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 $\mathcal{X}$.

Correction

Soient f et g dans $\mathcal{X}$. Alors $f \circ g$ est continue, strictement croissante, et, pour tout x dans $\mathbb{R}$,

$$f \circ g(x+1) = f(g(x+1)) = f(g(x)+1) = f(g(x)) + 1,$$

donc $f \circ g \in \mathcal{X}$.
Pour f^n, on conclut par récurrence immédiate.

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

Correction

On montre par récurrence que pour tout n dans $\mathbb{N}$, $\mathcal{P}_n$: $\boxed{f(n) = f(0) + n}$. L'initialisation est évidente et, pour l'hérédité, si $n \in \mathbb{N}$ est tel que $\mathcal{P}_n$ est vraie, on a $f(n+1) = f(n) + 1 = f(0) + n + 1$. D'où l'hérédité et le résultat.
Ainsi, $\boxed{f(n) = f(0) + n \underset{n\to+\infty}{\longrightarrow} +\infty}$.
De même, on montre facilement que pour tout n dans $\mathbb{N}$, $f(-n) = f(0) - n \underset{n\to+\infty}{\longrightarrow} -\infty$.

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

Correction

La fonction f est strictement croissante, non majorée (par la question précédente), non minorée (par la question précédente), donc, d'après le théorème de la limite monotone, $\boxed{f(x) \underset{x\to+\infty}{\longrightarrow} +\infty \text{ et } f(x) \underset{x\to-\infty}{\longrightarrow} -\infty.}$
De plus, étant continue, on en déduit, par le théorème de la bijection, que f est $\boxed{\text{bijective de } \mathbb{R} \text{ dans } \mathbb{R}.}$
Enfin, par le théorème de la bijection f^{-1} est aussi $\boxed{\text{continue et strictement croissante.}}$
De plus, pour tout x dans $\mathbb{R}$, $f(x+1) = f(x) + 1$ donc, si $y \in \mathbb{R}$,

$$f(f^{-1}(y) + 1) = f(f^{-1}(y)) + 1 = y + 1,$$

d'où, par bijectivité de f,

$$\boxed{f^{-1}(y) + 1 = f^{-1}(y+1),}$$

ce qui assure que f^{-1} est dans $\mathcal{X}$.

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

Correction

On vient de démontrer que $\mathcal{X}$ était un sous-groupe de l'ensemble des bijections continues de $\mathbb{R}$ dans $\mathbb{R}$ (en ajoutant à ce que l'on a déjà démontré que $\boxed{\mathrm{Id}_{\mathbb{R}} \text{ est bien dans } \mathcal{X}}$)

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.

Correction

Soit $f \in \mathcal{X}$. Alors φ_f est continue par composition de fonctions continues. De plus, pour x dans $\mathbb{R}$,

$$\varphi_f(x+1) = \mathrm{e}^{2i\pi f(x+1)} = \mathrm{e}^{2i\pi(f(x)+1)} = \mathrm{e}^{2i\pi f(x)+2i\pi} \boxed{= \varphi_f(x),}$$

d'où la 1-périodicité de φ_f.

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 $\mathbb{R}$, $g(x) = f(x) + n$.

Correction

Comme $\varphi_f = \varphi_g$, on en déduit que pour tout x dans $\mathbb{R}$, $\mathrm{e}^{2i\pi f(x)} = \mathrm{e}^{2i\pi g(x)}$, donc que l'on dispose de $n(x)$ dans $\mathbb{Z}$ tel que $2i\pi f(x) = 2i\pi g(x) + 2i\pi n(x)$, c'est-à-dire que

$$\boxed{f(x) = g(x) + n(x).}$$

(**attention !** Le n dépend, a priori, de x ! ! !) Ceci signifie que $h = f - g$ est une fonction $\boxed{\text{continue, à valeurs dans } \mathbb{Z}.}$ On montre alors qu'elle est constante. Si ce n'était pas le cas, on disposerait de deux entiers $a < b$, de deux réels x_a et x_b tels que $h(x_a) = a$ et $h(x_b) = b$. Mais alors, $a + \dfrac{1}{2} \in [a, b]$ donc, par le théorème des valeurs intermédiaires, on disposerait de c dans $[x_a, x_b]$ tel que $h(c) = a + \dfrac{1}{2} \notin \mathbb{Z}$, absurde.

Donc h est constante. On note n sa valeur : on a alors $\boxed{\forall x \in \mathbb{R},\ f(x) = g(x) + n.}$

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}.

Correction

τ_α est clairement bijective de $\mathbb{R}$ dans $\mathbb{R}$, strictement croissante, et on a bien, pour tout x, $\tau_\alpha(x+1) = \tau_\alpha(x) + 1$.

