Exercices d'algèbre M1S2 (théorie de Galois)

R. Noot

Année 2008/2009

1 Degrés, polynômes minimaux

1.1 Soit K un corps.

(a) Soit A une K-algèbre (associative et unitaire) de dimension finie. Montrer que A est intègre si et seulement si A est une *algèbre à division*, c'est-à-dire que tout élément $a \neq 0 \in A$ admet un inverse bilatère.

(b) Soit $P(X) \in K[X]$ avec $P \neq 0$. Montrer que les conditions suivantes sont équivalentes.
- $P(X)$ est irréductible.
- L'anneau $K[X]/(P(X))$ est intègre.
- L'anneau $K[X]/(P(X))$ est un corps.

1.2 Soient K un corps et L une extension de K. Soit $\alpha \in L$ algébrique sur K de degré n et de polynôme minimal $P(X)$. Montrer que

$$K(\alpha) = \left\{ \sum_{i=0}^{n-1} a_i \alpha^i \mid a_i \in K \right\} \cong K[X]/(P).$$

Montrer que $(1, \alpha, \ldots, \alpha^{n-1})$ est une K-base de $K(\alpha)$.

1.3 Soient K un corps, L une extension de K et A une L-algèbre.

(a) Supposez que $\{\alpha_i\}_{i \in I}$ est une K-base de L et que $\{\beta_j\}_{j \in J}$ est une L-base de A. Montrer que $\{\alpha_i \beta_j\}_{i \in I, j \in J}$ est une K-base de A.

(b) Montrer que si $[L : K]$ et $\dim_L A$ sont finies alors $\dim_K A$ est finie.

(c) Montrer que si $\dim_K A$ est finie alors $[L : K]$ et $\dim_L A$ sont finies.

(d) Montrer que $\dim_K A = [L : K] \dim_L A$ lorsque ces dimensions sont finies.

1.4 Soit K un corps. On considère la K-algèbre $M_n(K)$, pour $n \geq 1$.

(a) Soit $a \in K$. Trouver le polynôme minimal sur K de la matrice

$$A = \begin{pmatrix} a & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & a \end{pmatrix}.$$

(b) Soit $A \in M_n(K)$ une matrice sous forme réduite de Jordan. Déterminer le polynôme minimal de A sur K (en fonction de la forme de Jordan).

(c) Soit K algébriquement clos. Montrer que pour tout polynôme unitaire et non-constant $P \in K[X]$ de degré $\leq n$, il existe $A \in M_n(K)$ avec polynôme minimal P.

(d) Soit à nouveau K quelconque et soit $P \in K[X]$ unitaire et non-constant de degré n. Montrer qu'il existe $A \in M_n(K)$ avec polynôme minimal P.

1.5 (a) Existe-t-il un corps (strictement) intermédiaire entre $\mathbf{R}$ et $\mathbf{C}$?

(b) Donner une extension non-triviale de $\mathbf{C}$.

(c) Soit p un nombre premier. Existe-t-il un corps infini de caractéristique $p > 0$?

(d) Soient L une extension de $\mathbf{C}$ et $\alpha \in L \backslash \mathbf{C}$. α peut-il être algébrique sur $\mathbf{C}$?

(e) Soient $K \subset L$ une extension de corps, $P \in K[X]$ un polynôme irréductible et $\alpha \in L$ une racine de P. Montrer que si $F \in K[X]$ tel que $F(\alpha) = 0$, alors P divise F dans $K[X]$.

(f) Soit $K \subset L \subset M$ une suite d'extensions de corps et soit $\alpha \in M$ algébrique sur L. Est-ce que α est algébrique sur K ? Est-ce que la réponse à la question est différente si on suppose en plus que $\alpha \notin L$?

(g) Soit $K \subset L \subset M$ une suite d'extensions. Montrer que M/K est une extension algébrique si et seulement si les extensions M/L et L/K sont algébriques.

1.6 On fixe un corps K et on considère la K-algèbre (associative) E des endomorphismes K-linéaires de $K[X]$.

(a) Montrer que pour tout $P \in K[X]$ la multiplication par P, notée simplement P, appartient à E.

(b) Soit $\partial \colon K[X] \to K[X]$ l'application $P \mapsto P'$. Montrer que $\partial \in E$.

(c) Soit $A(K) \subset E$ la sous-algèbre engendrée par X (donc la multiplication par X) et ∂. On appelle cette algèbre *l'algèbre des opérateurs différentiels sur* $K[X]$ ou encore *l'algèbre de Weyl* en une variable. Montrer que $\partial X - X\partial = 1$ et conclure que $A(K)$ n'est pas commutative.

(d) Montrer que tout élément de $A(K)$ s'exprime sous la forme d'une somme finie $\sum \alpha_{i,j} X^i \partial^j$ avec les $\alpha_{i,j} \in K$.

1.7 Trouver des $\mathbf{Q}$-bases de $\mathbf{Q}(\sqrt{2})$, de $\mathbf{Q}(\sqrt[3]{2})$ et de $\mathbf{Q}(\sqrt{3}, i)$.

1.8 Montrer que $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$ (comme sous-corps de $\mathbf{R}$). De façon générale, pour $\alpha_1, \alpha_2 \in \mathbf{C}$, a-t-on $\mathbf{Q}(\alpha_1, \alpha_2) = \mathbf{Q}(\alpha_1 + \alpha_2)$?

1.9 Montrer les énoncés suivants :

(a) $X^3 - 2$ est irréductible sur $\mathbf{Q}(\sqrt{2})$.

(b) $[\mathbf{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbf{Q}] = 6$ (donner une $\mathbf{Q}$-base de $\mathbf{Q}(\sqrt{2}, \sqrt[3]{2})$).

(c) $\mathbf{Q}(2^{1/6}) = \mathbf{Q}(\sqrt{2}, \sqrt[3]{2})$.

1.10 (a) Est-ce que $X^4 - 2$ est irréductible sur $\mathbf{Q}(\sqrt{2})$?

(b) Calculer $[\mathbf{Q}(\sqrt{2}, \sqrt[4]{2}) : \mathbf{Q}]$.

(c) Trouver un entier $n > 0$ tel que $\mathbf{Q}(2^{1/n}) = \mathbf{Q}(\sqrt{2}, \sqrt[4]{2})$.

1.11 Soient $\alpha, \beta \in \mathbf{C}$.

(a) Supposez que $[\mathbf{Q}(\alpha) : \mathbf{Q}] = [\mathbf{Q}(\beta) : \mathbf{Q}] < \infty$. Montrer que si $\alpha \in \mathbf{Q}(\beta)$, alors $\mathbf{Q}(\alpha) = \mathbf{Q}(\beta)$.

(b) Considérer $\sqrt{3}, i, j = e^{2i\pi/3} \in \mathbf{C}$. A-t-on $\sqrt{3} \in \mathbf{Q}(j)$, $i \in \mathbf{Q}(j)$ resp. $j \in \mathbf{Q}(i)$?

(c) Calculer les degrés sur $\mathbf{Q}$ des extensions $\mathbf{Q}(\sqrt{3}, j)$, $\mathbf{Q}(\sqrt{3}, i, j)$, $\mathbf{Q}(\sqrt{3}, i)$ et $\mathbf{Q}(\sqrt{3} + i)$. Donner toutes les inclusions et toutes les égalités entre ces extensions.

1.12 Soit $\alpha = \sqrt[3]{2} \in \mathbf{R}$.

(a) Soit $\beta \in \mathbf{Q}(\alpha) \backslash \mathbf{Q}$. Montrer que β est de degré 3 sur $\mathbf{Q}$. A-t-on $\mathbf{Q}(\beta) = \mathbf{Q}(\alpha)$?

(b) Soit $\gamma = 2 - \alpha$. Quel est le polynôme minimal de γ sur $\mathbf{Q}(\alpha)$, sur $\mathbf{Q}$? Calculer les coordonnées de γ^{-1} dans la $\mathbf{Q}$-base $(1, \alpha, \alpha^2)$ de $\mathbf{Q}(\alpha)$ et trouver son polynôme minimal sur $\mathbf{Q}$.

1.13 (a) Montrer que $P(X) = X^3 - X + 1$ est irréductible sur $\mathbf{Q}$.

(b) On note a une racine de $P(X)$ dans $\mathbf{C}$ et $b = 2a^2 - 3a + 2$. Exprimer b^{-1} comme combinaison linéaire, à coefficients dans $\mathbf{Q}$, de 1, a et a^2. (On pourrait procéder d'au moins trois manières différentes : par une méthode des coefficients indéterminés, par l'algorithme d'Euclide et après avoir calculé le polynôme minimal de b.)

(c) Soit $c = (a^7 - 1)/(a^4 + a^2 + 1)$. Exprimer c comme combinaison linéaire, à coefficients dans $\mathbf{Q}$, de 1, a et a^2.

1.14 Soient K un corps et L une extension de K. Soit $\alpha \in L$ algébrique sur K de degré impair. Montrer que α^2 est algébrique sur K et que $K(\alpha) = K(\alpha^2)$. Existe-t-il un corps K, α algébrique de degré pair sur K avec $K(\alpha) = K(\alpha^2)$ (resp. $K(\alpha) \neq K(\alpha^2)$) ?

1.15 (a) Soient K un corps et $P \in K[X]$ irréductible de degré 3. Montrer que si L est une extension de K telle que P soit réductible sur L, alors $[L : K]$ est divisible par 3.

