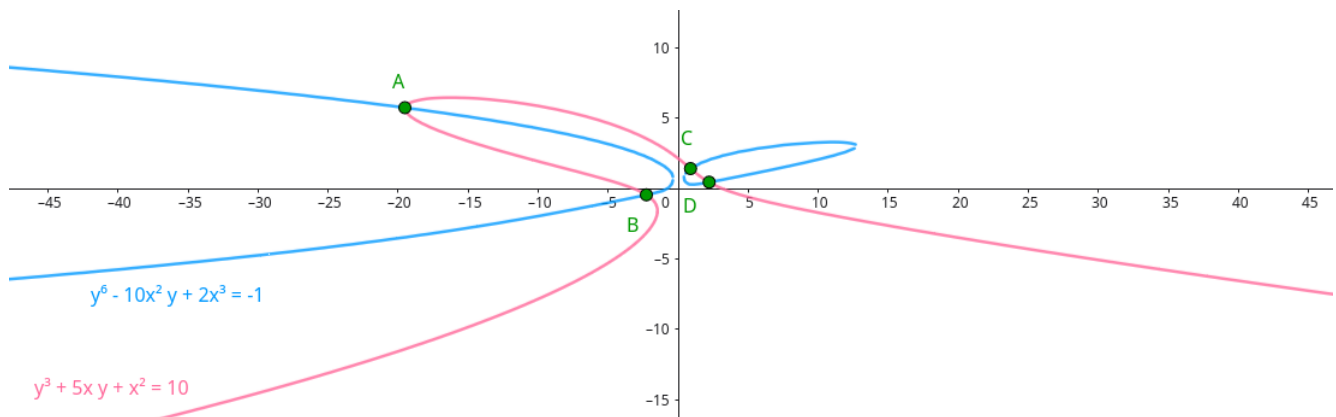


## Devoir maison n°4 ★★



|                                                                           |   |
|---------------------------------------------------------------------------|---|
| 1. Présentation du sujet .....                                            | 1 |
| 2. Structure de $\mathbf{K}$ -algèbre .....                               | 1 |
| 3. L'algèbre $\mathbf{K}[X, Y]$ des polynômes en deux indéterminées ..... | 3 |
| 4. Résultant de deux polynômes en une indéterminée .....                  | 7 |
| 5. Le théorème de Bézout sur les courbes algébriques planes .....         | 9 |

### 1. Présentation du sujet

Ce problème est consacré à l'algèbre  $\mathbf{K}[X, Y]$  des polynômes en deux indéterminées.

La première partie porte sur la définition et sur l'étude de quelques propriétés  $\mathbf{K}[X, Y]$  et plus particulièrement aux différences entre  $\mathbf{K}[X, Y]$  et  $\mathbf{K}[X]$ .

La deuxième partie est consacrée à l'étude du résultant de deux polynômes et à la démonstration d'un résultat sur les courbes paramétrées polynomiales de  $\mathbf{C}^2$ .

Enfin, la troisième partie a pour objectif la démonstration du théorème de Bézout relatif aux points d'intersection de deux courbes algébriques planes (cf. fin du document).

### 2. Structure de $\mathbf{K}$ -algèbre

Dans tout le problème,  $\mathbf{K}$  désigne un corps infini.

**Définition 1 ( $\mathbf{K}$ -algèbre).** — Soit  $A$  un ensemble muni de trois applications :

- $+_A : A \times A \longrightarrow A, (x, y) \longmapsto x +_A y$  (loi de composition interne) ;
- $\times_A : A \times A \longrightarrow A, (x, y) \longmapsto x \times_A y$  (loi de composition interne) ;
- $\cdot : \mathbf{K} \times A \longrightarrow A, (\lambda, x) \longmapsto \lambda \cdot x$  (loi de composition externe à domaine d'opérateurs dans  $\mathbf{K}$ ).

On dit que  $(A, +_A, \times_A, \cdot)$  est une  $\mathbf{K}$ -algèbre si les propriétés suivantes sont vérifiées.

(A1)  $(A, +_A, \cdot)$  est un  $\mathbf{K}$ -espace vectoriel.

(A2)  $(A, +_A, \times_A)$  est un anneau.

(A3) les trois opérations  $\times_A$ ,  $\cdot$  et  $\times_K$  vérifient la propriété de compatibilité suivante :

$$\forall (\lambda, \mu, x, y) \in K \times K \times A \times A \quad (\lambda \cdot x) \times_A (\mu \cdot y) = (\lambda \times_K \mu) \cdot (x \times_A y).$$

Les exemples de  $K$ -algèbres abondent :

- $(K, +_K, \times_K, \times_K)$ ;
- $(\mathcal{M}_n(K), +, \times, \cdot)$ , où  $n$  est un entier naturel non nul ;
- $(\mathcal{L}(E), +, \circ, \cdot)$ , où  $E$  est un  $K$ -espace vectoriel ;
- $(K[X], +, \times, \cdot)$ ;
- $(\mathcal{F}(X, K), +, \times, \cdot)$ , où  $X$  est un ensemble non vide ;

où, à chaque fois, les opérations sont les additions internes, multiplications internes et multiplications externes par un scalaire sont les lois usuelles.

**Définition 2 (sous- $K$ -algèbre).** — Soit  $(A, +, \times, \cdot)$  une  $K$ -algèbre. Une partie  $B$  de  $A$  est appelée sous- $K$ -algèbre de  $(A, +, \times, \cdot)$  si  $B$  est à la fois un sous- $K$ -espace vectoriel de  $(A, +, \cdot)$  et un sous-anneau de  $(A, +, \times)$ .

