Extensions

Exercice 1. (Critère d'Eisenstein)
Le but de cet exercice est de prouver le critère d'irréductibilité suivant : si $\mathrm{P}(\mathrm{X}) = a_n\mathrm{X}^n + \cdots + a_1\mathrm{X} + a_0$ est un polynôme à coefficients dans A factoriel, tel qu'il existe p un élément irréductible de A qui divise tous les coefficients de P sauf a_n et tel que p^2 ne divise pas a_0 alors P est irréductible dans K[X] où K est le corps des fractions de A.

1. Montrer que l'on peut se ramener au cas où les coefficients de P sont premiers entre eux dans leur ensemble.
2. On raisonne par l'absurde et on suppose que $\mathrm{P} = \mathrm{RS}$ dans K[X] avec R et S non constants. Montrer que l'on peut se ramener au cas où R et S sont à coefficients dans A.
3. Conclure.
4. Montrer que si $p \in \mathbf{N}$ est premier et divise $a \in \mathbf{Z}$ mais que p^2 ne divise pas a alors $\mathrm{X}^n + a$ est irréductible dans $\mathbf{Q}[\mathrm{X}]$.
5. Montrer que $\mathrm{X}^{p-1} + \cdots + \mathrm{X} + 1$ est irréductible dans $\mathbf{Q}[\mathrm{X}]$.

Exercice 2. (Échauffement)

1. Soit L/K une extension de degré n. Que dire si $n = 1$? Que dire d'une sous-extension L'/K de degré n (c'est-à-dire d'un corps L' tel que $\mathrm{K} \subset \mathrm{L}' \subset \mathrm{L}$ et $[\mathrm{L}' : \mathrm{K}] = n$) ?
2. Soit L/K une extension. Soit $a \in \mathrm{L}$ algébrique sur K, de degré n et de polynôme minimal $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$. Soit également $b \in \mathrm{L}$ algébrique sur K de degré m. On suppose que m et n sont premiers entre eux. Quel est le degré de $\mathrm{K}[a, b]/\mathrm{K}$? Montrer que P est irréductible sur $\mathrm{K}[b]$. Que vaut $\mathrm{K}[a] \cap \mathrm{K}[b]$?
3. Soit L/K une extension et $x \in \mathrm{L}$ algébrique sur K, de degré impair. Montrer que x^2 est également algébrique sur K et que $\mathrm{K}[x^2] = \mathrm{K}[x]$.
4. Montrer que $\mathbf{Q}$ possède des extensions de tout degré.
5. Déterminer les extensions finies de $\mathbf{C}$.
6. Montrer que le corps $\overline{\mathbf{Q}}$ est dénombrable.

Exercice 3. Donner les degrés des extensions suivantes et en donner des bases.

(a) $\mathbf{Q}[\sqrt{2}]/\mathbf{Q}$, $\mathbf{Q}[\sqrt[3]{2}]/\mathbf{Q}$, $\mathbf{Q}[\sqrt{2}, \sqrt[3]{2}]/\mathbf{Q}$, $\mathbf{Q}[\sqrt{2}, \sqrt[3]{2}]/\mathbf{Q}[\sqrt{2}]$ et $\mathbf{Q}[\sqrt{2}, \sqrt[3]{2}]/\mathbf{Q}[\sqrt[3]{2}]$.

(b) $\mathbf{Q}[\sqrt{2}, \sqrt{3}]/\mathbf{Q}$, $\mathbf{Q}[\sqrt{2}, \sqrt{3}]/\mathbf{Q}[\sqrt{2}]$ et $\mathbf{Q}[\sqrt{2}, \sqrt{3}]/\mathbf{Q}[\sqrt{3}]$. Comparer $\mathbf{Q}[\sqrt{2}+\sqrt{3}]$ à $\mathbf{Q}[\sqrt{2}, \sqrt{3}]$ et donner le polynôme minimal de $\sqrt{2} + \sqrt{3}$ sur $\mathbf{Q}$.

(c) $\mathbf{Q}[j]/\mathbf{Q}$, pour $j = e^{2i\pi/3}$. A-t-on $\sqrt{3} \in \mathbf{Q}[j]$? $i \in \mathbf{Q}[j]$? $j \in \mathbf{Q}[i]$?

