DM d'Alix 0

Yvann Le Fay

Août 2019

1 Partie I. Les nombres de Liouville

Un nombre algébrique est un nombre complexe qui est racine d'un polynôme à coefficients dans $\mathbb{Q}$, un nombre transcendant est un nombre complexe qui n'est pas algébrique.

1.1 Partie A. Développement décimal illimité

On note dans cette partie α un nombre réel de l'intervalle [0,1]. On pose pour tout $n \in \mathbb{N}^*$, $a_n = E(10^n\alpha) - 10E(10^{n-1}\alpha)$.

1. Montrer que pour tout $n \in \mathbb{N}^*$, $a_n \in [\![0;9]\!]$.
2. Montrer que pour tout $n \in \mathbb{N}^*$, $\frac{E(10^n\alpha)}{10^n} = \sum_{k=1}^{n} \frac{a_k}{10^k} = 0{,}a_1a_2\ldots a_n$.
3. En déduire que la suite $u_n = \sum_{k=1}^{n} \frac{a_k}{10^k}$ converge vers un réel que l'on précisera.
   La suite $0{,}a_1a_2\ldots a_n\ldots$ est appelée développement décimal illimité (propre) du réel α.
4. Dans cette question, le nombre α est un rationnel de forme irréductible $\frac{p}{q}$.
   (a) On note r_k le reste de la division euclidienne de 10^kp par q. Montrer qu'il existe deux entiers $n < m$ tels que $r_n = r_m$.
   (b) Montrer que pour tout $i \in \mathbb{N}^*$,$a_{n+i} = E(10^i\frac{r_n}{q}) - 10E(10^{i-1}\frac{r_n}{q}) = a_{m+i}$. On pourra écrire que $10^n\alpha = q_nq + r_n$ pour un certain entier q_n. En déduire que la suite $(a_k)_{k\in\mathbb{N}}$ est périodique à partir d'un certain rang.
5. On note pour $n \geq 1$, $u_n = \sum_{k=1}^{n} \frac{1}{10^{k!}}$ et $v_n = \sum_{k=1}^{n!} \frac{1}{10^k}$.
   (a) Montrer que pour tout $n \geq 1$, $u_n \leq v_n$. Montrer que la suite v_n converge et enfin que la suite u_n converge vers un réel $\alpha \in [0{,}1]$.
   (b) Déterminer la suite (a_k) du développement décimal illimité de α. En déduire que α est un nombre irrationnel.

1.2 Partie B. Nombres de Liouville

1. Dans toute cette partie on note α un nombre algébrique irrationnel et $P(X) = \sum_{k=0}^{n} a_kX^k$, un polynôme de $\mathbb{Q}[X]$. On pose $I_\alpha = \{U \in \mathbb{Q}[X] : U(\alpha) = 0\}$.
   (a) Montrer que I_α est un sous-groupe du groupe $(\mathbb{Q}[X], +)$.
   (b) Justifier l'existence d'un polynôme μ_α appartenant à I_α et qui est unitaire et de degré minimal.
   (c) Montrer que si $U \in I_\alpha$ alors $\mu_\alpha \mid U$.
   (d) Montrer que $I_\alpha = \mu_\alpha\mathbb{Q}[X]$. Discuter de l'unicité du polynôme μ_α.
2. Montrer que le polynôme μ_α n'a aucune racine rationnelle et que les racines de μ_α sont simples.
3. On note d le degré de μ_α.
   (a) Montrer qu'li existe un polynôme $P \in \mathbb{Z}[X]$ de degré d tel que $P(\alpha) = 0$.
   (b) Pour tous $\frac{p}{q} \in \mathbb{Q}$, montrer qu'il existe un entier $N \in \mathbb{Z}^*$ tel que $P\left(\frac{p}{q}\right) = \frac{N}{q^d}$. En déduire que $\left|P\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^d}$.
4. On note $\frac{p}{q}$ un rationnel de l'intervalle $[\alpha - 1, \alpha + 1]$.
   (a) Montrer q'il existe $c_{p,q} \in [\alpha - 1{,}\alpha + 1]$ tel que $P\left(\frac{p}{q}\right) = \left(\frac{p}{q} - \alpha\right)P'(c_{p,q})$.
   (b) Justifier l'existence de $\max_{[\alpha-1,\alpha+1]} |P'| = C$ et montrer que $C > 0$.
   (c) On pose $C' = \min(1{,}1/C)$. Montrer que pour tout rationnel $\frac{p}{q} \in \mathbb{Q}$, $\left|\alpha - \frac{p}{q}\right| \geq \frac{C'}{q^d}$.