Par exemple, si  $n$  est un entier naturel supérieur ou égal à 2,  $\mathcal{T}_n^+(K)$  est une sous- $K$ -algèbre de  $(\mathcal{M}_n(K), +, \times, \cdot)$ .

Les sous- $K$ -algèbres d'une  $K$ -algèbre fournissent de nouveaux exemples de  $K$ -algèbres, comme nous l'apprend la proposition suivante.

**Proposition 3 (structure naturelle de  $K$ -algèbre sur une sous- $K$ -algèbre).** — Soient  $(A, +, \times, \cdot)$  une  $K$ -algèbre et  $B$  une sous- $K$ -algèbre de  $(A, +, \times, \cdot)$ . Alors les applications induites :

- $+_B : B \times B \longrightarrow B, (x, y) \longmapsto x +_A y$  ;
- $\times_B : B \times B \longrightarrow B, (x, y) \longmapsto x \times_A y$  ;
- $\cdot : K \times B \longrightarrow B, (\lambda, x) \longmapsto \lambda \cdot x$  ;

sont biens définies et  $(B, +_B, \times_B, \cdot_B)$  est une  $K$ -algèbre.

**Définition 4 (morphisme de  $K$ -algèbres).** — Soient  $(A_1, +_1, \times_1, \cdot_1)$  et  $(A_2, +_2, \times_2, \cdot_2)$  deux  $K$ -algèbres. Une application  $f : (A_1, +_1, \times_1, \cdot_1) \longrightarrow (A_2, +_2, \times_2, \cdot_2)$  est appelé morphisme de  $K$ -algèbres si les deux propriétés suivantes sont vérifiées :

1.  $f$  est une application  $K$ -linéaire de  $(A_1, +_1, \cdot_2)$  vers  $(A_2, +_2, \cdot_2)$  ;
2.  $f$  est un morphisme d'anneaux de  $(A_1, +_1, \times_1)$  et  $(A_2, +_2, \times_2)$ .

Par exemple, si  $n$  est un entier supérieur ou égal à 2 et  $M \in \mathcal{M}_n(\mathbf{R})$ , l'application :

$$\varphi \left| \begin{array}{l} (K[X], +, \times, \cdot) \longrightarrow (\mathcal{M}_n(\mathbf{R}), +, \times, \cdot) \\ P = \sum_{k=0}^{+\infty} a_k X^k \longmapsto P(M) := \sum_{k=0}^{+\infty} a_k M^k \end{array} \right.$$

un morphisme de  $\mathbf{R}$ -algèbres, qui joue un rôle important dans la réduction de la matrice  $M$ .

**Définition 5 (isomorphisme de  $\mathbf{K}$ -algèbres).** — Un morphisme de  $\mathbf{K}$ -algèbres qui est bijectif est appelé isomorphisme de  $\mathbf{K}$ -algèbres.

Par exemple, si  $E$  est un  $\mathbf{K}$ -espace vectoriel de dimension finie  $n \geq 1$  et  $\mathcal{B}$  est une base de  $E$ , alors : l'application :

$$\varphi \left| \begin{array}{ccc} (\mathcal{L}(E), +, \circ, \cdot) & \longrightarrow & (\mathcal{M}_n(\mathbf{K}), +, \times, \cdot) \\ u & \longmapsto & \text{Mat}_{\mathcal{B}}(u) \end{array} \right.$$

est un isomorphisme de  $\mathbf{K}$ -algèbres, qui joue un rôle clé dans l'étude des endomorphismes des espaces de dimension finie.

### 3. L'algèbre $\mathbf{K}[X, Y]$ des polynômes en deux indéterminées

Notons  $E = \mathcal{F}(\mathbf{K}^2, \mathbf{K})$  l'algèbre des applications de  $\mathbf{K}^2$  vers  $\mathbf{K}$ . Etant donné un couple  $(n, m) \in \mathbf{N}^2$ , notons  $P_{n,m}$  l'application :

$$P_{n,m} \left| \begin{array}{ccc} \mathbf{K}^2 & \longrightarrow & \mathbf{K} \\ (x, y) & \longmapsto & x^n y^m. \end{array} \right.$$

**Q1.** — Démontrer que la famille  $(P_{n,m})_{(n,m) \in \mathbf{N}^2}$  est libre dans  $E$ .

Toute partie finie de  $\mathbf{N}^2$  est incluse dans un produit cartésien  $\llbracket 0, N \rrbracket^2$ , pour un certain  $N \in \mathbf{N}$ . Il suffit donc de démontrer que pour tout  $N \in \mathbf{N}$ , la famille finie  $(P_{n,m})_{(n,m) \in \llbracket 0, N \rrbracket^2}$  est libre.

