1. Anneaux et algèbres

Exercice 1. Soient $\mathrm{A}, \mathrm{B}, \mathrm{C}$ des anneaux et $f : \mathrm{A} \to \mathrm{C}$, $g : \mathrm{B} \to \mathrm{C}$ des homomorphismes d'anneaux. Montrer que $\mathrm{D} = \{(a, b) \in \mathrm{A} \times \mathrm{B} \mid f(a) = g(b)\}$ est un sous-anneau de $\mathrm{A} \times \mathrm{B}$.

Exercice 2. Soit A un anneau.

(1) Montrer qu'il existe un unique homomorphisme d'anneaux $f_{\mathrm{A}} : \mathbf{Z} \to \mathrm{A}$.

(2) Montrer qu'il existe un unique entier $n \geqslant 0$ tel que $\mathrm{Ker}(f_{\mathrm{A}}) = n\mathbf{Z}$. On appelle cet entier la *caractéristique* de A.

(3) Montrer qu'un anneau fini est de caractéristique non nulle.

(4) Montrer que la caractéristique d'un anneau intègre est soit 0, soit un nombre premier.

(5) Soit $\varphi : \mathrm{A} \to \mathrm{B}$ un homomorphisme d'anneaux. Montrer que la caractéristique de B divise celle de A.

Exercice 3. Un élément a d'un anneau A est *nilpotent* s'il existe un entier $n \geqslant 1$ pour lequel on ait $a^n = 0$.

(1) Montrer que l'ensemble N des éléments nilpotents de A est un idéal de A.

(2) Montrer que A/N ne possède pas d'élément nilpotent non nul.

Exercice 4. Si A est un anneau, on note $\mathrm{A}^\times$ l'ensemble de ses unités.

(1) Soit A un anneau. Montrer que $(\mathrm{A}^\times, \times)$ est un groupe.

(2) Soient A, B des anneaux. Montrer que $(\mathrm{A} \times \mathrm{B})^\times = \mathrm{A}^\times \times \mathrm{B}^\times$.

Exercice 5. Soit $\varphi : \mathrm{A} \to \mathrm{B}$ un homomorphisme d'anneaux.

(1) Montrer que $\varphi(\mathrm{A}^\times)$ est inclus dans $\mathrm{B}^\times$.

(2) On note $\varphi^\times$ l'application de $\mathrm{A}^\times$ dans $\mathrm{B}^\times$ définie par $a \mapsto \varphi(a)$. Montrer que c'est un homomorphisme de groupes.

(3) Si φ est injective (resp. surjective, bijective), qu'en est-il de $\varphi^\times$?

(4) Si $\varphi^\times$ est injective (resp. surjective, bijective), qu'en est-il de φ ?

Exercice 6. Soient A, B des anneaux. Discuter l'injectivité (resp. la surjectivité) de l'application $\varphi \mapsto \varphi^\times$ de $\mathrm{Hom}(\mathrm{A}, \mathrm{B})$ dans $\mathrm{Hom}(\mathrm{A}^\times, \mathrm{B}^\times)$.

Exercice 7.

(1) Montrer que, pour $n \in \{1, 2, 3, 4\}$, il existe un anneau A tel que le groupe $\mathrm{A}^\times$ soit d'ordre n.

(2) Montre qu'il n'existe pas d'anneau A tel que le groupe $\mathrm{A}^\times$ soit d'ordre 5.

(3) Montrer qu'il existe un anneau A tel que $\mathrm{A}^\times$ soit isomorphe à $\mathbf{Z}$.

2. Polynômes

Exercice 8. Soit k un corps de caractéristique 0. Déterminer l'ensemble des polynômes $f \in k[\mathrm{X}]$ tels que le polynôme dérivé f' divise f.

Exercice 9. Soit k un corps de caractéristique non nulle p.

(1) Soit $f \in k[\mathrm{X}]$. Montrer que $f' = 0$ si, et seulement si, $f \in k[\mathrm{X}^p]$.

(2) Déterminer l'ensemble des polynômes $f \in k[\mathrm{X}]$ tels que f' divise f.