(d) $\mathbf{Q}[\sqrt{3}, j]/\mathbf{Q}$, $\mathbf{Q}[\sqrt{3}, i, j]/\mathbf{Q}$, $\mathbf{Q}[\sqrt{3}, i]/\mathbf{Q}$ et $\mathbf{Q}[\sqrt{3} + i]/\mathbf{Q}$.

(e) $\mathbf{Q}\left[\cos\dfrac{2\pi}{3}\right]/\mathbf{Q}$, $\mathbf{Q}\left[\sin\dfrac{2\pi}{3}\right]/\mathbf{Q}$, $\mathbf{Q}\left[\cos\dfrac{2\pi}{5}\right]/\mathbf{Q}$ et $\mathbf{Q}\left[\sin\dfrac{2\pi}{5}\right]/\mathbf{Q}$.

Exercice 4. Soit $\mathrm{P} = \mathrm{X}^3 + 2\mathrm{X} + 2 \in \mathbf{Q}[\mathrm{X}]$ et soit $a \in \mathbf{C}$ une racine de P.

1. Montrer que P est irréductible.

2. Exprimer $\frac{1}{a}$, $\frac{1}{a^2+a+1}$ et $u = a^6 + 3a^4 + 2a^3 + 6a$ en fonction de 1, a et a^2.
3. Montrer que u est algébrique sur $\mathbf{Q}$ et déterminer son polynôme minimal.

Exercice 5.

1. Soit L/K une extension algébrique. Montrer que si $f : \mathrm{L} \to \mathrm{L}$ est un morphisme de corps K-linéaire, f est un automorphisme.
2. Soit $\mathrm{K} \subset \mathrm{K}' \subset \mathrm{K}''$ trois corps. On suppose que l'extension K'/K est algébrique. Montrer que tout élément $a \in \mathrm{K}''$ algébrique sur K' est algébrique sur K.
3. Montrer que $\overline{\mathbf{Q}}$ est algébriquement clos.
4. 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 6. Soit K un corps et $\mathrm{L} = \mathrm{K}(\mathrm{X})$.

1. L'élément $\mathrm{X} \in \mathrm{L}$ est-il algébrique sur K ?
2. Déterminer les éléments de L algébriques sur K.
3. Montrer que si $\beta \in \mathrm{L} \setminus \mathrm{K}$, L est algébrique sur $\mathrm{K}(\beta)$.

Exercice 7. Soit $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ un polynôme de degré 4. Montrer que P est irréductible si et seulement si pour toute extension L/K de degré ≤ 2, P n'a pas de racine dans L. Généraliser ce critère à un polynôme de degré n.

Exercice 8.

1. Montrer que -1 n'est pas une somme de carrés dans $\mathbf{R}$ (!)
2. Soit $\beta = e^{2i\pi/3}\sqrt[3]{2} \in \mathbf{C}$ et $\mathrm{K} = \mathbf{Q}(\beta)$. Montrer que -1 n'est pas une somme de carrés dans K.

Exercice 9. (Extensions biquadratiques)

1. Soit K un corps de caractéristique différente de 2. Soit L/K une extension de degré 2 (*extension quadratique*).
   (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 10. Soit $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$ le corps à deux éléments.

1. Déterminer tous les polynômes irréductibles de $\mathbf{F}_2[X]$ de degré inférieur ou égal à 4.
2. Utiliser un polynôme irréductible de degré 3 pour construire une extension $\mathbf{F}_8/\mathbf{F}_2$ de degré 3. Montrer, en exhibant un isomorphisme explicite, que toutes ces extensions sont isomorphes.
3. Montrer que $\mathbf{F}_8^\times$ est cyclique en en exhibant un générateur.
4. Démontrer que tous les éléments de $\mathbf{F}_8$ sont algébriques sur $\mathbf{F}_2$ et donner leur polynôme minimal.
5. Reprendre ces trois dernières questions pour une extension $\mathbf{F}_{16}/\mathbf{F}_2$ de degré 4.

Exercice 11. Montrer que le polynôme minimal de $\sqrt{3}+\sqrt{2}$ sur $\mathbf{Q}$ est réductible dans $\mathbf{F}_p[X]$ pour tout nombre premier p.