Travail d'Étude et de Recherche

Année 2021

Résultant de deux polynômes et applications

Naïs LÉVÊQUE

Encadrante : Catherine LABEYE-VOISIN

Table des matières

Introduction

Nous aborderons la théorie du résultant et nous l'appliquerons à l'étude de l'intersection de deux courbes planes définies par des équations polynomiales.
Nous définirons le résultant de deux polynômes de $A[T]$ où A est un anneau commutatif unitaire et intègre et nous énoncerons quelques-unes de ses propriétés fondamentales.
Nous montrerons le théorème de Bézout faible qui donne une majoration du nombre de points d'intersection de deux courbes planes par le produit des degrés totaux des deux polynômes qui les définissent.
Ensuite, nous étudierons différents types d'intersection et leur relation avec le résultant de ces deux polynômes. Nous verrons aussi l'intérêt de travailler sur un corps algébriquement clos, ce que nous ferons par la suite, et de prendre en compte les points à l'infini.
À chaque courbe plane, nous associerons donc une courbe du plan projectif, ce qui permet de compléter la courbe affine initiale par ses points à l'infini.
Nous utiliserons une carte adaptée et des coordonnées adaptées pour compter le nombre de points d'intersection de deux courbes projectives planes, en pondérant par la multiplicité qui apparaît dans le résultant des deux polynômes S et T qui définissent ces courbes dans les coordonnées adaptées.
Nous montrerons que ce nombre est égal au produit des degrés totaux de S et T.

I - Généralités sur le résultant

Soit A un anneau commutatif unitaire intègre, et soit $K = Fr(A)$ son corps des fractions.

I.A Définition

On considère $P, Q \in A[X]$ et on note $P = a_0X^p + \cdots + a_p$ et $Q = b_0X^q + \cdots + b_q$.
On définit, $\forall n \in \mathbb{N}, A_n[X]$ le A sous-module libre de $A[X]$ composé des polynômes de degrés strictement inférieurs à n, qui a pour base $\mathcal{B}_n = (X^{n-1}, \cdots, 1)$.
De même, $\forall n, m \in \mathbb{N}$, on note $\mathcal{B}_{n,m}$ la base du A-module libre $A_n[X] \times A_m[X]$ et alors on a : $\mathcal{B}_{n,m} = ((X^{n-1}, 0), \cdots, (X, 0), (1, 0), (0, X^{m-1}), \cdots, (0, X), (0, 1))$.
On considère alors le morphisme de A-modules libres :

$$\begin{aligned} \Phi : A_q[X] \times A_p[X] &\longrightarrow A_{p+q}[X] \\ (U, V) &\longmapsto UP + VQ \end{aligned}$$

Définition : Le **résultant de P et Q en degré (p, q)**, noté $res(P, Q)$ est le déterminant de la matrice de Φ dans les bases $\mathcal{B}_{q,p}$ et $\mathcal{B}_{p+q}$:

$$res(P, Q) = \det \mathcal{M}(\Phi, \mathcal{B}_{p+q}, \mathcal{B}_{q,p}) \in A$$

$$\text{avec } \mathcal{M}(\Phi, \mathcal{B}_{p+q}, \mathcal{B}_{q,p}) = \begin{pmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & \ddots & & \vdots & b_1 & \ddots & & \vdots \\ \vdots & & \ddots & 0 & \vdots & & \ddots & 0 \\ \vdots & & & a_0 & \vdots & & & b_0 \\ a_p & & & a_1 & b_q & & & b_1 \\ 0 & \ddots & & \vdots & 0 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & a_p & 0 & \cdots & 0 & b_q \end{pmatrix}.$$

Notation : Dans ce qui suit, on va considérer des polynômes P et Q à plusieurs indéterminées $X_1, \cdots, X_n$ et on notera $res_{X_i}(P, Q)$ le résultant des polynômes P et Q vus comme polynômes en X_i.

I.B Premières propriétés du résultant

Proposition 1 : Soient $P, Q \in A[X]$: $res(P,Q) = (-1)^{pq} res(Q,P)$.

Preuve : Si on note C_i la $i$ème colonne de la matrice dont le déterminant est $res(P,Q)$, alors on cherche à transformer $(C_1, \cdots, C_q, C_{q+1}, \cdots, C_{p+q})$ en $(C_{q+1}, \cdots, C_{q+p}, C_1, \cdots, C_q)$ par produits de transpositions.
Dans un premier temps, on envoie C_{q+1} à la position 1 par le biais de q transpositions. On réitère l'opération sur la colonne C_{q+2} envoyée à la position 2 par le produit de q transpositions. Finalement, on peut passer de l'une à l'autre des matrices par le produit de pq transpositions que l'on note τ_j pour j entre 1 et pq, et alors :

$$\begin{aligned} res(P,Q) &= \det(C_1, \cdots, C_q, C_{q+1}, \cdots, C_{p+q}) \\ &= \det(\tau_1 \cdots \tau_{pq}(C_{q+1}, \cdots, C_{q+p}, C_1, \cdots, C_q)) \\ &= (-1)^{pq} \det(C_{q+1}, \cdots, C_{q+p}, C_1, \cdots, C_q) \\ &= (-1)^{pq} res(Q,P). \end{aligned}$$

Lemme 2 : Soit $\psi : A^r \longrightarrow A^r$ un morphisme de A-modules, $\mathcal{B}, \mathcal{B}'$ deux bases de A^r. On a l'équivalence :

$$\psi \text{ injective} \Leftrightarrow \det \mathcal{M}(\psi, \mathcal{B}, \mathcal{B}') \neq 0.$$

Preuve : On note Ω la matrice $\mathcal{M}(\psi, \mathcal{B}, \mathcal{B}')$.
Montrons que ψ est injective si et seulement si $\det(\Omega) \neq 0$.
On note C_i la colonne i de Ω.
$\Leftarrow$ Soit $x \in A^r$ tel que $\psi(x) = 0$. Par définition de $\mathcal{M}(\psi, \mathcal{B}, \mathcal{B}')$, on a $\psi(x) = \Omega x$ et donc on a $\Omega x = 0$ et alors en appliquant : ${}^t\mathrm{com}(\Omega)\Omega = \det(\Omega).I_r$ à x, on a :
$\det(\Omega).x = {}^t\mathrm{com}(\Omega)\Omega.x = 0$.
Comme $\det(\Omega)$ est supposé non nul, on a alors $x = 0$ par intégrité de A, d'où l'injectivité de ψ.
$\Rightarrow$ On raisonne par contraposée.
Supposons que $\det(\Omega) = 0$, on a alors les colonnes de Ω qui forment une famille liée et donc il existe un vecteur colonne V non nul de K^r tel que $\Omega V = 0$.
On multiplie V par le produit des dénominateurs de ses coefficients et alors on a un nouveau vecteur colonne U non nul à coefficients dans A^r cette fois-ci tel que $\Omega U = 0$ et alors $\psi(U) = 0$, donc ψ n'est pas injective puisque $\psi(U) = \psi(0) \not\Rightarrow U = 0$, d'où la conclusion.

Proposition 3 : Soient $P, Q \in A[X]$ où P est de degré p et Q est de degré inférieur ou égal à q. Les assertions sont équivalentes :

(1) Φ est injective
(2) $res(P, Q) \neq 0$
(3) P et Q sont premiers entre eux dans $K[X]$.

Preuve : Par le **Lemme 2**, (1) $\Leftrightarrow$ (2) est vérifiée.
Il reste donc à montrer que (1) $\Leftrightarrow$ (3).

(3) $\Rightarrow$ (1) : On suppose que P et Q sont premiers entre eux dans $K[X]$.
Soit (U, V) dans $A^{(q)}[X] \times A^{(p)}[X]$ tel que $\Phi(U, V) = 0$.
Ainsi, $UP + VQ = 0$ et donc on a $UP = -VQ$ $(*)$.
Comme $K[X]$ est principal et que P et Q sont premiers entre eux, on a $Q|U$ et $P| - V$ par le lemme de Gauss, donc $\exists F, F' \in K[X]$ tels que :
$-V = FP$ et $U = F'Q$ et alors en remplaçant dans l'expression $(*)$, on a $F'QP = FPQ$ donc $F = F'$ car P et Q sont non nuls (ils sont premiers entre eux).
D'autre part, on a $deg(V) = deg(F) + deg(P)$.
Si $F \neq 0$, alors $deg(F) \geq 0$ et alors on aurait $deg(V) \geq deg(P) = p$ et comme $deg(V) < p$ par hypothèse, on aboutit à une contradiction, donc $F = 0$.
Ainsi, $V = 0$ et $U = 0$ donc $(U, V) = 0_{A^{(q)}[X] \times A^{(p)}[X]}$, ce qui donne l'injectivité de Φ.

(1) $\Rightarrow$ (3) : On raisonne par contraposée.
On suppose donc que P et Q ne sont pas premiers entre eux.
Il existe donc un polynôme H non nul de $K[X]$ tel que $P = HP_1$ et $Q = HQ_1$ et P_1, Q_1 sont de degrés respectifs strictement inférieur à p et de degré strictement inférieur à q.
Ainsi, en multipliant P_1 et Q_1 par b le produit des dénominateurs des coefficients de P_1 et Q_1, on a $bP_1 \in A^{(p)}[X]$ et $bQ_1 \in A^{(q)}[X]$.
D'autre part, on a $PQ = HP_1Q = HQ_1P$ donc $P_1Q = Q_1P$ et donc $bP_1Q - bQ_1P = 0$, *i.e.*$\Phi(bQ_1, -bP_1) = 0$, ce qui montre que Φ n'est pas injective car $bP_1 \neq 0$.

Lemme général : On considère le morphisme d'évaluation suivant :

$$\begin{aligned} e : &\mathbb{Z}[X_1, \cdots, X_s] \longrightarrow A. \\ &X_i \longmapsto x_i \end{aligned}$$

Soient $P, Q \in \mathbb{Z}[X_1, \cdots, X_s][T]$, et $\tilde{P}, \tilde{Q} \in A[T]$ tels que :

$$P = \sum_{i=0}^{p} A_i T^i \qquad Q = \sum_{j=0}^{q} B_j T^j \qquad \tilde{P} = \sum_{i=0}^{p} e(A_i) T^i \qquad \tilde{Q} = \sum_{j=0}^{q} e(B_j) T^j.$$

Alors on a : $\boxed{res(\tilde{P},\tilde{Q}) = e(res(P,Q))}$.

Preuve : On note $(r_{i,j})_{1\leq i,j\leq p+q}$ la matrice dont le déterminant est $res(\tilde{P},\tilde{Q})$ et $(R_{i,j})_{1\leq i,j\leq p+q}$ la matrice dont le déterminant est $res(P,Q)$ et alors $\forall i,j \in [\![1,p+q]\!], r_{i,j} = e(R_{i,j})$.
D'autre part, la formule du déterminant nous donne que :

$$\begin{aligned} res(\tilde{P},\tilde{Q}) &= \sum_{\sigma\in S_{p+q}} \epsilon(\sigma) \prod_{i=1}^{p+q} r_{\sigma(i),i} \\ &= \sum_{\sigma\in S_{p+q}} \epsilon(\sigma) \prod_{i=1}^{p+q} e(R_{\sigma(i),i}) \\ &= e\Big(\sum_{\sigma\in S_{p+q}} \epsilon(\sigma) \prod_{i=1}^{p+q} R_{\sigma(i),i}\Big) \quad \text{car } e \text{ est un morphisme d'anneaux} \\ &= e(res(P,Q)). \end{aligned}$$

Théorème 4 : On note $P(T) = U(T-X_1)\cdots(T-X_p)$ et $Q(T) = V(T-Y_1)\cdots(T-Y_q)$ des polynômes de $\mathbb{Z}[U,V,X_1,\cdots,X_m,Y_1,\cdots,Y_n][T]$. Alors :

$$\begin{aligned} res_T(P,Q) &= U^pV^q \prod_{i=1}^{p}\prod_{j=1}^{q}(X_i - Y_j) \\ &= U^p \prod_{i=1}^{p} Q(X_i) = (-1)^{pq}V^q \prod_{j=1}^{q} P(Y_j). \end{aligned}$$

Preuve : On a $P(T) = A_0T^p + \cdots + A_p = U(T-X_1)\cdots(T-X_p)$
et $Q(T) = B_0T^q + \cdots + B_q = V(T-Y_1)\cdots(T-Y_q)$.
En appliquant les relations coefficients-racines, on a :

$$\begin{aligned} \forall i \in [\![0,p]\!], A_i &= (-1)^i A_0 \Sigma_i(X_1,\cdots,X_p) \\ &= (-1)^i U \Sigma_i(X_1,\cdots,X_p) \\ &=: UZ_i. \\ \forall j \in [\![p+1,p+q]\!], B_j &= (-1)^j B_0 \Sigma_j(Y_1,\cdots,Y_q) \\ &= (-1)^j V \Sigma_j(Y_1,\cdots,Y_q) \\ &=: VW_j. \end{aligned}$$

Comme $res_T(P,Q) = \sum_{\sigma\in S_{p+q}} \epsilon(\sigma) \prod_{i=1}^{p+q} R_{\sigma(i),i}$

et que $\forall i \leq q, R_{\sigma(i),i} = A_{\sigma(i)-i}$et $\forall j > q, R_{\sigma(i),i} = B_{q+\sigma(i)-i}$, on a :

$$\begin{aligned} res_T(P,Q) &= \sum_{\sigma \in S_{p+q}} \epsilon(\sigma) \prod_{i \leq q} A_{\sigma(i)-i} \prod_{i>q} B_{q+\sigma(i)-i} \\ &= \sum_{\sigma \in S_{p+q}} \epsilon(\sigma) \prod_{i \leq q} UZ_{\sigma(i)-i} \prod_{i>q} VW_{q+\sigma(i)-i} \\ &= U^q V^p \sum_{\sigma \in S_{p+q}} \epsilon(\sigma) \prod_{i \leq q} Z_{\sigma(i)-i} \prod_{i>q} W_{q+\sigma(i)-i}. \end{aligned}$$