Un nombre de Liouville est un nombre irrationnel α pour tous entiers $d > 0$, toutes constantes $C' > 0$, il existe $\frac{p}{q} \in \mathbb{Q}$ tel que $\left|\alpha - \frac{p}{q}\right| < \frac{C}{q^d}$. En particulier, un nombre de Liouville n'est pas un nombre algébrique.

1.3 Partie C. Où l'on exhibe un nombre transcendant

On note α le réel obtenu à la question 1.1.5. On veut montrer que α est un nombre de Liouville. On suppose par l'absurde que α est un nombre algébrique. Il existe alors $C' > 0$ et $d \in \mathbb{N}^*$ tel que pour tous rationnels $\frac{p}{q}$, $\left|\alpha - \frac{p}{q}\right| \geq \frac{C'}{q^d}$.

1. Montrer pour tous entiers n, p strictements positifs que $0 \leq u_{n+p} - u_n \leq \frac{10}{9\times 10^{(n+1)!}}$. En déduire que $0 \leq \alpha - u_n \leq \frac{10}{9\times 10^{(n+1)!}}$.
2. Montrer que pour tous $n \in \mathbb{N}^*$, $\frac{C'}{10^{dn!}} \leq \frac{10}{9\times 10^{(n+1)!}}$.
3. Expliquer pourquoi l'inégalité précédente ne peut pas être vérifiée pour tout entier n non nul. Conclure

C'est le premier exemple de nombre transcendant connu. Mais cela laisse entier la question de la transcendance des nombres usuels comme π, e et il faudra attendre les résultats de Lindemann et de Hermitte pour avoir confirmation du caractère transcendant de ces nombres. La partie suivante étudie quelques propritétés des nombres algébriques.

2 Partie II. Les nombres algébriques

Pour α, β deux nombres algébriques, on note $\mathbb{Q}[\alpha] = \{P(\alpha) : P \in \mathbb{Q}[X]\}$ et $\mathbb{Q}[\alpha, \beta] = \{P(\alpha, \beta) : P \in \mathbb{Q}[X, Y]\}$. On pourra utiliser librement que $\mathbb{C}$ est un $\mathbb{Q}$-espace vectoriel.

2.1 Partie A. Structure de $\mathbb{Q}[\alpha]$

On notera μ_α le polynôme minimal de α et d son degré.

1. Montrer que $(\mathbb{Q}[\alpha], +, \times)$ est un anneau.
2. (a) Montrer que $(\mathbb{Q}[\alpha], +, \cdot)$ est un $\mathbb{Q}$-ev.
   (b) Montrer que pour tout $x \in \mathbb{Q}[\alpha]$, il existe $P \in \mathbb{Q}_{d-1}[X]$ tel que $x = P(\alpha)$.
   (c) En déduire que la famille $(1,\alpha, \ldots \alpha^{d-1})$ est une base de $\mathbb{Q}[\alpha]$.
3. On fixe x_0 un élément non nul de $\mathbb{Q}[\alpha]$ et f l'application
$$f : \begin{cases} \mathbb{Q}[\alpha] \to \mathbb{Q}[\alpha] \\ x \quad\;\; \mapsto xx_0 \end{cases}$$
   Montrer que f est une application linéaire injective. Montrer que $(\mathbb{Q}[\alpha], +, \cdot)$ est un corps.

2.2 Partie B. Le théorème de l'élément primitif

On note $\alpha_1, \ldots, \alpha_d$ et $\beta_1, \ldots, \beta_q$ les racines respectivement de μ_α et μ_β dans $\mathbb{C}$. On convient que $\alpha_1 = \alpha$ et $\beta_1 = \beta$.

