

Feuille d'exercices 7

Exercice 1. Soient p un nombre premier et $f \in \mathbf{F}_p[T]$ un polynôme irréductible. Considérons la \mathbf{F}_p -algèbre

$$B = \mathbf{F}_p[T]/(f),$$

munie du morphisme de Frobenius

$$F : B \rightarrow B, b \mapsto b^p.$$

Montrer que

$$\dim_{\mathbf{F}_p} \text{Ker}(F - \text{Id} : B \rightarrow B) = 1.$$

Réciproquement, est-ce que cette condition implique que f est irréductible ?

Exercice 2. Soient q une puissance d'un nombre premier p et $n \geq 1$ un entier.

(i) Montrer que l'extension $\mathbf{F}_{q^n}/\mathbf{F}_q$ est galoisienne de groupe de Galois cyclique d'ordre n engendré par $x \mapsto x^q$.

(ii) Expliciter la correspondance de Galois pour cette extension.

Exercice 3. Soit $x = \sqrt[4]{2}$, et $K = \mathbf{Q}[x, i]$.

(i) Montrer que K est galoisienne sur \mathbf{Q} , que

$$[K : \mathbf{Q}] = 8,$$

puis que $\text{Gal}(K/\mathbf{Q})$ est isomorphe au groupe diédral D_4 .

(ii) Expliciter la correspondance de Galois dans l'extension K/\mathbf{Q} .
En particulier, donner tous les sous-corps de degré 2 et 4 de K .

Exercice 4. (Une preuve par la théorie de Galois du théorème de d'Alembert-Gauss) Soit K une extension finie de \mathbf{R} , on veut montrer que $K = \mathbf{R}$ ou \mathbf{C} .

(i) Montrer que si K/\mathbf{R} est de degré 2, alors $K \simeq \mathbf{C}$.

(ii) Montrer que si K/\mathbf{R} est de degré impair, alors $K = \mathbf{R}$.

(iii) Montrer que \mathbf{C} n'admet pas d'extension de degré 2.

(iv) Supposons K/\mathbf{R} galoisienne finie. Montrer l'existence d'une tour d'extensions

$$\mathbf{R} \subset K_1 \subset K_2 \subset \cdots \subset K_n = K$$

telle que $[K_1 : \mathbf{R}]$ est impair et, pour $i = 1, \dots, n-1$, $[K_{i+1} : K_i] = 2$.

On pourra utiliser les résultats suivants de théorie des groupes (admis). Soient G un groupe fini et p un nombre premier. Écrivons $|G| = p^\alpha m$ où $(p, m) = 1$. Alors il existe un sous-groupe $P \subset G$ de cardinal p^α (*Théorème de Sylow*). De plus, si $m = 1$ il existe une suite de sous-groupes $G_1 \subset G_2 \subset \cdots \subset G_\alpha = G$, avec $|G_i| = p^i$ et G_i distingué dans G .

(v) Conclure.

Exercice 5.

(i) Montrer que $5 + \sqrt{21}$ n'est pas un carré dans $\mathbf{Q}[\sqrt{21}]$

Soient

$$z = \sqrt{5 + \sqrt{21}} \text{ et } K = \mathbf{Q}[z].$$

(ii) Montrer $[K : \mathbf{Q}] = 4$.

(iii) Soit

$$z' = \sqrt{5 - \sqrt{21}}.$$

Montrer $z' \in K$ [Calculer zz']. En déduire les conjugués (sur \mathbf{Q}) de z puis que K/\mathbf{Q} est galoisienne.

Soit $G = \text{Gal}(K/\mathbf{Q})$.

(iv) Montrer qu'il existe un unique élément $g \in G$ tel que $g(z) = -z$.

(v) Montrer qu'il existe un unique élément $h \in G$ tel que $h(z) = z'$.

(vi) Montrer qu'on a $g(z') = -z'$ et $h(z') = z$. En déduire que g et h commutent puis que

$$G \simeq (\mathbf{Z}/2\mathbf{Z})^2.$$

(vii) Décrire les sous-corps de K .

Exercice 6. On considère le polynôme

$$P(X) = X^3 - 3X - 4 \in \mathbf{Q}[X].$$

(i) Montrer que P est un polynôme irréductible dans $\mathbf{Q}[X]$.

Soit

$$x = \sqrt[3]{2 + \sqrt{3}}.$$

(ii) Montrer que 2 divise $[\mathbf{Q}[x] : \mathbf{Q}]$.

(iii) Montrer que

$$[\mathbf{Q}[x] : \mathbf{Q}] = 6.$$

(iv) Est-ce que $\mathbf{Q}[x]/\mathbf{Q}$ est galoisienne ?

(v) Montrer que x admet un unique conjugué y réel distinct de x .

(vi) Montrer que

$$\mathbf{Q}[x] = \mathbf{Q}[y].$$

(vii) Exprimer chaque racine de P comme combinaison linéaire de deux conjugués de x . En déduire le corps de décomposition K de P dans \mathbf{C} .

(viii) Déterminer $[K : \mathbf{Q}]$.