Extensions de corps I

Exercice 1. Charles Hermite a démontré en 1873 que e est un nombre transcendant sur $\mathbf{Q}$; en 1882, Ferdinand von Lindemann a démontré la même chose pour π. En admettant ces résultats, montrer que $e+\pi$ et $e\pi$ ne peuvent pas être simultanément algébriques sur $\mathbf{Q}$.

Exercice 2. (Les corps finis comme corps de décomposition) Soit $p > 0$ un nombre premier.

1. Soit $\mathrm{L}/\mathbf{F}_p$ une extension finie, avec $|\mathrm{L}| = q$. Montrer que L est un corps de décomposition de $\mathrm{X}^q - \mathrm{X} \in \mathbf{F}_p[\mathrm{X}]$ sur $\mathbf{F}_p$.
2. Montrer, réciproquement, que si $q = p^d$ avec $d \in \mathbf{N}^*$, alors tout corps de décomposition de $\mathrm{X}^q - \mathrm{X} \in \mathbf{F}_p[\mathrm{X}]$ sur $\mathbf{F}_p$ est fini de cardinal q.

Exercice 3. (Corps de rupture et corps de décomposition)

1. Montrer que $\mathrm{P}(\mathrm{X}) = \mathrm{X}^3 - 2 \in \mathbf{Q}[\mathrm{X}]$ est irréductible. Montrer que $\mathbf{Q}(\sqrt[3]{2})$ est un corps de rupture de P sur $\mathbf{Q}$. Montrer qu'il n'est pas un corps de décomposition de P sur $\mathbf{Q}$. Montrer que $\mathbf{Q}(\sqrt[3]{2}, \zeta_3)$ est un corps de décomposition de P sur $\mathbf{Q}$.
2. Soit $n > 1$ et $\Phi_n(\mathrm{X}) \in \mathbf{Z}[\mathrm{X}]$ le n-ième polynôme cyclotomique. Trouver un corps de rupture de Φ_n sur $\mathbf{Q}$ et montrer que c'est également un corps de décomposition.

Exercice 4. (Extensions biquadratiques)

1. Soit K un corps de caractéristique différente de 2. Soit L/K une extension de degré 2.
   (a) Soit $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ un polynôme unitaire de degré 2. Démontrer qu'il existe $a, b \in \mathrm{K}$ tels que $\mathrm{P} = (\mathrm{X} - a)^2 - b$.
   (b) Démontrer qu'il existe un élément non nul α de L tel que $\alpha^2 \in \mathrm{K}$ et $\mathrm{L} = \mathrm{K}(\alpha)$.
   (c) On conserve les notations de la question (b). Soit $\beta \in \mathrm{L}$ tel que $\mathrm{L} = \mathrm{K}(\beta)$ et $\beta^2 \in \mathrm{K}$. Démontrer que $\beta/\alpha \in \mathrm{K}$.
2. Soient p et q deux nombres premiers distincts.
   (a) Déterminer le degré de l'extension $\mathbf{Q}(\sqrt{p}, \sqrt{q})/\mathbf{Q}$.
   (b) Soit $\beta \in \mathbf{Q}(\sqrt{p}, \sqrt{q})$ tel que $\beta^2 \in \mathbf{Q}$. Démontrer qu'un des éléments β, $\beta/\sqrt{p}$, $\beta/\sqrt{q}$, $\beta/\sqrt{pq}$ appartient à $\mathbf{Q}$. (On pourra discuter suivant que β appartient à $\mathbf{Q}(\sqrt{p})$ ou pas).
   (c) Donner la liste des sous-extensions de $\mathbf{Q}(\sqrt{p}, \sqrt{q})/\mathbf{Q}$.
   (d) Calculer $(\sqrt{p} + \sqrt{q})^2$. Déterminer le polynôme minimal de $\sqrt{p} + \sqrt{q}$ sur $\mathbf{Q}$.

Exercice 5. Soit k un corps, $\mathrm{P} \in k[\mathrm{X}]$ irréductible de degré $n \geq 2$ et K une extension de k de degré m, avec $\operatorname{pgcd}(m, n) = 1$. Montrer que P est encore irréductible dans $\mathrm{K}[\mathrm{X}]$.

Exercice 6. Le but de cet exercice est de montrer que si L/K est une extension de corps séparable et finie, alors il existe un élément $\theta \in \mathrm{L}$ tel que $\mathrm{L} = \mathrm{K}(\theta)$.

