ENS Lyon et Cachan – filière MP – année 2000

(corrigé)

Préliminaires

1. Vérifier que $A[X]$ est bien un sous-anneau de $K[X]$.
2. Montrer que si P et Q sont deux éléments de $A[X]$, alors $\mathrm{Res}_K(P,Q)$ est un élément de A.
3. Soit $\mathbb{C}[X][Y]$ le sous-anneau de l'anneau des polynômes $\mathbb{C}(X)[Y]$ sur le corps $\mathbb{C}(X)$. Montrer que tout élément P de $\mathbb{C}[X][Y]$ s'écrit de façon unique sous la forme $P(X,Y)=\sum_{i,j\geqslant 0} a_{i,j}X^iY^j$ avec $a_{i,j}\in\mathbb{C}$ 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 $d(P)=\max\{i+j \mid a_{i,j}\neq 0\}$ est un entier naturel bien défini, appelé *degré total* de P.

Partie I – la propriété fondamentale du résultant

4. Montrer que 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 : $AP=BQ$.
5. Quelle est la dimension sur K de $K[X]_d$?
6. Soit f l'application :
$$f:\begin{cases} K[X]_{m-1}\times K[X]_{n-1} & \to & K[X]_{m+n-1} \\ (A,B) & \mapsto & AP+BQ \end{cases}.$$
   Montrer que f est une application linéaire, et que sa matrice dans des bases *ad hoc* que l'on précisera est la transposée de la matrice résultante de l'énoncé.
7. Montrer que P et Q sont premiers entre eux dans $K[X]$ si et seulement si : $\mathrm{Res}_K(P,Q)\neq 0$.
8. Montrer que pour tout $\lambda\in K$ non nul, on a :
$$\mathrm{Res}_K\left(\lambda^n P\left(\frac{X}{\lambda}\right),\lambda^m Q\left(\frac{X}{\lambda}\right)\right)=\lambda^{mn}\mathrm{Res}_K(P(X),Q(X)).$$

Partie II – une courbe unicursale

9. Soient $(x,y)\in\mathbb{R}^2$ et $\mathscr{C}$ le support de la courbe paramétrée par $t\mapsto(t^2+t,t^3+2t^2)$. Posons $P_x=X^2+X-x$ et $Q_y=X^3+2X^2-y$. Alors :
$$\begin{aligned}(x,y)\in\mathscr{C} &\iff \exists t_0\in\mathbb{R},\quad x=t_0^2+t_0,\quad y=t_0^3+2t_0^2\\ &\iff \exists t_0\in\mathbb{R},\quad P_x(t_0)=Q_y(t_0)=0\\ &\iff \exists t_0\in\mathbb{R},\quad X-t_0\mid P_x,\quad X-t_0\mid Q_y\\ &\implies \mathrm{pgcd}(P_x,Q_y)\neq 1 \qquad (*)\\ &\iff \mathrm{Res}\,(P_x,Q_y)=0. \qquad (q.7)\end{aligned}$$
   Or on trouve après calculs (faire $L_5\leftarrow L_5-L_3$, développer par rapport à la dernière colonne, recommencer) :
$$\mathrm{Res}\,(P_x,Q_y)=\begin{vmatrix}-x&1&1&0&0\\0&-x&1&1&0\\0&0&-x&1&1\\-y&0&2&1&0\\0&-y&0&2&1\end{vmatrix}=\begin{vmatrix}-x&1&1&0\\0&-x&1&1\\-y&0&2&1\\0&-y&x&1\end{vmatrix}$$

$$
\begin{aligned}
&= \begin{vmatrix} -x & 1 & 1 & 0 \\ 0 & -x & 1 & 1 \\ -y & x & 1 & 0 \\ 0 & x-y & x-1 & 0 \end{vmatrix} \\
&= \begin{vmatrix} -x & 1 & 1 \\ -y & x & 1 \\ 0 & x-y & x-1 \end{vmatrix} \\
&= \begin{vmatrix} -x & 1 & 1 \\ x-y & x-1 & 0 \\ x(x-1) & x-y-(x-1) & 0 \end{vmatrix} \\
&= \Big((x-y)^2 - (x-y)(x-1)\Big) - x(x-1)^2 \\
&= -x^3 + y^2 + 2x^2 - xy - y,
\end{aligned}
$$

donc finalement :

$$(x,y) \in \mathscr{C} \Longrightarrow -x^3 + y^2 + 2x^2 - xy - y = 0.$$

Pour montrer l'implication réciproque, il suffit de remonter ce raisonnement ; seule l'implication réciproque $(*)$ nous manque. Justifions-la.

