Contrôle continu n° 2

Exercice 1

On considère le polynôme $P(X) = X^4 - 2X^2 + 9 \in \mathbb{Q}[X]$.

1. Vérifier que $P(X) = (X - \sqrt{2} - i)(X - \sqrt{2} + i)(X + \sqrt{2} - i)(X + \sqrt{2} + i)$ dans $\mathbb{C}[X]$.
2. Montrer que P est irréductible dans $\mathbb{Q}[X]$. Quelle est sa décomposition en facteurs irréductibles dans $\mathbb{Q}(i)[X]$?
3. On note $K = \mathbb{Q}(i + \sqrt{2})$. Montrer que $K = \mathbb{Q}(i, \sqrt{2})$ et que c'est le corps de décomposition de P dans $\mathbb{C}$.
4. On note G le groupe des automorphismes de K.
   (a) Quel est le cardinal de G ?
   (b) Montrer qu'il existe $\varphi \in G \setminus \{\mathrm{id}_K\}$ laissant invariant chaque élément de $\mathbb{Q}(i)$. Quel est l'ordre de φ ?
   (c) Montrer qu'il existe $\psi \in G \setminus \{\mathrm{id}_K\}$ laissant invariant chaque élément de $\mathbb{Q}(\sqrt{2})$. Quel est l'ordre de ψ ?
   (d) Montrer que $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Correction :

1. *Regrouper une racine et son opposé simplifie le calcul.*
2. *Il n'y a pas de racine rationnelle. Si P avait une décomposition en produit de deux facteurs irréductible de degré 2 sur $\mathbb{Q}[X]$, alors ce serait également une factorisation sur $\mathbb{R}[X]$. En regroupant une racine et son conjugué on obtient la décomposition en facteurs irréductibles de P sur $\mathbb{R}[X]$: $P(X) = (X^2 - 2\sqrt{2}X + 3)(X^2 + 2\sqrt{2}X + 3)$, dont aucun des facteurs n'est dans $\mathbb{Q}[X]$.*

   Le polynôme P n'a pas non plus de racines dans $\mathbb{Q}(i)$. En regroupant différemment les racines, on obtient la décomposition $P(X) = ((X-i)^2 - 2)((X+i)^2 - 2) = (X^2 - 2iX - 3)(X^2 + 2iX - 3)$ dont les facteurs sont bien irréductibles.
3. *On a clairement $K \subset \mathbb{Q}(i, \sqrt{2})$. D'après la question précédente, $[K : \mathbb{Q}] = \deg P = 4$ et comme $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \leq 4$, on a l'égalité. De plus toutes les racines de P sont clairement dans $\mathbb{Q}(i, \sqrt{2})$, donc ce corps de rupture est aussi le corps de décomposition.*
4. *(a) Tout automorphisme de K laisse invariant le sous-corps premier $\mathbb{Q}$. Comme K est monogène, un automorphisme de K est entièrement spécifié par l'image de $i + \sqrt{2}$ qui doit être une autre racine de son polynôme minimal P. Étant donné que P a quatre racines distinctes dans K, il y a donc quatre automorphimes distincts de K et $\#G = 4$.*

   (b) On écrit $K = \mathbb{Q}(i)(\sqrt{2})$. Un automorphisme de K fixant $\mathbb{Q}(i)$ est donc entièrement déterminé par l'image de $\sqrt{2}$, qui doit être une autre racine de son polynôme minimal sur $\mathbb{Q}(i)$ qui est $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$. Il existe donc $\phi \in G \setminus \{id_K\}$, qui laisse invariant $\mathbb{Q}(i)$ et envoie $\sqrt{2}$ sur $-\sqrt{2}$.

   On a alors $\varphi^2(\sqrt{2}) = \varphi(-\sqrt{2}) = \sqrt{2}$ et $\varphi^2(i) = i$, donc φ est d'ordre 2.

   (c) Idem en écrivant $K = \mathbb{Q}(\sqrt{2})(i)$.

   (d) G contient id_K, φ, ψ et $\varphi \circ \psi$ qui sont bien distincts (il suffit de regarder leurs actions sur $\pm i, \pm\sqrt{2}$). On a alors un isomorphisme explicite $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to G$, $(1,0) \mapsto \varphi$, $(0,1) \mapsto \psi$.