1. Démontrer l'assertion quand K est un corps fini.

2. Soit F un corps infini, L/F une extension de la forme $\mathrm{L} = \mathrm{F}(\alpha, \beta)$ avec β separable sur F, $\overline{\mathrm{L}}$ une clôture algébrique de L, $m_{\alpha,\mathrm{F}}$, $m_{\beta,\mathrm{F}} \in \mathrm{K}[\mathrm{X}]$ les polynômes minimaux de α et β. On pose

$$\mathrm{S} = \left\{ \frac{\alpha' - \alpha}{\beta - \beta'} \,\middle|\, \alpha' \text{ est racine de } m_{\alpha,\mathrm{F}} \text{ et } \beta' \text{ est une racine de } m_{\beta,\mathrm{F}} \text{ différente de } \beta \right\}.$$

Montrer que si $\lambda \in \mathrm{F} \setminus \mathrm{S}$, alors $\mathrm{K}(\alpha, \beta) = \mathrm{K}(\alpha + \lambda\beta)$.

3. En déduire que si K un corps infini et si L/K est une extension séparable et finie, alors il existe un élément $\theta \in \mathrm{L}$ tel que $\mathrm{L} = \mathrm{K}(\theta)$.

4. En déduire que si K est parfait et que L/K est une extension finie, alors il existe un élément $\theta \in \mathrm{L}$ tel que $\mathrm{L} = \mathrm{K}(\theta)$.

5. On pose $\mathrm{K} = \mathbf{F}_p(\mathrm{T}, \mathrm{U})$ et $\mathrm{L} = \mathrm{K}(\sqrt[p]{\mathrm{T}}, \sqrt[p]{\mathrm{U}})$ le corps obtenu en adjoignant une racine p-ième à T et U. Définir précisément L et montrer que L/K est une extension finie dont on précisera le degré. Montrer que tout élément $\alpha \in \mathrm{L}$ vérifie $\alpha^p \in \mathrm{K}$ et en déduire qu'il n'existe pas de $\alpha \in \mathrm{L}$ tel que $\mathrm{L} = \mathrm{K}(\alpha)$.

Exercice 7. (Un critère d'irréductibilité sur les corps finis) Soit K un corps fini ; on note q son cardinal et on en fixe une clôture algébrique $\overline{\mathrm{K}}$.
On rappelle que pour n un entier supérieur ou égal à 1,

– l'ensemble des racines dans $\overline{\mathrm{K}}$ du polynôme $\mathrm{X}^{q^n} - \mathrm{X}$ est l'unique sous-corps de cardinal q^n de $\overline{\mathrm{K}}$; on le note ici K_n.
– tout corps de cardinal q^n contenant K est isomorphe à K_n, comme corps et comme K-algèbre.

Soit P un polynôme à coefficients dans K, de degré d ; montrer que P est irréductible dans K si et seulement s'il vérifie les deux conditions suivantes :

(i) P divise $\mathrm{X}^{q^d} - \mathrm{X}$;

(ii) pour tout nombre premier p divisant d, P et $\mathrm{X}^{q^{d/p}} - \mathrm{X}$ sont premiers entre eux.

Exercice 8. (Indépendance linéaire des caractères)

1. Soit G un monoïde, M un corps, et $\chi_1, \ldots, \chi_n$ des caractères distincts [1] de G dans M. Montrer que si $c_1, \ldots, c_n \in \mathrm{M}$ sont tels que

$$c_1\chi_1(g) + \cdots + c_n\chi_n(g) = 0$$

pour tout $g \in \mathrm{G}$, alors $c_1 = \cdots = c_n = 0$.

2. En déduire que si L/K et M/K sont des extensions, alors tout ensemble fini de plongements de L dans M est linéairement indépendant.

3. Soit M un corps et $\alpha_1, \ldots, \alpha_n \in \mathrm{M}^\times$. Montrer que s'il existe $c_1, \ldots, c_n \in \mathrm{M}$ tels que

$$\forall k \in \mathbf{N}, c_1\alpha_1^k + \cdots + c_n\alpha_n^k = 0,$$

alors $c_1 = \cdots = c_n = 0$.

1. Un *caractère* de G dans M est une application $\chi : \mathrm{G} \to \mathrm{M}^\times$ telle que $\chi(gg') = \chi(g)\chi(g')$ pour tous $g, g' \in \mathrm{G}$ et $\chi(1_\mathrm{G}) = 1_\mathrm{K}$.