(b) Soient $K \subset L$ une extension de corps et $\alpha, \beta \in L$ algébriques sur K de degrés n et m respectivement avec m et n premiers entre eux. Montrer que l'on a $[K(\alpha, \beta) : K] = mn$ et déterminer $K(\alpha) \cap K(\beta)$.

1.16 Soient K un corps, L une extension finie de K et $\alpha \in L$.

(a) Montrer que α est algébrique sur K de degré au plus $[L : K]$.

(b) Montrer que l'application $m_\alpha \colon L \to L,\ x \mapsto \alpha x$ est une application K-linéaire.

(c) Soit P_α le polynôme caractéristique de m_α. Montrer que $P_\alpha \in K[X]$ et que $P_\alpha(\alpha) = 0$.

(d) Trouver les polynômes minimaux sur $\mathbf{Q}$ de $\sqrt{2}+\sqrt{3}+\sqrt{6}$, de $\sqrt[3]{2}+\sqrt{2}$ et de $i + j$ ($j = e^{2i\pi/3}$).

(e) Soient $L = \mathbf{Q}[X]/(X^3 - X - 1)$, $\alpha = \bar{X} \in L$ et $\beta = \alpha^2 - 2\alpha$. Montrer que L est un corps et trouver le polynôme minimal de β sur $\mathbf{Q}$.

1.17 Soient K un corps et L une extension de K. Montrer que L est une extension algébrique de K si et seulement si toute sous-K-algèbre de L est un corps.

1.18 On admet que π est transcendant sur $\mathbf{Q}$.

(a) Est-ce que $\sqrt{\pi}$ est algébrique sur $\mathbf{Q}$, sur $\mathbf{R}$?

(b) Montrer que $\sqrt{\pi}$ est algébrique sur $\mathbf{Q}(\pi)$ et donner son polynôme minimal.

(c) Montrer que π^2 est algébrique sur $\mathbf{Q}(\pi^3)$, que $\pi^2 \notin \mathbf{Q}(\pi^3)$ et que π^2 est de degré 3 sur $\mathbf{Q}(\pi^3)$.

1.19 Soient $K \subset L$ une extension de corps et $\alpha \in L$ transcendant sur K. Montrer que tout $\beta \in K(\alpha) - K$ est transcendant sur K. En admettant que π est transcendant sur $\mathbf{Q}$, montrer que π^i est transcendant sur $\mathbf{Q}$ pour $i \geq 2$.

2 Polynômes symétriques

Soient k un anneau commutatif unitaire et $n > 0$ un entier. Pour $e_1, \ldots, e_n \in \mathbf{N}$ on notera $\underline{e} = (e_1, \ldots, e_n) \in \mathbf{N}^n$. Pour donner une définition rigoureuse de l'anneau $k[X_1, \ldots, X_n]$ des polynômes en n variables à coefficients dans k, on considère l'ensemble $A = \mathrm{App}_f(\mathbf{N}^n, k)$ des applications $P \colon \mathbf{N}^n \to k$ *à support fini*, c'est à dire les applications P telles qu'il existe un sous-ensemble fini $S \subset \mathbf{N}^n$ tel que $P(\underline{e}) = 0$ pour $\underline{e} \notin S$. On munit A de lois binaires $+$ et $\cdot$ en posant $(P + Q)(\underline{e}) = P(\underline{e}) + P(\underline{e})$ et

$$P \cdot Q(\underline{e}) = \sum_{\substack{\underline{k},\underline{\ell} \in \mathbf{N}^n \\ \underline{k}+\underline{\ell}=\underline{e}}} P(\underline{k})Q(\underline{\ell})$$

pour $P, Q \in A$.

2.1 Montrer que les lois $+$ et $\cdot$ sont bien des lois internes sur A et qu'elles munissent l'ensemble A d'une structure de k-algèbre (associative, unitaire et commutative).

Pour faire le lien avec la notion intuitive de polynôme on écrit $\underline{X}^{\underline{e}} = \prod_{i=1}^{n} X_i^{e_i}$ pour l'application donnée par $\underline{X}^{\underline{e}}(\underline{e}) = 1$ et $\underline{X}^{\underline{e}}(\underline{d}) = 0$ si $\underline{d} \neq \underline{e}$. Tout $P \in A$ s'écrit alors comme combinaison linéaire finie des monômes $\underline{X}^{\underline{e}}$, c'est-à-dire $P = \sum_{\underline{e} \in S} a_{\underline{e}} X^{\underline{e}}$ où $a_{\underline{e}} = P(\underline{e}) \in k$ et $S \subset \mathbf{N}^n$ est un sous-ensemble fini. Le produit correspond au produit habituel des polynômes.
Si B est une k-algèbre, $\underline{b} = (b_1, \ldots, b_n) \in B^n$ et $\underline{e} \in \mathbf{N}^n$ on écrit $\underline{b}^{\underline{e}} = \prod_{i=1}^{n} b_i^{e_i}$ et on définit l'application $\mathrm{ev}_{\underline{b}} \colon A \to B$ par $\mathrm{ev}_{\underline{b}}(P) = \sum_{\underline{e} \in \mathbf{N}^n} P(\underline{e}) \underline{b}^{\underline{e}}$.

2.2 Montrer que $\mathrm{ev}_{\underline{b}}$ est bien une application $A \to B$ et que c'est même un morphisme de k-algèbres.

Soit $I_n = \{1, \ldots, n\}$, muni de l'action naturelle (à gauche) du groupe symétrique S_n.

2.3 En sachant que $\mathbf{N}^n$ est l'ensemble des applications $\mathrm{App}(I_n, \mathbf{N})$, montrer que l'action de S_n sur I_n définit une action (à gauche) de S_n sur A par des morphismes de k-algèbres.

Intuitivement, le morphisme $\sigma \colon A \to A$ associé à $\sigma \in \mathrm{S}_n$ n'est autre que $\mathrm{ev}_{\sigma(\underline{X})} \colon A \to A$, où $\sigma(\underline{X}) = (X_{\sigma(1)}, \ldots, X_{\sigma(n)}) \in A^n$. C'est l'unique endomorphisme de la k-algèbre A tel que $\sigma(X_i) = X_{\sigma(i)}$ pour $i = 1, \ldots, n$.

2.4 Montrer que

$$B = A^{\mathrm{S}_n} = \{P \in A \mid \sigma(P) = P \text{ pour tout } \sigma \in \mathrm{S}_n\}$$

est une sous-k-algèbre de A. On dit que B est l'algèbre des *polynômes symétriques* à coefficients dans k.

2.5 Soit $\Lambda(T) \in A[T]$ le polynôme

$$\Lambda(T) = \prod_{i=1}^{n} (T - X_i) = T^n + \sum_{j=1}^{n} (-1)^j \sigma_j T^{n-j},$$

avec $\sigma_j \in A$ pour $j = 1, \ldots, n$. Les σ_j sont donc des polynômes en $X_1, \ldots, X_n$ à coefficients dans k (qui dépendent de n).

(a) Exprimer les σ_j comme polynômes en $X_1, \ldots, X_n$.

(b) Montrer que S_n opère sur $A[T]$ par des morphismes de k-algèbres et que $A[T]^{\mathrm{S}_n} = B[T]$.

(c) Montrer $\sigma_j \in B$ pour $j = 1, \ldots, n$. Les σ_j sont appelés les *polynômes symétriques élémentaires*.

On introduit deux notions importantes pour ce qui est à suivre.

– Le *degré* d'un monôme $\underline{X}^{\underline{e}} = X_1^{e_1} \cdots X_n^{e_n}$ est $e_1 + \cdots + e_n$. Le degré d'un polynôme P est le maximum des degrés des monômes paraissant dans P avec un coefficient non nul.
– On définit *l'ordre lexicographique* sur $\mathbf{N}^n$ de la façon suivante. On dit qu'un élément $\underline{e} = (e_1, \ldots, e_n) \in \mathbf{N}^n$ *précède* $\underline{e}' = (e'_1, \ldots, e'_n) \in \mathbf{N}^n$ dans l'ordre lexicographique s'il existe un indice j tel que $e_i = e'_i$ pour $1 \leq i < j$ et $e_j > e'_j$. On note $\underline{e} \succ \underline{e}'$ ou encore $\underline{e}' \prec \underline{e}$. Si $\underline{e}, \underline{e}' \in \mathbf{N}^n$, alors on est dans un (et un seul) des cas suivants : $\underline{e} \succ \underline{e}'$, $\underline{e} = \underline{e}'$ ou $\underline{e} \prec \underline{e}'$. Si $P \in k[X_1, \ldots, X_n]$, alors le *degré lexicographique* de P est le plus grand exposant (c'est à dire l'exposant qui précède tous les autres) $\underline{e}$ dans l'ordre lexicographique tel que le coefficient de $\underline{X}^{\underline{e}}$ dans P soit non nul.

2.6 Montrer que si P et Q sont des polynômes unitaires de degrés lexicographiques $\underline{d}$ et $\underline{e}$ respectivement, alors le produit PQ est de degré lexicographique $\underline{d} + \underline{e}$.

2.7 Supposons que $d_1 \geq d_2 \geq \cdots \geq d_n \geq 0$. Montrer que

$$\sigma_1^{d_1 - d_2} \sigma_2^{d_2 - d_3} \cdots \sigma_{n-1}^{d_{n-1} - d_n} \sigma_n^{d_n}$$

est de degré lexicographique $\underline{d}$.