Ainsi, $U^q V^p$ divise $res_T(P,Q)$.(1)
D'autre part, on considère le morphisme d'anneaux

$$\Psi : \mathbb{Z}[U, V, X_1, \cdots, \widehat{X_i}, \cdots, X_p, Y_1, \cdots, Y_q][X_i] \longrightarrow \mathbb{Z}[U, V, X_1, \cdots, \widehat{X_i}, \cdots, X_p, Y_1, \cdots, Y_q]$$

qui à X_i associe Y_j. Ainsi, $\Psi(P)$ et $\Psi(Q)$ ont une racine commune, à savoir Y_j donc par la **Proposition 3**, $res_T(\Psi(P), \Psi(Q)) = 0$ et alors le **Lemme général** nous donne que $\Psi(res_T(P,Q)) = 0$.
Donc $\forall i \in [\![1,p]\!]$ et $\forall j \in [\![1,q]\!]$, $X_i - Y_j$ divise $res_T(P,Q)$.
Comme ils sont de degré 1 et tous distincts, on a :

$$\prod_{i \in [\![1,p]\!], j \in [\![1,q]\!]} (X_i - Y_j) \text{ qui divise } res(P,Q).(2)$$

Donc les conditions (1) et (2) donnent que

$$S := U^q V^p \prod_{i \in [\![1,p]\!], j \in [\![1,q]\!]} (X_i - Y_j) \text{ divise } res_T(P,Q).$$

Et donc $\exists W \in \mathbb{Z}[U, V, X_1, \cdots, X_p, Y_1, \cdots, Y_q]$ tel que $res_T(P,Q) = SW$ et donc tel que $deg_U(res_T(P,Q)) = deg_U(S) + deg_U(W)$.
Or, on a $deg_U(res_T(P,Q)) = deg_U(S) = q$ et donc on a $deg_U(W) = 0$.
De même, $deg_V(res_T(P,Q)) = deg_V(S) = p$ donc W est aussi une constante par rapport à V.
De plus, pour tout $i \in [\![1,p]\!]$, on a $deg_{X_i}(res_T(P,Q)) = deg_{X_i}(S) = q$ (car les polynômes symétriques élémentaires ont un degré par rapport à X_i égal à 1) donc W est une constante par rapport aux variables X_i.
Il en est de même pour les variables Y_j pour j allant de 1 à q.
Ainsi, W est une constante par rapport à chacune des variables donc $W = \lambda \in \mathbb{Z}$.
On a donc $res(P,Q) = \lambda S$.
Pour trouver λ, on évalue l'expression en $(0, \cdots, 0, Y_1, \cdots, Y_q)$.
$S(0, \cdots, 0, Y_1, \cdots, Y_q) = (-1)^{pq} U^q V^p \prod_{j=1}^{q} Y_j^p$.
$res_T(P,Q)(0, \cdots, 0, Y_1, \cdots, Y_q) = res_T(\tilde{P}, \tilde{Q})(Y_1, \cdots, Y_q)$ où

$\tilde{P}(T) = UT^p$ et $\tilde{Q}(T) = V(T - Y_1)\cdots(T - Y_q)$.
On a donc, en écrivant la matrice, que :

$$\begin{aligned} res_T(P,Q)(0,\cdots,0,Y_1,\cdots,Y_q) &= res_T(\tilde{P},\tilde{Q})(Y_1,\cdots,Y_q) \\ &= U^q B_q^p = U^q((-1)^q V\Sigma_q(Y_1,\cdots,Y_q))^p \\ &= (-1)^{pq}U^qV^p\Sigma_q(Y_1,\cdots,Y_q)^p \\ &= (-1)^{pq}U^qV^p(\prod_{j=1}^{q} Y_j)^p \\ &= (-1)^{pq}U^qV^p\prod_{j=1}^{q} Y_j^p \\ &= S(0,\cdots,0,Y_1,\cdots,Y_q). \end{aligned}$$

On a donc que $\lambda = 1$, et alors $R = S$, ce qui confirme la première formule du théorème. En reprenant la définition de $P(T)$, on a directement les deux égalités suivantes (le $(-1)^{pq}$ vient de $X_i - Y_j = -(Y_j - X_i)$).

Corollaire 5 : Soit A un anneau. Soient P et $Q \in A[T]$, $P = u\prod_{i=1}^{p}(T - \alpha_i)$, $Q = v\prod_{j=1}^{q}(T - \beta_j)$.
Alors $res_T(P,Q) = u^p v^q \prod_{i=1}^{p}\prod_{j=1}^{q}(\alpha_i - \beta_j) = u^p\prod_{i=1}^{p} Q(\alpha_i) = (-1)^{pq}v^q\prod_{j=1}^{q} P(\beta_j)$.

Preuve : On utilise P_0 et Q_0 du **Théorème 4** (qui s'appelaient P et Q) et le morphisme d'évaluation :

$$\begin{aligned} e :&\mathbb{Z}[U,V,X_1,\cdots,X_m,Y_1,\cdots,Y_n] \longrightarrow A. \\ &X_i \longmapsto \alpha_i \qquad Y_j \longmapsto \beta_j \\ &U \longmapsto u \qquad V \longmapsto v \end{aligned}$$

On applique le **Lemme général** en notant que $P = e(P_0)$ et que $Q = e(Q_0)$, et alors $e(res_T(P_0,Q_0)) = res_T(P,Q)$.
Ainsi, $res_T(P,Q) = u^p v^q \prod_{i=1}^{p}\prod_{j=1}^{q}(\alpha_i - \beta_j) = u^p\prod_{i=1}^{p} Q(\alpha_i) = (-1)^{pq}v^q\prod_{j=1}^{q} P(\beta_j)$.

II - Théorème de Bézout faible

Dans cette partie, on va montrer que pour P et Q deux polynômes de $A[X,Y]$ de degrés totaux respectifs p et q, l'intersection de $C_P = V(P) = \{(x,y) \in A^2 / P(x,y) = 0\}$ avec $C_Q = V(Q) = \{(x,y) \in A^2 / Q(x,y) = 0\}$ contient au plus pq points, et nous verrons plus tard que dans le cas particulier où P et Q sont des polynômes homogènes, $C_P \cap C_Q$ contient exactement pq points.

II.A Préliminaires

On commence par montrer des résultats intermédiaires sur le résultant de P et Q.

Proposition 1 : Soient $P, Q \in A[X]$, alors, $\exists U_1 \in A^{(q)}[X]$ et $\exists V_1 \in A^{(p)}[X]$ tels que :

$$res(P,Q) = U_1 P + V_1 Q.$$

Preuve : Soit Ω la matrice de Φ dans les bases $\mathcal{B}_{q,p}$ et $\mathcal{B}_{p+q} = (X^{p+q}, \cdots, X, 1)$.
Comme $res(P,Q) \in A$, on assimile $res(P,Q)$ le polynôme constant au vecteur dans A^{p+q} dont les coefficients sont $(0, \cdots, 0, res(P,Q))$ dans la base $\mathcal{B}_{p+q}$.
Montrer ce résultat revient à montrer que $res(P,Q)$ est dans l'image de Φ.
Soient $u = {}^t(0, \cdots, 0, 1) \in A^{p+q}$ et $v \in A[X]^q \times A[X]^p$ de coordonnées ${}^t cof(\Omega)u$ dans la base $B_{q,p}$.
On a $\Phi(v) = \Omega {}^t cof(\Omega) u$.
Comme $I_{p+q} det(\Omega) = \Omega {}^t cof(\Omega)$, $\Phi(v)$ est le polynôme constant égal à $res(P,Q)$.
Donc $res(P,Q)$ est bien dans l'image de Φ, d'où l'existence de U_1 et V_1.

Dans la suite, on considèrera un corps k.

Proposition 2 : Soient $P, Q \in k[X,Y] (= k[X][Y])$ de degrés totaux respectifs p et q. Alors $deg(res_Y(P,Q)) \leq pq$.

Preuve : On note $P(Y) = a_0(X)Y^m + \cdots + a_m(X)$ et $Q(Y) = b_0(X)Y^n + \cdots + b_n(X)$.
Comme P et Q sont de degrés totaux p et q, on a : $\forall i \in [\![0, m]\!], deg_{(X,Y)} a_i(X) Y^{m-i} \leq p$, donc $deg_X a_i(X) + m - i \leq p$, $i.e, deg_X a_i(X) \leq p - m + i$.
De même, $\forall j \in [\![0, n]\!], deg_{(X,Y)} b_j(X) Y^{n-j} \leq q$ donc $deg_X b_j(X) \leq q - n + j$.

Par définition du déterminant, on a :

$$\begin{aligned} res_Y(P,Q) &= \sum_{\sigma \in S_{m+n}} \epsilon(\sigma) \prod_{i=1}^{m+n} r_{\sigma(i),i} \\ &= \sum_{\sigma \in S_{m+n}} \epsilon(\sigma) \prod_{i \leq n} r_{\sigma(i),i} \prod_{i > n} r_{\sigma(i),i} \\ &= \sum_{\sigma \in S_{m+n}} \epsilon(\sigma) \prod_{i \leq n} a_{\sigma(i)-i}(X) \prod_{i > n} b_{n+\sigma(i)-i}(X) \end{aligned}$$

et alors par passage au degré, on a :

$$\begin{aligned} deg_X(res_Y(P,Q)) &\leq deg_X\left(\prod_{i\leq n} a_{\sigma(i)-i}(X)\prod_{i>n} b_{n+\sigma(i)-i}(X)\right) \\ &= \sum_{i\leq n} deg_X a_{\sigma(i)-i}(X) + \sum_{i>n} deg_X b_{n+\sigma(i)-i}(X) \\ &\leq \sum_{i\leq n}(p-m+\sigma(i)-i) + \sum_{i>n}(q-\not{m}+\not{m}+\sigma(i)-i) \\ &= n(p-m)+mq+\sum_{i=1}^{m+n}(\sigma(i)-i) \\ &\leq q(p-m)+mq, \ \text{ car } n\leq q \text{ et } \sum_{i=1}^{m+n}(\sigma(i)-i)=0 \\ &= pq. \end{aligned}$$

On a donc bien $deg_X(res_Y(P,Q)) \leq pq$.

Lemme 3 : Soient $P, Q \in k[X,Y]$, si P et Q sont premiers entre eux, alors $res_X(P,Q)$ n'est pas le polynôme nul.

Preuve : On va montrer que P et Q sont premiers entre eux dans $k(Y)[X]$.
On note : $P(X,Y) = \prod_{i=1}^{s} A_i(Y)\prod_{j=1}^{t} B_j(X,Y)$ et $Q(X,Y) = \prod_{k=1}^{s'} A'_k(Y)\prod_{l=1}^{t'} B'_l(X,Y)$ les décompositions de P et Q en produits d'irréductibles de $k[Y][X]$, et on a $deg_X B_j \geq 1$ et $deg_X B'_l \geq 1$.
Dans $k(Y)[X]$, on a $P(X,Y) = u\prod_{j=1}^{t} B_j(X,Y)$ et $Q(X,Y) = v\prod_{l=1}^{t'} B'_l(X,Y)$, u et v dans $k(Y)$.
Comme les B_j et les B'_l sont irréductibles dans $k[Y][X]$, par le lemme de Gauss, ils sont aussi irréductibles dans $k(Y)[X]$.
Comme P et Q sont premiers entre eux dans $k[Y][X]$, $\forall j,l, B_j$ n'est pas associé à B'_l, donc P et Q sont premiers entre eux dans $k(Y)[X]$.
Donc par la **Proposition 3 I.B**, $res_X(P,Q)$ n'est pas le polynôme nul.

Corollaire 4 : Soient $P, Q \in k[X,Y]$. Si P et Q sont premiers entre eux, alors $C_P \cap C_Q$ est fini.

Preuve : Soit $(x,y) \in V(P)\cap V(Q)$. On a alors $P(x,y) = Q(x,y) = 0$.
On considère P et Q dans $k[X][Y]$ et alors par la **Proposition 1**, $\exists U_1, V_1 \in k[X][Y]$ tels

que $res_Y(P,Q)(X) = U_1(X,Y)P(X,Y) + V_1(X,Y)Q(X,Y)$.
Ainsi, $res_Y(P,Q)(x) = 0$ et comme par la **Proposition 2**, $deg_X(res_Y(P,Q)) \leq pq$, on a au plus pq possibilités pour x, car par le **Lemme 3**, $res_Y(P,Q)$ n'est pas le polynôme nul.
On fait le même raisonnement en considérant P et Q dans $k[Y][X]$ et cela nous donne au plus pq possibilités pour y. On a donc un nombre fini de couples $(x,y) \in V(P) \cap V(Q)$, *i.e.*$V(P) \cap V(Q)$ est fini.

II.B Théorème de Bézout faible

Théorème de Bézout faible : Soient $P, Q \in k[X,Y]$ premiers entre eux, de degrés respectifs totaux p et q. Alors $|C_P \cap C_Q| \leq pq$.

