Solution de Carine Apparicio et Pierre Charollois (adaptations R.Cabane).

Partie préliminaire

1°) $A[X]$ est non vide ; si P et Q sont deux éléments de $A[X]$ on voit que $P-Q$ appartient à $A[X]$. On en déduit que $(A[X],+)$ est un sous-groupe de $(K[X],+)$. On vérifie enfin que 1 appartient à $A[X]$ et que $A[X]$ est stable pour la multiplication. On peut alors conclure que $A[X]$ est un sous-anneau de $K[X]$.

2°) La matrice résultante $M=(m_{ij})$ est à coefficients dans l'anneau A ; donc

$$\mathrm{Res}_K(P,Q)=\sum_{\sigma\in S_{n+m}}\varepsilon(\sigma)m_{1,\sigma(1)}\dots m_{n+m,\sigma(n+m)}\in A\,.$$

3°) Soit $P\in\mathbb{C}[X][Y]$ i.e. $P(X,Y)=\sum\limits_{j\geqslant 0}P_j(X)Y^j$ avec $P_j(X)\in\mathbb{C}[X]$, où l'écriture est unique. Or $P_j(X)$ s'écrit de façon unique $\sum\limits_{i\geqslant 0}a_{ij}X^i$. D'où l'existence et l'unicité de l'écriture $P(X,Y)=\sum\limits_{i,j\geqslant 0}a_{i,j}X^iY^j$. L'ensemble $\{i+j\ /\ a_{i,j}\neq 0\}$ est une partie finie non vide de $\mathbb{N}$, elle a donc un plus grand élément.

Partie I : Généralités sur le résultant

1°) Si P et Q ne sont pas premiers entre eux, ils ont un facteur commun D de degré $0<d\leqslant min(n,m)$. On a alors $P=BD$ et $Q=AD$, puis $AP=ABD=BQ$ avec $\deg(A)<m$ et $\deg(B)<n$ pour A et B non nuls.

Réciproquement, supposons que $AP=BQ$, alors P et Q ne peuvent être premiers entre eux car P diviserait nécessairement B, ce qui n'est pas vu leurs degrés respectifs.

2°) a) $(1,X,\dots,X^d)$ est par nature une base de $K[X]_d$; l'espace est donc de dimension $d+1$.

b) f est clairement linéaire. Choisissons $\{(1,0),(X,0),\dots,(X^{m-1},0),(0,1),\dots,(0,X^{n-1})\}$ comme base de l'espace de départ $K[X]_{m-1}\times K[X]_{n-1}$ (par exemple en remarquant qu'elle est libre et de cardinal $m+n$), et $\{1,X,\dots,X^{n+m-1}\}$ comme base de l'espace d'arrivée. On vérifie directement que la matrice de f est alors la transposée de la matrice résultante.

3°) D'après **I2°**, l'application f est linéaire entre deux espaces vectoriels de même dimension $m+n$. Elle est donc bijective si et seulement si son noyau est réduit à $\{0\}$ i.e. si P et Q sont premiers entre eux (cf **I1°**). C'est pourquoi P et Q sont premiers si, et seulement si $\det(f)\neq 0$, d'où le résultat puisqu'une matrice et sa transposée ont même déterminant.

4°) Il suffit de l'écrire ! $R_\lambda:=\mathrm{Res}_C(\lambda^nP(\frac{X}{\lambda}),\lambda^mQ(\frac{X}{\lambda}))$ vaut :

$$\left|\begin{array}{cccccccccccc}
a_0\lambda^n & a_1\lambda^{n-1} & \cdots & & & a_{n-1}\lambda & a_n & 0 & \cdots & 0 \\
0 & a_0\lambda^n & \ddots & & & & \ddots & \ddots & & 0 \\
\vdots & \ddots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\
0 & \cdots & 0 & a_0\lambda^n & a_1\lambda^{n-1} & a_2\lambda^{n-2} & \cdots & a_{n-1}\lambda & a_n & \\
b_0\lambda^m & b_1\lambda^{m-1} & \cdots & b_{m-1}\lambda & b_m & 0 & \cdots & 0 & 0 & \\
0 & b_0\lambda^m & \ddots & & b_{m-1}\lambda & b_m & \ddots & & 0 & \\
\vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & & \vdots & \\
\vdots & & \ddots & \ddots & \ddots & & \ddots & & 0 & \\
0 & \cdots & \cdots & 0 & b_0\lambda^m & b_1\lambda^{m-1} & \cdots & b_m & &
\end{array}\right|$$

(m lignes, puis n lignes ; n colonnes, puis m colonnes)

Multiplions la colonne C_j par λ^{j-1} pour j entre 1 et $m+n$. On peut alors mettre en facteur sur la ligne L_i : λ^{n+i-1} pour les m premières lignes ($i=1\dots m$), et λ^{i-1} pour les n suivantes ($i=m+1\dots m+n$).

