MPSI 1

Mathématiques
DS 05

Samedi 10 janvier – 8h-12h

- Durée : 4 heures.
  - Prenez **10 minutes** pour lire le sujet en entier et décider de la stratégie que vous adopterez.
  - Prenez **10 minutes** au moins à la fin des 4 heures pour vous relire !
- Toute calculatrice ou appareil électronique est interdit.
- Le sujet est composé de deux problèmes indépendants.
- **Consignes de présentations.**
  - Les pages doivent être **numérotées.**
  - Les résultats doivent être **mis en valeur** (encadrés ou soulignés).
  - Les questions doivent être **numérotées**. Une question non numérotée, c'est une question potentiellement non corrigée.
  - Les questions doivent être **faites dans l'ordre** : si vous admettez une question, laissez de la place à l'endroit où elle est censée être pour y revenir ensuite. Changez de copie ou de page quand vous changez de grande partie.
- À tout moment, vous pouvez admettre le résultat d'une question pour pouvoir continuer : il suffit de le préciser clairement sur la copie.
- Si vous voyez ce qui semble être une erreur d'énoncé, indiquez-le sur la copie.
- Laissez de la place dans une marge à gauche pour pouvoir noter plus facilement le devoir.
- Une réponse fausse, si elle ne laisse pas paraître de calculs intermédiaires, compte 0 points ; avec calculs intermédiaires elle peut rapporter quelques points.

♫ Bon courage ! ♫

Problème 1. Nombre de rotation d'un homéomorphisme du cercle

A. Étude d'un ensemble de fonctions

On note $\mathcal{X}$ l'ensemble des applications $f : \mathbb{R} \to \mathbb{R}$ continues, strictement croissantes, vérifiant, pour tout x dans $\mathbb{R}$, $f(x+1) = f(x) + 1$.

1. Démontrer que pour f et g dans $\mathcal{X}$, $f \circ g$ est dans $\mathcal{X}$, et que pour tout n dans $\mathbb{N}$, $f^n = \underbrace{f \circ \cdots \circ f}_{n \text{ fois}}$ est dans $\mathcal{X}$.

2. Pour f dans $\mathcal{X}$, déterminer la limite de $(f(n))_{n\in\mathbb{N}}$ et de $(f(-n))_{n\in\mathbb{N}}$.

3. Soit f dans $\mathcal{X}$. Montrer que f est bijective et que f^{-1} est aussi dans $\mathcal{X}$.

4. Au vu des questions précédentes, que peut-on dire de l'ensemble $\mathcal{X}$?

Pour f dans $\mathcal{X}$, on définit

$$\varphi_f : \left|\begin{array}{l} \mathbb{R} \to \mathbb{U} \\ x \mapsto \mathrm{e}^{2i\pi f(x)} \end{array}\right. .$$

5. Démontrer que, pour $f \in \mathcal{X}$, φ_f est une fonction continue et 1-périodique.

6. Démontrer que si f et g sont dans $\mathcal{X}$, $\varphi_f = \varphi_g$ si, et seulement s'il existe $n \in \mathbb{Z}$ tel que pour tout x dans $\mathbb{R}$, $g(x) = f(x) + n$.

7. Démontrer que si $f \in \mathcal{X}$, alors pour tout $(\alpha, \beta) \in \mathbb{R}^2$ vérifiant $\mathrm{e}^{2i\pi\alpha} = \mathrm{e}^{2i\pi\beta}$, on a $\varphi_f(\alpha) = \varphi_f(\beta)$.

La question précédente permet de définir l'application $R_f : \mathbb{U} \to \mathbb{U}$, qui, à tout élément $z = \mathrm{e}^{2i\pi\theta}$ de $\mathbb{U}$ associe $\mathrm{e}^{2i\pi f(\theta)}$. Cette quantité est indépendante du choix de θ (par la question précédente), donc R_f est bien définie. On admet que R_f est bijective et que pour tout k dans $\mathbb{Z}$, $R_f^k = R_{f^k}$.