Preuve : Soit (a,b) dans $C_P \cap C_Q$, alors on sait que $P(a,b) = Q(a,b) = 0$. On note N_a et N_b le nombre de a resp. b possible et on note $r := |C_P \cap C_Q|$.
Par la **Proposition 1**, $\exists U_1 \in k^{(q)}[X][Y]$ et $\exists V_1 \in k^{(p)}[X][Y]$ tels que :
$res_Y(P,Q)(X) = U_1(X,Y)P(X,Y) + V_1(X,Y)Q(X,Y)$
En évaluant l'expression précédente en (a,b), on obtient :
$res_Y(P,Q)(a) = U_1(a,b)P(a,b) + V_1(a,b)Q(a,b) = 0$
Ainsi, a est une racine de $res_Y(P,Q)$ donc $N_a \leq deg(res_Y(P,Q))$ et par la **Proposition 2**, $deg(res_Y(P,Q)) \leq pq$ donc $N_a \leq pq$.
En considérant $res_Y(P,Q)$ comme polynôme en Y (P et Q comme polynômes de $k[Y][X]$), on a de même $N_b \leq pq$. On a donc $r \leq N_a \times N_b \leq p^2q^2$. Ce n'est pas encore la majoration voulue. On va montrer qu'on peut toujours se ramener au cas où toutes les abscisses sont distinctes.
Comme $C_P \cap C_Q$ est fini, on note $C_P \cap C_Q = \{(a_1,b_1), \cdots, (a_r,b_r)\}$.
Une droite reliant (a_i,b_i) à (a_j,b_j) est d'équation : $(a_j - a_i)y + (b_i - b_j)x + c = 0$, où c est une constante.
Remarque : On rappelle que les droites d'équations $ay + bx + c = 0$ *et* $a'y + b'x + c' = 0$ *sont parallèles si et seulement si* $ab' - ba' = 0$.
Comme K est infini, il existe μ et $\lambda \in K$ différents tels que $\forall i \neq j$:
$(a_j - a_i) + (b_i - b_j)\lambda \neq 0$ et $(a_j - a_i) + (b_i - b_j)\mu \neq 0$ (il suffit de prendre λ et $\mu \notin \left\{ \frac{a_i - a_j}{b_i - b_j} / i \neq j, b_i \neq b_j \right\}$).
Ainsi, par la remarque précédente, on a que :
$(D_1) : -\lambda y + x = 0$ et $(D_2) : -\mu y + x = 0$ sont des droites passant par l'origine, parallèles à aucune des droites reliant un (a_i,b_i) à un (a_j,b_j).
On note (x_1,y_1) les coordonnées dans la nouvelle base (v_1,v_2).
Soient S et T les polynômes de $k[X,Y]$ tels que :
$C_P = \{(x_1,y_1) \in k^2 / S(x_1,y_1) = 0\}$ et $C_Q = \{(x_1,y_1) \in k^2 / T(x_1,y_1) = 0\}$.
En notant (e_1,e_2) la base de départ, on a $v_1 = \lambda e_1 + e_2$ et $v_2 = \mu e_1 + e_2$ et donc $x = \lambda x_1 + \mu y_1$

et $y = x_1 + y_1$,
d'où $S(x_1, y_1) = P(x, y) = P(\lambda x_1 + \mu y_1, x_1 + y_1)$
et $T(x_1, y_1) = Q(x, y) = Q(\lambda x_1 + \mu y_1, x_1 + y_1)$.
Par construction de S et T, $|V(P) \cap V(Q)| = |V(S) \cap V(T)|$.
Il reste donc à vérifier que $deg(res_{Y_1}(S, T)) \leq pq$.

$$\text{On a : } P(X, Y) = \sum_{i=0}^{n} a_{n-i}(X)Y^i, \text{ avec } deg(a_{n-i}) \leq m \text{ et } m + n = p.$$

$$\text{et alors } S(X, Y) = \sum_{i=0}^{n} a_{n-i}(\lambda X + \mu Y)(X + Y)^i =: \sum_{i=0}^{n} d_i(X, Y).$$

Ainsi, on a

$$\begin{aligned} deg_{(X,Y)}(S(X, Y)) &\leq \max_{i \in \{0,\cdots,n\}} \left\{ deg_{(X,Y)}(d_i(X, Y)) \right\} \\ &= \max_{i \in \{0,\cdots,n\}} \left\{ deg_{(X,Y)}(a_{n-i}(\lambda X + \mu Y, X + Y) + i) \right\} \\ &\leq \max_{i \in \{0,\cdots,n\}} \{m + i)\} \\ &= m + n = p. \end{aligned}$$

On raisonne de même pour dire que $deg_{(X,Y)}(T(X, Y)) \leq q$.
Donc par la **Proposition 2**, $deg(res_{Y_1}(S, T)) \leq pq$ et donc il y a au plus pq abscisses possibles.
Comme dans ce nouveau repère, toutes les abscisses sont différentes, on a :
$|V(S) \cap V(T)| \leq deg(res_{Y_1}(S, T))$.
Donc finalement, on a bien $|C_P \cap C_Q| \leq pq$.

III - Intersections transverses ou non et résultant

Dans cette partie, nous allons calculer des résultants de polynômes P et Q de $k[X, Y]$, où k est un corps algébriquement clos et en déduire les points d'intersection de $C_P = V(P) = \{(x, y) \in k^2 / P(x, y) = 0\}$ avec $C_Q = V(Q) = \{(x, y) \in k^2 / Q(x, y) = 0\}$.
Pour cela, on va utiliser le lemme suivant qui lie les racines de $res(P, Q)$ aux intersections des deux courbes C_P et C_Q.

III.A Intersections et résultant

Lemme : Il existe $b \in k$ tel que $(a, b) \in V(P) \cap V(Q)$ si et seulement si a est racine de $res_Y(P, Q)$.

Preuve : Soit $(a,b) \in V(P) \cap V(Q)$ alors on a $P(a,b) = Q(a,b) = 0$.
Comme il existe U et V tels que $res(P,Q)(X) = U(X,Y)P(X,Y) + V(X,Y)Q(X,Y)$, a est tel que $res(P,Q)(a) = 0$ par évaluation de l'expression précédente en (a,b). Donc a est racine de $res(P,Q)$.
Réciproquement, supposons que a est racine de $res(P,Q)$.
On considère le morphisme d'évaluation suivant
$ev_a : k[X] \longrightarrow k$ tel que $X \mapsto a$.
Ce morphisme fournit un nouveau morphisme $e\tilde{v}_a : k[X,Y] \longrightarrow k[Y]$ qui envoie X sur a, Y sur Y et $t \in k$ sur t.
$res(P,Q) \in k[X]$ donc on a $e\tilde{v}_a(res(P,Q)) = res(P,Q)(a) = 0$.
D'autre part, on a :

$$res(P,Q)(X) = \sum_{\sigma \in S_{m+n}} \epsilon(\sigma) \prod_{i=1}^{m+n} r_{\sigma(i),i}(X)$$

$$res(e\tilde{v}_a(P), e\tilde{v}_a(Q))(X) = \sum_{\sigma \in S_{m+n}} \epsilon(\sigma) \prod_{i=1}^{m+n} e\tilde{v}_a(r_{\sigma(i),i}(X)).$$

Comme $e\tilde{v}_a$ est un morphisme, on a : $e\tilde{v}_a(res(P,Q)) = res(e\tilde{v}_a(P), e\tilde{v}_a(Q))$.
Ainsi, $res(e\tilde{v}_a(P), e\tilde{v}_a(Q)) = 0$ et donc $e\tilde{v}_a(P)$ $(= P(a,Y))$ et $e\tilde{v}_a(Q)$ $(= Q(a,Y))$ ne sont pas premiers entre eux dans $k[Y]$. Comme k est algébriquement clos, ils ont donc une racine commune donc il existe $b \in k$ tel que $P(a,b) = Q(a,b)$, i.e. $(a,b) \in V(P) \cap V(Q)$.

Preuve alternative du sens direct : On note : $P(X,Y) = \sum a_{p-i}(X)(Y-b)^i$
et $Q(X,Y) = \sum b_{p-j}(X)(Y-b)^j$. On a alors :
$P(a,b) = 0 \Leftrightarrow a_p(a) = 0$ (car $\forall i \geq 1, (Y-b)^i(a,b) = 0$).
De même, on a $Q(a,b) = 0 \Leftrightarrow b_q(a) = 0$.
Ainsi, $(a,b) \in V(P) \cap V(Q) \Leftrightarrow a_p(a) = b_q(a) = 0$.
On écrit maintenant le résultant de P et Q dans la base des $((Y-b)^i)_i$:

$$res(P,Q)(X) = \det \begin{pmatrix} a_0(X) & 0 & \cdots & 0 & b_0(X) & 0 & \cdots & 0 \\ a_1(X) & \ddots & & \vdots & b_1(X) & \ddots & & \vdots \\ \vdots & & \ddots & 0 & \vdots & & \ddots & 0 \\ \vdots & & & a_0(X) & \vdots & & & b_0(X) \\ a_p(X) & & & a_1(X) & b_q(X) & & & b_1(X) \\ 0 & \ddots & & \vdots & 0 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & a_p(X) & 0 & \cdots & 0 & b_q(X) \end{pmatrix}$$

et alors on a que :
$a_p(a) = b_q(a) = 0$

$$\Rightarrow res(P,Q)(a) = \det \begin{pmatrix} a_0(a) & 0 & \cdots & 0 & b_0(a) & 0 & \cdots & 0 \\ a_1(a) & \ddots & & \vdots & b_1(a) & \ddots & & \vdots \\ \vdots & & \ddots & 0 & \vdots & & \ddots & 0 \\ \vdots & & & a_0(a) & \vdots & & & b_0(a) \\ 0 & & & a_1(a) & 0 & & & b_1(a) \\ 0 & \ddots & & \vdots & 0 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

$$= 0$$

(en développant par rapport à la dernière ligne qui est une ligne nulle).
Ceci donne que $(a,b) \in V(P) \cap V(Q) (\Leftrightarrow a_p(a) = b_q(a) = 0) \Rightarrow res(P,Q)(a) = 0$.

III.B Exemples

Dans tous les exemples de cette partie, on a pris P et Q des polynômes de $\mathbb{R}[X,Y]$ de degrés totaux 2. D'après le théorème de Bézout faible, on s'attend donc à trouver au plus quatre points d'intersection entre les courbes C_P et C_Q.

Exemple 1 : Soient $P = 4X^2 + 4Y^2 - 17$ et $Q = XY - 1$.
On sait par le **Lemme III.A**, que pour trouver les points d'intersection des courbes C_P et C_Q, il faut trouver les racines de $res(P,Q)$. On commence donc par le calculer :

$$res_Y(P,Q) = \det \begin{pmatrix} 4 & X & 0 \\ 0 & -1 & X \\ 4X^2 - 17 & 0 & -1 \end{pmatrix} = 4 + X^2(4X^2 - 17) = 4X^4 - 17X^2 + 4.$$

Donc $res_Y(P,Q) = 0 \Leftrightarrow 4X^4 - 17X^2 + 4 = 0$ et alors en posant $Z = X^2$,
on résout $4Z^2 - 17Z + 4 = 0$, on a $\Delta = 17^2 - 16 \times 4 = 225 = 15^2$, et alors $Z^2 = \frac{1}{4}$ ou 4
Ainsi, si (a,b) est dans $C_P \cap C_Q$, alors $a = \frac{1}{2}$ ou $-\frac{1}{2}$ ou 2 ou -2.
On trouve b en calculant $P(a,b)$ et $Q(a,b)$ qui doivent valoir 0.

- Si $a = \frac{1}{2}$ ou $a = -\frac{1}{2}$:

$$\begin{aligned} P(a,b) = 0 &\Leftrightarrow 1 + 4b^2 - 17 = 0 \\ &\Leftrightarrow 4b^2 - 16 = 0 \\ &\Leftrightarrow b^2 = 4 \\ &\Leftrightarrow b = 2 \text{ ou } b = -2. \end{aligned}$$

Il reste à vérifier lesquels des points $(\frac{1}{2}, 2)$, $(\frac{1}{2}, -2)$, $(-\frac{1}{2}, -2)$ et $(-\frac{1}{2}, 2)$ sont aussi des zéros de Q.
On a $Q(\frac{1}{2}, 2) = 0$, $Q(-\frac{1}{2}, -2) = 0$, $Q(-\frac{1}{2}, 2) \neq 0$ et $Q(\frac{1}{2}, -2) \neq 0$.
Ainsi, $(\frac{1}{2}, 2)$ et $(-\frac{1}{2}, -2)$ sont des zéros communs à P et Q.

- Si $a = 2$ ou $a = -2$:

$$\begin{aligned} P(a,b) = 0 &\Leftrightarrow 4b^2 - 1 = 0 \\ &\Leftrightarrow b^2 = \frac{1}{4} \\ &\Leftrightarrow b = \frac{1}{2} \text{ ou } -\frac{1}{2}. \end{aligned}$$

Il reste à vérifier lesquels des points $(2, \frac{1}{2})$, $(2, -\frac{1}{2})$, $(-2, -\frac{1}{2})$ et $(-2, \frac{1}{2})$ sont aussi des zéros de Q.
On a $Q(2, \frac{1}{2}) = 0$, $Q(-2, \frac{1}{2}) = 0$, $Q(-2, -\frac{1}{2}) \neq 0$ et $Q(2, -\frac{1}{2}) \neq 0$.
Ainsi, $(2, \frac{1}{2})$ et $(-2, -\frac{1}{2})$ sont des zéros communs à P et Q.