Soit  $N \in \mathbf{N}$  et soit  $(\lambda_{n,m})_{(n,m) \in \llbracket 0, N \rrbracket^2}$  une famille de scalaires telle que :

$$\sum_{n=0}^N \sum_{m=0}^N \lambda_{n,m} P_{n,m} = 0_E.$$

Alors pour tout  $(x, y) \in \mathbf{K}^2$  :

$$\sum_{n=0}^N \sum_{m=0}^N \lambda_{n,m} x^n y^m = 0_{\mathbf{K}}.$$

Soit  $y \in \mathbf{K}$  fixé. Alors :

$$\forall x \in \mathbf{K} \quad \sum_{n=0}^N \left( \sum_{m=0}^N \lambda_{n,m} y^m \right) x^n = 0_{\mathbf{K}}.$$

Comme le corps  $\mathbf{K}$  est infini, on en déduit que le polynôme :

$$\sum_{n=0}^N \left( \sum_{m=0}^N \lambda_{n,m} y^m \right) X^n$$

est nul. Ses coefficients sont donc tous nuls, i.e. :

$$\forall n \in \llbracket 0, N \rrbracket \quad \sum_{m=0}^N \lambda_{n,m} y^m = 0.$$

Soit  $n \in \llbracket 0, N \rrbracket$  fixé. D'après ce qui précède :

$$\forall y \in \mathbf{K} \quad \sum_{m=0}^N \lambda_{n,m} y^m = 0.$$

Comme le corps  $\mathbf{K}$  est infini, on en déduit que le polynôme :

$$\sum_{m=0}^N \lambda_{n,m} Y^m$$

est nul. Ses coefficients sont donc tous nuls, i.e. :

$$\forall m \in \llbracket 0, N \rrbracket \quad \lambda_{n,m} = 0.$$

Ainsi, pour tout  $(n, m) \in \llbracket 0, N \rrbracket^2$ ,  $\lambda_{n,m} = 0$ . La famille  $(P_{n,m})_{(n,m) \in \llbracket 0, N \rrbracket^2}$  est donc libre.

Le sous-espace vectoriel :

$$\text{Vect}(\{P_{n,m} : (n, m) \in \mathbf{N}^2\})$$

est noté  $\mathbf{K}[X, Y]$  et appelé espace des polynômes en deux indéterminées sur le corps  $\mathbf{K}$ .

**Q2.** — Démontrer que  $\mathbf{K}[X, Y]$  est une sous- $\mathbf{K}$ -algèbre de  $E$ .

Seule la stabilité par produit requiert une explication. Soit  $(P, Q) \in \mathbf{K}[X, Y]^2$ . Il existe deux familles de scalaires  $(\lambda_{n,m})_{(n,m) \in \mathbf{N}^2}$  et  $(\mu_{n,m})_{(n,m) \in \mathbf{N}^2}$  à supports finis telles que pour tout  $(x, y) \in \mathbf{K}^2$  :

$$P(x, y) = \sum_{(n,m) \in \mathbf{N}^2} \lambda_{n,m} x^n y^m$$

et

$$Q(x, y) = \sum_{(n,m) \in \mathbf{N}^2} \mu_{n,m} x^n y^m.$$

Pour tout  $(n, m) \in \mathbf{N}^2$ , posons  $\gamma_{n,m} = \sum_{k+l=n, p+q=m} \lambda_{k,p} \mu_{l,q}$ . Cette famille est bien définie et à support fini car, si  $N \in \mathbf{N}^*$  est tel que :

$$\text{supp}((\lambda_{n,m})_{(n,m) \in \mathbf{N}^2}) \subset \llbracket 0, N \rrbracket^2 \quad \text{et} \quad \text{supp}((\mu_{n,m})_{(n,m) \in \mathbf{N}^2}) \subset \llbracket 0, N \rrbracket^2$$

alors :

$$\text{supp}((\gamma_{n,m})_{(n,m) \in \mathbf{N}^2}) \subset \llbracket 0, 2N \rrbracket^2.$$

De plus, pour tout  $(x, y) \in \mathbf{K}^2$  :

$$(PQ)(x, y) = \sum_{(n,m) \in \mathbf{N}^2} \gamma_{n,m} x^n y^m.$$

Donc  $PQ \in \mathbf{K}[X, Y]$ .

La fonction  $P_{1,0}$  est notée  $X$  et la fonction  $P_{0,1}$  est notée  $Y$ .

Soit  $P \in \mathbf{K}[X, Y] \setminus \{0\}$ .

**Q3.** — Démontrer qu'il existe une famille de scalaires presque nulle  $(a_{k,l})_{(k,l) \in \mathbf{N}^2}$  telle que :

$$P = \sum_{(k,l) \in \mathbf{N}^2} a_{k,l} X^k Y^l.$$

Il existe une famille de scalaires presque nulle  $(a_{k,\ell})$  telle que pour tout  $(x, y) \in \mathbb{K}^2$  :

$$P(x, y) = \sum_{(k,\ell) \in \mathbb{N}^2} a_{k,\ell} x^k y^\ell = \sum_{(k,\ell) \in \mathbb{N}^2} a_{k,\ell} P_{k,0}(x, y) P_{0,\ell}(x, y) = \sum_{(k,\ell) \in \mathbb{N}^2} a_{k,\ell} P_{1,0}(x, y)^k P_{0,1}(x, y)^\ell .$$

$$\text{Donc } P = \sum_{(k,\ell) \in \mathbb{N}^2} a_{k,\ell} X^k Y^\ell .$$

**Q4.** — Démontrer que l'ensemble  $\{k + \ell : (k, \ell) \in \mathbb{N}^2 \text{ et } a_{k,\ell} \neq 0\}$  possède un élément maximum, noté  $n$ .

Cela provient du fait que  $P$  est non nul : l'ensemble en question est une partie de  $\mathbb{N}$  finie. Il est majoré puisque  $(a_{k,\ell})$  est à support fini.

On appelle alors degré de  $P$  l'entier  $n$ , que l'on notera  $\deg P$ . Si  $P = 0$ , on posera  $\deg P = -\infty$ .

Soit  $(P, Q) \in \mathbb{K}[X, Y]^2$ .

**Q5.** — Démontrer que :

$$\deg P + Q \leq \max \{ \deg P, \deg Q \} .$$

Dans quel cas y a-t-il égalité ?