On trouve ainsi $\mathrm{Res}_{\mathbb{C}}(P(X),Q(X))$. Tenant compte des opérations effectuées, on obtient par multilinéarité du déterminant $R_\lambda=\lambda^\alpha\mathrm{Res}_{\mathbb{C}}(P(X),Q(X))$ avec

$$\alpha=\sum_{i=1}^{m}(n+i-1)+\sum_{i=m+1}^{m+n}(i-1)-\sum_{j=1}^{m+n}(j-1)=mn.\ \blacklozenge$$

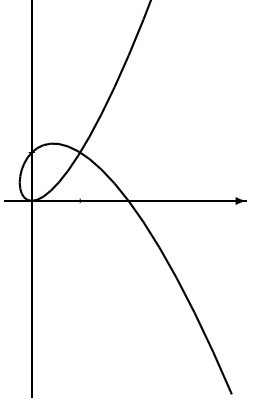
Autre méthode : on peut utiliser un changement de base.

Partie II : Une courbe unicursale

Soit $\mathcal{C}$ la courbe paramétrée par t ; $(x,y)\in\mathcal{C}$ si et seulement si les polynômes $P_x(T)=T^2+T-x$ et $Q_y(T)=T^3+2T^2-y$ ont une racine commune $t_0\in\mathbb{R}$.

Si c'est le cas, alors P_x et Q_y ne sont pas premiers entre eux, donc par **I.3** $\mathrm{Res}_{\mathbb{C}}(P_x,Q_y)=0$ où ce déterminant est de taille 5×5 car P_x est de degré 2 pour tout x, et Q_y de degré 3. On a alors éliminé t et obtenu une équation non triviale pour x et y : tous calculs faits, on obtient

$$-x^3+y^2+2x^2-xy-y=0\,.$$



Réciproquement, supposons que (x, y) vérifie l'équation cartésienne ci-dessus. D'après **I.3**, $P_x(T)$ et $Q_y(T)$ ne sont pas premiers entre eux dans $\mathbb{C}[T]$ car leur résultant est nul. Ils ont donc un pgcd $D(T) \in \mathbb{C}[T]$, en fait dans $\mathbb{R}[T]$ puisque P_x et Q_y sont réels, de degré 1 ou 2. D'où :
Cas 1. $D(T) = T - t_0$, la racine (réelle !) t_0 de D est commune à P_x et Q_y, et $(x, y) \in \mathcal{C}$.
Cas 2. $D(T)$ est de degré 2, i.e. $P_x(T)$ divise $Q_y(T)$, et le calcul mène à $x = 1, y = 1$. Mais alors P_1 et Q_1 ont deux racines communes, celles de P_1, valant $(-1 \pm \sqrt{5})/2$ donc réelles. D'où $(1, 1) \in \mathcal{C}$, c'est même l'unique point double de $\mathcal{C}$.
Remarques : ce n'est pas la seule méthode pour cette question, les degrés étant ici petits les calculs exprimant t en fonction de x puis reportant ceci dans y pouvaient être menés à la main. La calculatrice résoud aussi cette question ! Mais elle ne fait rien d'autre que de calculer $\mathrm{Res}_{\mathbb{C}}(P_x, Q_y)\ldots$