Ensuite,

$$\varphi_{\tau_\alpha} : \left| \begin{array}{l} \mathbb{R} \to \mathbb{U} \\ x \mapsto \mathrm{e}^{2i\pi(x+\alpha)} = \mathrm{e}^{2i\pi\alpha}\mathrm{e}^{2i\pi x} \end{array} \right. ,$$

donc

$$R_{\tau_\alpha} : \left| \begin{array}{l} \mathbb{U} \to \mathbb{U} \\ z \mapsto \mathrm{e}^{2i\pi\alpha} z \end{array} \right. .$$

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.

Correction

Soit x dans $\mathbb{R}$. Alors $\varphi(x+1) = f(x+1) - x - 1 = f(x) + 1 - x - 1 = f(x) - x = \varphi(x)$, donc φ est 1-périodique.

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

Correction

Soient x et y dans $\mathbb{R}$. Alors

$$\varphi(y) - \varphi(x) = f(y) - f(x) - y + x.$$

Dans le cas où $x \leqslant y < x + 1$, on sait déjà que f est strictement croissante donc $f(y) - f(x) \geqslant 0$ et $x - y > -1$, donc $\boxed{\varphi(y) - \varphi(x) - y + x > -1}$.
Ensuite, $-y + x \leqslant 0$ et, comme $y < x + 1$, $f(y) - f(x) < f(x+1) - f(x) = 1$. Ainsi,

$$\boxed{\varphi(y) - \varphi(x) - y + x < 1 + 0 = 1.}$$

Dans le cas où y est quelconque, on dispose de k dans $\mathbb{Z}$ tel que $y + k \in [x, x+1[$. Mais $\varphi(y) = \varphi(y + k)$, $\boxed{\text{on peut donc conclure.}}$

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 $M_n = \sup_{x \in \mathbb{R}} f^n(x) - x$ et de $m_n = \inf_{x \in \mathbb{R}} f^n(x) - x$.

Correction

Comme, par la question 1., $f^n \in \mathcal{X}$, on en déduit, par la question précédente, que $\varphi_n : x \mapsto f^n(x) - x$ est 1-périodique. Étant continue sur le **segment** $[0, 1]$, on en déduit, par le théorème des bornes atteintes, que φ_n est bornée sur $[0, 1]$ et y atteint ses bornes. De plus, par 1-périodicité, $\varphi_n(\mathbb{R}) = \varphi_n([0, 1])$, donc φ_n est bornée sur $\mathbb{R}$ et atteint ses bornes, ce qui assure l'existence de m_n et M_n.

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

Correction

Comme, pour tout n dans $\mathbb{N}^*$, $f^n \in \mathcal{X}$, on peut appliquer la question 10. à φ_n et obtenir que pour tous y et x, $\varphi(y) - \varphi(x) \in]-1, 1[$. Mais alors, si x et y sont tels que $m_n = \varphi_n(x)$ et $M_n = \varphi_n(y)$, on a $\boxed{0 \leqslant M_n - m_n = \varphi_n(y) - \varphi_n(x) < 1}$.

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

Correction

Soit $(n, p) \in (\mathbb{N}^*)^2$. Soit x_0 tel que $m_{n+p} = f^{n+p}(x_0) - x_0$ (l'existence de ce x_0 est assurée par le théorème des bornes atteintes). Alors

$$\begin{aligned} m_{n+p} &= f^{n+p}(x_0) - x_0 \\ &\boxed{= f^n(f^p(x_0)) - f^p(x_0) + f^p(x_0) - x_0} \\ &= \varphi_n(f^p(x_0)) - \varphi_p(x_0) \\ &\boxed{\geqslant m_n + m_p.} \end{aligned}$$

Ensuite, l'inégalité $M_{n+p} \leqslant M_n + M_p$ se démontre symétriquement.
Enfin, l'inégalité $m_{n+p} \leqslant M_{n+p}$ vient simplement du fait que le minimum est inférieur au maximum.

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}.

Correction

Soit $(k, n) \in (\mathbb{N}^*)^2$. Alors on remarque que $2m_n \leqslant m_{2n}$, et, par récurrence immédiate, $nm_k \leqslant m_{nk}$. De même, $M_{nk} \leqslant kM_n$, d'où $nm_k \leqslant kM_n$, c'est-à-dire que $\boxed{\dfrac{m_k}{k} \leqslant \dfrac{M_n}{n}.}$

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).