- Soit  $(P, Q) \in \mathbb{K}[X, Y]^2$ . Soient  $P, Q \in \mathbb{K}[X, Y]$ , soient  $(a_{(k,\ell) \in \mathbb{N}^2})$  et  $(b_{(k,\ell) \in \mathbb{N}^2})$  des familles de scalaires à supports finis telles que :

$$P = \sum_{(k,\ell) \in \mathbb{N}^2} a_{k,\ell} X^k Y^\ell \quad \text{et} \quad Q = \sum_{(k,\ell) \in \mathbb{N}^2} b_{k,\ell} X^k Y^\ell .$$

Alors :

$$P + Q = \sum_{(k,\ell) \in \mathbb{N}^2} (a_{k,\ell} + b_{k,\ell}) X^k Y^\ell .$$

Notons  $n = \deg P$  et  $m = \deg Q$ . Supposons par exemple que  $n \leq m$ . Alors pour tout  $(k, \ell) \in \mathbb{N}^2$  tel que  $k + \ell > m$ ,  $a_{k,\ell} = b_{k,\ell} = 0$ , donc  $\deg P + Q \leq m$ .

- Il y a égalité si et seulement si  $\deg P \neq \deg Q$  ou si  $\deg P = \deg Q = n$  et s'il existe  $(k, \ell) \in \mathbb{N}^2$  tel que  $k + \ell = n$  et  $a_{k,\ell} + b_{k,\ell} \neq 0$ .

**Q6.** — Supposons  $Q \neq 0$ . Démontrer que :

$$\deg PQ = \deg P + \deg Q .$$

Si  $P = 0$ , alors l'assertion est claire. Supposons donc  $P \neq 0$  et posons  $n = \deg P$  et  $m = \deg Q$ . Ainsi :

$$P = \sum_{k,\ell \leq n} a_{k,\ell} X^k Y^\ell \quad \text{et} \quad Q = \sum_{k,\ell \leq m} b_{k,\ell} X^k Y^\ell .$$

Alors :

$$PQ = \sum_{k+\ell \leq n, i+j \leq m} a_{k,\ell} b_{i,j} X^{k+i} Y^{\ell+j} .$$

On voit que  $\deg PQ \leq nm$ .

Démontrons que cette inégalité est en fait une égalité, en introduisant :

$$k := \min \{k' \in \llbracket 0, n \rrbracket : a_{k', n-k'} \neq 0\} \quad \text{et} \quad i := \min \{i' \in \llbracket 0, m \rrbracket : b_{i', m-i'} \neq 0\}.$$

Le coefficient devant  $X^{k+i}Y^{n+m-k-i}$  est :

$$\begin{aligned} \sum_{\substack{k'+l' \leq n, i'+j' \leq m \\ k'+i'=k+i, l'+j'=n+m-k-i}} a_{k', l'} b_{i', j'} &= \sum_{\substack{k'+l'=n, i'+j'=m \\ k'+i'=k+i}} a_{k', l'} b_{i', j'} \\ &= \sum_{k'+i'=k+i} a_{k', n-k'} b_{i', m-i'} \\ &= a_{k, n-k} b_{i, m-i} \neq 0. \end{aligned}$$

En effet, si  $k' < k$  alors  $a_{k', n-k'} = 0$  et, si  $k' + i' = k + i$ ,  $k' > k$  alors  $i' < i$  et  $b_{i', m-i'} = 0$ . Ainsi  $\deg PQ = nm$ .

**Q7.** — Démontrer qu'il n'existe pas de couple  $(Q, R) \in \mathbf{K}[X, Y]^2$  tel que  $Y = XQ + R$  avec  $\deg R < \deg X$ .

Raisonnons par l'absurde et supposons donné un couple  $(Q, R)$  tel que  $Y = XQ + R$  avec  $\deg R < \deg X$ . Pour tout  $(x, y) \in \mathbf{K}^2$ ,  $y = Q(x, y)x + R(x, y)$ . Comme  $\deg X = 1$ , alors  $\deg R \leq 0$  donc  $R$  est une constante  $c \in \mathbf{K}$ . En évaluant la relation en  $(0, 0)$ , on trouve  $c = 0$ . Donc  $Y = QX$ . Ainsi,  $1 = \deg Y = \deg QX = \deg Q + 1$  donc  $\deg Q = 0$  et  $Q$  est une constante  $c' \neq 0$ . Donc pour tout  $(x, y) \in \mathbf{K}^2$ ,  $y = c'x$ . En évaluant cette égalité en  $(0, 1)$ , on trouve  $0 = c'$ , absurde.

Ainsi, la division euclidienne telle qu'on la connaît dans  $\mathbf{K}[X]$  ne se généralise pas à  $\mathbf{K}[X, Y]$ .

Soit  $(P, Q) \in \mathbf{K}[X, Y]^2$ . On dit que  $P$  divise  $Q$ , et on écrit  $P \mid Q$ , s'il existe un polynôme  $R \in \mathbf{K}[X, Y]$  tel que  $Q = PR$ . On dira que  $P$  et  $Q$  sont premiers entre eux si les seuls polynômes divisant à la fois  $P$  et  $Q$  sont les polynômes de degré 0.

**Q8.** — Démontrer que les polynômes  $X$  et  $Y$  sont premiers entre eux, mais qu'il n'existe pas de couple  $(U, V) \in \mathbf{K}[X, Y]^2$  tel que  $UX + VY = 1$ .

