

Feuille d'exercices 5

Soient k un corps parfait et Ω une clôture algébrique de k . On rappelle qu'une sous-extension finie K/k de Ω est *galoisienne* si pour chaque $x \in K$, tous les k -conjugués de x dans Ω appartiennent à K . D'après un résultat du cours, il est équivalent de demander que l'inclusion naturelle $\text{Hom}_k(K, K) \subset \text{Hom}_k(K, \Omega)$ soit une égalité, de sorte que $|\text{Hom}_k(K, K)| = [K : k]$. Le groupe $\text{Gal}(K/k) = \text{Hom}_k(K, K)$ est appelé *groupe de Galois* de K/k . Si $x \in K$, les k -conjugués de x sont alors permutés transitivement par $\text{Gal}(K/k)$.

Si $P \in k[X]$, on note R_P l'ensemble de ses racines dans Ω et $\text{Gal}(P, k)$ le groupe de Galois de l'extension galoisienne $k(R_P)$ sur k .

Exercice 1. Soient $K_1 \subset \Omega$ et $K_2 \subset \Omega$ des extensions galoisiennes de k . Montrer que $K_1 \cap K_2$ et $K_1 K_2$ sont aussi galoisiens sur k .

Exercice 2. Soit $P \in k[X]$ un polynôme irréductible de degré n et soit $G = \text{Gal}(P, k)$.

- (i) Rappeler pourquoi $|R_P| = n$.
- (ii) En déduire que n divise $|G|$ et que $|G|$ divise $n!$.

Exercice 3. Soit $g \in \mathbf{Q}[X]$ le polynôme cubique unitaire dont les racines réelles sont $x_1 = 2 \cos(2\pi/7)$, $x_2 = 2 \cos(4\pi/7)$ et $x_3 = 2 \cos(6\pi/7)$.

- (i) Vérifier que $g = X^3 + X^2 - 2X - 1$.
- (ii) Montrer que g est irréductible.
- (iii) Montrer que $\mathbf{Q}(x_1)$ est un corps de décomposition de g .
- (iv) En déduire $\text{Gal}(g)$.
- (v) Indiquer une méthode pour calculer le *discriminant* de g , $\Delta = \prod_{i < j} (x_i - x_j)^2$.

Exercice 4. Soient $f = X^4 - 4X^2 - 1 \in \mathbf{Q}[X]$ et $g = Y^2 - 4Y - 1 \in \mathbf{Q}[Y]$.

- (i) Pourquoi le groupe $\text{Gal}(g, \mathbf{Q})$ est-il un quotient de $G = \text{Gal}(f, \mathbf{Q})$?
- (ii) Montrer que G est un sous-groupe de $\mathfrak{S}_{R_f}$ *compatible* avec la partition

$$\{\{\sqrt{2 + \sqrt{5}}, -\sqrt{2 + \sqrt{5}}\}, \{\sqrt{2 - \sqrt{5}}, -\sqrt{2 - \sqrt{5}}\}\}$$

de R_f . (On dit qu'une permutation σ d'un ensemble fini E est *compatible* avec une partition de E lorsque $x \sim y$ implique $\sigma(x) \sim \sigma(y)$ pour $\sim$ la relation d'équivalence dont les classes sont la partition considérée.)

- (iii) En déduire que G est contenu dans le groupe diédral du carré.
- (iv) Montrer qu'il existe un élément $\sigma \in G$ tel que $\sigma(\sqrt{2 + \sqrt{5}})$ est égal à $\sqrt{2 - \sqrt{5}}$ ou $-\sqrt{2 - \sqrt{5}}$.
- (v) Montrer qu'il existe un élément $\tau \in G$ échangeant $\sqrt{2 - \sqrt{5}}$ et $-\sqrt{2 - \sqrt{5}}$ mais fixant $\sqrt{2 + \sqrt{5}}$.
- (vi) En déduire que G est le groupe diédral tout entier.

Exercice 5. Soit p premier et soient σ, τ respectivement une transposition et un p -cycle dans $\mathfrak{S}_p$. On note $G \subseteq \mathfrak{S}_p$ le sous-groupe engendré par τ et σ . Sans perte de généralité on pourra supposer que $\tau = (1, 2 \cdots, p)$ et $\sigma = (i, i+l)$ avec $1 \leq i < i+l \leq p$. Dans la suite, on considèrera tous les entiers modulo p .

- (i) Montrer que $(i+l, i+2l)$ appartient à G , puis qu'il en est de même pour $(i, i+2l)$.
- (ii) Montrer que $(i, i+kl) \in G$ pour tout $k \in \mathbf{N}$.
- (iii) En déduire que $G = \mathfrak{S}_p$.

Exercice 6. Soient $P = X^5 - 4X + 2 \in \mathbf{Q}[X]$ et $G = \text{Gal}(P, \mathbf{Q})$.

- (i) Vérifier que P est irréductible sur $\mathbf{Q}$.
- (ii) Montrer que P a exactement trois racines réelles. En déduire que G , vu comme groupe de permutations des racines de P dans $\mathbf{C}$, contient une transposition.
- (iii) Montrer que G contient un 5-cycle.
- (iv) Montrer que $G = \mathfrak{S}_5$. (On pourra utiliser l'exercice précédent.)
- (v) Modulo 257, P se décompose sous la forme $P = (X+91)(X-53)(X-31)(X^2-7X-118)$. Indiquer une méthode pour montrer que le dernier facteur est irréductible. (On verra plus tard que cela force G à contenir une transposition.)

Exercice 7. Soit $\overline{\mathbf{Q}} \subset \mathbf{C}$ le corps des nombres algébriques. On se propose de montrer que le groupe $\text{Aut}_{\mathbf{Q}}(\overline{\mathbf{Q}})$ (« groupe de Galois absolu de $\mathbf{Q}$ ») est infini non dénombrable.

- (i) Soit $(X_n)_{n \geq 1}$ une famille d'ensembles finis, et pour tout $n \geq 1$ soit $f_n : X_{n+1} \rightarrow X_n$ une application surjective. On note $\lim_n X_n$ l'ensemble des suites $(x_n)_{n \geq 1}$ telles que pour tout $n \geq 1$, $x_n \in X_n$ et $f_n(x_{n+1}) = x_n$. Montrer que si $|X_n| \rightarrow \infty$ quand $n \rightarrow \infty$ alors $\lim_n X_n$ est infini non dénombrable. (On pourra penser à l'argument diagonal de Cantor)
- (ii) Montrer qu'il existe une famille $(K_n)_{n \geq 1}$, où $K_n \subset \overline{\mathbf{Q}}$ est une extension galoisienne de $\mathbf{Q}$ et $K_n \subset K_{n+1}$, telle que $\overline{\mathbf{Q}} = \bigcup_{n \geq 1} K_n$.
- (iii) Montrer que l'application $\sigma \mapsto (\sigma|_{K_n})_n$ définit une bijection $\text{Aut}_{\mathbf{Q}}(\overline{\mathbf{Q}}) \xrightarrow{\sim} \lim_n \text{Gal}(K_n/\mathbf{Q})$.
- (iv) Conclure.