ÉNS de Lyon — Agrégation
2018-2019 — Option C

TD Polynômes et résultants

Exercice 1 — Élimination —

1. Pour quelles valeurs de $\alpha \in \mathbb{R}$ les équations $x^3 + 2\alpha x^2 + (\alpha^2+1)x + 1 = 0$ et $x^2 + \alpha x + 1 = 0$ ont-elles au moins une racine commune dans $\mathbb{R}$?
2. Soit k un corps algébriquement clos. Soient $a, b, c, a', b', c' \in k$ avec $aa' \neq 0$. Donner une condition nécessaire et suffisante pour que les équations $ax^2 + bx + c = 0$ et $a'x^2 + b'x + c = 0$ aient une racine commune dans k. Que peut-on dire si k n'est pas algébriquement clos ?

Exercice 2 — Calcul du résultant en pratique — Soient P et Q deux polynômes à coefficients dans un corps k, de degrés $p \geq 1$ et $q \geq 1$ et de coefficients dominants a et b respectivement. On suppose $p \geq q$.

1. On note $\tilde{P} = P - (a/b)X^{p-q}Q$, et d le degré de $\tilde{P}$. Montrer
$$\mathrm{Res}_{p,q}(P,Q) = (-1)^{q(p-d)} b^{p-d} \mathrm{Res}_{d,q}(\tilde{P}, Q).$$
2. On note R le reste de la division euclidienne de P par Q, qu'on suppose non nul. Exprimer $\mathrm{Res}_{p,q}(P,Q)$ en fonction de $\mathrm{Res}(R,Q)$.
3. En déduire un algorithme pour calculer $\mathrm{Res}(P,Q)$ sans faire de calcul de déterminant. Donner approximativement sa complexité.
4. Que se passe-t-il si on remplace le corps k par un anneau intègre quelconque A ?

Exercice 3 — Intersections d'ensembles algébriques — Soient $f, g \in k[x_1, \ldots, x_n]$ tels que x_1 apparaît dans f et dans g. On pose $I = \langle f, g \rangle$, et $I_1 = I \cap k[x_2, \ldots, x_n]$. On pose $h = \mathrm{Res}_{x_1}(f,g)$. Soient $u, v \in k[x_2, \ldots, x_n]$ les coefficients dominants respectifs de f et g vus comme polynômes en x_1.

1. Montrer que $h \in I_1$.
2. Montrer que $h = 0$ si et seulement si f et g ont un facteur commun dans lequel x_1 apparaît.
3. On suppose à partir de maintenant k algébriquement clos. Soit $(a_2, \ldots, a_n) \in k^{n-1}$ un zéro de h. Montrer que soit il existe $a_1 \in k$ tel que $(a_1, a_2, \ldots, a_n)$ est un zéro commun de f et g, soit $(a_2, \ldots, a_n)$ est un zéro de u ou v.
4. Montrer que : soit il existe $a_1 \in k$ tel que $(a_1, a_2, \ldots, a_n)$ est un zéro commun de f et g, soit $(a_2, \ldots, a_n)$ est un zéro commun de u et v.
Si $(a_2, \ldots, a_n)$ est un zéro de v mais pas u, on pourra remplacer g par $g + x_1^N f$ pour N assez grand.

5. En considérant $f = x_1x_2 - 1$, $g = x_1x_3 - 1$, vérifier que si u et v s'annulent il n'existe pas forcément de a_1 complétant la solution.
6. Donner un exemple qui montre que les résultats précédents sont faux si k n'est pas algébriquement clos.

Exercice 4 — Courbes paramétrées — Pour chacune des courbes paramétrées du plan suivantes, donner une équation implicite de la courbe. Que penser de l'image de la paramétrisation par rapport à l'équation obtenue ?

1. $x(t) = 1 + t$, $y(t) = 1 + t^3$.
2. $x(t) = t + t^2$, $y(t) = t^3$.
3. $x(t) = \frac{1+t^2}{1-t^2}$, $y(t) = \frac{2t}{1-t^2}$.

