

5. Groupes de Galois (discriminant, réduction modulo p , ...)

Exercice 5.1 Soient K un corps, $f \in K[X]$ un polynôme non constant et unitaire de degré n . On note x_i , $1 \leq i \leq n$, ses racines dans une clôture algébrique de K . On rappelle que le discriminant de f vaut $\Delta = \delta^2$ où $\delta = \prod_{i < j} (x_i - x_j)$.

1. Montrer que $\Delta = (-1)^{n(n-1)/2} \prod_{i=1}^n f'(x_i)$.
2. Calculer Δ pour $f(X) = X^n + bX + c$ en fonction de n , b et c .
3. On suppose désormais f séparable et $\text{car}(K) \neq 2$. On identifie $G = \text{Gal}_K(f)$ à un sous-groupe de S_n . Montrer que pour tout $\sigma \in G$, $\sigma(\delta) = \epsilon(\sigma) \cdot \delta$ où $\epsilon(\sigma)$ est la signature de σ .
4. Montrer que $\Delta \in K$.
5. Montrer que Δ possède une racine carrée dans K si et seulement si G est isomorphe à un sous-groupe de A_n .
6. Si $\delta \notin K$, on pose $H = \{\sigma \in G \mid \sigma \text{ est une permutation paire des racines de } f\}$. Montrer que H est un sous-groupe d'indice 2 de G et que si L est le corps des racines de f alors $L^H = K[\delta]$.
7. Déterminer Δ et $\mathbb{Q}[\delta]$ pour le polynôme $f = X^3 - 2$ sur \mathbb{Q} .

Exercice 5.2 Soit L le corps de décomposition de $X^n - a \in K[X]$, où $0 \neq a \in K$. On suppose que la caractéristique de K ne divise pas n (par exemple $\text{car}(K) = 0$).

1. Montrer que L est une extension galoisienne de K .
2. Montrer que $L = K[\alpha, \xi]$ où $\alpha^n = a$ et ξ est une racine primitive n -ième de l'unité.
3. Montrer que tout $\sigma \in \text{Gal}(L/K)$ est caractérisé par son effet sur α et ξ , et qu'on a $\sigma(\alpha) = \xi^s \alpha$ et $\sigma(\xi) = \xi^r$, où $r, s \in \mathbb{N}$ et r est premier avec n .
4. Montrer qu'avec les notations précédentes, on a un homomorphisme de groupes injectif :

$$\begin{array}{ccc} \text{Gal}(L/K) & \longrightarrow & GL_2(\mathbb{Z}/n\mathbb{Z}) \\ \sigma & \mapsto & \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} \end{array}$$

5. Soit $H = \left\{ \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} \mid r, s \in \mathbb{N} \text{ et } (r, n) = 1 \right\} \subset GL_2(\mathbb{Z}/n\mathbb{Z})$. Montrer que H possède un sous-groupe normal cyclique d'ordre n , à quotient abélien. En déduire que $\text{Gal}(L/K)$ possède un sous-groupe normal cyclique d'ordre d , avec d/n , à quotient abélien.
6. Que se passe-t-il si $\xi \in K$?

Exercice 5.3 Soit $f \in \mathbb{Q}[X]$ un polynôme irréductible de degré p premier > 2 . On suppose que l'équation $f(X) = 0$ est résoluble par radicaux sur \mathbb{Q} . Montrer que le nombre de racines réelles de f est 1 ou p .

Application : montrer que l'équation $X^7 + 7X^4 - 7 = 0$ n'est pas résoluble par radicaux.

Exercice 5.4 Soit $f(X) = X^6 + 22X^5 + 6X^4 + 12X^3 - 52X^2 - 14X - 30$.

1. Montrer que f est irréductible sur \mathbb{Q} .
2. En réduisant modulo 5, montrer que $G = \text{Gal}_{\mathbb{Q}}(f)$ contient une transposition.
3. En réduisant modulo 3, montrer que G contient un 5-cycle.
4. Vérifier qu'un sous-groupe transitif de S_n qui contient une transposition et un $n-1$ -cycle est égal à S_n . En déduire que $G \simeq S_6$.

Exercice 5.5 Soit λ un entier non divisible par 5. On note $\mu = 5\lambda^2 - 1$ et $f(X) = X^5 + 5\mu X - 4\mu$.

1. Montrer que f est irréductible sur \mathbb{Q} .
2. On note x_i , $1 \leq i \leq 5$, les racines de f dans \mathbb{C} , et on identifie $G = \text{Gal}_{\mathbb{Q}}(f)$ à un sous-groupe de S_5 . Vérifier que f a une et une seule racine réelle et en déduire que G contient un produit de 2 transpositions disjointes.
3. Prouver que G est contenu dans A_5 .

On suppose désormais que $\lambda^2 \equiv 1 \pmod{7}$.

4. a. En réduisant f modulo 7, montrer que G contient un 3-cycle.
- b. En déduire que $G = A_5$.
5. Soit L le corps des racines de f sur \mathbb{Q} . Si M est une extension galoisienne de \mathbb{Q} , contenue dans L , prouver que

$$M = \mathbb{Q} \quad \text{ou} \quad M = L.$$

6. On pose :

$$g(X) = \prod_{1 \leq i < j \leq 5} (X - (x_i + x_j)).$$

- a. Montrer que $g \in \mathbb{Q}[X]$ et que g est séparable de degré 10.
- b. Quel est le corps des racines de g sur \mathbb{Q} ? L'équation $g(X) = 0$ est-elle résoluble par radicaux sur \mathbb{Q} ?
- c. Montrer que g est irréductible sur \mathbb{Q} .
7. Soit H le sous-groupe de G engendré par les permutations $(1, 2)(3, 4)$ et $(1, 2)(3, 5)$. Montrer que $|H| \geq 6$, et en utilisant la question 6, trouver un élément primitif sur \mathbb{Q} du corps des invariants L^H .

Exercice 5.6 Soit n un entier ≥ 3 et p un nombre premier impair $\geq n-2$.

1. Montrer qu'il existe $f_1, f_2, f_3 \in \mathbb{Z}[X]$, f_1 et f_2 unitaires,

$$\deg f_1 = n-1, \quad \deg f_2 = 2, \quad \deg f_3 \leq n-1,$$

avec f_1 irréductible modulo 2, f_2 irréductible modulo p , et tels que :

$$f(X) = pXf_1(X) - (p-1) \prod_{i=1}^{n-2} (X-i)f_2(X) + 2pf_3(X)$$

est irréductible sur \mathbb{Q} . Prouver que $\text{Gal}_{\mathbb{Q}}(f) = S_n$.

2. En déduire l'existence d'une extension L de degré n sur \mathbb{Q} telle que pour tout sous-corps K de L , on ait :

$$K = \mathbb{Q} \quad \text{ou} \quad K = L.$$