Extensions de corps

Exercice 1. [Quelques cas particuliers intéressants]

(*a*) Montrer que sur un corps K de caractéristique p, tout élément a exactement une racine p-ième. En déduire le nombre maximal de racines n-ièmes de l'unité dans K.

(*b*) Soit K un corps quelconque et $L = K(X)$. Montrer que pour toute fraction rationnelle non constante $R = P/Q$, l'extension $K(X)/K(R)$ est finie. En déduire que l'extension $K(R)/K$ est infinie.

Exercice 2. [Corps de décomposition et extension normale]

Une extension L de K est *normale* si tout polynôme irréductible de $K[X]$ ayant une racine dans L est scindé sur L.

(*a*) Donner les corps de décomposition sur $\mathbb{Q}$ des polynômes X^2+X+1, $(X^3-2)(X^2-2)$, (X^5-7) et leurs degrés.

(*b*) Montrer que le corps de décomposition d'un polynôme de degré au plus n est de degré au plus $n!$.

(*c*) Si $P \in K[X]$, L est le corps de décomposition de P sur K et K' une extension intermédiaire entre K et L, montrer que le corps de décomposition de P sur K' est encore L.

(*d*) En déduire que tout corps de décomposition sur K est une extension normale de K.

(*e*) Réciproquement, montrer que toute extension normale finie de K est un corps de décomposition sur K.

(*f*) Montrer que L/K finie est normale si et seulement si il y a autant d'automorphismes de L sur K que de K-plongements de L dans $\overline{K}$.

Exercice 3. [Résultant et polynômes minimaux]

Soit A un anneau commutatif unitaire et

$$P = \sum_{k=0}^{m} a_k X^k, \quad Q = \sum_{\ell=0}^{n} b_\ell X^\ell \in A[X]$$

de degrés respectifs m et n supérieurs ou égaux à 1. Le *résultant* de P et Q, noté $\mathrm{Res}(P,Q)$, est alors le déterminant de la matrice de taille $(m+n)$

$$\begin{pmatrix}
a_m & 0 & \cdots & 0 & b_n & 0 & \cdots 0 & \\
a_{m-1} & a_m & \ddots & \vdots & \vdots & b_n & \ddots & \vdots \\
\vdots & a_{m-1} & \ddots & 0 & \vdots & & \ddots & 0 \\
\vdots & \vdots & \ddots & a_m & b_1 & & & b_n \\
a_0 & & & a_{m-1} & b_0 & \ddots & \vdots & \vdots \\
0 & \ddots & & \vdots & 0 & \ddots & b_1 & \vdots \\
\vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 & b_1 \\
0 & \cdots & 0 & a_0 & 0 & \cdots & 0 & b_0
\end{pmatrix}$$

(*a*) Montrer que c'est le déterminant de $(S,T) \mapsto PS+QT$ de $A_{n-1}[X] \times A_{m-1}[X]$ à $A_{m+n-1}[X]$ pour certains choix naturels de base de ces espaces. Comparer $\mathrm{Res}(P,Q)$ et $\mathrm{Res}(Q,P)$, et $\mathrm{Res}(aP,bQ)$ à $\mathrm{Res}(P,Q)$ si a et b ne sont pas diviseurs de zéro.

(*b*) Montrer que si $\varphi : A \to B$ est un morphisme d'anneaux,

$$\mathrm{Res}(\varphi(P),\varphi(Q)) = \varphi(\mathrm{Res}(P,Q))$$

pour le morphisme induit $\varphi : A[X] \to B[X]$ (terme à terme sur les coefficients), si $\deg \varphi(P) = m$ et $\deg \varphi(Q) = n$. Que peut-on dire si $\deg \varphi(P) = m$ et $\deg \varphi(Q) < n$?