Supposons : $\operatorname{pgcd}(P_x, Q_y) \neq 1$. Notons $D \in \mathbb{R}[X]$ ce pgcd. Comme il divise P_x en particulier, il est de degré 1 ou 2. S'il est de degré 1, alors il est de la forme $D = X - a$ avec $a \in \mathbb{R}$ et $X - a$ divise donc P_x et Q_y, ce qui démontre l'implication réciproque de $(*)$. S'il est de degré 2, alors le fait qu'il divise P_x (lui aussi de degré 2) implique que D et P_x sont associés ; comme ils sont tous les deux unitaires, on a : $D = P_x$, et donc P_x divise Q_y. Faisons une division euclidienne de Q_y par P_x pour voir à quelle condition sur x et y c'est vérifié :

$$
\begin{array}{l|l}
X^3 + 2X^2 - y & X^2 + X - x \\
\cline{2-2}
-(X^3 + X^2 - xX) & X + 1 \\
\cline{1-1}
X^2 + xX - y & \\
-(X^2 + X - x) & \\
\cline{1-1}
(x-1)X + x - y &
\end{array}
$$

donc : $Q_y = (X+1)P_x + (x-1)X + x - y$. Or P_x divise Q_y, donc le reste dans cette division euclidienne est nul, c'est-à-dire : $x - 1 = 0$, et : $x - y = 0$. En bref, on est dans le cas : $x = y = 1$. Le discriminant de P_1 est égal à 5 et il admet donc pour racine $t_0 = \frac{-1+\sqrt{5}}{2}$ (peu importe ce que vaut l'autre racine). Ainsi t_0 est une racine commune à P_1 et Q_1, donc $(x,y) = (1,1) \in \mathscr{C}$ par les équivalences ci-dessus : ceci achève de démontrer l'implication réciproque.

En conclusion :

$$(x,y) \in \mathscr{C} \Longleftrightarrow -x^3 + y^2 + 2x^2 - xy - y = 0.$$

Partie III – entiers algébriques

10. Posons : $P_1 = \sum_{i=0}^{n_1} a_i X^i$, et : $P_2 = \sum_{j=0}^{n_2} b_j X^j$, avec les a_i et b_j entiers, ainsi que $a_{n_1} = b_{n_2} = 1$ (suivant la définition d'un entier algébrique, on peut prendre P_1 et P_2 ainsi). On a alors :

$$P_1(X-Y) = \sum_{i=0}^{n_1} a_i (X-Y)^i = \sum_{i=0}^{n_1} \sum_{k=0}^{i} a_i \binom{i}{k} X^{i-k} (-1)^k Y^k = \sum_{k=0}^{n_1} \left(\sum_{i=k}^{n_1} (-1)^k a_i \binom{i}{k} X^{i-k} \right) Y^k,$$

donc : $P_1 = \sum_{k=0}^{n_1} Q_k(X)Y^k$, avec :

$$\forall k \in [\![0, n_1]\!], \quad Q_k(X) = (-1)^k \sum_{i=k}^{n_1} a_i \binom{i}{k} X^{i-k} = (-1)^k \sum_{i=0}^{n_1-k} a_{i+k} \binom{i+k}{k} X^i. \qquad (*)$$

Comme les coefficients binomiaux et les a_{i+k} sont des entiers, on a $Q_k(X) \in \mathbb{Z}[X]$ pour tout $k \in [\![0, n_1]\!]$, donc $P_1(X-Y)$ est dans $\mathbb{Z}[X][Y]$. On voit de plus directement que $P_2(Y)$ est dans $\mathbb{Z}[Y]$, donc dans $\mathbb{Z}[X][Y]$. Par la question 2, le résultant $S = \mathrm{Res}_{\mathbb{Q}(X)}(P_1(X-Y), P_2(Y))$ est dans $\mathbb{Z}[X]$. Il reste à montrer qu'il est unitaire, de degré n_1n_2, et qu'il annule z_1+z_2. Ce dernier résultat découle immédiatement de la question 7, puisque :

$$S(z_1+z_2) = 0 \iff \mathrm{pgcd}(P_1(z_1+z_2-Y), P_2(Y)) \neq 1,$$

et ces deux polynômes ne sont pas premiers entre eux puisqu'ils possèdent z_2 comme racine commune : $P_1(z_1+z_2-z_2) = P_1(z_1) = 0$, et : $P_2(z_2) = 0$. Ils sont donc tous les deux divisibles par $X - z_2$, d'où le résultat. Ainsi S admet z_1+z_2 pour racine.

