Sujet Maison

LE RÉSULTANT

"Mais je ne m'arrête point à expliquer ceci plus en détail, à cause que je vous ôterais le plaisir de l'apprendre par vous-même, et l'utilité de cultiver votre esprit en vous exerçant..."
René Descartes

La notion de résultant a été introduite pour la première fois par Newton dans des cas partculiers (1707) et par Euler (1748, 1764) et par Bézout (1764) dans le cas général. [1]

✍

1. La théorie générale

Soit $\mathbb{K}$ un corps. On note par $\mathbb{K}_n[T]$ l'ensemble des polynômes à une indéterminée T de degré inférieur ou égal à n.

(1) Soit $P = a_0 + a_1T + \cdots + a_pT^p$ et $Q = b_0 + b_1T + \cdots + b_qT^q$ deux polynômes de degré p et q respectivement. On considère l'application linéaire

$$\begin{array}{rcccl} \rho & : & \mathbb{K}_{q-1}[T] \times \mathbb{K}_{p-1}[T] & \to & \mathbb{K}_{p+q-1}[T] \\ & & (U,V) & \mapsto & PU+QV\ . \end{array}$$

Écrire la matrice $\mathcal{R}es(P,Q)$, appelée *matrice résultant* (ou de Sylvester) de P et Q, de l'application linéaire ρ dans les bases

$$\big((1,0),\ldots,(T^{q-1},0),(0,1),\ldots,(0,T^{p-1})\big) \text{ et } (1,T,\ldots,T^{p+q-1}) \text{ respectivement .}$$

(2) Décrire le noyau de l'application ρ.

(3) On définit le *résultant* $\mathrm{Res}(P,Q)$ de P et Q comme le déterminant de la matrice $\mathcal{R}es(P,Q)$. Montrer que $\mathrm{Res}(P,Q) = 0$ si et seulement si P et Q ne sont pas premiers entre eux.

Remarque. On peut définir de la même manière le résultant de deux polynômes à coefficients dans un anneau A comme le déterminant de la matrice résultant.

(4) Montrer que $\mathrm{Res}(P,Q) \in \mathrm{Im}\,\rho$.

(5) Si P et Q sont premiers entre eux, en conclure une formule (universelle) pour les polynômes apparaissant dans le théorème de Bézout.

1. La présentation, la lisibilité, l'orthographe, la qualité de la rédaction, *la clarté et la précision des raisonnements* entreront pour une part importante dans l'appréciation des copies. Toute réponse non justifiée ne recevra aucun point.

2. Règles de calcul

"L'expérience prouve qu'il ne sert à rien de connaître le résultant si l'on ne possède pas suffisamment de règles de calcul ..."

Nicolas Bourbaki

On travaille maintenant sur un corps $\mathbb{K}$ algébriquement clos [2]. On peut donc écrire les deux polynômes P et Q de la manière suivante

$$P = a_p(T-x_1)\cdots(T-x_p) \quad \text{et} \quad Q = b_q(T-y_1)\cdots(T-y_q) \ .$$

(1) Montrer les relations

$$\mathrm{Res}(P,Q) = (-1)^{pq}{a_p}^q{b_q}^p \prod_{\substack{1\leqslant i\leqslant p\\ 1\leqslant j\leqslant q}} (x_i-y_j) = (-1)^{pq}{a_p}^q \prod_{1\leqslant i\leqslant p} Q(x_i) = {b_q}^p \prod_{1\leqslant j\leqslant q} P(y_j)$$

(2) Montrer que

$$\mathrm{Res}(P,Q) = (-1)^{pq}\mathrm{Res}(Q,P)$$

et que

$$\mathrm{Res}(P,Q) = (-1)^{qr}{b_q}^{p-r}\mathrm{Res}(G,B) \ ,$$

où $P = AQ+B$ est la division euclidienne de P par Q, avec $r = \deg B$.

(3) En déduire un algorithme pour calculer le résultant et le comparer au calcul à partir du déterminant de la matrice résultant.

(4) Calculer de trois manières différentes le résultant $\mathrm{Res}(aX^2+bX+c, dX+e)$.

3. Le discriminant

On définit le *disciminant* d'un polynôme $P = a_0 + a_1T + \cdots + a_pT^p$ comme le résultant de P et de P' (au signe et à coefficient près) :

$$\Delta(P) := (-1)^{\frac{n(n-1)}{2}} \frac{\mathrm{Res}(P,P')}{a_p} \ .$$

(1) Montrer que

$$\Delta(aX^2+bX+c) = b^2-4ac \quad \text{(Étonnant non ?)} \quad \text{et} \quad \Delta(X^3+pX+q) = -4p^3-27q^2 \ .$$

(2) Si $\mathbb{K}$ est algébriquement clos, montrer que $\Delta(P)=0$ si et seulement si P a une racine de multiplicité supérieure ou égale à 2.

(3) Si $P = a_p(T-x_1)\cdots(T-x_p)$, montrer que

$$\Delta(P) = a_p^{2p-2} \prod_{1\leqslant i,j\leqslant p} (x_i-x_j)^2 \ .$$

4. Application : élimination

(1) Déterminer la nature des deux courbes algébriques réelles du plan définies par les polynômes $P = X^2-XY+Y^2-1$ et $Q = 2X^2+Y^2-Y-2$ et calculer leurs points d'intersection. Représenter vos résultats graphiquement.

(2) Utiliser le résultant pour fabriquer un polynôme à coefficients entiers qui a $\sqrt{2}+\sqrt[3]{7}$ comme racine.