Correction

Déjà, pour tout n dans $\mathbb{N}^*$, $\dfrac{m_n}{n} \leqslant \dfrac{M_1}{1}$, donc $A = \left\{\dfrac{m_n}{n}, n \in \mathbb{N}^*\right\}$ est une partie de $\mathbb{R}$, non vide, majorée : $\boxed{\text{elle admet une borne supérieure}}$. De même, $\inf(B)$, où $B = \left\{\dfrac{M_n}{n}, n \in \mathbb{N}^*\right\}$, existe.
Ensuite, on note $\alpha = \sup(A)$ et $\beta = \inf(B)$. On sait que pour tous k et n,

$$\frac{m_k}{k} \leqslant \frac{M_n}{n}.$$

À k fixé, $\dfrac{m_k}{k}$ est un minorant de B, donc $\dfrac{m_k}{k} \leqslant \beta$. Donc β majore A, donc $\boxed{\alpha \leqslant \beta.}$
Ensuite, par la question 12., on sait que pour tout n dans $\mathbb{N}^*$,

$$\frac{m_n}{n} > \frac{M_n}{n} - \frac{1}{n}.$$

Mais $\frac{m_n}{n} \leqslant \alpha$ et $\frac{M_n}{n} \geqslant \beta$ donc, pour tout n dans $\mathbb{N}^*$, $\boxed{\alpha > \beta - \frac{1}{n}.}$ D'où, en passant à la limite dans les inégalités larges, $\boxed{\alpha \geqslant \beta.}$

$\boxed{\text{On conclut donc que } \alpha = \beta.}$

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 $f^n(x_n) = x_n + n\rho(f)$.

Correction

Soit $g : x \mapsto f^n(x) - x - n\rho(f)$. Alors g est continue sur $\mathbb{R}$.

Son minimum est $\boxed{m_n - n\rho(f) = n\left(\frac{m_n}{n} - \rho(f)\right) \leqslant 0}$, car $\rho(f) = \sup(A)$. De même, son maximum est $M_n - n\rho(f) = n\left(\frac{M_n}{n} - \rho(f)\right)$ $\boxed{\geqslant 0}$ car $\rho(f) = \inf(B)$.

Ainsi, par le théorème des valeurs intermédiaires, g s'annule : on dispose de x_n tel que $g(x_n) = 0$, i.e. $\boxed{f^n(x_n) = x_n + n\rho(f).}$

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 $\frac{f^n(x)}{n} \to \rho(f)$, quand $n \to +\infty$.

Correction

Par la question 10 appliquée à φ_n, on sait que pour tous x et y,

$$-1 < \varphi_n(x) - \varphi_n(y) < 1.$$

En prenant $y = x_n$, on obtient exactement

$$\boxed{-1 < f^n(x) - x - n\rho(f) < 1,}$$

ce qui est l'inégalité désirée.

En divisant par n et par théorème d'encadrement, on en déduit que $\frac{f^n(x) - x}{n} \underset{n\to+\infty}{\longrightarrow} \rho(f)$, ou encore que $\boxed{\frac{f^n(x)}{n} \underset{n\to+\infty}{\longrightarrow} \rho(f)}$.

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

Correction

L'application R_f fait « tourner » un élément de $\mathbb{U}$. Dans le cas où $f = \tau_\alpha$, c'est clairement cela, R_f est la rotation d'angle α. Le nombre de rotation correspond à, en moyenne, de combien R_f fait tourner un élément de $\mathbb{U}$ (par « en moyenne », on entend la moyenne sur les itérés de R_f).

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 $k \in \mathbb{Z}$, $\rho\left(f^k\right) = k\rho(f)$.

Correction

On sait, comme $f \circ g = g \circ f$, que pour tout n dans $\mathbb{N}$, $(f \circ g)^n = f^n \circ g^n$.
Par la question 17. appliquée en $g^n(x)$, on sait que

$$-1 < f^n(g^n(x)) - g^n(x) - n\rho(f) < 1,$$

d'où, en divisant par n,

$$-\frac{1}{n} < \frac{(f \circ g)^n(x)}{n} - \frac{g^n(x)}{n} - \rho(f) < \frac{1}{n},$$

d'où, par passage à la limite dans les inégalités larges,

$$\rho(f \circ g) - \rho(g) - \rho(f) = 0,$$

d'où $\boxed{\rho(f \circ g) = \rho(f) + \rho(g)}$.
La deuxième relation se déduit par récurrence immédiate.

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

Correction

Déjà, si $\rho(f)$ est nul, on sait qu'il existe x_1 tel que $f(x_1) - x_1 - 1 \times \rho(f) = 0$, i.e. $\boxed{f(x_1) = x_1}$. Donc f admet un point fixe.
Ensuite, si f admet un point fixe x_0, alors pour tout n dans $\mathbb{N}$, $f^n(x_0) = x_0$ et donc $\boxed{\frac{f^n(x_0)}{n} = \frac{x_0}{n} \underset{n\to+\infty}{\longrightarrow} 0}$, donc $\boxed{\rho(f) = 0}$.

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.

