i=0}^{n} b_i(X)Y^i \in \mathbb{K}[X,Y].$$

Par symétrie, on a clairement $\deg_X(Q) = \deg_Y(Q)$. Mais nous avons $\deg(\eta) = \deg_X(Q)$ et $\deg_Y(Q) = \deg_Y(H_1) = n$, donc $\deg(\eta) = n$. Par conséquent

$$[\mathbb{K}(X) : \mathbb{K}(\eta)][\mathbb{K}(\eta) : \mathbb{L}] = [\mathbb{K}(X) : \mathbb{L}] = n = \deg(\eta) = [\mathbb{K}(X) : \mathbb{K}(\eta)]$$

qui implique $[\mathbb{K}(\eta) : \mathbb{L}] = 1$, c'est-à-dire $\mathbb{L} = \mathbb{K}(\eta)$. □

Retour sur le degré d'une paramétrisation. Supposons donc donnée une courbe rationnelle $\mathcal{C}$ paramétrée par

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

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 3.6 *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.

Exercice 3.3 *Montrer que si $\mathbb{K}$ est un corps algébriquement clos, alors* $\deg(\phi)$ *est le nombre de points dans une fibre générique de $\phi_{|\mathcal{C}} : \mathbb{A}^1_{\mathbb{K}} \xrightarrow{\phi} \mathcal{C} \subset \mathbb{A}^2_{\mathbb{K}}$.*

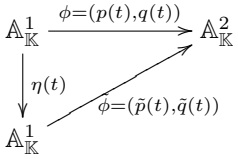
Pour finir ce paragraphe, mentionnons que l'égalité $\deg(\phi) = 1$ n'implique pas que ϕ est une application injective, mais seulement génériquement injective, comme on peut le voir sur la paramétrisation

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

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 $(0, 0)$.

3.1.3 Reparamétrisation propre d'une courbe rationnelle

Un corollaire immédiat du théorème de Lurröth est que toute courbe rationnelle admet une paramétrisation propre (ou birationnelle), c'est-à-dire une paramétrisation de degré 1. En effet, d'après Lurröth, 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

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

Noter que la preuve du théorème de Lurröth ramène la détermination d'une paramétrisation birationnelle à partir d'une paramétrisation quelconque d'une courbe rationnelle à un calcul du polynôme minimal de t sur $\mathbb{K}(p(t), q(t))$.

3.2 Implicitation d'une courbe rationnelle

Supposons donnée une courbe rationnelle $\mathcal{C}$ paramétrée par (21), où $\mathbb{K}$ désigne toujours un corps. L'objectif de ce paragraphe est de montrer comment on peut convertir cette représentation paramétrée de $\mathcal{C}$ en une représentation implicite, c'est-à-dire une équation $f(x, y)$ telle que $V(f) = \mathcal{C}$.

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 3.7 *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 3.8 *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 3.9 *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).

Équation implicite et résultant. On suppose à présent donnée une courbe rationnelle (donc irréductible) $\mathcal{C}$ représentée par une paramétrisation, comme dans (21),

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

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 $\operatorname{pgcd}(p_1, p_2) = \operatorname{pgcd}(q_1, q_2) = 1$. Rappelons que l'idéal $I_{\mathcal{C}}$ n'est autre que le noyau de l'application (voir le lemme 3.2)

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

Théorème 3.10 *Avec les notations précédentes, on a l'égalité entre idéaux de $\mathbb{K}[x,y]$*

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

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 $I_{\mathcal{C}} = (\operatorname{Res}_{m,n}(f,g))$. D'après la proposition 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 $(\operatorname{Res}_{m,n}(f,g)) \subset I_{\mathcal{C}}$. 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 $\operatorname{Res}_{m,n}(f,g) \neq 0$ dans $\mathbb{K}[x,y]$ d'après la proposition 1.4. Pour montrer l'autre inclusion, c'est-à-dire $I_{\mathcal{C}} \subset (\operatorname{Res}_{m,n}(f,g))$, 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 3.8.

