Algèbre – Examen

Correction

Exercice 1. Nous avons

$$X^{12} - 1 = \Phi_{1,\mathbb{Q}} \times \Phi_{2,\mathbb{Q}} \times \Phi_{3,\mathbb{Q}} \times \Phi_{4,\mathbb{Q}} \times \Phi_{6,\mathbb{Q}} \times \Phi_{12,\mathbb{Q}}.$$

De $X^6 - 1 = \Phi_{1,\mathbb{Q}} \times \Phi_{2,\mathbb{Q}} \times \Phi_{3,\mathbb{Q}} \times \Phi_{6,\mathbb{Q}}$, nous obtenons $X^{12} - 1 = (X^6 - 1) \times \Phi_{4,\mathbb{Q}} \times \Phi_{6,\mathbb{Q}}$. Il en suit $X^6 + 1 = \Phi_{4,\mathbb{Q}} \times \Phi_{6,\mathbb{Q}}$. De

$$X^4 - 1 = \Phi_{1,\mathbb{Q}} \times \Phi_{2,\mathbb{Q}} \times \Phi_{4,\mathbb{Q}} = (X^1 - 1) \times \Phi_{4,\mathbb{Q}},$$

nous obtenons $\Phi_{4,\mathbb{Q}} = X^2 + 1$. Finalement nous avons

$$\Phi_{12,\mathbb{Q}} = \frac{X^6 + 1}{X^2 + 1} = X^4 - X^2 + 1$$

Exercice 2.

a. Nous avons $L = K(a, b) = K(a)(b)$. Notons P et Q les polynômes irréductibles de b sur K et $K(a)$ respectivement. Par hypoyhèses nous avons $\deg(P) = [K(a) : K] = n$. De $P \in K[X] \subseteq K(a)[X]$ et $P(b) = 0$, nous obtenons que P est un polynôme annulateur de b dans $K(a)[x]$ et donc Q divise P. Ainsi nous avons

$$[L : K(a)] = [K(a)(b) : K(b)] = \deg(Q) \leq \deg(P) = [K(b) : K] = n.$$

b. Nous avons $[L : K] = [L : K(a)] \times [K(a) : K] \leq n \times m$ par le **a**. Par ailleurs les relations $[L : K] = [L : K(a)] \times [K(a) : K]$ et $[L : K] = [L : K(b)] \times [K(b) : K]$ impliquent que m et n sont des diviseurs de $[L : K]$. L'entier $[L : K]$ étant un mutliple de m et n, c'est un multiple de $\text{ppcm}(m, n) = m \times n$. Nous obtenons ainsi $m \times n \leq [L : K] \leq n \times m$, ce qui implique $[L : K] = m \times n$.

Exercice 3.

a. L'élément $b = a^2$ appartient à $K(a)$. Comme a est algébrique sur K, l'extension $K(a)/K$ est finie et donc algébrique. Ainsi tout élément de $K(a)$ est algébrique sur K, c'est donc en particulier le cas pour b. Par ailleurs le polynôme $P = X^2 - b$ appartient à $K(b)[X]$ et admet a comme racine. Le polynôme $\text{Irr}(a, K(b))$ est donc de degré au plus 2, ce qui implique $[K(a) : K(b)] \leq 2$.

b. Nous avons $[K(a) : K] = [K(a) : K(b)] \times [K(b) : K]$. Comme $[K(a) : K]$ est impair nous avons nécessairement $[K(a) : K(b)] \neq 2$. Du **a** nous obtenons $[K(a) : K(b)] = 1$ et donc l'égalité $K(a) = K(b)$.

Exercice 4. Soient $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ et $\alpha = \sqrt{2} + \sqrt{3}$.

a. Le polynôme $X^2 - 2$ de $\mathbb{Q}[X]$ annule $\sqrt{2}$ et est irréductible par Eisenstein (avec $p = 2$). Le degré $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ est donc 2. De même $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 3$ avec $\mathrm{Irr}(\sqrt{3}, \mathbb{Q}) = X^2 - 3$. La famille $(1, \sqrt{2})$ est donc une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Supposons par l'abusrde que $\sqrt{3}$ appartienne à $\mathbb{Q}(\sqrt{2})$. Alors il existerait a et b dans $\mathbb{Q}$ tels que $\sqrt{3} = a + b\sqrt{2}$. Nous aurions donc $3 = a + 2b^2 + 2ab\sqrt{2}$. Comme 3 est dans $\mathbb{Q}$ et que $(1, \sqrt{2})$ est une $\mathbb{Q}$-base le coefficient $2ab$ est nul et donc a ou b est nul.
Pour $a = 0$, on obtient $3 = 2b^2$. En posant $b = \frac{p}{q}$ avec $p, q \in \mathbb{Z}$ et $\mathrm{pgcd}(p, q) = 1$, nous obtenons $3q^2 = 2p^2$. Le lemme de Gauß implique alors que p puis p^2 divise 3 et donc $p = 1$. De même nous devons avoir $q = 1$. et donc $3 = 2$, ce qui est impossible. Pour $b = 0$, on obtient $\sqrt{3} = a \in \mathbb{Q}$, ce qui est impossible. Nous avons ainsi établi $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.
Nous avons

