ALGÈBRE GÉNÉRALE

par David Blottière, le 16 septembre 2023 à 10h32

DS* N°1

3 HEURES

SOMMAIRE

§ 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

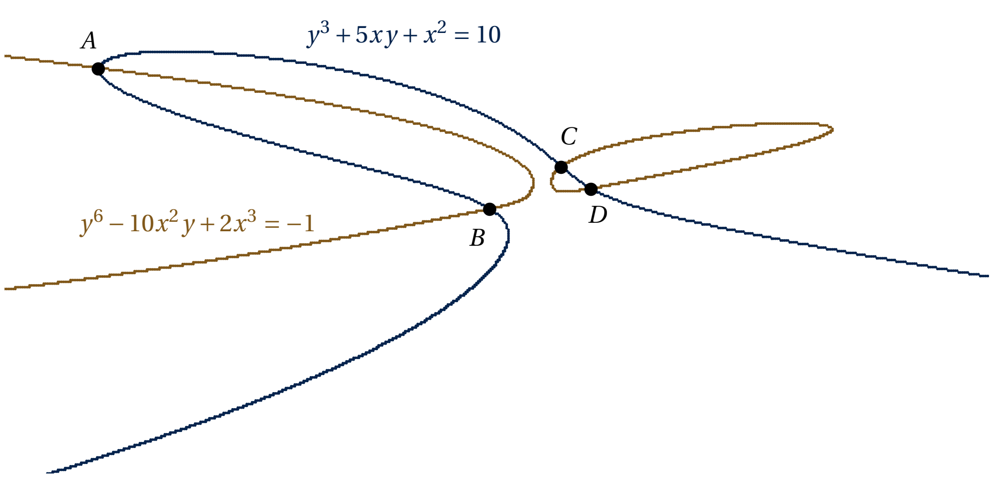
Ce problème est consacré à l'algèbre $\mathbf{K}[X, Y]$ *des polynômes en deux indéterminées.*

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.

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 <u>espace des polynômes en deux indéterminées sur le corps $\mathbf{K}$</u>.

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

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

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

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

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

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

On appelle alors <u>degré de P</u> 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 :

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

Dans quel cas y a-t-il égalité ?

Q11. — Supposons $Q \neq 0$. Démontrer que :

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

Q12. — Démontrer qu'il n'existe pas de couple $(Q,R) \in \mathbf{K}[X,Y]^2$ tel que $Y = XQ + R$ avec $\deg(R) < \deg(X)$.

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 <u>divise</u> 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 <u>premiers entre eux</u> 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 $UX + VY = 1$.

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 :

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

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.

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

Le déterminant de cette matrice est appelé <u>*résultant*</u> *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.

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

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

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.

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* $a_0(X), \ldots, a_n(X)$. *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* $a_0(X), \ldots, a_n(X)$ *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 $C_X(PQ) = 1$.

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

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.

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 $Q = Q_1 D$.

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.

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.

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

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