Partiel, mercredi 26 mars 2014, 14h30-16h30

Les règles du jeu :

1. Vous pouvez utiliser tout résultat du cours ... sauf si la question est de démontrer un tel résultat.

2. Les documents, sauf les notes de cours de M. Tchoudjem sur sa page internet, ainsi que la communication avec les autres étudiants ne sont pas autorisés.

3. Les questions à l'enseignant sont encouragées.

4. Il y a 5 exercices (25 points à gagner) qui attendent vos réponses. Bon travail ...

Un peu de théorie

Exercice 1 (Rappels) a) (1 pt) Soit L/K une extension galoisienne finie. Soit $\alpha \in L$. Montrer que α est un élément primitif si et seulement si le cardinal de son orbite sous l'action de $\mathrm{Gal}(L/K)$ est $[L : K]$.

b) (2 pts) Soient $K \leq L$ deux corps. On suppose que L est le corps de décomposition d'un polynôme séparable $P \in K[X]$. Montrer que l'action de $\mathrm{Gal}(L/K)$ sur les racines de P est transitive si et seulement si P est irréductible sur K.

c) (1 pt) Soit K un corps. Montrer que si L est le corps décomposition d'un polynôme $P \in K[X]$, alors l'extension L/K est une extension normale.

Exercice 2 (Éléments primitifs : théorie) Soient K un corps *infini* et $L = K(\alpha, \beta)$ une extension algébrique. On suppose aussi que β est séparable sur K. L'objectif de cet exercice est de montrer que L/K contient un élément primitif.

On définit P et Q les polynômes minimaux de α et de β respectivement. Leurs degrés sont notés d_P et d_Q respectivement. On fixe une extension Ω de L où P et Q sont scindés. On note leurs ensembles de racines respectifs $\{\alpha_1, \ldots, \alpha_{d_P}\}$ et $\{\beta_1, \ldots, \beta_{d_Q}\}$, avec $\alpha_1 = \alpha$ et $\beta_1 = \beta$.

a) (1 pt) Montrer qu'il existe $t \in K$ tel que $t \neq \frac{\alpha_i - \alpha_k}{\beta_l - \beta_j}$ pour tous $1 \leq i, k \leq d_P$ et $1 \leq j \neq l \leq d_Q$. En déduire que $\alpha_i + t\beta_j \neq \alpha_k + t\beta_l$ pour tous $1 \leq i, k \leq d_P$ et $1 \leq j \neq l \leq d_Q$.

b) (1 pt) Montrer que le PGCD unitaire $h(X)$ des polynômes $Q(X)$ et $P(\alpha + t\beta - tX)$ dans $K(\alpha + t\beta)[X]$ est de degré au moins 1. (*Vous pouvez expliciter une racine commune*)

c) (3 pts) Montrer que h est linéaire. Quel est son terme constant ? (*Le polynôme Q n'a pas de racine multiple*).

d) (1 pt) Déduire du point précédent que $K(\alpha, \beta) = K(\alpha + t\beta)$.

Un peu de pratique

Exercice 3 (Éléments primitifs : pratique) Soient P le polynôme $X^5 - 2$ sur $\mathbb{Q}$, L le corps de décomposition de P sur $\mathbb{Q}$.

a) (0.5 pt) Montrer que P irréductible sur $\mathbb{Q}$.

b) (0.5 pt) Montrer que $L/\mathbb{Q}$ est une extension galoisienne.

c) (0.5 pt) Soit μ une racine primitive cinquième de 1. Montrer que $\mu \in L$ et que $[\mathbb{Q}(\mu) : \mathbb{Q}] = 4$.

d) (1.5 pts) Montrer que $L = \mathbb{Q}(\mu, 2^{1/5})$ et que $[L : \mathbb{Q}] = 20$. Quel est le polynôme minimal de $2^{1/5}$ sur $\mathbb{Q}(\mu)$?

e) (1 pt) Montrer que $\mathrm{Gal}(L/\mathbb{Q})$ n'est pas commutatif.

f) (1 pt) Montrer que $\mathrm{Gal}(L/\mathbb{Q}(\mu))$ est distingué dans $\mathrm{Gal}(L/\mathbb{Q})$.

g) (3 pts) Montrer que pour tout $0 \leq i \leq 4$, il existe un élément de $\mathrm{Gal}(L/\mathbb{Q})$ qui fixe μ et transforme $2^{1/5}$ en $2^{1/5}\mu^i$. Montrer que pour tout $1 \leq i \leq 4$, il existe un élément de $\mathrm{Gal}(L/\mathbb{Q})$ qui fixe $2^{1/5}$, et qui transforme μ en μ^i. Déterminer l'orbite de $2^{1/5} + \mu$ sous l'action du groupe de Galois $\mathrm{Gal}(L/\mathbb{Q})$ et en déduire que $2^{1/5} + \mu$ est un élément primitif de $L/\mathbb{Q}$.

Exercice 4 (Corps finis) Soient e, m deux entiers strictement supérieurs à 1. On fixe un nombre premier p qui ne divise pas e et q une puissance non nulle de p.

a) (3 pts) On note :

$$\Phi_e = \prod_{x \text{ d'ordre } e \text{ dans } \mathbb{F}_{q^m}} (X - x) .$$

Montrer que $\Phi_e \in \mathbb{F}_q[X]$. Montrer que le groupe de Galois de Φ_e sur $\mathbb{F}_q$ est cyclique engendré par l'automorphisme $t \mapsto t^q$. En utilisant la question b) de l'exercice 1, montrer que si Φ_e est irréductible sur $\mathbb{F}_q$, alors le groupe des inversibles de $\mathbb{Z}/e\mathbb{Z}$ est cyclique engendré par $q \bmod e$.

b) (1 pt) Montrer que Φ_{12} est réductible sur tout corps fini de caractéristique $\neq 2, 3$.

Exercice 5 (Éléments transcendants) On définit $K = \mathbb{C}(t^4)$ et $L = \mathbb{C}(t)$, où t est transcendant sur $\mathbb{C}$. On pose $P(X) = X^4 - t^4$.

a) (1 pt) Montrer que L est le corps de décomposition de P sur K. En déduire que L/K est une extension galoisienne de degré ≤ 4.

b) (2 pts) Déterminer $\mathrm{Gal}(L/K)$ et en déduire l'irréductibilité du polynôme P sur K (*trouver d'abord l'ordre de l'automorphisme $t \longmapsto \sqrt{-1}\, t$*).