Examen partiel

Mardi 4 mars 2008 - Corrigé

Exercice 1

On se place dans une clôture algébrique Ω du corps $\mathbb{F}_3$ et on considère le polynôme $P = X^4 + X^2 - 1$ sur $\mathbb{F}_3$.

Soit α une racine de P dans Ω.

1. Montrer que $\mathbb{F}_3(\alpha^2) = \mathbb{F}_9$.
   Solution. *α^2 est racine de $X^2 + X - 1$. Ce polynôme de degré 2 est irréductible sur $\mathbb{F}_3$ car il n'a pas de racines dans $\mathbb{F}_3$. C'est donc le polynôme minimal de α^2 sur $\mathbb{F}_3$. D'où $[\mathbb{F}_3(\alpha^2) : \mathbb{F}_3] = 2$ et $\mathbb{F}_3(\alpha^2) = \mathbb{F}_9$.*
2. Calculer α^8.
   Solution. *$\alpha^4 = 1 - \alpha^2$. Donc $\alpha^8 = (1-\alpha^2)^2 = 1 + \alpha^4 - 2\alpha^2 = 1 + 1 - \alpha^2 - 2\alpha^2 = -1$.*
3. En déduire $[\mathbb{F}_3(\alpha) : \mathbb{F}_3]$ et l'entier q tel que $\mathbb{F}(\alpha) = \mathbb{F}_q$.
   Solution. *$\alpha^8 = -1$, donc $\alpha^9 = -\alpha \neq \alpha$ et $\alpha \notin \mathbb{F}_9 = \mathbb{F}_3(\alpha^2)$. De plus $[\mathbb{F}_3(\alpha) : \mathbb{F}_3(\alpha^2)] \leq 2$. Donc $[\mathbb{F}_3(\alpha) : \mathbb{F}_3(\alpha^2)] = 2$, $[\mathbb{F}_3(\alpha) : \mathbb{F}_3] = 4$ et $\mathbb{F}_3(\alpha) = \mathbb{F}_{81}$.*
4. Déterminer l'ensemble des conjugués de α sur $\mathbb{F}_3$.
   Solution. *On obtient les conjugués en appliquant le frobénius, ce qui donne : α, α^3, $\alpha^9 = -\alpha$ et $-\alpha^3$.*

   Soit β une racine carrée de α danx Ω.
5. Montrer que $\beta \notin \mathbb{F}_3(\alpha)$.
   Solution. *$\beta^{80} = \alpha^{40} = (-1)^5 = -1$. Donc $\beta \notin \mathbb{F}_3(\alpha) = \mathbb{F}_{81}$.*
6. En déduire que $X^8 + X^4 - 1$ est irréductible sur $\mathbb{F}_3$.
   Solution. *$[\mathbb{F}_3(\beta) : \mathbb{F}_3(\alpha)] = 2$. Donc $[\mathbb{F}_3(\beta) : \mathbb{F}_3] = 8$. De plus β est racine de $X^8 + X^4 - 1$ car α est racine de $X^4 + X^2 - 1$. Donc $X^8 + X^4 - 1$ est les polynôme minimal de β sur $\mathbb{F}_3$ et est donc irréductible*

Exercice 2

1. (a) Déterminer $[\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}]$.
   Solution. *$X^4 - 5$ est d'Einsenstein en 5 donc irréductible sur $\mathbb{Q}$ et $[\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] = 4$.*

   (b) Quels sont les conjugués de $\sqrt[4]{5}$ sur $\mathbb{Q}$?
   Solution. *Les conjugués de $\sqrt[4]{5}$ sont les racines de $X^4 - 5$: $\pm\sqrt[4]{5}$, $\pm i\sqrt[4]{5}$.*

   (c) L'extension $\mathbb{Q}(\sqrt[4]{5})$ est-elle normale sur $\mathbb{Q}$?
   Solution. *Non car $i\sqrt[4]{5} \notin \mathbb{Q}(\sqrt[4]{5})$.*

   (d) Déterminer le groupe des automorphismes de $\mathbb{Q}(\sqrt[4]{5})$.
   Solution. *Un automorphisme de $\mathbb{Q}(\sqrt[4]{5})$ est déterminé par l'image de $\sqrt[4]{5}$ dans $\mathbb{Q}(\sqrt[4]{5})$. Il n'y a donc que l'identité et l'automorphisme qui envoie $\sqrt[4]{5}$ sur $-\sqrt[4]{5}$. Ce groupe est isomorphe au groupe $\mathbb{Z}/2\mathbb{Z}$.*

   Soit $K = \mathbb{Q}(i, \sqrt[4]{5})$.
2. (a) Expliquer pourquoi K est une extension galoisienne de degré 8.
   Solution. *K est le corps des racines de $X^4 - 5$ sur $\mathbb{Q}$. C'est donc une extension normale donc galoisienne car la caractéristique est nulle. On a $[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{5})(i) : \mathbb{Q}(\sqrt[4]{5})][\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] = 2 \times 4 = 8$.*

