Université Paul Sabatier-Toulouse 3.
Master 1 de mathématiques fondamentales.
Algèbre. Examen du 22 janvier 2008[1]*.*

I. Soient $\mathbb{F}_5$ un corps à 5 éléments et le polynôme

$$P(X) = X^5 - X + 1 \in \mathbb{F}_5[X].$$

(1) Montrer que $P(X)$ n'a pas de racine dans $\mathbb{F}_5$.

(2) Soient $\mathbb{F}_5^{\mathrm{alg}}$ une clôture algébrique de $\mathbb{F}_5$ et $\alpha \in \mathbb{F}_5^{\mathrm{alg}}$ tel que $\alpha^2 = 2$.

  (a) Montrer que $\mathbb{F}_5(\alpha)$ est une extension de degré 2 de $\mathbb{F}_5$.

  (b) Montrer que $P(X)$ n'a pas de racine dans $\mathbb{F}_5(\alpha)$.

(3) *En déduire* que $P(X)$ est irréductible sur $\mathbb{F}_5$.

II. Soient $\mathbb{F}_5$ un corps à 5 éléments, $K = \mathbb{F}_5(T)$ une corps de fractions rationnelles à une indéterminée et le polynôme

$$Q(X) = X^5 - X + T \in K[X].$$

(1) Montrer que $Q(X)$ est irréductible sur K.

(2) Soient K^{alg} une clôture algébrique de K et $\theta \in K^{\mathrm{alg}}$ une racine de $Q(X)$.

  (a) Montrer que, si θ' est une autre racine de $Q(x)$ (dans K^{alg}), alors $\theta - \theta' \in \mathbb{F}_5$; en déduire que $K(\theta)/K$ est une extension galoisienne.

  (b) Montrer que l'application

$$\mathrm{Gal}(K(\theta)/K) \to \mathbb{F}_5 \quad , \quad \sigma \mapsto \sigma(\theta) - \theta$$

  est un isomorphisme de groupes.

[1] La durée de l'épreuve est de quatre heures.
Tous les documents sont interdits.
L'énoncé comporte trois pages.

III. Soit le polynôme

$$P(X) = X^4 + 2X^2 - 2 \in \mathbb{Q}[X].$$

Soient les nombres complexes $\alpha = \sqrt{\sqrt{3}-1}$ et $\beta = i\sqrt{\sqrt{3}+1}$.

(1) Montrer que $P(X)$ est irréductible sur $\mathbb{Q}$, que ses quatre racines dans $\mathbb{C}$ sont $\pm\alpha$ et $\pm\beta$.

(2) Montrer

(a) que $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha, i\sqrt{2})$ (on pourra par exemple remarquer que $\alpha\beta = i\sqrt{2}$),

(b) que les extensions $\mathbb{Q}(\alpha)/\mathbb{Q}(\sqrt{3})$ et $\mathbb{Q}(\alpha,\beta)/\mathbb{Q}(\alpha)$ sont de degré 2,

(c) que l'extension $\mathbb{Q}(\alpha,\beta)/\mathbb{Q}$ est galoisienne de degré 8.

(3) montrer

(a) $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{3}),\mathbb{C})$ a deux éléments, u_1 et u_2, caractérisés par

$$u_1(\sqrt{3}) = \sqrt{3} \quad \text{et} \quad u_2(\sqrt{3}) = -\sqrt{3},$$

(b) que u_1 (resp. u_2) se prolonge en deux $\mathbb{Q}$-homomorphismes de $\mathbb{Q}(\alpha)$ dans $\mathbb{C}$, notés $u_{1,1}$ et $u_{1,2}$ (resp. $u_{2,1}$ et $u_{2,2}$) caractérisés par

$$u_{1,1}(\alpha) = \alpha \quad \text{et} \quad u_{1,2}(\alpha) = -\alpha,$$
$$u_{2,1}(\alpha) = \beta \quad \text{et} \quad u_{2,2}(\alpha) = -\beta,$$

que $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha),\mathbb{C}) = \{u_{i,j} \ / \ i,j = 1,2\}$.