Correction

Écrivons $\rho(f) = \frac{p}{q}$, où $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$. Alors on sait que l'on dispose de $x_q \in \mathbb{R}$ tel que $f^q(x_q) - x_q - q\rho(f) = 0$, c'est-à-dire que $\boxed{f^q(x_q) - x_q = p}$. Mais alors, si $z = \mathrm{e}^{2i\pi x_q}$, on a

$$\boxed{R_f^q(z) = \mathrm{e}^{2i\pi f(x_q)} = \mathrm{e}^{2i\pi(x_q+p)} = \mathrm{e}^{2i\pi x_q} = z,}$$

donc R_f admet une orbite périodique.

22. Établir la réciproque.

Correction

Supposons que R_f admette une orbite périodique. Alors on dispose de zz dans $\mathbb{U}$ et de k dans $\mathbb{N}^*$ tel que $R_{f^k}(z) = z$, i.e., si $z = \mathrm{e}^{2i\pi\alpha}$,

$$\mathrm{e}^{2i\pi f^k(\alpha)} = \mathrm{e}^{2i\pi\alpha},$$

donc on dispose de ℓ dans $\mathbb{Z}$ tel que $f^k(\alpha) = \alpha + \ell$. On en déduit que, pour tout n dans $\mathbb{N}$,

$$f^{nk}(\alpha) = \alpha + n\ell,$$

d'où

$$\boxed{\frac{f^{nk}(\alpha)}{nk} = \frac{\alpha}{n} + \frac{\ell}{k},}$$

et comme $\left(\frac{f^{nk}(\alpha)}{nk}\right)_{n\in\mathbb{N}^*}$ est une suite extraite de $\left(\frac{f^n(\alpha)}{n}\right)_{n\in\mathbb{N}^*}$, on en déduit, en faisant tendre n vers $+\infty$, que

$$\boxed{\rho(f) = \frac{\ell}{k} \in \mathbb{Q}.}$$

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 $\zeta \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$.

Correction

Déjà, on vérifie que ζ est un morphisme de corps : soient z et z' dans $\mathbb{C}$. Alors

$$\overline{1} = 1,\ \overline{z + z'} = \overline{z} + \overline{z'} \text{ et } \overline{z \times z'} = \overline{z} \times \overline{z'}.$$

De plus, la conjugaison est une involution, donc est bijective.
Enfin, si $x \in \mathbb{R}$, $\overline{x} = x$, donc $\mathbb{R}$ est invariant par la conjugaison.
On en déduit donc que $\zeta \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$.

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

Correction

Soit $\varphi \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$. Alors si $z \in \mathbb{C}$, on dispose de a et b dans $\mathbb{R}$ tels que $z = a + ib$. Donc

$$\varphi(z) = \varphi(a) + \varphi(i)\varphi(b) = a + \varphi(i)b.$$

Or, $i^2 = -1$, donc $\varphi(i)^2 = -1$, donc $\varphi(i) = \pm i$.

- si $\varphi(i) = i$, alors $\varphi(z) = a + ib$, donc $\varphi = \mathrm{Id}_{\mathbb{C}}$
- si $\varphi(i) = -i$, alors $\varphi(z) = a - ib$, donc $\varphi = \zeta$.

Ainsi, $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) \subset \{\mathrm{Id}_{\mathbb{C}}, \zeta\}$. Comme l'inclusion réciproque est évidente, le résultat est démontré !

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

Correction

Déjà, $\mathrm{Id}_{\mathbb{K}}$ est bien un automorphisme de corps de $\mathbb{K}$ qui préserve $\mathbb{L}$.
Ensuite, soient φ et ψ deux éléments de $\mathrm{Aut}_{\mathbb{L}}(\mathbb{K})$. Alors

- $\varphi \circ \psi$ est bien un morphisme de corps (on peut le vérifier mais on l'a déjà fait pour les morphismes de groupes)
- si $x \in \mathbb{L}$, $\varphi \circ \psi(x) = \varphi(\psi(x)) = \varphi(x) = x$

Ainsi, $\varphi \circ \psi \in \mathrm{Aut}_{\mathbb{L}}(\mathbb{K})$.

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 $z = a + \omega b$.

Correction

Soit $z \in \mathbb{L}[\omega]$. L'existence du couple (a,b) est juste donnée par la définition de $\mathbb{L}[\omega]$. Pour l'unicité, soient (a,b,a',b') 4 éléments de $\mathbb{L}$ vérifiant $a+\omega b = a' + \omega b'$. Si on avait $b \neq b'$, alors on aurait

$$\boxed{\omega = (a-a')(b-b')^{-1} \in \mathbb{L},}$$

ce qui est absurde. Donc $b = b'$ et, par conséquent, $a = a'$. D'où l'unicité de l'écriture.

