

Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications

Plan: comme d'habitude il faut éviter le piège de la leçon "fourre-tout". A priori il ne faut pas s'attarder sur la notion de polynôme irréductible puisqu'on s'intéresse aux racines. Il faut plutôt axer la leçon sur les racines: leur nombre, leur localisation, les méthodes pour les trouver...

- Dans une première partie, après avoir rappelé que l'on supposait connu la notion de polynôme, de polynôme dérivée..., on définira les notions élémentaires: racine, multiplicité. On enchaînera avec les propriétés élémentaires: leur nombre est majorée par le degré, sur \mathbb{C} il est même égal (théorème de d'Alembert-Gauss). Enfin on passera aux relations coefficients racines et aux sommes de Newton en donnant des applications par exemple: calculer une somme de tangente, équations dont les racines forment un triangle équilatéral, ellipse de Steiner...
- Dans la deuxième partie, je pense qu'il faut s'intéresser au coeur de la leçon: la localisation des racines. On commencera par \mathbb{Q} (c'est facile, il y a un nombre fini de test à faire), puis sur \mathbb{R} avec les lemmes de Rolle, Descartes puis le théorème de Sturm, et enfin sur \mathbb{C} avec le théorème de Gauss-Lucas, diverses majoration du module des racines, minoration de la séparation des racines. Enfin on fera un paragraphe sur les méthodes pour trouver des racines: méthode de Newton (sur \mathbb{R}), de Laguerre (sur \mathbb{C})
- Dans les thèmes plus évolués, on pourra traiter (dans le désordre et à organiser):
 - le degré 2, 3, 4 avec des formules et évoquer le cas de degré supérieur ou égal 5 où, d'après Galois, il n'y pas de formule par radicaux;
 - polynôme d'interpolation de Lagrange: partage de secret;
 - méthode de Newton et de Laguerre;
 - nombres algébriques avec des exemples et des contre-exemples: transcendance de π ;
 - polynômes orthogonaux avec les points de Gauss;
 - les polynômes cyclotomiques....théorème de Kronecker
 - Continuité des racines des polynômes.
 - le résultant avec des applications: calcul de polynômes minimaux de certains entiers algébriques, propriétés topologiques sur certains ensemble de matrices (exemple: l'ensemble des matrices possédant n valeurs propres distinctes est un ouvert connexe de $\mathbb{M}_n(\mathbb{C})$), calcul de l'intersection de deux coniques (plus généralement théorie de l'élimination);
 - calcul du nombre de racines au moyen de la signature d'une forme quadratique (généralisation du discriminant en degré 2).
 - code BCH
 - étant donnée une matrice symétrique A , il existe une matrice P produit de $(n - 2)$ matrices de Householder, telle que PAP soit tridiagonale (Ciarlet p.120). En appliquant alors la méthode de Givens, on obtient des valeurs approchées des valeurs propres: les polynômes caractéristiques des mineurs principaux forment une suite de Sturm ce qui permet de localiser les racines aussi précisément que l'on veut par exemple par dichotomie (Ciarlet p.123).

Développements

- Le lemme de Descartes.
- Le théorème de Sturm.
- Diverses majorations du module des racines d'un polynôme.
- Séparation entre les racines.

- Points de Gauss.
- Résultant et applications.
- Ellipse de Steiner.
- Continuité des racines avec l'application aux matrices complexes à valeurs propres distinctes.
- Gauss-Lucas avec application.
- Transcendance de π .
- Signature d'une forme quadratique pour calculer le nombre de racines réelles.
- Sommes de Newton
- Théorème de Kronecker: un polynôme unitaire de $\mathbb{Z}[X]$ dont les racines complexes sont toutes de module inférieur ou égal à 1 alors ce sont des racines de l'unité.
- Polynôme de Tchebychev: en particulier on montre que $\sup_{x \in [-1,1]} |P(x)| \geq \frac{1}{2^{n-1}}$ où P est unitaire réel de degré n ; on a égalité si et seulement si $P = \frac{T_n}{2^{n-1}}$.

Questions

- Soit $P(X) \in \mathbb{Q}[X]$ et x une racine de $P(X)$ de multiplicité strictement supérieure à $(\deg P)/2$; montrez que $x \in \mathbb{Q}$.
- Soit $P(X) = a_n X^n + \dots + a_1 X + a_0$ un polynôme à coefficient dans \mathbb{Z} . Montrez que si a/b est une racine rationnelle de P alors $b|a_n$ et $a|a_0$ puis que pour tout $m \in \mathbb{Z}$, $(bm - a)|P(m)$.
- Soient $\alpha, \beta, \gamma, \delta$ les racines complexes de $X^4 - 2X^3 + aX^2 + bX - 1$; trouvez a, b pour que l'on ait $\alpha + \beta = \gamma + \delta$ et $\alpha\beta = -\gamma\delta$ et donnez les racines.
- Soient a, b, c des nombres complexes; montrez qu'une condition nécessaire et suffisante pour que les points A, B, C du plan réel, d'affixes respectives a, b, c , forment un triangle isocèle rectangle en A , est $c^2 + b^2 - 2a(b+c) + 2a^2 = 0$. En déduire qu'une CNS pour que les solutions a, b, c de l'équation $x^3 + px + q$ forment un triangle rectangle isocèle est $27q^2 - 50p^3 = 0$.
- Soit P un polynôme réel totalement décomposé dans \mathbb{R} . Montrez que si $z \in \mathbb{C}$ alors z est réel et est une racine multiple de P . (appliquez simplement le théorème de Rolle).
- Trouvez les solutions du système d'équations

$$\begin{cases} x^2 + y^2 + z^2 = 2 \\ x^3 + y^3 + z^3 = 2 \\ x^4 + y^4 + z^4 = 2 \end{cases}$$

- Soient a_1, \dots, a_n des nombres strictement positifs; montrez que $(a_1 \dots a_n)^{1/n} \leq \frac{a_1 + \dots + a_n}{n}$ et déterminez tous les polynômes à coefficients 1, -1, 0 ayant toutes leurs racines réelles.
- Soit $P(X) = a_d X^d + \dots + a_0 \in \mathbb{C}[X]$ avec $a_d \neq 0$. Montrez que si α est une racine de P , on a

$$|\alpha| \leq M := \sup_{0 \leq i < d} \left(d \frac{|a_i|}{|a_d|} \right)^{\frac{1}{d-i}}$$

- Soient P et Q deux polynômes non constants de $\mathbb{C}[X]$ tels que l'ensemble des racines de P (resp. $P - 1$) soit égal à l'ensemble des racines de Q (resp. $Q - 1$). Montrez que $P = Q$

