TD3 : Extensions de corps

Exercice 1. Soit $a \in \mathbb{C}$ algébrique sur $\mathbb{Q}$ et P le polynôme minimal de a sur $\mathbb{Q}$.
On suppose que a est racine d'un polynôme unitaire de $\mathbb{Z}[X]$ (autrement dit, a est un entier algébrique).
Montrer que $P \in \mathbb{Z}[X]$.

Exercice 2. Soient k un corps et $f, g \in k[X, Y]$ deux polynômes premiers entre eux. On note

$$\mathcal{C}_f = \{(x, y) \in k^2 : f(x, y) = 0\} \quad \text{et} \quad \mathcal{C}_g = \{(x, y) \in k^2 : g(x, y) = 0\},$$

de sorte que $\mathcal{C}_f$ et $\mathcal{C}_g$ sont deux courbes de k^2. On va montrer que l'intersection de ces deux courbes est un ensemble de cardinalité finie.

1. Soit $P \in k[X, Y] \simeq k[X][Y] \subset k(X)[Y]$. Expliquer comment déduire de la décomposition en produits d'irréductibles de P dans $k[X][Y]$ celle dans $k(X)[Y]$.
2. Montrer que f et g vus comme éléments de $k(X)[Y]$ sont premiers entre eux.
3. Montrer que l'ensemble A des abscisses des points de $\mathcal{C}_f \cap \mathcal{C}_g$ est de cardinalité finie.
4. En déduire que $\mathcal{C}_f \cap \mathcal{C}_g$ est un ensemble fini.

Exercice 3. Soient $P = X^3 + 2X + 2$ et a une racine de P dans $\mathbb{C}$.

1. Montrer que P est irréductible sur $\mathbb{Q}[X]$. Que vaut $[\mathbb{Q}(a) : \mathbb{Q}]$?
2. Exprimer $u = a^{-1}$, $v = a^6 + a^4 + 3a^3 - a^2 + 3$ et $w = (a^2 + a + 1)^{-1}$ en fonction de $1, a$ et a^2.
3. Quel est le polynôme minimal de v sur $\mathbb{Q}$?

Exercice 4.

1. Montrer que i et j sont algébriques sur $\mathbb{Q}$ et déterminer $[\mathbb{Q}(i) : \mathbb{Q}]$, $[\mathbb{Q}(j) : \mathbb{Q}]$.
2. Calculer $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}]$, $[\mathbb{Q}(\sqrt{3}, j) : \mathbb{Q}]$ et $[\mathbb{Q}(\sqrt{3}, i, j) : \mathbb{Q}]$.
3. Comparer $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}]$ et $[\mathbb{Q}(\sqrt{3} + i) : \mathbb{Q}]$.
4. Déterminer le polynôme minimal de $\sqrt{3} + i$ sur $\mathbb{Q}$.

Exercice 5.

1. Déterminer $[\mathbb{Q}(\sqrt{3}, \sqrt{7}) : \mathbb{Q}]$. Donner une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\sqrt{3}, \sqrt{7})$.
2. Comparer $[\mathbb{Q}(\sqrt{3}, \sqrt{7}) : \mathbb{Q}]$ et $[\mathbb{Q}(\sqrt{3} + \sqrt{7}) : \mathbb{Q}]$.
3. Déterminer le polynôme minimal de $\sqrt{3} + \sqrt{7}$ sur $\mathbb{Q}$.
4. Quelles sont les racines de $\mathrm{Irr}(\sqrt{3} + \sqrt{7}, \mathbb{Q})$ dans $\mathbb{C}$?

Exercice 6.

1. Les éléments de $\mathbb{Q}(\sqrt{2})$ ont-ils tous le même polynôme minimal sur $\mathbb{Q}$?

2. Deux extensions de corps de même degré sont-elles nécessairement isomorphes ?
3. Soient a et b deux entiers non nuls. Donner une condition nécessaire et suffisante pour que $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ (avec par convention $\sqrt{n} = i\sqrt{-n}$ si $n < 0$).

Exercice 7.

