Feuille 9 – Correspondance galoisienne

Exercice 1. Déterminer le groupe de Galois des polynômes et extensions de corps suivants, puis expliciter la correspondance de Galois dans chaque cas, en donnant des générateurs de chaque extension intermédiaire :

1. Le polynôme $X^3 - 2$ sur $\mathbb{Q}$.
2. Le polynôme $X^4 - 5$ sur $\mathbb{Q}$.
3. Le polynôme $X^4 + 1$ sur $\mathbb{Q}$.
4. Le polynôme $X^5 - 2$ sur $\mathbb{Q}$.
5. L'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.
6. L'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$.
7. L'extension $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}$, où $\alpha = (2 + \sqrt{2})(3 + \sqrt{6})$ (on commencera par étudier $\mathbb{Q}(\alpha)/\mathbb{Q}$).
8. Le polynôme $X^8 - 2$ sur $\mathbb{Q}$.

Exercice 2. Déterminer des éléments primitifs pour les extensions suivantes :

1. L'extension $\mathbb{Q}\left(\sqrt[3]{2}, j\right)/\mathbb{Q}$.
2. L'extension $\mathbb{Q}\left(\sqrt[4]{2}, i\right)/\mathbb{Q}$.
3. L'extension $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{5}\right)/\mathbb{Q}$.

Exercice 3. Montrer que si K est un corps de caractéristique différente de 2, et L/K une extension galoisienne de groupe de Galois isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$, alors il existe $a, b \in K$ tels que $L = K(\sqrt{a}, \sqrt{b})$.

Exercice 4. Soit $K \subseteq \mathbb{C}$ l'ensemble des nombres constructibles à la règle non graduée et au compas (c'est-à-dire : qui sont l'affixe d'un point du plan euclidien constructible à la règle non graduée et au compas, en partant des points d'affixe 0 et 1).

1. Montrer que K est un corps : c'est le plus petit sous-corps de $\mathbb{C}$ stable par extraction de racine carrée.
2. Montrer que $x \in \mathbb{C}$ est constructible si, et seulement s'il existe une suite d'extensions

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n, \tag{1}$$

   telle que $[K_i : K_{i-1}] = 2$ pour tout $i \in [\![1, n]\!]$, $K_0 = \mathbb{Q}$ et $x \in K_n$.
3. Montrer que toute extension galoisienne L/K de degré 2^n admet une suite d'extensions du type (1) avec $K_n = L$ et $K_0 = K$.
4. Montrer que si x est constructible, alors le degré de son polynôme minimal est une puissance de 2.
5. En déduire que $\cos\left(\frac{\alpha}{3}\right)$ n'est en général pas constructible à la règle non graduée et au compas pour $\alpha \in \mathbb{R}$ (problème de trisection de l'angle). De même pour $\sqrt[3]{2}$ (problème de la duplication du cube).
6. Démontrer le théorème de Gauss-Wantzel : un polygone à n côtés est constructible à la règle non graduée et au compas si, et seulement si n a pour décomposition en facteurs premiers $2^\alpha \prod_i p_i$, où les p_i sont des nombres premiers de Fermat (c'est-à-dire de la forme $2^{2^k} + 1$, avec $k \geqslant 0$).
7. Déterminer le groupe des automorphismes de $K \cap \mathbb{R}$.

Exercice 5. Montrer que :

$$\cos\left(\frac{2\pi}{17}\right) = \frac{1}{16}\Big(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}} + \sqrt{68+12\sqrt{17}-2\sqrt{34-2\sqrt{17}}-16\sqrt{34+2\sqrt{17}}+2\sqrt{578-34\sqrt{17}}}\Big).$$

On admet pour simplifier, même si on pourrait s'en passer (non trivialement), qu'une calculatrice nous permet de déterminer quel signe prendre, lorsqu'on a le choix entre deux racines carrées.

Exercice 6. Soit $P \in K[X]$ un polynôme séparable de degré n, dont le groupe de Galois sur K est isomorphe à $\mathfrak{S}_n$. Soit α une racine de P. Déterminer le groupe des K-automorphismes de $(D_K(P))^{\mathrm{Stab}_{\mathfrak{S}_n}(\alpha)}$.

Exercice 7. Soit L/K une extension galoisienne finie, et M_1, M_2 deux extensions intermédiaires galoisiennes sur K. Montrer que $M_1 \cap M_2$ est une extension galoisienne sur K, et déterminer son groupe de Galois en fonction de $\mathrm{Gal}(L/M_1)$ et $\mathrm{Gal}(L/M_2)$.

Exercice 8. Montrer, à l'aide de la théorie de Galois, que pour tout polynôme $P \in \mathbb{R}[X]$ réciproque (c'est-à-dire tel que $X^{\deg(P)} \cdot P\left(\frac{1}{X}\right) = P(X)$) peut s'écrire $P = X^{\deg(P)/2} Q\left(X + \frac{1}{X}\right)$ avec $Q \in \mathbb{R}[X]$. Le faire explicitement avec $P = X^4 + X^3 + X^2 + X + 1$.

Exercice 9. Pour $F \in K(X)$, on écrit $F = P/Q$ avec $P, Q \in K[X]$ et P et Q premiers entre eux, et on pose $\deg(F) = \max(\deg(P), \deg(Q))$ (ce n'est pas la définition usuelle).

1. Montrer que, si F n'est pas une constante, alors $[K(X) : K(F)] = \deg(F)$.
2. Montrer que tout K-automorphisme de $K(X)$ est déterminé par une fraction rationnelle de degré 1.
3. Montrer que le groupe G des K-automorphismes de $K(X)$ est isomorphe à $\mathrm{GL}_2(K)/K^*\mathrm{I}_2$.
4. Montrer G est engendré par les automorphismes déterminés par les fractions rationnelles $X + b$ (avec $b \in K$), aX (avec $a \in K^*$) et X^{-1}.
5. On suppose que K est infini. Montrer que G est infini, et déterminer $K(X)^G$.
6. Montrer que l'extension $\mathbb{C}(X)/\mathbb{C}\left(X^3 + \frac{1}{X^3}\right)$ est galoisienne, puis déterminer son groupe de Galois, les extensions intermédiaires et des éléments primitifs pour chacune.

   Dans la suite, on suppose que K est fini de cardinal q.

   (a) Déterminer l'ordre de G.

   (b) Montrer que $K(X)^G = K(F)$, où $F = \frac{(X^{q^2}-X)^{q+1}}{(X^q-X)^{q^2+1}}$.

   (c) Soit H_1 le sous-groupe de G des automorphismes déterminés par les fractions rationnelles $aX + b$ (avec $a \in K^*$ et $b \in K$). Montrer que $K(X)^{H_1} = K(Y)$, où $Y = (X^q - X)^{q-1}$.

   (d) Soit H_2 le sous-groupe de G des automorphismes déterminés par les fractions rationnelles $X + b$ (avec $b \in K$). Montrer que $K(X)^{H_2} = K(Z)$, où $Z = X^q - X$.

   (e) Soit H_3 le sous-groupe de G des automorphismes déterminés par les fractions rationnelles aX (avec $a \in K^*$). Montrer que $K(X)^{H_3} = K(T)$, où $T = X^{q-1}$.