- On considère le polynôme $X^{14} - 7.13.X^2 - 14.6X - 13.6$. Que pouvez vous dire du nombre de racines réelles positives et négatives de ce polynôme en utilisant la règle de Descartes puis celle de Sturm.
- On considère la courbe paramétrée $x(t) = t^2 + t + 1$, $y = \frac{t^2-1}{t^2+1}$. En donner une équation algébrique.
- Montrez que les racines sont continues en le polynômes.
- Montrez que l'ensemble des matrices complexe à valeurs propres distinctes, est un ouvert connexe de l'ensemble des matrices.
- Calculer le discriminant du polynôme $P(X) = X^3 + pX + q$
 - (i) En appliquant la définition.
 - (ii) En calculant la suite de Sturm $S(P, P')$.
- Calculer le résultant $R_Y(P, Q)$ des polynômes $P_X(Y) = X^2 - XY + Y^2 - 1$ et $Q_X(Y) = 2X^2 + Y^2 - Y - 2$ considérés comme des éléments de $\mathbb{R}[X][Y]$, i.e. comme des polynômes en Y à coefficients dans $\mathbb{R}[X]$. Trouver alors les points d'intersections des ellipses d'équations $P = 0$ et $Q = 0$.
- Soient A et B deux polynômes de $K[X]$ où K est un corps. Fabriquez un polynôme dont les racines sont les sommes d'une racine de A et d'une racine de B (on réfléchira à quels sont les Y solutions du système $A(X) = B(Y - X) = 0$). Construisez un polynôme à coefficients entiers qui possède $\sqrt{2} + \sqrt[3]{7}$ pour racine.

Exercices corrigés

Exercice 1. Soit $P(X) \in \mathbb{Q}[X]$ et x une racine de $P(X)$ de multiplicité strictement supérieure à $(\deg P)/2$; montrez que $x \in \mathbb{Q}$.

Preuve : On raisonne par récurrence sur le degré de P ; le résultat est évident pour P de degré 1, supposons alors le résultat vrai pour tout polynôme de degré inférieur ou égal à n et soit P de degré $n + 1$. On note $\delta = (P \wedge P')$ de degré supérieur ou égal à 1 par hypothèse car $\delta(x) = 0$. Ainsi δ divise P et donc P n'est pas irréductible ($\deg \delta < \deg P$). Soit donc $P = QR$ avec $\deg Q$ et $\deg R$ sont dans $\mathbb{Q}[X]$ de degré inférieurs à n . Par hypothèse on a $v_P(x) = v_Q(x) + v_R(x) > (n + 1)/2$ et donc soit $v_Q(x) > (\deg Q)/2$ soit $v_R(x) > (\deg R)/2$ et par hypothèse de récurrence $x \in \mathbb{Q}$.

Exercice 2. Soit $P(X) = a_n X^n + \dots + a_1 X + a_0$ un polynôme à coefficient dans \mathbb{Z} . Montrez que si a/b écrit sous forme irréductible, est une racine rationnelle de P alors $b|a_n$ et $a|a_0$ puis que pour tout $m \in \mathbb{Z}$, $(bm - a)|P(m)$.

Preuve : On écrit en multipliant par b^n : $a_n a^n + \dots + a_1 a b^{n-1} + a_0 b^n$ de sorte que b (resp. a) divise $a_n a^n$ (resp. $a_0 b^n$): on conclut en disant que a et b sont pris premiers entre eux.

Pour la deuxième partie $(bX - a)$ est un polynôme entier irréductible car de degré 1 et de contenu 1, qui divise $P(X)$ de sorte qu'il existe $Q(X)$ à coefficients entiers tel que $P(X) = (bX - a)Q(X)$ et donc $(bm - a)$ divise $P(m)$.

Exercice 3. Soient $\alpha, \beta, \gamma, \delta$ les racines complexes de $X^4 - 2X^3 + aX^2 + bX - 1$; trouvez a, b pour que l'on ait $\alpha + \beta = \gamma + \delta$ et $\alpha\beta = -\gamma\delta$ et donnez les racines.

Preuve : On a donc $\alpha + \beta + \gamma + \delta = 2 = 2(\alpha + \beta)$, $\alpha\beta\gamma\delta = 1 = -(\alpha\beta)^2$ de sorte que α, β (resp. γ, δ) sont les racines de $X^2 - X + i$ (resp. $X^2 - X - i$). En outre on a $(\beta + \alpha)(\gamma + \delta) + (\alpha\beta + \gamma + \delta) = -a = 1$ et $\alpha\beta(\gamma + \delta) + \gamma\delta(\alpha + \beta) = b = 0$.

Exercice 4. Soient a, b, c des nombres complexes; montrez qu'une condition nécessaire et suffisante pour que les points A, B, C du plan réel, d'affixes respectives a, b, c , forment un triangle isocèle rectangle en A , est $c^2 + b^2 - 2a(b + c) + 2a^2 = 0$. En déduire qu'une CNS pour que les solutions a, b, c de l'équation $x^3 + px + q$ forment un triangle rectangle isocèle est $27q^2 - 50p^3 = 0$.

Preuve : Une CNS pour que ABC soit rectangle isocèle en A est $b - a = \pm i(c - a)$, soit $(b - a)^2 + (c - a)^2 = 0$, i.e. $b^2 + c^2 + 2a^2 = 2a(b + c)$. En outre on a $a + b + c = 0$, $abc = -q$ et $ab + ac + bc = p$. Le but est alors d'éliminer dans la CNS a, b, c et de les remplacer par p et q ; on a $a^2 + b^2 + c^2 = (a + b + c)^2 - 2p = -2p$ de sorte que la CNS s'écrit $-2p + a^2 = -2a^2$ soit $3a^2 = 2p$. Or on a $a^3 = -pa + q \neq 0$ de sorte que la CNS s'écrit $-3pa + 3q = 2pa$, soit $a = \frac{3q}{5p}$. Ainsi l'équation $3a^2 = 2p$ devient $27q^2 - 50p^3 = 0$.