Exercice 2

1. Soit $\zeta \in \mathbb{C}$ une racine primitive 5-ème de l'unité.
   (a) Montrer que ζ est algébrique sur $\mathbb{Q}$ et donner son polynôme minimal P.
   En déduire $[\mathbb{Q}(\zeta) : \mathbb{Q}]$.
   (b) Quel est le corps de décomposition de P sur $\mathbb{Q}$?
2. On pose $\alpha = 2\cos\frac{2\pi}{5}$ et $\zeta = e^{\frac{2i\pi}{5}}$.
   (a) Vérifier que $\mathbb{Q}(\alpha) \subsetneq \mathbb{Q}(\zeta)$.
   (b) Montrer que ζ est une racine de $X^2 - \alpha X + 1$. Déterminer $[\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)]$ et $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.
   (c) Calculer $\mathrm{irr}(\alpha, \mathbb{Q})$, en déduire $\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$.
   (d) Calculer $\mathrm{irr}(\zeta, \mathbb{Q}(\sqrt{5}))$.
3. Prouver que $\mathrm{irr}(\zeta, \mathbb{Q}(i)) = P$.

Correction :

1. *(a) L'élément ζ est bien racine de $\Phi_5 = X^4 + X^3 + X^2 + X + 1$ donc est algébrique, et comme Φ_5 est irréductible dans $\mathbb{Q}[X]$ (cf cours), c'est son polynôme minimal P. Le degré est donc $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \Phi_5 = \varphi(5) = 4$.*
   (b) Les racines de P dans $\mathbb{C}$ sont $\zeta, \zeta^2, \zeta^3, \zeta^4$ qui sont toutes dans $\mathbb{Q}(\zeta)$. C'est donc à la fois le corps de rupture et de décomposition de P.
2. *(a) On a $\alpha = \zeta + \bar{\zeta} = \zeta + \zeta^{-1} \in \mathbb{Q}(\zeta)$ donc $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta)$. Par ailleurs, $\alpha \in \mathbb{R}$ donc $\mathbb{Q}(\alpha) \subset \mathbb{R}$, or $\mathbb{Q}(\zeta) \not\subset \mathbb{R}$, donc $\mathbb{Q}(\alpha) \subsetneq \mathbb{Q}(\zeta)$.*
   (b) On a $(X - \zeta)(X - \zeta^{-1}) = X^2 - \alpha X + 1$. Ce polynôme est irréductible dans $\mathbb{Q}(\alpha)$ puisque $\zeta \notin \mathbb{Q}(\alpha)$, c'est donc le polynôme minimal de ζ sur $\mathbb{Q}(\alpha)$ et $[\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)] = 2$. Par multiplicativité des degrés, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.
   (c) $\alpha = \zeta + \zeta^{-1} = \zeta + \zeta^4$, $\alpha^2 = \zeta^2 + \zeta - 2 + 2 = \zeta + \zeta^3 + 2$ donc $\alpha^2 + \alpha - 1 = \sum_{i=0}^{4} \zeta^i = 0$. Le polynôme unitaire $X^2 + X - 1 \in \mathbb{Q}[X]$ est annulateur de α et de degré 2, c'est donc son polynôme minimal sur $\mathbb{Q}$.

   Les racines dans $\mathbb{R}$ de $X^2 + X - 1$ sont $\frac{\pm\sqrt{5}-1}{4}$; comme $2\pi/5 \in [0; \pi/2]$, $\alpha \leq 0$, d'où l'égalité souhaitée.
   (d) On a clairement $\mathbb{Q}(\alpha) = \mathbb{Q}\left(\frac{\sqrt{5}-1}{4}\right) = \mathbb{Q}(\sqrt{5})$ donc c'est le même polynôme minimal que plus haut, soit $X^2 - \alpha X + 1$.
3. *Le polynôme P n'a pas de racine dans $\mathbb{Q}(i)$ (sinon $\mathbb{Q}(i)$ serait un corps de rupture de P sur $\mathbb{Q}$, or $[\mathbb{Q}(i) : \mathbb{Q}] = 2 \neq \deg P$).*
   Par l'absurde, si $P = \prod_{k=1}^{4}(X - \zeta^k)$ est un produit de deux facteurs dans $\mathbb{Q}(i)$, un des facteurs a pour racines ζ et ζ^k avec $k = 2, 3$ ou 4. Si $k = 2$ ou 3, alors le terme constant de $(X - \zeta)(X - \zeta^k)$ doit appartenir à $\mathbb{Q}(i)$ d'où $\zeta^{k+1} \in \mathbb{Q}(i)$, contradiction. Si $k = 4$, alors $(X - \zeta)(X - \zeta^4) = X^2 - \alpha X + 1 \notin \mathbb{Q}(i)$, contradiction.