Montrons enfin qu'il est unitaire et de degré n_1n_2. Pour cela, rappelons que S est le déterminant suivant (on se souvient que $b_{n_2} = 1$) :

$$\begin{vmatrix}
\overbrace{\begin{matrix} Q_0 & Q_1 & Q_2 & \cdots & \cdots & \cdots & Q_{n_1-1} \\ 0 & Q_0 & Q_1 & Q_2 & \cdots & \cdots & \cdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & & \\ 0 & \cdots & 0 & Q_0 & Q_1 & Q_2 & \cdots \end{matrix}}^{n_1}
\overbrace{\begin{matrix} Q_{n_1} & 0 & \cdots & 0 \\ Q_{n_1-1} & Q_{n_1} & \ddots & \vdots \\ & \ddots & \ddots & \vdots \\ \cdots & \cdots & Q_{n_1-1} & Q_{n_1} \end{matrix}}^{n_2} \right\} n_2 \\
\begin{matrix} b_0 & b_1 & \cdots & b_{n_2-1} & 1 & 0 & \cdots \\ 0 & b_0 & b_1 & \cdots & b_{n_2-1} & 1 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ \vdots & & \ddots & \ddots & \ddots & \ddots & \ddots \\ \vdots & & & \ddots & \ddots & \ddots & \ddots \\ \vdots & & & & \ddots & \ddots & \ddots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & b_0 \end{matrix}
\begin{matrix} \cdots & \cdots & \cdots & 0 \\ & & & \vdots \\ \ddots & & & \vdots \\ \ddots & \ddots & & \vdots \\ \ddots & \ddots & \ddots & \vdots \\ \ddots & \ddots & \ddots & 0 \\ b_1 & \cdots & b_{n_2-1} & 1 \end{matrix}
\right\} n_1
\end{vmatrix}$$

Pour déterminer son degré et son coefficient dominant, calculons le degré de chaque polynôme apparaissant en développant ce déterminant. Si $U_{i,j}$ désigne le coefficient (i,j) de la matrice résultante ci-dessus pour tout $(i,j) \in [\![1, n_1+n_2]\!]^2$, on a :

$$S = \sum_{\sigma \in S_{n_1+n_2}} \varepsilon(\sigma) \prod_{i=1}^{n_1+n_2} U_{i,\sigma(i)}.$$

Or pour tout $i \in [\![n_2+1, n_1+n_2]\!]$, le terme $U_{i,\sigma(i)}$ est égal soit à 0 soit à l'un des b_i, donc $\deg(U_{i,\sigma(i)}) \leqslant 0$ dans ce cas, puis :

$$\prod_{i=n_2+1}^{n_1+n_2} U_{i,\sigma(i)} \leqslant 0\,;$$

seuls les termes provenant des n_2 premières lignes contribuent au degré de $\prod_{i=1}^{n_1+n_2} U_{i,\sigma(i)}$. Pour $i \in [\![1, n_2]\!]$ on a : $U_{i,\sigma(i)} \in \{Q_0, \ldots, Q_{i-1}, 0\}$, donc l'explicitation des polynômes Q_k (identité $(*)$ ci-dessus) donne : $\forall i \in [\![1, n_2]\!]$, $\deg(U_{i,\sigma(i)}) \leqslant n_1$. Finalement :

$$\deg\left(\prod_{i=1}^{n_1+n_2} U_{i,\sigma(i)}\right) \leqslant \deg\left(\prod_{i=1}^{n_2} U_{i,\sigma(i)}\right) \leqslant n_1n_2.$$

Ainsi S est une somme de polynômes de degrés au plus n_1n_2, ce dont on déduit : $\deg(S) \leqslant n_1n_2$.
Pour montrer l'égalité et obtenir en prime le coefficient dominant, examinons pour quelles permutations σ le produit $\prod_{i=1}^{n_1+n_2} U_{i,\sigma(i)}$ est de degré exactement n_1n_2. Une condition nécessaire est que les n_2 premiers termes du produit soient tous égaux à Q_0, puisque $Q_1, \dots, Q_{n_1-1}$ sont de degré au plus $n_1 - 1$ par l'identité $(*)$. C'est réalisé en particulier pour $\sigma = \mathrm{id}$, et dans ce cas : $\prod_{i=1}^{n_1+n_2} U_{i,i} = Q_0^{n_2} \cdot 1^{n_1} = Q_0^{n_2}$. Montrons que c'est la seule permutation à convenir.
Soit $\sigma \in S_{n_1+n_2}$ telle que : $\forall i \in [\![1, n_2]\!]$, $\sigma(i) = i$ (condition nécessaire pour que le produit soit de degré n_1n_2, on l'a vu), et : $\sigma \neq \mathrm{id}$. Alors σ induit par restriction une permutation de $[\![n_2+1, n_1+n_2]\!]$, et on en déduit qu'il existe $j \in [\![n_2 + 1, n_1 + n_2]\!]$ tel que $\sigma(j) > j$ (cela sera démontré en remarque à la fin de la résolution). La description de la matrice résultante montre qu'on a dans ce cas : $U_{j,\sigma(j)} = 0$, donc :