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 (voir paragraphe 2.4), on déduit de la proposition 3.9 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

$$\frac{ap_1(t)q_2(t) + bq_1(t)p_2(t) + cp_2(t)q_2(t)}{\mathrm{pgcd}(p_2(t), q_2(t))} = 0 \tag{22}$$

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 3.1.3, 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

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

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 3.2, 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 3.11 *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 3.10 qui s'obtient á l'aide de l'équation polynomiale (22) dont on sait qu'elle est de degré $\deg(\phi)\deg(\mathcal{C})$. □

Application : 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 2.3.3 ; c'est un des avantages indéniables des résultants comme outil pour l'élimination.

3.3 Inversion d'une courbe rationnelle

Dans ce paragraphe, étant donnée une courbe rationnelle représentée par une paramétrisation (21), 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 (21)

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

où $\mathrm{pgcd}(p_1,p_2) = \mathrm{pgcd}(q_1,q_2) = 1$. 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

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

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 (2))

$$ {}^tS_{m,n}(p_1(t) - xp_2(t), q_1(t) - yq_2(t)) \begin{pmatrix} t^{m+n-1} \\ t^{m+n-2} \\ \vdots \\ t \\ 1 \end{pmatrix} = \begin{pmatrix} t^{n-1}(p_1(t) - xp_2(t)) \\ \vdots \\ t(p_1(t) - xp_2(t)) \\ p_1(t) - xp_2(t) \\ t^{m-1}(q_1(t) - yq_2(t)) \\ \vdots \\ t(q_1(t) - yq_2(t)) \\ q_1(t) - yq_2(t) \end{pmatrix}. \tag{23}$$

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,

$$\text{Res}_{m,n}(p_1(t) - xp_2(t), q_1(t) - yq_2(t)) = \sum_{i=1}^{m+n} c_i \Delta_i, \tag{24}$$

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 3.12 *Avec les notations précédentes, on a*

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

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 (24) montre que $\text{pgcd}(\Delta_1, \ldots, \Delta_{m+n})$ 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 (23), 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 $\mathcal{C}$. □

Exercice 3.4 *Réécrire ces deux dernières propositions en utilisant la matrice de Bézout au lieu de la matrice de Sylvester.*

Exemple 3.1 *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 3.10 : 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 3.12, 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,

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

4 Compléments en exercice

4.1 Résultant et déformation

Étant donnés deux entiers $m, n \geq 1$, on considère les polynômes

$$f(X) = a_0 X^m + a_1 X^{m-1} + \cdots + a_m$$
$$g(X) = b_0 X^n + b_1 X^{n-1} + \cdots + b_n$$

en la variable X à coefficients dans l'anneau $A := \mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_n]$. Le but de cet exercice est de montrer la propriété suivante :

Soient $p(X)$ et $q(X)$ deux polynômes non nuls dans $\mathbb{K}[X]$, $\mathbb{K}$ désignant un anneau factoriel, tels que $\deg(p) = m \geq deg(q) = n$. L'ordre de $\mathrm{Res}_{m,n}(f(X)+p(X), g(X)+q(X))$ vu comme polynôme multivarié dans $\mathbb{K}[a_0, \ldots, a_m, b_0, \ldots, b_n]$, c'est-à dire le plus petit des degrés des monômes apparaissant dans son développement, est le degré d'un plus grand diviseur commun de $p(X)$ et de $q(X)$, que nous noterons δ.

1. Montrer que cette propriété est vraie lorsque p et q sont premiers entre eux (i.e. $\delta = 0$).
2. On note $S_{m,n}(p, q)$ la matrice de Sylvester des polynômes p et q en degré (m, n). Montrer que son rang est $m + n - \delta$.
3. On introduit à présent les deux polynômes

$$h(X) = c_0 X^m + c_1 X^{m-1} + \cdots + c_m$$
$$l(X) = d_0 X^n + d_1 X^{n-1} + \cdots + d_n$$

en la variable X à coefficients indéterminés. On pose $R := A[c_0, \ldots, c_m, d_0, \ldots, d_n]$. Pour tout entier $r \in \{1, \ldots, m + n\}$ et toute suite d'entiers $i_1, i_2, \ldots, i_r$ telle que $1 \leq i_1 < \cdots < i_r \leq m + n$, on définit la matrice $M_{i_1,\ldots,i_r}$ comme étant la matrice $S_{m,n}(h, l)$ dans laquelle on a remplacé les colonnes $i_1, \ldots, i_r$ par les colonnes $i_1, \ldots, i_r$ de la matrice $S_{m,n}(f, g)$ respectivement.