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

Correction

Déjà, si $a \in \mathbb{L}$, $a = a + 0.\omega \in \mathbb{L}[\omega]$, donc $\mathbb{L} \subset \mathbb{L}[\omega]$.
Ensuite :

- $1 \in \mathbb{L}$ donc $1 \in \mathbb{L}[\omega]$,
- si $(x,y) \in \mathbb{L}[\omega]^2$, alors on dispose de $(a,b,c,d) \in \mathbb{L}^4$ vérifiant $x = a+\omega b$ et $y = c + \omega d$. Alors

  $$\boxed{x - y = (a-c) + \omega(b-d) \in \mathbb{L}[\omega]}$$

  et

  $$xy = (a+\omega b)(c+\omega d) = (ac + \omega^2 bd) + \omega(ad+bc).$$

  Mais $\omega^2 \in \mathbb{L}$, donc $ac + \omega^2 bd \in \mathbb{L}$, d'où $\boxed{xy \in \mathbb{L}[\omega].}$
- enfin, si $x \in \mathbb{L}[\omega] \setminus \{0\}$, alors $x = a + \omega b$ où $(a,b) \neq (0,0)$. De plus, $a - \omega b \neq 0$. On écrit alors,

  $$\begin{aligned} x^{-1} &= \frac{1}{a+\omega b} \\ &= \frac{a-\omega b}{a^2 - \omega^2 b^2} \\ &\boxed{= \frac{a}{a^2-\omega^2 b^2} - \frac{b}{a^2-\omega^2 b^2}\omega \in \mathbb{L}[\omega]} \end{aligned}$$

Donc $\mathbb{L}[\omega]$ est un sous-corps de $\mathbb{K}$.

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

Correction

Soit $\varphi \in \mathrm{Aut}_{\mathbb{L}}(\mathbb{L}[\omega])$. Alors pour tous (a,b) dans $\mathbb{L}^2$,

$$\varphi(a+\omega b) = \varphi(a) + \varphi(\omega)\varphi(b) = a + \varphi(\omega) b.$$

Mais $\omega^2 \in \mathbb{L}$, donc

$$\varphi(\omega)^2 = \varphi(\omega^2) = \omega^2,$$

donc $\varphi(\omega) = \pm\omega$.

- si $\varphi(\omega) = \omega$, alors $\varphi = \mathrm{Id}_{\mathbb{L}[\omega]}$.
- si $\varphi(\omega) = -\omega$, alors $\varphi : a + \omega b \mapsto a - \omega b$.

Réciproquement, de telles applications sont dans $\mathrm{Aut}_{\mathbb{K}}(\omega)$.

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 $\mathbb{Q}[i, \sqrt{2}]$.

Correction

On sait que $i^2 = -1 \in \mathbb{Q}$ donc, d'après la question précédente, $\mathbb{Q}[i]$ est un sous-corps de $\mathbb{C}$.
On sait que $\sqrt{2}^2 = 2 \in \mathbb{Q}$ donc, d'après la question précédente, $\mathbb{Q}[i, \sqrt{2}]$ est un sous-corps de $\mathbb{C}$.

B. Extensions cyclotomiques

Dans cette partie, on note $\mathbb{U}_n$ le groupe des racines de l'unité. On note $\omega_n = \mathrm{e}^{\frac{2i\pi}{n}}$, 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 $\xi = \omega_5 = \mathrm{e}^{\frac{2i\pi}{5}}$. 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.

Correction

Il suffit de dessiner un pentagone régulier ! On a, notamment $\xi^4 = \overline{\xi}$ et $\xi^3 = \overline{\xi^2}$.

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 $\displaystyle\sum_{k=0}^{4} \xi^k$? En déduire que

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

Correction

Notons $A = \left\{ \sum_{k=1}^{4} b_k \xi^k,\ (b_1, b_2, b_3, b_4) \in \mathbb{Q}^4 \right\}$. Déjà, trivialement, $A \subset \mathbb{Q}[\mathbb{U}_5]$.
Ensuite, on sait que la somme des racines n-ièmes de l'unité est nulle (si $n \geqslant 2$). Donc $\sum_{k=0}^{4} \xi^k = 0$. Donc si $x \in \mathbb{Q}[\mathbb{U}_5]$,

$$x = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4\xi^4 = (a_1 - a_0)\xi + (a_2 - a_0)\xi^2 + (a_3 - a_0)\xi^3 + (a_4 - a_0)\xi^4 \in A,$$

d'où l'inclusion réciproque et l'égalité !

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 $b = b'$.