   (b) En déduire l'irréductibilité de $X^4 - 5$ sur $\mathbb{Q}(i)$.
   Solution. *Par $[K : \mathbb{Q}] = [\mathbb{Q}(i)(\sqrt[4]{5}) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}]$, on déduit que $[\mathbb{Q}(i)(\sqrt[4]{5}) : \mathbb{Q}(i)] = 4$ et $X^4 - 5$ est irréductible sur $\mathbb{Q}(i)$.*

3. (a) Montrer qu'il existe un unique élément σ du groupe $\mathrm{Gal}(K/\mathbb{Q})$ tel que :

$$\sigma(i) = i \text{ et } \sigma(\sqrt[4]{5}) = i\sqrt[4]{5}.$$

Solution. *K est une extension galoisienne de $\mathbb{Q}(i)$ et par la question précédente $\sqrt[4]{5})$ et $i\sqrt[4]{5})$ sont conjugués au-dessus de $\mathbb{Q}(i)$. Il existe donc un automorphisme de K qui fixe i et envoie $\sqrt[4]{5})$ sur $i\sqrt[4]{5})$. Cet automorphisme est unique, car tout automorphisme de K est déterminé par l'image de i et de $\sqrt[4]{5})$.*

(b) Quel est l'ordre de σ ?
Solution. $\sigma^2(\sqrt[4]{5})) = \sigma(i\sqrt[4]{5}) = i \times isqrt[4]5) = -sqrt[4]5$, $\sigma^3(\sqrt[4]{5})) = -i\sqrt[4]{5}$ *et* $\sigma^4(\sqrt[4]{5})) = \sqrt[4]{5}$. *De plus $\sigma^4(i) = i$, donc σ^4 est égal à l'identité et σ est d'ordre 4.*

(c) Montrer qu'il existe un unique élément τ du groupe $\mathrm{Gal}(K/\mathbb{Q})$ tel que :

$$\tau(i) = -i \text{ et } \tau(\sqrt[4]{5}) = \sqrt[4]{5}.$$

Solution. *i et $-i$ sont conjugués au-dessus de $\mathbb{Q}(\sqrt[4]{5})$, d'où le résultat.*

(d) Montrer que les automorphismes σ et τ engendrent $\mathrm{Gal}(K/\mathbb{Q})$.
Solution. *σ engendre un sous-groupe d'ordre 4 qui fixe i. L'automorphisme τ n'est donc pas dans ce sous-groupe. Donc σ et τ engendrent au moins un sous-groupe d'ordre 8. On conclut car $\mathrm{Gal}(K/\mathbb{Q})$ est d'ordre 8, le degré de l'extension galoisienne K sur $\mathbb{Q}$.*

4. (a) Quels sont les conjugués de $\sqrt[4]{5} + i$?
Solution. *En appliquant σ, on obtient que $\sqrt[4]{5}+i$, $i\sqrt[4]{5}+i$, $-\sqrt[4]{5}+i$ et $-i\sqrt[4]{5}+i$ sont conjugués de $\sqrt[4]{5}+i$. Ensuite, en appliquant τ on obtient quatre autres conjugués : $\sqrt[4]{5}-i$, $-i\sqrt[4]{5}-i$, $-\sqrt[4]{5}-i$ et $i\sqrt[4]{5}-i$. Ce sont tous les conjugués car il y en a au plus 8 dans une extension galoisienne de degré 8.*

(b) En déduire que $\sqrt[4]{5} + i$ est un élément primitif de l'extension K sur $\mathbb{Q}$.
Solution. *$\sqrt[4]{5}+i$ a huit conjugués donc $[\mathbb{Q}(\sqrt[4]{5}+i) : \mathbb{Q}] = 8$ et $K = \mathbb{Q}(\sqrt[4]{5}+i)$.*

5. (a) Vérifier que $\tau \circ \sigma = \sigma^{-1} \circ \tau$.
Solution. *$\tau\circ\sigma(\sqrt[4]{5}+i) = \tau(i\sqrt[4]{5}+i) = -i\sqrt[4]{5}-i$ et $\sigma^{-1}\circ\tau(\sqrt[4]{5}+i) = \sigma^{-1}(\sqrt[4]{5}-i) = -i\sqrt[4]{5}-i$. Donc $\tau \circ \sigma = \sigma^{-1} \circ \tau$.*

(b) Quel est l'ordre du sous-groupe H de $\mathrm{Gal}(K/\mathbb{Q})$ engendré par τ et σ^2 ?
Solution. *comme $\tau^2 = id$, $\sigma^4 = id$ et $\tau \circ \sigma^2 = \sigma^2 \circ \tau$, on déduit que $H = \{id, \tau, \sigma^2, \tau \circ \sigma^2\}$ et donc que ce sous-groupe est d'ordre 4.*

(c) En déduire que $K^H = \mathbb{Q}(\sqrt{5})$.
Solution. *On vérifie facilement que $\sqrt{5} \in K^H$, d'où $\mathbb{Q}(\sqrt{5}) \subset K^H$. De plus $[K : K^H] = |H| = 4$ et donc $[K^H : \mathbb{Q}] = 2$. Il suit que $K^H = \mathbb{Q}(\sqrt{5})$.*