- Comme  $\deg X = 1$ , les seuls polynômes divisant  $X$  sont les polynômes de degré 0 et les polynômes de la forme  $\lambda X$  avec  $\lambda \neq 0$ . De même, les seuls polynômes divisant  $Y$  sont les polynômes de degré 0 et les polynômes de la forme  $\lambda Y$ , avec  $\lambda \neq 0$ . Comme  $X$  ne divise pas  $Y$  (d'après la question précédente), les seuls polynômes divisant à la fois  $X$  et  $Y$  sont les polynômes de degré 0. Donc  $X$  et  $Y$  sont premiers entre eux.
- Raisonnons par l'absurde et supposons donné un couple  $(U, V)$  tel que  $UX + VY = 1$ . En évaluant cette égalité en  $(x, y) = (0, 0)$  on trouve  $0 = 1$ , absurde.

Ainsi, le théorème de Bezout tel qu'on le connaît dans  $\mathbf{K}[X]$  ne se généralise pas tel quel aux polynômes en deux indéterminées.

#### 4. Résultant de deux polynômes en une indéterminée

Soient  $(n, m) \in \mathbf{N}^* \times \mathbf{N}^*$  et  $(A, B) \in \mathbf{K}[X]^2$  un couple de polynômes en une indéterminée tel que  $\deg A = n$  et  $\deg B = m$ . Notons  $\Phi$  l'application :

$$\Phi \left| \begin{array}{ccc} \mathbf{K}_{m-1}[X] \times \mathbf{K}_{n-1}[X] & \longrightarrow & \mathbf{K}_{n+m-1}[X] \\ (U, V) & \longmapsto & UA + VB. \end{array} \right.$$

**Q9.** — Démontrer que  $\Phi$  est bien définie et linéaire.

L'examen des degrés montre que  $f$  est bien définie. La linéarité est immédiate.

**Q10.** — Écrire la matrice de  $\Phi$  dans les bases canoniques de  $\mathbf{K}_{m-1}[X] \times \mathbf{K}_{n-1}[X]$  et  $\mathbf{K}_{n+m-1}[X]$ .

Si  $A(X) = \sum_{k=0}^n a_k X^k$  et  $B(X) = \sum_{k=0}^m b_k X^k$ . La base canonique de  $\mathbf{K}_{m-1}[X] \times \mathbf{K}_{n-1}[X]$  est :

$$((1, 0), (X, 0), \dots, (X^{m-1}, 0), (0, 1), (0, X), \dots, (0, X^{n-1})).$$

La matrice de  $\Phi$  dans les bases canoniques de  $\mathbf{K}_{m-1}[X] \times \mathbf{K}_{n-1}[X]$  se détermine à l'aide des calculs suivants :

$$\begin{aligned} \Phi(1, 0) &= A = a_0 + a_1 X + \dots + a_n X^n \\ \Phi(X, 0) &= AX = a_0 X + a_1 X^2 + \dots + a_n X^{n+1} \\ &\dots \\ \Phi(X^{m-1}, 0) &= a_0 X^{m-1} + a_1 X^m + \dots + a_n X^{n+m-1} \\ \Phi(0, 1) &= B = b_0 + b_1 X + \dots + b_m X^m \\ \Phi(0, X) &= BX = b_0 X + b_1 X^2 + \dots + b_m X^{m+1} \\ &\dots \\ \Phi(0, X^{n-1}) &= X^{n-1} B = b_0 X^{n-1} + b_1 X^n + \dots + b_m X^{n+m-1}. \end{aligned}$$

Ainsi la matrice demandée vaut :

$$\begin{pmatrix} a_0 & 0 & \dots & 0 & b_0 & 0 & \dots & \dots & \dots & \dots & 0 \\ a_1 & a_0 & & \vdots & b_1 & b_0 & & & & & \vdots \\ a_2 & a_1 & \ddots & 0 & \vdots & \vdots & \ddots & & & & \vdots \\ \vdots & \vdots & & a_0 & b_{m-1} & \vdots & & \ddots & & & \vdots \\ \vdots & \vdots & & a_1 & b_m & \vdots & & & \ddots & & \vdots \\ \vdots & \vdots & & \vdots & 0 & b_m & & & & \ddots & 0 \\ a_{n-1} & \vdots & & \vdots & 0 & 0 & \ddots & & & b_1 & b_0 \\ a_n & a_{n-1} & & a_{n-m+1} & 0 & 0 & & \ddots & & & b_1 \\ 0 & a_n & & \vdots & 0 & 0 & & & \ddots & & \vdots \\ 0 & & \ddots & \vdots & & \vdots & \vdots & & & \ddots & \vdots \\ 0 & 0 & \dots & a_n & 0 & 0 & \dots & \dots & \dots & 0 & b_m \end{pmatrix}.$$

Le déterminant de cette matrice est appelé résultant de  $A$  et  $B$ , et noté  $\text{Res}(A, B)$ .

**Q11.** — Démontrer que  $\text{Res}(A, B) \neq 0$  si et seulement si  $A$  et  $B$  sont premiers entre eux.

- On sait que  $\text{Res}(A, B) \neq 0$  si et seulement si  $\Phi$  est un isomorphisme. Montrons que  $\Phi$  est bijective si et seulement si  $A \wedge B = 1$ .
- Supposons d'abord  $\Phi$  bijective. Alors  $\Phi$  est surjective donc il existe  $(U, V) \in \mathbf{K}_{m-1}[X] \times \mathbf{K}_{n-1}[X]$  tel que  $UA + VB = 1$ . D'après le théorème de Bezout,  $A \wedge B = 1$ .
- Supposons  $A$  et  $B$  premiers entre eux. Soit  $(U, V) \in \ker(\Phi)$ . Alors  $UA = -VB$ . Comme  $A$  divise  $VB$ , par le théorème de Gauss,  $A$  divise  $V$ . Mais comme :

$$\deg V \leq n-1 < \deg A$$

il vient  $V = 0$ . Donc  $U = 0$ , et  $\Phi$  est injective. Comme  $\dim \mathbf{K}_{m-1}[X] \times \mathbf{K}_{n-1}[X] = \dim \mathbf{K}_{n+m-1}[X] = n+m$ ,  $\Phi$  est un isomorphisme.

