

Corrigé du contrôle classant 2017

Ce corrigé constitue un ensemble d'indications pour résoudre les exercices.

Il ne s'agit en aucun cas d'un modèle de rédaction pour le contrôle classant.

Exercice 1.

1) L'extension est clairement algébrique galoisienne de degré au plus 4. Mais $\sqrt{2} + \sqrt{3}$ admet pour polynôme annulateur $x^4 - 10x^2 + 1$ irréductible sur \mathbf{Q} . C'est donc un générateur de l'extension qui est de degré 4.

2) L'action sur $\{\sqrt{2}, -\sqrt{2}\} \cup \{\sqrt{3}, -\sqrt{3}\}$ fait du groupe de Galois un sous-groupe de $S_2 \times S_2$, il est donc isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$.

3) $x^2 = (2 + \sqrt{2})(3 + \sqrt{3}) \in M$ de degré 4 sur \mathbf{Q} . Ainsi $M = \mathbf{Q}[x^2]$.

4) L'extension est clairement algébrique car $\sqrt{2}$, $\sqrt{3}$, $\sqrt{\sqrt{2}+2}$ et $\sqrt{\sqrt{3}+3}$ sont algébriques sur \mathbf{Q} . De plus

$$\text{Conj}_{\mathbf{Q}, \overline{\mathbf{Q}}}(\sqrt{\sqrt{2}+2}) = \{\sqrt{\sqrt{2}+2}, -\sqrt{\sqrt{2}+2}, \sqrt{-\sqrt{2}+2}, -\sqrt{-\sqrt{2}+2}\},$$

avec une expression analogue quand $\sqrt{2}$ est remplacé par $\sqrt{3}$. Ainsi un conjugué de x est un des 16 produits d'un conjugué de $\sqrt{\sqrt{2}+2}$ et d'un conjugué de $\sqrt{\sqrt{3}+3}$. Parmi ces produits, au plus 8 sont différents.

5) Les conjugués x et $-x$ sont dans $\mathbf{Q}[x]$. Comme

$$x^{-1} = \sqrt{(2 - \sqrt{2})(3 - \sqrt{3})(2\sqrt{3})}^{-1},$$

on obtient le conjugué $2\sqrt{3}x^{-1}$ et $-2\sqrt{3}x^{-1}$. Puis $\sqrt{(2 - \sqrt{2})(3 + \sqrt{3})}x = (3 + \sqrt{3})\sqrt{2} \in M$ et donc $\pm\sqrt{(2 - \sqrt{2})(3 + \sqrt{3})} \subset M[x] \subset \mathbf{Q}[x]$. C'est analogue pour $\pm\sqrt{(2 + \sqrt{2})(3 - \sqrt{3})}$

6) Le degré est 4 ou 8. Si c'était 4, on aurait $E = M$ et $(2 + \sqrt{2})(3 + \sqrt{3})$ aurait une racine carrée dans M , ce qui n'est pas le cas. Le degré est donc 8.

- 7) $G' = \text{Gal}(E/M)$.
 8) Soit $g \in G'$ non trivial dans ce groupe et $g' \in G'$. Alors $(g')^{-1}gg' \neq e$ donc c'est g .
 9) Le quotient G/G' est isomorphe à $\text{Gal}(M/\mathbf{Q})$ commutatif.
 10) Non : on caractérise les éléments de G par leur action sur x ce qui permet de le vérifier.

Exercice 2.

- 1) σ est l'application qui envoie $f(X)$ sur $f(1-X)$. Elle est bien définie et c'est un morphisme de k -algèbre d'inverse elle-même. C'est donc un automorphisme de l'extension. C'est analogue pour τ .
 2) On a $(\sigma \circ \tau)(f(X)) = f(1 - X^{-1})$. Puis $(\sigma \circ \tau)^2(f(X)) = f(1 - \frac{1}{1-X^{-1}}) = f(\frac{X^{-1}}{X^{-1}-1})$ et $(\sigma \circ \tau)^3(f(X)) = f(X)$. Ainsi $(\sigma \circ \tau)^3 = \text{Id}$. Par ailleurs on voit que $(\sigma \circ \tau)(X) \neq X$, donc l'ordre est 3.
 3) On a vu dans 1) que σ et τ sont d'ordre 2. Le théorème de Lagrange implique que l'ordre de G est divisible par 2 et par 3, et donc par 6.
 4) Les éléments suivant forment un groupe : $\text{Id}, \sigma, \tau, \sigma\tau, \tau\sigma, \sigma\tau\sigma, \tau\sigma\tau$. En effet, le produit par un élément σ ou τ à droite ou à gauche redonne un élément de la liste. Par exemple

$$\tau(\sigma\tau\sigma) = (\tau\sigma)^{-1} = \sigma\tau.$$

D'après 3) ils sont distincts, c'est donc la liste des éléments de G .

