Extensions de corps

Exercice 1. [Résultats importants de base]

(*a*) *(Base téléscopique)* Soit $K \subset L \subset M$ une suite de corps avec M/L et L/K finies. Soient $(e_1, \cdots, e_m)$ une K-base de L et $(f_1, \cdots, f_n)$ une L-base de M.

Montrer que $(e_i f_j)_{1 \leq i \leq m, 1 \leq j \leq n}$ est une K-base de M, et en déduire que

$$[M : K] = [M : L][L : K].$$

Que peut-on en déduire sur les sous-extensions d'une extension de corps donnée ?

(*b*) Montrer que si L est une extension algébrique de K, tout morphisme de corps $\sigma : L \to L$ est un automorphisme.

(*c*) Si $L = K[\alpha]$ avec $P \in K[X]$ le polynôme minimal de α sur K et M est une autre extension de K, montrer que l'inclusion $K \to M$ se prolonge à L si et seulement si P a une racine dans M. Donner une borne sur le nombre maximal de plongements K-linéaires possibles de $K[\alpha]$ dans M.

Exercice 2. [Quelques exercices pour s'échauffer]

(*a*) Si α et β sont algébriques sur K de degrés respectifs m et n qui sont premiers entre eux, montrer que

$$[K(\alpha, \beta) : K] = mn = [K(\alpha) : K][K(\beta) : K].$$

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

(*c*) Donner un exemple d'extension L/K (infinie) telle que les seuls éléments de L algébriques sur K sont les éléments de K.

Exercice 3. [Construction de la clôture algébrique]

On fixe un corps K quelconque.

(*a*) Soit S l'ensemble des polynômes irréductibles de $K[X]$. On pose $A = K[(X_P)_{P \in S}]$ et I l'idéal de A engendré par les $P(X_P), P \in S$. Montrer que $I \neq A$.

(*b*) En prenant $\mathfrak{m}$ un idéal maximal de A contenant I, montrer que dans l'extension $K_1 = A/\mathfrak{m}$ de K, tout polynôme irréductible de $K[X]$ a une racine.

(*c*) Itérer le procédé pour construire une suite d'extensions de corps

$$K \subset K_1 \subset K_2 \subset \cdots$$

et montrer que $K_\infty = \bigcup_{n \in \mathbb{N}} K_n$ est un corps algébriquement clos.

(*d*) En posant $\overline{K}$ l'ensemble des éléments de K_∞ algébriques sur K, montrer que $\overline{K}$ est bien une clôture algébrique de K.

(*e*) Pour toute extension algébrique L de K, montrer qu'il existe un plongement de L dans $\overline{K}$ prolongeant l'inclusion $K \subset \overline{K}$. En déduire que la clôture algébrique de K est unique à isomorphisme près.

(*f*) Montrer que pour toute extension finie L de $\overline{K}$, il existe au plus $[L : K]$ plongements K-linéaires distincts de L dans $\overline{K}$. On note $[L : K]_s$ le nombre de ces plongements. Montrer que pour une extension finie M de L, $[M : K]_s = [M : L]_s [L : K]_s$ (utile pour l'exercice sur les extensions séparables).

Exercice 4. [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 5. [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 si $\mathrm{car}(K)=0$, P est toujours séparable, et que si $\mathrm{car}(K)=p$ 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 $\mathrm{car}(K)=p$, K est parfait si et seulement si son automorphisme de Frobenius $x \mapsto x^p$ est surjectif.

Exercice 6. [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 qu'il est immédiat 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 7. [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.