1. Montrer qu'il existe $c \in \mathbb{Q}$ tel que $\alpha_i + c\beta_j \neq \alpha + c\beta$ pour tous $(i,j) \in [\![1; d]\!] \times [\![2; q]\!]$. Le nombre c peut-il être nul ? On fixe un tel c.
2. Montrer que pour tout $n \in \mathbb{N}$, $(\alpha + c\beta)^n \in \mathrm{Vect}((a^i\beta^j)_{i,j})$. En déduire que $z = \alpha + c\beta$ est un nombre algébrique. On note $P(X) = \mu_\alpha(z - cX)$ et $Q(X) = \mu_\beta(X)$.
3. Montrer que les coefficients de $P(X)$ sont dans $\mathbb{Q}[z]$.
4. (a) Montrer que le reste de la division euclidienne de P par Q est un polynôme à coefficients dans $\mathbb{Q}[z]$.
   (b) En déduire que $\Delta(X) = P \wedge Q$ est un polynôme à coefficients dans $\mathbb{Q}[z]$.
   (c) Montrer que $\Delta(X) = X - \beta$.
   (d) Montrer que $\beta \in \mathbb{Q}[z]$ puis que $\alpha \in \mathbb{Q}[z]$.
5. Montrer que $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[z]$.
6. Montrer que l'ensemble des nombres algébriques est un sous-corps de $\mathbb{C}$.

2.3 Partie C. Méthode de Tchirnhauss de rechercue du polynôme minimal

Si $Q \in \mathbb{Q}[X]$ alors pour tout $s \in \mathbb{C}$, on note $Q_s(X) = Q(s - X)$.

1. On pose $P = X^2 + X + 1$ et $Q = X^2 - 2$. Donner une CNS sur le nombre s pour que P et Q_s aient une racine commune. On admet que la condition s'écrit $\Delta(s) = 0$ où Δ est un polynôme.
2. Déterminer les racines de $\Delta(s)$.
3. (a) trouver un polynôme à coefficients dans Q dont $j + \sqrt{2}$ est racine, en déduire le polynôme minimal de $j + \sqrt{2}$.
   (b) Même question pour $\sqrt{2} + \sqrt{3}$.

3 III. Les polynômes cyclotomiques

On dit que z est une racine primitive n-ième de l'unité si $\langle z \rangle = \mathbb{U}_n$. On note Z_n l'ensemble des racines primitives n-ièmes de l'unité. On appelle n-ième polynôme cyclotomique le polynôme,

$$\phi_n(X) = \prod_{z \in Z_n} (X - z)$$

1. Soit $k \in [\![0; n-1]\!]$. Montrer que $e^{\frac{2ik\pi}{n}} \in Z_n$ si et seulemnet si $k \wedge n = 1$. On note $\varphi(n) = |Z_n|$.
2. Soient m et n deux entiers premiers entre eux. Vérifier que l'application $\Psi : (u, v) \in Z_n \times Z_m \mapsto uv \in Z_{nm}$ est une bijection. En déduire que $\varphi(nm) = \varphi(n)\varphi(m)$.
3. Montrer que $\sum_{d|n} \varphi(d) = n$. En déduire le degré de $\prod_{d|n} \phi_d(X)$.
4. Soit $n \in \mathbb{N}^*$,
   (a) Montrer que les racines complexes du polynôme $X^n - 1$ sont simples.
   (b) Montrer que $X^n - 1 \mid \prod_{d|n} \phi_d(X)$ puis que $X^n - 1 = \prod_{d|n} \phi_d(X)$.
   (c) Justifier que $\phi_n(X) \in \mathbb{Z}[X]$ pour tout $n \in \mathbb{N}^*$.
5. Soient $p \in \mathbb{P}$ et $m \in \mathbb{N}$ tel que $p \nmid m$.
   (a) Soit $a \in \mathbb{N}$ tel que $\phi_m(a) = 0 \bmod p$. Montrer que $p \nmid a$ et que m est le plus petit entier naturel non nul tel que $a^m = 1 \bmod p$.
   (b) En déduire que l'ensemble des nombres premiers p tels que $p = 1$ dans $\mathbb{Z}/m\mathbb{Z}$ est infini.