Donc $C_P \cap C_Q$ est constitué des quatre points : $(2, \frac{1}{2}), (-2, -\frac{1}{2}), (\frac{1}{2}, 2)$ et $(-\frac{1}{2}, -2)$.
On le constate sur le graphe suivant :

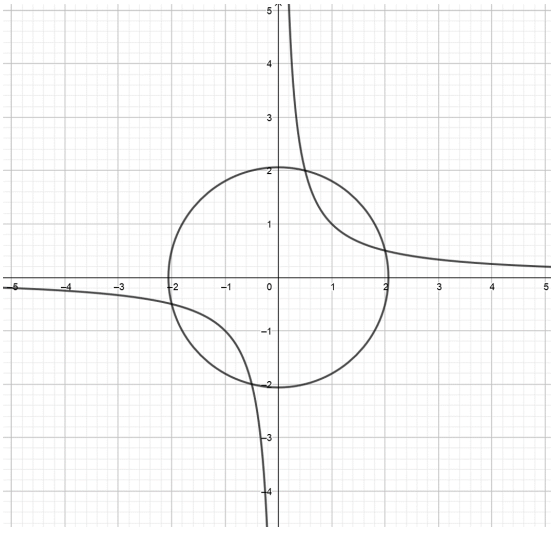

FIGURE 1 – C_P est le cercle, l'autre courbe est C_Q

Exemple 2 : Soient $P = X^2 + Y^2 - 2$ et $Q = XY - 1$.

$$res_Y(P,Q) = \det \begin{pmatrix} 1 & X & 0 \\ 0 & -1 & X \\ X^2-2 & 0 & -1 \end{pmatrix} = X^4 - 2X^2 + 1 = (X^2-1)^2 = (X-1)^2(X+1)^2.$$

Donc les valeurs possibles de a sont ± 1.
$P(\pm 1, b) = 0 \Leftrightarrow b^2 = 1 \Leftrightarrow b = \pm 1$.
Il reste à vérifier lesquels des points $(1,1), (1,-1), (-1,-1), (-1,1)$ sont des zéros de Q :
$Q(1,1) = 0$, $Q(1,-1) = -2$, $Q(-1,-1) = 0$, $Q(-1,1) = -2$.
Ainsi, $(1,1)$ et $(-1,-1)$ sont des zéros communs à P et Q.
On le constate en effet sur le graphe suivant :

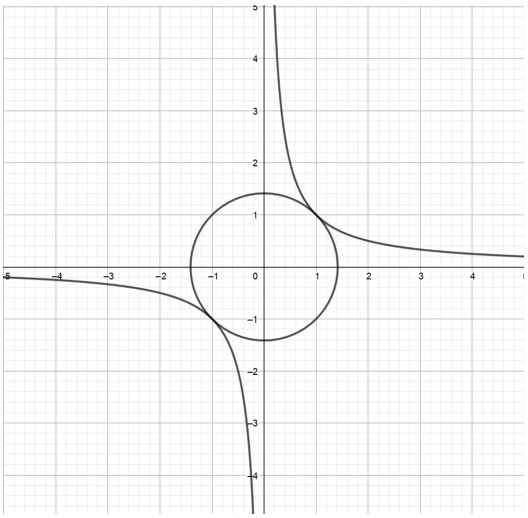

FIGURE 2 – C_P est le cercle, l'autre courbe est C_Q

Remarque : En ces deux points, les courbes ont une tangente commune.

Exemple 3 : Soient $P = X^2 + Y^2 - 1$ et $Q = XY - 1$.

$$res_Y(P,Q) = \det \begin{pmatrix} 1 & X & 0 \\ 0 & -1 & X \\ X^2-1 & 0 & -1 \end{pmatrix} = X^4 - X^2 + 1.$$

En posant $Z = X^2$, on est amené à résoudre $Z^2 - Z + 1 = 0$, qui nous donnerait des points de $\mathbb{C}^2$ mais qui n'a pas de racine dans $\mathbb{R}$, donc P et Q n'ont pas de zéros en commun dans $\mathbb{R}^2$, ce que l'on constate sur le graphe suivant :

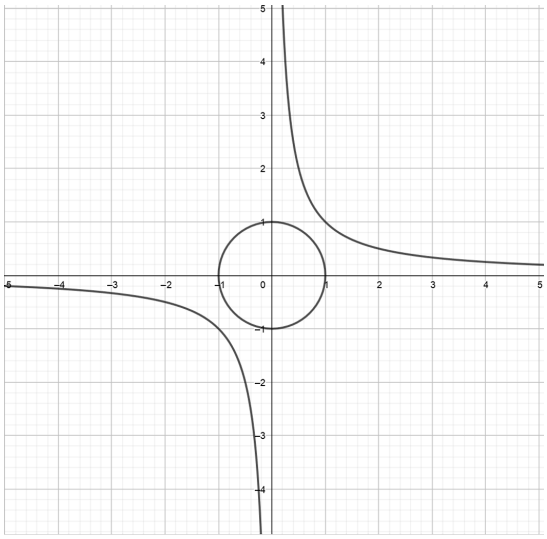

FIGURE 3 – C_P est le cercle, l'autre courbe est C_Q

Exemple 4 : Soient $P = X^2 + Y^2 - 1$ et $Q = Y^2 - X - 1$.

$$res(P,Q) = \det \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ X^2-1 & 0 & -X-1 & 0 \\ 0 & X^2-1 & 0 & -X-1 \end{pmatrix}$$

$$= \det \begin{pmatrix} 1 & 0 & 1 \\ 0 & -X-1 & 0 \\ X^2-1 & 0 & -X-1 \end{pmatrix} + \det \begin{pmatrix} 0 & 1 & 1 \\ X^2-1 & 0 & 0 \\ 0 & X^2-1 & -X-1 \end{pmatrix}$$

$$= (X+1)^2 + (X^2-1)(X+1) + (X^2-1)^2 + (X+1)(X^2-1)$$
$$= (X+1)^2 + (X-1)(X+1)^2 + (X-1)^2(X+1)^2 + (X-1)(X+1)^2$$
$$= (X+1)^2(1 + X - 1 + X^2 - 2X + 1 + X - 1)$$
$$= (X+1)^2X^2.$$

Les valeurs possibles de a sont donc 0 et -1.
$P(0,b) = 0 \Leftrightarrow b^2 = 1 \Leftrightarrow b = \pm 1$.
$P(-1,b) = 0 \Leftrightarrow b^2 = 0 \Leftrightarrow b = 0$.
Il reste à vérifier lesquels des points $(0,1), (0,-1), (-1,0)$ annulent le polynôme Q :
$Q(0,1) = 0$, $Q(0,-1) = -2$, $Q(-1,0) = 0$.
Ainsi, les zéros communs à P et Q sont $(0,1)$, $(0,-1)$ et $(-1,0)$.
On le constate sur le graphe suivant :

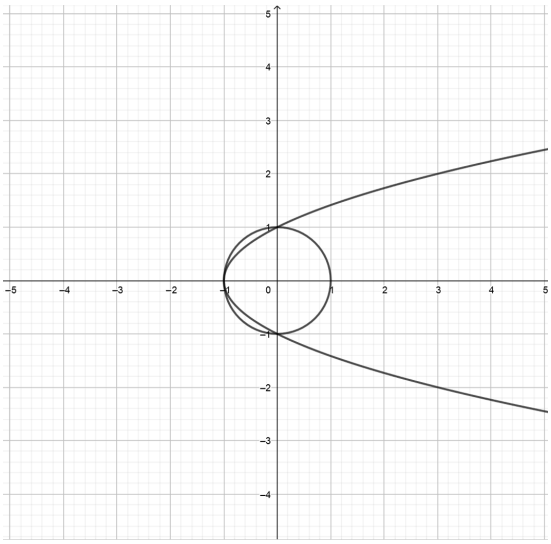

FIGURE 4 – C_P est le cercle, l'autre courbe est C_Q

Remarque : En $(-1, 0)$, les deux courbes ont une tangente commune.

Exemple 5 : Soient $P = X^2 + Y^2 - 4$ et $Q = Y^2 - 4X - 4$.

$$res(P,Q) = \det \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ X^2-4 & 0 & -4X-4 & 0 \\ 0 & X^2-4 & 0 & -4X-4 \end{pmatrix}$$

$$= \det \begin{pmatrix} 1 & 0 & 1 \\ 0 & -4X-4 & 0 \\ X^2-4 & 0 & -4X-4 \end{pmatrix} + \det \begin{pmatrix} 0 & 1 & 1 \\ X^2-4 & 0 & 0 \\ 0 & X^2-4 & -4X-4 \end{pmatrix}$$

$$= 16(X+1)^2 + 4(X+1)(X^2-4) + (X^2-4)^2 + 4(X+1)(X^2-4)$$
$$= 16X^2 + 32X + 16 + 4X^3 - 16X + 4X^2 - 16 + X^4 - 8X^2 + 16 + 4X^3 - 16X + 4X^2 - 16$$
$$= X^4 + 8X^3 + (16 + 4 - 8 + 4)X^2 + (32 - 16 - 16)X + 0$$
$$= X^2(X^2 + 8X + 16)$$
$$= X^2(X+4)^2.$$

Donc les abscisses possibles des points d'intersection sont 0 et -4.
$P(0, b) = 0 \Leftrightarrow b^2 = 4 \Leftrightarrow b = \pm 2$.
$P(-4, b) = 0 \Leftrightarrow b^2 = -15$, ce qui est impossible dans $\mathbb{R}$.
Il reste à vérifier lesquels des points $(0, 2)$ et $(0, -2)$ sont aussi des zéros de Q.
$Q(0, 2) = Q(0, -2) = 0$.
Ainsi, les zéros communs réels à P et Q sont $(0, 2)$ et $(0, -2)$ et on trouverait deux autres points dans $\mathbb{C}^2$.

On le constate sur le graphe suivant :

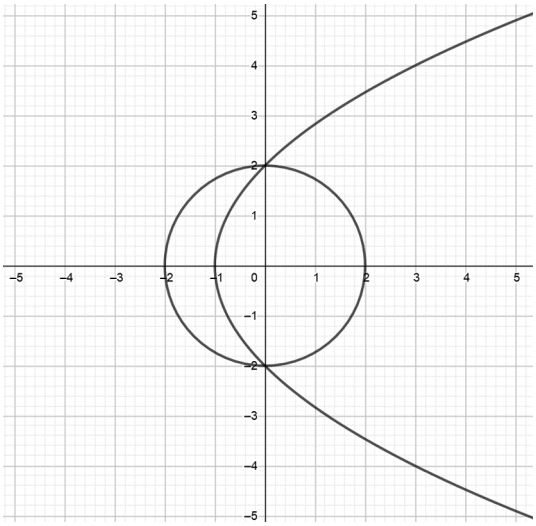

FIGURE 5 – C_P est le cercle, l'autre courbe est C_Q

Exemple 6 : Soient $P = Y^2 - X^2 - 1$ et $Q = Y - X^2$

$$res(P,Q) = \det \begin{pmatrix} 1 & 1 & 0 \\ 0 & -X^2 & 1 \\ -X^2 - 1 & 0 & -X^2 \end{pmatrix} = X^4 - X^2 - 1$$

En posant $Z = X^2$, on a $Z^2 - Z - 1 = 0 \Leftrightarrow Z = \frac{1 \pm \sqrt{5}}{2}$. Donc les racines de $res(P,Q)$ sont $\alpha := \sqrt{\frac{1+\sqrt{5}}{2}}$ et $-\alpha$.
Donc les abscisses possibles des points d'intersection sont α et $-\alpha$.
$Q(\alpha, b) = 0 \Leftrightarrow Q(-\alpha, b) = 0 \Leftrightarrow b = \alpha^2$.
Il reste à vérifier lesquels des points $(\alpha, \alpha^2), (-\alpha, \alpha^2)$ sont aussi des zéros de P.
$P(\alpha, \alpha^2) = \alpha^4 - \alpha^2 - 1 = 0$.
$P(-\alpha, \alpha^2) = \alpha^4 - \alpha^2 - 1 = 0$.
Ainsi, les zéros communs à P et Q sont (α, α^2) et $(-\alpha, \alpha^2)$ et on trouverait deux autres points dans $\mathbb{C}^2$.
On le constate sur le graphe suivant :

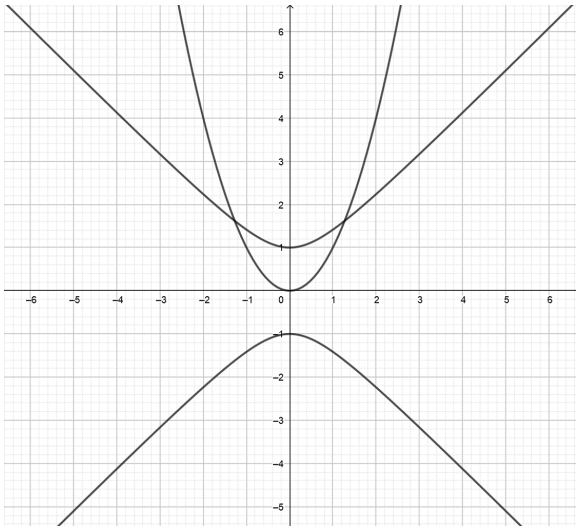

FIGURE 6 – C_P est la courbe symétrique par rapport à l'axe des abscisses, l'autre courbe est C_Q

Exemple 7 : Soient $P = Y^2 - X^2 - 1$ et $Q = -Y^2 + (2X+1)Y - X^2 + X$.

$$res(P,Q) = \det \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 2X+1 & -1 \\ -X^2-1 & 0 & -X^2+X & 2X+1 \\ 0 & -X^2-1 & 0 & -X^2+X \end{pmatrix}$$

$$= \det \begin{pmatrix} 1 & 2X+1 & -1 \\ 0 & -X^2+X & 2X+1 \\ -X^2-1 & 0 & -X^2+X \end{pmatrix} - \det \begin{pmatrix} 0 & 1 & -1 \\ -X^2-1 & 0 & 2X+1 \\ 0 & -X^2-1 & -X^2+X \end{pmatrix}$$

$$\begin{aligned}
&= (X^2-X)^2 - (2X+1)^2(X^2+1) + (X^2-X)(X^2+1) \\
&\quad - (-(X^2+1)^2 - (X^2-X)(X^2+1)) \\
&= (X^2-X)^2 - (2X+1)^2(X^2+1) + (X^2-X)(X^2+1) + (X^2+1)^2 \\
&\quad + (X^2-X)(X^2+1) \\
&= X^4 - 2X^3 + X^2 - (4X^2+4X+1)(X^2+1) + X^4 \\
&\quad + X^2 - X^3 - X + X^4 + 2X^2 + 1 + X^4 + X^2 - X^3 - X \\
&= X^4 - 2X^3 + X^2 - 4X^4 - 4X^2 - 4X^3 - 4X - X^2 - 1 + X^4 \\
&\quad + X^2 - X^3 - X + X^4 + 2X^2 + 1 + X^4 + X^2 - X^3 - X \\
&= (1-4+1+1+1)X^4 + (-2-4-1-1)X^3 + (1-4-1+1+2+1)X^2 \\
&\quad + (-4-1-1)X + 0 \\
&= -8X^3 - 6X \\
&= -2X(4X^2+3).
\end{aligned}$$

Contrairement aux exemples précédents, le résultant est de degré 3.
La seule abscisse possible dans $\mathbb{R}$ des points d'intersection de P et Q est 0.
$P(0,b) = 0 \Leftrightarrow b^2 = 1 \Leftrightarrow b = \pm 1$.