Exercice 10. Soit $f = a_0 + a_1\mathrm{X} + \ldots + a_n\mathrm{X}^n \in \mathbf{Z}[\mathrm{X}]$ de degré n. On suppose que f a une racine rationnelle, qu'on écrit p/q avec $p, q \in \mathbf{Z}$ premiers entre eux et $q \neq 0$. Montrer que p divise a_0 et que q divise a_n.

Exercice 11. Pour $f \in \mathbf{Z}[\mathrm{X}]$ non nul, on note $c(f)$ le plus grand diviseur commun aux coefficients de f, qu'on appelle le *contenu* de f.

(1) Soient $f, g \in \mathbf{Z}[\mathrm{X}]$ non nuls de contenu 1. Montrer que fg est de contenu 1.

(2) Soient $f, g \in \mathbf{Z}[\mathrm{X}]$ non nuls. Montrer que $c(fg) = c(f)c(g)$.

(3) Soit $f \in \mathbf{Z}[\mathrm{X}]$ non nul. Montrer que f est irréductible sur $\mathbf{Z}$ et si et seulement si f est irréductible sur $\mathbf{Q}$ et de contenu 1.

Exercice 12. Critère d'Eisenstein.

Soit $f \in \mathbf{Z}[\mathrm{X}]$ un polynôme unitaire de degré $n \geqslant 1$, qu'on écrit :

$$f = \mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + \cdots + a_1\mathrm{X} + a_0.$$

On suppose qu'il existe un nombre premier p divisant chaque a_i pour $0 \leqslant i \leqslant n-1$, et tel que p^2 ne divise pas a_0. Montrer que f est irréductible sur $\mathbf{Q}$.

Exercice 13.

(1) Montrer que, pour tout $n \geqslant 1$, le polynôme $\mathrm{X}^n - 2$ est irréductible sur $\mathbf{Q}$.

(2) Soit p un nombre premier et soit $\Phi_p = \mathrm{X}^{p-1} + \cdots + \mathrm{X} + 1$. Montrer que le polynôme $\Phi_p(\mathrm{X}+1)$ est irréductible sur $\mathbf{Q}$. En déduire que Φ_p est irréductible sur $\mathbf{Q}$, puis déterminer le polynôme minimal de $\exp(2i\pi/p)$ sur $\mathbf{Q}$.

Exercice 14. Pour $\mathrm{P} \in \mathbf{C}[\mathrm{X}]$ non nul, on pose $\mathrm{P}^* = \mathrm{X}^{\deg(\mathrm{P})}\mathrm{P}(1/\mathrm{X}) \in \mathbf{C}(\mathrm{X})$.

(1) Pour $\mathrm{P} \neq 0$, montrer que P^* est un polynôme.

(2) Montrer que, pour $k \geqslant 1$, il existe un unique polynôme unitaire $\mathrm{U}_k \in \mathbf{Z}[\mathrm{X}]$ tel que $\mathrm{X}^k + \mathrm{X}^{-k} = \mathrm{U}_k(\mathrm{X} + \mathrm{X}^{-1})$.

(3) Soit $\mathrm{P} \neq 0$ tel que $\mathrm{P}^* = \mathrm{P}$ et soit $n = \deg(\mathrm{P})$. Montrer qu'il existe $\mathrm{Q} \in \mathbf{C}[\mathrm{X}]$ de degré $[n/2]$ tel que :

$$\mathrm{P} = \begin{cases} \mathrm{X}^{n/2}\mathrm{Q}(\mathrm{X} + 1/\mathrm{X}) & \text{si } n \text{ est pair,} \\ (\mathrm{X}+1)\mathrm{X}^{(n-1)/2}\mathrm{Q}(\mathrm{X} + 1/\mathrm{X}) & \text{sinon.} \end{cases}$$

(4) Montrer que les coefficients de P et ceux de Q engendrent la même sous-$\mathbf{Z}$-algèbre de $\mathbf{C}$.

Exercice 15. Pour tout $\mathrm{P} \in \mathbf{C}[\mathrm{X}]$ non nul, on pose $\mathrm{P}^* = \mathrm{X}^{\deg(\mathrm{P})}\mathrm{P}(1-1/\mathrm{X})$. Quels sont les polynômes vérifiant $\mathrm{P}^* = \mathrm{P}$?

