1 Définition de corps et d'extensions

Exercice 1. Soit A un anneau. Quels sont les critères nécessaires et suffisants sur A pour que la phrase "Soit $P \in A[X]$. Alors son nombre de racines est majoré par son degré" soit vérifiée ? Donner des contre-exemples lorsque ces conditions ne sont pas vérifiées.

Exercice 2. Soit A un anneau fini et intègre. Montrer que A est un corps.

Exercice 3. [Retour d'oraux] Que peut-on dire de l'anneau $\mathbb{F}_{17}[X]/(X^2 - 11)$?

Exercice 4. [Retour d'oraux] L'ensemble des nombres algébriques sur $\mathbb{Q}$ est-il dénombrable ? Est-ce que $\mathbf{C}$ est la clôture algébrique de $\mathbf{Q}$?

Exercice 5. Soit $f \in \mathrm{Aut}_{\mathbf{Q}}(\mathbb{R})$. Montrer que f est forcément croissante. En déduire

$$\mathrm{Aut}_{\mathbf{Q}}(\mathbb{R}) = \{\mathrm{id}_{\mathbb{R}}\}.$$

Exercice 6. [FGN1. 3.16] Déterminer les automorphismes de $\mathbf{Q}(\sqrt{2})$.

Exercice 7. [Retour d'oraux] Est-ce qu'un corps fini peut être algébriquement clos ?

Exercice 8. Montrer que si a et b sont deux éléments non nuls d'un corps K de caractéristique différente de 2, alors $K(\sqrt{a}) = K(\sqrt{b})$ si et seulement si b/a est un carré dans K.

2 Degré d'une extension

Exercice 9. [Ortiz, III.1] Pour quels nombres premiers p et q a-t-on $\mathbf{Q}(\sqrt{p}) \subset \mathbf{Q}(\sqrt[3]{q})$?

Exercice 10. Soit L/K une extension finie de corps de degré m. Soit $P \in K[X]$ un polynôme irréductible de degré d, premier à m. Montrer que P est irréductible sur L.

Exercice 11. Soit K un corps de caractéristique $p \in \mathbb{N}$ et soit L une extension de K.

1. On suppose $p = 0$.
   (a) Montrer l'équivalence :
   $$[L : K] \leqslant n \iff \forall x \in L, [K(x) : K] \leqslant n$$
   (indication : on rappelle que toute extension finie de K est monogène).
   (b) Montrer qu'il est possible d'avoir à la fois :
   $$[L : K] = +\infty \text{ et } \forall x \in L, [K(x) : K] < \infty$$
2. On suppose $p > 0$. Montrer que 1.(a) peut être en défaut.

3 Polynômes irréductibles, polynômes minimal, racines

Exercice 12. [Retour d'oraux] Montrer que $X^3 + X + 1$ est irréductible sur $\mathbf{Q}(i)$.

Exercice 13. Déterminer le polynôme minimal de $1 + \sqrt[3]{2} + 3\sqrt[3]{4}$ sur $\mathbf{Q}$.

Exercice 14. [Perrin, Corollaire 4.12, page 83]

1. Soit $k \subset M$ une extension, et K et L deux corps intermédiaires. Soit KL le sous-corps de M engendré par K et L. Montrer que $[KL : L] \leqslant [K : k]$.
2. En déduire l'assertion suivante : soient α (resp. β) une racine n-ième (resp. m-ième) primitive de l'unité dans $\mathbf{C}$. On suppose que $n \cap m = 1$. Alors on a $\mathbf{Q}(\alpha) \cap \mathbf{Q}(\beta) = \mathbf{Q}$.

Exercice 15. [Ortiz, III.6, et exercice classique d'oraux] Soit $j = e^{\frac{2i\pi}{3}} = \frac{-1+i\sqrt{3}}{2}$.

1. Donner les polynômes minimaux sur $\mathbf{Q}$ des nombres complexes suivants :
   (a) $\sqrt[3]{7} + \sqrt{2}$
   (b) $i + j$
   (c) $j + \sqrt{3}$
   (d) $j\sqrt{2}$
   (e) $i + \sqrt{2}$
2. Soit $\zeta \in \mathbf{C}$ une racine primitive 5-ième de 1. Dans chacun des cas suivants, trouver le polynôme minimal de ζ sur K :
   (a) $K = \mathbf{Q}$
   (b) $K = \mathbf{Q}(i)$
   (c) $K = \mathbf{Q}(\sqrt{5})$ (considérer $\zeta + \zeta^{-1}$).