8. Si $\alpha \in \mathbb{R}$, on note $\tau_\alpha : \left|\begin{array}{l} \mathbb{R} \to \mathbb{R} \\ x \mapsto x + \alpha \end{array}\right.$. Vérifier rapidement que $\tau_\alpha \in \mathcal{X}$, donner l'expression de φ_{τ_α} et de R_{τ_α}.

B. Existence du nombre de rotation

Dans cette partie, on fixe une fonction f dans $\mathcal{X}$. On note, pour x dans $\mathbb{R}$, $\varphi(x) = f(x) - x$.

9. Démontrer que φ est périodique, de période 1.

10. Montrer que, pour tous $x, y \in \mathbb{R}$, $-1 < \varphi(y) - \varphi(x) < 1$. On pourra d'abord traiter le cas où $x \leqslant y < x + 1$.

11. Soit $n \in \mathbb{N}^*$. Démontrer que la fonction $\varphi_n : x \mapsto f^n(x) - x$ est périodique de période 1 et justifier l'existence de $M_n = \sup\limits_{x\in\mathbb{R}} f^n(x) - x$ et de $m_n = \inf\limits_{x\in\mathbb{R}} f^n(x) - x$.

12. Montrer que, pour tout $n \in \mathbb{N}^*, 0 \leqslant M_n - m_n < 1$.

13. Montrer que pour tous $n, p \in \mathbb{N}^*$, $m_n + m_p \leqslant m_{n+p} \leqslant M_{n+p} \leqslant M_n + M_p$.

14. En déduire que pour tous $k, n \in \mathbb{N}^*$, $\dfrac{m_k}{k} \leqslant \dfrac{M_n}{n}$.
On pourra comparer m_k et m_{kn}.

15. Déduire des questions 12. et 14. que $\sup\left\{\dfrac{m_n}{n}, n \in \mathbb{N}^*\right\} = \inf\left\{\dfrac{M_n}{n}, n \in \mathbb{N}^*\right\}$ (on justifiera brièvement l'existence de chacune des quantités).

On note $\rho(f)$ cette valeur commune et on l'appelle nombre de rotation de f.

16. Montrer que, pour tout $n \in \mathbb{N}^*$, il existe $x_n \in \mathbb{R}$ tel que $f^n(x_n) = x_n + n\rho(f)$.

17. En déduire que, pour tout $x \in \mathbb{R}$ et pour tout $n \in \mathbb{N}^*$, $-1 < f^n(x) - x - n\rho(f) < 1$. En déduire que $\dfrac{f^n(x)}{n} \to \rho(f)$, quand $n \to +\infty$.

18. Expliquer, à l'aide de la fonction R_f, l'appellation « nombre de rotation » .

C. Quelques propriétés de ρ

Soit $f \in \mathcal{X}$.

C-I. Généralités

19. Soit g dans $\mathcal{X}$ telle que $g \circ f = f \circ g$. Montrer que $\rho(g \circ f) = \rho(g) + \rho(f)$ et que pour tout $k \in \mathbb{Z}$, $\rho\left(f^k\right) = k\rho(f)$.

20. Montrer que $\rho(f)$ est nul si, et seulement si f a un point fixe.

C-II. Cas rationnel

On dit que R_f a une orbite périodique s'il existe $z \in \mathbb{U}$ et $k \in \mathbb{N}^*$ tel que $R_f^k(z) = z$, i.e. $R_{f^k}(z) = z$.

21. Démontrer que si $\rho(f) \in \mathbb{Q}$, alors R_f a une orbite périodique.

22. Établir la réciproque.

Épilogue. Si le DS ne portait que sur la continuité, j'aurais aussi poussé le devoir jusqu'à vous faire démontrer que si $\rho(f)$ est irrationnel, alors f a une « orbite dense » et qu'il existe une bijection continue h telle que $h \circ f = \tau_{\rho(f)} \circ h$.

Problème 2. Touchons du doigt la théorie de Galois

Le but de ce problème est de faire manipuler certaines notions qui sont à la base de ce qu'on appelle aujourd'hui la théorie de Galois.