1. Déterminer $[\mathbb{Q}(\sqrt[3]{3}, \sqrt{5}) : \mathbb{Q}]$. Donner une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\sqrt[3]{3}, \sqrt{5})$.
2. Comparer $[\mathbb{Q}(\sqrt[3]{3}, \sqrt{5}) : \mathbb{Q}]$ et $[\mathbb{Q}(\sqrt[3]{3} + \sqrt{5} : \mathbb{Q}]$.
3. Déterminer le polynôme minimal de $\sqrt[3]{3} + \sqrt{5}$ sur $\mathbb{Q}$.
4. Quelles sont les racines de $\mathrm{Irr}(\sqrt[3]{3} + \sqrt{5}, \mathbb{Q})$ dans $\mathbb{C}$?

Exercice 8. Soient $L \supset K \supset k$ une tour d'extension de corps et $a \in L$.
Montrer que si K est une extension algébrique de k et a est algébrique sur K, alors a est algébrique sur k.

Exercice 9. Soit α un élément algébrique sur un corps K.

1. Quels sont les degrés possibles de l'extension $K(\alpha) \supset K(\alpha^2)$?
2. Montrer que si $[K(\alpha) : K]$ est impair, alors $K(\alpha^2) = K(\alpha)$. La réciproque est-elle vraie ?

Exercice 10. Soient k un corps et $F \in k(X) \setminus k$; on pose $F = \frac{A}{B}$ avec $A, B \in k[X]$ premiers entre eux. On s'intéresse à $k(F)$, le sous-corps de $k(X)$ engendré par F.

1. Soit $P(X,T) = B(T)F(X) - A(T) \in k[X,T]$. Montrer que P définit un élément non nul de $k(F)[T]$, dont une racine est X.
2. En déduire que X est algébrique sur $k(F)$, et donc que F est transcendant sur k.
3. Montrer que $B(T)U - A(T)$ est un polynôme irréductible de $k[T,U]$, puis que c'est un polynôme irréductible de $k(U)[T]$.
4. En déduire que P est le polynôme minimal de X sur $k(F)$. Quel est le degré de l'extension $k(X) \supset k(F)$?

Exercice 11. Soient K, M deux corps et $\phi : K \to M$ un morphisme de corps.

1. Rappeler pourquoi ϕ est injective.
2. Montrer qu'il existe un surcorps $L \supset K$ ainsi qu'un morphisme de corps $\psi : L \to M$ tel que :
   — ψ est bijective
   — $\psi_{|K} = \phi$.

Exercice 12. Soit K un corps et $L = K(\alpha)$ une extension de K de degré fini engendrée par un élément α. Le but de cet exercice est de montrer que L ne contient qu'un nombre fini de sous-corps F tels que $K \subset F$.

1. Soit F un sous-corps de L qui contient K et A l'ensemble des coefficients du polynôme minimal $\mathrm{Irr}(\alpha, F)$ de α sur F.
   Montrer que $\mathrm{Irr}(\alpha, K(A)) = \mathrm{Irr}(\alpha, F)$ et en déduire que $K(A) = F$.
2. Montrer que $\mathrm{Irr}(\alpha, F) | \mathrm{Irr}(\alpha, K)$ dans $F[X]$.
3. En déduire une application injective de l'ensemble des sous-corps de L qui contiennent K dans l'ensemble des polynômes unitaires de $L[X]$ qui divisent $\mathrm{Irr}(\alpha, K)$ dans $L[X]$.
4. Montrer que $\mathrm{Irr}(\alpha, K)$ n'admet qu'un nombre fini de diviseurs unitaires dans $L[X]$. Conclure.

5. Application : on prend $K = \mathbb{Q}$ et $L = \mathbb{Q}(i, \sqrt{2})$.
   (a) Montrer que $L = \mathbb{Q}(i + \sqrt{2})$. Calculer $[L : \mathbb{Q}]$.
   (b) Quelles sont les racines de $\mathrm{Irr}(i + \sqrt{2}, \mathbb{Q})$ dans L ?
   (c) Établir la liste des sous-corps de L.