Exercice 16. Soit un entier $n \geqslant 1$ et soit $\omega = \exp(2i\pi/n) \in \mathbf{C}$. Montrer qu'un polynôme $f \in \mathbf{C}[\mathrm{X}]$ vérifie $f(\omega\mathrm{X}) = f$ si et seulement s'il appartient à $\mathbf{C}[\mathrm{X}^n]$.

Exercice 17. Soit un entier $n \geqslant 0$.

(1) Montrer qu'il existe un unique polynôme $\mathrm{T}_n \in \mathbf{Z}[\mathrm{X}]$ de degré n vérifiant la condition $\mathrm{T}_n(\cos(\theta)) = \cos(n\theta)$ pour tout $\theta \in \mathbf{R}$. Quelles sont ses racines complexes ?

(2) Calculer T_n pour $n \leqslant 7$. Lesquels sont irréductibles sur $\mathbf{Q}$?

(3) Déterminer une relation de récurrence linéaire d'ordre 2 entre les T_n, $n \geqslant 0$. En déduire que la série génératrice $\mathscr{T} = \sum_{n\geqslant 0} \mathrm{T}_n(\mathrm{X})\mathrm{Y}^n \in \mathbf{Z}[\mathrm{X}][\![\mathrm{Y}]\!]$ vérifie :

$$\mathscr{T} = \frac{1 - \mathrm{XY}}{1 - 2\mathrm{XY} + \mathrm{Y}^2}.$$

Exercice 18. Montrer que les polynômes $\mathrm{X}^4 + 1$ et $\mathrm{X}^6 + \mathrm{X}^3 + 1$ sont irréductibles sur $\mathbf{Q}$. Qu'en est-il du polynômes $\mathrm{X}^3 - 5\mathrm{X}^2 + 1$?

Exercice 19. Soit K un corps quelconque, et soient $a, b \in \mathrm{K}$ avec $a \neq 0$.

(1) Montrer que $f \mapsto f(a\mathrm{X}+b)$ définit un automorphisme de K-algèbre de K[X], qu'on notera $\theta_{a,b}$.

(2) Montrer que tout automorphisme de K-algèbre de K[X] est de la forme $\theta_{a,b}$.

(3) Montrer que le groupe $\mathrm{Aut}_{\mathrm{K}}(\mathrm{K}[\mathrm{X}])$ des automorphismes de K-algèbre de K[X] est isomorphe au groupe affine $\mathrm{GA}_1(\mathrm{K})$.

Exercice 20. Soit $\mathrm{P} \in \mathbf{Z}[\mathrm{X}]$ de degré $\geqslant 1$. Montrer que pour tous $n, k \in \mathbf{Z}$, l'entier $\mathrm{P}(n + k\mathrm{P}(n))$ est divisible par $\mathrm{P}(n)$. En déduire que P ne peut pas prendre que des valeurs premières sur $\mathbf{Z}$.

Exercice 21. Soit k un corps et soit $\mathrm{P} \in k[\mathrm{X}]$ un polynôme. Montrer que $\mathrm{P}(\mathrm{X}) - \mathrm{X}$ divise $\mathrm{P}(\mathrm{P}(\mathrm{X})) - \mathrm{X}$.

Exercice 22. Soit k un corps, et soit $f \in k(t)$ une fraction rationnelle induisant une application bijective de k dans k dont la réciproque soit aussi induite par une fraction rationnelle à coefficients dans k. Montrer que f est un polynôme de degré 1 sur k.

3. Extensions de corps

Exercice 23. Calculer le polynôme minimal sur $\mathbf{Q}$ de $\cos(2\pi/5)$, puis de $\cos(2\pi/7)$.

Exercice 24. On pose $\alpha = \sqrt{2} + \sqrt{3} \in \mathbf{C}$ et $\mathrm{K} = \mathbf{Q}(\alpha)$.

(1) Montrer que $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathrm{K}$.

(2) Calculer le polynôme minimal f de α sur $\mathbf{Q}$ et montrer que K contient toutes les racines complexes de f.

(3) Déterminer tous les sous-corps de K.