Exercice 5. Trouvez les solutions du système d'équations

$$\begin{cases} x^2 + y^2 + z^2 = 2 \\ x^3 + y^3 + z^3 = 2 \\ x^4 + y^4 + z^4 = 2 \end{cases}$$

Preuve : Les relations de Newton donnent $2 = \sigma_1^2 - 2\sigma_2 = \sigma_1^3 - 3\sigma_2\sigma_1 + 3\sigma_3 = \sigma_1^4 - 4\sigma_2\sigma_1^2 + 4\sigma_3\sigma_1 + 2\sigma_2^2$ soit $\sigma_2 = \sigma_1^2/2 - 1$ et $3\sigma_3 = 2 - \sigma_1^3 + 3\sigma_1(\sigma_1^2/2 - 1)$ et la dernière équation devient alors $\sigma_1(\sigma_1^3/6 - 2\sigma_1 + 8/3) = 0$. Les racines de $X^3 - 12X + 16$ étant 2 et -4 , on obtient alors $\sigma_1 = 0, 2, -4$ et donc $\sigma_2 = -1, 1, 7$ et $\sigma_3 = 2, 0, -6$. Les triplets (x, y, z) sont alors les racines des polynômes $X^3 - X - 2$, $X^3 - 2X^2 + X$, $X^3 + 4X^2 + 7X + 6$.

Exercice 6. Soient a_1, \dots, a_n des nombres strictement positifs; montrez que $(a_1 \cdots a_n)^{1/n} \leq \frac{a_1 + \dots + a_n}{n}$ et déterminez tous les polynômes à coefficients 1, $-1, 0$ ayant toutes leurs racines réelles.

Preuve : L'inégalité proposée découle directement de la concavité du logarithme $\frac{\ln a_1 + \dots + \ln a_n}{n} \leq \ln \frac{a_1 + \dots + a_n}{n}$. On applique cette inégalité aux carrés des racines de $P(X) = X^n - \sigma_1 X^{n-1} + \dots + (-1)^n \sigma_n$, soit $(\sigma_n^2)^{1/n} \leq \frac{\sigma_1^2 - 2\sigma_2}{n} \leq 3/n$, soit $n \leq 3$. Une inspection cas par cas donne $X \pm 1$, $X^2 \pm X - 1$, $X^3 + X^2 - X - 1$ et $X^3 - X^2 - X + 1$.

Exercice 7. Continuité des racines de polynômes Pour $P = a_n X^n + \dots + a_1 X + a_0$ un polynôme à coefficients complexes de degré n , on note $\|P\| = |a_n| + \dots + |a_0|$; $\|\cdot\|$ est une norme sur $\mathbb{C}_n[X]$.

(i) Pour $z \in \mathbb{C}$, une racine de P , montrez que $|z| \leq \frac{\|P\|}{|a_n|}$.

(ii) Soit $(P_k)_{k \in \mathbb{N}}$ une suite qui converge vers P dans $\mathbb{C}_n[X]$. Soit z une racine de P de multiplicité p . Montrez que pour tout $\epsilon > 0$, il existe k_0 tel que pour tout $k \geq k_0$, il y a au moins p racines de P_k dans la boule de centre z et de rayon ϵ .

Preuve : (i) Comme $\|P\| \geq |a_n|$, la relation est triviale si $|z| \leq 1$. Supposons $|z| > 1$, de l'égalité

$$a_n z^n = -(a_{n-1} z^{n-1} + \dots + a_0)$$

on en déduit que $|a_n| |z|^n \leq (\sum_{i=0}^{n-1} |a_i|) |z|^{n-1} \leq \|P\| |z|^{n-1}$ et donc $|z| \leq \frac{\|P\|}{|a_n|}$.

(ii) Remarquons déjà que la suite $\frac{\|P_k\|}{|a_{k,n}|}$ est convergente de sorte qu'elle est bornée et donc qu'il existe M tel que pour tout k et toute racine de P_k , son module est inférieur à M . On note K la boule de centre 0 et de rayon M . Il s'agit de prouver que pour k assez grand, l'ensemble I_k des racines de P_k dans la boule ouverte centrée en z et de rayon ϵ , est de cardinal p .

On raisonne par l'absurde et supposons que pour tout $k_0 \in \mathbb{N}$, il existe $k \geq k_0$ tel que le cardinal I_k est strictement inférieur à p . On numérote les racines $(x_{k,i})_{1 \leq i \leq n}$ de P_k de sorte que $|z - x_{k,i}|$ soit croissant. Ainsi on peut extraire une sous-suite $(P_{\psi(k)})_{k \in \mathbb{N}}$ telle que

$$p \leq i \leq n \quad |z - x_{\psi(k),i}| \geq \epsilon$$

La suite $((x_{\psi(k),1}, \dots, x_{\psi(k),n}))_{k \in \mathbb{N}}$ prend ses valeurs dans le compact K^n . Quitte à en extraire une sous-suite, on peut supposer que pour tout $1 \leq i \leq n$, $x_{\psi(k),i}$ converge vers y_i . En particulier pour tout $p \leq i \leq n$, $|y_i - z| \geq \epsilon$. Or $P_{\psi(k)}(X) = a_{\psi(k),n} \prod_{i=1}^n (X - x_{\psi(k),i})$ converge vers $P(X) = a_n \prod_{i=1}^n (X - y_i)$ ce qui fournit la contradiction.

Exercice 8. Montrez que l'ensemble des matrices complexe à valeurs propres distinctes, est un ouvert connexe de l'ensemble des matrices.

Preuve : Soit A une matrice possédant n valeurs propres distinctes de sorte que son polynôme caractéristique est scindé à racines simples. D'après la continuité du polynôme caractéristique et de celle des racines d'un polynôme, on en déduit que pour tout A' proche de A , le polynôme caractéristique de A' possède, sur \mathbb{C} , n racines distinctes. (Si A et A' sont réelles, alors leurs racines le sont aussi: pour A c'est vrai par hypothèse, pour A' , ses racines sont complexes conjuguées et proches de celles de χ_A , on conclut en remarquant que ces dernières sont simples.)

On rappelle que $GL_n(\mathbb{C})$ est connexe car c'est le complémentaire des zéros du déterminant qui est un polynôme en n^2 variables. Explicitement étant données P_1, P_2 deux matrices inversibles, on considère le polynôme $\det(P_1 z + (1-z)P_2)$. Le complémentaire de l'ensemble (fini) des zéros de ce polynôme est connexe; on considère alors un chemin qui relie 0 à 1 dans ce complémentaire, ce qui fournit un chemin de P_1 à P_2 dans $GL_n(\mathbb{C})$.

En ce qui concerne les matrices à valeurs propres distinctes, c'est le complémentaire des zéros du polynôme en n^2 variable définit comme le discriminant du polynôme caractéristique. Explicitement on procède comme ci-dessus.