2.8 Soit $0 \neq P \in B$ un polynôme symétrique de degré lexicographique $\underline{d} = (d_1, \ldots, d_n)$.

(a) Montrer que $d_1 \geq d_2 \geq \cdots \geq d_n$.

(b) Montrer par récurrence décroissante sur $\underline{d}$ qu'il existe $Q \in k[Y_1, \ldots, Y_n]$ tel que $P(X_1, \ldots, X_n) = Q(\sigma_1, \ldots, \sigma_n)$.

(c) Donner un algorithme pour calculer Q à partir de P.

2.9 (a) Soit $Q \in k[Y_1, \ldots, Y_n]$ tel que $Q(\sigma_1, \ldots, \sigma_n) = 0$. Montrer que $Q = 0$. (Indication : Si $Q \neq 0$, considérer $\underline{e} = (e_1, \ldots, e_n) \in \mathbf{N}^n$ maximal dans l'ordre lexicographique tel que le coefficient de $Y_1^{e_1 - e_2} Y_2^{e_2 - e_3} \cdots Y_{n-1}^{e_{n-1} - e_n} Y_n^{e_n}$ dans Q soit non nul.)

On dit que $\sigma_1, \ldots, \sigma_n$ sont *algébriquement indépendants sur k*.

(b) Soit P un polynôme symétrique. Montrer que le polynôme $Q \in k[Y_1, \ldots, Y_n]$ vérifiant $P(X_1, \ldots, X_n) = Q(\sigma_1, \ldots, \sigma_n)$ est unique.

2.10 Soit $\Lambda \in A[T]$ comme dans l'exercice 2.5, alors on pose

$$\Delta = \Delta(\Lambda) = \prod_{1 \leq i < j \leq n} (X_i - X_j)$$

et on définit le *discriminant* de Λ comme $D(\Lambda) = \Delta^2$. Montrer que $D(\Lambda)$ est un polynôme symétrique et trouver son expression en termes des polynômes symétriques élémentaires pour $n = 2, 3$.

2.11 Pour $d \geq 0$ on définit $p_d = \sum_{i=1}^{n} X_i^d \in A$. Montrer les *identités de Newton*

$$p_m + \sum_{j=1}^{m-1} (-1)^j \sigma_j p_{m-j} + (-1)^m m\sigma_m = 0 \quad \text{si } m \leq n,$$

$$p_m + \sum_{j=1}^{n} (-1)^j \sigma_j p_{n-j} = 0 \quad \text{si } m > n,$$

2.12 Soient Δ comme dans l'exercice 2.10 et M la matrice

$$M = \begin{pmatrix} 1 & X_1 & X_1^2 & \cdots & X_1^{n-1} \\ 1 & X_2 & X_2^2 & \cdots & X_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & X_n & X_n^2 & \cdots & X_n^{n-1} \end{pmatrix}$$

(a) Montrer que $\Delta = (-1)^{n(n-1)/2} \det(M)$. (Le déterminant $\det(M)$ est un déterminant de *Vandermonde*.)

(b) Montrer que

$${}^tMM = \begin{pmatrix} p_0 & p_1 & \cdots & p_{n-1} \\ p_1 & p_2 & \cdots & p_n \\ \vdots & \vdots & \ddots & \vdots \\ p_{n-1} & p_n & \cdots & p_{2n-2} \end{pmatrix}$$

et utiliser cette formule pour exprimer le discriminant $D(\Lambda)$ comme un déterminant.

(c) Combiner la formule pour Δ trouvée ci-dessus avec les identités de Newton pour exprimer le discriminant $D(\Lambda)$ en termes des polynômes symétriques élémentaires pour $n = 2, 3, 4$.

2.13 L'action de S_{n-1} sur $\{1, \ldots, n-1\}$ définit une inclusion $\mathrm{S}_{n-1} \subset \mathrm{S}_n$. Par restriction, le groupe S_{n-1} opère donc sur A. On note $\sigma'_1, \ldots, \sigma'_{n-1} \in A$ les polynômes symétriques élémentaires en $X_1, \ldots, X_{n-1}$.

(a) Montrer que $C = A^{\mathrm{S}_{n-1}}$ est une k-algèbre et que $C = k[\sigma'_1, \ldots, \sigma'_{n-1}, X_n]$.

(b) Montrer que $\sigma_1 = \sigma'_1 + X_n$ et que pour $\ell = 2, \ldots, n-1$ on a $\sigma_\ell = \sigma'_\ell + \sigma'_{\ell-1} X_n$.

(c) Montrer que $\sigma_1, \ldots, \sigma_{n-1}, X_n \in A$ sont algébriquement indépendants sur k. (Indication : Si $Q \in k[Y_1, \ldots, Y_n]$ vérifie $Q(\sigma_1, \ldots, \sigma_{n-1}, X_n) = 0$, considérer les termes du plus faible degré en X_n.)

(d) Montrer que $C = k[\sigma'_1, \ldots, \sigma'_{n-1}, X_n] = k[\sigma_1, \ldots, \sigma_{n-1}, X_n]$.

(e) Montrer que $\sigma'_\ell = (-1)^\ell X_n^\ell + \sum_{i=1}^{\ell}(-1)^{\ell-1}\sigma_i X_n^{\ell-i}$ (pour $\ell = 2, \ldots, n-1$). En déduire que, en tant que polynôme en X_n à coefficients dans $k[\sigma_1, \ldots, \sigma_{n-1}]$, σ_n est unitaire de degré n.

2.14 Soient R un anneau et $P \in R[T]$ un polynôme unitaire de degré $n \geq 1$. Comme d'usage, on note $R[P]$ le sous-R-algèbre de $R[T]$ engendré par P.

(a) Montrer que le système $(1, \ldots, T^{n-1})$ est libre sur $R[P]$. (Indication : Dans une expression $\sum_{i=0}^{n-1} a_i T^i$, avec $a_0, \ldots, a_{n-1} \in R[P]$ chercher le terme du plus grand degré en T.)

(b) Montrer que $R[T]$ est un $R[P]$-module libre de rang n, avec base $(1, \ldots, T^{n-1})$.

2.15 (a) En appliquant la question 2.14(b) avec $R = k[\sigma_1, \ldots, \sigma_{n-1}]$ et $P = \sigma_n$, montrer que $C = R[X_n]$ est un $B = R[\sigma_n]$-module libre de rang n.

(b) Montrer par récurrence sur n que l'ensemble des $X_1^{\nu(1)} \cdots X_n^{\nu(n)}$ tels que $0 \leq \nu(i) < i$ pour $1 \leq i \leq n$ est une B-base de A. En déduire que A est un B-module libre de rang $n!$. (Indication : Si on note $C = k[\sigma'_1, \ldots, \sigma'_{n-1}, X_n]$ alors $B \subset C \subset A$).

2.16 Soient $P(T) = T^n + \sum_{j=1}^{n} a_j T^{n-j} \in k[T]$ un polynôme unitaire de degré n et $I \subset A$ l'idéal engendré par les $a_i - (-1)^i \sigma_i$ pour $i = 1, \ldots, n$. Soit D le quotient A/I.

(a) Montrer que D est une k-algèbre unitaire et que P est décomposé sur D.

(b) Soit D' une k-algèbre sur laquelle P soit décomposé, $P(T) = \prod_{i=1}^{n}(X - \alpha_i)$ avec les $\alpha_i \in D'$. Montrer qu'il existe un unique morphisme de k-algèbres $f\colon D \to D'$ tel que $f(\bar{X}_i) = \alpha_i$. On dit que D est une *algèbre de décomposition universelle* de P sur k.

(c) Soit $J \subset B$ l'idéal engendré par les $a_i - (-1)^i \sigma_i$ pour $i = 1, \ldots, n$. Montrer que $B = k \oplus J$, puis déduire de 2.15(b) que $1 \notin I$.

(d) Supposons que k soit un corps. D'après le théorème de Krull, D admet un idéal maximal $\mathfrak{m}$. Montrer que $D/\mathfrak{m}$ est un corps de décomposition de P sur k.

2.17 Soient $P = T^d + \sum_{j=1}^{d} a_j T^{d-j} \in k[T]$ un polynôme unitaire de degré d et m une k-algèbre sur laquelle P est décomposé,

$$P(T) = \prod_{i=1}^{d}(T - \alpha_i).$$

Soit $\underline{\alpha} = (\alpha_1, \ldots, \alpha_d) \in m^d$ et considérons le morphisme d'évaluation $\mathrm{ev}_{\underline{\alpha}}\colon A \to m$.

(a) Montrer que $\mathrm{ev}_{\underline{\alpha}}(\sigma_i) = (-1)^i a_i$ pour $i = 1, \ldots, d$. En déduire que pour tout polynôme symétrique $P \in B$ on a $\mathrm{ev}_{\underline{\alpha}}(P) \in k$.

(b) On définit le *discriminant* de P comme

$$D(P) = \prod_{1 \leq i < j \leq d} (\alpha_i - \alpha_j)^2.$$

Montrer que $D(P) = \mathrm{ev}_{\underline{\alpha}}(D(\Lambda)) \in k$ et que $D(P)$ admet une expression comme un polynôme à coeffectients entiers en $a_1, \ldots, a_d$.

(c) Soit $P(T) = T^3 + pT + q$ avec $p, q \in k$. Exprimer le discriminant $D(P)$ en fonction de p et q.

3 Corps de décomposition

3.1 Soient K un corps et $P \in K[X]$. Les affirmations suivantes sont-elles vraies ?

(a) Il existe une extension L de K telle que P soit décomposé sur L.