Exercice 25. Soit L une extension algébrique d'un corps K, soit $\alpha \in \mathrm{L}$ et soit f le polynôme minimal de α sur K.

(1) Montrer que $\mathrm{K}(\alpha^2) \neq \mathrm{K}(\alpha)$ si et seulement si f est pair. Que pensez-vous qu'il se passe lorsque f est impair ?

(2) A quelle condition portant sur f a-t-on $\mathrm{K}(\alpha^3) \neq \mathrm{K}(\alpha)$?

Exercice 26. Est-il vrai que $\mathbf{Q}(\sqrt[3]{2} + \sqrt[3]{3}) = \mathbf{Q}(\sqrt[3]{2}, \sqrt[3]{3})$?

Exercice 27. Soit $\alpha = \sqrt[3]{2}$ et soit $j = \exp(2i\pi/3)$. Quels sont les sous-corps du corps $\mathrm{K} = \mathbf{Q}(\alpha, j)$?

Exercice 28. Soit $\alpha \in \mathbf{C}$ une racine de $\mathrm{X}^3 + \mathrm{X}^2 + \mathrm{X} + 2$ et soit $\mathrm{K} = \mathbf{Q}(\alpha)$. Exprimer $(\alpha^2 + \alpha + 1)(\alpha^2 + \alpha)$ et $(\alpha - 1)^{-1}$ sous la forme $a\alpha^2 + b\alpha + c$, avec $a, b, c \in \mathbf{Q}$.

Exercice 29. Soit $\alpha = \sqrt[4]{2} \in \mathbf{R}$. Quels sont les sous-corps de $\mathrm{K} = \mathbf{Q}(\alpha)$?

Exercice 30. Soit a un nombre rationnel strictement positif, et soit p un nombre premier. On suppose que $a^{1/p} \notin \mathbf{Q}$. Montrer que le polynôme $\mathrm{X}^p - a$ est irréductible sur $\mathbf{Q}$.

Exercice 31. Déterminer le polynôme minimal sur $\mathbf{Q}$ de $\sqrt{2} + \sqrt{3} + \sqrt{5}$.

Exercice 32. Calculer l'inverse de $\sqrt[3]{2} - 1$ dans $\mathbf{Q}(\sqrt[3]{2})$.

Exercice 33. On pose $f = \mathrm{X}^4 - 2\mathrm{X}^2 + 9 \in \mathbf{Q}[\mathrm{X}]$.

(1) Montrer que f est irréductible sur $\mathbf{Q}$.

(2) Décomposer f en deux facteurs de degré 2 dans $\mathbf{Q}(i)$.

(3) Montrer que le corps de décomposition de f dans $\mathbf{C}$ est $\mathbf{Q}(i+\sqrt{2})$.

Exercice 34. On note sin et cos les fonctions trigonométriques sinus et cosinus vues commes éléments de la $\mathbf{R}$-algèbre $\mathscr{C}^\infty(\mathrm{I}, \mathbf{R})$, avec $\mathrm{I} =]-\pi/2, \pi/2[$.

(1) Montrer que $\mathbf{R}(\sin)$ et $\mathbf{R}(\cos)$ sont des extensions transcendantes de $\mathbf{R}$.

(2) Montrer que sin est algébrique sur $\mathbf{R}(\cos)$, et calculer son degré.

(3) On note t la fonction $\theta \mapsto \tan(\theta/2)$. Montrer que $\mathbf{R}(\sin, \cos) = \mathbf{R}(t)$.

(4) Montrer que $\mathbf{R}(\sin) \cap \mathbf{R}(\cos) = \mathbf{R}(\sin^2) = \mathbf{R}(\cos^2)$, qu'on note K. Calculer le degré de $\mathbf{R}(\sin)$, puis de $\mathbf{R}(\cos)$, sur K.

(5) On pose $\tan = \sin / \cos$. Montrer que $\mathbf{R}(\tan)$ contient $\mathbf{R}(\sin^2)$. Calculer le degré de $\mathbf{R}(t)$ sur $\mathbf{R}(\tan)$, puis celui de $\mathbf{R}(\tan)$ sur $\mathbf{R}(\sin^2)$.

