Lycée Louis-Le-Grand, Paris
MPSI 4 – Mathématiques
A. Troesch

Pour le 04/04/2019

DM nº 16 : Polynômes

Problème 1 – Théorème de d'Alembert-Gauss

Nous donnons dans ce problème deux preuves du théorème de d'Alembert-Gauss, l'une essentiellement analytique, l'autre essentiellement algébrique (mais reposant sur une propriété analytique simple : l'analyse semble incontournable dans ce théorème).

Partie I – Démonstration analytique

Soit $P = \sum_{k=0}^{n} a_k X^k$ *un polynôme de* $\mathbb{C}[X]$*, qu'on suppose unitaire (sans perte de généralité), et non constant. Montrer le théorème de d'Alembert Gauss revient à montrer l'existence d'une racine de* P*.*

1. Montrer que $|P(z)| \to +\infty$ lorsque $|z| \to +\infty$ ($z \in \mathbb{C}$).

On peut donc considérer $M > 0$ tel que pour tout $z \in \mathbb{C}$, $|z| \geqslant M \Longrightarrow |P(z)| > |P(0)|$.

2. Justifier que le sous-ensemble $\overline{B}(0, M)$ de $\mathbb{C}$ est compact (c'est-à-dire qu'il vérifie la propriété de Bolzano-Weierstrass).
3. Justifier que $|P|$ admet un minimum sur $\overline{B}(0, M)$.

Notre but est de montrer que $P(z_0) = 0$*. Pour cela, on raisonne par l'absurde en supposant que ce n'est pas le cas.*
On note $z_0 \in \overline{B}(0, M)$ *un point en lequel* $|P|$ *atteint son minimum sur cet ensemble. et on fait un changement de variable permettant de centrer le minimum : on considère* Q *le polynôme* $Q(X) = P(z_0 + X)$*, et on pose* (b_k) *ses coefficients :*

$$Q(X) = \sum_{k=0}^{n} b_k X^k.$$

On note $\ell = \inf\{k \in \mathbb{N}^* \mid b_k \neq 0\}$*. Ainsi,*

$$Q(X) = b_0 + \sum_{k=\ell}^{n} b_k X^k.$$

Enfin, on pose c *une racine* ℓ*-ième de* $-\frac{b_0}{b_\ell}$*.*

4. Justifier que $b_0 \neq 0$
5. On pose f la fonction définie sur $\mathbb{R}$ par $f(t) = \left|\frac{Q(tc)}{b_0}\right|$. Montrer qu'il existe $\eta > 0$ tel que pour tout $t \in]0, \eta[$, $|f(t)| < 1$.
6. En déduire une contradiction et conclure.

Partie II – Corps de décomposition d'un polynôme

Soit $\mathbb{K}$ *un corps, et* P *un polynôme de* $\mathbb{K}[X]$*. On veut montrer l'existence d'un corps* $\mathbb{K}'$ *contenant* $\mathbb{K}$ *tel que* P *soit scindé dans* $\mathbb{K}'[X]$*. Si* $\mathbb{K}'$ *est minimal pour cette propriété, on dit que* $\mathbb{K}'$ *est un corps de décomposition de* $\mathbb{K}$*.*
Soit Q *un facteur irréductible (dans* $\mathbb{K}[X]$*) de* P*. On note* (Q) *l'idéal principal de* $\mathbb{K}[X]$ *engendré par* Q*, et on note* $\mathbb{K}_1 = \mathbb{K}[X]/(Q)$ *le quotient de* $\mathbb{K}[X]$ *par l'idéal* (Q) *(cela se comprend au sens d'un quotient de groupe).*

1. Justifier que les lois $+$ et $\times$ de $\mathbb{K}[X]$ passent au quotient et que les lois quotients définissent sur $\mathbb{K}_1$ une structure de corps.

2. Soit $\varphi : \mathbb{K}[X] \longrightarrow \mathbb{K}_1$ la projection canonique. Montrer que φ est un morphisme d'anneau, et que sa restriction à $\mathbb{K}$ est injective.

   Ainsi, on peut identifier $\mathbb{K}$ à son image $\Phi(\mathbb{K}) \subset \mathbb{K}_1$. Via cette identification, on peut considérer que $\mathbb{K} \subset \mathbb{K}_1$.

3. En considérant $\theta = \varphi(X)$, montrer que P, vu comme polynôme de $\mathbb{K}_1[X]$, admet une racine dans $\mathbb{K}_1$.
4. En raisonnant par récurrence, montrer l'existence d'un corps $\mathbb{K}_2$ contenant $\mathbb{K}$ dans lequel P est scindé.
5. Montrer l'existence d'un sous-corps minimal de $\mathbb{K}_2$ contenant $\mathbb{K}$, dans lequel P est scindé.

Partie III – Polynômes symétriques

Soit $\mathbb{K}[X_1, \ldots, X_n]$ l'anneau des polynômes à n indéterminées à coefficients dans $\mathbb{K}$, qui peut se définir récursivement par

$$\mathbb{K}[X_1, \ldots, X_n] = \mathbb{K}[X_1, \ldots, X_{n-1}][X_n].$$

Les éléments de $\mathbb{K}[X_1, \ldots, X_n]$ s'écrivent de façon unique comme combinaison linéaire de monômes $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$.
Soit $P \in \mathbb{K}[X_1, \ldots, X_n]$. On dit que P est symétrique si pour tout $\sigma \in \mathfrak{S}_n$, on a :

$$P(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

On définit les polynômes symétriques élémentaires :

$$\Sigma_k = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} X_{i_1} X_{i_2} \cdots X_{i_k}.$$

Le but de cette partie est de montrer que l'ensemble S des polynômes symétriques de $\mathbb{K}[X_1, \ldots, X_n]$ est le sous-anneau de $\mathbb{K}[X_1, \ldots, X_n]$ engendré par les polynômes symétriques élémentaires.