Correction

Soient a, a', b, b' quatre rationnels tels que $a \sin\frac{2\pi}{5} + b \sin\frac{4\pi}{5} = a' \sin\frac{2\pi}{5} + b' \sin\frac{4\pi}{5}$. Alors

$$(a - a') \sin\frac{2\pi}{5} + (b - b') \sin\frac{4\pi}{5} = 0,$$

donc

$$(a - a') \sin\frac{2\pi}{5} + 2(b - b') \sin\frac{2\pi}{5} \cos\frac{2\pi}{5} = 0,$$

donc

$$(a - a') + 2(b - b') \cos\frac{2\pi}{5} = 0,$$

car $\sin\frac{2\pi}{5} \neq 0$. Donc, si $b \neq b'$, $\cos\frac{2\pi}{5} = \frac{a - a'}{2(b' - b)} \in \mathbb{Q}$, ce qui est absurde car $\cos\frac{2\pi}{5} \notin \mathbb{Q}$. Donc $b = b'$, puis $a = a'$.

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 $[\![1, 4]\!]$, $b_k = c_k$.

Correction

Soient $(b_1, \ldots, b_4, c_1, \ldots, c_4)$ sont huit rationnels tels que

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

alors, par égalité des parties réelles et imaginaires, et comme ξ et ξ^4 sont conjugués, ainsi que ξ^2 et ξ^3,

$$(b_1 + b_4) \cos\frac{2\pi}{5} + (b_2 + b_3) \cos\frac{4\pi}{5} = (c_1 + c_4) \cos\frac{2\pi}{5} + (c_2 + c_3) \cos\frac{4\pi}{5},$$

donc $b_1 + b_4 = c_1 + c_4$ et $b_2 + b_3 = c_2 + c_3$. De même,

$$(b_1 - b_4)\sin\frac{2\pi}{5} + (b_2 - b_3)\sin\frac{4\pi}{5} = (c_1 - c_4)\sin\frac{2\pi}{5} + (c_2 - c_3)\sin\frac{4\pi}{5},$$

donc $b_1 - b_4 = c_1 - c_4$ et $b_2 - b_3 = c_2 - c_3$. Donc en sommant les égalités avec b_1 et b_4, on obtient $b_1 = c_1$, puis $b_i = c_i$ pour tout i dans $[\![1, 4]\!]$.

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 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \dots & \dots & \dots & \dots \end{pmatrix}$. Préciser sa décomposition en cycles à supports disjoints et sa signature. Calculer σ^2, σ^3 et σ^4.

Correction

On remarque que $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$. Ainsi, σ est le $\boxed{\text{4-cycle (1 2 4 3)}}$. σ est donc sa propre décomposition en cycles à supports disjoints, et $\boxed{\varepsilon(\sigma) = -1}$. On a donc

$$\boxed{\sigma^2 = (1\ 4) \circ (2\ 3),\ \sigma^3 = (1\ 3\ 4\ 2) \text{ et } \sigma^4 = \mathrm{Id}_{[\![1,4]\!]}.}$$

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. ?

Correction

Si l'écriture d'un élément de $\mathbb{Q}[\mathbb{U}_5]$ sous la forme $\displaystyle\sum_{k=1}^{4} b_k\xi^k$ n'était pas unique, alors deux écritures d'un même x pourraient aboutir à deux valeurs différentes de $\varphi(x)$.

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

Correction

Déjà, pour $k = 0$,

$$\varphi(\lambda) = \varphi(-\lambda\xi - \lambda\xi^2 - \lambda\xi^3 - \lambda\xi^4) = -\lambda\xi^2 - \lambda\xi^4 - \lambda\xi - \lambda\xi^3 = \lambda.$$

Ensuite, pour $k \in [\![1, 4]\!]$, $\sigma(k)$ est le reste de la division euclidienne de $2k$ par 5 : $2k = 5q + \sigma(k)$, donc $\xi^{2k} = \xi^{5q+\sigma(k)} = \xi^{\sigma(k)}$ car $\xi^5 = 1$.
Enfin, si $k \geqslant 5$, on note ℓ le reste de la division euclidienne de k par 5. On a alors $\lambda\xi^k = \lambda\xi^\ell$, donc

$$\varphi(\lambda\xi^k) = \varphi(\lambda\xi^\ell) = \lambda\xi^{\sigma(\ell)} = \lambda\xi^{2\ell}\boxed{= \lambda\xi^{2k},}$$

car $2k \equiv 2\ell[5]$.

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

Correction

On a démontré dans la question précédente que pour tout λ dans $\mathbb{Q}$, $\varphi(\lambda) = \lambda$.