(b) $K[X]/(P)$ est un corps de décomposition de $P(X)$.

(c) $K[X]/(P)$ n'est pas un corps de décomposition de $P(X)$.

(d) Mêmes questions sous l'hypothèse supplémentaire que $P \in K[X]$ soit irréductible.

3.2 Déterminer le corps de décomposition $L \subset \mathbf{C}$ sur $\mathbf{Q}$ de chacun des polynômes suivants.

(a) $X^4 + 1\,;\ X^6 - 8\,;\ X^3 - 1$

(b) $(X^2 - 3)(X^3 + 1)\,;\ X^3 + X + 2\,;\ X^3 + X^2 + 2\,;\ (X^4 - 2)(X^2 - 2)$

Dans chaque cas, calculer le degré de l'extension $L/\mathbf{Q}$. Pour chacun des polynômes de 3.2(a), trouver un élément $\alpha \in \mathbf{C}$ tel que $L = \mathbf{Q}(\alpha)$ ainsi que le polynôme minimal de α.

3.3 Soit $\alpha = \sqrt[3]{2}$.

(a) Montrer que $\mathbf{Q}(\alpha, i\sqrt{3}) \subset \mathbf{C}$ est un corps de décomposition de $X^3 - 2$ sur $\mathbf{Q}$.

(b) Quel est le degré de $\mathbf{Q}(\alpha, i\sqrt{3})$ sur $\mathbf{Q}$?

(c) $\mathbf{Q}(\alpha, i\sqrt{3})$ est-il isomorphe à $K = \mathbf{Q}[X]/(X^3 - 2)$?

(d) Donner la factorisation de $X^3 - 2$ sur $\mathbf{Q}(\alpha)$.

3.4 Soient les polynômes P_i $(1 \leq i \leq 4)$ donnés par

$$P_1(X) = X^4 - 7, \qquad P_2(X) = X^2 - 2X + 2,$$
$$P_3(X) = X^4 + 1, \qquad P_4(X) = X^4 + 2.$$

Pour chaque polynôme P_i, trouver un corps de décomposition L_i sur $\mathbf{Q}$ et calculer le degré $[L_i : \mathbf{Q}]$. Indiquer si L_i est isomorphe à $\mathbf{Q}[X]/(P_i)$ et donner la factorisation de P_i sur $\mathbf{Q}[X]/(P_i)$.

3.5 Soient k un corps $K = k(X)$, $L = k(Y)$, $n > 0$ un entier et

$$\begin{aligned} i = \mathrm{ev}_{Y^n} \colon K = k(X) &\to L = k(Y) \\ P(X) &\mapsto P(Y^n). \end{aligned}$$

(a) Montrer que i est un morphisme d'anneaux et munit donc L de la structure d'extension de K.

(b) Montrer que la famille $(1, Y, \ldots, Y^{n-1})$ dans L est libre sur K et déduire que $[L : K] \geq n$.

(c) Montrer que $L = K(Y)$, trouver un polynôme $P(T) \in K[T]$ de degré n tel que $P(Y) = 0$ et conclure que $[L : K] = n$.

(d) Soient $P(Y), Q(Y) \in k[Y]$ avec $Q \neq 0$. Montrer qu'il existe des fractions rationnelles $A_0(X), \ldots, A_{n-1}(X) \in K = k(X)$ telles que

$$\frac{P(Y)}{Q(Y)} = \sum_{i=0}^{n-1} A_i(X) Y^i.$$

(e) Donner un algorithme pour déterminer explicitement les $A_0, \ldots, A_{n-1}$ de la partie précédente. (Indication : traiter d'abord le cas (facile) où $Q(Y) = 1$, puis le cas où $P(Y) = 1$.)

(f) Montrer que L est un corps de décomposition de $T^n - X$ sur K si et seulement si le polynôme $T^n - 1$ est décomposé dans $k[T]$.

3.6 Soient $P \in K[X]$ de degré d et L un corps de décomposition de P sur K. Montrer que $[L : K]$ divise $d!$, donc en particulier $[L : K] \leq d!$.

3.7 Soient K un corps et $L = K(\alpha_1, \ldots, \alpha_n)$ une extension fini. Pour $i = 1, \ldots, n$ soit $P_i \in K[X]$ le polynôme minimal de α_i sur K. Soient enfin $P = \prod_{i=1}^n P_i$ et M un corps de décomposition de P sur K. Montrer qu'il existe un K-morphisme $L \to M$.

3.8 Soient K un corps, L une extension de K, $P \in K[X]$ et M un corps de décomposition de P sur L. Supposons que P soit réductible dans $L[X]$ mais irréductible dans $L'[X]$ pour toute sous-extension $L' \subset L$ de K avec $L' \neq L$. Montrer que M est un corps de décomposition de P sur K. (Indication : Montrer d'abord qu'il existe $M' \subset M$, un corps de décomposition de P sur K et ensuite que $L \subset M'$.)

3.9 Soient K un corps, L une extension de K de degré $p = [L : K]$ premier et $P \in K[X]$ un polynôme irréductible de degré d tel que P soit réductible dans $L[X]$. Le but de l'exercice est de prouver que p divise le degré de P.

Soient M un corps de décomposition de P sur L et $\alpha \in M$ une racine de P.

(a) Montrer que $[L(\alpha) : K] = pe$ pour un entier $e < d$.

(b) Montrer que d divise pe.

(c) Montrer que p divise d.

3.10 Les affirmations suivantes sont-elles vraies ? Justifier votre réponse.

(a) Il existe un corps à 6 éléments.

(b) Il existe un corps à 125 éléments.

(c) Si K est un corps fini, il existe $n \in \mathbf{Z}$ tel que $K \cong \mathbf{Z}/n\mathbf{Z}$.

(d) Si K est un corps fini, alors $(K, +)$ est cyclique.

(e) Le polynôme $X^5 + 5$ a des racines simples dans toute extension de $\mathbf{F}_7$.

(f) Le polynôme $X^7 + 5$ a des racines simples dans toute extension de $\mathbf{F}_7$.

3.11 Soient K un corps et $P \in K[X]$.

(a) Soit P irréductible. Montrer qu'on a $\operatorname{pgcd}(P, \partial_X P) \neq 1$ si et seulement si $\partial_X P = 0$.

(b) Soit $\operatorname{car}(K) = 0$. Montrer que $\partial_X P = 0$ si et seulement si P est constant.

(c) Soit $\operatorname{car}(K) = p > 0$. Montrer que $\partial_X P = 0$ si et seulement si il existe un polynôme $Q \in K[X]$ tel que $P(X) = Q(X^p)$.

(d) Montrer que si P est irréductible et K est un corps fini, alors $\partial_X P \neq 0$.

(e) En utilisant les idées de l'exercice 3.5, trouver un corps K, un polynôme irréductible $P \in K[X]$ de degré > 1 et un corps de décomposition L de P sur K tels que P n'a qu'une seule racine dans L.

4 Automorphismes de corps, groupe et correspondance de Galois

4.1 On considère le sous-corps $\mathbf{Q}(i, \sqrt{3}) \subset \mathbf{C}$.

(a) Montrer que $(1, i, \sqrt{3}, i\sqrt{3})$ est une $\mathbf{Q}$-base de $\mathbf{Q}(i, \sqrt{3})$.

(b) Montrer que pour tous $\epsilon_1, \epsilon_2 \in \{\pm 1\}$, l'application

$$\begin{aligned} f_{\epsilon_1,\epsilon_2} \colon \mathbf{Q}(i, \sqrt{3}) &\to \mathbf{Q}(i, \sqrt{3}) \\ a + bi + c\sqrt{3} + di\sqrt{3} &\mapsto a + b\epsilon_1 i + c\epsilon_2\sqrt{3} + d\epsilon_1\epsilon_2 i\sqrt{3} \end{aligned}$$

est un automorphisme de $\mathbf{Q}(i, \sqrt{3})$.

(c) Montrer que les $f_{\epsilon_1,\epsilon_2}$ sont les seuls automorphismes de $\mathbf{Q}(i,\sqrt{3})$.

(d) Montrer que le groupe des automorphismes de $\mathbf{Q}(i,\sqrt{3})$ est isomorphe à $\{\pm 1\}^2$.

4.2 Soient K un corps, $P \in K[X]$ un polynôme irréductible unitaire de degré 3 et L un corps de décomposition de P sur K. On note $\alpha_1, \alpha_2, \alpha_3 \in L$ les racines de P de sorte que $P(X) = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$ dans $L[X]$.

(a) Montrer que $[L:K] = 3$ ou 6.

(b) Supposez que les α_i ne sont pas deux à deux distincts.

i. Montrer que $\mathrm{car}(K) = 3$ et que $\alpha_1 = \alpha_2 = \alpha_3$.

ii. Déterminer $[L:K]$.

iii. Montrer que $\mathrm{Gal}(L/K) = 1$.

(c) Supposez que les α_i sont distincts et que $[L:K] = 3$. Montrer que l'action de $\mathrm{Gal}(L/K)$ sur $\{\alpha_1, \alpha_2, \alpha_3\}$ est transitive et que

$$\mathrm{Gal}(L/K) \cong \mathbf{Z}/3\mathbf{Z}.$$

(d) Supposez que $[L:K] = 6$. On rappelle que l'action de $\mathrm{Gal}(L/K)$ sur l'ensemble $\{\alpha_1, \alpha_2, \alpha_3\}$ identifie le groupe de Galois avec un sous-groupe $H \subset \mathrm{S}_3$.

i. En considérant les groupes $\mathrm{Gal}(L/K(\alpha_i))$, montrer que H contient les transpositions.

ii. Montrer que $\mathrm{Gal}(L/K) \cong \mathrm{S}_3$.

iii. Montrer que l'action de $\mathrm{Gal}(L/K)$ sur $\{\alpha_1, \alpha_2, \alpha_3\}$ est transitive.

