Université de Bordeaux

Master Agrégation
Révisions : extensions de corps

Exercice 1. Soient L/K une extension et $\alpha \in L$. Montrer que les conditions suivantes sont équivalentes :

(i) α est algébrique sur K ;
(ii) $K[\alpha]$ est un corps ;
(iii) $K(\alpha)$ est un K-espace vectoriel de dimension finie ;
(iv) il existe une sous-extension finie E de L/K telle que $\alpha \in E$.

Exercice 2. Montrer que le corps $\overline{\mathbf{Q}} = \{z \in \mathbf{C}\,;\, z \text{ est algébrique sur } \mathbf{Q}\}$ est dénombrable.

Exercice 3. (Liouville). Soit $\alpha \in \overline{\mathbf{Q}} \cap \mathbf{R}$ de degré $d > 1$ sur $\mathbf{Q}$. Montrer qu'il existe une constante $c(\alpha) \in \mathbf{R}_{>0}$ telle que pour tout $(p,q) \in \mathbf{Z} \times \mathbf{N}_{>0}$, on ait

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}.$$

En déduire que le nombre $\sum\limits_{n=0}^{\infty} \frac{1}{2^{n!}}$ est transcendant sur $\mathbf{Q}$.

Exercice 4. Soient L/K une extension algébrique et A un sous-anneau de L tel que $K \subset A$. Montrer que A est un corps.

Exercice 5. Montrer qu'une extension L/K est finie si et seulement si elle est algébrique et de type fini.

Exercice 6. Soient M/L et L/K deux extensions. Montrer que M/K est algébrique si et seulement si M/L et L/K sont algébriques.

Exercice 7. Soient Ω/K une extension, et L_1, L_2 deux sous-extensions. Montrer que l'extension composée L_1L_2/K est algébrique sur K si et seulement si L_1/K et L_2/K sont algébriques.

Exercice 8. Soient K un corps et $P \in K[X]$ de degré $d \in \mathbf{N}_{>0}$.
(1) Montrer que P admet un corps de décomposition sur K et que le degré de ce dernier sur K divise $d!$.
(2) Montrer que deux corps de décomposition de P sur K sont isomorphes comme extensions de K.

Exercice 9. (D'Alembert-Gauss). Le but de l'exercice est de prouver que le corps $\mathbf{C}$ est algébriquement clos. Soit $P \in \mathbf{C}[X]$ de degré $d > 0$: on veut montrer que P a une racine dans $\mathbf{C}$.
(1) Traiter le cas $d = 2$.
(2) Montrer qu'il suffit de traiter le cas où P est unitaire à coefficients réels, ce qu'on suppose désormais.
(3) Écrivons $d = 2^n m$ avec $n \in \mathbf{N}$ et $m \in \mathbf{N}_{>0}$ impair. On procède par récurrence sur n.

(a) Traiter le cas où $n = 0$.

(b) Supposons $n > 0$. Soient K un corps de décomposition de P sur $\mathbf{C}$, $x_1, \ldots, x_d \in K$ les racines de P et $c \in \mathbf{R}$. Pour $1 \leqslant i \leqslant j \leqslant d$, posons $y_{i,j} = x_i + x_j + cx_ix_j \in K$. Posons enfin

$$Q(X) = \prod_{1 \leqslant i \leqslant j \leqslant d} (X - y_{i,j}) \in K[X].$$

Montrer que $Q \in \mathbf{R}[X]$.

(c) En déduire qu'il existe $1 \leqslant i, j \leqslant n$ tels que $y_{i,j} \in \mathbf{C}$.

(d) Conclure en faisant varier c.

Exercice 10. Soient K un corps, L/K une extension de degré m et $P \in K[X]$ irréductible de degré d.
(1) On suppose m et d premiers entre eux. Montrer que P est irréductible dans $L[X]$ (on pourra considérer une extension de L engendrée par une racine de P).
(2) Que se passe-t-il si m et d ne sont pas premiers entre eux ?
(3) Prouver que le polynôme $X^{12} + 30X^8 + 36X + 24$ est irréductible sur $\mathbf{Q}\left(\sqrt[5]{7}\right)$.

Exercice 11. Soient L/K une extension et $\alpha \in L$ algébrique sur K tel que $\deg_K(\alpha)$ soit impair. Montrer que $K(\alpha) = K(\alpha^2)$.

Exercice 12. (1) Montrer que $\mathbf{Q}(\sqrt{5}, \sqrt{7}) = \mathbf{Q}(\sqrt{5} + \sqrt{7})$.
(2) Quel est le polynôme minimal de $\sqrt{5} + \sqrt{7}$ sur $\mathbf{Q}$?

Exercice 13. Posons $\alpha = \sqrt{1 + \sqrt{3}} \in \mathbf{R}$.
(1) Trouver le polynôme minimal P de α sur $\mathbf{Q}$.
(2) Démontrer que $K = \mathbf{Q}(\alpha, i\sqrt{2})$ est une extension de décomposition de $P \in \mathbf{Q}[X]$.
(3) Calculer le degré de K sur $\mathbf{Q}$.