   (a) Quelles sont les matrices $M_{1,2,\ldots,n}$, $M_{n+1,\ldots,m+n}$ et $M_{1,2,\ldots,m+n}$?

   (b) Justifier l'égalité suivante dans R :

$$\det(S_{m,n}(f + h, g + l)) = \det(S_{m,n}(h, l)) + \sum_{r=1}^{m+n} \sum_{1 \leq i_1 < \cdots < i_r \leq m+n} \det(M_{i_1,\ldots,i_r}).$$

   (c) En spécialisant $h(X)$ et $l(X)$ en $p(X)$ et $q(X)$ respectivement, en déduire que l'ordre de $\mathrm{Res}_{m,n}(f(X) + p(X), g(X) + q(X))$ est supérieur ou égal à δ (on pourra utiliser la question 2.).
4. Soient a et λ deux nouvelles indéterminées. Montrer que

$$\mathrm{Res}_{m,n}(\lambda a + p(X), a + q(X)) = a^\delta P(a, \lambda) \in \mathbb{K}[a, \lambda]$$

où $P(a, \lambda)$ est un polynôme dans $\mathbb{K}[a, \lambda]$ tel que $P(0, \lambda) \neq 0$ dans $\mathbb{K}[\lambda]$, puis conclure la preuve de la propriété annoncée.

4.2 Résultant et inertie.

Étant donnés deux entiers $m, n \geq 1$, on considère les polynômes

$$f(X) = a_0 X^m + a_1 X^{m-1} + \cdots + a_m$$
$$g(X) = b_0 X^n + b_1 X^{n-1} + \cdots + b_n$$

en la variable X à coefficients indéterminés dans l'anneau $A := \mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_n]$. Dans la suite, (f, g) désigne l'idéal de $A[X]$ engendré par les polynômes f et g ci-dessus. On va s'intéresser à l'idéal de A défini par $\mathcal{I} := (f, g) \cap A$.

1. Justifier le fait que l'idéal $\mathcal{I}$ n'est pas l'idéal nul de A.
2. On considère le morphisme d'anneaux

$$\begin{array}{rcl} A & \xrightarrow{\sigma} & \mathbb{Z}[a_0, \ldots, a_{m-1}, b_0, \ldots, b_{n-1}][X] \\ a_i & \mapsto & a_i \text{ si } 0 \leq i < m \\ b_i & \mapsto & b_i \text{ si } 0 \leq i < n \\ a_m & \mapsto & -a_0 X^m - a_1 X^{m-1} - a_2 X^{m-2} - \cdots - a_{m-1} X \\ b_n & \mapsto & -b_0 X^n - b_1 X^{n-1} - b_2 X^{n-2} - \cdots - b_{n-1} X. \end{array}$$

Montrer que son noyau est l'idéal $\mathcal{I}$. En déduire que $\mathcal{I}$ est un idéal premier de A.

3. Soit $0 \neq P \in \mathcal{I}$ et supposons fixé un entier $j \in \{0, \ldots, m\}$. Montrer que P dépend de a_j. On pourra procéder par l'absurde en s'aidant du morphisme d'anneaux

$$\begin{array}{rcl} A[X] & \stackrel{\phi}{\to} & A[X, X^{-1}] \\ X & \mapsto & X \\ a_i & \mapsto & a_i \text{ pour tout } i \text{ si } i \neq j \\ b_i & \mapsto & b_i \text{ pour tout } i \\ a_j & \mapsto & a_j - X^{-m+j} f(X) \end{array}$$

dont on vérifiera qu'il laisse invariant $g(X)$ et envoie $f(X)$ sur 0.