Partie III : L'anneau des entiers algébriques

1°) $P_1(X-Y) = R_0(X) + R_1(X)Y + \cdots + R_{n_1}(X)Y^{n_1}$ avec $R_i \in \mathbb{Z}[X]$, $\deg(R_i) \leqslant n_1 - i$, R_0 unitaire et $R_{n_1}(X) = (-1)^{n_1}$.
$P_2(X) = b_0 + b_1X + \ldots + b_{n_2}X^{n_2}$ avec $b_{n_2} = 1$.
On, calcule alors $S(X) = \mathrm{Res}_{\mathbb{Q}(X)}(P_1(X-Y), P_2(Y))$ qui vaut :

$$\left|\begin{array}{cccccccccc}
R_0 & R_1 & \ldots & \ldots\ldots & . & R_{n_1-1} & R_{n_1} & 0 & \ldots & \\
0 & R_0 & \ldots & . & . & . & . & . & 0 & \\
. & . & . & . & . & . & . & . & . & \\
0 & \ldots & 0 & R_0 & R_1 & R_2 & . & R_{n_1-1} & R_{n_1} & \\
b_0 & b_1 & \ldots & \ldots\ldots & b_{n_2} & 0 & \ldots\ldots & 0 & \ldots\ldots & \\
0 & b_0 & \ldots & . & . & b_{n_2} & 0 & \ldots\ldots & 0 & \\
. & . & . & . & . & . & . & . & . & \\
0 & \ldots & 0 & 0 & 0 & b_0 & b_1 & \ldots & b_{n_2} &
\end{array}\right| \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} n_2 \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} n_1 \end{array}$$

$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}_{n_1} \qquad \underbrace{\qquad\qquad\qquad}_{n_2}$$

Or, S est un polynôme à coefficients dans $\mathbb{Z}$ et si on note $(U_{i,j}(X))$ les coefficients de la matrice résultante on a

$$S(X) = \sum_{\sigma \in S_{n_1+n_2}} \varepsilon(\sigma) U(\sigma) \text{ où } U(\sigma) = U_{1,\sigma(1)} \ldots U_{n_1+n_2,\sigma(n_1+n_2)}.$$

Calculons (ou majorons) le degré des polynômes $U(\sigma)$:
$\deg(U_{i,\sigma(i)}) \leqslant n_1$ pour $1 \leqslant i \leqslant n_2$ et il y a égalité si et seulement si $\sigma(i) = i$ car les n_2 premières lignes ne font intervenir que des termes de degré au plus n_1, le degré n_1 étant obtenu si le terme se trouve sur la diagonale.
$\deg(U_{i,\sigma(i)}) \leqslant 0$ pour $i \geqslant n_2 + 1$. D'où $\deg(U(\sigma)) \leqslant n_1 n_2$. Ainsi le degré de S est inférieur ou égal a $n_1 n_2$ comme somme de polynômes de degrés inférieurs ou égaux à $n_1 n_2$.
La permutation identité donne le terme $U(id) = R_0(X)^{n_2}$ polynôme unitaire de degré $n_1 n_2$. Soit $\sigma(i) = i$ pour $i = 1 \ldots n_2$ et $\sigma \neq id$; $U(\sigma)$ comporte un terme nul provenant de la sous-matrice triangulaire inférieure est de taille (n_1, n_2) de la matrice résultante ; donc $U(\sigma) = 0$. De sorte que S est unitaire de degré $n_1 n_2$. Enfin $S(z_1 + z_2) = 0$ vu que $P_2(Y)$ et $P_1(z_1 + z_2 - Y)$ admettent z_2 comme racine commune.
2°) Vérifions que le produit de deux éléments de $\mathcal{O}$ est un élément de $\mathcal{O}$.
Soit z_1, z_2 dans $\mathcal{O}$ annulant les polynômes unitaires P_1 et P_2 de degrés respectifs n_1 et n_2. Comme P_1 est un polynôme de $\mathbb{Z}[X]$ de degré n_1, $Y^{n_1}P_1(\frac{X}{Y})$ appartient à $\mathbb{Z}[X, Y]$. Posons $\Pi(X) = \mathrm{Res}_{\mathbb{Q}(X)}(Y^{n_1}P_1(\frac{X}{Y}), P_2(Y))$; en écrivant la matrice résultante et en adaptant le raisonnement précédent, on obtient que Π est un polynôme à coefficients entiers unitaire de degré $n_1 n_2$. De plus $\Pi(z_1 z_2) = 0$ car $Y^{n_1}P_1(\frac{z_1 z_2}{Y})$ et $P_2(Y)$ ont z_2 comme racine commune.