(e) Dans chaque cas ci-dessus, déterminer $\mathrm{Gal}(K(\alpha_1)/K)$.

4.3 Soient K un corps, $P \in K[X]$ un polynôme irréductible unitaire de degré 3 avec $\partial_X P \neq 0$ et L un corps de décomposition de P sur K (comptées avec multiplicités). On note $\alpha_1, \alpha_2, \alpha_3$ let racines de P dans L.

(a) Montrer que

$$\Delta(P) = (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3) \in L$$

et que $D(P) = \Delta(P)^2 \in K$.

(b) Montrer que si $\Delta(P) \notin K$ alors $[L:K] = 6$.

(c) Soient $L' = K(\alpha_1) \subset L$ et $Q \in L'[X]$ le quotient de la division euclidienne de P par $X - \alpha_1$. Montrer que $\beta = Q(\alpha_1) \in L'$. Montrer que $\alpha_2 + \alpha_3 \in L'$ en l'exprimant en fonction de α_1 et les coefficients de P.

(d) Exprimer $\alpha_2 - \alpha_3$ en fonction de β et Δ, puis, dans le cas où $\mathrm{car}(K) \neq 2$, les racines α_2 et α_3 en fonction de α_1, β, Δ et les coefficients de P.

(e) Conclure que, si $\mathrm{car}(K) \neq 2$, alors $[L : K] = 3$ si et seulement si $\Delta(P) \in K$.

4.4 (a) Montrer que $P(X) = X^3 + X + 1$ est irréductible dans $\mathbf{Q}[X]$ et déterminer si son groupe de Galois (sur $\mathbf{Q}$) est isomorphe à $\mathbf{Z}/3\mathbf{Z}$ ou à S_3. (Indication : $P(X)$ n'a qu'une racine réelle.)

(b) Montrer que $Q(X) = X^3 - 3X + 1$ est irréductible dans $\mathbf{Q}[X]$ et déterminer si son groupe de Galois est isomorphe à $\mathbf{Z}/3\mathbf{Z}$ ou à S_3.

4.5 Soient $P(X) = X^4 - 2X^3 + 7X^2 - 6X + 12$ et $K \subset \mathbf{C}$ un corps de décomposition de P. Montrer que $i\sqrt{3}$ et $1 + i\sqrt{3}$ sont des racines de P. Existe-t-il $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ tel que $\sigma(i\sqrt{3}) = 1 + i\sqrt{3}$?

4.6 (a) Montrer que $\mathrm{Gal}(\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z})^2$.

(b) Donner les matrices des éléments de $\mathrm{Gal}(\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q})$ par rapport une $\mathbf{Q}$-base de $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ de votre choix.

4.7 Soient $K = \mathbf{F}_2[X]/(X^4 + X + 1)$ et $\alpha = \bar{X} \in K$.

(a) Décomposer $X^4 + X + 1$ en facteurs irréductibles dans $K[X]$.

(b) Montrer que $\mathrm{Gal}(K/\mathbf{F}_2)$ est isomorphe à $\mathbf{Z}/4\mathbf{Z}$.

(c) Factoriser $X^4 + X^3 + 1$, $X^4 + X^3 + X^2 + X + 1$ et $X^2 + X + 1$ dans $K[X]$.

(d) Trouver les générateurs de $K^\times$.

4.8 (a) Montrer que $P(X) = X^3 - 3$ est irréductible sur $\mathbf{F}_7$.

(b) Soient $K = \mathbf{F}_7[X]/(P)$ et $\alpha = \bar{X} \in K$. Montrer que $P(X)$ est décomposé sur K et exprimer les racines de $P(X)$ en fonction de α.

(c) Trouver l'orbite de α sous l'action de $\mathrm{Gal}(\mathbf{F}_{7^3}/\mathbf{F}_7)$.

4.9 (a) Déterminer le degré sur le corps de base d'un corps de décomposition du polynôme $P(X) = X^3 + X + 1$ sur $\mathbf{C}$, $\mathbf{R}$, $\mathbf{Q}$, $\mathbf{F}_2$, $\mathbf{F}_2[X]/(X^2 + X + 1)$, $\mathbf{F}_2[X]/(X^3 + X^2 + 1)$, $\mathbf{F}_3$ et sur $\mathbf{F}_5$.

(b) Dans chaque cas, déterminer si le groupe de Galois correspondant est isomorphe à $\{1\}$, $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/6\mathbf{Z}$ ou à S_3.

4.10 (a) Soient L/K une extension algébrique de corps et $\alpha \in L$. Montrer que l'ensemble $g(\alpha)$, pour g parcourant le groupe $\mathrm{Aut}_K(L)$ est fini.

(b) Montrer, sans utiliser le théorème 3.6 ou le corollaire 3.7 du cours, que si L/K est une extension finie de corps, alors $\mathrm{Gal}(L/K)$ est fini.

4.11 Soient $\alpha = \sqrt[3]{2}$ et $j = e^{2i\pi/3} \in \mathbf{C}$. On considère les extensions

$$\mathbf{Q}(j)/\mathbf{Q}, \quad \mathbf{Q}(\alpha)/\mathbf{Q}, \quad \mathbf{Q}(\alpha j)/\mathbf{Q}, \quad \mathbf{Q}(\alpha, j)/\mathbf{Q}(\alpha), \quad \mathbf{Q}(\alpha, j)/\mathbf{Q}(j), \quad \mathbf{Q}(\alpha, j)/\mathbf{Q}.$$

(a) Pour chacune de ces extensions, déterminer si son groupe de Galois est isomorphe à $\{1\}$, $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/6\mathbf{Z}$ ou à S_3.

(b) Lesquelles des extensions ci-dessus sont galoisiennes ?

4.12 (a) Trouver les sous-corps du corps $\mathbf{Q}(i, \sqrt{3})$ et les relations d'inclusion entre eux.

(b) Même question pour $\mathbf{Q}(\sqrt[3]{2}, j)$.

4.13 Soit L/K une extension galoisienne de corps de caractéristique différente de 2. On suppose que $\mathrm{Gal}(L/K) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Montrer qu'il existe $\alpha, \beta \in L$ avec $\alpha^2, \beta^2 \in K$ tels que $L = K(\alpha, \beta)$. Montrer que les seules extensions intermédiaires sont $K(\alpha)$, $K(\beta)$ et $K(\alpha\beta)$.

4.14 (a) Trouver tous les corps intermédiaires entre $\mathbf{Q}$ et $\mathbf{Q}(\sqrt{2}, \sqrt{3})$.

(b) En déduire que $\sqrt{5}$ est de degré 2 sur $\mathbf{Q}(\sqrt{2}, \sqrt{3})$.

(c) Si $L = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, montrer que $\mathrm{Gal}(L/\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z})^3$.

(d) Combien d'extensions de degré 4 (resp. 2) de $\mathbf{Q}$ sont contenues dans L ?

4.15 Soient $\alpha = \sqrt{6 + \sqrt{11}}$, $\beta = \sqrt{6 - \sqrt{11}} \in \mathbf{R}$ et $N = \mathbf{Q}(\alpha)$.

(a) Déterminer le polynôme minimal P de α sur $\mathbf{Q}$.

(b) Montrer que $\mathbf{Q}(\sqrt{11}) \subset N$ et calculer $[N : \mathbf{Q}(\sqrt{11})]$.

(c) Montrer que $\beta \in N$ et donner son expression dans la base $(1, \alpha, \alpha^2, \alpha^3)$.

(d) On pose $G = \mathrm{Gal}(N/\mathbf{Q})$. Est-ce que G est isomorphe à $\mathbf{Z}/4\mathbf{Z}$, à $(\mathbf{Z}/2\mathbf{Z})^2$ ou à un autre groupe ?

(e) Quels sont les degrés de $\alpha + \beta$ et $\alpha - \beta$ sur $\mathbf{Q}$?

(f) Est-ce que $\mathrm{Gal}(N/\mathbf{Q}(\alpha + \beta)) = \mathrm{Gal}(N/\mathbf{Q}(\alpha - \beta))$ (comme sous-groupes de G) ? Est-ce que $\mathrm{Gal}(N/\mathbf{Q}(\alpha + \beta)) \cong \mathrm{Gal}(N/\mathbf{Q}(\alpha - \beta))$?

(g) Trouver les corps intermédiaires entre N et $\mathbf{Q}$ et indiquer les relations d'inclusion entre eux. Pour chaque corps intermédiaire trouver le sous-groupe de $\mathrm{Gal}(N/\mathbf{Q})$ correspondant.

(h) Trouver $a, b \in \mathbf{Q}$ tels que $\alpha = \sqrt{a} + \sqrt{b}$ et $\beta = \sqrt{a} - \sqrt{b}$.

4.16 Soient $P(X) = X^4 - 12X^2 + 18$ et L un corps de décomposition de P sur $\mathbf{Q}$.

(a) Calculer $[L : \mathbf{Q}]$.

(b) Est-ce que $\mathrm{Gal}(L/\mathbf{Q})$ est isomorphe à $\mathbf{Z}/4\mathbf{Z}$, à $(\mathbf{Z}/2\mathbf{Z})^2$ ou à un autre groupe ?