1. Montrer que S est un sous-anneau de $\mathbb{K}[X_1, \ldots, X_n]$.
2. Pour $P \in \mathbb{K}[X_1, \ldots, X_n]$, on note $\mathrm{MD}(P)$ le monôme directeur de P, égal au monôme $aX_1^{\alpha_1} \ldots X_n^{\alpha_n}$ de la décomposition de P pour lequel $(\alpha_1, \ldots, \alpha_n)$ est maximal pour l'ordre lexicographique.

   Montrer que si P est un polynôme symétrique, alors

$$\mathrm{MD}(P) = aX_1^{\alpha_1} \ldots X_n^{\alpha_n} \Longrightarrow \alpha_1 \geqslant \cdots \geqslant \alpha_n.$$

3. Montrer que pour tout $P, Q \in \mathbb{K}[X_1, \ldots, X_n]$, $\mathrm{MD}(PQ) = \mathrm{MD}(P)\mathrm{MD}(Q)$.
4. Soit $\alpha_1 \geqslant \cdots \geqslant \alpha_n$ des entiers naturels. Montrer que

$$\mathrm{MD}(\Sigma_1^{\alpha_1 - \alpha_2} \cdots \Sigma_{n-1}^{\alpha_{n-1} - \alpha_n} \Sigma_n^{\alpha_n}) = X_1^{\alpha_1} \cdots X_n^{\alpha_n}.$$

5. En raisonnant par récurrence sur $(\alpha_1, \ldots, \alpha_n)$ le n-uplet des exposants du monôme directeur de P, montrer que tout polynôme symétrique s'ecrit comme combinaison linéaire de produits de polynômes symétriques élémentaires, et conclure. On pourra considérer l'ordre lexicographique sur les n-uplets $(\alpha_1, \ldots, \alpha_n)$, et on justifiera la validité de la « récurrence » ainsi faite sur l'ordre lexicographique.

Partie IV – Les polynômes de degré impair > 1 ne sont pas irréductibles dans $\mathbb{C}[X]$

On montre dans cette partie qu'un polynôme de degré impair strictement supérieur à 1 n'est pas irréductible. On rappelle que pour tout corps $\mathbb{K}$, l'anneau $\mathbb{K}[X]$ est principal, et on admettra que cela implique que $\mathbb{K}[X]$ est factoriel, donc que tout polynôme de $\mathbb{K}[X]$ se décompose de façon unique (à inversibles près, et à l'ordre près des facteurs) comme produit de polynômes irréductibles.

1. Soit $P \in \mathbb{R}[X]$ de degré impair. Montrer que P admet une racine réelle.

On considère $P \in \mathbb{C}[X]$ de degré impair $n = 2p + 1 > 1$.
Si $P = \displaystyle\sum_{k=0}^{n} a_k X^k$, on note $\overline{P} = \displaystyle\sum_{k=0}^{n} \overline{a_k} X^k$.
On suppose que P est unitaire et irréductible, et on pose $Q = P\overline{P}$.

2. Justifier que $P \notin \mathbb{R}[X]$ et $Q \in \mathbb{R}[X]$.
3. Montrer que Q est irréductible dans $\mathbb{R}[X]$

Soit $\mathbb{K}$ un corps de décomposition de Q sur $\mathbb{C}$, et $\alpha_1, \ldots, \alpha_{2n}$ les racines de Q (non nécessairement distinctes) dans $\mathbb{K}$. On définit le polynôme R par :

$$R = \prod_{1 \leqslant i < j \leqslant 2n} (X - (\alpha_i + \alpha_j)).$$

4. En remarquant que les coefficients de R sont symétriques en les α_i, montrer que $R \in \mathbb{R}[X]$.
5. Montrer que R admet une racine r dans $\mathbb{R}$. On définit :

$$S = Q\left(X + \frac{r}{2}\right) \qquad \text{et} \qquad T = Q\left(-X + \frac{r}{2}\right).$$

   Montrer que $S = T$. En déduire l'existence de $U \in \mathbb{R}[X]$ tel que $S(X) = U(X^2)$
6. En déduire l'existence d'une racine α de P et conclure.

Partie V – Preuve algébrique du théorème de d'Alembert-Gauss

1. Soit P un polynôme de $\mathbb{C}[X]$, et $\alpha_1, \ldots, \alpha_n$ ses racines (non nécessairement distinctes) dans un corps de décomposition $\mathbb{K}$ de P. On considère comme ci-dessus

$$R = \prod_{1 \leqslant i < j \leqslant n} (X - (\alpha_i + \alpha_j)).$$

   Justifier que $R \in \mathbb{C}[X]$, et qu'il existe un polynôme irréductible Q divisant R et dont la valuation 2-adique du degré est strictement inférieure à la valuation 2-adique de degré de P.
2. Montrer le théorème de d'Alembert-Gauss par récurrence sur la valuation 2-adique du degré de P, en adaptant la preuve de la partie IV.