Feuille 10 – Extensions abéliennes, cycliques, résolubilité par radicaux

Exercice 1. Soient K un corps de caractéristique différente de 2, et $c \in K$ qui n'est pas un carré. On note F le corps de décomposition de $X^2 - c$ et $x \in F$ une de ses racines. On choisit ensuite $\alpha = a + bx \in F$, où $a, b \in K$, et on note E le corps de décomposition de $X^2 - \alpha$ sur F.

1. Montrer que les propositions suivantes sont équivalentes.
   (a) E est galoisienne sur K.
   (b) E est normale sur K.
   (c) E est le corps de décomposition sur F de $X^2 - \alpha'$, où $\alpha' = a - bx$.
   (d) α' est un carré dans E.
   (e) $\alpha\alpha' = a^2 - cb^2$ est un carré dans K ou $c\alpha\alpha'$ est un carré dans K.

   Pour les questions suivantes, on suppose que α n'est pas un carré dans F.
2. Lorsque les conditions précédentes sont vérifiées, montrer que le groupe de Galois de E sur K est cyclique si et seulement si $c\alpha\alpha'$ est un carré dans K.
3. En déduire le groupe de Galois de E sur K lorsque $\alpha\alpha'$ est un carré dans K.

Exercice 2. Nous allons démontrer un théorème dû à Galois et Abel (indépendamment) : une équation de degré premier est résoluble par radicaux si, et seulement si deux de ses racines suffisent à exprimer toutes les autres (comme fractions rationnelles en ces racines).

1. Soit P un polynôme de degré p premier, irréductible sur $\mathbb{Q}$, de groupe de Galois résoluble par radicaux. Soient K son corps de décomposition sur $\mathbb{Q}$, et $\alpha_1, \ldots, \alpha_p$ ses racines.
   (a) Montrer que si on a l'extension suivante d'extensions radicales de degrés premiers :

   $$\mathbb{Q} = L_0 \subseteq L_0(\varepsilon) = L'_0 \subseteq \cdots \subseteq L'_{r-1} \subseteq L'_r = L,$$

   où ε est une racine primitive de l'unité, L'_{r-1} une extension ne contenant pas de racine de P et $L/\mathbb{Q}$ une extension galoisienne contenant K, alors P est irréductible sur L'_{r-1}, et se scinde sur L (on peut utiliser l'exercice 4 du TD8). En déduire que $\mathrm{Gal}(L/L'_{r-1}) = \mathbb{Z}/p\mathbb{Z}$.
   (b) Soit σ un générateur de $\mathrm{Gal}(L/L'_{r-1})$. Montrer qu'on peut numéroter les racines de P de sorte que σ envoie α_i sur α_{i+1}.
   (c) Soit τ un élément de $\mathrm{Gal}(L/L'_{r-2})$. Montrer que $\tau(\alpha_i) = \alpha_{ai+b \bmod p}$, où $a \not\equiv 0 \bmod p$.
   (d) En déduire que si $P = 0$ est résoluble par radicaux, avec P irréductible sur $\mathbb{Q}$ et de degré p premier, alors après numérotation adéquate des racines, toute permutation σ du groupe de Galois de P sur $\mathbb{Q}$ est de la forme $\sigma(\alpha_i) = \alpha_{ai+b \bmod p}$, où $a \not\equiv 0 \bmod p$.
   (e) Montrer la réciproque (indication : cela revient à montrer que le groupe affine $\mathbb{Z}/p\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^*$ est résoluble).
2. On passe à la démonstration du théorème de Galois et Abel.
   (a) Montrer que si $P = 0$ est résoluble par radicaux, avec P irréductible sur $\mathbb{Q}$ et de degré p premier, et $\alpha_1, \ldots, \alpha_p$ ses racines, alors son corps de décomposition est $\mathbb{Q}(\alpha_i, \alpha_j)$ pour tous i et j distincts.
   (b) Réciproquement, supposons que son corps de décomposition K est $\mathbb{Q}(\alpha_i, \alpha_j)$ pour tous i et j distincts. Justifier que cela revient à dire que tout automorphisme de Galois de $K/\mathbb{Q}$ a au plus un point fixe parmi les racines de P.
   (c) Montrer que $\mathrm{Gal}(K/\mathbb{Q})$ contient un p-cycle σ, et qu'il engendre un sous-groupe distingué de $\mathrm{Gal}(K/\mathbb{Q})$.