Exercice 9. Soit $P \in \mathbb{Z}[X]$, $P = a_0 + a_1X + \dots + a_dX^d$, avec $a_d \neq 0$, α_i les racines de P . On pose:

$$\text{sep}P = \inf_{\alpha_i \neq \alpha_j} |\alpha_i - \alpha_j|.$$

En posant $C = |a_d| + \sup_{1 \leq i \leq d-1} |a_i|$, montrez que pour $d \geq 3$:

$$\text{sep}P \geq (2C)^{-\frac{d(d-1)}{2}+1}.$$

Preuve : (a) Supposons d'abord que les racines de P sont simples. On peut supposer, quitte à changer les indices, que $\text{sep}P = |\alpha_1 - \alpha_2|$. Soit $D(P) \in \mathbb{Z}$ le discriminant de P . On a donc $1 \leq |D(P)|$ puisque les racines sont simples par hypothèse et

$$1 \leq |a_d|^{2d-2} \prod_{i < j} (\alpha_i - \alpha_j)^2, \text{ soit}$$

$$\frac{1}{(\alpha_1 - \alpha_2)^2} \leq |a_d|^{2d-2} \prod_{i < j, (i,j) \neq (1,2)} |\alpha_i - \alpha_j|^2.$$

Mais $|\alpha_i - \alpha_j| \leq |\alpha_i| + |\alpha_j| \leq 2\frac{C}{|a_d|}$, et il y a $\frac{d(d-1)}{2} - 1 = \frac{d^2-d-2}{2}$ facteurs $|\alpha_i - \alpha_j|^2$, ce qui donne:

$$\frac{1}{|\alpha_1 - \alpha_2|^2} \leq \frac{(2C)^{d^2-d-2}}{|a_d|^{d^2-3d}} \leq (2C)^{d^2-d-2}$$

(car $|a_d| \geq 1$ et $d^2 - 3d \geq 0$), d'où le résultat.

(b) Dans le cas général lorsque les racines de $P \in \mathbb{Z}[X]$ ne sont pas nécessairement simples), on peut supposer P primitif quitte à le diviser par son contenu (qui est un entier). On considère le polynôme $R = \text{PGCD}(P, P')$ que l'on peut supposer dans $\mathbb{Z}[X]$ et primitif; on a alors $P = QR$ dans $\mathbb{Z}[X]$, P et R étant primitifs. On peut alors appliquer la méthode de (a) au polynôme Q qui a les mêmes racines que P , mais avec multiplicité 1. On trouve donc, en notant d' le degré de Q , et en utilisant que $d' \leq d$:

$$\frac{1}{(\text{sep}P)^2} = \frac{1}{(\text{sep}Q)^2} \leq (2C)^{d'^2-d'-2} \leq (2C)^{d^2-d-2}.$$

Exercice 10. Polynômes de Tchebichev: Montrez qu'il existe un polynôme $T_n(X)$ à coefficients réels tel que $\cos(n\theta) = T_n(\cos\theta)$, de degré n et de coefficient dominant 2^{n-1} . En déduire le calcul de $\prod_{k=0}^{n-1} \cos(\frac{\pi}{2n} + \frac{k\pi}{n})$. Soit $P \in \mathbb{R}[X]$ unitaire de degré n ; montrez que $\sup_{x \in [-1,1]} |P(x)| \geq \frac{1}{2^{n-1}}$.

Preuve : On a classiquement $T_n(X) = \sum_{0 \leq 2k \leq n} (-1)^k \binom{n}{2k} X^{n-2k} (1-X^2)^k$. De manière évidente on a $\deg T_n \leq n$ et le calcul du coefficient en X^n dans l'expression précédente donne $\sum_{0 \leq 2k \leq n} \binom{2k}{n} = 2^{n-1}$.

On pose pour tout entier k , $\theta_k = \pi/2n + k\pi/n$ de sorte que les $\cos \theta_k$ pour $0 \leq k < n$, sont les racines simples de $T_n(X)$; ainsi on a $\prod_{k=0}^{n-1} \cos(\theta_k) = (-1)^n T_n(0)/2^{n-1}$ soit 0, si n est impair et $(-1)^{n/2}/2^{n-1}$ pour n pair.

Le graphe de $T_n(x)$ pour $x \in [-1, 1]$, oscille entre les valeurs -1 et 1 ; en fait pour tout $y \in]-1, 1[$, l'équation $T_n(x) = 2^{n-1}y$ a exactement n solutions distinctes dans $] -1, 1[$ [une dans chaque intervalle $]\cos(k\pi/n), \cos(k+1)\pi/n[$ pour $0 \leq k < n$. Ainsi étant donné un polynôme unitaire P de degré n tel que $|P(x)| < 1$ pour tout $x \in [-1, 1]$, l'équation $P(x) = T_n(x)/2^{n-1}$ a au moins une solution dans $]\cos(k\pi/n), \cos(k+1)\pi/n[$; en effet par hypothèse $P(\cos(k\pi/n) - T_n(\cos(k\pi/n)))/2^{n-1} < 0$ et $P(\cos(k+1)\pi/n) - T_n(\cos(k+1)\pi/n)/2^{n-1} > 0$. Or le polynôme $P - T_n/Z^{n-1}$ est de degré inférieur à $n-1$ et a au moins n racines, il est donc nul soit $P = T_n$ ce qui n'est pas, d'où le résultat.

Exercice 11. Soit $P(X) = a_dX^d + \dots + a_0 \in \mathbb{C}[X]$ avec $a_d \neq 0$. Montrez que si α est une racine de P , on a

$$|\alpha| \leq M := \sup_{0 \leq i < d} \left(d \frac{|a_i|}{|a_d|} \right)^{\frac{1}{d-i}}$$

Preuve : Soit $z \in \mathbb{C}$ tel que $|z| > M$ alors, pour $0 \leq i < d$, on a $|a_i| < \frac{|a_d|}{d} |z|^{d-i}$ et donc $|a_{d-1}z^{d-1} + \dots + a_0| < |a_d z^d|$ soit $P(z) \neq 0$.

Exercice 12. Soit P un polynôme à coefficients réels; on note $V(x)$ le nombre de changements de signes de la suite

$$(P(x), P'(x), \dots, P^{(d)}(x))$$

Soit $[a, b]$ un intervalle tel que $P(a)P(b) \neq 0$; montrez que le nombre de racines distinctes de P dans l'intervalle $[a, b]$ est inférieur ou égal à $V(a) - V(b)$ et congru à $V(a) - V(b)$ modulo 2. En déduire le lemme de Descartes.

