ALGÈBRE GÉNÉRALE

par David Blottière, le 8 octobre 2023 à 20h05

UN CORRIGÉ

DS* N°1

Le sujet est adapté d'une épreuve posée au concours des ÉNS en 2000, en filière MP.

Le corrigé est une version légèrement remaniée d'un texte écrit par Benoît Saleur.

SOMMAIRE

§ 1. QUESTIONS DE COURS 1
§ 2. THÉORÈME DE BÉZOUT SUR LES COURBES ALGÉBRIQUES 1

§ 1. QUESTIONS DE COURS

Q1. — Énoncer le théorème de classification des groupes monogènes.

Q2. — Soit $n \in \mathbf{N}^*$. Énoncer le théorème sur les inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$, puis le démontrer.

Q3. — Énoncer le théorème des restes chinois.

Q4. — Soit $\mathbf{K}$ un corps. Énoncer le théorème décrivant les idéaux de $\mathbf{K}[X]$, puis le démontrer.

Q5. — Énoncer la formule de Leibniz dans $\mathbf{R}[X]$, puis la démontrer.

§ 2. THÉORÈME DE BÉZOUT SUR LES COURBES ALGÉBRIQUES

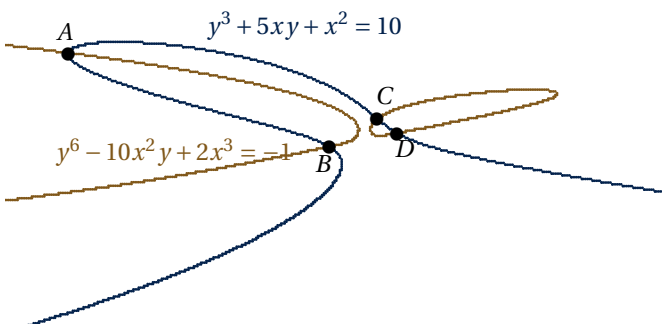
Ce problème est consacré à l'algèbre $\mathbf{K}[X,Y]$ des polynômes en deux indéterminées.

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'intersections de deux courbes algébriques planes (cf. question 26).

Illustration du théorème de Bézout : intersection de deux courbes algébriques planes



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

Partie I : L'algèbre $\mathbf{K}[X,Y]$ des polynômes en deux indéterminées

Notons $E = \mathscr{F}(\mathbf{K}^2, \mathbf{K})$ *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 :*

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

Q6. — 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 $[\![0,N]\!]^2$, pour un certain $N \in \mathbf{N}$. Il suffit donc de démontrer que pour tout $N \in \mathbf{N}$, la famille finie $\left(P_{n,m}\right)_{(n,m)\in[\![0,N]\!]^2}$ est libre.
Soit $N \in \mathbf{N}$ et soit $\left(\lambda_{n,m}\right)_{(n,m)\in[\![0,N]\!]^2}$ 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

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

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. :

$$\forall\, n \in [\![0,N]\!], \qquad \sum_{m=0}^{N} \lambda_{n,m}\, y^m = 0\,.$$

Soit $n \in [\![0,N]\!]$ fixé. D'après ce qui précède :

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

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. :

$$\forall\, m \in [\![0,N]\!], \qquad \lambda_{n,m} = 0\,.$$

Ainsi, pour tout $(n,m) \in [\![0,N]\!]^2$, $\lambda_{n,m} = 0$.La famille $\left(P_{n,m}\right)_{(n,m)\in[\![0,N]\!]^2}$ est donc libre. ■

Le sous-espace vectoriel :

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

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

Q7. — Démontrer que $\mathbf{K}[X,Y]$ est une sous algèbre de E.

Seule la stabilité par produit requiert une explication. Soit $(P,Q) \in \mathbf{K}[X,Y]^2$. Il existe deux famille $(\lambda_{n,m})_{(n,m)\in\mathbf{N}^2}$ 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 :

$$\operatorname{supp}\left((\lambda_{n,m})_{(n,m)\in\mathbf{N}^2}\right) \subset [\![0,N]\!]^2 \qquad \text{et} \qquad \operatorname{supp}\left((\mu_{n,m})_{(n,m)\in\mathbf{N}^2}\right) \subset [\![0,N]\!]^2$$

alors $\operatorname{supp}\left((\gamma_{n,m})_{(n,m)\in\mathbf{N}^2}\right) \subset [\![0,2N]\!]^2$. 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 $P \in \mathbf{K}[X,Y] \setminus \{0\}$.

Q8. — Démontrer qu'il existe une famille presque nulle $(a_{k,l})_{(k,l)\in\mathbf{N}^2}$ telle que :

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

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

$$P(x,y) = \sum_{(k,l)\in\mathbf{N}^2} a_{k,l} x^k y^l = \sum_{(k,l)\in[\![0,N]\!]^2} a_{k,l} P_{k,0}(x,y) P_{0,l}(x,y) = \sum_{(k,l)\in\mathbf{N}^2} a_{k,l} P_{1,0}(x,y)^k P_{0,1}(x,y)^l .$$

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

Q9. — Démontrer que l'ensemble $\{k+\ell \in \mathbf{N} \,:\, a_{k,\ell} \neq 0\}$ possède un élément maximum, noté n.