Exercice 35. Pour $n \geqslant 1$, on note C_n la fonction $\theta \mapsto \cos(n\theta)$ vue comme élément de la $\mathbf{R}$-algèbre $\mathscr{C}^\infty(\mathbf{R}, \mathbf{R})$.

(1) Pour tout $n \geqslant 1$, montrer que $\mathbf{R}(\mathrm{C}_n)$ est une extension transcendante de $\mathbf{R}$.

(2) Pour tout $n \geqslant 1$, montrer que $\mathrm{C}_n \in \mathbf{R}(\mathrm{C}_1)$ et que $\mathbf{R}(\mathrm{C}_1)$ est de degré fini sur $\mathbf{R}(\mathrm{C}_n)$. Calculer ce degré.

(3) Comparer $\mathbf{R}(\mathrm{C}_2, \mathrm{C}_3)$ et $\mathbf{R}(\mathrm{C}_1)$.

4. Homomorphismes d'extensions de corps

Exercice 36. On pose $\alpha = \sqrt[3]{2}$ et $j = \exp(2i\pi/3)$.

(1) On pose $\mathrm{K} = \mathbf{Q}(\alpha)$. Montrer que le groupe $\mathrm{Aut}_{\mathbf{Q}}(\mathrm{K})$ est trivial.

(2) On pose $\mathrm{L} = \mathrm{K}(j)$. Montrer que le groupe $\mathrm{Aut}_{\mathbf{Q}}(\mathrm{L})$ est isomorphe à S_3.

Exercice 37. Soit $\mathrm{K} = \mathbf{Q}(\sqrt{2}+\sqrt{3})$. Montrer que le groupe $\mathrm{Aut}_{\mathbf{Q}}(\mathrm{K})$ est isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

Exercice 38. Soit $\mathrm{L} = \mathbf{F}_2(\mathrm{X})$ et soit $\mathrm{K} = \mathbf{F}_2(\mathrm{X}^2)$. Montrer que L est de degré 2 sur K et que $\mathrm{Aut}_{\mathrm{K}}(\mathrm{L})$ est trivial.

Exercice 39. Trouver un polynôme unitaire $f \in \mathbf{Q}[\mathrm{X}]$ de degré 4 dont les nombres complexes $i\sqrt{3}$ et $1 + i\sqrt{3}$ soient des racines. Si K est le sous-corps de $\mathbf{C}$ engendré par les racines de f, existe-t-il un automorphisme σ de K tel que $\sigma(i\sqrt{3}) = 1+i\sqrt{3}$?

Exercice 40. Soit $f = \mathrm{X}^3 + a\mathrm{X} + b$ un polynôme irréductible dans $\mathbf{Q}[\mathrm{X}]$, et soit D son corps de décomposition sur $\mathbf{Q}$. On pose $d = -27b^2 - 4a^3$ et on note x_1, x_2, x_3 les trois racines de f dans D.

(1) On note $\mathrm{K}_1 = \mathrm{Q}(x_1)$. Montrer que D est une extension de K_1 de degré $\leqslant 2$, engendrée par x_2. Décrire les éléments de $\mathrm{Hom}_{\mathbf{Q}}(\mathrm{K}_1, \mathrm{D})$, et en déduire que le groupe $\mathrm{G} = \mathrm{Aut}(\mathrm{D})$ est d'ordre 3 ou 6, selon que $\mathrm{D} = \mathrm{K}_1$ ou non.

(2) Montrer que tout $\sigma \in \mathrm{G}$ définit une permutation $\bar{\sigma} \in \mathrm{S}_3$ telle que :

$$\sigma(x_i) = x_{\bar{\sigma}(i)}, \quad i \in \{1, 2, 3\}.$$

Montrer que $\sigma \mapsto \bar{\sigma}$ est un homomorphisme injectif de groupes de G dans S_3, d'image notée $\bar{\mathrm{G}}$. En déduire que $\bar{\mathrm{G}}$ contient le groupe alterné A_3.