Preuve : Si x est une racine d'un $P^{(i)}$ pour $i > 0$ avec $P(x) \neq 0$, alors $V(x^+) - V(x^-)$ est un nombre négatif pair: en effet soit $[i, i+r] \subset [1, d-1]$ un segment tel que $P^{(j)}(x) = 0$ pour $i \leq j \leq i+r$ et $P^{(i-1)}(x)P^{(i+r+1)} \neq 0$, on remarque que $i+r < d$ car $P^{(d)}$ est une constante non nulle, on a alors $P^{(i+k)}(x+h) = h^{r+1-k}P^{(i+r+1)}(x) + o(h^2)$ de sorte le nombre de changements de signes de la sous-suite $(P^{(i)}(x^-), \dots, P^{(i+r+1)}(x^-))$ est maximal tandis que celui de $(P^{(i)}(x^+), \dots, P^{(i+r+1)}(x^+))$ est minimal, de sorte que la différence du nombre de changements de signes de la sous-suite $(P^{(i-1)}, \dots, P^{(i+r+1)})$ est négatif ou nul. On conclut alors aisément que $V(x^+) - V(x^-)$ est négatif ou nul; ce nombre est de plus pair car les signes des deux extrémités $P, P^{(d)}$ est le même en x^- et x^+ et que le signe de $P^{(d)}(x)$ est égal au signe de $P(x)$ multiplié par $(-1)^{V(x)}$.

Si x est une racine de P d'ordre r , le même raisonnement permet de conclure que $V(x^-) - V(x^+)$ est égal à $k + 2l$ pour un certain entier l .

On en déduit alors facilement l'énoncé de l'exercice, et le lemme de Descartes en découle directement.

Exercice 13. Soit $F(x) = \sum_{i=0}^n P_i(x)e^{\alpha_i x}$ où $P_i \in \mathbb{R}[X]$ est de degré d_i ; montrez que le nombre de zéros de F dans \mathbb{R} est fini et inférieur ou égal à $\sum_{i=0}^n d_i + n$ et que cette borne est atteinte.

Preuve : On pose $G(x) = e^{-\alpha_0 x} F(x)$ et on raisonne par récurrence sur la somme m des degrés des P_i , le premier cas, $m = 0$ étant évident; par hypothèse de récurrence $G^{(d_0)}$ a alors au plus $\sum_{i=1}^n d_i + (n-1)$ zéros réels de sorte que d'après le théorème de Rolle G a au plus $\sum_{i=0}^n d_i + n$ zéros réels.

Exercice 14. Soit $P \in \mathbb{C}[X]$; montrez que les zéros complexes de P' sont dans l'enveloppe convexe des zéros de P .

Soit $K \subset \mathbb{C}$ un convexe, montrez que l'ensemble des $\omega \in \mathbb{C}$ tels que les solutions de $P(z) = \omega$ soient contenues dans K , est un convexe de \mathbb{C} .

Indication: considérez $Q(Z) = (P(Z) - \omega_1)^{n_1} (P(Z) - \omega_2)^{n_2}$.

Preuve : Soit $z \in \mathbb{C}$ une racine de P' et supposons $P(z) \neq 0$; on écrit $\frac{P'(z)}{P(z)} = \sum_{i=1}^n \frac{1}{z - z_i} = 0$ soit $\sum_{i=1}^n \frac{z - z_i}{|z - z_i|^2} = 0$ et donc $z = \frac{\sum_{i=1}^n \frac{z_i}{|z - z_i|^2}}{\sum_{i=1}^n \frac{1}{|z - z_i|^2}}$ soit z est un barycentre à coefficients strictement positifs des z_i et appartient donc à l'enveloppe convexe des z_i .

On pose $Q(z) = (P(z) - \omega_1)^{n_1} (P(z) - \omega_2)^{n_2}$ et donc $Q'(z) = (n_1 + n_2)P'(z)(P(z) - \omega_1)^{n_1-1} (P(z) - \omega_2)^{n_2-1} [P(z) - \frac{n_1\omega_2 + n_2\omega_1}{n_1 + n_2}]$. Soit alors $E = \{\omega \in \mathbb{C} / \{z / P(z) = \omega\} \subset K\}$; ainsi pour tous $\omega_1, \omega_2 \in E$ et tous $n_1, n_2 \in \mathbb{N}^\times$, on a $\{z / P(z) = \frac{n_1\omega_2 + n_2\omega_1}{n_1 + n_2}\} \subset \{z / Q'(z) = 0\}$. Or $\{z / Q'(z) = 0\}$ est inclu dans l'enveloppe convexe des zéros de $P(z) - \omega_1$ et $P(z) - \omega_2$ et donc contenu dans K car K est convexe. On conclut alors par un petit argument de topologie en utilisant le fait que \mathbb{Q} est dense dans \mathbb{R} .

Exercice 15. Soient $P \in \mathbb{R}[X]$ et z_1, \dots, z_n ses racines complexes. On note $s_k = \sum_{i=1}^n z_i^k$ et on introduit la forme quadratique q sur \mathbb{R}^n définie sur la base canonique $(e_i)_{1 \leq i \leq n}$ par la forme bilinéaire $f(e_i, e_j) = s_{i+j-2}$. Montrez que la signature de q est $(r + s, s)$ où r (resp. s) est le nombre de racines réelles (resp. complexes non réelles) distinctes de P : $n = r + 2s$.

En déduire l'énoncé suivant:

Pour $1 \leq k \leq n-1$, il existe des polynômes $P_{k,n} \in \mathbb{R}[X_1, \dots, X_n]$ à n variables tels que pour tout $P(X) = X^n - a_{n-1}X^{n-1} + \dots + (-1)^n a_0 \in \mathbb{R}[X]$, P est scindé à racines simples réelles si et seulement si $P_{k,n}(a_0, \dots, a_{n-1}) > 0$, $\forall k = 1, \dots, n-1$.

Remarque: Quel retrouve-t-on pour $n = 2$?