Exercice 5 — Intersection de surfaces algébriques — On se donne deux surfaces S et S' dans $\mathbb{R}^3$ données par les équations $S : F(x, y, z) = 0$ et $S' : G(x, y, z) = 0$. On note $C = S \cap S'$.

1. Montrer que la projection orthogonale de C sur le plan (Oxy) est incluse dans le lieu des zéros du polynôme $R = \mathrm{Res}_z(F, G) \in \mathbb{R}[x, y]$.
2. Y a-t-il nécessairement égalité ?
3. Majorer le degré de la courbe C en fonction des degrés de F et G.

Exercice 6 — Nombres algébriques — En utilisant le résultant, montrer que si α et β sont des nombres algébriques, alors $\alpha + \beta$ et $\alpha\beta$ sont également algébriques.

Exercice 7 — Soit $P \in \mathbb{C}[X]$ un polynôme de degré n. On note $\alpha_1, \ldots, \alpha_n$ les racines de P, comptées avec multiplicité.

1. Soit $Q \in \mathbb{C}[X]$ non constant. Montrer que $\mathrm{Res}_X(P(X), Q(X) - T)$ est égal, à une constante près que l'on déterminera, à $\prod_{i=1}^{n}(T - Q(\alpha_i))$.
2. Soit $F \in \mathbb{C}(X)$ une fraction rationnelle non constante. Donner une façon de calculer $\prod_{i=1}^{n}(T - F(\alpha_i))$. Que se passe-t-il si une racine de P est un pôle de F ?
3. Application : on prend $F(X) = X^3/(X^2 + 1)$. Calculer $\sum_{i=1}^{n} F(\alpha_i)$ pour $P(X) = X^4 + X + 1$ puis $P(X) = X^4 + 1$.

Exercice 8 — Pseudo-division euclidienne — Soit A un anneau intègre. Soit U et V dans $A[X]$, de degrés u et v respectivement, et c le coefficient dominant de V.

1. Montrer qu'il existe des polynômes uniques Q et R dans $A[X]$ tels que $\deg R < v$ et $c^{u-v+1}U = QV + R$.

On appelle Q le pseudo-quotient et R le pseudo-reste de la pseudo-division euclidienne de U par V.

2. Calculer Q et R pour

(a) $U = 2X^2 + X + 3$ et $V = 6X - 1$ dans $\mathbb{Z}[X]$;

(b) $U = Y^3 + X + Y$ et $V = XY + 1$ dans $\mathbb{C}[X][Y]$ et dans $\mathbb{C}[Y][X]$.

3. Quel est l'interprétation géométrique des pseudo-restes trouvés en (b) ?

Exercice 9 — PGCD de polynômes — Soit A un anneau intègre factoriel. On rappelle qu'alors $A[X]$ est aussi factoriel. On note $U \wedge V$ un PGCD de U et V au sens des anneaux factoriels. On note $c(U)$ le contenu de $U \in A[X]$, c'est-à-dire le (en fait un) PGCD de ses coefficients. Enfin, on note $p(U) = U/c(U)$ la partie primitive de U.

1. Soient U et V deux polynômes primitifs de $A[X]$, et R le pseudo-reste de la division de U par V. Montrer que $U \wedge V = V \wedge p(R)$.
2. Supposons que l'on dispose d'un algorithme de calcul de PGCD dans A. Donner un algorithme de calcul de PGCD dans $A[X]$.
3. Application à :

   (a) $U = 2X^3 - 5X^2 + X + 2$ et $V = 6X^3 + X^2 + X + 1$ dans $\mathbb{Z}[X]$.

   (b) $U = 3X^3Y^2 + 4X^2Y + XY^2 + X + Y$ et $V = X^3Y - X^2Y^2 + X^2 + XY^2 - XY + Y$ dans $\mathbb{C}[X, Y]$ (en les considérant comme des polynômes en Y puis comme des polynômes en X).

   (c) $U = X + YZ + 5XZ^2$ et $V = XY - 2ZY^2 + X^3$ dans $\mathbb{C}[X, Y, Z]$.

   Quelle est la commande Sage qui permet de faire ces calculs ?