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \times [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

Comme $X^2 - 3 \in \mathbb{Q}[X] \subseteq \mathbb{Q}(\sqrt{2})[X]$ est un polynôme annulateur de $\sqrt{3}$ dans $\mathbb{Q}(\sqrt{2})[X]$ nous avons

$$[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \leq \deg(X^2 - 3) = 2.$$

Le corps $\mathbb{Q}(\sqrt{2})$ ne contenant pas $\sqrt{3}$ nous avons $\mathbb{Q}(\sqrt{2})(\sqrt{3}) \neq \mathbb{Q}(\sqrt{2})$. Il en suit $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \neq 1$ puis $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ et donc $[K : \mathbb{Q}] = 2 \times 2 = 4$.

b. Nous avons

$$\begin{aligned}
\alpha^3 - 9\alpha &= (\sqrt{2} + \sqrt{3})^3 - 9\sqrt{2} - 9\sqrt{3} \\
&= (\sqrt{2})^3 + 3(\sqrt{2})^2\sqrt{3} + 3\sqrt{2}(\sqrt{3})^2 + (\sqrt{3})^3 - 9\sqrt{2} - 9\sqrt{3} \\
&= 2\sqrt{2} + 6\sqrt{3} + 9\sqrt{2} + 3\sqrt{3} - 9\sqrt{2} - 9\sqrt{3} \\
&= 2\sqrt{2}.
\end{aligned}$$

et donc $\sqrt{2} = \frac{1}{2}(\alpha^3 - 9\alpha)$ appartient à $\mathbb{Q}(\alpha)$. Il en suit que $\sqrt{3} = \alpha - \sqrt{2}$ est aussi un élément de $\mathbb{Q}(\alpha)$ et donc $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\alpha)$. Comme α appartient à K nous avons $\mathbb{Q}(\alpha) \subseteq K$ puis $K = \mathbb{Q}(\alpha)$.

c. Le degré de $\mathbb{Q}(\alpha)/\mathbb{Q}$ est $[K : \mathbb{Q}] = 4$. Ainsi le polynôme irréductible de α sur $\mathbb{Q}$ est de degré 4. Nous avons $\alpha^2 = (\sqrt{2} + \sqrt{3})^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6}$ et donc

$$\alpha^4 = (5 + 2\sqrt{6})^2 = 25 + 20\sqrt{6} + 24 = 49 + 20\sqrt{6},$$

puis $\alpha^4 - 10\alpha^2 = 49 + 20\sqrt{6} - 50 - 20\sqrt{6} = -1$ et donc $\alpha^4 - 10\alpha^2 + 1 = 0$. On pose note P le polynôme unitaire $X^4 - 10X^2 + 1$. On a $P(\alpha) = 0$, $P \in \mathbb{Q}(X)$ et $\deg(P) = \deg(\mathrm{Irr}(\alpha, \mathbb{Q})$ et donc $\mathrm{Irr}(\alpha, \mathbb{Q}) = X^4 - 10X + 1$.

d. De $4 = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] \times [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})]$, nous obtenons $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] = 2$. Ainsi $\deg(\mathrm{Irr}(\alpha, \mathbb{Q}(\sqrt{2})) = 2$. De même $\deg(\mathrm{Irr}(\alpha, \mathbb{Q}(\sqrt{3})) = 2$. Nous avons $\alpha^2 = 5 + 2\sqrt{6}$ et donc

$$\alpha^2 - 2\sqrt{2}\alpha = 5 + 2\sqrt{6} - 2\sqrt{2}^2 - 2\sqrt{6} = 1.$$

Ainsi $X^2 - 2\sqrt{2}X - 1 \in \mathbb{Q}(\sqrt{2})[X]$ est annulateur de α. Comme il est de degré 2 nous avons $\mathrm{Irr}(\alpha, \mathbb{Q}(\sqrt{2})) = X^2 - 2\sqrt{2}X - 1$. De même nous obtenons

$$\alpha^2 - 2\sqrt{3}\alpha = 5 + 2\sqrt{6} - 2\sqrt{6} - 2\sqrt{3}^2 = -1$$

puis $\mathrm{Irr}(\alpha, \mathbb{Q}(\sqrt{3})) = X^2 - 2\sqrt{3}X + 1$

Exercice 5.

a. Posons $P(X) = X^2 - X - 1$. Nous avons $P(0) = -1 \equiv 2 \mod 3$, $P(1) = -1 \equiv 2 \mod 3$ et $P(2) = 4 - 2 - 1 \equiv 1 \mod 3$. Le polynôme P n'a donc pas de racines dans $\mathbb{F}_3$. Comme il est de degré ≤ 3, il est irréductible dans $\mathbb{F}_3[X]$.