Preuve : Pour $x = \sum_{i=1}^n x_i e_i$ et $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, on a

$$f(x, x) = \sum_{1 \leq p, q \leq n} x_p x_q s_{p+q-2} = \sum_{1 \leq p, q, k \leq n} x_p x_q z_k^{p+q-2} = \sum_{k=1}^n \left(\sum_{p=1}^n x_p z_k^{p-1} \right)^2.$$

On note $\alpha_1, \dots, \alpha_r$ les racines réelles distinctes de P , m_1, \dots, m_r leur multiplicité, et $\beta_1, \bar{\beta}_1, \dots, \beta_s, \bar{\beta}_s$ les racines complexes de P , n_1, \dots, n_s leur multiplicité. On a alors $f(x, x) = \sum_{k=1}^r m_k \left(\sum_{p=1}^n x_p \alpha_k^{p-1} \right)^2 + \sum_{k=1}^s n_k \left(\sum_{p=1}^n x_p (\beta_k^{p-1} + \bar{\beta}_k^{p-1}) \right)^2$ qui est donc égal à $\sum_{k=1}^r n_k ({}^t X A_k)^2 + 2 \sum_{k=1}^s n_k [({}^t X B_k)^2 - ({}^t X C_k)^2]$ avec $A_k = \begin{pmatrix} 1 \\ \alpha_k \\ \vdots \\ \alpha_k^{n-1} \end{pmatrix}$ et $B_k + iC_k =$

$\begin{pmatrix} 1 \\ \beta_k \\ \vdots \\ \beta_k^{n-1} \end{pmatrix}$. Or la matrice $(A_1, \dots, A_r, B_1 + iC_1, \dots, B_s + iC_s)$ est une matrice de Vandermonde et est donc

inversible, de sorte que la famille $(A_1, \dots, A_r, B_1, \dots, B_s, C_1, \dots, C_s)$ est libre sur \mathbb{R} . Ainsi la signature de q est $(r + s, s)$.

Pour montrer la proposition, il suffit alors de remarquer que $r = n$ est équivalent à dire que q est définie positive

ce qui est équivalent à demander la stricte positivité des mineurs principaux $\Delta_i = \begin{vmatrix} s_0 & \cdots & s_{i-1} \\ \vdots & & \vdots \\ s_{i-1} & \cdots & s_{2i-2} \end{vmatrix}$ pour

$1 \leq i \leq n$; en remarquant que pour $i = 1$, on a $s_0 = n > 0$, on obtient $n - 1$ polynômes en n variables.

En particulier pour $n = 2$, $P(X) = X^2 - \sigma_1 X - \sigma_2$, on obtient $P_{1,2} = s_0 s_2 - s_1^2$ avec $s_0 = 2, s_1 = \sigma_1$ et $s_2 = \sigma_1^2 - 2\sigma_2$ soit $P_{1,2} = \sigma_1^2 - 4\sigma_1 \sigma_2$ qui est le discriminant bien connu.

Exercice 16. Partage de secret: Soit p un nombre premier "grand"; tous les entiers considérés dans la suite seront supposés inférieurs à p . Soit s_0 un entier. On choisit alors $n - 1$ entiers s_1, \dots, s_{n-1} "au hasard" (inférieur à p donc) et soit P le polynôme $\sum_{i=0}^{n-1} s_i X^i$.

(1) On introduit les n formes linéaires: $f_i : Q \in \mathbb{Q}_{n-1}[X] \mapsto Q(i) \in \mathbb{Q}$. En considérant les polynômes de Lagrange

$$L_i(X) = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} \frac{X - j}{i - j}$$

montrer que la famille $(f_i)_{0 \leq i \leq n-1}$ est libre. Montrer alors que la connaissance des $P(i)$ pour $1 \leq i \leq n$, permet de retrouver s_0 .

(2) On fixe $1 \leq i_0 \leq n$; décrivez

$$\bigcap_{\substack{1 \leq i \leq n \\ i \neq i_0}} \text{Ker } f_i$$

On suppose connu les $P(i)$ pour $1 \leq i \neq i_0 \leq n$. Sachant que $P(X)$ est de la forme $\sum_{i=0}^{n-1} s_i X^i$, que sait-on sur s_0 ?

(3) On suppose désormais connue la congruence modulo p des $P(i)$ pour $i \neq i_0$, i.e. le reste de la division euclidienne de $P(i)$ par p . Montrer alors que l'on ne sait rien sur s_0 .

Indication (on l'admettra) : l'ensemble des restes de la division euclidienne par p de $\lambda \frac{n!}{i_0}$ lorsque λ décrit \mathbb{Z} , est égal à $\{0, 1, \dots, p - 1\}$.

(4) Le code pour déclencher une frappe nucléaire est un nombre inférieur à p que seul le président connaît. Au cas où celui-ci serait dans l'impossibilité d'agir, il est prévu que son état major constitué de n membres puissent déclencher la frappe sans que toutefois $n - 1$ parmi eux y parviennent. Proposer une solution mathématique à ce problème en vous inspirant des questions précédentes.

(5) Généraliser la question précédente au cas où l'on voudrait que k d'entre eux le puissent sans que $k - 1$ n'y parviennent.

Preuve : (1) Le polynôme $\sum_{i=0}^{n-1} P(i)L_i(X) - P(X)$ est dans $\mathbb{Q}_{n-1}[X]$ et appartient à l'intersection des noyaux $\text{Ker } f_i$ où f_i est la forme linéaire $Q \in \mathbb{Q}_n[X] \mapsto Q(i) \in \mathbb{Q}$. Or la famille des $(f_i)_{0 \leq i \leq n-1}$ est libre; en effet étant donnée une relation $\sum_i \lambda_i f_i = 0$, en la testant sur L_i , on obtient $\lambda_i = 0$. Ainsi l'espace vectoriel $\bigcap_{i=0}^{n-1} \text{Ker } f_i$ est de dimension nulle de sorte que $P(X) = \sum_{i=0}^{n-1} P(i)L_i(X)$.

(2) Comme précédemment soit $Q \in \mathbb{Q}_{n-1}[X]$ tel que $Q(i) = P(i)$ pour tout $0 \leq i \neq i_0 \leq n-1$. Ainsi $P - Q$ appartient à $\bigcap_{\substack{0 \leq i \leq n-1 \\ i \neq i_0}} \text{Ker } f_i$ qui est de dimension 1 engendré par $\prod_{0 \leq i \neq i_0 \leq n-1} (X - i)$ de sorte qu'il existe $\lambda \in \mathbb{Q}$ tel

que $Q(X) = P(X) + \lambda \prod_{i \neq i_0} (X - i)$; or Q est à coefficients dans \mathbb{Z} de sorte que $\lambda \in \mathbb{Z}$. Ainsi pour le coefficient constant de Q on obtient $s_0 + (-1)^{n-1} \lambda \frac{n!}{i_0}$ où $\lambda \in \mathbb{Z}$ est non déterminé; on connaît alors s_0 à un multiple de $\frac{n!}{i_0}$ près. Si $p < \frac{n!}{i_0}$, alors s_0 est connu.

(3) l'indication correspond à dire que $\frac{n!}{i_0}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$, on le prouve en écrivant une relation de Bezout...

Comme précédemment on a $s_0 + \lambda \frac{n!}{i_0}$ or $\frac{n!}{i_0}$ est inversible, de sorte que lorsque λ décrit $\mathbb{Z}/p\mathbb{Z}$, $s_0 + \lambda \frac{n!}{i_0}$ aussi; bref on ne sait rien sur s_0 .