4. Déduire de la question précédente que si $0 \neq P \in \mathcal{I}$ alors P dépend de $a_0, \ldots, a_m$ et de $b_0, \ldots, b_n$ sans exception.
5. Choisissons un quelconque des $a_0, \ldots, a_m$ ou $b_0, \ldots, b_n$ et notons le u. On note A' l'anneau A auquel on enlève u, c'est-à-dire $A = A'[u]$.
   (a) Pour tout $P \in \mathcal{I}$ on note $\deg_u(P)$ le degré de P en tant que polynôme en la variable u (à coefficients dans A'). Montrer que l'entier

   $$s := \inf\{\deg_u(P) \text{ où } 0 \neq P \in \mathcal{I}\}$$

   est supérieur ou égal à 1.
   (b) En déduire qu'il existe un polynôme irréductible, que l'on notera $R \in A$, tel que $\deg_u(R) = s$.
   (c) Montrer qu'alors R divise tout $P \in \mathcal{I}$ et donc que $\mathcal{I}$ est un idéal principal. Justifier que $\mathcal{I}$ n'a que deux générateurs possibles : R et $-R$.
6. On va maintenant montrer que $\mathrm{Res}_{m,n}(f, g) \in A$ est un générateur de $\mathcal{I}$. Soit $0 \neq P \in \mathcal{I}$; il existe donc des polynômes $h_1(X), h_2(X) \in A[X]$ tels que $P = h_1(X)f(X) + h_2(X)g(X) \in A$.
   (a) Justifier le fait que $h_1(X)$ et $h_2(X)$ sont des polynômes non nuls dont nous noterons $d_1 \geq 0$ et $d_2 \geq 0$ les degrés respectifs. On pose également $d := \max(d_1, d_2) \geq 0$.
   (b) Montrer que $\mathrm{Res}_{m,n+d}(f, h_2 g) \in A$ est non nul et que $\mathrm{Res}_{m,n}(f, g)$ le divise.
   (c) En déduire que $\mathrm{Res}_{m,n}(f, g)$ divise P.
   (d) Conclure que $\mathrm{Res}_{m,n}(f, g)$ est un polynôme irréductible de A, générateur de l'idéal $\mathcal{I}$ appelé idéal des *formes d'inerties de degré zéro* de f et de g.
7. Une autre façon de voir que $\mathrm{Res}_{m,n}(f, g)$ est un générateur de $\mathcal{I}$ est de montrer qu'il est irréductible dans A.
   (a) Justifier cette assertion.
   (b) On procède par récurrence sur l'entier $r = m + n$. Montrer que $\mathrm{Res}_{m,n}(f, g)$ est irréductible si $r = 2$ (rappelons que l'on a supposé que $m, n \geq 1$).
   (c) Fixons à présent un entier $r \geq 3$ et supposons que $\mathrm{Res}_{m,n}(f, g)$ est irréductible si $2 \leq m+n < r$. En observant séparément les deux spécialisation de $\mathrm{Res}_{m,n}(f, g)$ envoyant a_0 sur 0 puis b_0 sur 0, montrer que $\mathrm{Res}_{m,n}(f, g)$ est bien irréductible (on pensera à utiliser la propriété de bi-homogénéité du résultant en les $a_0, \ldots, a_m$ d'une part, et en les $b_0, \ldots, b_n$ d'autre part).

4.3 Quasi-homogénéité généralisée du résultant

Étant donnés deux entiers $m, n \geq 1$, on considère les polynômes

$$f(X) = a_0 X^m + a_1 X^{m-1} + \cdots + a_m$$
$$g(X) = b_0 X^n + b_1 X^{n-1} + \cdots + b_n$$

en la variable X à coefficients dans l'anneau $A := \mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_n]$. Le but de cette partie est de montrer la propriété suivante :

Soient r et s deux entiers, $0 \leq r \leq m$, $0 \leq s \leq n$. Si l'on gradue l'anneau A en posant

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

alors le degré de n'importe quel terme de $\mathrm{Res}_{m,n}(f,g) \in A$ *est supérieur ou égal à* rs *(resp.* rs*).*

1. Expliquer comment on déduit le cas $\deg(a_i) = \max(0, r-m+i)$, $\deg(b_j) = \max(0, s-n+j)$, du cas $\deg(a_i) = \max(0, r-i)$, $\deg(b_j) = \max(0, s-j)$. Dans toute la suite on supposera que l'on est dans ce dernier cas.
2. Justifier que la propriété annoncée est vraie si $(r = 0, s = 0)$ et si $(r = m, s = n)$. Nous supposerons désormais que nous ne sommes pas dans un de ces deux cas.
3. Introduisant une nouvelle variable t, on considère les polynômes

$$\begin{aligned} \overline{f}(X) &:= a_0 t^r X^m + \cdots + a_{r-1} t X^{m-r+1} + a_r X^{m-r} + \cdots + a_m, \\ \overline{g}(X) &:= b_0 t^s X^n + \cdots + b_{s-1} t X^{n-s+1} + b_s X^{n-s} + \cdots + b_n. \end{aligned}$$

