TD 7
Vers la théorie de Galois

Exercice 1 (Extensions purement inséparables). Une extension algébrique L/K est dite *purement inséparable* si tout élément de L séparable sur K est dans K.

1. Soit L/K une extension algébrique avec K de caractéristique strictement positive p. Montrer que les conditions suivantes sont équivalentes :
   (a) l'extension L/K est purement inséparable ;
   (b) pour tout élément α de L, il existe $n \geq 0$ tel que α^{p^n} appartienne à K ;
   (c) tout élément de L a un polynôme minimal sur K de la forme $X^{p^n} - a$ pour un $n \geq 0$ et un a dans K.
2. Soit L/K une extension finie purement inséparable, avec K de caractéristique strictement positive p. Montrer le degré de L/K est une puissance de p.
3. Donner un exemple non trivial d'extension purement inséparable.

Exercice 2 (Degrés de séparabilité et d'inséparabilité). Soit L/K une extension algébrique.

1. On appelle *clôture séparable* de K dans L l'ensemble K^{s} formé des éléments de L séparables sur K. Montrer que K^{s} est un sous-corps de L.
2. Montrer que l'extension L/K^{s} est purement inséparable.
3. On appelle *degré de séparabilité* (respectivement *degré d'inséparabilité*) de L/K le degré de l'extension K^{s}/K (respectivement de l'extension L/K^{s}). Que signifie que le degré de séparabilité (respectivement d'inséparabilité) vaut 1 ?
4. On suppose que l'extension L/K n'est pas séparable. En déduire que la caractéristique de K divise le degré de L sur K.

Exercice 3 (Transitivité de la séparabilité). Soient K/k et L/K deux extensions séparables. Montrer que L/k est une extension séparable. (On pourra utiliser l'exercice précédent.)

Exercice 4 (Finitude du nombre de sous-corps intermédiaires). Soient L/K une extension finie et $\mathcal{E}$ l'ensemble des extensions intermédiaires de L/K, *i.e.* des corps E telles que $K \subset E \subset L$. Le but de cet exercice est de démontrer que $\mathcal{E}$ est fini si et seulement si l'extension L/K est monogène.

1. Supposons $\mathcal{E}$ fini.
   (a) Montrer que L/K est monogène si K est un corps fini.

(b) On suppose maintenant K infini et L engendrée sur K par deux éléments α et β. Montrer qu'il existe c dans K tel que L soit engendrée sur K par $\alpha + c\beta$.

(c) Conclure.

2. Réciproquement, supposons L engendrée par α sur K.

   (a) Soit E une extension intermédiaire. Montrer que E est engendrée sur K par les coefficients du polynôme minimal de α sur E.

   (b) Conclure.

3. Donner un exemple d'extension L/K finie telle que $\mathcal{E}$ soit infini.

Exercice 5 (Extensions normales). On dit qu'une extension algébrique L/K est *normale* si tout polynôme irréductible de $K[X]$ ayant une racine dans L est scindé sur L. Le but de cet exercice est de démontrer qu'une extension finie L/K est normale si et seulement si L est le corps de décomposition d'un polynôme sur K.

1. Montrer le sens direct de l'énoncé.
2. Réciproquement, soient f un polynôme à coefficients dans K et L le corps de décomposition de f sur K. Notons $\alpha_1, \ldots, \alpha_n$ les racines de f dans L.

   (a) Soit g un polynôme à coefficients dans K admettant une racine $h(\alpha_1, \ldots, \alpha_n)$ dans L. On considère le polynôme
   $$s(X) = \prod_{\sigma \in S_n} \left(X - h(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}\right).$$
   Montrer que s est à coefficients dans K.

   (b) En déduire que L/K est une extension normale.

Exercice 6 (Extensions galoisiennes). On dit qu'une extension algébrique est *galoisienne* si elle est normale et séparable. Si L/K est une extension, on notera $\mathrm{Gal}(L/K)$ le groupe des automorphismes de L qui fixent K élément par élément. On appelle ce groupe le *groupe de Galois* de L/K.

1. Montrer qu'une extension finie L/K est galoisienne si et seulement si L est le corps de décomposition d'un polynôme séparable sur K.
2. Soit L/K une extension galoisienne finie. Montrer que l'ordre de $\mathrm{Gal}(L/K)$ est le degré de L sur K.

Exercice 7 (Corps fixe). Soient L/K une extension finie et G son groupe de Galois. On notera L^G le sous-corps de L formé des α fixés par tout élément de G.

1. On suppose L/K galoisienne. Montrer que $L^G = K$.
2. Réciproquement, supposons $L^G = K$.

   (a) Soit α dans L. Notons $\alpha_1, \ldots, \alpha_r$ les images distinctes de α par les éléments de G. On considère le polynôme
   $$h(X) = \prod_{i=1}^{r} (X - \alpha_i).$$
   Montrer que h est le polynôme minimal de α sur K.

   (b) En déduire que L/K est galoisienne.