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

Pour le 11/04/2019

DM n° 17 : Polynômes, espaces vectoriels

Problème 1 – La quadrature du cercle

Le but de ce problème est de démontrer la transcendance de π, résultat prouvé par Lindemann à la fin du 19e siècle, et qui met fin à plusieurs siècles, voire millénaires de recherche sur la quadrature du cercle : en effet, une conséquence de la transcendance de π est l'impossibilité de construire à la règle et au compas un carré de même aire qu'un cercle donné.

On commence par l'étude de propriétés des nombres algébriques, le point nous intéressant plus particulièrement étant la stabilité par produit. Ceci nous permet de nous ramener à l'étude de la transcendance de $\mathrm{i}\,\pi$, qu'on étudie en remarquant de ce nombre vérifie une équation simple $\mathrm{e}^{\mathrm{i}\,\pi}+1=0$.

On pourra admettre que si A est un anneau intègre et si $P \in A[X_1,\dots,X_n]$ est un polynôme symétrique en les X_i (c'est-à-dire invariant par permutation des variables), de degré n, alors il peut s'écrire comme polynôme à coefficients dans A, de degré au plus n, en les polynômes symétriques élémentaires

$$\Sigma_k = \sum_{1\leqslant i_1<\dots<i_k\leqslant n} X_{i_1}\cdots X_{i_k},$$

propriété démontrée dans un DM.

Partie I – Extensions algébriques

Soit K un corps. On appelle extension de K un corps L tel que K soit un sous-corps de L. Soit L une extension de K, et $\alpha \in L$. On dit que α est algébrique sur K s'il existe un polynôme $P \in K[X]$ non nul tel que $P(\alpha)=0$.
Par exemple, dire d'un élément α de $\mathbb{C}$ est algébrique sur $\mathbb{Q}$ équivaut à dire qu'il existe un polynôme à coefficients rationnels $P\neq 0$ tel que $P(\alpha)=0$. Quitte à multiplier les coefficients par le ppcm des dénominateurs des coefficients, cela équivaut à dire qu'il existe un polynôme non nul à coefficients entiers annulant α.
Un élément $\alpha \in L$ non algébrique sur K sera dit transcendant sur K.

1. **Degré d'une extension**
   (a) Soit L une extension de K. Montrer que L est un espace vectoriel sur K. Si L est de dimension finie sur K, on note $[L:K]$ sa dimension, appelée degré de l'extension L sur K.
   (b) Soit L une extension de K de degré fini $[L:K]$, et M une extension de L de degré fini $[M:L]$. En considérant la famille (a_ib_j), où (a_i) est une base de L sur K et (b_j) une base de M sur L, montrer que M est une extension de K de degré fini, et qu'on a la relation :

$$[M:K]=[M:L][L:K].$$

2. **Adjonction d'un élément à un corps**
   (a) Soit $\alpha \in L$. On note $K(\alpha)$ le plus petit sous-corps de L contenant K et α. Justifier l'existence de $K(\alpha)$, et justifier que c'est une algèbre sur K.
   (b) On suppose dans cette question que α est algébrique.
      i. Justifier l'existence d'un polynôme unitaire de degré minimal P_α tel que $P_\alpha(\alpha)=0$, et justifier que P_α est irréductible dans $K[X]$.
      ii. Soit φ_α l'unique application K-linéaire de $K[X]$ dans $K[\alpha]$ telle que pour tout $k\in\mathbb{N}$, $\varphi(X^k)=\alpha^k$. Justifier que φ est un morphisme d'algèbre (c'est-à-dire qu'en plus d'être une application linéaire, c'est aussi un morphisme d'anneau), et déterminer son noyau.

iii. En déduire que $K(\alpha)$ est isomorphe à $K[X]/(P_\alpha)$, où (P_a) désigne l'idéal engendré par P_α

iv. Soit $p : K[X] \mapsto K[X]/(P_\alpha)$ la projection canonique associant à un polynôme P sa classe dans le quotient. Montrer que $(p(1), \cdots, p(X^{d-1}))$ est une base du K-espace vectoriel $K[X]/(P_\alpha)$, où $d = \deg(P_\alpha)$.

3. **Caractérisation des éléments algébriques**

   Montrer que $\alpha \in L$ est algébrique sur K si et seulement si l'extension $K(\alpha)$ sur K est de degré fini, ce qu'on note $[K(\alpha) : K] < +\infty$.

4. **Produit d'éléments algébriques**.

   On dit que l'extension L sur K est algébrique si et seulement si tout élément $\alpha \in L$ est algébrique sur K.

   (a) Montrer que si $[L : K]$ est fini, alors L est algébrique sur K.

   (b) Soit L une extension du corps K et M une extension du corps L. Montrer que si $\alpha \in M$ est algébrique sur K, alors il est algébrique sur L.

   (c) En déduire que si L est une extension de K, et si deux éléments α et β de L sont algébriques, alors $K(\alpha)(\beta)$ (corps obtenu en ajoignant β au corps obtenu en adjoignant α à K) est algébrique sur K.

   (d) En déduire que le produit de deux nombres algébriques est algébrique.