$$\prod_{i=1}^{n_1+n_2} U_{i,\sigma(i)} = 0.$$

En conclusion, S est la somme de $Q_0^{n_2}$ (obtenu pour $\sigma = \mathrm{id}$), qui est de degré n_1n_2 et de polynômes de degrés au plus $n_1n_2 - 1$, donc S est de degré n_1n_2. De plus son coefficient dominant est celui de Q_0^{n-2}, qui est égal à $a_{n_1} = 1$ d'après $(*)$, donc S est unitaire : ce qu'il fallait démontrer.
Ceci achève de montrer que S est unitaire, à coefficients entiers, de degré n_1n_2 et annule $z_1 + z_2$.
Remarque. Justifions que si σ est une permutation de $[\![n_2 + 1, n_1 + n_2]\!]$ distincte de l'identité alors il existe $j \in [\![n_2 + 1, n_1 + n_2]\!]$ tel que $\sigma(j) > j$. La démonstration vaudrait en remplaçant $[\![n_2 + 1, n_1 + n_2]\!]$ par n'importe quelle partie finie non vide de $\mathbb{N}$, c'est ce que nous allons faire pour alléger les notations, en remplaçant cet ensemble par $[\![1, n]\!]$.
Nous allons montrer la contraposée. Soit σ une permutation de $[\![1, n]\!]$ telle que : $\forall j \in [\![1, n]\!]$, $\sigma(j) \leqslant j$. Supposons que $\{k \in [\![1, n]\!] \mid \sigma(k) \neq k\}$ est non vide : soit k un entier dans cet ensemble, et qui est minimal pour cette propriété. On a donc : $\sigma(k) < k$, puisque $\sigma(k) \leqslant k$ par hypothèse et $\sigma(k) \neq k$. Reformulé autrement en notant $j = \sigma(k)$, on a : $j < k$, et donc, par minimalité de k on a : $\sigma(j) = j = \sigma(k)$. Par injectivité de σ, cela implique : $j = k$, ce qui est absurde puisque $j < k$. Par l'absurde, l'ensemble $\{k \in [\![1, n]\!] \mid \sigma(k) \neq k\}$ est vide, donc $\sigma = \mathrm{id}$. Ceci montre que si une permutation de $[\![1, n]\!]$ vérifie : $\forall j \in [\![1, n]\!]$, $\sigma(j) \leqslant j$, alors $\sigma = \mathrm{id}$.
(On pouvait aussi raisonner par récurrence sur j.)

11. Tout d'abord, $\mathcal{O}$ est une partie de $\mathbb{C}$ non vide puisqu'elle contient tous les entiers relatifs (pour tout $a \in \mathbb{Z}$, cet entier est racine du polynôme unitaire $X - a \in \mathbb{Z}[X]$), stable par somme par la question précédente, et stable par symétrique par rapport à la + (en effet, si $z \in \mathcal{O}$ est annulé par $P \in \mathbb{Z}[X]$ unitaire, alors $(-1)^{\deg(P)}P(-X)$ est dans $\mathbb{Z}[X]$, unitaire, et admet $-z$ pour racine). Il reste à justifier la stabilité par produit. Pour cela, on montre en raisonnant comme dans la question précédente que si $(z_1, z_2) \in \mathcal{O}^2$ est un couple d'entiers algébriques, annulés par des polynômes unitaires P_1 et P_2 à coefficients entiers, alors $Y^nP_1\left(\frac{X}{Y}\right)$ est dans $\mathbb{Z}[X][Y]$, et le résultant :

$$S = \mathrm{Res}_{\mathbb{Q}(X)}\left(Y^nP_1\left(\frac{X}{Y}\right), P_2(Y)\right)$$

annule z_1z_2 (car $Y^nP_1\left(\frac{z_1z_2}{Y}\right)$ et $P_2(Y)$ admettent z_2 comme racine commune et ne sont donc pas premiers entre eux), et est unitaire à coefficients entiers. D'où le résultat.
Exemple. Trouvons ainsi un polynôme unitaire de $\mathbb{Z}[X]$ annulant $\sqrt[3]{2} + \sqrt{3}$. Comme $P_1 = X^3 - 2$ et $P_2 = X^2 - 3$ annulent respectivement $\sqrt[3]{2}$ et $\sqrt{3}$ en étant unitaires et à coefficient entiers, un polynôme qui convient est :

$$\mathrm{Res}_{\mathbb{Q}(X)}(P_2(X-Y), P_1(Y)) = \begin{vmatrix} X^2-3 & -2X & 1 & 0 & 0 \\ 0 & X^2-3 & -2X & 1 & 0 \\ 0 & 0 & X^2-3 & -2X & 1 \\ -2 & 0 & 0 & 1 & 0 \\ 0 & -2 & 0 & 0 & 1 \end{vmatrix} = X^6-9X^4-4X^3+27X^2-36X-23.$$