Exercice 3

1. Décrire l'ensemble des sous-corps de $\mathbb{F}_{p^n}$ où p est un entier premier et $n \in \mathbb{N}^*$.

2. Soit $K \supset k$ une extension de corps finis. Montrer qu'il existe $\alpha \in K$ tel que $K = k(\alpha)$.
3. Soit $k = \mathbb{F}_q$ un corps fini et $P \in k[X]$ un polynôme irréductible de degré d. Montrer que le corps de rupture et le corps de décomposition de P coïncident.
4. Soit $n \in \mathbb{N}^*$. Pour $\alpha \in \mathbb{F}_{2^n}$, on pose

$$\mathrm{Tr}(\alpha) = \sum_{k=0}^{n-1} \alpha^{2^k} \quad \text{et} \quad p(\alpha) = \alpha^2 + \alpha.$$

   (a) Montrer que Tr et p sont deux applications $\mathbb{F}_2$-linéaires de $\mathbb{F}_{2^n}$ dans lui-même et déterminer $\ker p$.

   (b) Montrer que Tr est une application polynomiale et en déduire que ce n'est pas l'application nulle.

   (c) Montrer que $\mathrm{Im}\,\mathrm{Tr} = \ker p$, puis que $\ker \mathrm{Tr} = \mathrm{Im}\, p$.

   (d) Soit $a \in \mathbb{F}_{2^n}$. Montrer que le polynôme $X^2 + X + a \in \mathbb{F}_{2^n}[X]$ a des racines dans $\mathbb{F}_{2^n}$ si et seulement si $\mathrm{Tr}(a) = 0$.

   (e) On suppose $n = 2m + 1$. Montrer que si $\mathrm{Tr}(a) = 0$, alors $x = \sum_{k=0}^{m-1} a^{2^{2k+1}}$ est une racine de $X^2 + X + a$.

<u>*Correction*</u> *:*

1. *Cours.*
2. *Cf TD.*
3. *Cours.*
4. *(a) La linéarité provient du Frobenius et on a clairement* $\ker(p) = \{0; 1\} = \mathbb{F}_2$.

   (b) Il est clair que Tr est polynomiale de degré 2^{n-1} *donc possède au plus* 2^{n-1} *dans le corps* $\mathbb{F}_{2^n}$ *à* 2^n *éléments. Ce n'est donc pas l'application polynomiale nulle.*

   (c) Pour tout $\alpha \in \mathbb{F}_{2^n}$*,*

$$p(Tr(\alpha)) = \left(\sum_{k=0}^{n-1} \alpha^{2^k}\right)^2 + \sum_{k=0}^{n-1} \alpha^{2^k} = \sum_{k=0}^{n-1} (\alpha^{2^k})^2 + \sum_{k=0}^{n-1} \alpha^{2^k} = \sum_{k=0}^{n-1} \alpha^{2^{k+1}} + \sum_{k=0}^{n-1} \alpha^{2^k} = \alpha^{2^n} + \alpha = 0,$$

   donc $\mathrm{Im}\ Tr \subset \ker p = \{0; 1\}$*. Si l'inclusion était stricte, on aurait* $\mathrm{Im}\ Tr = \{0\}$ *donc* $Tr = 0$*, ce qui n'est pas.*

   Pour la deuxième assertion, le théorème du rang donne l'égalité des dimensions. Par ailleurs, pour tout $\alpha \in \mathbb{F}_{2^n}$*,*

$$Tr(p(\alpha)) = Tr(\alpha^2 + \alpha) = Tr(\alpha^2) + Tr(\alpha).$$

   Or

$$Tr(\alpha^2) = \sum_{k=0}^{n-1} (\alpha^2)^{2^k} = \sum_{k=0}^{n-1} \alpha^{2^{k+1}} = \sum_{k=1}^{n} \alpha^{2^k} = \sum_{k=0}^{n-1} \alpha^{2^k},$$

   car $\alpha^{2^n} = \alpha^0$*. Donc* $Tr(\alpha^2) = Tr(\alpha)$ *d'où* $Tr(p(\alpha)) = 0$*. On en déduit que* $\mathrm{Im}\, p \subset \ker Tr$*.*

   (d) $X^2 + X + a$ *a des racines dans* $\mathbb{F}_{2^n} \Leftrightarrow a \in \mathrm{Im}(p) \Leftrightarrow a \in \ker Tr$*.*

   (e) On suppose $Tr(a) = 0$*. Alors*

$$x^2 + x = (\sum_{k=0}^{m-1} a^{2^{2k+1}})^2 + \sum_{k=0}^{m-1} a^{2^{2k+1}} = \sum_{k=0}^{m-1} a^{2^{2k+2}} + \sum_{k=0}^{m-1} a^{2^{2k+1}} = \sum_{l=1}^{2m} a^{2^l} = a + Tr(a) = a.$$