Il reste à vérifier lesquels des points $(0,1)$ et $(0,-1)$ sont aussi des zéros de Q.
$Q(0,1) = -1+1 = 0$ et $Q(0,-1) = -1-1 \neq 0$.
Ainsi, le zéro commun à P et Q dans $\mathbb{R}^2$ est $(0,1)$.
On le constate sur le graphe suivant :

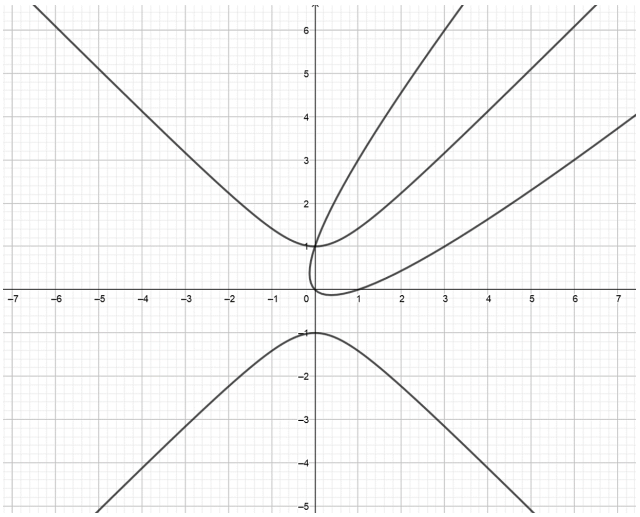

FIGURE 7 – C_P est la même courbe que dans la figure 6, l'autre courbe est C_Q

On trouverait deux autres points dans $\mathbb{C}^2$ et nous allons voir aussi que les deux courbes ont un point commun à l'infini.

III.C Intersections transverses et résultant

Définition : L'intersection de deux courbes en un point (a,b) est dite **transverse** si les deux courbes ont des tangentes sécantes en (a,b).

On rappelle que pour un polynôme P de $k[X,Y]$, la tangente à $C_P = V(P)$ en $(a,b) \in k^2$ a pour équation :

$$\frac{\partial P}{\partial X}(a,b)(X-a) + \frac{\partial P}{\partial Y}(a,b)(Y-b) = 0.$$

Lemme : Soit k un corps algébriquement clos. Si $V(P)$ et $V(Q)$ ont une intersection non tranverse en (a,b), alors a est racine multiple du résultant de P et Q.

Preuve : Soit $(a,b) \in V(P) \cap V(Q)$ tel que les tangentes de $V(P)$ et $V(Q)$ en (a,b)

sont les mêmes.
On peut donc se ramener au cas où on a :

$$\frac{\partial P}{\partial X}(a,b)(X-a)+\frac{\partial P}{\partial Y}(a,b)(Y-b)=\frac{\partial Q}{\partial X}(a,b)(X-a)+\frac{\partial Q}{\partial Y}(a,b)(Y-b).$$

Donc on a : $\frac{\partial P}{\partial X}(a,b)=\frac{\partial Q}{\partial X}(a,b)$ et $\frac{\partial P}{\partial Y}(a,b)=\frac{\partial Q}{\partial Y}(a,b)$. (1)

Avec les notations précédentes, on a : $P(X,Y)=\sum_{i=0}^{p}a_{p-i}(X)(Y-b)^i$
et $Q(X,Y)=\sum_{j=0}^{q}b_{q-j}(X)(Y-b)^j$.
On a alors :

$$\begin{aligned}
\frac{\partial P}{\partial X}(X,Y)&=\sum_{i=0}^{p}a'_{p-i}(X)(Y-b)^i \Rightarrow \frac{\partial P}{\partial X}(a,b)=a'_p(a)\\
\frac{\partial Q}{\partial X}(X,Y)&=\sum_{j=0}^{q}b'_{q-j}(X)(Y-b)^i \Rightarrow \frac{\partial Q}{\partial X}(a,b)=b'_q(a)\\
\frac{\partial P}{\partial Y}(X,Y)&=\sum_{i=1}^{p}ia_{p-i}(X)(Y-b)^{i-1} \Rightarrow \frac{\partial P}{\partial Y}(a,b)=a_{p-1}(a)\\
\frac{\partial Q}{\partial Y}(X,Y)&=\sum_{j=1}^{q}jb_{q-j}(X)(Y-b)^{j-1} \Rightarrow \frac{\partial Q}{\partial Y}(a,b)=b_{q-1}(a).
\end{aligned}$$

Et donc par (1) : $a'_p(a)=b'_q(a)$ et $a_{p-1}(a)=b_{q-1}(a)$.
Donc $X-a$ divise $(a_{p-1}-b_{q-1})(X)$.
Comme (a,b) est dans $V(P)\cap V(Q)$, on a aussi que $a_p(a)=b_q(a)=0$.
Ainsi, a est racine de $N:=(a_p-b_q)(X)$ et de $N'=(a'_p-b'_q)(X)$ donc $(X-a)^2$ divise N.
D'autre part, comme le déterminant est invariant par la transformation $C_{p+q}\leftarrow C_{p+q}-C_q$, on a que :

$$res(P,Q)(X)=\det\begin{pmatrix}
a_0(X) & 0 & \cdots & 0 & b_0(X) & 0 & \cdots & 0\\
a_1(X) & \ddots & & \vdots & b_1(X) & \ddots & & \vdots\\
\vdots & & \ddots & 0 & \vdots & & \ddots & 0\\
\vdots & & & a_0(X) & \vdots & & & *\\
a_p(X) & & & a_1(X) & b_q(X) & & & *\\
0 & \ddots & & \vdots & 0 & \ddots & & \vdots\\
\vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots\\
0 & \cdots & 0 & a_p(X) & 0 & \cdots & 0 & b_q(X)-a_p(X)
\end{pmatrix}.$$

Et alors, en développant par rapport à la dernière ligne, on obtient qu'il existe F et G

dans $k[X]$ tels que :

$$\begin{aligned} res(P,Q)(X) &= a_p(X)F(X) + (b_q(X) - a_p(X))G(X) \\ &= a_p(X)F(X) + N(X)G(X) \end{aligned}$$

avec

$$F(X) = (-1)^q \det \begin{pmatrix} a_0(X) & 0 & \cdots & 0 & b_0(X) & 0 & \cdots & 0 & 0 \\ a_1(X) & \ddots & & \vdots & b_1(X) & \ddots & & \vdots & \vdots \\ \vdots & & \ddots & 0 & \vdots & & \ddots & 0 & 0 \\ \vdots & & & a_0(X) & \vdots & & & b_0(X) & * \\ a_p(X) & & & a_1(X) & b_q(X) & & & b_1(X) & * \\ 0 & \ddots & & \vdots & 0 & \ddots & & \vdots & \vdots \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & a_p(X) & 0 & \cdots & 0 & b_q(X) & b_{q-1}(X) - a_{p-1}(X) \end{pmatrix}$$

et alors, en évaluant en a, on a que $F(a) = 0$ (car $a_p(a) = b_q(a) = 0$ et $b_{q-1}(a) - a_{p-1}(a) = 0$ donc la dernière ligne de la matrice est nulle). Donc $X - a$ divise $F(X)$.
De même, comme $a_p(a) = 0$, on a $X - a$ divise $a_p(X)$ donc $(X-a)^2$ divise $a_p(X)F(X)$. De plus, comme $(X-a)^2$ divise aussi $N(X)$, on a finalement que $(X-a)^2$ divise $res(P,Q)(X)$. Donc a est une racine multiple de $res(P,Q)(X)$.

Remarques :
- Dans l'exemple 2 précédent, on a constaté qu'en $(1,1)$ et en $(-1,-1)$, C_P et C_Q avaient une tangente commune et donc par le lemme précédent, 1 et -1 sont racines multiples de $res_Y(P,Q)$, c'est en effet le cas car on avait calculé $res_Y(P,Q) = (X-1)^2(X+1)^2$.
- Dans l'exemple 4 précédent, on a constaté qu'en $(-1,0)$, C_P et C_Q avaient une tangente commune, ce qui implique par ce lemme, que -1 est racine multiple du résultant, ce qui est vérifié par $res_Y(P,Q) = (X=1)^2X^2$.
- Dans l'exemple 4, 0 est aussi racine multiple du résultant, et on remarque que 0 est l'abscisse de deux points d'intersection distincts.

IV - Géométrie projective

On considère k un corps algébriquement clos.
Le but de cette partie est d'introduire quelques définitions de géométrie projective que nous utiliserons pour trouver les expressions des polynômes P_1 et Q_1 de $k[X,Y,Z]$ qui généralisent les polynômes P et Q.
Ils sont tels que C_P et C_Q soient les courbes obtenues par intersection entre les surfaces portées par P_1 et Q_1 et le plan $\{z = 1\}$.

Ensuite, on montrera que l'on peut trouver un plan dans k^3 dans lequel sont visibles tous les points d'intersection.

IV.A Définitions

Définition : Soit E un k-espace vectoriel. L'**espace projectif** déduit de E est l'ensemble des droites vectorielles de E. On le note $\mathbb{P}(E)$.

Remarque : Si $E = k^n$, on note : $\mathbb{P}(k^n) = \mathbb{P}_{n-1}(k)$.

On considère la projection $\pi : E\backslash\{0\} \longrightarrow \mathbb{P}(E)$.

Définition : Soit $x = (x_0, \cdots, x_{n-1}) \in k^n\backslash\{0\}$.
On note $(x_0 : \cdots : x_{n-1})$ les **coordonnées homogènes** de $\pi(x) \in \mathbb{P}_{n-1}(k)$.
On a donc que $\forall \lambda \in k^*, (x_0 : \cdots : x_{n-1}) = (\lambda x_0 : \cdots : \lambda x_{n-1})$.

Dans la suite, on va s'intéresser uniquement au cas où $E = k^3$.
On dira qu'un point $(a : b : c)$ de $\mathbb{P}_2(k)$ est un **point à l'infini** si $c = 0$.

Un point à l'infini correspond donc à une droite vectorielle de E qui est contenue dans le plan d'équation $z = 0$, et qui par conséquent ne rencontre pas le plan d'équation $z = 1$.

Dans la suite nos figures seront a priori dans le plan d'équation z=1, et les points à l'infini sont ceux que nous ne verrons pas dans ce plan.

IV.B Homogénéisation d'un polynôme

Soit $P = \sum_{i+j\leq m} a_{ij} X^i Y^j$ un polynôme de degré m de $k[X, Y]$.
Nous allons maintenant regarder C_P dans le plan d'équation $z = 1$.
Donc $C_P = \{(x, y, 1) \in k^3 / P(x, y) = 0\}$ et on note $\tilde{C_P}$ la réunion des droites vectorielles de k^3 épointées en 0 s'appuyant sur C_P.

On cherche à expliciter l'équation de $\tilde{C_P}$:

$$M \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \tilde{C_P} \Leftrightarrow \exists \lambda \in k^*, \exists N \in C_P / \vec{OM} = \lambda \vec{ON}, \text{ avec } N \begin{pmatrix} x_1 \\ y_1 \\ 1 \end{pmatrix}$$
$$\Leftrightarrow \exists \lambda \in k^*, \exists x_1, y_1 \in k / P(x_1, y_1) = 0 \text{ et } x = \lambda x_1, y = \lambda y_1, z = \lambda$$
$$\Leftrightarrow \exists x_1, y_1 \in k / \sum_{i+j\leq m} a_{ij} x_1^i y_1^j = 0 \text{ et } x = z x_1, y = z y_1, z \neq 0$$
$$\Leftrightarrow \exists x_1, y_1 \in k / \sum_{i+j\leq m} a_{ij} x_1^i y_1^j = 0, x_1 = \tfrac{x}{z} \text{ et } y_1 = \tfrac{y}{z}, z \neq 0$$
$$\Leftrightarrow \sum_{i+j\leq m} a_{ij} (\tfrac{x}{z})^i (\tfrac{y}{z})^j = 0, z \neq 0$$

$\Leftrightarrow \sum_{i+j\leq m} a_{ij}x^iy^jz^{m-i-j} = 0$ et $z \neq 0$
$\Leftrightarrow (x, y, z)$ est un zéro de $P_1 = \sum_{i+j\leq m} a_{ij}X^iY^jZ^{m-i-j}$ et $z \neq 0$.

Remarquons que le polynôme P_1 est un polynôme homogène de degré m et est tel que $P_1(X, Y, 1) = P(X, Y)$, on l'appellera l'**homogénéisé de P**.
On a montré que $\boxed{\tilde{C}_P = \{(x, y, z) \in k^3/P_1(x, y, z) = 0 \text{ et } z \neq 0\}}$.
On note $S_{P_1} = \{(x, y, z) \in k^3/P_1(x, y, z) = 0\}$, l'adhérence de $\tilde{C}_P$, et alors on a $C_P = S_{P_1} \cap \{z = 1\}$. On notera par ailleurs $\gamma_P = \{(x : y : z) \in \mathbb{P}_2(k)/P_1(x, y, z) = 0\}$. C'est la courbe projective associée à C_P.

Remarque : Le polynôme P_1 homogénéisé de P ne se factorise pas par Z puisqu'il contient au moins un monôme X^iY^j avec $i + j = m$.

IV.C Exemples de recherche des points à l'infini

En gardant les mêmes notations que précédemment, les points à l'infini de C_P sont les points de $\pi(S_{P_1} \cap \{z = 0\})$.
Ainsi, pour trouver les points à l'infini pour un polynôme P, il faut commencer par calculer son homogénéisé P_1, puis déterminer $S_{P_1} \cap \{z = 0\}$ et pour finir, son image par la projection π.
On va rechercher en particulier les points à l'infini dans les exemples 6 et 7 de la partie III.B.