(c) Donner un générateur de chacune des extensions intermédiaires entre L et $\mathbf{Q}$.

4.17 Soient $L = \mathbf{Q}[X]/(X^4+1)$ et $\alpha = \bar{X} \in L$.

(a) Montrer que L est un corps et déterminer $[L : \mathbf{Q}]$.

(b) Montrer que pour tout $k \in \mathbf{Z}$ impair, il existe un unique $\rho_k \in \mathrm{Gal}(L/\mathbf{Q})$ tel que $\rho_k(\alpha) = \alpha^k$.

(c) Montrer que l'application

$$\begin{aligned} 2\mathbf{Z}+1 &\to \mathrm{Gal}(L/\mathbf{Q}) \\ k &\mapsto \rho_k \end{aligned}$$

induit un isomorphisme de groupes $(\mathbf{Z}/8\mathbf{Z})^\times \cong \mathrm{Gal}(L/\mathbf{Q})$.

(d) Montrer que $L \cong \mathbf{Q}(\sqrt{2}, i)$.

(e) Trouver les sous-corps de $\mathbf{Q}(\sqrt{2}, i)$ pour chaque sous-corps, déterminer le sous-groupe de $(\mathbf{Z}/8\mathbf{Z})^\times$ correspondant.

4.18 Soit $\alpha = \sqrt[5]{7} \in \mathbf{R} \subset \mathbf{C}$.

(a) Déterminer $[\mathbf{Q}(\alpha) : \mathbf{Q}]$.

(b) Montrer que $\mathrm{Gal}(\mathbf{Q}(\alpha)/\mathbf{Q}) = 1$.

(c) Soit $\omega = e^{2i\pi/5}$. Déterminer $[\mathbf{Q}(\omega) : \mathbf{Q}]$.

(d) Montrer que $L = \mathbf{Q}(\alpha, \omega)$ est un corps de décomposition de $X^5 - 7$ sur $\mathbf{Q}$.

(e) Montrer que $\mathrm{Gal}(L/\mathbf{Q}(\omega)) \cong \mathbf{Z}/5\mathbf{Z}$.

(f) Montrer qu'il existe $\rho \in \mathrm{Gal}(L/\mathbf{Q})$ tel que $\rho(\omega) = \omega$ et $\rho(\alpha) = \omega\alpha$.

(g) Montrer qu'il existe $\tau \in \mathrm{Gal}(L/\mathbf{Q})$ tel que $\tau(\omega) = \omega^2$ et $\tau(\alpha) = \alpha$.

(h) Montrer que

$$\mathrm{Gal}(L/\mathbf{Q}) = \{\rho^a\tau^b \mid a, b \in \mathbf{Z}, 0 \le a \le 4, 0 \le b \le 3\}.$$

(i) D'après la question précédente, pour tous $a, b, c, d \in \mathbf{Z}$, le produit $\rho^a\tau^b\rho^c\tau^d$ s'écrit sous la forme $\rho^e\tau^f$ avec $0 \le e \le 4$ et $0 \le f \le 3$. Exprimer e et f en fonction de a, b, c, d.

4.19 Montrer que le groupe de Galois de $X^4 - 2$ sur $\mathbf{Q}$ est isomorphe à D_4. Même question pour celui de $X^4 + 2$.

4.20 Soient $K \subset L \subset M$ des extensions finies de corps.

(a) Supposons que M/L et L/K soient des extensions galoisiennes. Est-ce que cela implique que M/K est galoisienne ?

(b) Supposons à présent M/K galoisienne. Est-ce que M/L est galoisienne ? Est-ce que L/K est galoisienne ?

(c) Supposons que M/K est galoisienne et que $\mathrm{Gal}(M/K)$ est abélien. Est-ce que M/L est galoisienne ? Est-ce que L/K est galoisienne ?

4.21 Les affirmations suivantes sont-elles exactes ? Justifier votre réponse.

(a) Soient L/K une extension galoisienne finie et $\alpha, \beta \in L$ deux éléments avec le même polynôme minimal sur K. Alors il existe $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma(\alpha) = \beta$.

(b) L'énoncé précédent est vrai pour toute extension finie L/K, pas nécessairement galoisienne.

(c) Soient L/K une extension galoisienne finie et $\alpha, \beta \in L$ deux éléments tel qu'il existe $\sigma \in \mathrm{Gal}(L/K)$ avec $\sigma(\alpha) = \beta$. Alors α et β ont le même polynôme minimal sur K.

(d) L'énoncé précédent est vrai pour toute extension finie L/K, pas nécessairement galoisienne.

(e) Soit L/K une extension finie avec la propriété que pour tout couple d'éléments $\alpha, \beta \in L$ avec le même polynôme minimal sur K, il existe $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma(\alpha) = \beta$. Alors L/K est une extension galoisienne.

(f) Il existe un $\alpha \in \mathbf{Q}(j)$ tel que α^2 appartient à $\mathbf{Q}$ et $\mathbf{Q}(\alpha) = \mathbf{Q}(j)$.

4.22 Soit L un corps. Si $M_1, M_2 \subset L$ sont des sous-corps, alors on définit $M_1 M_2$ comme l'intersection des sous-corps M de L tels que $M_1 \subset M$ et $M_2 \subset M$:

$$M_1 M_2 = \bigcap_{M \supset M_1, M_2} M.$$

Soient $K \subset L$ une extension galoisienne finie, M_1, M_2 des corps intermédiaires, $G = \mathrm{Gal}(L/K)$ et $H_i = \mathrm{Gal}(L/M_i) \subset G$. Montrer que $H_1 \cap H_2 = \mathrm{Gal}(L/M_1 M_2)$ et que $M_1 M_2 = L^{H_1 \cap H_2}$.

4.23 Soit G un groupe. Si $H_1, H_2 \subset G$ sont des sous-groupes, alors on définit $H_1 H_2$ comme l'intersection des sous-groupes H de G tels que $H_1 \subset H$ et $H_2 \subset H$:

$$H_1 H_2 = \bigcap_{H \supset H_1, H_2} H.$$

Soient $K \subset L$ une extension galoisienne finie, M_1, M_2 des corps intermédiaires, $G = \mathrm{Gal}(L/K)$ et $H_i = \mathrm{Gal}(L/M_i) \subset G$. Montrer que $H_1 H_2 = \mathrm{Gal}(L/M_1 \cap M_2)$ et que $M_1 \cap M_2 = L^{H_1 H_2}$.

4.24 (a) Soient G un groupe, H_1 et H_2 deux sous-groupes distingués de G tels que $H_1 \cap H_2 = \{e\}$ et $G = H_1H_2$. Montrer que $G \cong H_1 \times H_2$.

(b) Soient K un corps, L une extension galoisienne finie de K, L' et L'' des extensions galoisiennes de K contenues dans L. Montrer que si $L' \cap L'' = K$ et $L'L'' = L$, alors $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(L/L') \times \mathrm{Gal}(L/L'')$.

(c) Soient $P_1, P_2 \in K[X]$ premiers entre eux et de degrés respectifs n_1 et n_2. Soient L un corps de décomposition de $P = P_1P_2$ et $L_1, L_2 \subset L$ les corps de décomposition de P_1 et de P_2 dans L respectivement. Les affirmations suivantes sont-elles vraies ? Justifier les réponses.

i. $\mathrm{Gal}(L/K)$ est isomorphe à un sous-groupe de $\mathrm{S}_{n_1} \times \mathrm{S}_{n_2}$.

ii. $\mathrm{Gal}(L/K)$ est isomorphe à $\mathrm{Gal}(L/L_1) \times \mathrm{Gal}(L/L_2)$.

iii. $\mathrm{Gal}(L/K)$ est isomorphe à $\mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$.

4.25 Soient K un corps infini, L une extension de K et A une K-algèbre. Supposons que $\phi_1, \ldots, \phi_n \colon A \to L$ sont des K-morphismes distincts et que $f \in L[X_1, \ldots, X_n]$ est un polynôme tel que

$$f(\phi_1(x), \ldots, \phi_n(x)) = 0 \quad \text{pour tout } x \in A.$$

Le but de cet exercice est de montrer que dans ce cas $f = 0$. On peut résumer ce résultat en disant que les morphismes $\phi_1, \ldots, \phi_n$ sont *algébriquement indépendants*.

(a) Soit $g \in L[Y_1, \ldots, Y_m]$ un polynôme tel que $g(\alpha_1, \ldots, \alpha_m) = 0$ pour tous $\alpha_1, \ldots, \alpha_m \in K$. Montrer par récurrence sur m que $g = 0$.

(b) Soit

$$B = \{(\phi_1(a), \ldots, \phi_n(a)) \mid a \in A\} \subset L^n.$$

Montrer que B engendre L^n en tant que L-espace vectoriel. En déduire qu'il existe $a_1, \ldots, a_n \in A$ tels que la matrice $M = (\phi_i(a_j)) \in \mathrm{Mat}_n(L)$ soit inversible.

(c) Soit $g \in L[Y_1, \ldots, Y_n]$ défini par

$$g(Y_1, \ldots, Y_n) = f\left(\sum_{j=1}^{n} \phi_1(a_j)Y_j, \ldots, \sum_{j=1}^{n} \phi_n(a_j)Y_j\right)$$

vérifie $g(y_1, \ldots, y_n) = 0$ pour tout $(y_1, \ldots, y_n) \in K^n$ et en déduire que $g = 0$.

(d) Montrer que $f = 0$.

