

Feuille d'exercices 6

Exercice 1. On suppose que k est un corps parfait de caractéristique $\neq 2$. Soit $P = X^3 + aX + b \in k[X]$ irréductible ; on note $\alpha_1, \alpha_2, \alpha_3$ ses racines dans un corps de décomposition K de P . On rappelle que le discriminant $\delta(P) = \left(\prod_{i < j} (\alpha_i - \alpha_j)\right)^2$ vaut $-4a^3 - 27b^2$.

(i) Montrer que le groupe de Galois de P sur k vaut $\mathfrak{A}_3$ ou $\mathfrak{S}_3$ selon que $\delta(P)$ est un carré ou non dans k .

(ii) Dans tous les cas, décrire les sous-extensions de K/k .

(iii) Donner un polynôme explicite de $\mathbf{Q}[X]$ dont le groupe de Galois sur $\mathbf{Q}$ est $\mathbf{Z}/3\mathbf{Z}$ (resp. $\mathfrak{S}_3$).

(iv) On ne suppose plus k de caractéristique différente de 2. Soit $f \in k[Z_1, Z_2, Z_3] = Z_1Z_2^2 + Z_2Z_3^2 + Z_3Z_1^2$. Montrer qu'une permutation $\sigma \in \mathfrak{S}_3$ est paire si et seulement si $\sigma(f) = f$. (On fait agir $\mathfrak{S}_3$ par permutation des variables.)

(v) Montrer que $R_f(P) = \prod_{\sigma \in \mathfrak{S}_3/\mathfrak{A}_3} (T - \sigma(f)(\alpha_1, \alpha_2, \alpha_3))$ appartient à $k[T]$ et l'exprimer en fonction de a et b .

(iv) En déduire que si k est de caractéristique 2, le groupe de Galois de P est contenu dans $\mathfrak{A}_3$ ou $\mathfrak{S}_3$ selon que $1 + a^3b^{-2}$ est de la forme $x^2 + x$ ($x \in k$) ou pas.

Exercice 2. 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 3. 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 4. Soient k parfait, K/k une extension galoisienne finie, et L_1, L_2 deux sous- k -extensions. On note L_1L_2 le sous-corps engendré par L_1 et L_2 , et on pose $G_i = \text{Gal}(K/L_i)$.

(i) Montrer que $\text{Gal}(K/L_1L_2) = G_1 \cap G_2$ et que $\text{Gal}(K/L_1 \cap L_2)$ est le sous-groupe de $\text{Gal}(K/k)$ engendré par G_1 et G_2 .

(ii) Supposons $K = L_1L_2$, L_1/k et L_2/k galoisiennes, et $k = L_1 \cap L_2$. Montrer que $\text{Gal}(K/k) \simeq G_1 \times G_2$.

Exercice 5. Soit $P(x) \in k[x]$ un polynôme irréductible de degré n et K un corps de décomposition.

- (i) Montrer que si $\text{Gal}(K/k)$ est abélien alors $[K : k] = n$.
- (ii) Est-ce que la réciproque est vraie ?
- (iii) ($k = \mathbf{Q}$) On suppose que $P(x)$ a des racines réelles et des racines imaginaires. Montrer que $\text{Gal}(K/k)$ n'est pas abélien. Donner un contre-exemple si P n'est plus supposé irréductible.

Exercice 6. (Normes et traces) Soit k un corps parfait et soit K/k une extension galoisienne finie de groupe de Galois $\text{Gal}(K/k) = G$. On considère les applications suivantes :

$$N_{K/k} : K \rightarrow K, \quad x \mapsto \prod_{\sigma \in G} \sigma(x)$$

(norme relative de K à k) et

$$\text{Tr}_{K/k} : K \rightarrow K, \quad x \mapsto \sum_{\sigma \in G} \sigma(x)$$

(norme relative de K à k).

- (i) Montrer que $N_{K/k}$ et $\text{Tr}_{K/k}$ sont en fait à valeurs dans k , i.e. $N_{K/k}(x) \in k$ et $\text{Tr}_{K/k}(x) \in k$ pour tout $x \in K$.
- (ii) Montrer que $K \rightarrow K^\vee = \text{Hom}_{k\text{-ev}}(K, k)$, $x \mapsto \text{Tr}_{K/k}(x \cdot)$ est un isomorphisme de k -espaces vectoriels.
- (iii) Montrer que

$$N_{K/k}(xy) = N_{K/k}(x)N_{K/k}(y), \quad \text{Tr}_{K/k}(x+y) = \text{Tr}_{K/k}(x) + \text{Tr}_{K/k}(y)$$

pour tout $x \in K$.

(iv) Supposons que $K = k(\sqrt{D})$ où $D \in k$ n'est pas un carré. Calculer $N_{K/k}(a + b\sqrt{D})$ et $\text{Tr}_{K/k}(a + b\sqrt{D})$.

(v) Plus généralement, pour $\alpha \in K$ de polynôme minimal $P(X) = a_0 + \cdots + a_d X^d$, calculer $N_{K/k}(\alpha)$ et $\text{Tr}_{K/k}(\alpha)$ en fonction de d , de $n = [K : k] = |G|$ et de $a_0, \dots, a_d$.

(vi) Soit $\alpha \in K^*$ et $\sigma \in G$. Montrer que $N_{K/k}(\alpha/\sigma(\alpha)) = 1$ et $\text{Tr}(\alpha - \sigma(\alpha)) = 0$.

(vii) On suppose maintenant que G est cyclique. Montrer que si $\text{Tr}_{K/k}(\alpha) = 0$ alors il existe $x \in K$ et $g \in G$ tel que $\alpha = x - g(x)$.

[Note : le 'Hilbert Satz 90' fournit un analogue multiplicatif de (vi) : si $\beta \in K$ vérifie $N_{K/k}(\beta) = 1$, alors il existe $x \in K$ et $g \in G$ tels que $\beta = x/g(x)$.