   Soit k le plus grand entier tel que

$$\mathrm{Res}_{m,n}(\overline{f}, \overline{g}) = t^k R_1(a_i, b_j, t) \text{ dans } A[t]$$

   où $R_1(a_i, b_j, 0) \neq 0$. Montrer que, dans $A[X,t]$,

$$R_1(a_0, \ldots, a_{m-1}, a_m - \overline{f}, b_0, \ldots, b_{n-1}, b_n - \overline{g}, t) = 0$$

   et en déduire que $R_1(a_i, b_j, t) \in (\overline{f}, \overline{g}) \cap A[t] \subset A[X,t]$.
4. Déduire de la question précédente que $\mathrm{Res}_{m-r,n-s}(f_{m-r}, g_{n-s})$ divise $R_1(a_i, b_j, 0)$ dans A où

$$f_{m-r}(X) := a_r X^{m-r} + \cdots + a_m \quad \text{et} \quad g_{n-s}(X) := b_s X^{n-s} + \cdots + b_n.$$

5. On considère à présent les polynômes

$$\begin{aligned} \tilde{f}(X) &:= a_0 X^m + \cdots + a_r X^{m-r} + a_{r+1} t X^{m-r-1} + \cdots + a_m t^{m-r}, \\ \tilde{g}(X) &:= b_0 X^n + \cdots + b_s X^{n-s} + b_{s+1} t X^{n-s-1} + \cdots + b_n t^{n-s}. \end{aligned}$$

   et on note l le plus grand entier tel que

$$\mathrm{Res}_{m,n}(\tilde{f}, \tilde{g}) = t^l R_2(a_i, b_j, t) \text{ dans } A[t]$$

   où $R_2(a_i, b_j, 0) \neq 0$. Montrer comme précédemment que $\mathrm{Res}_{r,s}(f_r^\star, g_s^\star)$ divise $R_2(a_i, b_j, 0)$ dans A où

$$f_r^\star(X) := a_r X^r + \cdots + a_0 \quad \text{et} \quad g_s^\star(X) := b_s X^s + \cdots + b_0.$$

   Pour cela, on pourra tout d'abord montrer que $\mathrm{Res}(\tilde{f}, \tilde{g}) = \mathrm{Res}(f^\star, g^\star)$ où

$$\begin{aligned} f^\star(X) &:= a_0 + \cdots + a_r X^r + a_{r+1} t X^{r+1} + \cdots + a_m t^{m-r} X^m, \\ g^\star(X) &:= b_0 + \cdots + b_s X^s + b_{s+1} t X^{s+1} + \cdots + b_n t^{n-s} X^n. \end{aligned}$$

6. Montrer que $t^{rs}\mathrm{Res}(\tilde{f}, \tilde{g}) = t^{(m-r)(n-s)}\mathrm{Res}(\overline{f}, \overline{g})$ dans $A[t]$ (on pourra tout d'abord calculer $t^{m-r}\overline{f}(X/t)$ et $t^{n-s}\overline{g}(X/t)$). En déduire que $R_1(a_i, b_j, 0) = R_2(a_i, b_j, 0)$.
7. Montrer que $\mathrm{Res}_{m-r,n-s}(f_{m-r}, g_{n-s})$ et $\mathrm{Res}_{r,s}(f_r^\star, g_s^\star)$ sont premiers entre eux dans A. En déduire l'égalité

$$R_1(a_i, b_j, 0) = c\,\mathrm{Res}_{m-r,n-s}(f_{m-r}, g_{n-s})\mathrm{Res}_{r,s}(f_r^\star, g_s^\star) \text{ dans } A$$