(*c*) On suppose ici que A est un anneau intègre et $K = \operatorname{Frac} A$. Montrer que $\operatorname{Res}(P, Q)$ est le déterminant de la multiplication par $\overline{Q}$ dans $K[X]/(P)$. En déduire que pour tous polynômes non constants $P, Q, R \in A[X]$,

$$\operatorname{Res}(P, QR) = \operatorname{Res}(P, Q) \operatorname{Res}(P, R),$$

et que si

$$P = a \prod_{i=1}^{m} (X - \alpha_i), \quad Q = b \prod_{j=1}^{n} (X - \beta_j),$$

alors

$$\operatorname{Res}(P, Q) = a^n b^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j).$$

(*d*) Si $Q + PS$ est un polynôme de degré au plus n, donner une relation entre $\operatorname{Res}(P, Q)$ et $\operatorname{Res}(P, Q + PS)$. En déduire un algorithme efficace de calcul du résultant.

(*e*) Montrer que sur un anneau factoriel A, $\operatorname{Res}(P, Q) = 0$ si et seulement si P et Q n'ont pas de facteur commun non constant.

(*f*) Soit K un corps et $A = K[X_1, \cdots, X_{n-1}]$. Soient $P, Q \in K[X_1, \cdots, X_n, X]$, on note $\operatorname{Res}_X(P, Q)$ le résultant de P et Q vus comme polynômes dans $A[X]$. C'est donc un polynôme en $n - 1$ variables sur K. Montrer que pour tout $(x_1, \cdots, x_{n-1}) \in K^{n-1}$,

$$(\operatorname{Res}_X(P, Q))(x_1, \cdots, x_{n-1}) = 0 \Longleftrightarrow \exists x \in \overline{K}, P(x_1, \cdots, x_{n-1}, x) = Q(x_1, \cdots, x_{n-1}, x) = 0$$

à moins que les coefficients dominants de P ou Q soient nuls en $(x_1, \cdots, x_{n-1})$.

(*g*) On va maintenant appliquer ce résultat aux nombres algébriques : si $\alpha \in \overline{\mathbb{Q}}$ et $\beta \in \overline{\mathbb{Q}}$ sont deux nombres algébriques de polynômes minimaux respectifs P et Q, considérer

$$\operatorname{Res}_T(P(X), Q(T - X)), \operatorname{Res}_T(P(X), X^{\deg Q} Q(T/X)).$$

En déduire des polynômes annulateurs de $\alpha + \beta$ et $\alpha\beta$.

(*h*) Faire de même pour trouver un polynôme annulateur de $R(\alpha)$ avec $R \in \mathbb{Q}[X]$.

(*i*) Appliquer cette méthode à $\sqrt{2} + \sqrt{3}, 2\sqrt{7} - j, \sqrt[5]{3} + i$.

Exercice 4. [Extensions séparables]

Un polynôme $P \in K[X]$ est *séparable* si dans une (toute) extension où il est scindé, il est à racines simples. Un élément α algébrique sur K est *séparable* sur K si son polynôme minimal sur K est séparable. Une extension algébrique L/K est *séparable* si tous ses éléments sont séparables sur K.

(*a*) Montrer que P est séparable si et seulement si P et P' sont premiers entre eux. Montrer que pour un polynôme irréductible P, si $\operatorname{car}(K) = 0$, P est toujours séparable, et que si $\operatorname{car}(K) = p$ premier, P est séparable si et seulement si il ne s'écrit pas $P = Q(X^p)$ avec $Q \in K[X]$.

(*b*) Montrer qu'une extension finie L/K est séparable si et seulement si il y a exactement $[L : K]$ K-plongements distincts de L dans $\overline{K}$.

(*c*) Montrer qu'une extension finie L/K est séparable si et seulement si elle est engendrée par des éléments séparables sur K.

(*d*) Un corps K est *parfait* si toute extension finie de K est automatiquement séparable. Montrer que tout corps de caractéristique 0 est parfait, et que si $\operatorname{car}(K) = p$, K est parfait si et seulement si son automorphisme de Frobenius $x \mapsto x^p$ est surjectif.