b. Comme P est irréductible, l'idéal (P) de $\mathbb{F}_3[X]$ est premier. Comme P est non nul, (P) est non nul et donc (P) est un idéal maximal de $\mathbb{F}_3[X]$ car $\mathbb{F}_3[X]$ est principal. Il en suit que le quotient $\mathbb{F}_3[X]/(P)$ est un corps. Comme $K = \mathbb{F}_3(\alpha)$ et $\mathrm{Irr}(\alpha, \mathbb{F}_3) = P$ qui est de degré 2, on a $[K : \mathbb{F}_3] = 2$ et donc

$$\mathrm{card}(K) = \mathrm{card}(\mathbb{F}_3)^{[K:\mathbb{F}_3]} = 3^2 = 9.$$

c. On a $\alpha^2 = \alpha + \overline{1} \neq 1$ puis $\alpha^4 = (\alpha + \overline{1})^2 = \alpha^2 + \overline{2}\alpha + \overline{1} = \overline{3}\alpha + \overline{2} = \overline{2}$ et enfin $\alpha^8 = \overline{2}^2 = \overline{4} = \overline{1}$. L'élément α est donc d'ordre 8.

d. Le groupe multiplicatif K^* est engendré par α.

Exercice 6. Posons $P = X^3 - 2$ et soit α une racine réélle de P. Notons $K = \mathbb{Q}(\alpha)$.

a. Le polynôme P est irréductible par Eisenstein ($p = 2$). Nous avons donc $[K : \mathbb{Q}] = \deg(\mathrm{Irr}(\alpha, \mathbb{Q})) = \deg(P) = 3$.

b. Les deux autres racines de P sont $j\alpha$ et $j^2\alpha$ où $j = e^{\frac{2i\pi}{3}}$. En effet

$$P(j^k\alpha) = j^{3k}\alpha^3 + 2 = \alpha^3 + 2 = P(\alpha) = 0.$$

c. Le corsp $\mathbb{K}$ ne contient que des réels et $j\alpha$ n'en est pas un. Ainsi K ne contient pas les K-conjugués de α et donc l'extension n'est pas normale.

d. Il y'a trois $\mathbb{Q}$-isomorphismes de K dans $\mathbb{C}$:

$$\psi_1 : \alpha \mapsto \alpha, \qquad \psi_2 : \alpha \mapsto j\alpha, \qquad \psi_3 : \alpha \mapsto j^2\alpha.$$

e. On pose $L = K(j)$ où $j = e^{\frac{2i\pi}{3}}$.

i. Nous avons

$$Q = \mathrm{Irr}(j, \mathbb{Q}) = \Phi_{3,\mathbb{Q}} = (X^3 - 1)/\Phi_{1,\mathbb{Q}} = (X^3 - 1)/(X - 1) = X^2 + X + 1.$$

ii. Comme j n'appartient pas à K le polynôme $\mathrm{Irr}(j, K)$ est de degré au moins 2. Or le polynôme Q est de degré 2 et appartient à $\mathbb{Q}[X] \subset K[X]$. D'où $\mathrm{Irr}(j, \mathbb{K}) = 2$ puis

$$[L : \mathbb{Q}] = [L : K] \times [K : \mathbb{Q}] = \deg(Q) \times 3 = 6.$$

f. L'extension $L/\mathbb{Q}$ est finie car de degré 6, séparable car $\mathbb{Q}$ est de caractéristique 0. Nous avons $L = \mathbb{Q}(\alpha, j)$ et le corps de décomposition de P sur K est $M = \mathbb{Q}(\alpha, j\alpha, j^2\alpha)$. De $j\alpha \in L$ et $j^2\alpha \in L$ nous avons $M \subseteq L$. Par ailleurs $j = \frac{j\alpha}{\alpha} \in M$ et donc $L \subseteq M$. Ainsi $L = M$ et L est le corps de décomposition de P sur K. L'extension L/K est donc normale puis galoisienne.

g. Les éléments de G sont

φ	α	j	$o(\varphi)$
φ_1	α	j	1
φ_2	α	j^2	2
φ_3	$j\alpha$	j	3
φ_4	$j\alpha$	j^2	2
φ_5	$j^2\alpha$	j	3
φ_6	$j^2\alpha$	j^2	2

h. Nous avons $(\varphi_2 \circ \varphi_4)(\alpha) = \varphi_2(\varphi_4(\alpha)) = \varphi_2(j\alpha) = j^2\alpha$ ainsi que $(\varphi_4 \circ \varphi_2)(\alpha) = \varphi_4(\varphi_2(\alpha)) = \varphi_4(\alpha) = j\alpha$. Ainsi $\varphi_2 \circ \varphi_4 \neq \varphi_4 \circ \varphi_2$ et le groupe G est non commutatif. Comme G est d'ordre 6 et non commutatif, G est isomorphe à $\mathfrak{S}_3$ le groupe symétrique de rank 3.