École polytechnique 2022-2023
Théorie de Galois

Feuille d'exercices 9

Exercice 1. Soit $K = \mathbf{Q}[\sqrt{d}]$ avec $d < 0$. Montrer que, pour tout $n \geq 2$, K n'est pas contenu dans une extension galoisienne cyclique de degré 2^n de $\mathbf{Q}$.

Exercice 2. (Théorème d'Artin–Schreier)

Soient K un corps de caractéristique zéro, p un nombre premier et a un élément de K qui n'est pas une puissance p-ième dans K.

(i) Montrer que $X^p - a$ est irréductible dans $K[X]$.

(ii) Si $r \geq 0$, montrer que $X^{p^r} - a$ est irréductible dans $K[X]$, sauf si $p = 2$ et a est de la forme $-4x^4$ avec $x \in K$.

Supposons maintenant K algébriquement clos et soit $k \subset K$ une extension finie.

(iii) Montrer que si -1 est un carré dans k, alors $K = k$ (se ramener au cas où $k \subset K$ est de degré premier).

(iv) Montrer qu'en général $K = k[\sqrt{-1}]$.

Plus généralement le théorème d'Artin–Schreier caractérise les corps K tels que $[\overline{K} : K] < +\infty$ comme étant les corps réels clos, des généralisations du corps des nombres réels.

Exercice 3. (Théorème de Hilbert 90). Soit L/K une extension galoisienne. La norme d'un élément $x \in L$ est définie par la formule

$$N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x)$$

(i) Montrer que, si $x \in L$, alors $N_{L/K}(x) \in K$.

(ii) Soient $\sigma_1, \ldots, \sigma_n$ des morphismes distincts de groupes de $L^\times$ vers $L^\times$. Montrer qu'ils forment une famille libre dans le L-espace vectoriel des applications de $L^\times$ dans L.

On suppose désormais que L/K est une extension cyclique de degré n. Soit σ un générateur de $\mathrm{Gal}(L/K)$.

(iii) Soit $x \in L$. Montrer que $N_{L/K}(x) = 1$ si et seulement s'il existe $y \in L^\times$ tel que $x = y\sigma(y)^{-1}$ (on pourra considérer l'application $\mathrm{Id} + x\sigma + x\sigma(x)\sigma^2 + \cdots + x \cdots \sigma^{n-2}(x)\sigma^{n-1}$ de $L^\times$ dans L).

(iv) Si $\mu_n(K)$ est de cardinal n, fixons ζ un générateur de $\mu_n(K)$. Calculer $N_{L/K}(\zeta)$ et retrouver le résultat de classification des extensions cycliques.

Exercice 4. Soit $L|K$ une extension galoisienne de groupe $G = \mathrm{Gal}(L/K)$.

(i) La trace d'un élément $x \in L$ est définie par $\mathrm{tr}_{L/K}(x) = \sum_{\sigma \in G} \sigma(x)$. Vérifier que $\mathrm{tr}_{L/K}$ est un morphisme de groupes additifs de L vers K.

(ii) Montrer qu'il existe $x \in L$ tel que $\mathrm{tr}_{L/K}(x) = 1$ (utiliser la question (ii) de l'exercice 3).

(iii) On note

$$Z^1(G, L) = \{(c_\sigma)_\sigma \in L^G \mid \forall \sigma, \tau \in G \quad c_{\sigma\tau} = c_\sigma + \sigma(c_\tau)\}.$$

Vérifier que, pour $x \in L$ et $c_\sigma = \sigma(x) - x$, on a $(c_\sigma)_\sigma \in Z^1(G, L)$. Réciproquement, montrer que tout $(c_\sigma)_\sigma \in Z^1(G, L)$ est de cette forme là (regarder pour $y \in L$ la quantité $\sum_{\tau \in G} \tau(y)c_\tau$).

On suppose maintenant que K est un corps parfait de caractéristique p dont on note $\overline{K}$ une clôture algébrique et on suppose $L \subset \overline{K}$.

(iv) Soit $y \in L$ tel que $y^p - y \in K$. Vérifier que

$$\sigma \longmapsto \sigma(y) - y$$

définit un morphisme de groupes $\mathrm{Gal}(L/K) \to \mathbf{Z}/p\mathbf{Z}$ et montrer qu'en faisant varier de tels y on obtient ainsi tous les morphismes $\mathrm{Gal}(L/K) \to \mathbf{Z}/p\mathbf{Z}$.

(v) Montrer qu'il existe une bijection entre les sous-$\mathbf{F}_p$-espaces vectoriels de dimension finie de $K/(F - \mathrm{Id})(K)$ et les extensions finies galoisiennes de K dans $\overline{K}$ dont le groupe de Galois est un groupe abélien de p-torsion, où $F : \overline{K} \to \overline{K}$ désigne le Frobenius $x \mapsto x^p$ (par un groupe abélien de p-torsion, on entend un groupe isomorphe à $(\mathbf{Z}/p\mathbf{Z})^k$ pour un certain entier k).

Exercice 5. Soit $n \geq 2$ un entier. Montrer que le discriminant du polynôme $X^n + aX + b$ est

$$(-1)^{\frac{n(n-1)}{2}} \left(n^n b^{n-1} + (1-n)^{n-1} a^n\right).$$

Exercice 6. Soient k un corps parfait et $P = X^3 + aX + b \in k[X]$ un polynôme irréductible dont on note $\alpha_1, \alpha_2, \alpha_3$ les racines dans un corps de décomposition K de P. On rappelle que le discriminant $\Delta(P)$ de P est $\left(\prod_{i<j}(\alpha_i - \alpha_j)\right)^2$. (On peut vérifier, cf. exercice 5, qu'il est égal à $-4a^3 - 27b^2$.)

1. Supposons que $\Delta(P)$ soit un carré dans k. Que peut-on dire du groupe de Galois G de P ?
2. Soit $f = Z_1 Z_2^2 + Z_2 Z_3^2 + Z_3 Z_1^2 \in k[Z_1, Z_2, Z_3]$. Montrer qu'une permutation $\sigma \in \mathfrak{S}_3$ est paire si et seulement si $\sigma(f) = f$. (On fait agir $\mathfrak{S}_3$ par permutation des variables.)
3. Montrer que $R_f(P) = \prod_{\sigma \in S_3/A_3}(T - \sigma(f)(\alpha_1, \alpha_2, \alpha_3))$ appartient à $k[T]$ et l'exprimer en fonction de a et b.
4. En déduire que si k est de caractéristique 2, le groupe de Galois de P est contenu dans A_3 ou pas selon que $1 + a^3 b^{-2}$ est de la forme $x^2 + x$ ($x \in k$) ou pas.