FEUILLE 10

Exercice 1 — Soit k un corps et soit $f \in k[X]$ un polynôme séparable. On rappelle que le groupe de Galois $\mathrm{Gal}(f)$ de f est le groupe de Galois d'une extension de décomposition k'/k de f.

(i) Démontrer que f est irréductible si et seulement si $\mathrm{Gal}(f)$ opère transitivement sur l'ensemble $\mathscr{R}$ des racines de f dans k'.

(ii) On suppose k de caractéristique distincte de 2. Démontrer que $\mathrm{Gal}(f)$ opère par permutations paires de $\mathscr{R}$ si et seulement si le discriminant de f [(1)] est un carré dans k. [(iii)] Si $k = \mathbb{Q}$ et si $f \in \mathbb{Q}[X]$ un polynôme irréductible admettant au moins une racine réelle et une racine non réelle, démontrer que le groupe $\mathrm{Gal}(f)$ n'est pas abélien.

Exercice 2 (*Polynômes de degré 3*) — Dans cet exercice, k est un corps de caractéristique différente de 2 et 3.

Soit $f = X^3 + pX + q \in k[X]$ un polynôme séparable et soient x_1, x_2, x_3 les trois racines de f dans une extension de décomposition K/k. On adjoint à K une racine cubique primitive de l'unité ρ.

(i) Vérifier le discriminant de f est $\delta = -27q^2 - 4p^3$. Quelles sont les possibilités pour $\mathrm{Gal}(f)$?

(ii) Justifier que l'extension $K(\rho)/k(\sqrt{\delta}, \rho)$ est cyclique. On pose

$$\alpha = x_1 + \rho x_2 + \rho^2 \beta \quad \text{et} \quad \beta = x_1 + \rho^2 x_2 + \rho^2 x_3.$$

Calculer α^3 et β^3 en observant que

$$(x_1 - x_2)(x_2 - x_3)(x_1 - x_3) = (x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1) - (x_1^2 x_3 + x_2^2 x_1 + x_3^2 x_2).$$

(iii) Exprimer x_1, x_2 et x_3 en fonction de α et β.

(iv) Vérifier que l'on a $\alpha\beta = -3p$. En déduire que l'une des racines de f s'écrit sous la forme $u + v$ avec $uv = -p/3$ puis vérifier que u^3 et v^3 sont les racines d'un polynôme de degré 2.

Exercice 3 (*Polynômes de degré 4*) — Dans cet exercice, k est un corps de caractéristique différente de 2 et 3.

1) Soit $f = X^4 + pX^2 + qX + r \in k[X]$ un polynôme séparable et soient x_1, x_2, x_3, x_4 ses racines dans une extension de décomposition K/k. On désigne par V le sous-groupe de $\mathfrak{S}_4$ constitué des quatre éléments 1, $(1,2)(3,4)$, $(1,3)(2,4)$ et $(1,4)(2,3)$ (*Viergruppe* de Klein).

(i) On pose

$$\alpha = (x_1 + x_2)(x_3 + x_4), \quad \beta = (x_1 + x_3)(x_2 + x_4) \quad \text{et} \quad \gamma = (x_1 + x_4)(x_2 + x_3).$$

Vérifier que ces trois éléments de K sont distincts et que $\mathfrak{S}_4$ opère transitivement sur $\{\alpha, \beta, \gamma\}$. En déduire que $k(\alpha, \beta, \gamma)$ est une extension galoisienne de k, de groupe $\mathrm{Gal}(f)/\mathrm{Gal}(f) \cap V$.

(ii) La *résolvante cubique* de f est le polynôme $g = (X - \alpha)(X - \beta)(X - \gamma)$. Déterminer ses coefficients en fonction de ceux de f et vérifier que f et g ont le même discriminant.

(iii) Vérifier que $x_1 + x_2$ (resp. $x_1 + x_3$; resp. $x_1 + x_4$) est une racine carrée de $-\alpha$ (resp. de $-\beta$; resp. de $-\gamma$) puis que l'on $(x_1 + x_2)(x_1 + x_3)(x_1 + x_4) = -q$. Conclure.

2) On désigne par C_4 le sous-groupe cyclique de $\mathfrak{S}_4$ engendré par $(1,2,3,4)$ et par D_4 le sous-groupe engendré par $(1,2,3,4)$ et $(1,3)$.

---

(1) Écrivant f sous la forme $a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$ avec $a_n \neq 0$, on rappelle que le discriminant de f est défini par l'identité

$$\mathrm{disc}(f) = a_n^{2n-2} D(-a_{n-1}/a_n, a_{n-2}/a_n, \ldots, (-1)^n a_0/a_n),$$

où $D(\Sigma_1, \ldots, \Sigma_n)$ est le polynôme $\prod_{1 \leqslant i < j \leqslant n} (X_i - X_j)^2$ exprimé en fonction des polynômes symétriques élémentaires.

(i) Démontrer que tout sous-groupe transitif de $\mathfrak{S}_4$ d'ordre divisible par 4 est conjugué à l'un des sous-groupes suivants :

$$\mathfrak{S}_4,\ \mathfrak{A}_4,\ \mathrm{V},\ \mathrm{D}_4,\ \mathrm{C}_4.$$

(ii) Déterminer $(\mathrm{G} : \mathrm{V} \cap \mathrm{G})$ pour chacun des sous-groupes précédents.