Partie IV : Un peu de géométrie algébrique dans le plan

1°) Décomposons P_1 et Q_1 dans $\mathbb{C}(X)[Y]$ en facteurs irréductibles.
$P_1(X, Y) = X(Y - i)(Y + i)$ et $Q_1(X, Y) = (XY)^2(Y + \frac{1}{X})$. Ils n'ont pas de facteur commun, ils vérifient donc (C_1). De plus, X divise P_1 et Q_1 dans $\mathbb{C}[X][Y]$, donc P_1, Q_1 ne vérifient pas (C_2). On a $\deg(P_1) = 3, \deg(Q_1) = 5$.
Dans le deuxième exemple, ni Y ni $Y - \frac{1}{X}$ ne divisent P_2. Ainsi, P_2 et Q_2 n'ont pas de facteur commun dans $\mathbb{C}(X)[Y]$, ils vérifient (C_1). De plus, les coefficients de P_2 sont X et $X + 1$, aucun polynôme en X non constant ne peut les diviser simultanément, donc P_2, Q_2 vérifient (C_2) ; enfin, $\deg(P_2) = 3$.
$Q_3(X, Y) = P_3(X, Y)(X - Y)$. P_3 et Q_3 vérifient (C_2), pas (C_1), et leur degré respectif est 1 et 2.
2°) a) Puisque P et Q vérifient (C_1), on peut écrire une relation de Bezout : $\widetilde{A}P + \widetilde{B}Q = 1$ avec $\widetilde{A}$ et $\widetilde{B}$ dans $\mathbb{C}(X)[Y]$. En chassant les dénominateurs il vient $AP + BQ = C$ avec A et B dans $\mathbb{C}[X][Y]$ et $C \in \mathbb{C}[X]$, tous non nuls.
b) Supposons d'abord que P et Q vérifient (C_1) et (C_2). Prenons (x_0, y_0) solution du système associé. D'après **IV.2-a** on doit avoir $C(x_0) = 0$. D'où un nombre fini de x_0 possibles.
(C_2) permet d'écrire une relation de Bezout $1 = \sum A_i(X)P_i(X) + B_j(X)Q_j(X)$. Evaluant ceci en x_0, on obtient en particulier qu'au moins un des polynômes $P(x_0, Y) = \sum_{i=0}^{n} P_i(x_0)Y^i$ et $Q(x_0, Y) = \sum_{j=0}^{m} Q_j(x_0)Y^j$ n'est pas nul. Or y_0 doit être racine de ce polynôme non nul, d'où un nombre fini de possibilités pour y_0 à x_0 fixé. Au final le système a un nombre fini de solutions.

soit $x_0 \in \mathbb{C}$ une racine de D. Alors tout $(x_0, y), y \in \mathbb{C}$ est solution du système.

Enfin, si P et Q ne vérifient pas (C_1), ils ont un facteur commun $\widetilde{F}(X,Y) \in \mathbb{C}(X)[Y]$ qui n'est pas dans $\mathbb{C}(X)$. Après avoir chassé les dénominateurs on obtient des relations dans $\mathbb{C}[X][Y]$: $F(X,Y)R(X,Y) = P(X,Y)S(X)$ et $F(X,Y)T(X,Y) = Q(X,Y)U(X)$ avec S et U dans $\mathbb{C}[X]$ non nuls.

$F(X,Y) = \sum_{k=0}^{f} P_k(X)Y^k$ avec $P_f(X)$ non nul, $f \geqslant 1$. Alors pour tout $x_1 \in \mathbb{C}$ n'annulant ni S ni U ni P_f (il y en a une infinité !), le polynôme $F(x_1, Y)$ est non constant, et il a une racine $y_1 \in \mathbb{C}$. Ainsi le système a une infinité de solutions (x_1, y_1).

3°) Ecrivons $P(X,Y) = \sum_{k=0}^{\deg(P)} H_k(X,Y)$ en regroupant dans $H_k(X,Y)$ tous les termes de degré total k de P. H_k est la composante homogène de degré k de P. On écrit $H_{\deg(P)} = \sum_{i+j=\deg(P)} a_{ij}X^iY^j$ où un des a_{ij} est non nul par (0.3).