   où $c \in \mathbb{Z} \setminus \{0\}$.
8. Justifier que $\mathrm{Res}_{r,s}(f_r^\star, g_s^\star)$ est (quasi-)homogène de degré rs et que $\mathrm{Res}_{m-r,n-s}(f_{m-r}, g_{n-s})$ est (quasi-)homogène de degré nul. En déduire que $R_1(a_i, b_j, 0)$ est (quasi-)homogène de degré rs, puis que $k = rs$, ce qui démontre la propriété annoncée.
9. Montrer que $c = (-1)^{(n-s)r}$ (on pourra pour cela considérer, par exemple, la spécialisation $f \mapsto a_0 X^m + a_m$ et $g \mapsto b_s X^{n-s}$) et justifier que *la somme des termes de degré* rs *de* $\mathrm{Res}_{m,n}(f,g)$ *vaut exactement* $(-1)^{(n-s)r}\mathrm{Res}_{r,s}(f_r^\star, g_s^\star)\mathrm{Res}_{m-r,n-r}(f_{m-r}, g_{n-s}) \in A$.

4.4 Multiplicité d'une courbe algébrique plane en un point

Soit $\mathbb{K}$ un corps algébriquement clos et $f(x,y) \in \mathbb{K}[x,y]$ un polynôme non constant définissant la courbe algébrique plane $\mathcal{C} := V(f(x,y))$ dans le plan. Étant donné un point P du plan, le but de cet exercice est de définir la notion de multiplicité du point P pour la courbe $\mathcal{C}$, puis d'en donner une propriété importante. Pour la suite, on pose

$$f(x,y) = a_0(x)y^m + a_1(x)y^{m-1} + \cdots + a_{m-1}(x)y + a_m(x)$$

où $a_i(x) \in \mathbb{K}[x]$ pour tout $i = 0, \ldots, m$, $a_0(x) \neq 0$ et, introduisant une nouvelle indéterminée $\overline{y}$, on définit le polynôme

$$F(x,y,\overline{y}) := a_0(x)y^m + a_1(x)y^{m-1}\overline{y} + \cdots + a_{m-1}(x)y\overline{y}^{m-1} + a_m(x)\overline{y}^m$$

qui n'est autre que l'homogénéisé de $f(x,y)$ par rapport à y en degré m. Nous supposerons en outre que $m \geq 1$ et que $P = (0,0)$, hypothèses auxquelles on peut se ramener par un simple changement linéaire de coordonnées.

1. On note $\Delta_{\lambda:\mu}$ la droite du plan qui passe par le point P d'équation $\mu y - \lambda x = 0$. Montrer que
$$\mathrm{Res}_{m,1}(f(x,y), \mu y - \lambda x) = (-1)^m F(x, \lambda x, \mu).$$
2. Déduire que $i(\mathcal{C}, \Delta_{\lambda:\mu}; P) \in \mathbb{N}$ est constant pour tout les couples $(\lambda : \mu)$ sauf éventuellement un nombre fini. On définit la multiplicité de $\mathcal{C}$ en P, et on la note $\mathfrak{m}_P(\mathcal{C})$, le nombre
$$\mathfrak{m}_P(\mathcal{C}) := \inf_{(\lambda:\mu)\in\mathbb{P}^1} i(\mathcal{C}, \Delta_{\lambda:\mu}; P).$$
3. Montrer que $\mathfrak{m}_P(\mathcal{C}) = 0$ si et seulement si $P \notin \mathcal{C}$.
4. Montrer que $\mathfrak{m}_P(\mathcal{C}) = 1$ si et seulement si $P \in \mathcal{C}$ est un point régulier de $\mathcal{C}$.
5. Expliquer pourquoi on peut supposer $\mathfrak{m}_P(\mathcal{C}) \leq m$, quitte à faire un changement linéaire de coordonnées.

À partir de maintenant on suppose donné un autre polynôme $g(x,y) \in \mathbb{K}[x,y]$ non constant définissant la courbe algébrique plane $\mathcal{D} := V(g(x,y))$ dans le plan. Comme pour $f(x,y)$, on pose

$$g(x,y) = b_0(x)y^n + b_1(x)y^{n-1} + \cdots + b_{n-1}(x)y + b_n(x)$$

où $b_i(x) \in \mathbb{K}[x]$ pour tout $i = 0, \ldots, n$, $b_0(x) \neq 0$ et, introduisant une nouvelle indéterminée $\overline{y}$, on définit le polynôme

$$G(x,y,\overline{y}) := b_0(x)y^n + b_1(x)y^{n-1}\overline{y} + \cdots + b_{n-1}(x)y\overline{y}^{n-1} + b_d(x)\overline{y}^n$$

qui n'est autre que l'homogénéisé de $g(x,y)$ par rapport à y en degré n. Nous supposerons également que $n \geq 1$ (cas auquel on peut se ramener par un simple changement linéaire de coordonnées). Nous allons montrer l'inégalité suivante :

$$i(\mathcal{C}, \mathcal{D}; P) \geq \mathfrak{m}_P(\mathcal{C})\mathfrak{m}_P(\mathcal{D}). \tag{25}$$