(4) Le code est s_0 . On tire au sort les s_i , et on transmet $P(i)$ modulo p à la personne numérotée i . D'après (2), les n personnes réunies peuvent reconstituer s_0 alors que d'après (3), $n-1$ quelconques ne le peuvent pas.

(5) De la même façon soit $P(X) = \sum_{i=0}^{k-1} s_i X^i$ et on transmet $P(i)$ à la personne i pour $1 \leq i \leq n$. Comme précédemment, k personnes quelconques peuvent reconstituer P et donc s_0 alors que $k-1$ quelconques ne le peuvent pas

Remarque: Si une personne malintentionnée i_0 transmet une mauvaise valeur distincte de $P(i_0)$ alors que toutes les autres transmettent leur $P(i)$, la personne i_0 sera la seule à connaître le code s_0 . Bien sur s'il y a deux qui trichent, personne ne sait rien.

Exercice 17. Soient P et Q deux polynômes non constants de $\mathbb{C}[X]$ tels que l'ensemble des racines de P (resp. $P-1$) soit égal à l'ensemble des racines de Q (resp. $Q-1$). Montrez que $P = Q$.

Preuve : Soit $R = P - Q$, on a $\deg R \leq n$ et on va montrer que R a plus de $n+1$ racines ce qui impliquera que R est nul. Par hypothèse R s'annule sur les racines de P et de $P-1$. Le nombre de racines distinctes de P est égal à $\deg P - \deg P \wedge P'$. Or comme P et $P-1$ sont premiers entre eux, $P \wedge P'$ et $(P-1) \wedge P'$ sont deux diviseurs distincts de P' de sorte que $\deg P \wedge P' + \deg (P-1) \wedge P' \leq n-1$. Il en résulte que R s'annule sur plus de $2n - (n-1) = n+1$ racines distinctes.

Exercice 18. On considère le polynôme $X^{14} - 7.13X^2 - 14.6X - 13.6$. Que pouvez vous dire du nombre de racines réelles positives et négatives de ce polynôme en utilisant la règle de Descartes puis celle de Sturm.

Preuve : D'après le lemme de Descartes, le nombre de racines réelles positives est inférieur à

$$V(P) = V(-13.6, -14.6, -7.13, 1) = 1$$

tout en y étant congru modulo 2, ce qui donne donc exactement 1 racine positive. En ce qui concerne les racines réelles négatives, on considère le polynôme $P(-X) = X^{14} - 7.13X^2 + 14.6X - 13.6$ de sorte que le nombre de racines négatives est inférieur à $V(P(-X)) = V(-13.6, 14.6, -7.13, 1) = 3$ tout en y étant congru modulo 2 ce qui donne une ou trois racines réelles négatives.

Afin de déterminer le nombre de racines négatives, on applique la règle de Sturm, soit $P'(X) = 14(X^{13} - 13X - 6)$ de sorte que modulo P' , on a $X^{13} \equiv 13X + 6 \pmod{P'}$ soit $P(X) \equiv X(13X + 6) - 7.13X^2 - 14.6X - 13.6 \equiv -13.6(X^2 + X + 1) \pmod{P'}$. On pose $P_1 = 13.6(X^2 + X + 1)$ de sorte que $X^3 \equiv 1 \pmod{P_1}$ et donc $X^{13} \equiv X \pmod{P_1}$ de sorte que $P' \equiv -14(X - 13X + 6) \equiv -14.6(2X + 1) \pmod{P_1}$. On pose $P_2 = 14.6(2X + 1)$ de sorte que $P_1 \equiv 13.6((-1/2)^2 + (-1/2) + 1) \equiv 13.6.3/4 \pmod{P_2}$. La règle de Sturm donne alors que le nombre de racines réelles négatives de P est égale à $V(P, P', -\infty) - V(P, P', 0) = V(1, -14, 13.6, -12, 3/4) - V(-13.6, -6.14, 13.6, 12, 3/4) = 4 - 1 = 3$. On retrouve par ailleurs que le nombre de racines réelles positives est égale à $V(P, P', 0) - V(P, P', +\infty) = V(-13.6, -6.14, 13.6, 12, 3/4) - V(1, 14, 13.6, 12, 3/4) = 1 - 0 = 1$.

Exercice 19. On considère la courbe paramétrée $x(t) = t^2 + t + 1$, $y = \frac{t^2 - 1}{t^2 + 1}$. En donner une équation algébrique.

Preuve : L'équation algébrique est donnée par le résultant des polynômes à coefficient dans $\mathbb{Q}[x, y]$, $t^2 + t + 1 - x$ et $t^2 - 1 - y(t^2 + 1)$, soit

$$\begin{vmatrix} 1 & 1 & 1-x & 0 \\ 0 & 1 & 1 & 1-x \\ 1-y & 0 & -1-y & 0 \\ 0 & 1-y & 0 & -1-y \end{vmatrix}$$

soit $y^2x^2 - 2yx^2 + (y+x)^2 - 2x + 3 = 0$.

Exercice 20. Calculer le discriminant du polynôme $P(X) = X^3 + pX + q$

(i) En appliquant la définition.

(ii) En calculant la suite de Sturm $S(P, P')$.

Preuve : (i) Il s'agit de calculer le déterminant suivant

$$\begin{vmatrix} q & p & 0 & 1 & 0 \\ 0 & q & p & 0 & 1 \\ p & 0 & 3 & 0 & 0 \\ 0 & p & 0 & 3 & 0 \\ 0 & 0 & p & 0 & 3 \end{vmatrix}$$

On peut par exemple faire les manipulations suivantes sur les lignes: $L_5 \leftarrow L_5 - 3L_2$ et $L_4 \leftarrow L_4 - 3L_1$ ce qui donne la matrice suivante:

$$\begin{vmatrix} q & p & 0 & 1 & 0 \\ 0 & q & p & 0 & 1 \\ p & 0 & 3 & 0 & 0 \\ -3q & -2p & 0 & 0 & 0 \\ 0 & -3q & -2p & 0 & 0 \end{vmatrix}$$

ce qui donne $4p^3 + 27q^2$.