A. Automorphismes de corps

Soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$. $(\mathbb{K}, +, \times)$ est donc un corps. On note $\mathrm{Bij}(\mathbb{K}, \mathbb{K})$ l'ensemble des bijections de $\mathbb{K}$ dans $\mathbb{K}$. On rappelle que $(\mathrm{Bij}(\mathbb{K}, \mathbb{K}), \circ)$ est un groupe.
On note $\mathrm{Aut}(\mathbb{K})$ l'ensemble des automorphismes de corps de $\mathbb{K}$, c'est-à-dire des morphismes de corps de $\mathbb{K}$ dans $\mathbb{K}$ qui sont bijectifs.
Si $\mathbb{L}$ est un sous-corps de $\mathbb{K}$, on note $\mathrm{Aut}_{\mathbb{L}}(\mathbb{K})$ l'ensemble des automorphismes de $\mathbb{K}$ qui laissent $\mathbb{L}$ invariant :

$$\mathrm{Aut}_{\mathbb{L}}(\mathbb{K}) = \{\varphi \in \mathrm{Aut}(\mathbb{K}),\ \forall x \in \mathbb{L},\ \varphi(x) = x\}.$$

1. On définit ζ l'application de conjugaison : $\forall z \in \mathbb{C},\ \zeta(z) = \overline{z}$. Vérifier que $\zeta \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$.

2. Démontrer que $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{Id}_{\mathbb{C}}, \zeta\}$.

3. Démontrer que $\mathrm{Aut}_{\mathbb{L}}(\mathbb{K})$ est un sous-groupe de $(\mathrm{Bij}(\mathbb{K}, \mathbb{K}), \circ)$.

Dans cette partie, on considère $\omega \in \mathbb{K} \setminus \mathbb{L}$ tel que $\omega^2 \in \mathbb{L}$. On note $\mathbb{L}[\omega] = \{a + \omega b,\ (a, b) \in \mathbb{L}^2\}$.

4. Démontrer que pour tout z dans $\mathbb{L}[\omega]$, il existe un unique couple $(a, b) \in \mathbb{L}^2$ tel que $z = a + \omega b$.

5. Démontrer que $\mathbb{L}[\omega]$ est un sous-corps de $\mathbb{K}$ contenant $\mathbb{L}$.

6. Démontrer brièvement que $\mathrm{Aut}_{\mathbb{L}}(\mathbb{L}[\omega])$ contient deux éléments.

7. **Application.** Démontrer que $\mathbb{Q}[i]$ est un sous-corps de $\mathbb{C}$, puis que $(\mathbb{Q}[i])[\sqrt{2}]$ est lui aussi un sous-corps de $\mathbb{C}$. On notera ce corps $\mathbb{Q}[i, \sqrt{2}]$.

B. Extensions cyclotomiques

Dans cette partie, on note $\mathbb{U}_n$ le groupe des racines de l'unité. On note $\omega_n = e^{\frac{2i\pi}{n}}$, ce qui assure que $\mathbb{U}_n = \{\omega_n^k,\ k \in [\![0, n-1]\!]\}$. On note

$$\mathbb{Q}[\mathbb{U}_n] = \left\{ \sum_{k=0}^{n} \alpha_k \omega_n^k,\ (\alpha_0, \dots, \alpha_{n-1}) \in \mathbb{Q}^n \right\}.$$

On admet que $\mathbb{Q}[\mathbb{U}_n]$ est un sous-corps de $(\mathbb{C}, +, \times)$ (ce n'est pas du tout évident !). Le but de cette partie est de comprendre la structure de $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\mathbb{U}_n])$ pour certaines valeurs de n.

B-I. Le cas de $\mathbb{U}_5$

Afin d'alléger les notations, on note $\xi = \omega_5 = e^{\frac{2i\pi}{5}}$. On donne $\cos \dfrac{2\pi}{5} = \dfrac{\sqrt{5} - 1}{4}$.

8. Dessiner approximativement les ξ^k pour k allant de 0 à 4. Montrer sur le dessin quels sont les éléments, parmi les ξ^k, qui sont conjugués.