Soient x et y dans $\mathbb{Q}[\mathbb{U}_5]$, $x = \sum_{k=1}^{4} a_k \xi^k$ et $y = \sum_{k=1}^{4} b_k \xi^k$. Alors, déjà,

$$\begin{aligned}\varphi(x+y) &= \varphi\left(\sum_{k=1}^{4}(a_k+b_k)\xi^k\right)\\ &= \sum_{k=1}^{4}(a_k+b_k)\xi^{\sigma(k)}\\ &= \sum_{k=1}^{4} a_k\xi^{\sigma(k)} + \sum_{k=1}^{4} b_k\xi^{\sigma(k)}\\ &\boxed{= \varphi(x)+\varphi(y).}\end{aligned}$$

Ensuite,

$$\begin{aligned}\varphi(xy) &= \varphi\left(\sum_{k=1}^{4}\sum_{\ell=1}^{4} a_k b_\ell \xi^{k+\ell}\right)\\ &= \sum_{k=1}^{4}\sum_{\ell=1}^{4} \varphi(a_k b_\ell \xi^{k+\ell}) \text{ par additivité.}\\ &= \sum_{k=1}^{4}\sum_{\ell=1}^{4} b_\ell \xi^{2(k+\ell)} \text{ par la question précédente.}\\ &= \left(\sum_{k=1}^{4} a_k\xi^{2k}\right)\left(\sum_{k=1}^{4} b_k\xi^{2k}\right)\\ &\boxed{= \varphi(x)\varphi(y).}\end{aligned}$$

Enfin, φ est bien bijectif, de bijection réciproque définie par

$$\boxed{\varphi\left(\sum_{k=1}^{4} a_k\xi^k\right) = \sum_{k=1}^{4} a_k\xi^{\sigma^{-1}(k)}.}$$

$\boxed{\text{On en déduit que } \varphi \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\mathbb{U}_5]).}$

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 $\psi = \varphi^k$.

Correction

On sait que $\psi(\xi)^5 = \psi(\xi^5) = \psi(1) = 1$, donc $\psi(\xi) \in \mathbb{U}_5$. De plus, $\psi(\xi) \neq 1$ car, sinon, $\psi(\xi) = \psi(\xi^2)$, donc ψ n'est pas un automorphisme. Ensuite,

$$\psi\left(\sum_{k=1}^{4} a_k\xi^k\right) = \sum_{k=1}^{4}\psi(a_k)\psi(\xi^k) = \sum_{k=1}^{4}\psi(a_k)\xi^k,$$

car ψ est un automorphisme de corps. On distingue alors :

- Si $\psi(\xi) = \xi$, $\psi = \mathrm{Id}_{\mathbb{Q}[\mathbb{U}_5]} = \varphi^0$.
- Si $\psi(\xi) = \xi^2$, alors $\psi(\xi^2) = \xi^4$, $\psi(\xi^3) = \xi^6 = \xi$, $\psi(\xi^4) = \xi^3$, donc $\psi = \varphi$,
- Si $\psi(\xi) = \xi^3$, $\psi(\xi^2) = \xi^6 = \xi$, $\psi(\xi^3) = \xi^9 = \xi^4$ et $\psi(\xi^4) = \xi^1 2 = \xi^2$. On remarque alors que

$$\psi\left(\sum_{k=1}^{4} a_k \xi^k\right) = \sum_{k=1}^{4} a_k \xi^{\sigma^{-1}(k)} = \sum_{k=1}^{4} a_k \xi^{\sigma^3(k)} = \varphi^3\left(\sum_{k=1}^{4} a_k \xi^k\right)$$

- Enfin, si $\psi(\xi) = \xi^4$, $\psi = \varphi^2$.

D'où le résultat !

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

Correction

On en déduit que $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\mathbb{U}_5]) = \{\mathrm{Id}_{\mathbb{Q}[\mathbb{U}_5]}, \varphi, \varphi^2, \varphi^3\}$. C'est un groupe par la question 2, et en posant

$$f : \left| \begin{array}{c} \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\mathbb{U}_5]) \to \mathbb{U}_4 \\ \varphi^k \mapsto i^k \end{array} \right. ,$$

on définit un isomorphisme entre $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\mathbb{U}_5])$ et $\mathbb{U}_4$.

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.

Correction

On sait que $\omega_8 = \mathrm{e}^{\frac{2i\pi}{8}} = \mathrm{e}^{\frac{i\pi}{4}} = \dfrac{\sqrt{2}}{2} + \dfrac{\sqrt{2}}{2} i$.