Cela provient du fait que P est non nul : l'ensemble en question est non vide. Il est majoré puisque $(a_{k,l})$ 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 $(P,Q) \in \mathbf{K}[X,Y]^2$.

Q10. — Démontrer que :

$$\deg(P+Q) \leqslant \max\{\deg(P), \deg(Q)\}.$$

Dans quel cas y a-t-il égalité ?

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

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

Alors :

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

Notons $n=\deg(P)$ et $m=\deg(Q)$. Supposons par exemple que $n\leqslant m$. Alors pour tout $(k,l)\in\mathbf{N}^2$ tel que $k+l>m$, $a_{k,l}=b_{k,l}=0$, donc $\deg(P+Q)\leqslant m$. Il y a égalité si et seulement si $\deg(P)\neq\deg(Q)$ ou si $\deg(P)=\deg(Q)=n$ et s'il existe $(k,l)\in\mathbf{N}^2$ tel que $k+l=n$ et $a_{k,l}+b_{k,l}\neq 0$. ■

Q11. — 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 :

$$P=\sum_{k,l\leqslant n}a_{k,l}X^kY^l\qquad\text{et}\qquad Q=\sum_{k,l\leqslant m}b_{k,l}X^kY^l\,.$$

Alors :

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

On voit que $\deg(PQ)\leqslant nm$.
Démontrons que cette inégalité est en fait une égalité, en introduisant :

$$k:=\min\left\{k'\in[\![0,n]\!]\,:\,a_{k',n-k'}\neq 0\right\}\qquad\text{et}\qquad i:=\min\left\{i'\in[\![0,m]\!]\,:\,b_{i',n-i'}\neq 0\right\}.$$

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

$$\sum_{\substack{k'+l'\leqslant n\,,\,i'+j'\leqslant m\\ k'+i'=k+i\,,\,l'+j'=n+m-k-i}}a_{k',l'}\,b_{i',j'}=\sum_{\substack{k'+l'=n\,,\,i'+j'=m\\ k'+i'=k+i}}a_{k',l'}\,b_{i',j'}=\sum_{k'+i'=k+i}a_{k',n-k'}\,b_{i',m-i'}=a_{k,n-k}b_{i,m-i}\neq 0.$$

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 $\deg(PQ)=nm$. ■

Q12. — 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 $\deg(R)\leqslant 0$ 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' non nulle. 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.

Q13. — 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 λX avec $\lambda\neq 0$. De même, les seuls polynômes divisant Y sont les polynômes de degré 0 et les polynômes de la forme λY, 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.*

Q14. — Déterminer un idéal non principal de $\mathscr{I}$ de $\mathbf{K}[X,Y]$, i.e. un idéal $\mathscr{I}$ tel qu'il n'existe pas de polynôme $A \in \mathbf{K}[X,Y]$ tel que :

$$\mathscr{I} = A\mathbf{K}[X,Y] := \left\{P \in \mathbf{K}[X,Y] \,:\, \exists Q \in \mathbf{K}[X,Y] \text{ tel que } P = AQ\right\}.$$

Considérons l'ensemble $\mathscr{I} = X\mathbf{K}[X,Y] + Y\mathbf{K}[X,Y]$. Il est aisé de vérifier que $\mathscr{I}$ est un idéal de $\mathbf{K}[X,Y]$. Raisonnons par l'absurde et supposons qu'il existe $A \in \mathbf{K}[X,Y]$ tel que $\mathscr{I} = A\mathbf{K}[X,Y]$. Comme $X \in \mathscr{I}$, il existe $P \in \mathbf{K}[X,Y]$ tel que $X = AP$, donc A divise X. De même, A divise Y, donc A est de degré 0. Comme $\mathscr{I}$est stable par la multiplication par les constante, on en déduit que $1 \in A$. Donc il existe $(U,V) \in \mathbf{K}[X,Y]^2$ tel que $1 = UX + VY$, ce qui est absurde. ■

Ainsi, les idéaux de $\mathbf{K}[X,Y]$ *ne sont pas tous principaux, contrairement aux idéaux de* $\mathbf{K}[X]$.

Partie II : Résultant de deux polynômes

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 :*

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

Q15. — Démontrer que Φ est bien définie et linéaire.

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

Q16. — Écrire la matrice de Φ dans les bases canoniques de $\mathbf{K}_{m-1}[X] \times \mathbf{K}_{n-1}[X]$ et $\mathbf{K}_{n+m-1}[X]$.

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 : $((1,0),(X,0),...,(X^{m-1},0),(0,1),(0,X),...,(0,X^{n-1}))$. La matrice de Φ dans les bases canoniques de $\mathbf{K}_{m-1}[X] \times \mathbf{K}_{n-1}[X]$ se détermine à l'aide des calculs suivants :

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

Ainsi la matrice 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 $\mathrm{Res}(A,B)$.