(3) On pose :

$$\Delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \in \mathrm{D}^\times.$$

Montrer que $\Delta^2 = d$ et en déduire que $\mathbf{Q}(\Delta)$ est de degré $\leqslant 2$ sur $\mathbf{Q}$. *(On pourra remarquer que* $\Delta^2 = -f'(x_1)f'(x_2)f'(x_3)$*.)*

(4) On suppose que d est un carré de $\mathbf{Q}^\times$. Montrer que $\bar{\mathrm{G}} = \mathrm{A}_3$. *(On pourra étudier l'action de* S_3 *sur* Δ*.)* En déduire que D est galoisienne et de degré 3 sur $\mathbf{Q}$.

(5) On suppose que d n'est pas un carré de $\mathbf{Q}^\times$. Montrer que $[\mathrm{D} : \mathbf{Q}] = 6$ et que $\bar{\mathrm{G}} = \mathrm{S}_3$. *(On pourra utiliser* $\mathbf{Q}(\Delta)$*.)* Montrer que D est galoisienne sur $\mathbf{Q}$.

Exercice 41. Soit K un corps de caractéristique $\neq 2$ et soit L une extension de K de degré 2.

(1) Soit $\alpha \in \mathrm{L}$. Montrer que $\mathrm{L} = \mathrm{K}(\alpha)$ si et seulement si $\alpha \notin \mathrm{K}$.

(2) Montrer qu'il existe un $\alpha \in \mathrm{L}^\times$ tel que $\alpha^2 \in \mathrm{K}^\times$ et $\mathrm{L} = \mathrm{K}(\alpha)$. En déduire que $\mathrm{Aut}_{\mathrm{K}}(\mathrm{L})$ est isomorphe au groupe $\mathbf{Z}/2\mathbf{Z}$.

Exercice 42. Soit K un corps de caractéristique égale à un nombre premier p, et soit $a \in \mathrm{K}$. On note τ_a le K-automorphisme de $\mathrm{K}(\mathrm{X})$ défini par $\mathrm{X} \mapsto \mathrm{X} + a$. Montrer que le sous-corps des τ_a-invariants de $\mathrm{K}(\mathrm{X})$ est égal à $\mathrm{K}(f_a)$, avec $f_a = \mathrm{X}^p - a^{p-1}\mathrm{X}$.

Exercice 43. Soit K un corps.

(1) Montrer que l'application de $\mathrm{Aut}_{\mathrm{K}}(\mathrm{K}(\mathrm{X}))$ dans $\mathrm{K}(\mathrm{X})$ définie par $\sigma \mapsto \sigma(\mathrm{X})$ est injective.

(2) Montrer que son image, notée H_{K}, est constituée des homographies de $\mathrm{K}(\mathrm{X})$, c'est-à-dire des fractions de la forme :

$$\frac{a\mathrm{X} + b}{c\mathrm{X} + d}, \quad ad - bc \neq 0.$$

(3) Montrer que $\mathrm{H_K}$, muni de la loi $(f, g) \mapsto f \circ g$, est un groupe, et montrer que $\sigma \mapsto \sigma(\mathrm{X})$ est un isomorphisme de groupes.

(4) Montrer que l'application :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathrm{K}) \mapsto \frac{a\mathrm{X}+b}{c\mathrm{X}+d} \in \mathrm{H_K}$$

est un homomorphisme surjectif de groupes. Quel est son noyau ?

5. Correspondance de Galois

Exercice 44. On pose :

$$\alpha = \sqrt{\frac{1+\sqrt{5}}{2}}.$$

(1) Montrer que $\mathrm{L} = \mathbf{Q}(\alpha)$ contient $\mathrm{K} = \mathbf{Q}(\sqrt{5})$, et calculer le degré de L sur K.

(2) Montrer que L est galoisienne sur K et que K est galoisienne sur $\mathbf{Q}$.

(3) Déterminer le polynôme minimal de α sur $\mathbf{Q}$ et calculer ses racines complexes.

(4) En déduire que L n'est pas galoisienne sur $\mathbf{Q}$.

Exercice 45. On pose :

$$\alpha = \sqrt{3+\sqrt{3}}.$$

(1) Trouver un polynôme de degré 4 dans $\mathbf{Q}[\mathrm{X}]$ annulant α, puis calculer le degré de α sur $\mathbf{Q}$.