(e) Montrer que la condition que F soit infini est essentielle.

4.26 Soit L/K une extension galoisienne finie de corps.

(a) Soit $\alpha \in L$. Montrer que l'ordre de l'orbite de α sous l'action de $\mathrm{Gal}(L/K)$ est égal au degré de α sur K.

(b) Montrer que pour tout $\alpha \in L$ l'extension $L/K(\alpha)$ est galoisienne.

(c) Soit $M \subset L$ une sous-extension de K. Montrer que L/M est une extension galoisienne. (Indication : Utiliser une récurrence sur le nombre de générateurs de M sur K.)

4.27 Soient L/K une extension galoisienne finie de corps et $M \subset L$ une sous-extension de K.

(a) Soit $\alpha \in L$ avec $\alpha \notin M$. Montrer qu'il existe un morphisme de M-algèbres $f\colon M(\alpha) \to L$ vérifiant $f(\alpha) \neq \alpha$.

(b) Montrer que f se prolonge en $\tilde{f} \in \mathrm{Gal}(L/M)$ avec $\tilde{f}(\alpha) \neq \alpha$.

(c) Montrer que L/M est une extension galoisienne.

4.28 Soient k un corps, $K = k(T)$ le corps des fractions rationnelles à coefficients dans k et

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,k).$$

(a) Montrer que $\frac{aT+b}{cT+d} \in K$ est transcendant sur k.

(b) Montrer qu'il existe un unique morphisme de k-algèbres $\phi_A\colon K \to K$ tel que $\phi_A(T) = \frac{aT+b}{cT+d}$.

(c) Montrer que l'application

$$\begin{aligned} K \times \mathrm{GL}(2,k) &\to K \\ (R, A) &\mapsto \phi_A(R) \end{aligned}$$

définit une action à droite de $\mathrm{GL}(2,k)$ sur K par des automorphismes de k-algèbres.

4.29 Soient k un corps et $K = k(T)$. Fixons $R \in K$ avec $R \notin k$ et posons $L = k(R) \subset K$. On écrit $R = \frac{P}{Q}$ avec $P, Q \in k[T]$ premiers entre eux et $Q \neq 0$ et on note $n = \max(\deg(P), \deg(Q))$.

(a) Montrer que T est de degré au plus n sur L. En déduite que $[K : L] \leq n$.

(b) On veut montrer que $[K : L] = n$. En considérant $R - \lambda$ pour $\lambda \in k$ convenable, se ramener au cas où $\deg(P) \neq \deg(Q)$.

(c) On suppose désormais que $\deg(P) \neq \deg(Q)$. Soient $F_i(X,Y) \in k[X,Y]$, pour $i = 0, \ldots, n-1$, des polynômes homogènes tels que

$$\sum_{i=0}^{n-1} F_i(P,Q)X^i = 0.$$

Montrer que $F_i(X,Y) = 0$ pour $i = 0, \ldots, n-1$.

(d) Déduire de la question précédente que le système $1, X, \ldots, X^{n-1}$ est libre sur L et conclure que $[L : K] = n$.

4.30 Soient k un corps et $K = k(T)$ comme dans l'exercice 4.29. Le but de cet exercice est de montrer que le groupe $\mathrm{Aut}_k(K)$ des k-automorphismes de K est isomorphe à $\mathrm{PGL}(2,k) = \mathrm{GL}(2,k)/k^\times$.

(a) En utilisant l'exercice 4.28, montrer qu'il existe un morphisme injectif

$$\phi\colon \mathrm{PGL}(2,k) \to \mathrm{Aut}_k(K).$$

(Attention : $\mathrm{Aut}_k(K)$ opère à gauche sur K.)

(b) Soit $f\colon K \to K$ un k-automorphisme. Utiliser l'exercice 4.29 pour montrer qu'il existe $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2,k)$ telle que $f(T) = \frac{aT+b}{cT+d}$. Conclure que ϕ est un isomorphisme.

4.31 Soient les notations comme dans l'exercice 4.30.

(a) Si k est fini, montrer que $\mathrm{PGL}(2,k)$ est fini. En déduire que $K^{\mathrm{PGL}(2,k)} \neq k$.

(b) Supposez que k soit infini. Déterminer $K^{\mathrm{PGL}(2,k)}$.

5 Corps finis

5.1 Soit k un corps de caractéristique $p > 0$.

(a) Montrer que l'application $\sigma\colon k \to k$ définie par $x \mapsto x^p$ est un morphisme de corps. On dit que σ est l'endomorphisme de *Frobenius* de k.

(b) Montrer que si k est fini, alors σ est un automorphisme.

(c) Soient $d \geq 1$ un entier et $q = p^d$. Montrer que l'ensemble des racines du polynôme $X^q - X$ est un sous-corps de k.

5.2 Soit k un corps fini.

(a) Montrer que k est de caractéristique $p > 0$ et que le corps premier k_0 de k s'identifie à $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

(b) Montrer que k est une extension finie de k_0 et en déduire que $|k| = p^d$ pour $d \geq 1$ un entier.

(c) Soit $q = |k|$. Montrer que k est l'ensemble des racines de $X^q - X$ et en déduire que k est un corps de décomposition de $X^q - X$ sur $\mathbf{F}_p$.

5.3 Démontrer le théorème 5.1 en montrant qu'un corps k d'ordre $q = p^d$ est un corps de décomposition de $X^q - X$ sur $\mathbf{F}_p$ et que, réciproquement, tout corps de décomposition de $X^q - X$ sur $\mathbf{F}_p$ est un corps d'ordre q.

Théorème 5.1

– *Soit q un entier. Il existe un corps fini d'ordre q si et seulement s'il existe un nombre premier p et un entier $d \geq 1$ tels que $q = p^d$.*

– *Deux corps finis sont isomorphes si et seulement s'ils ont le même ordre.*

5.4 Soient p un nombre premier et $d, d' \geq 1$ des entiers tels que $d'|d$.

(a) Montrer que (pour tout anneau A) le polynôme $Y^{d'} - 1$ divise $Y^d - 1$ dans $A[X]$.

(b) Soient $q' = p^{d'}$ et $q = p^d$. Montrer que $q' - 1$ divise $q - 1$.

(c) Montrer que $X^{q'} - X$ divise $X^q - X$ dans $\mathbf{F}_p[X]$.

(d) Soit k un corps fini d'ordre q. Montrer que l'ensemble des racines de $X^{q'} - X$ dans k est un sous-corps d'ordre q'.

(e) Démontrer le théorème 5.2.

Théorème 5.2 *Soient p un nombre premier, $d, d' \geq 1$ des entiers, $q = p^d$ et $q' = p^{d'}$. Soit k un corps fini d'ordre q. Alors k contient un sous-corps d'ordre q' si et seulement si d' divise d. Si c'est le cas, alors ce sous-corps est unique.*

Pour $q = p^d$ on désigne parfois par $\mathbf{F}_q$ un corps d'ordre q mais c'est un notation à utiliser avec précaution. En effet, $\mathbf{F}_q$ n'est déterminé qu'à isomorphisme (non-canonique) près. Si d' divise d et $q' = p^{d'}$, alors $\mathbf{F}_{q'}$ est isomorphe à un sous-corps de $\mathbf{F}_q$, mais l'inclusion $\mathbf{F}_{q'} \hookrightarrow \mathbf{F}_q$ n'est pas définie.

5.5 Soient k' un corps fini et k une extension finie de k'. On note p la caractéristique de k' (et de k) et on fixe d', d tels que $|k'| = p^{d'}$ et $|k| = p^d$. D'après le théorème 5.2, on a $d'|d$.

(a) Montrer que $[k : k'] = d/d'$.

(b) Soit $\sigma\colon k \to k$ comme dans l'exercice 5.1. Montrer que $\sigma^{d'} \in \mathrm{Gal}(k/k')$.

(c) Calculer l'ordre de $\sigma^{d'}$ dans le groupe $\mathrm{Gal}(k/k')$.

(d) Démontrer le théorème 5.3.

Théorème 5.3 *Soient k' un corps fini, d'ordre $p^{d'}$, et k une extension finie de k'. Alors k/k' est une extension galoisienne. Le groupe $\mathrm{Gal}(k/k')$ est cyclique, engendré par $\sigma^{d'}$ où $\sigma\colon k \to k$ est comme dans l'exercice 5.1.*

5.6 Soit k un corps fini d'ordre q. En utilisant le fait que le groupe multiplicatif $k^\times$ est l'ensemble des racines de $X^{q-1} - 1$, démontrer le théorème 5.4.

Théorème 5.4 *Si k est un corps fini alors le groupe multiplicatif $k^\times$ est cyclique.*

5.7 Soient k un corps fini et $p = \mathrm{car}(k)$.

(a) Soit α un générateur de $k^\times$. Montrer que $k = \mathbf{F}_p(\alpha)$.

(b) Démontrer le corollaire 5.5.

(c) Démontrer la première partie du corollaire 5.6.

5.8 Soient p un nombre premier, $d, d' \geq 1$ des entiers et $P \in \mathbf{F}_p[X]$ irréductible de degré d'. On note $q = p^d$ et $q' = p^{d'}$.

(a) Supposez que d' divise d. En utilisant le fait que $\mathbf{F}_p[X]/(P)$ est un corps de décomposition de $X^{q'} - X$ sur $\mathbf{F}_p$, montrer que P divise $X^{q'} - X$ et $X^q - X$.