Exercice 5. [Théorème de l'élément primitif]

Le *théorème de l'élément primitif* dit que pour toute extension finie séparable L/K, il existe $\alpha \in L$ tel que $L = K[\alpha]$ (autrement dit, on peut engendrer L par un seul élément et non plusieurs). Le but de cet exercice est de prouver le théorème.

(*a*) Montrer le théorème si L et K sont des corps finis. On suppose maintenant qu'ils sont infinis.

(*b*) Montrer qu'il suffit de prouver le théorème pour $L = K[\alpha, \beta]$ avec certains éléments α, β, ce qu'on suppose pour la suite.

On pose $\alpha_1 = \alpha, \cdots, \alpha_n$ les conjugués (distincts) de α dans $\overline{K}$ et $\beta_1, \cdots, \beta_m$ les conjugués (distincts) de β dans $\overline{K}$. On choisit $\lambda \in K$ différent des $(\alpha - \alpha_i)/(\beta - \beta_j)$ pour tous $1 < i \leq n, 1 < j \leq m$. On va montrer que $\Theta = \alpha + \lambda\beta$ est primitif (i.e $L = K[\Theta]$).

(*c*) On note P et Q les polynômes minimaux respectifs de α et β sur K. Montrer que le polynôme minimal de β sur $K[\Theta]$ divise à la fois Q et $P(\Theta - \lambda X)$. En déduire qu'il est de degré 1 grâce à notre choix de λ (et car L/K est séparable), donc que $K[\beta] \subset K[\Theta]$. Conclure.

(*d*) (*Preuve théorique*) Supposons L/K séparable de degré n, et $\sigma_1, \cdots, \sigma_n$ les plongements distincts de L dans $\overline{K}$. Montrer que pour $1 \leq i < j \leq n$ l'ensemble $V_{i,j} = \{x \in L, \sigma_i(x) = \sigma_j(x)\}$ est un K-espace vectoriel, et que leur réunion ne peut pas être tout L si L est infini. En déduire le théorème de l'élément primitif dans ce cas.

(*e*) Déduire du théorème de l'élément primitif qu'une extension séparable finie L/K n'a qu'un nombre fini de sous-extensions.

Exercice 6. [Extensions galoisiennes]

Une extension finie L/K est *galoisienne* si elle est à la fois normale et séparable.

(*a*) Montrer que L/K finie est galoisienne si et seulement si elle a exactement $[L : K]$ K-automorphismes : on note le groupe des automorphismes $\mathrm{Gal}(L/K)$, et on l'appelle groupe de Galois de L sur K.

(*b*) Montrer que L/K finie est galoisienne si et seulement si c'est le corps de décomposition d'un polynôme séparable sur K. En déduire que si $K \subset K' \subset L$ et L/K est galoisienne, alors L/K' est galoisienne et $\mathrm{Gal}(L/K') = \{\sigma \in \mathrm{Gal}(L/K), \sigma_{|K'} = \mathrm{Id}_{K'}\}$. Trouver un contre-exemple pour K'/K.

(*c*) (*Lemme d'Artin*)Pour L un corps et G un groupe fini d'automorphismes de L, montrer que L/L^G est galoisienne de groupe de Galois G.

(*d*) (*Correspondance de Galois*) Supposons que L/K est finie galoisienne. Montrer que les applications $H \mapsto L^H$ et $K' \mapsto \mathrm{Gal}(L/K')$ sont des bijections réciproques entre les sous-groupes de $\mathrm{Gal}(L/K)$ et les sous-extensions de L/K. Comment caractériser les sous-extensions telles que K'/K est encore de Galois ?

(*e*) Montrer que toute extension finie de corps finis est galoisienne et décrire son groupe de Galois.

(*f*) Pour $n \geq 1$, montrer que l'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est galoisienne et que son groupe de Galois est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$.

(*g*) Montrer que toute extension de degré 2 entre deux corps de caractéristique différente de 2 est galoisienne.