Exemple 6 :
Prenons le polynôme $\boxed{P = Y^2 - X^2 - 1}$.
Par le calcul général précédent, on obtient que $P_1 = Y^2 - X^2 - Z^2$.
Alors, on a $S_{P_1} = \{(x, y, z) \in k^3/y^2 - x^2 - z^2 = 0\}$,
et donc $S_{P_1} \cap \{z = 0\} = \{x^2 = y^2\}$.
Donc finalement, les points à l'infini de C_P sont, pour tout $x \in k$, $\pi(x, x, 0), \pi(-x, x, 0)$ et $\pi(x, -x, 0)$, c'est-à-dire $(1 : 1 : 0), (-1 : 1 : 0)$ et $(1 : -1 : 0)$.

Prenons le polynôme $\boxed{Q = Y - X^2}$.
Par le calcul général, on obtient que $Q_1 = YZ - X^2$.
Alors on a $S_{Q_1} = \{(x, y, z) \in k^3/yz = x^2\}$,
et donc $S_{Q_1} \cap \{z = 0\} = \{x^2 = 0\}$.
Donc finalement, le seul point à l'infini de C_Q est $\forall y \in k, \pi(0, y, 0) = (0 : 1 : 0)$.

Ainsi, on peut dire que les courbes C_P et C_Q n'ont pas de point d'intersection à l'infini.

Exemple 7 :
On prend le même polynôme P que dans l'exemple 1.
On prend cette fois $\boxed{Q = -Y^2 + (2X+1)Y - X^2 + X}$ et le calcul général nous donne que $Q_1 = -Y^2 + (2X+Z)Y - X^2 + XZ$,
et alors $S_{Q_1} = \{(x,y,z) \in k^3 / -y^2 + (2x+z)y - x^2 + xz = 0\}$,
donc $S_{Q_1} \cap \{z=0\} = \{(y-x)^2 = 0\} = \{y = x\}$.
Donc finalement, le seul point à l'infini de C_Q est $\forall x \in k, \pi(x,x,0) = (1:1:0)$.

Ainsi, on peut dire que les courbes C_P et C_Q ont un point d'intersection à l'infini, qui est le point $(1:1:0)$.

IV.D Exemples de recherche de l'intersection

On reprend encore les exemples 6 et 7 et dans cette partie, on va trouver les points d'intersection entre $\gamma_P = \pi(S_{P_1})$ et $\gamma_Q = \pi(S_{Q_1})$.
Pour calculer les points d'intersection, on va calculer le résultant de P_1 et Q_1, les homogénéisés respectifs de P et Q.

Exemple 6 : Les homogénéisés de P et Q sont :
$\boxed{P_1 = Y^2 - X^2 - Z^2}$ et $\boxed{Q_1 = ZY - X^2}$

$$res_Y(P_1,Q_1)(X,Z) = \det \begin{pmatrix} 1 & Z & 0 \\ 0 & -X^2 & Z \\ -(X^2+Z^2) & 0 & -X^2 \end{pmatrix} = X^4 - Z^2(X^2+Z^2)$$

$$= X^4 - Z^2X^2 - Z^4.$$

On cherche X_1, X_2, X_3, X_4 en fonction de Z tels que
$X^4 - Z^2X^2 - Z^4 = (X-X_1)(X-X_2)(X-X_3)(X-X_4)$.
On pose $T = X^2$ tel que $T^2 - Z^2T - Z^4 = 0$.
$\Delta = 5Z^4$ donc $T = \alpha^2Z^2$ ou $T = \beta^2Z^2$ où $\beta^2 = \frac{1-\sqrt{5}}{2} < 0$, et alors $T = -b^2Z^2$, où $b^2 = -\beta^2 > 0$.
Donc on a $X_1 = \alpha Z$, $X_2 = -\alpha Z$, $X_3 = ibZ$ et $X_4 = -ibZ$.
D'où : $res_Y(P_1,Q_1)(X,Z) = (X-\alpha Z)(X+\alpha Z)(X-ibZ)(X+ibZ)$.

Ainsi, il existe d tel que $(c,d,e) \in V(P_1) \cap V(Q_1) \Leftrightarrow c = \alpha e$ ou $c = -\alpha e$ ou $c = ibe$ ou $c = -ibe$.

$*$ Si $c = \alpha e$:

$$\begin{aligned} P_1(\alpha e, d, e) = Q_1(\alpha e, d, e) = 0 &\Leftrightarrow d^2 - \alpha^2 e^2 - e^2 = 0 \text{ et } ed = \alpha^2 e^2 \\ &\Leftrightarrow d = e = 0 \text{ ou } (d = \alpha^2 e \text{ et } d^2 = (1+\alpha^2)e^2, e \neq 0) \\ &\Leftrightarrow d = e = 0 \text{ ou } (d = \alpha^2 e \text{ et } \alpha^4 e^2 = (1+\alpha^2)e^2, e \neq 0) \\ &\Leftrightarrow d = e = 0 \text{ ou } (d = \alpha^2 e,\ e \neq 0) \text{ (car } \alpha^4 = 1 + \alpha^2) \\ &\Leftrightarrow (c, d, e) = (0, 0, 0) \text{ ou } (\alpha e, \alpha^2 e, e), e \neq 0 \\ &\Leftrightarrow (c, d, e) = (\alpha e, \alpha^2 e, e). \end{aligned}$$

$*$ Si $c = -\alpha e$:

$$\begin{aligned} P_1(-\alpha e, d, e) = Q_1(-\alpha e, d, e) = 0 &\Leftrightarrow d^2 - \alpha^2 e^2 - e^2 = 0 \text{ et } ed = \alpha^2 e^2 \\ &\Leftrightarrow (c, d, e) = (-\alpha e, \alpha^2 e, e), \text{ par le même calcul.} \end{aligned}$$

$*$ Si $c = ibe$:

$$\begin{aligned} P_1(ibe, d, e) = Q_1(ibe, d, e) = 0 &\Leftrightarrow d^2 + b^2 e^2 - e^2 = 0 \text{ et } ed = -b^2 e^2 \\ &\Leftrightarrow d = e = 0 \text{ ou } (d = -b^2 e \text{ et } d^2 = (1-b^2)e^2, e \neq 0) \\ &\Leftrightarrow d = e = 0 \text{ ou } (d = b^2 e \text{ et } b^4 e^2 = (1-b^2)e^2, e \neq 0) \\ &\Leftrightarrow d = e = 0 \text{ ou } d = b^2 e \text{ (car } b^4 = 1 - b^2) \\ &\Leftrightarrow (c, d, e) = (0, 0, 0) \text{ ou } (c, d, e) = (ibe, -b^2 e, e). \end{aligned}$$

$*$ Si $c = -ibe$:

$$\begin{aligned} P_1(-ibe, d, e) = Q_1(-ibe, d, e) = 0 &\Leftrightarrow d^2 + b^2 e^2 - e^2 = 0 \text{ et } ed = -b^2 e^2 \\ &\Leftrightarrow (c, d, e) = (0, 0, 0) \text{ ou } (c, d, e) = (-ibe, -b^2 e, e), \\ &\text{par le même calcul.} \end{aligned}$$

On obtient deux intersections réelles entre γ_P et γ_Q : $(\alpha : \alpha^2 : 1)$ et $(-\alpha : \alpha^2 : 1)$ et deux intersections complexes : $(ib : -b^2 : 1)$ et $(-ib : -b^2 : 1)$.

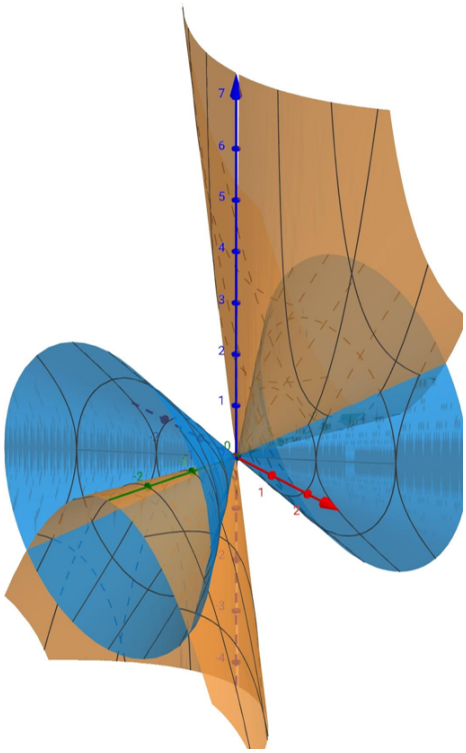

FIGURE 8 – S_{P_1} est en bleu, S_{Q_1} est en orange

Exemple 7 : Les homogénéisés de P et Q sont :
$\boxed{P_1 = Y^2 - X^2 - Z^2}$ et $\boxed{Q_1 = -Y^2 + (2X + Z)Y + XZ - X^2}$

$$res_Y(P_1, Q_1)(X, Z) = \det \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 2X+Z & -1 \\ -(X^2+Z^2) & 0 & XZ-X^2 & 2X+Z \\ 0 & -(X^2+Z^2) & 0 & XZ-X^2 \end{pmatrix}$$

$$= det \begin{pmatrix} 1 & 2X+Z & -1 \\ 0 & XZ-X^2 & 2X+Z \\ -(X^2+Z^2) & 0 & XZ-X^2 \end{pmatrix} - det \begin{pmatrix} 0 & 1 & -1 \\ -(X^2+Z^2) & 0 & 2X+Z \\ 0 & -(X^2+Z^2) & XZ-X^2 \end{pmatrix}$$

$= (XZ - X^2)^2 - (2X + Z)^2(X^2 + Z^2) - (X^2 + Z^2)(XZ - X^2) + (X^2 + Z^2)^2 - (X^2 + Z^2)(XZ - X^2)$
$= (XZ - X^2)^2 - 2(X^2 + Z^2)(XZ - X^2) - (2X + Z)^2(X^2 + Z^2) + (X^2 + Z^2)^2$
$= (XZ - X^2)^2 + (X^2 + Z^2)(-2XZ + 2X^2 - 4X^2 - 4XZ - Z^2 + X^2 + Z^2)$
$= (XZ - X^2)^2 + (X^2 + Z^2)(-6XZ - X^2)$
$= \cancel{X^2Z^2} - 2X^3Z + \cancel{X^4} - 6X^3Z - \cancel{X^4} - 6XZ^3 - \cancel{X^2Z^2}$
$= -8X^3Z - 6XZ^3$
$= -2Z^4X_1(4X_1^2 + 3)$, avec $X_1 = \frac{X}{Z}$.

Ainsi, il existe $d \in \mathbb{R}$ tel que $(c,d,e) \in V(P_1) \cap V(Q_1)$ si et seulement si $e = 0$ ou ($e \neq 0$ et $\frac{c}{e} = 0$).
$*$ Si $e = 0$:

$$\begin{aligned} P_1(c,d,0) = Q_1(c,d,0) = 0 &\Leftrightarrow d^2 = c^2 \text{ et } -d^2 + 2cd - c^2 = 0 \\ &\Leftrightarrow c = d \\ &\Leftrightarrow (c,d,e) = (c,c,0). \end{aligned}$$

$*$ Si $e \neq 0$ et $c = 0$:

$$\begin{aligned} P_1(0,d,e) = Q_1(0,d,e) = 0 &\Leftrightarrow d^2 = e^2 \text{ et } -d^2 + ed = 0 \\ &\Leftrightarrow d = \pm e \text{ et } (d = 0 \text{ ou } d = e) \\ &\Leftrightarrow d = e \\ &\Leftrightarrow (c,d,e) = (0,d,d). \end{aligned}$$

On obtient deux intersections réelles entre γ_P et γ_Q : $(1:1:0)$ et $(0:1:1)$.
Il y a deux autres points imaginaires.

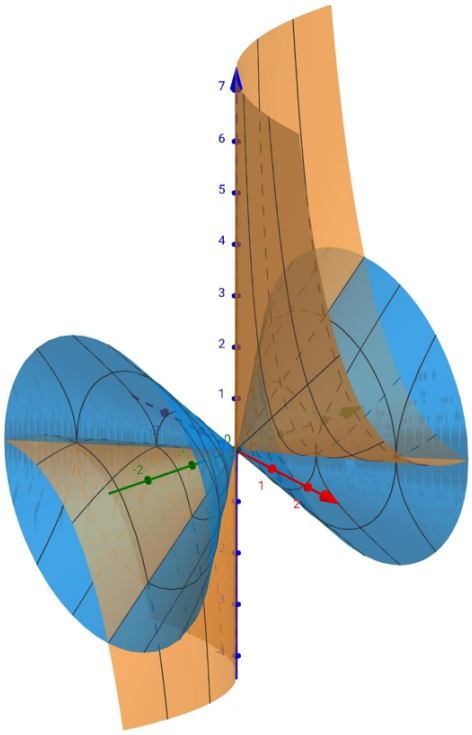

FIGURE 9 – S_{P_1} est en bleu, S_{Q_1} est en orange

IV.E Résultant de polynômes homogènes

On va montrer ici un résultat qui nous donne le degré du résultant de deux polynômes homogènes.

Théorème : Si P et Q sont des polynômes homogènes de $A[Y_0, \cdots, Y_n]$ de degrés respectifs p et q, en considérant P et Q comme des éléments de $A[Y_1, \cdots, Y_n][Y_0]$, alors $res_{Y_0}(P,Q) \in A[Y_1, \cdots, Y_n]$ est un polynôme homogène de degré pq en $Y_1, \cdots, Y_n$.