Exercice 13. (Dénombrabilité de $\bar{\mathbb{Q}}$)

1. On rappelle que $\bar{\mathbb{Q}}$ désigne l'ensemble des nombres complexes algébriques sur $\mathbb{Q}$.
   Démontrer que $\bar{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$.
2. Pour tout $n \in \mathbb{N}$, on note $\mathbb{Q}_n[X]$ l'espace vectoriel des polynômes de $\mathbb{Q}[X]$ de degré inférieur ou égal à n.
   Montrer que $\mathbb{Q}_n[X]$ est dénombrable.
3. Montrer que $\mathbb{Q}[X]$ est dénombrable. En déduire que $\bar{\mathbb{Q}}$ est dénombrable.
4. Montrer que $\mathbb{C}$ contient une infinité non dénombrable d'éléments transcendants sur $\mathbb{Q}$.

Exercice 14. (Théorème de l'élément primitif)
Soit K un corps de caractéristique 0 et L une extension finie de K, engendrée par deux élements α et β. On veut prouver qu'il existe un élement $\theta \in L$ tel que $L = K(\theta)$ (on dit que θ est un élément primitif de l'extension).

1. Soient $P_\alpha = \mathrm{Irr}(\alpha, K)$ et $P_\beta = \mathrm{Irr}(\beta, K)$. On considère une extension M de L dans laquelle P_α et P_β sont scindés, par exemple une clôture algébrique de L. On note $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_m$ les racines de P_α dans M, et $\beta_1 = \beta, \beta_2, \dots, \beta_n$ celles de P_β.
   (a) Justifier que K est de cardinalité infinie. En déduire qu'il existe $\lambda \in K$ tel que $\lambda \neq \frac{\alpha - \alpha_i}{\beta - \beta_j}$ pour tout (i, j) avec $1 \leq i \leq m$ et $1 < j \leq n$.
   (b) On pose $\theta = \alpha - \lambda\beta \in L$ et $Q = \mathrm{Irr}(\beta, K(\theta))$.
   Montrer que $P_\alpha(\theta + \lambda X)$ est un polynôme non nul de $K(\theta)[X]$ dont β est racine. En déduire que $Q | P_\alpha(\theta + \lambda X)$ et $Q | P_\beta$ dans $K(\theta)[X]$.
   (c) Montrer que $P_\alpha(\theta + \lambda X)$ et P_β sont scindés à racines simples dans $M[X]$, et que β est leur seule racine commune.
   (d) En déduire que $Q = X - \beta$, puis que $L = K(\theta)$.
2. Généralisation : soit L une extension finie d'un corps K de caractéristique 0. Montrer qu'il existe $\theta \in L$ tel que $L = K(\theta)$.
3. Déterminer un élément primitif des extensions suivantes de $\mathbb{Q}$:
   (a) $\mathbb{Q}(j, \sqrt[3]{2})$
   (b) $\mathbb{Q}(e^{2i\pi/n}, e^{2i\pi/m})$ avec $(m, n) \in (\mathbb{N}^*)^2$
   (c) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, \sqrt[5]{5})$.

Exercice 15.

1. Montrer que l'identité est le seul automorphisme de corps de $\mathbb{Q}$.
   Même question avec $\mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z}, +, \times)$ où p est un nombre premier.
2. (a) Soit L un corps de caractéristique 0. Montrer que L contient un sous-corps k isomorphe à $\mathbb{Q}$, et que tout automorphisme de corps de L induit l'identité sur k.

(b) Soit L un corps de caractéristique p où p est un nombre premier. Montrer que L contient un sous-corps k isomorphe à $\mathbb{F}_p$, et que tout automorphisme de corps de L induit l'identité sur k.

