3. Groupes de Galois

Exercice 3.1 Soit $\alpha = \sqrt{3+\sqrt{3}} \in \mathbb{R}$.

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

Exercice 3.2 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 le corps des racines du polynôme $X^5 - 2$ sur $\mathbb{Q}$. Calculer $[L : \mathbb{Q}]$.
2. Montrer qu'il existe $\sigma, \tau \in G = \mathrm{Gal}(L/\mathbb{Q})$ tels que $\sigma(\alpha) = \omega\alpha$, $\sigma(\omega) = \omega$ et $\tau(\alpha) = \alpha$, $\tau(\omega) = \omega^2$.
3. Vérifier que $G = \langle \sigma, \tau \rangle$ et en déduire la structure du groupe G.
4. Décrire, à l'aide de α et ω, tous les sous-corps de L de degré 2 et de degré 10. Trouver parmi ces sous-corps ceux qui sont des extensions galoisiennes de $\mathbb{Q}$.

Exercice 3.3 Soient n un entier ≥ 1 et p un nombre premier qui ne divise pas n. On pose $\Phi(X) = \Phi_{n,\mathbb{F}_p}(X)$ le polynôme cyclotomique correspondant et $G = \mathrm{Gal}_{\mathbb{F}_p}(\Phi)$.

1. Montrer que $\bar{p}$ est d'ordre $|G|$ dans le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.
2. En déduire que Φ est irréductible sur $\mathbb{F}_p$ si et seulement si $\bar{p}$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

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 :

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

2. a. Vérifier que les conjugués $\sigma(\alpha)$, $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ sont tous distincts.
   b. En déduire que $K = \mathbb{Q}(\alpha)$.
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. Soit f le polynôme minimal de θ sur $\mathbb{Q}$. Quelles sont les racines de f ? Calculer les coefficients 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 $\mathbb{Q}$.

Exercice 3.6 On note $K = \mathbb{Q}(X)$. Soit $P(X) \in K \setminus \mathbb{Q}$, on définit l'application σ_P de K dans K par

$$\sigma_P(A(X)) = A(P(X)).$$

1. Soit $P \in K$ tel qu'il existe $Q \in K$ avec $Q(P(X)) = P(Q(X)) = X$. Montrer que σ_P est un $\mathbb{Q}$-automorphisme de K.

On note Γ le groupe des matrices 2×2 à coefficients entiers et de déterminant 1. On associe à la matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, la fraction rationnelle

$$P_M(X) = \frac{aX + b}{cX + d}.$$

2. Montrer que $P_M(X) \in K \setminus \mathbb{Q}$ pour tout $M \in \Gamma$ et que $P_M(X) = X$ si et seulement si $M = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
3. Montrer que $P_{M^{-1}}(P_M(X)) = X$ pour tout $M \in \Gamma$ et que pour $M, N \in \Gamma$, on a $P_{MN}(X) = P_M(P_N(X))$.
4. Déduire des questions précédentes, que si on pose $\sigma_M = \sigma_{P_{M^{-1}}}$, l'application $M \mapsto \sigma_M$ est un morphisme de groupe de Γ dans le groupe $\mathrm{Aut}_{\mathbb{Q}}(K)$ des $\mathbb{Q}$-automorphismes de K de noyau $\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Soit $S(X) \in K \setminus \mathbb{Q}$. On pose $k = \mathbb{Q}(S(X))$.

5. Montrer que K/k est une extension algébrique en exhibant un polynôme dans $k[T]$ dont X est racine.
6. Soit $M \in \Gamma$ tel que $\sigma_M(S(X)) = S(X)$. Montrer que $\sigma_M \in \mathrm{Aut}_k(K)$. En déduire que M est d'ordre fini dans Γ.
7. Déduire de ce qui précède qu'il n'existe pas de polynôme $A(X) \in \mathbb{Q}(X)$ vérifiant $A\left(\frac{X}{X+1}\right) = A(X)$.