1. Discriminant de 2 polynômes

Kest un corps, $\overline{K}$ sa clôture algébrique. Soit $P=\sum_{i=0}^{d} a_i X^i \in K[X]$, unitaire ($a_d=1$) de degré d dont les racines (non forcément distinctes) dans $\overline{K}$ sont notées $\alpha_1,\ldots,\alpha_d$. On définit le discriminant de P par $\mathrm{Dis}(P)=\prod_{1\leqslant i<j\leqslant d}(\alpha_i-\alpha_j)^2$.

1. Montrer qu'il existe un polynôme à coefficients entiers $D_d(u_1,\ \ldots,\ u_d)$ tel que $\mathrm{Dis}(P)=D_d(a_1,\ldots,a_d)$. En déduire que $\mathrm{Dis}(P)\in K$.
2. Montrer que $\mathrm{Dis}(P)=(-1)^{d(d-1)/2}\mathrm{Res}_X(P,P')$
3. Montrer que les propriétés suivantes sont équivalentes
   i. P et P' ont un facteur en commun non constant
   ii. P a une racine multiple dans $\overline{K}$
   iii. $\mathrm{Dis}(P)=0$

On suppose maintenant que $a_d\neq 0$ et a_d non forcément égal à 1 et on pose :

$$\mathrm{Dis}(P)=\mathrm{lc}(P)^{2d-2}\prod_{1\leqslant i<j\leqslant d}(\alpha_i-\alpha_j)^2$$

4. Montrer que $\mathrm{lc}(P)\,\mathrm{Dis}(P)=(-1)^{\frac{d(d-1)}{2}}\mathrm{Res}(P,P')$.

Correction.

1. On considère les indéterminées $T_1,\ .\ .\ .\ ,\ T_d$. On remarque que $\prod_{1\leqslant i<j\leqslant d}(T_i-T_j)^2$ est un polynôme symétrique en les T_i. Il s'écrit donc, et de manière unique, comme polynôme $\Pi(e_1,\ .\ .\ .\ ,\ e_d)$ à coefficients entiers en les polynômes symétriques élémentaires des T_i. On pose alors $D_d(u_1,\ldots,u_d)=\Pi(-u_1,u_2,\ldots,(-1)^d u_d)$. On a bien, pour tout corps K et tout polynôme unitaire $P=\sum_{i=0}^{d} a_i X^i\in K[X], \mathrm{Dis}(P)=D_d(a_1,a_2,\ldots,a_d)$.

2. $\mathrm{Res}(P,\ P')=\prod_{i=1}^{d}P'(\alpha_i)=\prod_{i=1}^{d}\prod_{j\neq i}(\alpha_i-\alpha_j)=(-1)^{\frac{d(d-1)}{2}}\prod_{1\leqslant i<j\leqslant d}(\alpha_i-\alpha_j)=(-1)^{\frac{d(d-1)}{2}}\mathrm{Dis}(P)$

3. Il suffit de se rappeler que $\mathrm{Res}\left(\frac{1}{a_d}P,\frac{1}{a_d}P'\right)=a_d^{2d-1}\mathrm{Res}(P,P')$

2. Majoration des racines d'un poylynôme de $\mathbb{Z}[X]$

Soit $P=\sum_{i=0}^{d} a_i\ X^i\in\mathbb{Z}[X]$, unitaire ($a_d=1$) de degré d. Montrer que pour tout $\alpha\in\mathbb{C}$ tq $P(\alpha)=0$

1. $|\alpha|<1+\max_{i=0}^{d}(|a_i|)$
2. Si $\forall i=0\ldots d,\ a_i\geqslant 0$, alors P n'a aucune racine réelle positive. Si $\alpha\in\mathbb{R}^{+\star}$, alors $\alpha<2\left(\max_{a_i<0}(-a_i)^{\frac{1}{d-i}}\right)$

Correction

1. Supposons $A=\max_{i=0}^{n-1}(|a_i|)$. Pour tout $x\in\mathbb{R}$ tel que $|x|\geq A+1$,

$$|P(x)|\geq|x|^n-A\left(|x|^{n-1}+\ldots+1\right)=|x|^n-\frac{A(|x|^n-1)}{|x|-1}.$$

Comme $|x|\geq A+1$, alors $1\geq A/(|x|-1)$ et donc $|x|^n\geq A|x|^n/(|x|-1)$, ce qui implique $|P(x)|\geq A/(|x|-1)>0$.