Exercice 14. Posons $K = \mathbf{Q}(\sqrt{2}, \sqrt[3]{7}) \subset \mathbf{R}$.
(1) Que vaut $[K : \mathbf{Q}]$?
(2) Donner une base de K vu comme $\mathbf{Q}$-espace vectoriel.
(3) En déduire que le polynôme minimal de $\alpha := \sqrt{2} + \sqrt[3]{7}$ sur $\mathbf{Q}$ n'est pas de degré 2 ou 3.
(4) En déduire que $K = \mathbf{Q}(\alpha)$ et calculer le polynôme minimal de α sur $\mathbf{Q}$.

Exercice 15. Soient $P \in \mathbf{Q}[X]$ irréductible unitaire de degré d et $K \subset \mathbf{C}$ une extension de $\mathbf{Q}$ contenant une racine α de P. Supposons que K ne contient pas de racine cubique de α.
(1) Montrer que le polynôme $X^3 - \alpha$ est irréductible sur $\mathbf{Q}(\alpha)$.
(2) Soit $\beta \in \mathbf{C}$ une racine cubique de α. Calculer $[\mathbf{Q}(\beta) : \mathbf{Q}]$ en fonction de d, et en déduire que $P(X^3)$ est irréductible sur $\mathbf{Q}$.

Exercice 16. Soit K un corps, $a \in K$, et p un nombre premier. Montrer que le polynôme $X^p - a$ est irréductible dans $K[X]$ si et seulement s'il n'a pas de racine dans K.

Exercice 17. On pose $K = \mathbf{R}(Y)$ et $P(X, Y) = X^4 + X^2 + Y^6$. Soit L une extension de décomposition de $P \in K[X]$.
(1) On choisit une racine f de P dans L. Prouver que $L = K(f)$.
(2) Démontrer que P est irréductible dans $\mathbf{R}[X, Y]$. Quel est le degré de L sur K ?

Exercice 18. Soient K un corps, L une extension algébrique de K et $\sigma\colon L \to L$ un K-morphisme.
(1) Soient $y \in L$ et P le polynôme minimal de y sur K. Notons R l'ensemble des racines de P dans L. Montrer que $\sigma(R) = R$.
(2) En déduire que σ est bijective.

Exercice 19. Soit p un nombre premier. On pose $Q(X) = X^6 + p^2$, on choisit une racine complexe α de Q et on pose $K = \mathbf{Q}(\alpha)$.
(1) Prouver que $i \in K$.
(2) Démontrer que K contient une racine du polynôme $X^3 - p$.
(3) En déduire le degré de K sur $\mathbf{Q}$. Le polynôme $\mathbf{Q}$ est-il irréductible dans $\mathbf{Q}[X]$?

Exercice 20. Soit K un corps fini de cardinal q. Montrer que $\prod_{\alpha \in K} (X - \alpha) = X^q - X$ dans $K[X]$.

Exercice 21. Soit G un groupe abélien (noté multiplicativement).
(1) Soient $x \in G$ d'ordre n et $y \in G$ d'ordre m avec $\mathsf{pgcd}(n, m) = 1$. Montrer que xy est d'ordre nm.
(2) Supposons G fini, et notons d le ppcm des ordres des éléments de G (on appelle d *l'exposant* de G). Montrer que G contient un élément d'ordre d.
(3) Soit F un corps. Montrer que tout sous-groupe fini de $F^\times$ est cyclique.

Exercice 22. On pose $K = \mathbf{F}_2[Y]/\langle Y^4 + Y + 1\rangle$ et on note α la classe de Y dans K. Posons $\beta = \alpha^2 + \alpha$.
(1) Montrer que K est un corps.
(2) Trouver le polynôme minimal de β sur $\mathbf{F}_2$. Quel est le cardinal de $\mathbf{F}_2(\beta)$?
(3) Factoriser $X^3 + 1$ dans $K[X]$.
(4) Quel est le polynôme minimal de α sur $\mathbf{F}_2(\beta)$?

Exercice 23. On pose $A = \mathbf{F}_3[Y]/\langle Y^4 + Y - 1\rangle$ et on note α la classe de Y dans A.
(1) Calculer α^{16} et α^{40}.
(2) En déduire que A est un corps.
(3) Trouver le polynôme minimal de $\alpha + 1$ sur $\mathbf{F}_3$.
(4) Quel est le degré de α^{10} sur $\mathbf{F}_3$?

Exercice 24. Soient p un nombre premier et X, Y deux indéterminées. On pose

$$K = \mathbf{F}_p(X^p, Y^p) \subset L = \mathbf{F}_p(X, Y).$$

(1) Montrer que $[L : K] = p^2$.
(2) Montrer que L/K n'est pas monogène.
(3) Exhiber une infinité de sous-extensions de L/K.