Preuve : On note $P = A_0 Y_0^p + \cdots + A_p$, où les A_i sont des polynômes de $A[Y_1, \cdots, Y_n]$ homogènes de degré i ; et $Q = B_0 Y_0^q + \cdots + B_q$, où les B_j sont des polynômes de $A[Y_1, \cdots, Y_n]$ homogènes de degré totaux j. On les note :

$$\begin{aligned} A_i(Y_1, \cdots, Y_n) &= \sum_{i_1+\cdots+i_n=i} a_{i_1,\cdots,i_n} Y_1^{i_1} \cdots Y_n^{i_n} \\ \text{et } B_j(Y_1, \cdots, Y_n) &= \sum_{j_1+\cdots+j_n=j} a_{j_1,\cdots,j_n} Y_1^{j_1} \cdots Y_n^{j_n}. \end{aligned}$$

On a alors :

$$res_{Y_0}(P,Q)(Y_1, \cdots, Y_n) = \det \begin{pmatrix} A_0 & 0 & \cdots & 0 & B_0 & 0 & \cdots & 0 \\ A_1 & \ddots & & \vdots & B_1 & \ddots & & \vdots \\ \vdots & & \ddots & 0 & \vdots & & \ddots & 0 \\ \vdots & & & A_0 & \vdots & & & B_0 \\ A_p & & & A_1 & B_q & & & B_1 \\ 0 & \ddots & & \vdots & 0 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & A_p & 0 & \cdots & 0 & B_q \end{pmatrix}.$$

On remarque que pour tout $i \in [\![0, p]\!]$ et $j \in [\![0, q]\!]$, on a :

$$\begin{aligned} A_i(TY_1, \cdots, TY_n) &= \sum_{i_1+\cdots+i_n=i} a_{i_1,\cdots,i_n} T^i Y_1^{i_1} \cdots Y_n^{i_n} \\ &= T^i A_i(Y_1, \cdots, Y_n) \\ \text{et } B_j(TY_1, \cdots, TY_n) &= \sum_{j_1+\cdots+j_n=j} a_{j_1,\cdots,j_n} T^j Y_1^{j_1} \cdots Y_n^{j_n} \\ &= T^j B_j(Y_1, \cdots, Y_n) \end{aligned}$$

et donc on a par le **Lemme général** avec le morphisme d'évaluation de $A[Y_1, \cdots, Y_n]$ dans lui-même qui à Y_i associe TY_i :

$$res_{Y_0}(P,Q)(TY_1, \cdots, TY_n) = \det \begin{pmatrix} A_0 & 0 & \cdots & 0 & B_0 & 0 & \cdots & 0 \\ TA_1 & \ddots & & \vdots & TB_1 & \ddots & & \vdots \\ \vdots & & \ddots & 0 & \vdots & & \ddots & 0 \\ \vdots & & & A_0 & \vdots & & & B_0 \\ T^pA_p & & & TA_1 & T^qB_q & & & TB_1 \\ 0 & \ddots & & \vdots & 0 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & T^pA_p & 0 & \cdots & 0 & T^qB_q \end{pmatrix}.$$

En multipliant la première colonne par T, puis la deuxième par T^2 , ... , la q-ème par T^q, et la $(q+1)$-ème par T, ... , puis la dernière par T^p et en posant $r = 1+\cdots+p+1+\cdots+q$, on obtient que :
$T^r res_{Y_0}(P,Q)(TY_1, \cdots, TY_n)$

$$= \det \begin{pmatrix} TA_0 & 0 & \cdots & 0 & TB_0 & 0 & \cdots & 0 \\ T^2A_1 & \ddots & & \vdots & T^2B_1 & \ddots & & \vdots \\ \vdots & & \ddots & 0 & \vdots & & \ddots & 0 \\ \vdots & & & T^qA_0 & \vdots & & & T^pB_0 \\ T^{p+1}A_p & & & T^{q+1}A_1 & T^{q+1}B_q & & & T^{p+1}B_1 \\ 0 & \ddots & & \vdots & 0 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & T^{p+q}A_p & 0 & \cdots & 0 & T^{p+q}B_q \end{pmatrix}.$$

et alors, on peut factoriser la ligne i par T^i. Cela donne :
$T^r res_{Y_0}(P,Q)(TY_1, \cdots, TY_n) = T^{1+\cdots+(p+q)} res_{Y_0}(P,Q)(Y_1, \cdots, Y_n)$,
d'où $res_{Y_0}(P,Q)(TY_1, \cdots, TY_n) = T^{1+\cdots+(p+q)-r} res_{Y_0}(P,Q)(Y_1, \cdots, Y_n)$
et donc $d^o_T res_{Y_0}(P,Q)(TY_1, \cdots, TY_n) = 1+\cdots+(p+q)-r = \frac{(p+q)(p+q+1)}{2} - \frac{p(p+1)}{2} - \frac{q(q+1)}{2}$
$= \frac{\cancel{p^2}+pq+\cancel{p}+pq+\cancel{q^2}+q-\cancel{p^2}-\cancel{p}-\cancel{q^2}-\cancel{q}}{2} = pq.$
Ainsi, $res_{Y_0}(P,Q)(TY_1, \cdots, TY_n) = T^{pq} res_{Y_0}(P,Q)(Y_1, \cdots, Y_n)$.
On note $res_{Y_0}(P,Q)(Y_1 \cdots, Y_n) = \sum_{k_1,\cdots,k_n} r_{k_1,\cdots,k_n} Y_1^{k_1} \cdots Y_n^{k_n}$
et donc $res_{Y_0}(P,Q)(TY_1 \cdots, TY_n) = \sum_{k_1,\cdots,k_n} r_{k_1,\cdots,k_n} T^{k_1+\cdots+k_n} Y_1^{k_1} \cdots Y_n^{k_n}$.
Et alors on a que : $\sum_{k_1,\cdots,k_n} r_{k_1,\cdots,k_n} T^{k_1+\cdots+k_n} Y_1^{k_1} \cdots Y_n^{k_n} = T^{pq} res_{Y_0}(P,Q)(Y_1, \cdots, Y_n)$,
et donc $k_1 + \cdots + k_n = pq$, donc le polynôme $res_{Y_0}(P,Q)$ est homogène de degré pq.
Alors finalement, $d^o_T res_{Y_0}(P,Q)(TY_1, \cdots, TY_n) = d^o_{Y_1,\cdots,Y_n} res_{Y_0}(P,Q)(Y_1, \cdots, Y_n) = pq$.

IV.F Changement de carte

Jusqu'ici, on a travaillé dans la carte d'équation $\{z = 1\}$, dans cette partie, on va montrer que l'on peut trouver un plan dans lequel toutes les droites vectorielles contenues dans $S_{P_1} \cap S_{Q_1}$ laissent une trace.

IV.F.1) Résultats

Lemme 1 : Soient $u_1, ..., u_s$ s vecteurs de $k^n \setminus \{0\}$, il existe un hyperplan vectoriel de k^n qui ne contient aucun d'entre eux.

Preuve : Soit $(e_1, \cdots, e_n)$ une base de k^n.
Pour tout $x \in k^n$, il existe $(x_1, \cdots, x_n) \in k^n$ tels que $x = \sum_{i=1}^n x_i e_i$.
$(e_1^*, \cdots, e_n^*)$ base de $(k^n)^*$, où :

$$\begin{aligned} e_i^* : k^n &\longrightarrow k. \\ x &\mapsto x_i \end{aligned}$$

On cherche à montrer qu'il existe $\phi \in (k^n)^*$ telle que $\forall j \in [\![1, s]\!], \phi(u_j) \neq 0$, car alors $ker(\phi)$ est un hyperplan vectoriel de k^n (car noyau d'une forme linéaire) qui ne contient aucun des u_j.
On remarque que pour $\phi \in (k^n)^*$, on a $\phi = \phi_1 e_1^* + \cdots \phi_n e_n^*$, où $\phi_i = \phi(e_i)$, et que :

$$\begin{aligned} u_j \in ker(\phi) &\Leftrightarrow \phi(u_j) = 0 \\ &\Leftrightarrow \sum_{i=1}^n e_i^*(u_j)\phi_i = 0 \\ &\Leftrightarrow P_j(\phi_1, \cdots, \phi_n) = 0, \text{ où } P_j = e_1^*(u_j)X_1 + \cdots + e_n^*(u_j)X_n \in k[X_1, \cdots, X_n]. \\ &\Leftrightarrow (\phi_1, \cdots, \phi_n) \text{ est un zéro de } P_j. \end{aligned}$$

On suppose par l'absurde que pour tout $\phi \in (k^n)^*$, il existe $j \in [\![1, s]\!]$ tel que $\phi(u_j) = 0$.
i.e. $\forall \phi \in (k^n)^*, \exists j \in [\![1, s]\!] / P_j(\phi_1, \cdots, \phi_n) = 0$.
i.e. $\forall (\phi_1, \cdots, \phi_n) \in k^n, \exists j \in [\![1, s]\!] / P_j(\phi_1, \cdots, \phi_n) = 0$.
On pose :

$$P = \prod_{j=1}^s P_j$$

et alors $\forall (\phi_1, \cdots, \phi_n) \in k^n$, on a $P(\phi_1, \cdots, \phi_n) = 0$.
Donc P est le polynôme nul car le corps k est infini.
Donc il existe $j \in [\![1, s]\!]$ tel que P_j est le polynôme nul et donc tous ses coefficients sont nuls, c'est-à-dire que $\forall i \in [\![1, n]\!], e_i^*(u_j) = 0$ donc u_j est le vecteur nul, ce qui est exclu par hypothèse.

Donc il existe un hyperplan vectoriel de k^n qui ne contient aucun des vecteurs u_j.

Lemme 2 : Une courbe projective qui ne contient pas la droite de $\mathbb{P}_2(k)$ d'équation $z = 0$ a un nombre fini de points à l'infini.

Preuve : On va prendre la courbe projective $\gamma_P = \{(x : y : z) \in \mathbb{P}_2(k)/P_1(x, y, z)\}$, où $P_1 = \sum_{i+j\leq m} a_{ij} X^i Y^j Z^{m-i-j}$ est un polynôme de $k[X, Y, Z]$ homogène de degré m.
Si on pouvait factoriser P_1 par Z, alors tous les points $(a, b, 0)$ seraient des zéros de P_1 et la courbe γ_P contiendrait la droite à l'infini, ce qui est exclu.
L'écriture de P_1 contient donc des termes $a_{ij}X^iY^j$ non nuls avec $i + j = m$.
Soit $(a : b : 0) \in \mathbb{P}_2(k)$.

$$\begin{aligned}
\text{Si } b \in k^*, \text{ alors } (a : b : 0) \in \gamma_P &\Leftrightarrow P_1(a, b, 0) = 0 \\
&\Leftrightarrow \sum_{i+j=m} a_{ij} a^i b^j = 0 \\
&\Leftrightarrow b^m \sum_{i+j=m} a_{ij} \frac{a^i}{b^i} = 0 \\
&\Leftrightarrow \frac{a}{b} \text{ est racine de } \sum_{i+j=m} a_{ij} (T)^i.
\end{aligned}$$

Ce polynôme non nul de $k[T]$ possède un nombre fini de racines.

$$\begin{aligned}
\text{Si } a \in k^*, \text{ alors } (a : b : 0) \in \gamma_P &\Leftrightarrow P_1(a, b, 0) = 0 \\
&\Leftrightarrow \sum_{i+j=m} a_{ij} a^i b^j = 0 \\
&\Leftrightarrow a^m \sum_{i+j=m} a_{ij} \frac{b^j}{a^j} = 0 \\
&\Leftrightarrow \frac{b}{a} \text{ est racine de } \sum_{i+j=m} a_{ij} (T)^i.
\end{aligned}$$

Ce polynôme non nul de $k[T]$ possède un nombre fini de racines.
Ainsi, γ_P n'a qu'un nombre fini de points à l'infini.

Lemme 3 : Soient P et Q deux polynômes de $k[X, Y]$ premiers entre eux et P_1 et Q_1 les polynômes obtenus en homogénéisant P et Q.
Il existe un plan affine H_1 de k^3 dans lequel toutes les droites vectorielles contenues dans $S_{P_1} \cap S_{Q_1}$ laissent une trace, *i.e.*$\forall v \in S_{P_1} \cap S_{Q_1}$, $vect(v) \cap H_1$ est un point.

Preuve : On remarque que $S_{P_1} \cap S_{Q_1}$ est une réunion de droites vectorielles, du fait que les polynômes P_1 et Q_1 sont homogènes.
Prenons H_0 un plan vectoriel de k^3 qui ne contient aucune des droites vectorielles contenues dans $S_{P_1} \cap S_{Q_1}$.
Dans un premier temps, on va montrer que ce plan existe.
Par le **Lemme 2**, $\gamma_P \cap \gamma_Q$ a un nombre fini de points à l'infini donc $S_{P_1} \cap S_{Q_1}$ possède un nombre fini de droites vectorielles contenues dans le plan d'équation $z = 0$.
Les autres droites vectorielles de $S_{P_1} \cap S_{Q_1}$ rencontrent le plan d'équation $z = 1$ en des points de $V(P) \cap V(Q)$ où $P = P_1(X, Y, 1)$ et $Q = Q_1(X, Y, 1)$.
Comme P et Q sont premiers entre eux dans $k[X, Y]$, le **Corollaire 4** affirme que ces points sont en nombre fini.
Ainsi, $S_{P_1} \cap S_{Q_1}$ est une réunion finie de droites vectorielles, ce qui revient à dire que $\gamma_P \cap \gamma_Q$ est un ensemble fini de points.
De plus, si H est un hyperplan vectoriel, $v \in H \setminus \{0\} \Leftrightarrow$ la droite vectorielle dirigée par v est contenue dans H.
Ainsi, par le **Lemme 1**, l'hyperplan H_0 existe.
On considère maintenant H_1 un plan affine de k^3 de direction H_0, distinct de H_0.
Alors $\forall v \in S_{P_1} \cap S_{Q_1}, vect(v) \cap H_1$ est un point.
En effet, $vect(v) \not\subset H_0$ car H_0 ne contient aucun vecteur de $S_{P_1} \cap S_{Q_1}$.
Soit f une forme linéaire sur k^3 telle que $H_0 = \ker(f)$ et $H_1 = f^{-1}(\{1\})$.
On a donc $f(v) \in k^*$ donc il existe un unique $\lambda \in k^*$ tel que $\lambda f(v) = 1$ $(= f(\lambda v))$
et donc $vect(v) \cap H_1 = \{\lambda v\}$.
Ainsi, H_1 est un plan affine de k^3 où toutes les droites vectorielles de $S_{P_1} \cap S_{Q_1}$ laissent une trace.