4) Déterminer le groupe de Galois de chacun des polynômes suivants de $\mathbb{Q}[\mathrm{X}]$:

$$\mathrm{X}^4 - 4\mathrm{X} + 2,\ \ \mathrm{X}^4 + 4\mathrm{X}^2 + 2,\ \ \mathrm{X}^4 - 10\mathrm{X}^2 + 4,\ \ \mathrm{X}^4 - 2.$$

Exercice 4 — Soit p un nombre premier impair et soit ξ une racine primitive p-ème de l'unité dans $\mathbb{C}$. On pose $\mathrm{G} = \mathrm{Gal}(\mathbb{Q}(\xi)|\mathbb{Q})$ et on désigne par H le sous-groupe de G d'indice 2.

(i) Démontrer que le sous-corps de $\mathbb{Q}(\xi)$ fixé par H est le corps de décomposition du polynôme $\mathrm{X}^2 + \mathrm{X} + \alpha\beta$, où

$$\alpha = \sum_{\sigma \in \mathrm{H}} \sigma(\xi) \quad \text{et} \quad \beta = \sum_{\sigma \in \mathrm{G}-\mathrm{H}} \sigma(\xi).$$

(ii) Vérifier que l'on a $1 - 4\alpha\beta = \tau^2$, où

$$\tau = \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \xi^a.$$

En déduire que le sous-corps fixé par H est $\mathbb{Q}(\sqrt{p})$ si $p \equiv 1 \pmod 4$, de $\mathbb{Q}(\sqrt{-p})$ si $p \equiv 3 \pmod 4$.

(iii) Démontrer que toute extension quadratique de $\mathbb{Q}$ est contenue dans une extension cyclotomique [(2)].

Exercice 5 (*Un théorème de Galois*) — Galois a démontré qu'une équation est résoluble par radicaux si et seulement si toute racine s'exprime K-rationnellement en fonction de deux quelconques d'entre-elles.

1. Vérifier que l'ensemble $\mathfrak{B}_p$ des permutations de $\mathbb{Z}/p\mathbb{Z}$ de la forme $x \mapsto ax+b$, $a, b \in \mathbb{Z}/p\mathbb{Z}$, est un sous-groupe transitif et résoluble de $\mathfrak{S}(\mathbb{Z}/p\mathbb{Z})$ d'ordre $p(p-1)$. Vérifier également qu'un élément $x \mapsto ax+b$ de $\mathfrak{B}_p$ est d'ordre p si et seulement si $a = 1$ et $b \neq 0$.

2. Soit réciproquement G un sous-groupe transitif et résoluble du groupe symétrique $\mathfrak{S}(\mathbb{Z}/p\mathbb{Z})$. On considère une suite de composition

$$(1) = \mathrm{G}_0 \lhd \mathrm{G}_1 \lhd \ldots \lhd \mathrm{G}_r = \mathrm{G}$$

de G à quotients cycliques d'ordre premier.

(i) Démontrer que chacun des groupes $\mathrm{G}_1, \ldots, \mathrm{G}_r$ opère transitivement sur $\mathbb{Z}/p\mathbb{Z}$; en déduire que G_1 est engendré par une permutation circulaire τ.

(ii) Vérifier qu'il existe une permutation $\sigma \in \mathfrak{S}(\mathbb{Z}/p\mathbb{Z})$ telle que $\sigma \mathrm{G}_2 \sigma^{-1} \subset \mathfrak{B}_p$.

(iii) En raisonnant par récurrence sur r, démontrer que G_1 est un sous-groupe distingué de G et en déduire que $\sigma \mathrm{G} \sigma^{-1}$ est un sous-groupe de $\mathfrak{B}_p$.

Soit K un corps, soit $\mathrm{P} \in \mathrm{K}[\mathrm{T}]$ un polynôme irréductible de degré premier p et soit L un corps de décomposition de P ; on identifie le groupe de Galois de l'extension L/K à un sous-groupe du groupe des permutations de l'ensemble des racines de P dans L.

3. Supposons qu'il existe deux racines distinctes $\alpha,\ \beta$ de P dans L telles que $\mathrm{L} = \mathrm{K}(\alpha, \beta)$.

(i) Vérifier que $[\mathrm{L} : \mathrm{K}] \leq p(p-1)$.

(ii) Vérifier que le groupe $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ contient une permutation circulaire d'ordre p puis que deux telles permutations engendrent le même sous-groupe.

(iii) Démontrer que le groupe $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ est résoluble.

4. Supposons réciproquement que le groupe $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ soit résoluble. Démontrer que l'on a $\mathrm{L} = \mathrm{K}(\alpha, \beta)$ pour toutes racines distinctes $\alpha,\ \beta$ de P dans L.

[(2)] Plus généralement, toute extension galoisienne de $\mathbb{Q}$ à groupe de Galois *abélien* est contenue dans $\mathbb{Q}$ (théorème de Kronecker-Weber)