TD mp* : le résultant

Soit $\mathbf{K}$ un corps, $P = \sum_{k=0}^{n} a_k X^k$ un polynôme de degré n sur $\mathbf{K}$. Pour m entier naturel donné on définit la matrice de format $(m+n) \times m$:

$$M(P,m) = \begin{pmatrix} a_0 & 0 & \dots & \dots & 0 \\ a_1 & a_0 & \ddots & & \vdots \\ \vdots & a_1 & \ddots & \ddots & \vdots \\ a_n & \vdots & \ddots & \ddots & 0 \\ 0 & a_n & & \ddots & a_0 \\ \vdots & \ddots & \ddots & & a_1 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 0 & a_n \end{pmatrix} \quad (m \text{ colonnes})$$

Soit deux polynômes P et Q de degrés respectifs $n \geq 1$ et $m \geq 1$. On définit $\rho(P,Q)$ comme le déterminant de la matrice définie par blocs : $\Big(M(P,m) | M(Q,n)\Big)$.

1. De quelle famille de polynômes (et dans quel espace ?) $\Big(M(P,m) | M(Q,n)\Big)$ est-elle la matrice dans la base canonique ?

2. Montrer l'équivalence des trois propriétés suivantes :

   (i) P et Q ont un diviseur commun de degré supérieur ou égal à 1.

   (ii) il existe un polynôme U non nul de degré au plus $m-1$ et un polynôme V non nul de degré au plus $n-1$ tels que $UP = VQ$.

   (iii) $\rho(P,Q) = 0$.

   On suggère de montrer (i)$\Leftrightarrow$(ii) *et* (ii)$\Leftrightarrow$(iii).

3. Calculer $\rho(P,P')$ pour $P = aX^2 + bX + c$ puis pour $P = X^3 + pX + q$. Interpréter.

4. En utilisant de simples outils d'analyse, donner une condition nécessaire et suffisante pour que le polynôme à coefficients réels $X^3 + pX + q$ ait trois racines réelles distinctes.

5. *Question ens :* Soient a, b deux nombres complexes algébriques : il existe deux polynômes P et Q à coefficients rationnels, non nuls, dont a et b soient respectivement racines.
   Montrer que $P(a+b-X)$ et $Q(X)$ ont une racine commune.
   En considérant par exemple le polynôme $P(Y-X)$, comme polynôme de $(\mathbf{Q}(Y))[X]$, montrer qu'il existe un polynôme à coefficients rationnels dont $a+b$ est racine. Application : $a=\sqrt{2}$, $b=\sqrt{3}$.

1. La matrice $\Big(M(P,m)|M(Q,n)\Big)$ est la matrice dans la base canonique de la famille $\left(P, XP, \ldots, X^{m-1}P, Q, XQ, \ldots, X^{n-1}Q\right)$.

---

2. (i)$\Rightarrow$ (ii) : Si P et Q ont un diviseur D de degré ≥ 1, on écrit $P = DP_1$, $Q = DQ_1$, on a alors $Q_1P = P_1Q$, et $\deg(Q_1) \leq m-1$, $\deg(P_1) \leq n-1$.

(ii)$\Rightarrow$ (iii) : La relation $UP - VQ = 0$ est alors une relation de dépendance linéaire entre les vecteurs $\left(P, XP, \ldots, X^{m-1}P, Q, XQ, \ldots, X^{n-1}Q\right)$ (il suffit de développer U et V dans la base canonique pour s'en rendre compte), donc la famille est liée dans $\mathbf{K}_{n+m-1}[X]$. Donc son déterminant dans la base canonique, $\rho(p,q)$, est nul.

(iii)$\Rightarrow$ (i) : il me semble assez naturel de faire le détour par (ii)…ce qui fait qu'on montrera, contrairement à l'habitude, les équivalences (i)$\Leftrightarrow$ (ii) et (ii)$\Leftrightarrow$(iii).

(iii)$\Rightarrow$ (ii), donc : la nullité de $\rho(P,Q)$ donne l'existence d'une combinaison linéaire nulle à coefficients non tous nuls de la famille $\left(P, XP, \ldots, X^{m-1}P, Q, XQ, \ldots, X^{n-1}Q\right)$…ce qui montre l'existence de U, V **pas tous les deux nuls** tels que $UP - VQ = 0$. Mais il est impossible que l'un des deux polynômes U et V soit nul et pas l'autre, d'où le résultat.

(ii)$\Rightarrow$ (i) : Si $UP = VQ$, alors $P|VQ$. Supposons $P \wedge Q = 1$. Alors $P|V$ (Gauss), ce qui, pour des raisons de degré et de non nullité de V, est contradictoire. On a donc $P \wedge Q \neq 1$, d'où (i).

---

3. Pour $P = aX^2 + bX + c$,

$$\rho(P,P') = \begin{vmatrix} c & b & 0 \\ b & 2a & b \\ a & 0 & 2a \end{vmatrix} = a(4ac - b^2)$$

Pour $P = X^3 + pX + q$,

$$\rho(P, P') = \begin{vmatrix} q & 0 & p & 0 & 0 \\ p & q & 0 & p & 0 \\ 0 & p & 3 & 0 & p \\ 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 \end{vmatrix} = 4p^3 + 27q^2$$

---

4. La dérivée de $x \longmapsto x^3 + px + q$ est $x \longmapsto 3x^2 + p$. Si $p \geq 0$, la fonction croissante $x \mapsto x^3 + px + q$ ne peut pas avoir exactement trois points d'annulation sur $\mathbf{R}$. Supposons $p < 0$. La dérivée s'annule en les points $x_1 = \sqrt{\dfrac{-p}{3}}$ et $x_1 = -\sqrt{\dfrac{-p}{3}}$. Et le tableau de variations montre qu'il y a trois racines distinctes si et seulement si

$$(x_1^3 + px_1 + q)(x_2^3 + px_2 + q) < 0$$

ce qui équivaut à

$$\left(\frac{2p}{3}x_1 + q\right)\left(\frac{2p}{3}x_2 + q\right) < 0$$

ce qui, compte tenu de $x_1 + x_2 = 0$ et $x_1 x_2 = p/3$ s'écrit

$$4p^3 + 27q^2 < 0$$

---

5. $\rho(P(Y - X), Q(X))$ est un élément de $\mathbf{Q}[Y]$, et il admet $a + b$ pour racine, car $\rho(P(a + b - X), Q(X)) = 0$ (en raison d'une racine commune, b, à $P(a + b - X)$ et $Q(X)$).
Pour l'application numérique, prenons $P = X^2 - 2$ et $Q = X^2 - 3$. Alors $P(Y - X) = X^2 - 2YX + Y^2 - 2$ et, en considérant P et Q comme polynômes à coefficients dans $\mathbf{Q}(Y)$, leur résultant vaut

$$\rho = \begin{vmatrix} Y^2 - 2 & 0 & -3 & 0 \\ -2Y & Y^2 - 2 & 0 & -3 \\ 1 & -2Y & 1 & 0 \\ 0 & 1 & 0 & 1 \end{vmatrix}$$

on trouve $Y^4 - 10Y^2 + 1$.