Notons  $R$  l'application définie par :

$$R \left| \begin{array}{ccc} \mathbf{K}^2 & \longrightarrow & \mathbf{K} \\ (x, y) & \longmapsto & \text{Res}(A-x, B-y). \end{array} \right.$$

**Q12.** — Démontrer que  $R \in \mathbf{K}[X, Y]$ .

Pour tout  $(x, y) \in \mathbf{K}^2$ , on a :

$$R(x, y) = \begin{vmatrix} a_0 - x & 0 & \dots & 0 & b_0 - y & 0 & \dots & \dots & \dots & \dots & 0 \\ a_1 & a_0 - x & & \vdots & b_1 & b_0 - y & & & & & \vdots \\ a_2 & a_1 & \ddots & 0 & \vdots & \vdots & \ddots & & & & \vdots \\ \vdots & \vdots & & a_0 - x & b_{m-1} & \vdots & & \ddots & & & \vdots \\ \vdots & \vdots & & a_1 & b_m & \vdots & & \ddots & & & \vdots \\ \vdots & \vdots & & \vdots & 0 & b_m & & & \ddots & & 0 \\ a_{n-1} & \vdots & & \vdots & 0 & 0 & \ddots & & b_1 & b_0 - y & \\ a_n & a_{n-1} & & a_{n-m+1} & 0 & 0 & & \ddots & & & b_1 \\ 0 & a_n & & \vdots & 0 & 0 & & \ddots & & & \vdots \\ 0 & & \ddots & \vdots & & \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & a_n & 0 & 0 & \dots & \dots & \dots & 0 & b_m \end{vmatrix}.$$

Donc  $R(x, y)$  est obtenu comme une somme de produits de scalaires et de fonctions polynômes en  $x$  et  $y$  de degrés 1 (les fonctions  $a_0 - x$  et  $b_m - y$ ). Il s'agit donc d'une fonction polynomiale en deux variables.

**Q13.** — Supposons ici que  $\mathbf{K} = \mathbf{C}$ . Notons  $\Gamma = \{(A(z), B(z)) : z \in \mathbf{C}\}$ . Démontrer que pour tout  $(x, y) \in \mathbf{C}^2$  :

$$(x, y) \in \Gamma \iff R(x, y) = 0.$$

Ce résultat subsiste-t-il si  $\mathbf{K} = \mathbf{R}$  ?

- Soit  $(x, y) \in \mathbf{C}^2$ . Alors  $(x, y) \in \Gamma$  si et seulement s'il existe  $z \in \mathbf{C}$  tel que  $A(z) = x$  et  $B(z) = y$ , si et seulement s'il existe  $z \in \mathbf{C}$  tel que  $(A(z) - x, B(z) - y) = (0, 0)$ , si et seulement si les polynômes  $A(X) - x$  et  $B(X) - y$  ont une racine commune. Or, deux polynômes complexes ont

une racine commune si et seulement s'il ne sont pas premiers entre eux (le résultat ne subsiste pas dans  $\mathbf{R}$ ). Ainsi,  $(x, y) \in \Gamma$  si et seulement si  $R(x, y) = 0$ .

- **N.B.** : Ainsi, l'ensemble décrit en extension  $\Gamma$  peut être vu comme l'ensemble des zéros d'un polynôme en deux variables.
- Ce résultat est faux dans  $\mathbf{R}$  car des polynômes peuvent n'avoir aucune racine commune sans pour autant être premiers entre eux (par exemple :  $A(X) = X^2 + 1$  et  $B(X) = X(X^2 + 1)$  n'ont aucune racine réelle en commun mais ils ne sont pas premiers entre eux puisque leur PGCD vaut  $A$ ).

## 5. Le théorème de Bézout sur les courbes algébriques planes

Posons  $\mathbf{L} = \mathbf{K}(X)$  le corps des fractions rationnelles sur  $\mathbf{K}$ .

Alors  $\mathbf{L}[Y] = \mathbf{K}(X)[Y]$  désigne l'algèbre des polynômes sur le corps  $\mathbf{L}$ , i.e. l'algèbre des polynômes dont les coefficients sont des fractions rationnelles en  $X$ . Un élément  $P$  de  $\mathbf{L}[Y]$  est de la forme :

$$P(Y) = \sum_{k=0}^n a_k(X) Y^k$$

où les  $a_k(X)$  sont des fractions rationnelles en  $X$ .

On notera  $\mathbf{K}[X][Y]$  le sous-ensemble de  $\mathbf{L}[Y]$  constitué des polynômes de la forme :

$$P(Y) = \sum_{k=0}^n a_k(X) Y^k$$

où les  $a_k(X)$  sont des polynômes en  $X$ . L'ensemble  $\mathbf{K}[X][Y]$  est clairement muni d'une structure de  $\mathbf{K}$ -espace vectoriel.