Remarquons que $(X+\alpha Y)^iY^j = \alpha^iY^{i+j} + r_{ij}(X,Y)$ où $r_{ij}(X,Y)$ est encore homogène de degré $i+j$, avec un degré partiel en $Y < i+j$, d'après la formule du binôme. Ainsi $H_{\deg(P)}(X+\alpha Y, Y) = Y^{\deg(P)} \sum_{i+j=\deg(P)} a_{ij}\alpha^i + r(X,Y)$ où ce reste r a un degré partiel en Y inférieur à $\deg(P)$.

De plus on a $\deg(H_k(X+\alpha Y, Y)) < \deg(P)$ dès que $k < \deg(P)$.

Finalement, il suffit de choisir α hors de l'ensemble fini des racines du polynôme non nul $\sum_{i+j=\deg(P)} a_{ij}Z^i$ pour s'assurer que $n = \deg(P)$. De même pour Q.

4°) On multiplie lignes et colonnes du déterminant exactement de la même manière qu'en **I.4** : la colonne C_j par z^{j-1} pour j entre 1 et $m+n$. On obtient $R(z) =$

$$\left|\begin{array}{cccccccccc}
P_0 & P_1z & \dots & \dots & \dots & P_{n-1}z^{n-1} & P_nz^n & 0 & \dots & \\
0 & P_0z & \dots & \dots & . & \dots & \dots & . & 0 & \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & . & . & \\
0 & \dots & 0 & P_oz^{m-1} & P_1z^m & \dots & \dots & P_{n-1}z^{n+m-2} & P_nz^{n+m-1} & \\
Q_0 & Q_1z & \dots & Q_{m-1}z^{m-1} & Q_mz^m & 0 & \dots & 0 & \dots & \\
0 & Q_0z & \dots & \dots & \dots & \dots & 0 & \dots & 0 & \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & . & \dots & \\
0 & \dots & 0 & 0 & 0 & Q_0z^{n-1} & Q_1z^n & \dots & Q_mz^{m+n-1} &
\end{array}\right|$$

(m lignes, puis n lignes ; n colonnes, puis m colonnes)

$P_k(X)$ est de degré au plus $n-k$, $Q_l(X)$ au plus $m-l$. On met en facteur sur les m premières lignes z^{n+i-1} (avec $i = 1 \dots m$). Les coefficients de ces lignes sont alors nuls ou du type $\frac{P_k(z)}{z^{n-k}}$, donc bornés quand $|z| \to \infty$.

On met en facteur sur les n lignes suivantes z^{i-1} $(i = m+1 \dots n+m)$, les coefficients deviennent des $\frac{Q_l(z)}{z^{m-l}}$ bornés quand $|z| \to \infty$, ou restent nuls.

Finalement, puisqu'un déterminant est polynômial en ses coefficients, on a obtenu que $R(z)/z^\alpha$ était borné quand $|z| \to \infty$, où α vaut :

$\alpha = \sum_{i=1}^{m}(n+i-1) + \sum_{i=m+1}^{m+n}(i-1) - \sum_{j=1}^{m+n}(j-1) = mn$. $R(X)$ étant un polynôme, $\frac{R(z)}{z^{mn}}$ borné converge vers 0 ou vers le coefficient dominant de R quand $|z| \to \infty$.

5°) Notons $\{(x_1,y_1),(x_2,y_2),\dots,(x_N,y_N)\}$ les solutions du système.

Effectuons de nouveau le changement linéaire bijectif déjà utilisé en **IV.3** $(x,y) \to (x+\alpha y, y)$ pour que tous ces points aient des abscisses différentes et que $n = \deg(P)$, $m = \deg(Q)$ (cette seconde condition aura son importance…).

Il suffit pour la première condition de choisir α tel que $x_i + \alpha y_i \neq x_j + \alpha y_j$, pour $i \neq j$ soit au plus N valeurs à éviter pour α ; Il reste alors à compter les x_i pour majorer N (cf figure 1 ci-dessous).

Pour réaliser en même temps la seconde condition, on a vu en **IV.3** qu'il suffisait que α évite en plus un nombre fini de valeurs.

Fixons désormais un tel α_0. On remarque que le système modifié a aussi N solutions, donc par **IV.2-b**, les polynômes modifiés vérifient encore (C_1) et (C_2). On les notera encore P et Q dans la suite.

