ENS Lyon-Cachan 2000

Les parties II, III et IV sont des applications indépendantes de la partie I. Dans la partie préliminaire ainsi que dans la première partie, K désigne un corps qui peut être quelconque. Dans les trois parties d'applications, K sera égal respectivement à $\mathbb{R}$, à $\mathbb{Q}(X)$, et enfin à $\mathbb{C}(X)$. L'anneau des polynômes à coefficients dans K sera le plus souvent noté $K[X]$ – cependant, il sera noté $K[Y]$ lorsque K sera lui même un corps de fractions rationnelles.

D'autre part, soient m, n deux entiers naturels non-nuls. Si $P(X) = \sum_{i=0}^{n} a_i X^i$ et $Q(X) = \sum_{j=0}^{m} b_j X^j$ sont deux éléments de $K[X]$ de degrés respectifs n et m, on appelle résultant de P et Q (noté $\mathrm{Res}_K(P,Q)$, ou bien $\mathrm{Res}(P,Q)$ si aucune confusion n'est possible) le déterminant de la matrice carrée à coefficients dans K de taille $(n+m, n+m)$ suivante, dite *matrice résultante* :

$$\begin{array}{c}
\left|\begin{array}{cccccccc}
a_0 & a_1 & \cdots & a_{n-1} & a_n & 0 & \cdots & 0 \\
0 & a_0 & \ddots & & \ddots & \ddots & & 0 \\
\vdots & \ddots & \ddots & \ddots & & & \ddots & \vdots \\
0 & \cdots & 0 & a_0 & a_1 & a_2 & \cdots \; a_{n-1} & a_n \\
b_0 & b_1 & \cdots & b_{m-1} & b_m & 0 & \cdots & 0 \\
0 & b_0 & \ddots & & b_{m-1} & b_m & \ddots & 0 \\
\vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\
\vdots & & \ddots & \ddots & \ddots & & \ddots & 0 \\
0 & \cdots & \cdots & 0 & b_0 & b_1 & \cdots & b_m
\end{array}\right|
\\
\underbrace{\hphantom{a_0 \quad a_1 \quad \cdots \quad a_{n-1} \quad a_n}}_{n} \quad \underbrace{\hphantom{0 \quad \cdots \quad 0 \quad b_m}}_{m}
\end{array}
\begin{array}{l}
\left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} m \\
\left.\vphantom{\begin{array}{c}b\\b\\b\\b\\b\end{array}}\right\} n \\
\vphantom{\underbrace{a}_{n}}
\end{array}$$

où chaque a_i apparait exactement m fois, et chaque b_j apparait n fois. Noter que les m premiers coefficients diagonaux sont égaux à a_0, et que les n derniers sont égaux à b_m.
Enfin, si A est un sous-anneau de K, on notera $A[X]$ le sous-anneau de l'anneau des polynômes $K[X]$, constitué des polynômes dont tous les coefficients sont dans A.

Partie préliminaire

Soit A un sous-anneau de K.

0–1- Vérifier que $A[X]$ est bien un sous anneau de $K[X]$.

0–2- Montrer que si P, Q sont deux éléments de $A[X]$, alors $\mathrm{Res}_K(P,Q)$ reste un élément de A.

0–3- Soit $\mathbb{C}[X][Y]$ le sous-anneau de l'anneau des polynômes $\mathbb{C}(X)[Y]$ sur le corps $\mathbb{C}(X)$ défini dans l'introduction pour $A = \mathbb{C}[X]$ et $K = \mathbb{C}(X)$. Montrer que tout élément P de $\mathbb{C}[X][Y]$ s'écrit de façon unique sous la forme $P(X,Y) = \sum_{i,j\geqslant 0} a_{i,j} X^i Y^j$ avec $a_{ij} \in \mathbb{C}$ nul sauf pour un nombre fini de couples (i,j). En déduire que si $P \neq 0$ est un élément de $\mathbb{C}[X][Y]$ s'écrivant comme ci-dessus, alors le nombre $d(P) = \mathrm{Max}\{i+j \ / \ a_{i,j} \neq 0\}$ est un entier naturel bien défini, appelé degré total de P.

Partie I : La propriété fondamentale du résultant.

Soient $P(X) = \sum_{i=0}^{n} a_i X^i$ et $Q(X) = \sum_{j=0}^{m} b_j X^j$ deux polynômes de $K[X]$ de degrés n et m.

I–1- Montrer que les polynômes P et Q ne sont pas premiers entre eux dans $K[X]$ si, et seulement si, il existe deux polynômes A et B non-nuls de $K[X]$, de degrés $\deg A < m$ et $\deg B < n$, tels que $AP = BQ$.

I–2- On note $K[X]_d$ le sous-espace vectoriel de $K[X]$ constitué des polynômes de degré inférieur ou égal à d.

I–2-a- Quelle est la dimension sur K de $K[X]_d$?

I–2-b- Soit f l'application

$$f : \begin{cases} K[X]_{m-1} \times K[X]_{n-1} & \to \quad K[X]_{m+n-1} \\ \qquad (A,B) & \mapsto \quad AP + BQ\,. \end{cases}$$

Montrer que f est une application linéaire, et que sa matrice dans des bases ad-hoc que l'on précisera des espaces vectoriels source et but est la transposée de la matrice résultante de l'énoncé.

