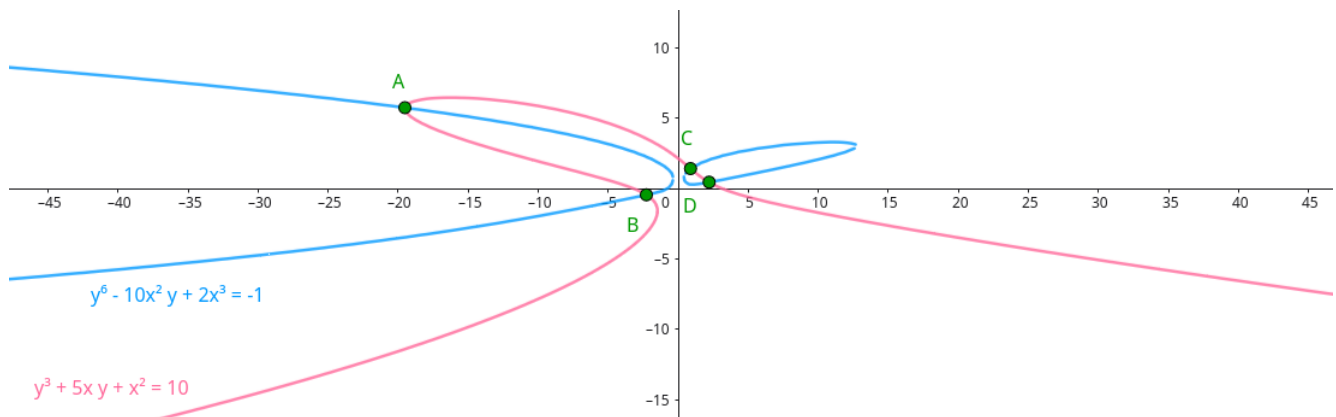


Devoir maison n°4 ★★



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	4
5. Le théorème de Bézout sur les courbes algébriques planes	4

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 $\mathbf{K}$. Étant 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 .

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 .

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 :

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

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

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

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

Q5. — Démontrer que :

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

Dans quel cas y a-t-il égalité ?

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

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

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

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 $UX + VY = 1$.

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 Φ 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 Φ est bien définie et linéaire.

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

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.

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

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 $\mathbf{K} = \mathbf{R}$?

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 :

$$\Theta \left| \begin{array}{ccc} \mathbf{K}[X][Y] & \longrightarrow & \mathbf{K}[X, Y] \\ \sum_{k=0}^n \left(\sum_{\ell=0}^{n_k} a_{k,\ell} X^\ell \right) Y^k & \longmapsto & \sum_{k=0}^n \sum_{\ell=0}^{n_k} a_{k,\ell} X^\ell Y^k \end{array} \right.$$

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

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 $C_X(PQ) = 1$.

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

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.

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 $Q = Q_1 D$.

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.

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 $(P, Q) \in \mathbb{K}[X, Y]^2$ un couple de polynômes en deux indéterminées. Si P et Q sont premiers entre eux, alors l'ensemble :

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

est fini.

Q20. — Démontrer le théorème 7.

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 $P \in \mathbb{K}[X, Y]$, $Q \in \mathbb{K}[X, Y]$ premiers entre eux :

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