On rappelle que

$$\mathbb{Q}[\mathbb{U}_5] = \left\{ \sum_{k=0}^{4} a_k \xi^k,\ (a_0, a_1, a_2, a_3, a_4) \in \mathbb{Q}^5 \right\},$$

et que l'on a admis qu'il s'agissait d'un sous-corps de $\mathbb{C}$.

9. Que vaut $\sum_{k=0}^{4} \xi^k$? En déduire que

$$\mathbb{Q}[\mathbb{U}_5] = \left\{ \sum_{k=1}^{4} b_k \xi^k,\ (b_1, b_2, b_3, b_4) \in \mathbb{Q}^4 \right\}. \tag{1}$$

10. Démontrer que pour tous rationnels a, a', b, b', si $a \sin \frac{2\pi}{5} + b \sin \frac{4\pi}{5} = a' \sin \frac{2\pi}{5} + b' \sin \frac{4\pi}{5}$, alors $a = a'$ et $b = b'$.

On admet que pour tous rationnels a, a', b, b', si $a \cos \frac{2\pi}{5} + b \cos \frac{4\pi}{5} = a' \cos \frac{2\pi}{5} + b' \cos \frac{4\pi}{5}$, alors $a = a'$ et $b = b'$.

11. Démontrer qu'une écriture sous la forme (1) est unique, c'est-à-dire que si $(b_1, \ldots, b_4, c_1, \ldots, c_4)$ sont huit rationnels tels que

$$\sum_{k=1}^{4} b_k \xi^k = \sum_{k=1}^{4} c_k \xi^k,$$

alors pour tout k dans $[\![1, 4]\!]$, $b_k = c_k$.

On définit σ sur $[\![1, 4]\!]$ par : pour tout k dans $[\![1, 4]\!]$, $\sigma(k)$ est le reste de la division euclidienne de $2k$ par 5.

12. Vérifier que $\sigma \in \mathcal{S}_4$, représenter cette permutation sous la forme $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix}$.

Préciser sa décomposition en cycles à supports disjoints et sa signature. Calculer σ^2, σ^3 et σ^4.

On définit alors φ sur $\mathbb{Q}[\mathbb{U}_5]$ par : $\forall (b_1, b_2, b_3, b_4) \in \mathbb{Q}^4$,

$$\varphi(b_1\xi + b_2\xi^2 + b_3\xi^3 + b_4\xi^4) = b_1\xi^{\sigma(1)} + b_2\xi^{\sigma(2)} + b_3\xi^{\sigma(3)} + b_4\xi^{\sigma(4)}.$$

13. Quelle est l'utilité de la question 11. ?

14. Démontrer que pour tout k $\boxed{\text{dans } \mathbb{N}}$, pour tout λ dans $\mathbb{Q}$, $\varphi(\lambda\xi^k) = \lambda\xi^{2k}$.

15. Démontrer que φ est dans $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{U}_5)$.

Réciproquement, soit ψ dans $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{U}_5)$.

16. En distinguant selon les valeurs de $\psi(\xi)$, démontrer qu'il existe k dans $[\![0, 3]\!]$ tel que $\psi = \varphi^k$.

17. Conclure que $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\mathbb{U}_5])$ est un groupe à 4 éléments, isomorphe à $\mathbb{U}_4$.

B-II. Le cas de $\mathbb{U}_8$

On admet toujours que $\mathbb{Q}[\mathbb{U}_8]$ est un sous-corps de $\mathbb{C}$.

18. Que vaut ω_8 ? Donner notamment sa forme algébrique.

19. Démontrer que $\sqrt{2}$ et i sont dans $\mathbb{Q}[\mathbb{U}_8]$, puis que $\mathbb{Q}[i, \sqrt{2}] \subset \mathbb{Q}[\mathbb{U}_8]$.

20. Conclure que $\mathbb{Q}[\mathbb{U}_8] = \mathbb{Q}[i, \sqrt{2}]$.

21. Démontrer enfin que $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\mathbb{U}_8]) = \{\mathrm{Id}, \alpha, \beta, \gamma\}$ où $\alpha^2 = \beta^2 = \gamma^2 = \mathrm{Id}$. Ce groupe est-il isomorphe à $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{U}_5)$?