(2) Montrer que $\sqrt{2} \notin \mathbf{Q}(\alpha)$, puis que $\mathrm{K} = \mathbf{Q}(\alpha, \sqrt{2})$ est le corps de décomposition de f sur $\mathbf{Q}$.

(3) Montrer que $\mathrm{Gal}(\mathrm{K}/\mathbf{Q})$ est non abélien et d'ordre 8. Est-il isomorphe à $\mathrm{D_4}$ ou à $\mathrm{Q_8}$?

Exercice 46. Soit :

$$\alpha = \sqrt[3]{2+\sqrt{2}}.$$

(1) Trouver un polynôme de degré 6 dans $\mathbf{Q}[\mathrm{X}]$ annulant α.

(2) Calculer le degré de α sur $\mathbf{Q}$.

(3) Calculer le polynôme minimal de α^2 sur $\mathbf{Q}$.

(4) On pose $j = \exp(2i\pi/3)$. Montrer que $\mathrm{E} = \mathbf{Q}(\alpha, \sqrt[3]{2}, j)$ est le corps de décomposition de $\mathrm{Pmin}_{\mathbf{Q}}(\alpha)$ sur $\mathbf{Q}$.

(5) Montrer que $\sqrt[3]{2}$ n'appartient pas à $\mathbf{Q}(\alpha)$. En déduire la valeur de $[\mathrm{E} : \mathbf{Q}]$.

(6) Calculer $\mathrm{Gal}(\mathrm{E}/\mathbf{Q})$.

Exercice 47. Soit :

$$w = \sqrt{2-\sqrt{2}} + i\sqrt{\sqrt{2}-1}.$$

(1) Montrer que $|w| = 1$, et en déduire que $w^{-1} = \sqrt{2-\sqrt{2}} - i\sqrt{\sqrt{2}-1}$.

(2) Trouver un polynôme de degré 4 dans $\mathbf{Q}[\mathrm{X}]$ annulant $\beta = (w + w^{-1})/2$.

(3) Montrer que les racines complexes du polynôme $f = \mathrm{X}^4 - 4\mathrm{X}^2 + 2$ sont :

$$x_1 = \sqrt{2+\sqrt{2}},\ x_2 = \sqrt{2-\sqrt{2}},\ x_3 = -\sqrt{2+\sqrt{2}},\ x_4 = -\sqrt{2-\sqrt{2}}.$$

(4) Montrer que le corps de décomposition E de f sur $\mathbf{Q}$ est $\mathbf{Q}(\sqrt{2-\sqrt{2}})$.

(5) Montrer qu'il existe un unique $\sigma \in \mathrm{G} = \mathrm{Gal}(\mathrm{E}/\mathbf{Q})$ tel que $\sigma(x_1) = x_2$.

(6) Montrer que σ opère sur les racines de f comme le cycle $(1\ 2\ 3\ 4) \in \mathrm{S}_4$, et que G est engendré par σ. En déduire que $\mathrm{G} \simeq \mathbf{Z}/4\mathbf{Z}$.

(7) Montrer que $\mathrm{E}^{\sigma^2} = \mathbf{Q}(\sqrt{2})$. En déduire qu'il existe un unique homomorphisme surjectif de groupes $\Phi : \mathrm{G} \to \mathrm{Gal}(\mathbf{Q}(\sqrt{2})/\mathbf{Q}) \simeq \mathbf{Z}/2\mathbf{Z}$.

(8) Montrer que les quatre racines complexes du polynôme $g = \mathrm{X}^4 - 2\mathrm{X}^2 - 1$ sont :

$$y_1 = \sqrt{\sqrt{2}+1},\ y_2 = i\sqrt{\sqrt{2}-1},\ y_3 = -\sqrt{\sqrt{2}+1},\ y_4 = -i\sqrt{\sqrt{2}-1}.$$

(9) Montrer que le corps de décomposition E′ de g sur $\mathbf{Q}$ est $\mathbf{Q}(i, \sqrt{\sqrt{2}+1})$.

(10) Montrer que la conjugaison complexe $z \mapsto \bar{z}$ est un élément de $\mathrm{G}' = \mathrm{Gal}(\mathrm{E}'/\mathbf{Q})$ que l'on notera γ.