1. Montrer que (25) est vrai si $\mathfrak{m}_P(\mathcal{C}) = 0$ ou $\mathfrak{m}_P(\mathcal{D}) = 0$.
2. Montrer que (25) est vrai si $\mathfrak{m}_P(\mathcal{C}) = \mathfrak{m}_P(\mathcal{D}) = 1$.
3. Montrer que
$$\deg(a_i(x)) \geq \max(0, \mathfrak{m}_P(\mathcal{C}) - m + i) \text{ pour tout } i = 0, \ldots, m$$
et que
$$\deg(b_j(x)) \geq \max(0, \mathfrak{m}_P(\mathcal{D}) - n + j) \text{ pour tout } j = 0, \ldots, n.$$
4. Déduire l'inégalité (25) de la question précédente en utilisant le résultat de l'exercie 4.3.
5. Pour finir, montrer que l'inégalité (25) est une égalité si et seulement si les courbes $\mathcal{C}$ et $\mathcal{D}$ n'ont pas de tangente commune en P (avec les notations de l'exercice 4.3, on remarquera que $f_r^\star$, respectivement $g_s^\star$, est homogène en x, y de degré r, respectivement s).

4.5 Points singuliers et rationnalité d'une courbe algébrique plane

L'objectif de cet exercice est de montrer le résultat suivant :

Une courbe irréductible de $\mathbb{P}^2(\mathbb{C})$ de degré $d \geq 1$ possède au plus $\frac{(d-1)(d-2)}{2}$ points singuliers disctincts. De plus une telle courbe possédant (au moins) $\frac{(d-1)(d-2)}{2}$ points singuliers disctincts est rationnelle.

On rappelle que les courbes de degré d dans $\mathbb{P}^2(\mathbb{C})$ forment un espace projectif de dimension $\frac{d(d+3)}{2}$ par la correspondance

$$\sum_{0\leq i,j,i+j\leq d} a_{i,j}X^iY^jZ^{d-i-j} \leftrightarrow (a_{0,0} : \cdots : a_{i,j} : \cdots) \in \mathbb{P}^{\frac{d(d+3)}{2}}.$$

Par exemple, l'ensemble des courbes de degré d passant par un point donné correspond à un espace linéaire de dimension $\frac{d(d+3)}{2} - 1$, i.e. un hyperplan, dans $\mathbb{P}^{\frac{d(d+3)}{2}}$.