2. Si tous les a_i sont positifs, et si il en existe au moins 1 non nul, alors $P(X)>0,\forall x\in\mathbb{R}^{+\star}$

3. Soit $\alpha \in \mathbb{R}^{+\star}$. $P(\alpha) = \sum_{i=0}^{d} a_i \alpha^i$ et on pose $b = \max_{a_i<0} (-a_i)^{\frac{1}{d-i}}$. Comme $a_d = 1$ et $\alpha > 0$, alors $P(\alpha) = 0 \Rightarrow 1 = -\sum_{i=0}^{d-1} \frac{a_i}{\alpha^{d-i}}$.

Ainsi, $1 \leqslant \sum_{(i=0)\wedge(a_i<0)}^{d-1} \frac{-a_i}{\alpha^{d-i}} \leqslant \sum_{i=0}^{d-1} \left(\frac{b}{\alpha}\right)^{d-i}$ et $1 \leqslant \sum_{i=1}^{d} \left(\frac{b}{\alpha}\right)^{i} < \sum_{i>1} \left(\frac{b}{\alpha}\right)^{i} = \frac{b}{\alpha}\left(\frac{1}{1-\frac{b}{\alpha}}\right) = \frac{b}{\alpha - b}$ et donc $\alpha < 2\,b$.

3. Séparation des racines d'un polynôme de $\mathbb{Z}[X]$

Soit $P = \sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X]$ de degré d sans facteur carré, dont les racines complexes sont notées $\alpha_1, \ldots, \alpha_d$.

On définit la borne de Mahler de P par $M(P) = |a_n| \prod_{k=1}^{d} \max(1, |\alpha_k|)$ et le séparateur de P comme étant la distance minimale entre 2 racines distintes de P : $\mathrm{sep}(P) = \min_{i \neq j} |\alpha_i - \alpha_j|$. On note $||P||_2 = \sqrt{\sum_{i=0}^{d} a_i^2}$.

1) Soit

$$P_d = \begin{bmatrix} 1 & \ldots & 1 \\ \alpha_1 & \ldots & \alpha_d \\ \vdots & & \vdots \\ \alpha_1^{d-1} & \ldots & \alpha_d^{d-1} \end{bmatrix}$$

Montrer que $a_d^{2d-2} \det(P_d)^2 = |\mathrm{Discrim}(P)|$

2) On ordonne les racines de P de telle sorte que $|\alpha_1| \geq \ldots \geq |\alpha_m| \geq 1 \geq |\alpha_{m+1}| \geq \ldots |\alpha_d|$.
Monter que

$$\frac{\det(P_d)}{(\alpha_i - \alpha_j)} = \begin{vmatrix} 1 & \ldots & 1 & 0 & 1 & \ldots & 1 \\ \alpha_1 & \ldots & \alpha_{i-1} & q_1 & \alpha_{i+1} & \ldots & \alpha_d \\ \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{d-1} & \ldots & \alpha_{i-1}^{d-1} & q_{d-1} & \alpha_{i-1}^{d+1} & \ldots & \alpha_d^{d-1} \end{vmatrix}$$

avec $q_1 = 1$ et $q_l = \alpha_i^{l-1} + \alpha_i^{l-2}\alpha_j + \ldots + \alpha_i \alpha_j^{l-2} + \alpha_j^{l-1}$ pour $l > 1$.

3) Montrer que si on suppose $i > j$, $\frac{\mathrm{Discrim}(P)}{a_d^{2d-2} |(\alpha_i - \alpha_j) \prod_{i=1\ldots m} \alpha_i^{d-1}|^2} \leq \frac{d^{d-1}\, d\,(d-1)\,(2\,d-1)}{6}$

4) En déduire que $\mathrm{sep}(P)^2 \geq \frac{3}{(M(P)^{d-1})^2} \cdot \frac{1}{d^{d+2}}$

5) Montrer que pour tout $z \in \mathbb{C}^*$, $||\,(\bar{z}x - 1)P(x)||_2 = ||\,(x - z)\,P(x)||_2$

6) On suppose que $P(x) = a_n \prod_{i=1}^{d} (X - \alpha_i)$ et pour tout m tel que $d > m \geqslant 0$, on pose $Q(X) = a_n \prod_{i=1}^{m} (\bar{\alpha_i} X - 1) \prod_{i=m+1}^{d} (x - \alpha_i)$.

a) Montrer que $\|P\|_2^2 = ||\,Q||_2^2 \geq |a_n|^2 \prod_{i=1}^{m} |\bar{\alpha_i}|^2 + |a_n|^2 \prod_{i=m+1}^{d} |\alpha_i|^2$

b) En déduire que $\mathrm{sep}(P) \geq \sqrt{\frac{3}{d^{d+2}}} \cdot \frac{1}{||\,P||_2^{d-1}}$.