**Q14.** — Démontrer que l'application :

$$\Theta : \left[ \sum_{k=0}^n \left( \sum_{\ell=0}^{n_k} a_{k,\ell} X^\ell \right) Y^k \right] \mapsto \sum_{k=0}^n \sum_{\ell=0}^{n_k} a_{k,\ell} X^\ell Y^k$$

est bien définie et un isomorphisme de  $\mathbf{K}$ -algèbres.

- On laisse au lecteur le soin de vérifier que  $\mathbf{K}[X][Y]$  est une sous-algèbre de  $\mathbf{L}[Y]$  et que l'application donnée est un morphisme d'algèbres (laborieux à écrire mais sans difficulté).
- L'injectivité provient de la liberté de la famille  $(X^k Y^\ell)_{(k,\ell) \in \mathbb{N}^2}$  établie dans la première question du problème, et la surjectivité provient du caractère générateur de cette famille (par définition de  $\mathbf{K}[X, Y]$ ).

Ainsi, on pourra identifier un élément de  $\mathbf{K}[X, Y]$  avec un polynôme en une variable  $Y$  dont les coefficients sont des polynômes en  $X$ .

Étant donné un polynôme :

$$P = \sum_{k=0}^n a_k(X) Y^k \in \mathbf{K}[X][Y]$$

on notera  $C_X(P)$  le PGCD des polynômes  $a_0(X), \dots, a_n(X)$ . On dit que  $C_X(P)$  est le contenu de  $P$ , et on dit que  $P$  est primitif si  $C_X(P) = 1$ , i.e. si les polynômes  $a_0(X), \dots, a_n(X)$  sont premiers entre eux.

Soit  $(P, Q) \in \mathbf{K}[X][Y]^2$ .

**Q15.** — Supposons que  $C_X(P) = C_X(Q) = 1$ . Démontrer que  $C_X(PQ) = 1$ .

Notons  $P(X) = \sum_{k=0}^n a_k(X)Y^k$  et  $Q(X) = \sum_{k=0}^m b_k(X)Y^k$ . Il existe des polynômes  $c_k(X)$ , avec  $0 \leq k \leq n+m$ , tels que :

$$PQ(X) = \sum_{k=0}^{n+m} c_k(X)Y^k.$$

Raisonnons par l'absurde et supposons qu'il existe  $R \in \mathbf{K}[X]$  irréductible non constant divisant tous les  $c_k(X)$ . Comme  $c_X(P) = 1$ ,  $R$  ne divise pas tous les coefficients de  $A$ , donc il existe  $k$  minimal tel que  $R$  ne divise pas  $a_k$ . De même, il existe  $\ell$  minimal tel que  $R$  ne divise pas  $b_\ell$ . Or :

$$c_{k+\ell}(X) = a_0 b_{k+\ell} + \dots + a_{k-1} b_{\ell+1} + a_k b_\ell + a_{k+1} b_{\ell-1} + \dots + a_{k+\ell} b_0.$$

Par minimalité de  $k$ ,  $a_0 b_{k+\ell}, \dots, a_{k-1} b_{\ell+1}$  sont divisibles par  $R$ , et par minimalité de  $\ell$ ,  $b_0 a_{k+\ell}, \dots, a_{k+1} b_{\ell-1}$  sont divisibles par  $R$ . Comme  $c_{k+\ell}$  est divisible par  $R$ , alors  $a_k b_\ell$  est divisible par  $R$ . Donc comme  $R$  est irréductible,  $R$  divise  $a_k$  ou  $R$  divise  $b_\ell$ , ce qui est absurde.

**Q16.** — Démontrer qu'en général,  $C_X(PQ) = C_X(P)C_X(Q)$ .

Soit  $P, Q \in \mathbf{K}[X][Y]$ . Posons  $\tilde{P} = \frac{P}{C_X(P)}$  et  $\tilde{Q} = \frac{Q}{C_X(Q)}$ . Alors  $c_X(\tilde{P}) = c_X(\tilde{Q}) = 1$ . Donc  $c_X(\tilde{P}\tilde{Q}) = 1$ .  
Donc :

$$c_X(PQ) = c_X(P) c_X(Q)$$

car  $c_X(\lambda P) = \lambda c_X(P)$ , si  $\lambda \in \mathbf{K}$ .

On souhaite démontrer le théorème suivant.

**Théorème 6.** — Soit  $(P, Q) \in \mathbf{K}[X, Y]^2$  deux polynômes en deux indéterminées premiers entre eux (au sens de la question 8). Il existe un polynôme  $\Delta \in \mathbf{K}[X]$  non nul et un couple  $(U, V) \in \mathbf{K}[X, Y]^2$  tels que  $UP + VQ = \Delta$ .

Les quatre questions suivantes sont consacrées à la démonstration du théorème 6. Donnons-nous donc deux polynômes  $P, Q \in \mathbf{K}[X, Y]$  premiers entre eux.

**Q17.** — On peut considérer  $P$  et  $Q$  comme des éléments de  $\mathbf{K}[X][Y]$ , donc de  $\mathbf{L}[Y]$ . Supposons  $P$  et  $Q$  premiers entre eux dans  $\mathbf{L}[Y]$ . Démontrer que le théorème ci-dessus s'en déduit.

Supposons  $P$  et  $q$  premiers entre eux dans  $\mathbf{L}[Y]$ . Comme  $\mathbf{L}$  est un corps, le théorème de Bezout s'applique et il existe  $(U, V) \in \mathbf{L}[Y]^2$  tel que  $UP + VQ = 1$ .

Il existe des polynômes  $A, B \in \mathbf{K}[X]$  tels que  $AU \in \mathbf{K}[X][Y]$  et  $BV \in \mathbf{K}[X][Y]$  (e.g.  $A$  est le PPCM des dénominateurs des coefficients de  $U$  et  $B$  est le PPCM des dénominateurs des coefficients de  $V$ ).