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

Correction

Déjà, $\omega_8 \in \mathbb{Q}[\mathbb{U}_8]$ et $\omega_8^7 \in \mathbb{Q}[\mathbb{U}_8]$, donc

$$\omega_8 + \omega_8^7 \in \mathbb{Q}[\mathbb{U}_8], \text{ i.e. } \boxed{\sqrt{2} \in \mathbb{Q}[\mathbb{U}_8].}$$

Ensuite, comme $(\omega_8, \sqrt{2}) \in \mathbb{Q}[\mathbb{U}_8]^2$, $\sqrt{2}\omega_8 \in \mathbb{Q}[\mathbb{U}_8]$, donc $1 + i \in \mathbb{Q}[\mathbb{U}_8]$, d'où, comme $1 \in \mathbb{Q} \subset \mathbb{Q}[\mathbb{U}_8]$, $\boxed{i \in \mathbb{Q}[\mathbb{U}_8].}$

Le fait que $\sqrt{2}$ soit dans $\mathbb{Q}[\mathbb{U}_8]$ et que $\mathbb{Q}[\mathbb{U}_8]$ soit un corps assure que $\mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\mathbb{U}_8]$. Mais comme i est aussi dans $\mathbb{Q}[\mathbb{U}_8]$, tous les $a + ib$, avec (a, b) $\boxed{\text{dans } \mathbb{Q}[\sqrt{2}]}$ sont dans $\mathbb{Q}[\mathbb{U}_8]$. Ceci assure que

$$\mathbb{Q}[\sqrt{2}][i] \subset \mathbb{Q}[\mathbb{U}_8], \text{ i.e. } \mathbb{Q}[i, \sqrt{2}] \subset \mathbb{Q}[\mathbb{U}_8].$$

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

Correction

On doit remarquer que

$$\boxed{\mathbb{Q}[i, \sqrt{2}] = \{a + b\sqrt{2} + ci + di\sqrt{2},\ (a, b, c, d) \in \mathbb{Q}^4\}.}$$

Une fois que l'on a remarqué cela, on remarque enfin que les éléments de $\mathbb{U}_8$ sont

$$\pm 1,\ \pm i,\ \pm\frac{\sqrt{2}}{2} \pm \frac{\sqrt{2}}{2} i,$$

$\boxed{\text{qui sont tous des éléments de } \mathbb{Q}[i, \sqrt{2}].}$ Ainsi, $\mathbb{Q}[i, \sqrt{2}]$ étant un corps, alors pour tous $(a_0, \dots, a_7) \in \mathbb{Q}^8$, on a $\sum_{k=0}^{7} a_k \omega_8^k \in \mathbb{Q}[i, \sqrt{2}]$.
D'où l'inclusion réciproque et l'égalité.

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 $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{U}_5)$?

Correction

Soit ψ dans $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{U}_5)$. Alors $\psi(i)^2 = \psi(i)^2 = -1$, donc $\psi(i) = \pm 1$. De même, $\psi(\sqrt{2})^2 = \psi(\sqrt{2}^2) = \psi(2) = 2$, donc $\psi(2) = \pm\sqrt{2}$. On a donc 4 possibilités :

(a) $\psi(i) = i$ et $\psi(\sqrt{2}) = \sqrt{2}$. Mais alors $\psi(a + ib + \sqrt{2}c + i\sqrt{2}d) = a + ib + \sqrt{2}c + i\sqrt{2}d$, donc $\psi = \mathrm{Id}_{\mathbb{Q}[i,\sqrt{2}])}$.

(b) $\psi(i) = -i$ et $\psi(\sqrt{2}) = \sqrt{2}$. Alors

$$\psi(a + ib + c\sqrt{2} + i\sqrt{2}d) = a - ib + c\sqrt{2} - i\sqrt{2}d.$$

On vérifie facilement (un peu comme φ de la partie $\mathbb{U}_5$) que l'on définit alors un élément de $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[i, \sqrt{2}])$, nommons-le α. On voit aussi que $\alpha^2 = \mathrm{Id}_{\mathbb{Q}[i,\sqrt{2}])}$.

(c) $\psi(i) = i$ et $\psi(\sqrt{2}) = -\sqrt{2}$. On définit un troisième automorphisme que l'on note β, vérifiant aussi $\beta^2 = \mathrm{Id}_{\mathbb{Q}[i,\sqrt{2}])}$.

(d) $\psi(i) = -i$ et $\psi(\sqrt{2}) = -\sqrt{2}$. On définit un quatrième automorphisme γ vérifiant $\gamma^2 = \mathrm{Id}_{\mathbb{Q}[i,\sqrt{2}])}$ et, aussi $\alpha \circ \beta = \beta \circ \alpha = \gamma$.

On a alors un groupe à 4 éléments. Il n'est pas isomorphe à $\mathbb{U}_4$ car il n'est pas cyclique. Il est, en fait, isomorphe à $\{-1, 1\}^2$, ou bien au sous-groupe de $\mathcal{S}_4$ défini par $\{\mathrm{Id}, (1\ 2), (3\ 4), (1\ 2) \circ (3\ 4)\}$. Cette dernière description du groupe permet de voir ce groupe comme un groupe de permutation des racines : on permute éventuellement i et $-i$, ou $\sqrt{2}$ et $-\sqrt{2}$.