THÉORIE DE GALOIS II

Exercice 1 (*Discriminant*) — Soit K un corps et soit $P \in K[T]$ un polynôme séparable sur K de degré n. On désigne par $\mathscr{R}$ l'ensemble des racines de P dans une clôture algébrique de K.

1. Justifier que le groupe de Galois de l'extension $K[\mathscr{R}]/K$ s'identifie à un sous-groupe du groupe symétrique $\mathfrak{S}(\mathscr{R})$.

2. Soit
$$D = (-1)^{\frac{n(n-1)}{2}} \prod_{x \neq y \in \mathscr{R}} (x-y)$$
Vérifier que D est un élément de K puis démontrer que, lorsque K est de caractéristique différente de 2, l'image de $\mathrm{Gal}(K[\mathscr{R}]/K)$ dans $\mathfrak{S}(\mathscr{R})$ est contenue dans le groupe alterné $\mathfrak{A}(\mathscr{R})$ si et seulement si D est un carré dans K. (*Indication : numéroter les racines $\xi_1, \ldots, \xi_n$ de P et considérer l'élément $\prod_{i<j}(\xi_i - \xi_j)$ de $K[\mathscr{R}]$.*)

3. Soit a le coefficient dominant de P. Démontrer les identités
$$a^n D = (-1)^{\frac{n(n-1)}{2}} \prod_{x \in \mathscr{R}} P'(x) \quad \text{et} \quad a^{n-1} D = (-1)^{\frac{n(n-1)}{2}} n^n \prod_{x' \in \mathscr{R}'} P(x'),$$
où $\mathscr{R}'$ est l'ensemble des racines de P' dans une clôture algébrique de K. En déduire D lorsque $P = T^2 + aT + b$ et lorsque $P = T^3 + pT + q$.

Exercice 2 (*Extensions cyclotomiques*) — Soit K un corps et soit $n \geq 1$ un entier naturel premier à la caractéristique de K. On désigne par $K(\mu_n)$ une extension de K engendrée par les racines n-èmes de l'unité.

1. Vérifier que l'extension $K(\mu_n)/K$ est galoisienne.

2. Démontrer qu'il existe un homomorphisme injectif de groupes et un seul
$$\chi : \mathrm{Gal}(K(\mu_n)/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$$
tel que, pour toute racine n-ème de l'unité ζ et tout $\sigma \in \mathrm{Gal}(K(\mu_n)/K)$,
$$\sigma(\zeta) = \zeta^{\chi(\sigma)}.$$

3. Vérifier qu'il existe un unique polynôme unitaire et séparable $\Phi_n \in K[T]$ dont les racines dans toute clôture algébrique $\overline{K}$ de K soient les racines primitives n-èmes de l'unité dans $\overline{K}$ (c'est-à-dire les éléments d'ordre n dans $\overline{K}^\times$) puis justifier que l'homomorphisme χ est un isomorphisme si et seulement si le polynôme Φ_n est irréductible sur K.

4. On suppose $K = \mathbb{Q}$ dans cette question. Soit ζ une racine n-ème primitive de l'unité, de polynôme minimal $P \in \mathbb{Q}[T]$, soit p un nombre premier ne divisant pas n et soit $Q \in \mathbb{Q}[X]$ le polynôme minimal de ζ^p.

(i) Démontrer que les polynômes P et Q sont à coefficients entiers.

(ii) Prouver que $Q(T^p)$ divise P dans $\mathbb{Z}[T]$.

(iii) En déduire que les réductions modulo p de P et Q ont un facteur irréductible commun dans $\mathbb{F}_p[T]$, puis que l'on a $P = Q$.

(iv) En conclusion, démontrer que le polynôme Φ_n est irréductible sur $\mathbb{Q}$ et à coefficients entiers.

Exercice 3 (*Extensions cycliques : théorie de Kummer*) — Soit K un corps et soit $n \geq 2$ un entier naturel. On suppose tout d'abord que le groupe $\mu_n(K)$ des racines n-èmes de l'unité dans K est d'ordre n.

1. Soit $a \in K^\times$ et soit α une racine du polynôme $T^n - a$ dans une clôture algébrique de K.

Démontrer que l'extension $K(\alpha)/K$ est galoisienne et que l'application
$$\mathrm{Gal}(K(\alpha)/K) \to \mu_{\mathbf{n}}(K), \quad \sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$$
est un homomorphisme de groupes injectif, d'image le sous-groupe $\mu_d(K)$ où d est le plus petit entier ≥ 1 tel que $\alpha^d \in K$.

2. Soit L/K une extension galoisienne finie dont le groupe de Galois G est cyclique et d'ordre n, engendré par un élément σ.

Étant donnés un élément α de L et une racine n-ème de l'unité $\zeta \in \mu_n(\mathrm{K})$, on appelle *résolvante de Lagrange* de α et ζ l'élément (ζ,α) de L défini par

$$(\zeta,\alpha) = \alpha + \zeta^{-1}\sigma(\alpha) + \zeta^{-2}\sigma^2(\alpha) + \ldots + \zeta^{1-n}\sigma^{n-1}(\alpha).$$

(i) Vérifier que l'on a $\sigma(\zeta,\alpha) = \zeta(\zeta,\alpha)$ et en déduire que $(\zeta,\alpha)^n$ appartient à K.