Posons alors  $\tilde{U} = AU$ ,  $\tilde{V} = BV$  et  $\Delta = AB$ . On a bien  $\tilde{U}P + \tilde{V}Q = \Delta$ .

On est donc ramenés à démontrer que  $P$  et  $Q$  sont premiers entre eux dans  $\mathbf{L}[Y]$ . Raisonnons par l'absurde et supposons qu'il existe un polynôme irréductible  $\tilde{D} \in \mathbf{L}[Y]$  divisant  $P$  et  $Q$  dans  $\mathbf{L}[Y]$ .

**Q18.** — Démontrer qu'il existe un polynôme  $D \in \mathbf{K}[X][Y]$ , de degré supérieur ou égal à 1, et un couple de polynômes  $(P_1, Q_1) \in \mathbf{L}[Y]^2$  tels que  $P = P_1 D$  et  $Q = Q_1 D$ .

Il existe deux polynômes  $A_1, B_1 \in \mathbf{L}[Y]$  tels que  $P = \tilde{D} A_1$  et  $Q = \tilde{D} B_1$ .

Or, il existe un polynôme  $d_1 \in \mathbf{K}[X]$  tel que  $D = d_1 \tilde{D} \in \mathbf{K}[X][Y]$ , e.g.  $d_1$  est le PPCM des dénominateurs des coefficients de  $\tilde{D}$ .

Posons  $P_1 = \frac{A_1}{d_1}$  et  $Q_1 = \frac{B_1}{d_1}$ . On a  $P = DP_1$  et  $Q = DQ_1$ .

**Q19.** — À l'aide de la question 16, démontrer que  $P_1, Q_1 \in \mathbf{K}[X][Y]$  et conclure la démonstration du théorème 6 par l'absurde.

- Quitte à diviser  $D$  par  $c_X(D)$  et multiplier  $P_1$  par  $c_X(D)$ , on peut toujours supposer que  $c_X(D) = 1$ . Il existe un polynôme  $R \in \mathbf{K}[X]$  et un polynôme  $R_1 \in \mathbf{K}[X, Y]$  tels que  $P_1 = \frac{R_1}{R(X)}$ . Alors  $R(X)P = R_1 D$ .
- Passons aux contenus. D'après Q16 :

$$R(X)c_X(P) = c_X(R_1)$$

donc  $R(X)$  divise  $R_1(X)$ . Les coefficients de  $P_1(X)$  sont donc des polynômes en  $X$  (et non simplement des fractions rationnelles), donc  $P_1(X) \in \mathbf{K}[X][Y]$ . De même, on montre que  $Q_1 \in \mathbf{K}[X][Y]$ .

- On vient de démontrer que  $P$  et  $Q$  ont un diviseur irréductible commun  $D$  dans  $\mathbf{K}[X][Y]$ . Ils ne sont donc pas premiers entre eux, ce qui est absurde. Ainsi,  $P$  et  $Q$  sont premiers entre eux dans  $\mathbf{L}[Y]$ .
- Si  $P$  et  $Q$  sont premiers entre eux dans  $\mathbf{K}[X, Y]$ , d'après ce qui précède, ils le sont aussi dans  $\mathbf{L}[Y]$ , donc d'après 127, le théorème 6 s'en déduit.
- **N.B.** Le polynôme  $\Delta$  est non nul (il est le produit des dénominateurs de deux polynômes de  $\mathbf{L}[Y]$ , cf. question Q17).

On souhaite, pour finir, démontrer une version faible du théorème de Bézout sur les courbes algébriques, dont l'énoncé précis ne nous est pas simplement accessible.

**Théorème 7 (version faible du théorème de Bézout).** — Soit  $(P, Q) \in \mathbf{K}[X, Y]^2$  un couple de polynômes en deux indéterminées. Si  $P$  et  $Q$  sont premiers entre eux, alors l'ensemble :

$$\{(x, y) \in \mathbf{K}^2 : P(x, y) = Q(x, y) = 0\}$$

est fini.

**Q20.** — Démontrer le théorème 7.

Supposons  $P$  et  $Q$  premiers entre eux. Il existe  $(U, V) \in \mathbf{K}[X, Y]^2$  et  $\Delta \in \mathbf{K}[X]$  tels que  $UP + VQ = \Delta$ . Soit alors  $(x, y) \in \mathbf{K}^2$  tel que  $P(x, y) = Q(x, y) = 0$ .

- Alors  $\Delta(x) = 0$ , donc comme  $\Delta$  est non nul,  $x$  ne peut prendre qu'un nombre fini de valeurs.

- Par symétrie du problème, on peut montrer que  $y$  ne peut prendre qu'un nombre fini de valeurs.

Ainsi :

$$\{(x, y) \in \mathbf{K}^2 : P(x, y) = Q(x, y) = 0\}$$

est fini.

**Remarque conclusive.** Le théorème de Bézout, qui parut dans le « Mémoire sur plusieurs classes d'équations de tous les degrés qui admettent une solution algébrique », publié par la revue *Histoires de l'Académie Royale des Sciences de Paris* en 1764, est plus précis. Il implique notamment que, pour tout  $P \in \mathbf{K}[X, Y]$ ,  $Q \in \mathbf{K}[X, Y]$  premiers entre eux :

$$\text{card}\left(\{(x, y) \in \mathbf{K}^2 : P(x, y) = Q(x, y) = 0\}\right) \leq \deg P \times \deg Q .$$