(ii) On suppose pour commencer $p \neq 0$. En notant que $X^2 \equiv -p/3 \pmod{3X^2 + p}$, on obtient $X^3 + pX + q \equiv \frac{2pX}{3} + q \pmod{3X^2 + p}$ soit $P_1(X) = -(\frac{2pX}{3} + q)$. Ensuite on a $3X^2 + p \equiv 3(\frac{-3q}{2p})^2 + p \equiv \frac{27q^2 + 4p^3}{4p^2} \pmod{P_1}$. Ainsi P et P' sont premiers entre eux, si et seulement si $27q^2 + 4p^3 \neq 0$ de sorte que $P(X) = X^3 + pX + q$ et P' ont une racine commune si et seulement si $27q^2 + 4p^3 = 0$, de sorte que le discriminant est égale à $27q^2 + 4p^3$ (cf. le corollaire (5.3.3)).

Pour $p = 0$, on a $X^3 + q \equiv q \pmod{3X^2}$ de sorte que $P(X) = X^3 + q$ et P' ont une racine commune si et seulement si $q = 0$, soit si et seulement si $27q^2 = 0$, d'où le résultat.

Exercice 21. Calculer le résultant $R_Y(P, Q)$ des polynômes $P_X(Y) = X^2 - XY + Y^2 - 1$ et $Q_X(Y) = 2X^2 + Y^2 - Y - 2$ considérés comme des éléments de $\mathbb{R}[X][Y]$, i.e. comme des polynômes en Y à coefficients dans $\mathbb{R}[X]$. Trouver alors les points d'intersections des ellipses d'équations $P = 0$ et $Q = 0$.

Preuve : On considère donc $P_X(Y)$ et $Q_X(Y)$ comme des polynômes à coefficients dans $\mathbb{C}[X]$. Le résultant est alors donné par le déterminant

$$\begin{vmatrix} 1 & -X & X^2 - 1 & 0 \\ 0 & 1 & -X & X^2 - 1 \\ 1 & -1 & 2X^2 - 2 & 0 \\ 0 & 1 & -1 & 2X^2 - 2 \end{vmatrix}$$

Un calcul aisé nous donne alors $3X(X^2 - 1)(X - 1)$.

Les points d'intersection cherchés ont pour abscisse 0, 1 et -1 ce qui donne, en calculant Y , les points (0, -1), (1, 0), (1, 1) et (-1, 0), soit 4 points réels (pour rappel le théorème de Bezout donne 4 points à priori complexe dans le plan projectif).

Exercice 22. Soient $C_X(Y) = X^2 + Y^2 + bY + c$ et $P_X(Y) = X^2 + Y + g$ où b, c, g sont des réels.

(a) Calculer le résultant $R_Y(C, P)$.

(b) Donner une condition sur b, c, g pour que les points d'intersection de l'ellipse C avec la parabole P aient la même abscisse (réelle ou complexe).

(c) Donner des conditions sur b, c, g pour que tous les points d'intersection de P et C soient réels. Retrouvez cette condition en utilisant la règle de Sturm.

Preuve : (i) Le résultant est donné par le déterminant

$$\begin{vmatrix} 1 & b & X^2 + c \\ 1 & X^2 + g & 0 \\ 0 & 1 & X^2 + g \end{vmatrix}$$

soit $X^4 + (2g - b + 1)X^2 + (g^2 - bg + c)$: c'est évidemment ce que l'on trouve en éliminant Y dans les deux équations. On pose dans la suite $\alpha = 2g - b + 1$ et $\beta = g^2 - bg + c$.

(ii) Si on veut 4 points de même abscisse, i.e. $P(X) = X^4 + \alpha X^2 + \beta = (X - x_0)^4$, il faut $x_0 = 0$ ce qui revient à imposer $\alpha = \beta = 0$.

(iii) Pour avoir 4 racines réelles il faut et il suffit que l'équation $Z^2 + \alpha Z + \beta = 0$ ait deux racines réelles positives, soit $\delta = \alpha^2 - 4\beta \geq 0$, $\beta \geq 0$ et $\alpha \leq 0$ (la somme des racines et le produit doivent être positifs).

En utilisant la règle de Sturm, on effectue les divisions euclidiennes suivantes:

$$\begin{aligned} X^4 + \alpha X^2 + \beta &= (4X^3 + 2\alpha X) \frac{X}{4} - (-X^2 \frac{\alpha}{2} - \beta) \\ 4X^3 + 2\alpha X &= (-X^2 \frac{\alpha}{2} - \beta) (-X \frac{8}{\alpha}) - (-X \frac{2\delta}{\alpha}) \\ -X^2 \frac{\alpha}{2} - \beta &= (-X \frac{2\delta}{\alpha}) X \frac{\alpha^2}{4\delta} - \beta \end{aligned}$$

de sorte que $V(P, P', -\infty) = V(1, -4, -\alpha/2, 2\delta/\alpha, \beta)$ et $V(P, P', +\infty) = V(1, 4, -\alpha/2, -2\delta/\alpha, \beta)$. Si on veut 4 racines réelles il faut $V(P, P', -\infty) - V(P, P', +\infty) = 4$ soit $V(P, P', -\infty) = 4$ et $V(P, P', +\infty) = 0$ soit $\alpha \leq 0$, $\delta \geq 0$ et $\beta \geq 0$.

Exercice 23. (i) Soient A et B deux polynômes de $K[X]$ où K est un corps. Fabriquez un polynôme dont les racines sont les sommes d'une racine de A et d'une racine de B (on réfléchira à quels sont les Y solutions du système $A(X) = B(Y - X) = 0$).

(ii) Construisez un polynôme à coefficients entiers qui possède $\sqrt{2} + \sqrt[3]{7}$ pour racine.

Preuve : (i) Le système en d'équations $A(X) = B(Y - X) = 0$ possède comme solutions les couples $(x_a, x_b + x_a)$ où x_a (resp. x_b) décrit les solutions de $A(X) = 0$ (resp. $B(X) = 0$). On considère alors les polynômes $A(X)$ et $B(Y - X)$ comme des polynômes à valeurs dans $K[Y]$ et on introduit leur résultant qui est un polynôme en Y dont les zéros sont d'après ce qui précède, exactement les sommes des zéros de A avec ceux de B .

(ii) Appliquons ce qui précède à $A(X) = X^2 - 2$ et $B(X) = X^3 - 7$. Le résultant en question est donné par le déterminant

$$\begin{vmatrix} 1 & 0 & -2 & 0 & 0 \\ 0 & 1 & 0 & -2 & 0 \\ 0 & 0 & 1 & 0 & -2 \\ -1 & 3Y & -3Y^2 & Y^3 - 7 & 0 \\ 0 & -1 & 3Y & -3Y^2 & Y^3 - 7 \end{vmatrix}$$

soit après calcul $Y^6 - 6Y^4 - 14Y^3 + 12Y^2 - 84Y + 41$.