(d) En déduire que $\mathrm{Gal}(K/\mathbb{Q})$ est résoluble.

3. Soient $p \geqslant 3$, et $P \in \mathbb{Q}[X]$ irréductible de degré p. Montrer que si $P = 0$ est résoluble par radicaux, alors le nombre de ses racines réelles est 1 ou p.

Exercice 3. Soit ζ_{25} une racine primitive 25-ième de l'unité.

1. Donner une sous-extension de $\mathbb{Q}(\zeta_{25})/\mathbb{Q}$ dont le groupe de Galois sur $\mathbb{Q}$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$.
2. Montrer qu'elle est engendrée par $x = \zeta_{25} + \zeta_{25}^{-1} + \zeta_{25}^{7} + \zeta_{25}^{-7}$. En déduire explicitement l'existence d'un polynôme de degré 5 dont le groupe de Galois sur $\mathbb{Q}$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$.

Exercice 4. Soient $\mathbb{F}_q$ un corps fini à $q = p^n$ éléments, où p est premier et n pair, et $K = \mathbb{F}_q(T)$.

1. Montrer que les polynômes $P = X^{p^2} - TX + T$ et $Q = X^{p^2-1} - T$ sont irréductibles dans $K[X]$. Soient α et β des racines, respectivement, de P et Q (dans une clôture algébrique de K).
2. Montrer que l'ensemble des racines de P est $\{\alpha + u \mid u \in \bar{K} \text{ et } u \cdot Q(u) = 0\}$.
3. Montrer que $K(\beta)/K$ est une extension galoisienne, et déterminer son groupe de Galois.
4. Montrer que le corps de décomposition de P sur K est $K(\alpha, \beta)$, puis que $K(\alpha, \beta)/K$ est une extension galoisienne de degré $p^2(p^2 - 1)$.
5. Montrer que le groupe de Galois de $K(\alpha, \beta)/K(\beta)$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$.
6. Montrer que $K(\alpha, \beta)/K$ est résoluble par radicaux.

Exercice 5. Soient $K = \mathbb{C}(T)$ et ζ_n une racine primitive n-ième de l'unité. On note σ le $\mathbb{C}$-automorphisme de K défini par $\sigma(T) = \zeta_n T$ et τ celui défini par $\tau(T) = T^{-1}$.

1. Vérifier que $\sigma^n = \tau^2 = (\sigma\tau)^2 = \mathrm{id}_K$. En déduire que le sous-groupe $G = \langle \sigma, \tau \rangle$ de $\mathrm{Aut}_{\mathbb{C}}(K)$ est de cardinal $2n$.
2. Soit $E = K^G$. Montrer que $E = \mathbb{C}\left(T^n + T^{-n}\right)$ et justifier que K/E est une extension galoisienne de degré $2n$.
3. Donner des extensions intermédiaires justifiant que K/E est résoluble par radicaux.

Exercice 6. Nous allons démontrer le théorème 90 de Hilbert sous sa forme additive : soient L/K une extension galoisienne cyclique de degré n, de groupe de Galois engendré par un automorphisme σ, et x un élément de L. Montrer que $\mathrm{Tr}_{L/K}(x) = 0$ si, et seulement s'il existe $y \in L$ tel que $x = y - \sigma(y)$.

Exercice 7. Montrer qu'une extension galoisienne de degré p d'un corps K de caractéristique p est le corps de décomposition du polynôme $X^p - X - a$ sur K, pour un certain $a \in K$. Une telle extension est dite d'Artin-Schreier.