I–3- Montrer que P et Q sont premiers entre eux dans $K[X]$ si, et seulement si, $\mathrm{Res}_K(P,Q) \neq 0$.

I–4- Montrer que pour tout λ non nul, on a

$$\mathrm{Res}_{\mathbb{C}}(\lambda^n P(\frac{X}{\lambda}), \lambda^m Q(\frac{X}{\lambda})) = \lambda^{mn}\,\mathrm{Res}_{\mathbb{C}}(P(X), Q(X))\,.$$

Partie II : Une courbe unicursale.

On considère la courbe plane de $\mathbb{R}^2$ paramétrée par $t \in \mathbb{R}$:

$$\begin{cases} x(t) = t^2 + t \\ y(t) = t^3 + 2t^2 \end{cases}$$

Quelle est l'équation cartésienne de la courbe dans le plan ?

Partie III : Entiers algébriques.

On note $\mathcal{O}$ l'ensemble des nombres complexes z pour lesquels il existe un polynôme non-nul $P(X) \in \mathbb{Z}[X]$ (l'anneau des polynômes à coefficients dans $\mathbb{Z}$), qui soit *unitaire* (c'est-à-dire par définition de coefficient dominant égal à 1), et vérifiant $P(z) = 0$.

III–1- Soient z_1 et z_2 des éléments de $\mathcal{O}$, annulant les polynômes P_1 et P_2 de degrés respectifs n_1 et n_2. Montrer que le polynme (en X) $\mathrm{Res}_{Q(X)}(P(X-Y), P(Y))$ est un élément de $\mathbb{Z}[X]$, unitaire de degré n_1n_2 annulant la somme $z_1 + z_2$.

III–1- Montrer que $\mathcal{O}$ est un sous-anneau de $\mathbb{C}$.

Partie IV : Équations algébriques : le théorème de Bézout faible.

On se donne deux polynômes P et Q non nuls de $\mathbb{C}[X][Y]$, et on se propose d'étudier le nombre de solutions (z_1, z_2) dans $\mathbb{C}^2$ du système d'équations

$$\begin{cases} P(z_1, z_2) = 0 \\ Q(z_1, z_2) = 0\,. \end{cases}$$

On considère les deux conditions suivantes sur P et Q :

(C_1) P et Q sont premiers entre eux dans l'anneau de polynômes $\mathbb{C}(X)[Y]$ à coefficients dans le corps $\mathbb{C}(X)$.

(C_2) En notant les dcompositions de P et Q sous la forme $P(X,Y) = \sum_{i=0}^{n} P_i(X)Y^i$ et $Q(X,Y) = \sum_{j=0}^{m} Q_j(X)Y^j$ avec $P_n(X)Q_m(X) \neq 0$ dans $\mathbb{C}[X]$, il n'y a aucun facteur non-constant commun aux $n+m+2$ polynômes

$$P_0(X), P_1(X), \dots, P_n(X), Q_0(X), \dots, Q_m(X)$$

dans l'anneau des polynômes $\mathbb{C}[X]$.

Enfin, on note $d(P)$ et $d(Q)$ les degrés totaux de P et de Q définis en 0-3-.

IV–1- Exemples. Parmi les trois couples de polynômes suivants, lesquels vérifient (C_1) ? Lesquels vérifient (C_2) ? Quels sont leurs degrés totaux ?

$$(P_1(X,Y) = XY^2 + X, \quad Q_1(X,Y) = X^2Y^3 + XY^2);$$

$$(P_2(X,Y) = XY^2 + X + 1, \quad Q_2(X,Y) = Q_1(X,Y));$$

$$(P_3(X,Y) = Y + X, \quad Q_3(X,Y) = X^2 - Y^2)\,.$$

IV-2-a- On suppose que P et Q vérifient (C_1). Montrer qu'il existe trois polynômes non nuls A, $B \in \mathbb{C}[X][Y]$, et $C \in \mathbb{C}[X]$, tels que $AP + BQ = C$.

IV-2-b- En déduire que le système étudié n'a qu'un nombre fini de solutions si, et seulement si, P et Q vérifient (C_1) et (C_2).

IV-3- Montrer que, par un changement de variables linéaire en (x, y), on peut se ramener au cas où $n = d(P)$ et $m = d(Q)$.

IV-4- On pose $R(X) = \mathrm{Res}_{\mathbb{C}(X)}(P(X,Y), Q(X,Y))$. La fonction polynômiale de $\mathbb{C}$ dans $\mathbb{C}$ associée à R sera notée $R(z)$. On suppose que $n = d(P)$ et $m = d(Q)$. Montrer que $\frac{R(z)}{z^{d(P)d(Q)}}$ admet une limite dans $\mathbb{C}$ lorsque $|z| \longrightarrow +\infty$.

IV-5- On suppose que P et Q vérifient (C_1) et (C_2). Montrer que le nombre de solutions du système est inférieur ou égal au produit $d(P)d(Q)$.

IV-6- Le système d'équations proposé a-t-il toujours $d(P)d(Q)$ solutions lorsque P et Q satisfont (C_1) et (C_2) ?