Exercice 16. [Gourdon algèbre, Chap. 2, 1, exercice 4]

1. Soit $P \in \mathbb{Q}[X]$ irréductible dans $\mathbb{Q}[X]$. Montrer que P n'a que des racines simples dans $\mathbb{C}$.
2. (Deux applications)
   (a) Soit $P \in \mathbb{Q}[X]$ un polynôme ayant une racine $\lambda \in \mathbb{C}$ d'ordre de multiplicité $\mu > \deg(P)/2$. Montrer que $\lambda \in \mathbb{Q}$.
   (b) Soit $P \in \mathbb{Q}[X], \deg(P) = 2n + 1$ avec $n \in \mathbb{N}^*$, tel que P admette une racine d'ordre n. Si $n \geqslant 2$, montrer que P admet une racine dans $\mathbb{Q}$.

Exercice 17. Soit $P = a_n X^n + \cdots a_1 X + a_0$ un polynôme à coefficients entiers. Soient p et q deux entiers. A quelles conditions p/q est racine de P ?

Exercice 18. [Retour d'oraux] Comment montrer directement que pour tout nombre premier p, Φ_p est irréductible sur $\mathbb{Q}$?

4 Corps de rupture, corps de décomposition

Exercice 19. Donner l'exemple d'un polynôme dont le corps de rupture n'est pas le corps de décomposition.

Exercice 20. Soit $P \in k[X]$ un polynôme de degré $n \geqslant 1$ et K un corps de décomposition de P. Montrer que $[K : k] \leqslant n!$.

Exercice 21. Calculer les corps de rupture (si le polynôme n'est pas irréductible, on prend un corps de rupture d'un de ses facteurs irréductibles) et les corps de décomposition des polynômes suivants sur $\mathbf{Q}$, et donner leurs degrés :

1. $\mathrm{X}^2 + 7$
2. $\mathrm{X}^3 - 2$
3. $\mathrm{X}^3 - 11$
4. $\mathrm{X}^4 + 1$
5. $\mathrm{X}^4 - 1$
6. $\mathrm{X}^4 + 2$
7. $\mathrm{X}^4 - 2$
8. $\mathrm{X}^4 + \mathrm{X}^2 + 1$
9. $\mathrm{X}^4 - 5\mathrm{X}^2 + 6$
10. $\mathrm{X}^p - 1$, où p est un nombre premier.

Exercice 22. [Vrai ou Faux]

Dire si les assertions suivantes sont vraies ou fausses, et justifier la réponse par un contre exemple ou une démonstration.

1. Deux corps de rupture d'un polynôme P sont isomorphes.
2. Deux corps de rupture d'un polynôme irréductible sont isomorphes à un unique isomorphisme de corps près.
3. Deux corps de décomposition d'un polynôme sont isomorphes.
4. Deux corps de décomposition d'un polynôme sont isomorphes à un unique isomorphisme près.
5. Le corps de rupture d'un polynôme irréductible est isomorphe à son corps de décomposition.
6. Il existe une fonction f telle que le degré de l'extension du corps de décomposition de tout polynôme P soit majoré par $f(\deg(\mathrm{P}))$.

5 Théorème de l'élément primitif

Exercice 23. [Retour d'oraux]

1. Quel est le degré de l'extension $[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}]$.
2. Pouvez-vous trouver un élément α primitif de cette extension ?

Exercice 24. [Retour d'oraux] Trouver un élément primitive de $\mathbf{Q}(\sqrt{3}, \sqrt{7})$.

Exercice 25. [Ortiz, III.7] Soient k un corps de caractéristique $p > 0$, $K = k(U, T)$ le corps des fractions rationnelles en deux indéterminées et $K_0 = k\left(U^p, T^p\right)$.

1. Montrer que $[K : K_0] = p^2$.
2. Montrer que si $x \in K$ alors $x^p \in K_0$.
3. En déduire que K n'est pas une extension monogène de K_0.