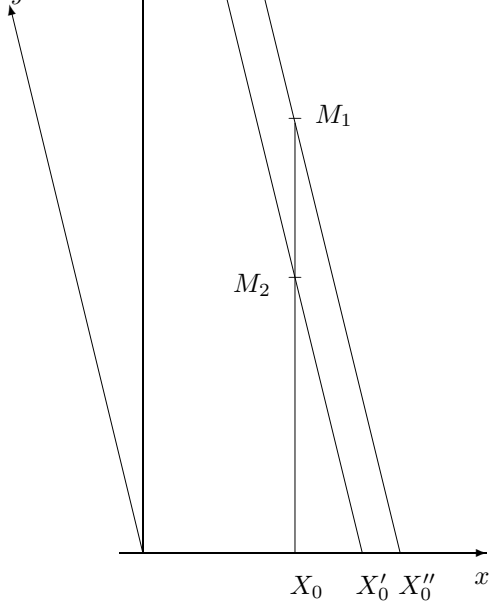


Figure 1 - *Séparation des abscisses.*

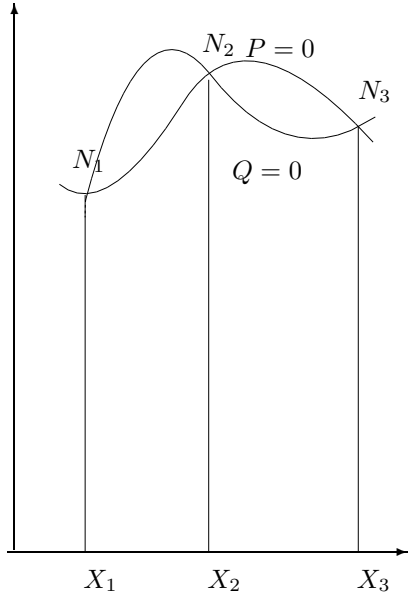


Figure 2 - *Projection des points d'intersection.*

Projetons le problème sur l'axe des abscisses (cf. figure 2) à l'aide du résultant :
Si (x_i, y_i) est solution du système alors $P(x_i, Y)$ et $Q(x_i, Y)$ ont une racine commune y_i, i.e. ne sont pas premiers entre eux. D'où $0 = \mathrm{Res}_{\mathbb{C}}(P(x_i, Y), Q(x_i, Y))$.
Attention, d'après les définitions, ce déterminant *ne vaut pas toujours* $R(x_i)$! Il est a priori de taille $\deg(P(x_i, Y)) + \deg(Q(x_i, Y))$ inférieure à $\deg(P) + \deg(Q)$. Heureusement on a pris la précaution de suivre **IV3°**, et on est assuré que même après évaluation en x_i, $P(x_i, Y)$ reste de degré $\deg(P)$ et de même $\deg(Q(x_i, Y)) = \deg(Q)$. De sorte que $\mathrm{Res}_{\mathbb{C}}(P(x_i, Y), Q(x_i, Y))$ est de taille $\deg(P) + \deg(Q)$, il vaut bel et bien $R(x_i)$.
Ainsi $R(x_i) = 0$. Or d'après **IV4°**, $R(X) \in \mathbb{C}[X]$ est de degré $\leqslant \deg(P)\deg(Q)$.
De plus, puisque P et Q vérifient (C_1), on vérifie grâce à **I3°** que R n'est pas un polynôme nul.
Finalement, R ayant au plus $\deg(P)\deg(Q)$ racines, on obtient $N \leqslant \deg(P)\deg(Q)$.
6°) Il n'y a pas toujours égalité. Choisissons $P_1(X, Y) = X - Y$ et $Q_1(X, Y) = X - Y + 1$. Ils vérifient (C_1) et (C_2) mais le système associé n'a pas de solution. Géométriquement, il s'agit de deux droites parallèles qui ne se coupent qu'à l'infini.
Prenons maintenant $P_2(X, Y) = X^2$ et $Q_2(X, Y) = Y$. Ils vérifient aussi (C_1) et (C_2). Le système associé n'a qu'une solution (0,0), alors que $\deg(P)\deg(Q) = 2$.
Cependant, on peut montrer (cf D.Perrin, Géométrie Algébrique) que si l'on se place dans le cadre projectif, et en tenant compte des multiplicités, le nombre de solutions du sytème est bien $\deg(P)\deg(Q)$ (Théorème de Bezout).