École polytechnique 2022-2023
Théorie de Galois

Feuille d'exercices 4

Exercice 1. (*Sous-groupes finis du groupe multiplicatif d'un corps*)

(i) Soient G un groupe et x, y deux éléments d'ordre fini de G. On suppose que $xy = yx$ et que les ordres respectifs n et m de x et y sont premiers entre eux. Montrer que xy est d'ordre fini nm.

On fixe dorénavant un corps k et $G \subseteq k^*$ un sous-groupe fini (multiplicatif).

(ii) Si $n = |G|$, montrer que $X^n - 1$ est scindé dans $k[X]$, ses racines étant exactement les éléments de G. En déduire que, pour tout d divisant n, le polynôme $X^d - 1$ est scindé à racines distinctes dans G.

(iii) Conclure que G est un groupe cyclique d'ordre n.

(On pourra commencer par montrer que, si p^r divise n avec p premier, alors G admet un élément d'ordre p^r, puis on construira un élément d'ordre n dans G.)

(iv) En déduire que, si k est un corps fini, alors k^* est cyclique (*Théorème de Gauss*).

Exercice 2. Soient P un polynôme irréductible dans $k[X]$ de degré d et L son corps de décomposition dans une clôture algébrique fixée de k.

(i) Montrer que $[L : k] \leq d!$. À quelle condition a-t-on égalité ?

(ii) Donner un exemple du cas d'égalité avec $d = 3$.

Exercice 3. Posons $\rho = e^{2i\pi/3}$ et considérons les extensions $K = \mathbf{Q}[\sqrt[3]{2}]$ et $L = K[\rho]$.

(i) Calculer $[K : \mathbf{Q}]$ et déterminer $\mathrm{Hom}_{\mathbf{Q}-\mathrm{alg}}(K, K)$.

(ii) Déterminer $\mathrm{Hom}_{\mathbf{Q}[\rho]\text{-alg}}(L, L)$.

(iii) Montrer que $\mathrm{Hom}_{\mathbf{Q}\text{-alg}}(L, L)$ est isomorphe au groupe $\mathfrak{S}_3$.

Exercice 4. Soit $P(X) = X^3 - X - 1 \in \mathbf{Q}[X]$.

(i) Montrer que P est irréductible sur $\mathbf{Q}$.

(ii) Soit $L = \mathbf{Q}[X]/(P)$ l'extension de degré 3 de $\mathbf{Q}$ correspondante. Montrer que, si x désigne la classe de X dans L, on a l'égalité $\mathbf{Q}[x] = \mathbf{Q}[x^2]$ dans L et exprimer x comme un polynôme en x^2.

(iii) Montrer que P possède une unique racine réelle, qui est un *nombre de Pisot-Vijayaraghavan* [1].

1. On appelle *nombre de Pisot-Vijayaraghavan* toute racine réelle positive d'un polynôme unitaire à coefficients entiers dont les autres racines sont des nombres complexes de module strictement inférieur à un. On peut montrer que la racine réelle

$$\sqrt[3]{\frac{1}{2} + \frac{1}{6}\sqrt{\frac{23}{3}}} + \sqrt[3]{\frac{1}{2} - \frac{1}{6}\sqrt{\frac{23}{3}}} \simeq 1,324717957244746025960$$

de P est le plus petit tel nombre.

Exercice 5. Soient k un corps de caractéristique p et $a \in k$.

(i) Soit $P(X) = X^p - X - a \in k[X]$. Montrer P est irréductible si et seulement s'il ne possède pas de racine.

(ii) Si P est irréductible et K est un corps de rupture de P, que dire du groupe $\mathrm{Hom}_{k\text{-alg}}(K, K)$?

Exercice 6. Soient k un corps et $f = T^d - a_1 T^{d-1} + a_2 T^{d-2} + \cdots + (-1)^d a_d \in k[T]$ un polynôme unitaire de degré d. Soit

$$A = k[X_1, \ldots, X_d]/\big((\sum_i X_i) - a_1, (\sum_{i<j} X_i X_j) - a_2, \ldots, \prod_i X_i - a_n\big).$$

le quotient de l'anneau de polynômes $k[X_1, \ldots, X_d]$ par l'idéal engendré par les

$$\sum_{i_1 < \cdots < i_r} X_{i_1} \cdots X_{i_r} - a_r$$

pour $1 \leq r \leq d$.

(i) Montrer que, par construction, l'image de f dans $A[T]$ est *scindée* sur A : on a l'égalité

$$f = \prod_{i=1}^{d} (T - x_i)$$

dans $A[T]$, où les x_i, $1 \leq i \leq d$, désignent les images des X_i dans A par la surjection canonique $k[X_1, \ldots, X_d] \twoheadrightarrow A$.

(ii) Soit $\mathfrak{m}$ un idéal maximal de A. Montrer que $A/\mathfrak{m}$ est un *corps de décomposition* de f sur k.