École Polytechnique
Algèbre et théorie de Galois MAT 451

Contrôle classant du 29 mai 2019 - 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.

On admet que le déterminant de Vandermonde $det((\alpha_i^{j-1})_{1\leq i,j\leq n})$ *est non nul pour* $n \geq 1$ *et des éléments distincts* α_i *d'un corps.*

Exercice 1

Soient K un corps parfait de caractéristique 2, Ω une clôture algébrique de K et $L \subset \Omega$ une extension galoisienne de degré 2 de K.

1) Montrer que le polynôme minimal de tout élément de L qui n'est pas dans K a trois coefficients non nuls.
2) Montrer qu'il existe $a \in K$ tel que L est le corps de décomposition du polynôme

$$P(X) = X^2 - X + a.$$

Dans la suite on notera ce polynôme P_a et son corps de décomposition L_a.
3) Ecrire la matrice des éléments de $\mathrm{Gal}(L/K)$ dans la base $(1, b)$ où b est une racine de $P(X)$.
4) Soient $a, a' \in K$ tels que les corps L_a, L_b sont des extensions galoisiennes de K de degré 2 comme ci-dessus. Montrer que

$$L_a = L_{a'}$$

si et seulement s'il existe $\beta \in K$ avec

$$a - a' = \beta^2 - \beta.$$

5) Commenter les résultats ci-dessus pour $K = \mathbf{F}_2$.

6) Soit $N \geq 1$. Déterminer et commenter le nombre de polynômes irréductibles dans $\mathbf{F}_{2^N}[X]$ de la forme

$$X^2 - X + a.$$

7) Montrer que si

$$X^2 - X + a \in \mathbf{F}_{2^N}[X]$$

est irréductible dans $\mathbf{F}_{2^N}[X]$, alors il divise

$$X^{(2^N)} + X + a.$$

8) Soient q une puissance d'un nombre premier p, $\mathbf{F}_q$ un corps de cardinal q et

$$f(X) = X^2 + aX + b \in \mathbf{F}_q[X].$$

Montrer que $f(X)$ est irréductible dans $\mathbf{F}_q[X]$ si et seulement s'il divise $X^q + X + a$.

Exercice 2

Soient L un corps et G un sous-groupe fini du groupe $\mathrm{Aut}(L)$ des automorphismes du corps L. On considère

$$K = L^G$$

l'ensemble des points fixes de L sous l'action de G.

1) Montrer que K est un sous-corps de L.

Pour $x \in L$, on note le stabilisateur

$$G_x = \{g \in G | g(x) = x\},$$

et l'orbite

$$G.x = \{g(x) | g \in G\}.$$

2) Montrer que pour $x \in L$, on a

$$K[x] \subset L^{G_x}.$$

On se propose de montrer l'inclusion réciproque selon une méthode dûe à Lagrange.

Soit $y \in L^{G_x}$.

3) Montrer qu'il existe une unique application

$$\phi : G.x \to G.y$$

telle que $\phi(x) = y$ et telle que pour tous $g \in G$ et $z \in G.x$:

$$\phi(g.z) = g.\phi(z).$$

4) Démontrer qu'il existe un unique polynôme $P(X) \in L[X]$ de degré strictement inférieur au cardinal $|G.x|$ qui prend les mêmes valeurs que ϕ sur $G.x$.

5) Conclure.

Exercice 3.

Soit p un nombre premier. On souhaite déterminer le nombre maximal d'anneaux de cardinal p^2 non isomorphes (c'est-à-dire le nombre de "classes d'isomorphisme" d'anneaux de cardinal p^2).

Soit A un anneau de cardinal p^2.

1) Montrer que la caractéristique de A est p ou p^2.

2) Montrer que si A est de caractéristique p^2, alors il est isomorphe à

$$\mathbf{Z}/p^2\mathbf{Z}.$$

3) Montrer que si A est de caractéristique p, alors il est isomorphe à un quotient de l'anneau des polynômes $\mathbf{F}_p[X]$.

4) Conclure.

Exercice 4

Soient $d \geq 1$ entier et $P(X) \in k[X]$ un polynôme irréductible à coefficients dans un corps parfait k de la forme

$$P(X) = 1 + a_1 X + \cdots + a_{d-1} X^{d-1} + a_d X^d + a_{d-1} X^{d+1} + \cdots + a_1 X^{2d-1} + X^{2d}.$$

Montrer que le groupe de Galois $\mathrm{Gal}(P, k)$ est d'ordre au plus $2^d d!$.