(11) Montrer qu'il existe un unique automorphisme $\sigma' \in \mathrm{G}'$ tel que σ' opère sur les racines de g comme le cycle $(1\ 2\ 3\ 4) \in \mathrm{S}_4$, et montrer que γ opère comme la transposition $(2\ 4)$.

(12) Montrer que G′ est engendré par σ' et γ.

(13) Trouver le sous-groupe Π de S_4 tel que G′ opère sur les racines de g comme Π.

(14) Montrer que $\mathbf{Q}(\sqrt{2})$ est un sous-corps de E′, et déterminer le sous-groupe $\mathrm{H} = \mathrm{Gal}(\mathrm{E}'/\mathbf{Q}(\sqrt{2}))$. On note Φ' l'homomorphisme surjectif :

$$\mathrm{G}' \to \mathrm{Gal}(\mathbf{Q}(\sqrt{2})/\mathbf{Q}) \simeq \mathbf{Z}/2\mathbf{Z}$$

de noyau H.

(15) Montrer que G′ possède cinq sous-groupes d'ordre 2 et trois sous-groupes d'ordre 4. Les déterminer explicitement, ainsi que les sous-corps d'invariants qui leur correspondent. Lesquels sont des extensions galoisiennes de $\mathbf{Q}$?

(16) Trouver un polynôme P unitaire de degré 8 dans $\mathbf{Q}[\mathrm{X}]$ annulant w.

(17) Déterminer toutes les racines complexes de P *(on remarquera que les coefficients de* P *sont symétriques).*

(18) Montrer que $\mathbf{Q}(w)$ est de degré 8 sur $\mathbf{Q}$. En déduire que P est irréductible sur $\mathbf{Q}$.

(19) Montrer que le corps de décomposition de P sur $\mathbf{Q}$, qu'on note L, est égal au corps de décomposition de fg sur $\mathbf{Q}$.

(20) Montrer que $\mathscr{G} = \{(a, a') \in \mathrm{G} \times \mathrm{G}' \mid \Phi(a) = \Phi'(a')\}$ est un sous-groupe de $\mathrm{G} \times \mathrm{G}'$, qui est isomorphe à $\mathrm{Gal}(\mathrm{L}/\mathbf{Q})$.

Exercice 48. Soit E une extension galoisienne de degré 4 de $\mathbf{Q}$ dont le groupe de Galois est cyclique, c'est-à-dire isomorphe à $\mathbf{Z}/4\mathbf{Z}$.

(1) Montrer qu'il existe $d \in \mathbf{Q}^\times$ qui n'est pas un carré dans $\mathbf{Q}$ et qui est tel que $\mathbf{Q}(\sqrt{d})$ soit l'unique sous-extension de degré 2 de E sur $\mathbf{Q}$.

(2) Montrer qu'il existe $a, b \in \mathbf{Q}$ tels que $d(a^2 - db^2)$ soit un carré non nul de $\mathbf{Q}$ et tel que $\mathrm{E} = \mathbf{Q}\left(\sqrt{a + b\sqrt{d}}\right)$.

(3) Montrer que d est une somme de deux carrés de $\mathbf{Q}$.

(4) Si $a', b' \in \mathbf{Q}$ vérifient $\mathrm{E} = \mathbf{Q}\left(\sqrt{a' + b'\sqrt{d}}\right)$, montrer que $d(a'^2 - db'^2)$ est un carré non nul de $\mathbf{Q}$.

(5) Inversement, soient des nombres rationnels $d, a, b \in \mathbf{Q}$ tels que d ne soit pas un carré dans $\mathbf{Q}$ et tel que $d(a^2 - db^2)$ soit un carré non nul dans $\mathbf{Q}$. Montrer que l'extension :

$$\mathrm{E}' = \mathbf{Q}\left(\sqrt{a + b\sqrt{d}}\right)$$

est une extension galoisienne de $\mathbf{Q}$ de degré 4 dont le groupe de Galois est cyclique. Puis montrer que le polynôme minimal de $\sqrt{a + b\sqrt{d}}$ sur $\mathbf{Q}$ est égal à $\mathrm{X}^4 - 2a\mathrm{X}^2 + (a^2 - db^2)$.