Proposition de Corrigé

1) La matrice P_d est une matrice de Vandermonde et donc $\det(P_d) = \prod_{i<j} (\alpha_i - \alpha_j)$, soit , en faisant apparaitre l'expression du discriminant $\det(P_d)^2 = (\prod_{i<j} (\alpha_i - \alpha_j)^2) = \frac{\mathrm{Discrim}(P)}{a_d^{2d-2}}$.

Pour le déterminant de la matrice de Vandermonde, si le résultat n'est pas connu, il se redémontre simplement :

On remplace la ligne $L_i \leftarrow L_i - \alpha_1 L_{i-1}$ en partant de L_d et en remontant vers L_2 ce qui nous donne :

$$\det(P_d) = \det\left(\begin{bmatrix} 1 & 1 & \dots & 1 \\ 0 & \alpha_2-\alpha_1 & \dots & \alpha_d-\alpha_1 \\ \vdots & & & \vdots \\ 0 & \alpha_2^{d-2}(\alpha_2-\alpha_1) & \dots & \alpha_d^{d-2}(\alpha_d-\alpha_1) \end{bmatrix}\right)$$

Puis en développant selon la première colonne :

$$=\det\left(\begin{bmatrix} \alpha_2-\alpha_1 & \dots & \alpha_d-\alpha_1 \\ & & \vdots \\ \alpha_2^{d-2}(\alpha_2-\alpha_1) & \dots & \alpha_d^{d-2}(\alpha_d-\alpha_1) \end{bmatrix}\right) = \prod_{i=2}^{n}(\alpha_i-\alpha_1)\det\left(\begin{bmatrix} 1 & \dots & 1 \\ \alpha_2 & \dots & \alpha_d \\ \vdots & & \vdots \\ \alpha_2^{d-2} & \dots & \alpha_d^{d-2} \end{bmatrix}\right)$$

On conclut par récurrence.

2) Il suffit de remarquer que si on retranche la j-ème ligne à la i-ème colonne de la matrice, cette dernière devient $[u_1 \dots, u_d]^T$ avec $u_l = \alpha_i^{l-1} - \alpha_j^{l-1} = (\alpha_i - \alpha_j) q_l$ et on utilise la multi-linéarité du déterminant pour conclure.

3) En divisant les m premières colonnes respectivement par α_i^{d-1} $i = 1 \dots m$ de sorte à avoir des entrées de valeur absolue inférieure à 1 sauf peut-être à la i-ième colonne, on peut voir que :

$$\left|\frac{\det(P_d)}{(\alpha_i-\alpha_j)\prod_{i=1\dots m}\alpha_i^{d-1}}\right|^2 \leq \prod_{j=1}^{d}\|C_j\|^2$$

Le entées de toutes les colonnes sauf peut-être la $i-$ eme sont de module <1 donc , pour $j \neq i$ $\|C_j\|^2 \leqslant d$. Pour ce qui est de la $i-$ eme colonne , comme $\alpha_i > \alpha_j$ $|q_l| = |\alpha_i^{l-1} + \alpha_i^{l-2}\alpha_j + \dots + \alpha_i\alpha_j^{l-2} + \alpha_j| \leqslant l|\alpha_i|^{l-1} \leqslant l$ puisque soit $|\alpha_i| < 1$ soit la i-eme colonne a été divisée par $|\alpha_i|^{d-1}$. Ainsi

$$\left|\frac{\det(P_d)}{(\alpha_i-\alpha_j)\prod_{i=1\dots m}\alpha_i^{d-1}}\right|^2 \leq \prod_{j=1}^{d}\|C_j\|^2 \leq d^{d-1}\sum_{i=0}^{d-1} i^2$$

On fait enfin apparaitre l'expression littérale du discriminant de P

$$\frac{\mathrm{Discrim}(P)}{a_d^{2d-2}|(\alpha_i-\alpha_j)\prod_{i=1\dots m}\alpha_i^{d-1}|^2} \leq \frac{d^{d-1}\,d\,(d-1)\,(2\,d-1)}{6}$$

