Feuille de TD 5

Théorie de Galois

Exercice 1. Montrer que si a et b sont deux éléments non nuls d'un corps K de caractéristique différente de 2, alors $K(\sqrt{a})$ est égal à $K(\sqrt{b})$ si et seulement si b/a est un carré dans K.

Exercice 2. Soit $K = \mathbb{Q}(i + \sqrt{2})$. Montrer que K est galoisien sur $\mathbb{Q}$. Calculer le degré de K sur $\mathbb{Q}$ et le groupe de Galois de $K/\mathbb{Q}$. Donner la liste des sous-corps de K.

Exercice 3. Soit $L = \mathbb{Q}(\sqrt{5})$ et $M = \mathbb{Q}(\sqrt{2 + \sqrt{5}})$. Déterminer les degrés des extensions $L/\mathbb{Q}$, $M/\mathbb{Q}$ et M/L. Indiquer lesquelles de ces extensions sont galoisiennes. Déterminer les polynômes minimaux de $\sqrt{2 + \sqrt{5}}$ sur $\mathbb{Q}$ et sur L.

Exercice 4. Soit a et b deux rationnels. Donner une condition suffisante pour que le polynôme $X^4 + aX^2 + b$ soit irréductible sur $\mathbb{Q}$. Donner une condition nécessaire et suffisante pour qu'alors son corps de rupture soit galoisien sur $\mathbb{Q}$. Que se passe-t-il dans le cas où b est négatif et $a^2 - 4b$ est positif, mais pas un carré rationnel ?

Exercice 5. Soit $K = \mathbb{Q}(\sqrt[3]{2})$ et L la clôture galoisienne de K sur $\mathbb{Q}$. Calculer le degré de L sur $\mathbb{Q}$, ainsi que le groupe de Galois de L/K. Donner la liste des sous-corps de L.

Exercice 6. Soit G le groupe de Galois de $X^5 - 2$ sur $\mathbb{Q}$. Quel est le cardinal de G ? Est-il abélien, résoluble ?

Exercice 7. Quel est le degré du corps de décomposition du polynôme $(X^3 - 5)(X^3 - 7)$ sur $\mathbb{Q}$?

Exercice 8. Déterminer le groupe de Galois de $X^6 - 5$ sur $\mathbb{Q}$ et sur $\mathbb{R}$.

Exercice 9. Trouver un élément primitif de $\mathbb{Q}(\sqrt{3}, \sqrt{7})$.

Exercice 10. Soit G le groupe de Galois de $(X^3 - 5)(X^4 - 2)$ sur $\mathbb{Q}$.

(1) Donner une présentation par générateurs et relations de G.

(2) Le groupe G est-il cyclique, diédral, symétrique ?

Exercice 11. Trouver un élément primitif du corps de décomposition de $(X^2 - 2)(X^2 - 5)(X^2 - 7)$.

Exercice 12. Soit ζ une racine primitive 12-ième de l'unité. Combien y a-t-il d'extensions comprises entre $\mathbb{Q}(\zeta^3)$ et $\mathbb{Q}(\zeta)$?

Exercice 13. Soit ζ une racine primitive 5-ième de l'unité.

(1) Décriver le groupe de Galois de $K = \mathbb{Q}(\zeta)/\mathbb{Q}$ et montrer que K contient un unique sous-corps de degré 2 sur $\mathbb{Q}$, à savoir $\mathbb{Q}(\zeta + \zeta^4)$.

(2) Donner le polynôme minimal de $\zeta + \zeta^4$ sur $\mathbb{Q}$.

(3) Donner le groupe de Galois de $(X^2 - 5)(X^5 - 1)$.

(4) Donner le groupe de Galois de $(X^2 + 3)(X^5 - 1)$.

Exercice 14. Notons K le corps $\mathbb{Q}(\sqrt{-15})$, f son automorphisme non trivial et α un élément de K tel que le polynôme $X^3 - \alpha$ soit irréductible sur K.

(1) Pourquoi existe-t-il un tel α ?

On note L le corps de décomposition de ce polynôme, et $\theta, j\theta, j^2\theta$ ses différentes racines dans L.

(2) Pourquoi sont-elles de cette forme ?

(3) Montrer que L est une extension galoisienne de K de degré 6 et que L contient $\sqrt{5}$.

(4) Montrer qu'il existe deux K-automorphismes σ et τ de L tels que

$$\sigma(\sqrt{5}) = \sqrt{5}, \quad \sigma(\theta) = j\theta, \quad \tau(\sqrt{5}) = -\sqrt{5}, \quad \tau(\theta) = \theta.$$

(5) Déterminer l'ordre des éléments σ et τ du groupe $\mathrm{Gal}(L/K)$ et calculer $\tau\sigma\tau^{-1}$. Établir la liste des extensions de K contenues dans L.

(6) On suppose désormais que $N_{K/\mathbb{Q}}(\alpha)$ est le cube d'un nombre rationnel b. Déterminer les différents conjugués de θ sur $\mathbb{Q}$. Montrer que l'extension $L/\mathbb{Q}$ est galoisienne de degré 12. Prouver qu'il est possible de prolonger l'automorphisme f de K en un automorphisme ϕ de L tel que $\phi(\sqrt{5}) = \sqrt{5}$ et $\phi(\theta) = b/\theta$. Calculer ϕ^2, $\phi\sigma\phi^{-1}$ et $\phi\tau\phi^{-1}$. Montrer que $\mathbb{Q}(\sqrt{5})$ admet une extension de degré 3 contenue dans L et galoisienne sur $\mathbb{Q}$.

Exercice 15. En réduisant modulo 2 et 3, montrer que le groupe de Galois de $X^5 - X - 1$ est le groupe symétrique S_5.