(c) que chaque $u_{a,b}$, $a,b = 1,2$, se prolonge en deux $\mathbb{Q}$-automorphismes de $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha, i\sqrt{2})$, notés $u_{a,b,c}$, $c = 1,2$, déterminés par

$$u_{a,b,1}(i\sqrt{2}) = i\sqrt{2} \quad \text{et} \quad u_{a,b,2}(i\sqrt{2}) = -i\sqrt{2},$$

que $G := \mathrm{Gal}(\mathbb{Q}(\alpha,\beta)/\mathbb{Q}) = \{u_{a,b,c} \ / \ a,b,c = 1,2\}$.

(4) Montrer que $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha + i\sqrt{2})$.

(5) Soient $\sigma = u_{2,2,2}$ et $\tau = u_{1,1,2}$, ce sont des éléments de $G = \mathrm{Gal}(\mathbb{Q}(\alpha,\beta)/\mathbb{Q})$. Montrer

(a) que $\circ(\sigma) = 4$, $\circ(\tau) = 2$, $\tau\sigma = \sigma^3\tau$, que

$$G = <\sigma,\tau> = \left\{\mathrm{Id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\right\},$$

(b) que $\mathbb{Q}(\alpha,\beta)^{<\tau>} = \mathbb{Q}(\alpha)$, que $\mathbb{Q}(\alpha,\beta)^{<\sigma>} = \mathbb{Q}(i\sqrt{6})$ et que $\mathbb{Q}(\alpha,\beta)^{<\sigma\tau>} = \mathbb{Q}(\alpha - \beta)$.

IV. Les questions (4) et (7) de ce problème sont facultatives, elles ne contribuent qu'à donner un supplément de points[2].

Soient p un nombre premier, $\mathbb{F}_p$ un corps à p éléments, $K = \mathbb{F}_p(T)$ un corps de fractions rationnelles et K^{alg} une clôture algébrique de K. Soit le polynôme

$$P(X) = X^{p^2} - TX^p - T \in K[X],$$

soient $\alpha \in K^{\mathrm{alg}}$ une racine de $P(X)$ et $\beta, \gamma \in K^{\mathrm{alg}}$ tel que

$$\beta^p = T \quad , \quad \gamma^{p(p-1)} = T.$$

(1) Montrer que $\gamma^{p-1} = \beta$ et que $\beta = \alpha^p/(\alpha+1)$.

(2) Montrer que $P(X)$ est irréductible sur K.

(3) Montrer que l'ensemble des racines de $P(X)$ dans K^{alg} est

$$\{\alpha + \lambda\gamma \ / \ \lambda \in \mathbb{F}_p\}\,.$$

Quel est le cardinal de cet ensemble ?

(4) Montrer que l'extension $K(\beta)/K$ est de degré p et est purement inséparable, que l'extension $K(\gamma)/K(\beta)$ est de degré $p-1$ et est séparable.

(5) Montrer que l'extension $K(\alpha^p)/K$ est de degré p et séparable, que l'extension $K(\alpha)/K(\alpha^p)$ est de degré p et purement inséparable.

(6) Montrer que $K(\alpha,\gamma)$ est une extension normale de K de degré $p^2(p-1)$, de degré de séparabilité $p(p-1)$.

(7) Soit $G = \mathrm{Gal}(K(\alpha,\gamma)/K)$, montrer que

$$(K(\alpha,\gamma))^G = K(\beta).$$

(8) On munit $\mathbb{F}_p \times \mathbb{F}_p^\times$ de l'opération définie par

$$(\lambda,\mu)\cdot(\lambda',\mu') = (\lambda + \mu\lambda', \mu\mu'),$$

on sait, ou on admet, que pour cette loi $\mathbb{F}_p \times \mathbb{F}_p^\times$ est un groupe (c'est un produit semi-direct standard). Montrer qu'il existe une application

$$G \to \mathbb{F}_p \times \mathbb{F}_p^\times \ , \ \sigma \mapsto \big(\gamma^{-1}(\sigma(\alpha)-\alpha), \gamma^{-1}\sigma(\gamma)\big)$$

et que cette application est un isomorphisme de groupes.

[2] l'inséparabilité n'ayant pas été suffisamment traitée en travaux dirigés.