Q17. — Démontrer que $\mathrm{Res}(A,B)\neq 0$ si et seulement si A et B sont premiers entre eux.

On sait que $\mathrm{Res}(A,B)\neq 0$ si et seulement si Φ est un isomorphisme. Montrons que Φ est bijective si et seulement si $A\wedge B=1$.
Supposons d'abord Φ bijective. Alors Φ 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 $\deg(V)=\leqslant n-1<\deg(A)$, alors $V=0$. Donc $U=0$, et Φ est injective.
Comme $\dim(\mathbf{K}_{m-1}[X]\times\mathbf{K}_{n-1}[X])=\dim(\mathbf{K}_{n+m-1}[X])=n+m$, Φ est un isomorphisme. ■

Notons R l'application définie par :

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

Q18. — Démontrer que $R\in\mathbf{K}[X,Y]$.

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

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

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. ■

Q19. — 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 Γ 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). ■

Partie III : Le théorème de Bézout

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.*

Q20. — Démontrer que l'application :

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

est bien définie et un isomorphisme d'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 $(X^k Y^l)_{(k,l)\in\mathbf{N}^2}$ 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* <u>*contenu*</u> *de* P, *et on dit que* P *est* <u>*primitif*</u> *si* $C_X(P) = 1$, *i.e. si les polynômes* $a_0(X),\dots,a_n(X)$ *sont premiers entre eux.*

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

Q21. — 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 $0 \leqslant k \leqslant n+m$, 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 l minimal tel que R ne divise pas b_l. Or :

$$c_{k+l}(X) = a_0 b_{k+l} + \cdots + a_{k-1}b_{l+1} + a_k b_l + a_{k+1}b_{l-1} + \cdots + a_{k+l}b_0.$$

Par minimalité de k, $a_0\, b_{k+l},\dots,a_{k-1}b_{l+1}$ sont divisibles par R, et par minimalité de l, $b_0\, a_{k+l},\cdots,a_{k+1}b_{l-1}$ sont

divisibles par R. Comme c_{k+l} est divisible par R, alors $a_k b_l$ est divisible par R. Donc comme R est irréductible, R divise a_k ou R divise b_l, ce qui est absurde. ■

Q22. — Démontrer qu'en général, $C_X(PQ) = C_X(P)C_X(Q)$.

Soit $P, Q \in \mathbf{K}[X][Y]$. Posons $\widetilde{P} = \dfrac{P}{C_X(P)}$ et $\widetilde{Q} = \dfrac{Q}{C_X(Q)}$. Alors $c_X(\widetilde{P}) = c_X(\widetilde{Q}) = 1$. Donc $c_X(\widetilde{P}\widetilde{Q}) = 1$. 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 A. — *Soit $(P, Q) \in \mathbf{K}[X, Y]^2$ deux polynômes en deux indéterminées premiers entre eux (au sens de la question 12). 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 A. Donnons-nous donc deux polynômes $P, Q \in \mathbf{K}[X, Y]$ premiers entre eux.

Q23. — 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 $\widetilde{U} = AU$, $\widetilde{V} = BV$ et $\Delta = AB$. On a bien $\widetilde{U}P + \widetilde{V}Q = \Delta$. ■

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 $\widetilde{D} \in \mathbf{L}[Y]$ divisant P et Q dans $\mathbf{L}[Y]$.

Q24. — 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 $P = \widetilde{D}A_1$ et $Q = \widetilde{D}B1$.
Or, il existe in polynôme $d_1 \in \mathbf{K}[X]$ tel que $D = d_1\widetilde{D} \in \mathbf{K}[X][Y]$ (e.G. d_1 est le PPCM des dénominateurs des coefficients de $\widetilde{D}$).
Posons $P_1 = \dfrac{A_1}{d_1}$ et $P_2 = \dfrac{B_1}{d_1}$. On a $P = DP_1$ et $Q = DQ_1$. ■

Q25. — À l'aide de la question 22, démontrer que $P_1, Q_1 \in \mathbf{K}[X][Y]$ et conclure la démonstration du théorème A 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 $P_1 = \dfrac{R_1}{R(X)}$. Alors $R(X)P = R_1 D$.
Passons aux contenus. D'après Q22 :

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

donc $R(X)$ divise $R_1(X)$, donc les coefficients de $P_1(X)$ sont 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 Q23, le théorème A s'en déduit.

Remarquons que le polynôme Δ est non nul (il est le produit des dénominateurs de deux polynômes de $\mathbf{L}[Y]$, cf. question Q23). ■

On souhaite, pour finir, démontrer le théorème de Bézout sur les courbes algébriques.

THÉORÈME B (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 :*

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

est fini.

Q26. — Démontrer le théorème B.

Soient 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 Δ 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 :

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

est fini. ■

REMARQUE. — *Le théorème de Bézout (1764) est plus précis. Il implique notamment que :*

$$\mathrm{Card}\left(\left\{(x,y) \in \mathbf{K}^2 \ : \ P(x,y) = Q(x,y) = 0\right\}\right) \leqslant \deg(P) \cdot \deg(Q).$$