Partie II – Transcendance de π

Dans cette partie, on dira simplement que $\alpha \in \mathbb{C}$ est « transcendant » ou « algébrique », à la place de « transcendant sur $\mathbb{Q}$ » ou « algébrique sur $\mathbb{Q}$ ».

On démontre la transcendance de π par l'absurde. Pour cela, on suppose que π est algébrique. On admettra que π n'est pas rationnel, propriété qu'on prouvera en exercice au courant de l'année.

1. Montrer que sous la supposition faite $\mathrm{i}\,\pi$ est algébrique.

2. Soit P un polynôme minimal unitaire annulant $\mathrm{i}\,\pi$, et soit n son degré.

   (a) Soit K un corps et L une extension de K. Soit Q et R deux polynômes de $K[X]$. Montrer que Q et R sont premier entre eux dans $K[X]$ si et seulement si ils sont premiers entre eux dans $L[X]$.

   (b) Justifier que P est irréductible dans $\mathbb{Q}[X]$, et que toutes ses racines dans $\mathbb{C}$ sont simples. On les note $\alpha_1, \ldots, \alpha_n$, en adoptant une numérotation de ces racines de sorte que $\alpha_1 = \mathrm{i}\,\pi$. Pourquoi peut-on affirmer que $n > 1$?

3. On définit le polynôme $Q_0 \in \mathbb{Z}[X, X_1, \ldots, X_n] = \mathbb{Z}[X][X_1, \ldots, X_n]$ par

$$Q_0 = X \prod_{k=1}^{n} \left(\prod_{1 \leqslant i_1 < \cdots < i_k \leqslant n} (X - X_{i_1} - \cdots - X_{i_k}) \right) = \prod_{I \subset [\![1,n]\!]} \left(X - \sum_{i \in I} X_i \right).$$

   (a) Montrer qu'en tant que polynôme des indéterminées $X_1, \ldots, X_n$ à coefficients dans $\mathbb{Z}[X]$, Q_0 est symétrique en $X_1, \ldots, X_n$.

   (b) On définit le polynôme $Q_1 \in \mathbb{C}[X]$ par :

$$Q_1(X) = Q_0(X, \alpha_1, \ldots, \alpha_n).$$

   On note $\gamma_0, \cdots, \gamma_s$ les racines non nécessairement distinctes de Q_1, pouvant donc s'exprimer facilement en fonction des α_i. On adopte une numérotation de ces racines de sorte que $\gamma_0 = 0$.

   Justifier que $Q_1 \in \mathbb{Q}[X]$.

   Il existe donc un polynôme Q_2 **à coefficients entiers**, dont les γ_i sont les racines, obtenu en multipliant Q_1 par un certain entier. On se donne un tel polynôme Q_2 dans la suite du problème.

   (c) En considérant le produit $\displaystyle\prod_{i=1}^{n} (\mathrm{e}^{\alpha_i} + 1)$, justifier que l'on a :

$$\mathrm{e}^{\gamma_0} + \cdots + \mathrm{e}^{\gamma_s} = 0.$$

Quitte à regrouper les exponentielles égales à 1 et à réindexer les γ_i, on peut supposer qu'on a une relation

$$e^{\gamma_1} + \cdots + e^{\gamma_r} + m = 0,$$

où les γ_i sont cette fois tous non nuls nuls, et m est un entier strictement positif. Ainsi, 0 est racine de multiplicité m de Q_2. On définit $Q \in \mathbb{Z}[X]$ par $Q_2 = X^m Q$. Ainsi, les racines de Q sont exactement les γ_i, $i \in [\![1, r]\!]$.

4. Soit c le coefficient dominant de Q et p un nombre premier. L'entier r est comme ci-dessus. On définit :

$$f(X) = \frac{c^{rp-1}}{(p-1)!} X^{p-1} (Q(X))^p \qquad \text{et} \qquad F(X) = f(X) + f'(X) + \cdots + f^{(rp+p-1)}(X).$$

(a) Soit g la fonction définie sur $\mathbb{R}$ par :

$$g(x) = e^{-x} F(x).$$

Exprimer g' en fonction de f.

(b) En déduire que pour tout $x \in \mathbb{R}$,

$$F(x) - e^x F(0) = -x \int_0^1 e^{(1-\lambda)x} f(\lambda x) d\lambda,$$

puis que

$$\sum_{j=1}^{r} F(\gamma_j) + mF(0) = -\sum_{j=1}^{r} \gamma_j \int_0^1 e^{(1-\lambda)\gamma_j} f(\lambda \gamma_j) d\lambda.$$

(c) Montrer que pour tout $k \in [\![1, p-1]\!]$, $f^{(k)}(\gamma_j) = 0$.

(d) En utilisant la symétrie en les γ_j de l'expression $\sum_{j=1}^{r} F(\gamma_j)$, montrer que $\sum_{k=1}^{r} F(\gamma_j)$ est un entier divisible par p.

(e) En déduire que

$$\sum_{j=1}^{r} F(\gamma_j) + mF(0) \equiv mc^{rp-1} c_0^p \ [p],$$

où c_0 est le coefficient constant de Q.

(f) En déduire que pour tout p premier suffisamment grand, $\sum_{j=1}^{r} F(\gamma_j) + mF(0)$ est un entier non nul.

5. Montrer que π est transcendant.