1. Montrer le résultat annoncé pour $d = 1$.
2. Montrer le résultat annoncé pour $d = 2$. Pour la rationnalité, on pourra choisir un point régulier P_0 sur $\mathcal{C}$ puis définir une paramétrisation de $\mathcal{C}$ en considérant l'intersection de $\mathcal{C}$ avec les droites du pinceau de droites de sommet P_0 (on pensera à simplifier les calculs en ramenant P_0 à l'origine par changement linéaire de coordonnées).
3. On suppose à présent donnée une courbe $\mathcal{C}$ de degré $d \geq 3$ possédant $\frac{(d-1)(d-2)}{2}$ points singuliers distincts que l'on note $S_1, \ldots, S_{\frac{(d-1)(d-2)}{2}}$. Choisissant $d-3$ points réguliers distincts sur $\mathcal{C}$, que l'on note $R_1, \ldots, R_{d-3}$, on considère le système linéaire $\mathcal{F}$ des courbes de degré $d-2$ passant par les points $S_1, \ldots, S_{\frac{(d-1)(d-2)}{2}}$, $R_1, \ldots, R_{d-3}$.
   (a) Montrer que $\mathcal{F}$ est de dimension au moins 1.
   (b) Supposons que $\mathcal{F}$ soit de dimension ≥ 2. Déduire que si P et P' sont deux points sur $\mathcal{C}$ qui sont distincts des points réguliers et singuliers déjà choisis sur $\mathcal{C}$ et distincts entre eux, alors il existe une courbe $\mathcal{D}$ de $\mathcal{F}$ qui passe par les points P et P'.
   (c) Après avoir justifier que $\mathcal{C}$ et $\mathcal{D}$ ont une intersection finie que l'on identifiera, utiliser le théorème de Bézout et la formule (25) pour obtenir une contradiction et ainsi conclure que $\mathcal{F}$ est de dimension 1.
   (d) Expliquer pourquoi le raisonnement précédent permet de montrer que $\mathcal{C}$ ne saurait avoir plus de $\frac{(d-1)(d-2)}{2}$ points singuliers distincts, et que si c'est le cas ces points sont doubles, i.e. de multiplicité 2.
4. Soit $\mathcal{B}$ une courbe de $\mathcal{F}$. On note $F(X,Y,Z) = 0$, resp. $G(X,Y,Z) = 0$, une équation implicite de $\mathcal{C}$, resp. $\mathcal{B}$. Justifier que, quitte à faire un changement de coordonnées projectives de $\mathbb{P}^2$, on peut supposer que $F, G \in \mathbb{C}[X,Y,T]$ sont de degré d et $d-2$ respectivement comme polynômes en Y.
5. Soit $\mathcal{B}'$ une courbe de $\mathcal{F}$ distincte de $\mathcal{B}$ et soit $G'(X,Y,Z) = 0$ une équation implicite de $\mathcal{B}'$. Montrer que toute courbe de $\mathcal{F}$ possède une équation de la forme
$$uG(X,Y,Z) + vG'(X,Y,Z) = 0$$
où $(u : v) \in \mathbb{P}^1(\mathbb{C})$.
6. Soit $R := \mathrm{Res}_{d,d-2}(F, uG + vG') \in \mathbb{C}[X,Z,u,v]$. Montrer que R est non nul, homogène de degré $d(d-2)$ en (X,Z) et homogène de degré d en (u,v).
7. Montrer que R est divisible par un polynôme $Q \in \mathbb{C}[X,Z]$ homogène de degré $d(d-2)-1$ associé à tous les points S_i et R_j. En déduire que le quotient de R par Q dans $\mathbb{C}[X,Z,u,v]$ est un polynôme de la forme
$$H(X,Z,u,v) := c(u,v)Z - a(u,v)X \in \mathbb{C}[X,Z,u,v]$$
où c et a sont homogènes de degré d dans $\mathbb{C}[u,v]$. Montrer également que H est irréductible.
8. De même, montrer que le quotient de $R' := \mathrm{Res}_{d,d-2}(F, uG + vG') \in \mathbb{C}[Y,Z,u,v]$ par un certain polynôme associé aux points S_i et R_j est de la forme
$$H'(Y,Z,u,v) := c'(u,v)Z - b(u,v)Y \in \mathbb{C}[Y,Z,u,v]$$
où c' et b sont homogènes de degré d dans $\mathbb{C}[u,v]$.

9. Montrer que $c(u,v)$ et $c'(u,v)$ diffèrent d'une constante multiplicative non nulle $\lambda \in \mathbb{C} : c(u,v) = \lambda c'(u,v)$.
10. Conclure en montrant que l'application rationnelle

$$h : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^2(\mathbb{C}) : (u : v) \mapsto (a(u,v) : \lambda b(u,v) : c(u,v))$$

est une paramétrisation de la courbe $\mathcal{C}$.

Références

[AJ06] François Apéry and Jean-Pierre Jouanolou. *Élimination : le cas d'une variable*. Hermann, collection Méthodes, 2006.

[Bou81] Nicolas Bourbaki. *Éléments de mathématique*. Masson, Paris, 1981. Algèbre. Chapitres 4 à 7. [Algebra. Chapters 4–7], Lecture Notes in Mathematics, 864.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[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.

[Jou91] Jean-Pierre Jouanolou. Le formalisme du résultant. *Adv. Math.*, 90(2) :117–263, 1991.

[Lan84] Serge Lang. *Algebra*. Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, second edition, 1984.