3. Automorphismes de $\mathbb{R}$.
   (a) Soit ϕ un automorphisme de corps de $\mathbb{R}$. Montrer que $\phi(\mathbb{R}^+) \subset \mathbb{R}^+$.
   (b) En déduire que ϕ est croissant (en tant qu'application $\mathbb{R} \to \mathbb{R}$), puis que ϕ est l'identité.
4. Automorphismes continus de $\mathbb{C}$.
   (a) Soit ϕ un automorphisme de corps **continu** de $\mathbb{C}$. Montrer que $\phi(x) = x$ pour tout $x \in \mathbb{R}$.
   (b) En déduire que ϕ est soit l'identité, soit la conjugaison complexe.
5. K-automorphismes de $K(X)$.
   (a) Montrer que tout K-automorphisme de $K(X)$ est de la forme $f \mapsto f(\frac{aX+b}{cX+d})$.
   Indication : utiliser l'exercice 10.
   (b) En déduire que le groupe des K-automorphismes de $K(X)$ est isomorphe à $PGL(2, K)$.

Exercice 16.

1. Montrer que le polynôme $P = X^3 - 2$ est irréductible dans $\mathbb{Q}[X]$.
   Justifier que $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de P, mais pas un corps de décomposition.
2. Soit $L = \mathbb{Q}(\sqrt[3]{2}, j)$. Montrer que L est le corps des racines de P.
3. Déterminer $[L : \mathbb{Q}]$.
4. (a) Quels sont les automorphismes du corps $\mathbb{Q}(j)$?
   (b) Quels sont les automorphismes du corps $\mathbb{Q}(\sqrt[3]{2})$?
5. (a) Montrer que pour tout $(k, l) \in \{1, 2\} \times \{0, 1, 2\}$, il existe un automorphisme $\phi_{k,l}$ de L tel que $\phi_{k,l}(\sqrt[3]{2}) = j^l \sqrt[3]{2}$ et $\phi_{k,l}(j) = j^k$.
   (b) Les automorphismes $\phi_{k,l}$ sont-ils les seuls automorphismes de corps de L ?
6. (a) Pour $(k, l) \in \{1, 2\} \times \{0, 1, 2\}$, montrer que $\phi_{k,l}(\sqrt[3]{2} + j)$ est une racine de $\mathrm{Irr}(\sqrt[3]{2} + j, \mathbb{Q})$.
   (b) Déterminer le degré de $\mathrm{Irr}(\sqrt[3]{2} + j, \mathbb{Q})$.

Exercice 17. (Suite de l'exercice 5.)

1. (a) Montrer qu'il existe un automorphisme du corps $\mathbb{Q}(\sqrt{3})$ qui envoie $\sqrt{3}$ sur $-\sqrt{3}$.
   (b) Existe-t-il d'autres automorphismes du corps $\mathbb{Q}(\sqrt{3})$ distincts de l'identité ?
2. On note $L = \mathbb{Q}(\sqrt{3}, \sqrt{7})$.
   (a) Montrer qu'il existe des automorphismes Φ_3 et Φ_7 du corps L qui vérifient $\Phi_3(\sqrt{3}) = -\sqrt{3}$ et $\Phi_3(\sqrt{7}) = \sqrt{7}$ d'une part et $\Phi_7(\sqrt{3}) = \sqrt{3}$ et $\Phi_7(\sqrt{7}) = -\sqrt{7}$ d'autre part.
   (b) Montrer qu'il existe un automorphisme $\Phi_{3,7}$ du corps L qui vérifie $\Phi_{3,7}(\sqrt{3}) = -\sqrt{3}$ et $\Phi_{3,7}(\sqrt{7}) = -\sqrt{7}$.
   (c) Les automorphismes Φ_3, Φ_7 et $\Phi_{3,7}$ sont-ils les seuls automorphismes du corps L distincts de l'identité ?

Exercice 18. Soient p un entier premier et $P = X^p - X - 1$ un polynôme de $\mathbb{Z}[X]$.

1. Soient $\bar{P}$ la classe d'équivalence de P dans $\mathbb{F}_p[X]$ et L un corps de rupture de $\bar{P}$ avec a une racine de $\bar{P}$ dans L.
   Montrer que l'ensemble des racines de $\bar{P}$ dans L est $\{a + i \bmod p : 0 \le i \le p - 1\}$.
2. En déduire que $\bar{P}$ est irréductible sur $\mathbb{F}_p[X]$ et donc sur $\mathbb{Z}[X]$ et sur $\mathbb{Q}[X]$.