- 5) L'application $S_3 \rightarrow G$ telle que $(12) \mapsto \sigma$ et $(13) \mapsto \tau$ définit un isomorphisme.
 6) On applique le Lemme d'Artin, on obtient une extension galoisienne de groupe de Galois G et donc de degré 6.
 7) On calcule $\tau(Y) = \frac{X^3-3X^2+1}{X(1-X)} = \sigma(Y)$.
 8) On a bien $\sigma(Z) = \sigma(Y)Y = Z$ et $\tau(Z) = \tau(Y)(\tau \circ \sigma(Y)) = Z$. Donc $Z \in K$.
 9) On a $ZX^2(X-1)(1-X) = (X^3-3X+1)(X^3-3X^2+1)$ ce qui donne une équation polynômiale de degré 6 en X à coefficients dans $k(Z)$.
 10) On a $[L : k(Z)] \geq 6$ et $[L : K] = 6$, donc $K = k(Z)$.
 11) Par la correspondance de Galois, c'est le nombre de sous-groupes de S_3 , c'est-à-dire 6.
 12) On a $(\tau \circ \sigma)(Y) = Y$ et donc $k(Y) \subset L^{\tau \circ \sigma}$. Notons que $[L : L^{\tau \circ \sigma}] = 3$. Mais X étant de degré au plus 3 sur $k(Y)$ d'après la formule définissant Y , on obtient $k(Y) = L^{\tau \circ \sigma}$.

Exercice 3.

- 1) $(F^*)^2$ est un sous-groupe distingué de F^* commutatif, le groupe quotient est l'ensemble des classes à gauche.
- 2) σ dans le groupe de Galois induit $\sigma : F^* \rightarrow F^*$ automorphisme de groupe tel que $\sigma((F^*)^2) = (F^*)^2$.
- 3) Soit $P(X)$ le polynôme minimal de α sur \mathbf{Q} . Alors $P(X^2)$ annule les $\sqrt{\alpha_i}$ qui sont donc algébriques de conjugués de la forme $\pm\sqrt{\alpha_j} \in K$. Par ailleurs les conjugués des éléments de F sont dans K .
- 4) Les conjugués de $\sqrt{\alpha_i}$ sur F sont $\pm\sqrt{\alpha_i}$. L'action de $\text{Gal}(K/F)$ sur $\{\pm\sqrt{\alpha_i}\}_{1 \leq i \leq n}$ donne donc un morphisme de groupe injectif vers $S_2^n \simeq (\mathbf{Z}/2\mathbf{Z})^n$ qui est par ailleurs commutatif.
- 5) Par hypothèse, on a un conjugué de α , disons $\beta = \alpha_2$, tel que $\beta \notin \alpha(F^*)^2$. Alors $\sqrt{\beta}$ est un conjugué de $\sqrt{\alpha}$, $\alpha \notin (F^*)^2$ (sinon $\beta \in (F^*)^2$ également) et $\sqrt{\beta} \notin \sqrt{\alpha}F^*$. Soit $L = F[\sqrt{\alpha}]$. Si $\sqrt{\beta} \in L$, alors $\sqrt{\beta} = \lambda + \mu\sqrt{\alpha}$ avec $\lambda, \mu \in F$, donc $2\lambda\mu\sqrt{\alpha} \in F$, donc $\mu = 0$, contradiction car $\sqrt{\beta} \notin F$ car $\sqrt{\alpha}$ ne l'est pas. Donc L/\mathbf{Q} n'est pas galoisienne. Donc $\text{Gal}(K/\mathbf{Q})$ n'est pas commutatif.

Exercice 4

- 1) Par nécessairement, par exemple $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ est \mathbf{C} -diagonalisable mais pas \mathbf{R} -diagonalisable. La réciproque est vraie, le polynôme annulateur sur k convient.
- 2) Non, par exemple on peut trouver deux matrices symétriques réelles qui ne commutent pas.
- 3) Un sens est clair car $X^q - X$ est scindé à racines simples dans \mathbf{F}_q . Réciproquement, les coefficients d'une matrices diagonales sont annulées par un $X^q - X$.
- 4) On a $(u+v)^2 = u+v$, $u^2 = u$, $v^2 = v$ et donc $uv + vu = 0$ ce qui implique la commutativité en caractéristique 2.