(ii) Supposons que ζ soit une racine primitive de l'unité et que l'on ait $\mathrm{L} = \mathrm{K}(\alpha)$. Démontrer qu'il existe un entier $k \geq 1$ tel que $(\zeta,\alpha^k) \neq 0$ (*Indication : appliquer le lemme de Dedekind*) et en déduire que L est le corps de décomposition du polynôme $\mathrm{T}^n - (\zeta,\alpha^k)^n$.

3) On ne suppose plus que le polynôme $\mathrm{T}^n - 1$ soit scindé sur K mais on fait seulement l'hypothèse que n est premier à la caractéristique de K. Soit $a \in \mathrm{K}$ et soit L un corps de décomposition du polynôme $\mathrm{T}^n - a$.

(i) Vérifier que le polynôme $\mathrm{T}^n - 1$ est scindé sur L. On note K_1 l'extension de K dans L engendrée par les racines n-èmes de l'unité.

(ii) Vérifier que les extensions L/K_1 et K_1/K sont galoisiennes et démontrer que leurs groupes respectifs s'identifient à des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ et $\mu_n(\mathrm{L})$.

(iii) Décrire complètement le groupe de Galois de l'extension L/K.

Exercice 4 (*Résolution par radicaux*) — Soit K un corps de caractéristique 0 et soit L/K une extension finie galoisienne de groupe G.

On dit que l'extension L/K est *résoluble par radicaux* s'il existe une tour d'extensions de corps

$$\mathrm{K} = \mathrm{K}_0 \subset \mathrm{K}_1 \subset \ldots \subset \mathrm{K}_r$$

telle que

– pour tout $i \geq 0$, K_{i+1} s'obtienne à partir de K_i par adjonction d'une racine n-ème d'un élément de K_i ;

– $\mathrm{L} \subset \mathrm{K}_r$.

En utilisant l'exercice précédent, démontrer que l'extension L/K est résoluble par radicaux si et seulement si le groupe G est *résoluble*, c'est-à-dire si et seulement s'il existe une suite de sous-groupes

$$(1) = \mathrm{G}_r \leq \mathrm{G}_{r-1} \leq \ldots \leq \mathrm{G}_1 \leq \mathrm{G}_0 = \mathrm{G}$$

telle que, pour tout $i \geq 0$, G_{i+1} soit distingué dans G_i et le groupe quotient $\mathrm{G}_i/\mathrm{G}_{i+1}$ soit abélien.

Exercice 5 (*Résolution par radicaux réels*) — Soit K un sous-corps de $\mathbb{R}$ et soit L une extension galoisienne finie de K dans $\mathbb{R}$.

1. Considérons un nombre réel $\alpha \in \mathbb{R}$ et un entier naturel $m \geq 1$ tel que $\alpha^m \in \mathrm{K}$. Notant d le plus petit entier strictement positif tel que $\beta = \alpha^d \in \mathrm{L}$, démontrer que l'extension $\mathrm{K}(\beta)/\mathrm{K}$ est de degré au plus 2.

2. Déduire de ce qui précède que, si l'extension L/K peut s'obtenir par extraction successives de racines n-èmes réelles, alors $[\mathrm{L} : \mathrm{K}]$ est une puissance de 2.

Exercice 6 (*Résolution par radicaux des équations de degré inférieur à 3*) — Soit K un corps de caractéristique distincte de 2 et 3.

1. Interpréter la résolution usuelle de l'équation $x^2 + ax + b = 0$ du point de vue de la théorie de Galois.

2. Soit $\mathrm{P} = \mathrm{T}^3 + p\mathrm{T} + q \in \mathrm{K}[\mathrm{T}]$; on suppose que P est irréductible et on rappelle que son discriminant est $\mathrm{D} = -4p^3 - 27q^2$.

(i) Quelles sont les possibilités pour le groupe de Galois d'un corps de décomposition L de P au-dessus de K ?

Soit K' l'extension de K obtenue en adjoignant les racines cubiques de l'unité et soit L' un corps de décomposition de P au-dessus K' ; on désigne par ρ une racine cubique primitive de l'unité dans K' et on note $x_1,\ x_2,\ x_3$ les racines de P dans L'.

(ii) Justifier que le groupe $\mathrm{Gal}(\mathrm{L}'/\mathrm{K}'(\sqrt{\mathrm{D}}))$ est cyclique. Ayant fixé un générateur σ, écrire les trois résolvantes de Lagrange $(1,x_1)$, (ρ,x_1) et (ρ^2,x_1) puis expliciter les éléments $(1,x_1)^3$, $(\rho,x_1)^3$ et $(\rho^2,x_1)^3$ de $\mathrm{K}'(\sqrt{\mathrm{D}})$. Expliciter également l'élément $(\rho,x_1)(\rho^2,x_1)$ de K'.

(iii) Exprimer les racines $x_1,\ x_2$ et x_3 de P en fonction des résolvantes $(1,x_1),\ (\rho,x_1)$ et (ρ^2,x_1) puis en déduire l'expression de $x_1,\ x_2$ et x_3 en fonction des coefficients de P.