4) $|\alpha_i - \alpha_j|^2 \geq \frac{\mathrm{Discrim}(P)}{|a_d^{d-1}\prod_{i=1\dots m}\alpha_i^{d-1}|^2}\cdot\frac{3}{d^{d+2}}$. Comme $P \in \mathbb{Z}[X]$ et P est sans facteurs carrés, alors $\mathrm{Discrim}(P) \in \mathbb{Z}^{*+}$, donc $|\alpha_i - \alpha_j|^2 \geq \frac{1}{|a_d^{d-1}\prod_{i=1\dots m}\alpha_i^{d-1}|^2}\cdot\frac{3}{d^{d+2}}$, ce qui montre l'inégalité :

$$\mathrm{sep}(P)^2 \geq \frac{3}{(M(P)^{d-1})^2}\cdot\frac{1}{d^{d+2}}.$$

5)

$$\begin{aligned}
||\,(\bar{z}\,x-1)P(x)||_2^2 &= \textstyle\sum_{k=0}^{d+1}|\bar{z}\,a_{k-1}-a_k|^2 = \sum_{k=0}^{d+1}(\bar{z}\,a_{k-1}-a_k)\,\overline{(\bar{z}\,a_{k-1}-a_k)} \\
&= \textstyle\sum_{k=0}^{d+1}|z|^2|a_{k-1}^2 + |a_k|^2 - 2\,\mathrm{Re}(z\overline{a_{k-1}}a_k) \\
&= (|z|^2+1)||\,P||_2^2 - \textstyle\sum_{k=0}^{d+1}2\,\mathrm{Re}(z\overline{a_{k-1}}a_k) \\
||\,(x-z)\,P(x)||_2^2 &= \textstyle\sum_{k=0}^{d+1}|a_{k-1}-z\,a_k|^2 = \sum_{k=0}^{d+1}(a_{k-1}-z\,a_k)\,\overline{(a_{k-1}-z\,a_k)} \\
&= \textstyle\sum_{k=0}^{d+1}a_{k-1}^2 + |z|^2||a_k|^2 - 2\,\mathrm{Re}(z\overline{a_{k-1}}a_k) \\
&= (|z|^2+1)||\,P||_2^2 - \textstyle\sum_{k=0}^{d+1}2\,\mathrm{Re}(z\overline{a_{k-1}}a_k)
\end{aligned}$$

6)a) D'après le 5) précédent, $||\,Q(x)||_2 = ||\,P(x)||_2$.

6)b) Le terme de tête de $Q(x)$ s'écrit $a_n\prod_{i=1}^{m}(\bar{\alpha}_i)$ et le terme constant de $Q(x)$ s'écrit $a_n\prod_{i=m+1}^{d}(\alpha_i)$. En particulier $||\,Q||_2^2 \geq |a_n|^2\prod_{i=1}^{m}|\bar{\alpha}_i|^2 + |a_n|^2\prod_{i=m+1}^{d}|\alpha_i|^2$.On peut choisir m tel que $|\alpha_i| \geq 1$, $\forall i > m$. Dans ce cas, $M(P)^2 = |a_n|^2\prod_{i=m+1}^{d}|\alpha_i|^2$ et donc $||\,P(x)||_2 = ||\,Q||_2^2 \geq M(P)^2$

4. Isolation des zéros réels d'un poylynôme de $\mathbb{Z}[X]$

Utiliser les 2 exercices précédents pour proposer un algorithme permettant d'isoler les racines réelles d'un polynôme de $\mathbb{Z}[X]$ par des intervalles à bornes rationnelles, c'est à dire fournir une liste disjointe d'intervalles à bornes rationnelles, chaque intervalle contenant une et une seule racine réelle, chaque racine réelle étant contenue dans au moins 1 intervalle.

Cet algorithme est-il efficace ?

Correction

1 - On applique l'algorithme d'Euclide dans $\mathbb{Q}[X]$ pour calculer le partie sans facteurs carrés de P

2 - On calcule un majorant M du module des racines de P

3 - On calcule un minorant m du séparateur des racines de P

4 - On construit calcule $k = \frac{2\,M}{m}$ ainsi que les points $x_i = -M + i\,m$

5 - pour chaque intervalle $]x_i, x_{i+1}]$, on calcule $P(x_i), P(x_{i+1})$.

- Si $P(x_i) = 0$ (resp. $P(x_{i+1}) = 0$) , alors x_i (resp x_{i+1}) est l'unique racine de P dans $[x_i, x_{i+1}]$
- Sinon, Il y a une racine dans $]x_i, x_{i+1}[$ si et seulement si $P(x_i)P(x_{i+1}) < 0$

L'algorithme n'est pas efficace puisqu'il va calculer un nombre "exponentiel" d'intervalles essentiellement égal à $k \approx O\left(\sqrt{d^{d+2}}\|P\|_2^{d-1}\right)$.