IV.F.2) Exemple

Nous allons considérer l'exemple des polynômes $\boxed{P = X^3 - Y^2}$ et $\boxed{Q = X - a}$, pour $a \in \mathbb{R}^*$.

$$res(P, Q)(Y) = \det \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & -a & 1 & 0 \\ 0 & 0 & -a & 1 \\ -Y^2 & 0 & 0 & -a \end{pmatrix} = -a^3 - \det \begin{pmatrix} 0 & 1 & 0 \\ 0 & -a & 1 \\ -Y^2 & 0 & -a \end{pmatrix} = Y^2 - a^3.$$

Donc $d = d_1 := a^{\frac{3}{2}}$ ou $d = d_2 := -a^{\frac{3}{2}}$.
On regarde maintenant quelles sont les valeurs possibles pour c pour que (c, d_1) soit dans $V(P) \cap V(Q)$.

$$\begin{aligned}(c,d_1)\in V(P)\cap V(Q) &\Leftrightarrow P(c,d_1)=0 \text{ et } Q(c,d_1)=0\\ &\Leftrightarrow c^3-d_1^2=0 \text{ et } c=a\\ &\Leftrightarrow c^3=a^3 \text{ et } c=a\\ &\Leftrightarrow c=a.\end{aligned}$$

Ainsi, $(a,a^{\frac{3}{2}})\in V(P)\cap V(Q)$.
On cherche maintenant les valeurs possibles pour c pour que $(c,d_2)\in V(P)\cap V(Q)$.

$$\begin{aligned}(c,d_2)\in V(P)\cap V(Q) &\Leftrightarrow P(c,d_2)=0 \text{ et } Q(c,d_2)=0\\ &\Leftrightarrow c^3-d_2^2=0 \text{ et } c=a\\ &\Leftrightarrow c^3=a^3 \text{ et } c=a\\ &\Leftrightarrow c=a.\end{aligned}$$

Donc les points d'intersection de C_P et C_Q sont $(a,a^{\frac{3}{2}})$ et $(a,-a^{\frac{3}{2}})$.
Ainsi, la carte donnée par $\{z=1\}$ n'est pas une carte dans laquelle on peut voir tous les points d'intersection.

Par le calcul général d'homogénisation, on a $P_1=X^3-Y^2Z$ et $Q_1=X-aZ$ et donc $S_{P_1}\cap\{z=0\}=(0:1:0)$ et $S_{Q_1}\cap\{z=0\}=(0:1:0)$.
Ainsi, C_P et C_Q ont un point d'intersection à l'infini : $(0:1:0)$.

On va maintenant chercher les intersections de S_{P_1} et S_{Q_1}.

$$res(P_1,Q_1)(Y,Z)=\det\begin{pmatrix}1&1&0&0\\0&-aZ&1&0\\0&0&-aZ&1\\-Y^2Z&0&0&-aZ\end{pmatrix}$$

$$=\det\begin{pmatrix}-aZ&1&0\\0&-aZ&1\\0&0&-aZ\end{pmatrix}-\det\begin{pmatrix}0&1&0\\0&-aZ&1\\-Y^2Z&0&-aZ\end{pmatrix}=Y^2Z-a^3Z^3=Z(Y^2-a^3Z^2)$$

$$=Z(Y-a^{\frac{3}{2}}Z)(Y+a^{\frac{3}{2}}Z).$$

Donc $(c,d,e)\in V(P_1)\cap V(Q_1)\Leftrightarrow e=0$ ou $d=a^{\frac{3}{2}}e$ ou $d=-a^{\frac{3}{2}}e$.

$*$ Si $e=0$: $P_1(c,d,0)=Q_1(c,d,0)=0\Leftrightarrow c=0$
et donc les $(0,d,0)$ pour $d\in\mathbb{R}$ sont des zéros communs à P_1 et Q_1.

$*$ Si $d = a^{\frac{3}{2}}e$: $P_1(c, a^{\frac{3}{2}}e, e) = Q_1(c, a^{\frac{3}{2}}e, e) = 0 \Leftrightarrow c = ae$
et donc les $(ae, a^{\frac{3}{2}}e, e)$ pour $e \in \mathbb{R}$ sont des zéros communs à P_1 et Q_1.

$*$ Si $d = -a^{\frac{3}{2}}e$: $P_1(c, -a^{\frac{3}{2}}e, e) = Q_1(c, -a^{\frac{3}{2}}e, e) = 0 \Leftrightarrow c = ae$
et donc les $(ae, -a^{\frac{3}{2}}e, e)$ pour $e \in \mathbb{R}$ sont des zéros communs à P_1 et Q_1.
Et donc $S_{P_1} \cap S_{Q_1}$ ont pour intersection $(0:1:0)$, $(a : a^{\frac{3}{2}} : 1)$ et $(a : -a^{\frac{3}{2}} : 1)$.

On introduit $H = \{y = 1\}$ et on va constater que dans cette carte-là, on voit bien les 3 points d'intersection attendus.
On a $\gamma_P \cap \gamma_Q = \Big\{(0:1:0), (a : a^{\frac{3}{2}} : 1), (a : -a^{\frac{3}{2}} : 1)\Big\}$.
Donc $S_{P_1} \cap S_{Q_1} \cap H = \Big\{(0,1,0), (a^{\frac{5}{3}}, 1, a^{\frac{2}{3}}), (-a^{\frac{5}{3}}, 1, -a^{\frac{2}{3}})\Big\}$.
On a donc trouvé une carte donnée par H dans laquelle on voit les trois points d'intersection, contrairement à ce que l'on voyait dans la carte portée par $\{z = 1\}$.

V - Conclusion

On rappelle dans un premier temps le contexte général.
k est un corps algébriquement clos. P et Q sont des polynômes de $k[X, Y]$ premiers entre eux.
On note $C_P = V(P)$ et $C_Q = V(Q)$ dans k^2.
On note m le degré total de P et n le degré total de Q.
Soient P_1 et Q_1 dans $k[X, Y, Z]$ les polynômes homogénéisés de P et Q.

$$P = \sum_{(i,j)\in\mathbb{N}^2, i+j\leq m} a_{ij}X^iY^j, \qquad P_1 = \sum_{(i,j)\in\mathbb{N}^2, i+j\leq m} a_{ij}X^iY^jZ^{m-i-j}$$
$$Q = \sum_{(i,j)\in\mathbb{N}^2, i+j\leq n} b_{ij}X^iY^j, \qquad Q_1 = \sum_{(i,j)\in\mathbb{N}^2, i+j\leq n} b_{ij}X^iY^jZ^{n-i-j}.$$

$V(P_1)$ et $V(Q_1)$ sont des surfaces de k^3 et on note $V(P_1) = S_{P_1}$ et $V(Q_1) = S_{Q_1}$.
On a : $C_P = S_{P_1} \cap \{z = 1\}$ et $C_Q = S_{Q_1} \cap \{z = 1\}$.
Les surfaces S_{P_1} et S_{Q_1} sont données par des équations homogènes.
$\forall v \in S_{P_1}, \forall \lambda \in k$, on a $\lambda v \in S_{P_1}$.
$\forall v \in S_{Q_1}, \forall \lambda \in k$, on a $\lambda v \in S_{Q_1}$.
$S_{P_1} \cap S_{Q_1}$ est réunion de droites vectorielles de k^3.
On peut donc définir deux courbes projectives γ_P et γ_Q de $\mathbb{P}_2(k)$ par :
$\gamma_P = \{(x : y : z) \in \mathbb{P}_2(k)/P_1(x, y, z) = 0\}$
$\gamma_Q = \{(x : y : z) \in \mathbb{P}_2(k)/Q_1(x, y, z) = 0\}$.

Dans la partie précédente, on a montré qu'il existait H_1 un hyperplan affine de k^3 dans lequel toutes les droites vectorielles de $S_{P_1} \cap S_{Q_1}$ laissent une trace.

Soit (v_1, v_2, v_3) une nouvelle base de k^3 avec v_1 et v_2 deux vecteurs de H_0 et v_3 un vecteur de H_1 (donc $f(v_3) = 1$), où H_0 est la direction de H_1.
On note $(\dot{x}, \dot{y}, \dot{z})$ les coordonnées des points dans cette nouvelle base (v_1, v_2, v_3) de k^3.

Soit A le point de k^3 de coordonnées $(0, 0, 1)$ dans le repère affine $(0, v_1, v_2, v_3)$ de k^3. Alors, (A, v_1, v_2) est un repère affine de H_1.

La trace de $S_{P_1} \cap S_{Q_1}$ dans H_1 est un ensemble fini de points et on a vu (dans la preuve du théorème de Bézout faible) qu'on pouvait choisir v_1 et v_2 de sorte que deux de ces points n'aient jamais la même abscisse, *i.e.* si $M = (\dot{x}, \dot{y}) \in S_{P_1} \cap S_{Q_1} \cap H_1$, alors $\forall N = (\dot{x}', \dot{y}') \in S_{P_1} \cap S_{Q_1} \cap H_1$, on a $M \neq N \Rightarrow \dot{x} \neq \dot{x}'$.

Dans cette base, S_{P_1} et S_{Q_1} ont pour équations respectives : $S_1(\dot{x}, \dot{y}, \dot{z}) = 0$
et $T_1(\dot{x}, \dot{y}, \dot{z}) = 0$, où S_1 et T_1 sont des polynômes homogènes de $k[X, Y, Z]$ de degrés respectifs m et n car le changement de coordonnées est linéaire.

On a donc $\gamma_P = \{(\dot{x} : \dot{y} : \dot{z}) \in \mathbb{P}_2(k) / S_1(\dot{x}, \dot{y}, \dot{z}) = 0\}$
et $\gamma_Q = \{(\dot{x} : \dot{y} : \dot{z}) \in \mathbb{P}_2(k) / T_1(\dot{x}, \dot{y}, \dot{z}) = 0\}$, et aucun point de $\gamma_P \cap \gamma_Q$ n'est à l'infini par rapport à la carte de $\mathbb{P}_2(k)$ donnée par H_1, *i.e.*$|\gamma_P \cap \gamma_Q| = |S_{P_1} \cap S_{Q_1} \cap H_1|$.

D'après le **Théorème II.C**, $res_Y(S_1, T_1) \in k[X, Z]$ est un polynôme homogène de degré mn.
D'après de **Lemme général**, $\forall (\dot{x}_0, \dot{z}_0) \in k^2$,
$res_Y(S_1, T_1)(\dot{x}_0, \dot{z}_0) = res_Y(S_1(\dot{x}_0, Y, \dot{z}_0), T_1(\dot{x}_0, Y, \dot{z}_0))$.
Ainsi, si $res_Y(S_1, T_1)(\dot{x}_0, \dot{z}_0) = 0$, alors $\exists \dot{y}_0 \in k / S_1(\dot{x}_0, \dot{y}_0, \dot{z}_0) = T_1(\dot{x}_0, \dot{y}_0, \dot{z}_0)$, et donc le point $(\dot{x}_0, \dot{y}_0, \dot{z}_0)$ de $\mathbb{P}_2(k)$ est dans $\gamma_P \cap \gamma_Q$, et donc $\dot{z}_0 \neq 0$.
Donc on a montré que $\forall (\dot{x}_0, \dot{z}_0) \in k^2, res_Y(S_1, T_1)(\dot{x}_0, \dot{z}_0) = 0 \Rightarrow \dot{z}_0 \neq 0$.
La contraposée donne que $\boxed{\forall \dot{x}_0 \in k, res_Y(S_1, T_1)(\dot{x}_0, 0) \neq 0}$.
En particulier, on ne peut pas factoriser $res_Y(S_1, T_1)$ par Z et donc il existe un monôme qui ne dépend que de X et donc comme $res_Y(S_1, T_1)$ est un polynôme homogène de degré mn, $\boxed{res_Y(S_1, T_1)(X, 1) \text{ est un polynôme de degré } mn}$.
Par le **Lemme général**, $res_Y(S_1, T_1)(X, 1) = res_Y(S_1(X, Y, 1), T_1(X, Y, 1))$.

On introduit les courbes $L_P = S_{P_1} \cap H_1$ et $L_Q = S_{Q_1} \cap H_1$ et alors dans le repère (A, v_1, v_2) de H_1, L_P a pour équation $S_1(\dot{x}, \dot{y}, 1) = 0$ et L_Q a pour équation $T_1(\dot{x}, \dot{y}, 1) = 0$.

On cherche dans la carte H_1 de $\mathbb{P}_2(k)$ les différents points d'intersection des courbes projectives γ_P et γ_Q, ce qui est cohérent puisque l'on sait que l'on voit tous les points de $\gamma_P \cap \gamma_Q$ dans H_1, ce sont les points de $L_P \cap L_Q$, et leurs abscisses sont les racines de $res_Y(S_1(X, Y, 1), T_1(X, Y, 1))$.
Notons $\alpha_1, \cdots, \alpha_s$ les racines de $res_Y(S_1(X, Y, 1), T_1(X, Y, 1))$.
$\gamma_P \cap \gamma_Q$ contient exactement s points d'intersection puisque par le choix du repère tous les points d'intersection ont des abscisses différentes.
Notons $\mu_1, \cdots, \mu_s$ la multiplicité de leurs abscisses comme racine de
$res_Y(S_1(X, Y, 1), T_1(X, Y, 1))$, alors on a $\boxed{\sum_{i=1}^{s} \mu_i = mn}$.
Cela est vrai pour tout choix de coordonnées adaptées à une carte de $\mathbb{P}_2(k)$ dans laquelle on voit tous les points d'intersection de γ_P et γ_Q et pour lesquelles les différents points d'intersection ont des abscisses différentes.

Références

• Joël Briançon, Philippe Maisonobe, *Éléments d'algèbre commutative*, Ellipses, 2004

• Daniel Perrin, *Résultant et discriminant*, https://www.imo.universite-paris-saclay.fr/~perrin/Sevres/resultant.pdf

• Michel Waldschmidt, *Le théorème de Bézout et le résultant de deux polynômes*, https://webusers.imj-prg.fr/~michel.waldschmidt/articles/pdf/Be%C3%8C%C2%81zoutRMS.pdf

• Claire Renard, *Géométrie projective*, 2013, https://www.normalesup.org/~crenard/geometrie-projective.pdf