(b) Supposez que P divise $X^q - X$. Montrer que d' divise d. (Indication : Si k est un corps de décomposition de $X^q - X$ sur $\mathbf{F}_p$, montrer que k contient un sous-corps isomorphe à $\mathbf{F}_p[X]/(P)$.)

(c) Démontrer la seconde partie du corollaire 5.6.

Corollaire 5.5 *Soit k un corps fini de caractéristique p. Alors il existe un polynôme irréductible $P \in \mathbf{F}_p[X]$ tel que $k \cong \mathbf{F}_p[X]/(P)$.*

Corollaire 5.6 *Soit p un nombre premier.*
– *Pour tout entier $d \geq 1$ il existe un polynôme irréductible $P \in \mathbf{F}_p[X]$ de degré d.*
– *Soient $d \geq 1$ un entier et $q = p^d$. Le polynôme $X^q - X$ est le produit des polynômes irréductibles unitaires dans $\mathbf{F}_p[X]$ de degrés divisant d.*

5.9 Dans tout l'exercice, p désigne un nombre premier et $n \geq 1$ un entier. Les affirmations suivantes sont-elles vraies ? Justifier votre réponse.

(a) Si K est un corps fini, alors $(K^\times, \cdot)$ est cyclique.

(b) Si $P \in \mathbf{F}_p[X]$ est un polynôme irréductible, alors $\mathbf{F}_p[X]/(P)$ est un corps de décomposition de $P(X)$.

(c) Soient $P, Q \in \mathbf{F}_p[X]$ irréductibles. Alors $\mathbf{F}_p[X]/(P) \cong \mathbf{F}_p[X]/(Q)$ si et seulement si $\deg(P) = \deg(Q)$.

(d) Si α est un générateur de $\mathbf{F}_{p^n}^\times$, son polynôme minimal sur $\mathbf{F}_p$ est de degré n.

(e) Si $\alpha \in \mathbf{F}_{p^n}^\times$ est de degré n sur $\mathbf{F}_p$, alors α est un générateur de $\mathbf{F}_{p^n}^\times$.

(f) Si α est un générateur de $\mathbf{F}_{p^n}^\times$, toute racine de son polynôme minimal sur $\mathbf{F}_p$ est aussi un générateur de $\mathbf{F}_{p^n}^\times$.

(g) Si $\alpha \in \mathbf{F}_{p^n}^\times$, toutes les racines de son polynôme minimal sur $\mathbf{F}_p$ ont le même ordre dans $\mathbf{F}_{p^n}^\times$.

(h) $\mathbf{F}_{p^n}^\times$ admet exactement n générateurs.

(i) Il existe une $\mathbf{F}_p$-base $(1, \alpha, \ldots, \alpha^{n-1})$ de $\mathbf{F}_{p^n}$ où α est un générateur de $\mathbf{F}_{p^n}^\times$.

(j) Il existe un polynôme irréductible $P \in \mathbf{F}_p[X]$ de degré n tel que la classe de X dans $\mathbf{F}_p[X]/(P)$ engendre $(\mathbf{F}_p[X]/(P))^\times$.

5.10 (a) Trouver les polynômes irréductibles sur $\mathbf{F}_2$ de degrés 2 et 4. Déterminer le nombre de polynômes irréductibles de degré 8 dans $\mathbf{F}_2[X]$.

(b) Trouver les polynômes irréductibles unitaires de degré 2 sur $\mathbf{F}_3$. Vérifier que $X^9 - X$ est le produit des polynômes irréductibles unitaires de degrés 1 et 2.

(c) Combien y a-t-il de polynômes irréductibles unitaires de degré 4 dans $\mathbf{F}_3[X]$?

(d) Trouver le produit des polynômes irréductibles unitaires sur $\mathbf{F}_2$ de degré 5.

(e) Trouver le produit des polynômes irréductibles unitaires dans $\mathbf{F}_3[X]$ de degré 6.

5.11 Soient p un entier premier et n un entier strictement positif.

(a) Trouver la somme des éléments de $\mathbf{F}_{p^n}$.

(b) Trouver le produit des éléments de $\mathbf{F}_{p^n}^\times$.

5.12 Trouver l'ordre du corps de décomposition de chacun des polynômes suivants sur les corps donnés. Si le degré sur le corps premier est au plus 4, trouver aussi un polynôme $P \in \mathbf{F}_p[X]$ tel que le corps de décomposition soit isomorphe à $\mathbf{F}_p[X]/(P)$.

(a) De $X^2 + X + 1$, $X^3 + 1$, $X^4 + 1$, $X^4 - X$, $X^4 + X^2 + 1$ et de $X^4 + X + 1$ sur $\mathbf{F}_2$, $\mathbf{F}_4$ et sur $\mathbf{F}_8$

(b) De $X^2 + X + 1$, $X^2 + X + 2$, $X^3 + 2$ et de $X^3 + 2X + 1$ sur $\mathbf{F}_3$, $\mathbf{F}_9$ et sur $\mathbf{F}_{27}$.

5.13 (a) Pour tout $n > 0$, trouver l'ordre d'un corps de décomposition de $X^2 + X + 1$ sur $\mathbf{F}_{2^n}$.

(b) Pour tout $n > 0$, trouver l'ordre d'un corps de décomposition de $X^3 - X + 1$ sur $\mathbf{F}_{3^n}$.

5.14 (a) Pour quels éléments $c \in \mathbf{F}_7$ est-ce que le polynôme $X^3 - c$ est irréductible sur $\mathbf{F}_7$?

(b) Soient $K = \mathbf{F}_7[X]/(X^3 - 2)$ et $\alpha = \bar{X} \in K$. Trouver l'ordre de α dans $K^\times$.

(c) Trouver un élément $\beta = a + b\alpha \in K$ (a et $b \in \mathbf{F}_7$) d'ordre 19. (Indication : calculer β^7 et remarquer que $21 = 19 + 2$.)

(d) Trouver un générateur de $K^\times$ ansi que son polynôme minimal sur $\mathbf{F}_7$.

5.15 Soient $K_1 = \mathbf{F}_5[X]/(X^2 + 2)$ et $K_2 = \mathbf{F}_5[X]/(X^2 + X + 2)$. On note $\alpha = \bar{X} \in K_1$.

(a) Montrer que K_1 et K_2 sont des corps.

(b) Trouver les $\beta \in K_2$ tels qu'il existe un isomorphisme $f\colon K_1 \to K_2$ avec $f(\alpha) = \beta$.

5.16 Dans $\mathbf{F}_2[X]$, on considère les trois polynômes suivants :

$$P_1(X) = X^4 + X + 1, \quad P_2(X) = X^4 + X^3 + 1, \quad P_3(X) = X^4 + X^3 + X^2 + X + 1.$$

et on pose $K_i = \mathbf{F}_2[X]/(P_i)$ $(1 \leq i \leq 3)$.

(a) Montrer que les K_i sont des corps, extensions de $\mathbf{F}_2$ et qu'ils sont deux à deux $\mathbf{F}_2$-isomorphes.

(b) Trouver un $\mathbf{F}_2$-isomorphisme $f\colon K_1 \to K_3$. Donner la matrice de f par rapport aux bases $(1, \bar{X}, \bar{X}^2, \bar{X}^3)$ de K_1 et $(1, \bar{X}, \bar{X}^2, \bar{X}^3)$ de K_3.

(c) Trouver un générateur de $K_i^\times$ pour $1 \leq i \leq 3$.

5.17 Soient p un nombre premier, $P \in \mathbf{F}_p[X]$, K une extension de $\mathbf{F}_p$ et $\alpha \in K$ une racine de P.

(a) Montrer que pour tout entier $i \geq 0$, $P(\alpha^{p^i}) = 0$.

(b) Supposer que P est irréductible. Montrer que P est décomposé sur K et que les racines de P dans sont les α^{p^i} pour $i = 0, \ldots, \deg(P) - 1$.

(c) Soient $p = 7$, $K = \mathbf{F}_7[X]/(X^3+X+1)$ et $\alpha = \bar{X} \in K$. Trouver des expressions de la forme $a + b\alpha + c\alpha^2$ (avec $a, b, c \in \mathbf{F}_7$) pour les racines de $X^3 + X + 1$ dans K.

5.18 Soient p un nombre premier et $\bar{\mathbf{F}}_p$ une clôture algébrique de $\mathbf{F}_p$. Pour tout entier $k \geq 1$ on note $\mathbf{F}_{p^k}$ l'ensemble des racines de $X^{p^k} - X$ dans $\bar{\mathbf{F}}_p$. Soient $n, m \geq 1$ des entiers.

(a) Montrer que $\mathbf{F}_{p^n}$ est un sous-corps de $\bar{\mathbf{F}}_p$. En déduire qu'il existe exactement un sous-corps de $\bar{\mathbf{F}}_p$ à p^n éléments.

(b) Montrer que $\mathbf{F}_{p^m}$ est un sous-corps de $\mathbf{F}_{p^n}$ si et seulement si $m|n$.

(c) Montrer que si $m|n$, alors il existe exactement un sous-corps de $\mathbf{F}_{p^n}$ à p^m éléments.

5.19 Trouver les corps intermédiaires entre $\mathbf{F}_2$ et $\mathbf{F}_{2^{12}}$ et indiquer les relations d'inclusion entre eux. Pour chaque corps intermédiaire trouver le sous-groupe de $\mathrm{Gal}(\mathbf{F}_{2^{12}}/\mathbf{F}_2)$ correspondant et indiquer les relations d'inclusion entre ces sous-groupes.