3. Groupes de Galois - Correspondance de Galois

Exercice 3.1 Soient $\alpha = \sqrt[5]{2} \in \mathbb{R}$ et $\omega \in \mathbb{C}$ une racine primitive cinquième de l'unité.

1. Montrer que $L = \mathbb{Q}(\alpha, \omega)$ est une extension Galoisienne de $\mathbb{Q}$.
2. Déterminer $[\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}]$ et $[\mathbb{Q}(\omega) : \mathbb{Q}]$. En déduire $[L : \mathbb{Q}]$.
3. Montrer qu'il existe $\sigma, \tau \in G = \mathrm{Gal}(L/\mathbb{Q})$ tels que $\sigma(\alpha) = \omega\alpha$, $\sigma(\omega) = \omega$ et $\tau(\alpha) = \alpha$, $\tau(\omega) = \omega^2$.
4. Vérifier que $G = \langle \sigma, \tau \rangle$ et en déduire la structure du groupe G.
5. Décrire, à l'aide de α et ω, tous les sous-corps de L de degré 2 et de degré 10 sur $\mathbb{Q}$. Déterminer parmi ces sous-corps ceux qui sont des extensions galoisiennes de $\mathbb{Q}$.

Exercice 3.2 Soit $\alpha = \sqrt{3 + \sqrt{3}} \in \mathbb{R}$.

1. Calculer le polynôme minimal P de α sur $\mathbb{Q}$.
2. Montrer que $L = \mathbb{Q}(\alpha, \sqrt{2})$ est le corps des racines de P sur $\mathbb{Q}$.
3. Montrer que 3 est irréductible dans l'anneau euclidien $Z[\sqrt{2}]$. En déduire que P est irréductible sur $\mathbb{Q}(\sqrt{2})$.
4. Quel est l'ordre de $G = \mathrm{Gal}_{\mathbb{Q}}(P)$?
5. Montrer que $H = \{\sigma \in G : \sigma(\sqrt{2}) = \sqrt{2}\}$ est un sous-groupe distingué de G, d'ordre 4. Montrer que H est cyclique.
6. Montrer que tout $z \in G \setminus H$ est d'ordre 2.
7. En déduire la structure du groupe G.
8. En utilisant la correspondance de Galois, décrire le treillis des sous-corps de L.

Exercice 3.3 Soient L/K une extension Galoisienne et $G = \mathrm{Gal}(L/K)$ son groupe de Galois. Alors G agit sur la L-algèbre $L[X]$ par

$$\sigma\left(\sum_i \lambda_i X^i\right) = \sum_i \sigma(\lambda_i) X^i$$

où $\sigma \in G$ et $\sum_i \lambda_i X^i \in L[X]$.

1. Soit α algébrique sur K tel que $L \subseteq K(\alpha)$. Soit Q le polynôme minimal de α sur L. Montrer que
$$\prod_{\sigma \in G} \sigma(Q)$$
est le polynôme minimal de α sur K.
2. Soit $P \in K[X]$ irréductible sur K. Montrer que l'ensemble des facteurs irréductibles unitaires de P dans $L[X]$ forme une G-orbite de $L[X]$. En particulier tous les facteurs irréductibles de P dans $L[X]$ ont même degré.

Exercice 3.4 On considère $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ et $\alpha = (2 + \sqrt{2})(3 + \sqrt{6})$.

1. a. Expliquer pourquoi K est une extension galoisienne de degré 4 sur $\mathbb{Q}$.
   b. Vérifier que le groupe $\mathrm{Gal}(K/\mathbb{Q})$ est engendré par les deux automorphismes suivant :

$$\begin{array}{rcl} \sqrt{2} & \mapsto & \sqrt{2} \\ \sqrt{3} & \mapsto & -\sqrt{3} \end{array} \quad et \quad \begin{array}{rcl} \sqrt{2} & \mapsto & -\sqrt{2} \\ \sqrt{3} & \mapsto & \sqrt{3} \end{array}$$

2. a. Vérifier que les conjugués $\sigma(\alpha)$, $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ sont tous distincts.
   b. En déduire que $K = \mathbb{Q}(\alpha)$.
   c. Calculer le polynôme minimal de $3+\sqrt{6}$ sur $\mathbb{Q}$. En déduire le polynôme minimal de α sur $\mathbb{Q}(\sqrt{2})$ puis sur $\mathbb{Q}$.
3. Pour chaque $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ non trivial, calculer explicitement le produit $\alpha \times \sigma(\alpha)$ et vérifier que ce produit est un carré dans K, mais n'est pas un carré dans le corps des invariants $K^{\langle\sigma\rangle}$.
4. On pose $\theta = \sqrt{\alpha}$ et $L = \mathbb{Q}(\theta)$.
   a. Montrer que θ n'appartient pas à K. (Indication : on pourra raisonner par l'absurde en utilisant la question précédente.)
   b. En déduire que $[L : \mathbb{Q}] = 8$.
   c. Déterminer le polynôme minimal f de θ sur $\mathbb{Q}$. Quelles sont les racines de f ?
   d. Montrer que L est galoisienne sur $\mathbb{Q}$. (Indication : on pourra de nouveau utiliser la question précédente.)
5. Soit $\tau \in G = \mathrm{Gal}(L/\mathbb{Q})$.
   a. Prouver qu'il existe $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ tel que $\tau(\alpha) = \sigma(\alpha)$.
   b. En utilisant la question 3, montrer que $K = K^{\langle\sigma\rangle}(\theta\tau(\theta))$.
   c. On suppose τ d'ordre 2. Déduire de ce qui précède que $L^{\langle\tau\rangle}$ contient K et finalement que $L^{\langle\tau\rangle} = K$.
6. a. Prouver que G a un unique élément d'ordre 2. Expliciter cet automorphisme.
   b. Reconnaître le groupe G.

Exercice 3.5 Soit n un entier ≥ 2. On suppose qu'il existe un sous-corps K de $\mathbb{C}$, extension cyclique de degré n de $\mathbb{Q}$ et tel que $\omega = \exp(2i\pi/n) \in K$.

1. Montrer que $\varphi(n)$ divise n et en déduire que n est de la forme $n = 2^a \cdot 3^b$ avec $a \geq 1$ et $b \geq 0$.
2. Montrer que $a = 1$. Indication : le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n = 2, 4, p^\alpha$ ou $2p^\alpha$ avec p premier impair et $\alpha \geq 1$.
3. Si $n > 2$, montrer qu'il existe $x \in \mathbb{C}$ tel que $x^3 \in \mathbb{Q}(\omega)$ et $K = \mathbb{Q}(\omega, x)$.
4. Réciproquement, $n = 2 \cdot 3^b$ étant donné, construire un exemple d'une telle extension cyclique K de $\mathbb{Q}$.