(3) Déterminer une équation cartésienne de la courbe paramétrée définie par

$$\begin{cases} x(t) = 1+t+t^2 \ , \\ y(t) = \dfrac{t^2-1}{t^2+1} \ , \end{cases}$$

pour $t \in \mathbb{R}$.

---

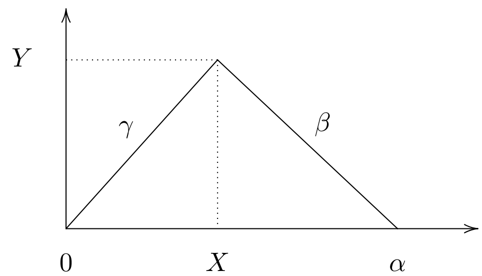
2. On rappelle le théorème de Steinitz (1910) qui affirme que tout corps se plonge dans un corps algébriquement clos. Les résultats de cette partie sont donc vrais pour tout corps.

(4) Démontrer la formule de Héron

$$S^2 = \frac{1}{16}(\alpha+\beta+\gamma)(-\alpha+\beta+\gamma)(\alpha-\beta+\gamma)(\alpha+\beta-\gamma)$$

donnant l'aire S d'un triangle en fonction des longueurs de ses trois côtés α, β et γ.

Indication. Pour se faire, on pourra se placer dans un repère orthonormé comme indiqué à la figure suivante.



Interprétez ensuite les formules donnant les aires du triangle de gauche, du triangle de droite et du rectangle global comme des polynômes à trois variables X, Y et S. Il ne reste plus qu'à éliminer X et Y.

5. Application : topologie

(1) Soient $P, Q \in \mathbb{R}[X]$ unitaires avec P de degré pair. Montrer que si le résultant $\mathrm{Res}(P,Q) < 0$, alors P admet au moins deux racines réelles $x_1 < x_2$ et Q une racine réelle $x_1 < y < x_2$. En conclure que tout polynôme $P \in \mathbb{R}[X]$ de degré pair vérifiant $\Delta(P) < 0$ a au moins 2 racines réelles.

(2) On note par $\mathrm{Diag}_n(\mathbb{C})$ l'ensemble des matrices diagonales de $\mathcal{M}_n(\mathbb{C})$ et par $\mathrm{Dist}_n(\mathbb{C})$ l'ensemble des matrices à valeurs propres distinctes de $\mathcal{M}_n(\mathbb{C})$. Montrer que $\mathrm{Dist}_n(\mathbb{C})$ est un ouvert de $\mathcal{M}_n(\mathbb{C})$ et que $\mathrm{Dist}_n(\mathbb{C}) = \mathring{\mathrm{Diag}}_n(\mathbb{C})$.

6. Application : arithmétique

Soit p un nombre premier impair. Pour tout nombre entier n, on définit le *symbole de Legendre* $\left(\frac{n}{p}\right)$ par $+1$ si l'image de n est un carré dans $\mathbb{F}_p$ et par -1 sinon.

(1) Montrer qu'il y a $\frac{p+1}{2}$ carrés dans $\mathbb{F}_p$ et montrer que si n est premier avec p, alors

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \ [p] \ .$$

(2) Montrer qu'il existe un polynôme $Q_p \in \mathbb{Z}[X]$ tel que

$$X^{p-1} + \cdots + X + 1 = X^{\frac{p-1}{2}} Q_p(X + \frac{1}{X}) \ .$$

(3) Soit q un nombre premier impair différent de p. Montrer que

$$\mathrm{Res}(Q_p, Q_q) = \pm 1 \quad \text{puis que} \quad \mathrm{Res}(Q_p, Q_q) = \left(\frac{q}{p}\right) \ .$$

(4) En conclure la *loi de réciprocité quadratique*[3] :

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \ .$$

3. appelée *Theorema Aureum*, c'est-à-dire *Théorème en Or* par Gauss loi-même.

7. Application : Géométrie algébrique

Il existe une jolie démonstration du théorème des zéros de Hilbert utilisant le résultant. Ce théorème est la porte d'entrée pour la géométrie algébrique. Malheureusement la marge est trop étroite pour que l'on puisse traiter cela ici ...

——— ✍ ———

Note historique. Dans son mémoire de 1764 à l'Académie des Sciences de Berlin : "Nouvelle manière d'éliminer les quantités inconnues des équations", Euler introduit le résultant en écrivant que, si deux polynômes $P = a_0 + a_1 T + \cdots + a_p T^p$ et $Q = b_0 + b_1 T + \cdots + b_p T^q$ ont une racine commune x, il existe des polynômes $P_1 = c_0 + c_1 T + \cdots + c_{p-1} T^{p-1}$ et $Q_1 = d_0 + d_1 T + \cdots + d_{q-1} T^{q-1}$ tels que

$$P = (T - x)P_1 \quad \text{et} \quad Q = (T - x)Q_1 \ .$$

On a donc $PQ_1 = P_1 Q$, ce qui conduit, en développant, à un système linéaire en les c_i et les d_j à $p + q$ équations à $p + q$ inconnues dont le déterminant doit être nul pour qu'il y ait une solution non nulle. Ce déterminant est celui que nous venons d'introduire. (Bien sur, Euler ne parle pas de déterminant, c'est Sylvester qui le fera en 1840, et n'écrit la formule explicite que pour des polynômes de petit degré.)

✉ Bruno Vallette : `vallette@math.univ-paris13.fr` .

☞ Page internet du cours : `www.math.univ-paris13.fr/~vallette/` .