

Examen final de théorie de Galois

lundi 27 mai 2013

Durée 3 heures

Documents autorisés

Exercice 1 Soit \mathbb{F}_q un corps fini à q éléments. Soit $\mathbb{F}_q(X)$ le corps des fonctions rationnelles d'une variable à coefficients dans \mathbb{F}_q .

Soit G le groupe des automorphismes de $\mathbb{F}_q(X)$ de la forme : $f(X) \mapsto f(aX+b)$ avec $a, b \in \mathbb{F}_q$, $a \neq 0$.

- 0,5 a) Déterminer $[\mathbb{F}_q(X) : \mathbb{F}_q(X)^G]$.
- 2 b) Soit $P := (X^q - X)^{q-1} \in \mathbb{F}_q(X)$. Montrer que $[\mathbb{F}_q(X) : \mathbb{F}_q(P)] \leq q(q-1)$ et en déduire que $\mathbb{F}_q(X)^G = \mathbb{F}_q(P)$.
- 1,5 c) Soit H le sous-groupe de G formé des automorphismes :

$$f(X) \mapsto f(X+b)$$

$b \in \mathbb{F}_q$. Montrer que $\mathbb{F}_q(X)^H = \mathbb{F}_q(X^q - X)$.

Exercice 2 Soit $\alpha := \sqrt{(2 + \sqrt{2})(3 + \sqrt{3})}$. On pose $E := \mathbb{Q}(\alpha)$.

- 0,5 a) Montrer que $F := \mathbb{Q}(\sqrt{2}, \sqrt{3})$ est une extension de degré 4 de \mathbb{Q} .
- 1+1 b) On pose $a := (2 + \sqrt{2})(3 + \sqrt{3})$. Montrer que $N_{F/\mathbb{Q}(\sqrt{2})}(a)$ n'est pas un carré dans $\mathbb{Q}(\sqrt{2})$. En déduire que a n'est pas un carré dans F .
- 0,5 c) Déduire de la question précédente le degré $[E : \mathbb{Q}]$. Montrer que les racines du polynôme minimal de α sur \mathbb{Q} sont :

$$\pm \sqrt{(2 \pm \sqrt{2})(3 \pm \sqrt{3})}$$

(indication : si $\sigma : E \rightarrow \mathbb{C}$ un morphisme de corps, alors $\sigma(\alpha)^2 = \sigma((2 + \sqrt{2})(3 + \sqrt{3}))$).

- d) Soit $\beta := \sqrt{(2 - \sqrt{2})(3 + \sqrt{3})}$. Montrer que $\alpha\beta \in F$ et en déduire que $\beta \in E$.
Montrer de même que $\pm \sqrt{(2 \pm \sqrt{2})(3 \pm \sqrt{3})} \in E$ et que l'extension E/\mathbb{Q} est galoisienne.
- 1,5 e) On pose $G := \text{Aut}_{\mathbb{Q}}(E) = \text{Gal}(E/\mathbb{Q})$. Justifier l'existence d'un $\sigma \in G$ tel que $\sigma(\alpha) = \beta$. Montrer que $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = \sqrt{3}$, $\sigma(\beta) = -\alpha$.
- 2 f) Justifier l'existence d'un $\tau \in G$ tel que $\tau(\alpha) = \sqrt{(2 + \sqrt{2})(3 - \sqrt{3})}$. Montrer que dans G , on a les relations :

$$\sigma^2 = \tau^2 = (\sigma\tau)^2$$

- 0,5 g) On note Q_8 le groupe de présentation :

$$\langle a, b : a^2 = b^2 = (ab)^2 \rangle$$

(on admet que c'est un groupe d'ordre 8). Montrer que $G \simeq Q_8$.

- h) Pour chacun des quatre corps intermédiaires

$$K = \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6}), \mathbb{Q}(\sqrt{2}, \sqrt{3}),$$

(à justifier) déterminer H un sous-groupe de G tel que $K = E^H$.

Exercice 3 a) Déterminer l'unique polynôme irréductible sur \mathbb{F}_2 de degré 2. En déduire que $X^4 + X + 1$ est irréductible sur \mathbb{F}_2 . Factoriser $X^4 + X + 1$ sur \mathbb{F}_3 . Montrer que le groupe de Galois sur \mathbb{Q} du polynôme $X^4 + X + 1$ est \mathfrak{S}_4 (indication : on peut par exemple calculer le discriminant).

3,5

b) Calculer le discriminant de $X^4 + 8X + 12$. Factoriser $X^4 + 8X + 12$ sur \mathbb{F}_5 (indication : il y a une racine parmi $-1, 0, 1$). En déduire que $X^4 + 8X + 12$ est soit irréductible sur \mathbb{Q} soit avec une racine dans \mathbb{Z} . Montrer que $X^4 + 8X + 12$ est irréductible sur \mathbb{Q} et que son groupe de Galois sur \mathbb{Q} est \mathfrak{A}_4 .

4,5

(dont 1,5 pour Δ)

Exercice 4 Soient a_1, \dots, a_n des entiers sans facteur carré, deux à deux premiers entre eux. On pose $L_k := \mathbb{Q}(a_1, \dots, a_k)$ si $1 \leq k \leq n$.

0,5 a) Montrer que l'extension L_k/\mathbb{Q} est galoisienne pour tout k .
On suppose que $[L_k : \mathbb{Q}] = 2^k$ pour un certain $1 \leq k < n$.

b) Montrer que :

1

$$\sqrt{a_{i_1} \dots a_{i_r}} : 0 \leq r \leq k, 1 \leq i_1 < \dots < i_r \leq k$$

est une base de L_k comme \mathbb{Q} -espace vectoriel.

1,5 c) Montrer que si $0 \leq r, s \leq k$ et si $1 \leq i_1 < \dots < i_r \leq k, 1 \leq j_1 < \dots < j_s \leq k$, avec $\{i_1, \dots, i_r\} \not\subseteq \{j_1, \dots, j_s\}$, alors il existe $\sigma \in \text{Gal}(L_k/\mathbb{Q})$ tel que $\sigma(\sqrt{a_{i_1} \dots a_{i_r}}) = -\sqrt{a_{i_1} \dots a_{i_r}}$ et $\sigma(\sqrt{a_{j_1} \dots a_{j_s}}) = \sqrt{a_{j_1} \dots a_{j_s}}$.

d) Montrer que si $\alpha \in L_k$ et si α a au moins deux coefficients non nuls dans la base

1,5

$$\sqrt{a_{i_1} \dots a_{i_r}} : 0 \leq r \leq k, 1 \leq i_1 < \dots < i_r \leq k$$

alors il existe $\sigma \in \text{Gal}(L_k/\mathbb{Q})$ tel que $\sigma(\alpha) \neq \pm\alpha$. En déduire que $\sqrt{a_{k+1}} \notin L_k$.

0,5

e) Montrer que $[L_n : \mathbb{Q}] = 2^n$.