École Polytechnique
Algèbre et théorie de Galois MAT 451

Contrôle classant du 29 mars 2017 - 3 heures

Avertissement

Les calculatrices et documents autres que le polycopié de cours sont interdits. La rédaction doit être concise et précise. Les exercices sont indépendants. Il n'est pas nécessaire de terminer le sujet pour avoir une excellente note.

Exercice 1.

Soient
$$M = \mathbf{Q}[\sqrt{2}, \sqrt{3}]$$
et $E = M[x]$ avec
$$x = \sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}.$$

1) Montrer que $M/\mathbf{Q}$ est une extensions galoisienne de degré 4.
2) Est-ce que le groupe de Galois $\mathrm{Gal}(M/\mathbf{Q})$ est cyclique ?
3) Montrer que $E = \mathbf{Q}[x]$.
4) Montrer que $E/\mathbf{Q}$ est algébrique et que x a au plus 8 conjugués sur $\mathbf{Q}$.
5) Montrer que $E/\mathbf{Q}$ est une extension galoisienne.
6) Déterminer le degré de $E/\mathbf{Q}$.
7) Montrer que $G = \mathrm{Gal}(E/\mathbf{Q})$ a un sous-groupe distingué d'ordre 2.
8) Montrer que les éléments de ce sous-groupe commutent avec tous les éléments de $\mathrm{Gal}(E/\mathbf{Q})$.
9) Montrer que G est résoluble.
10) Est-ce que G est commutatif ?

Exercice 2

Soit k un corps de caractéristique nulle et
$$L = k(X)$$

le corps des fractions rationelles à coefficients dans k. On rappelle qu'il est constitué des quotients
$$\frac{P(X)}{Q(X)}$$
de polynômes $P, Q \in k[X]$ avec Q non nul.

1) Montrer qu'il existent $\sigma, \tau \in \mathrm{Aut}_k(L)$ uniques tels que
$$\sigma(X) = 1 - X \text{ et } \tau(X) = X^{-1}.$$

Soit G le sous-groupe de $\mathrm{Aut}_k(L)$ engendré par σ et τ.

2) Calculer l'ordre de $\sigma \circ \tau$ dans le groupe G.
3) Montrer que l'ordre de G est divisible par 6.
4) En déduire que G a 6 éléments et les exprimer en fonction de σ et τ.
5) En déduire que $G \simeq S_3$.

Soit $K = L^G$ l'algèbre des éléments fixés par l'action de G.

6) Montrer que L/K est une extension galoisienne finie dont on donnera le degré.

Soit
$$Y = \frac{X^3 - 3X + 1}{X(X-1)} \in L.$$

7) Comparer $\tau(Y)$ et $\sigma(Y)$.

Soit
$$Z = Y\sigma(Y)$$
et $k(Z)$ le sous-corps de L engendré par k et par Z.

8) Est-ce que $k(Z) \subset K$?
9) Montrer que X est de degré au plus 6 sur $k(Z)$.
10) En déduire une expression de K.
11) Combien L contient-elle de sous $k(Z)$-algèbres ?
12) Déterminer $L^{\tau\circ\sigma}$ l'algèbre des éléments fixés par $\sigma \circ \tau$.

Exercice 3

Soit $F \subset \mathbf{C}$ une extension galoisienne de $\mathbf{Q}$.

1) Montrer qu'on peut définir le groupe quotient $F^*/(F^*)^2$.
2) Montrer que $\mathrm{Gal}(F/\mathbf{Q})$ agit sur ce groupe quotient.

On suppose qu'il existe $\alpha \in F^*$ dont la classe dans $F^*/(F^*)^2$ n'est pas fixe pour cette action.
On considère

$$\alpha = \alpha_1, \cdots, \alpha_n$$

ses $\mathbf{Q}$-conjugués dans F. Soit enfin

$$K = F[\sqrt{\alpha_1}, \cdots, \sqrt{\alpha_n}]$$

la F-algèbre engendrée par les racines carrées des α_i, $1 \leq i \leq n$.

3) Montrer que $K/\mathbf{Q}$ est galoisienne.

4) Montrer que le groupe de Galois $\mathrm{Gal}(K/F)$ est commutatif isomorphe à un sous-groupe du produit $(\mathbf{Z}/2\mathbf{Z})^n$ de n groupes d'ordre 2.

5) Est-ce que $\mathrm{Gal}(K/\mathbf{Q})$ est commutatif ?

Exercice 4

Soit E un espace vectoriel de dimension finie sur un corps K. On admet que pour $u \in \mathrm{End}_K(E)$ un endomorphisme de E, u est diagonalisable si et seulement si il est annulé par un polynôme $P(X) = a_n X^n + \cdots + a_0$ scindé à racines simples et à coefficients dans K. Cela signifie que :

$$a_n u^n + a_{n-1} u^{n-1} + \cdots + a_0 \mathrm{Id} = 0,$$

les puissances étant prises au sens de la composition. On dit alors que u est K-diagonalisable.

1) Supposons que K est une extension de k et que u est K-diagonalisable. Est-ce qu'alors u est k-diagonalisable ? Réciproque ?

Soient $u, v \in \mathrm{End}_K(E)$ K-diagonalisables tels que pour tous $\lambda \in K$,

$$u + \lambda v$$

est K-diagonalisable.

2) Est-ce que nécessairement $u \circ v = v \circ u$?

3) On suppose que $K = \mathbf{F}_q$ pour $q = p^N$ avec p premier. Montrer que w est $\mathbf{F}_q$-diagonalisable si et seulement si

$$w^q = w.$$

4) On suppose que $K = \mathbf{F}_2$. Montrer que

$$u \circ v = v \circ u.$$