Extensions : correction

Exercice 1.

1. Si $n = 1$, L est un K-espace vectoriel de dimension 1 donc $K = L$. Si L'/K est un sous-extension de degré n, L' est un sous-espace vectoriel de L tel que $\dim_K L = \dim_K L'$ donc $L = L'$.
2. Notons d le degré de l'extension $K[a,b]/K[b]$. C'est également le degré du polynôme minimal de a sur $K[b]$ (qui est un des facteurs de P dans $K[b][X]$). En particulier, $d \leq \deg P = n$. D'après le théorème de la base télescopique,

$$[K[a,b] : K] = [K[a,b] : K[b]] \cdot [K[b] : K] = dm \leq nm.$$

   En outre, toujours d'après le théorème de la base télescopique,

$$[K[a,b] : K] = [K[a,b] : K[a]] \cdot [K[a] : K] = [K[a,b] : K[a]] \cdot n$$

   est un multiple de n. Puisque n et m sont premiers entre eux, le degré $[K[a,b] : K]$ est un multiple de nm. Puisqu'il est égal à dm, on a donc $d = n$, ce qui entraîne $[K[a,b] : K] = nm$ et le polynôme minimal de a sur $K[b]$ est de degré n : c'est donc bien P.

   Par ailleurs, toujours à cause de la base télescopique, le degré $[K[a] \cap K[b] : K]$ divise à la fois n et m, donc $[K[a] \cap K[b] : K] = 1$ et $K[a] \cap K[b] = K$.
3. Les éléments de L algébriques sur K forment un corps, donc x^2 est algébrique sur K. On a évidemment $K[x^2] \subseteq K[x]$ et il s'agit de démontrer l'inclusion réciproque. Tautologiquement, x annule le polynôme $X^2 - x^2 \in K[x^2][X]$, donc x est algébrique sur $K[x^2]$ de degré 1 ou 2. On a donc $[K[x] : K[x^2]] \in \{1,2\}$. Mais, d'après le théorème de la base télescopique,

$$[K[x] : K] = [K[x] : K[x^2]] \cdot [K[x^2] : K].$$

   Puisque $[K[x] : K]$ est de degré impair, on a nécessairement $[K[x] : K[x^2]] = 1$ et $K[x^2] = K[x]$.
4. D'après le théorème de la base télescopique,

$$n = [L : K] = [L : K[a]] \cdot [K[a] : K].$$

   Cela entraîne que le degré $[K[a] : K]$ est fini et divise n. Puisque $[K[a] : K]$ est fini, a est algébrique et son polynôme minimal est de degré $[K[a] : K]$.
5. Le nombre $\sqrt[n]{2} \in \mathbf{R}$ est évidemment algébrique sur $\mathbf{Q}$, puisqu'il annule le polynôme $X^n - 2$. Ce dernier vérifie le critère d'Eisenstein pour $p = 2$, donc est irréductible. Le nombre $\sqrt[n]{2}$ est donc algébrique sur $\mathbf{Q}$ de degré n et $\mathbf{Q}\left[\sqrt[n]{2}\right]/\mathbf{Q}$ est une extension de degré n.
6. La seule extension finie de $\mathbf{C}$ est l'extension triviale $\mathbf{C}/\mathbf{C}$, de degré 1. En effet, si $L/\mathbf{C}$ est une extension finie, tout élément $\alpha \in L$ est algébrique sur $\mathbf{C}$. Son polynôme minimal est donc un polynôme irréductible $P \in \mathbf{C}[X]$ tel que $P(\alpha) = 0$. Mais les polynômes irréductibles sur $\mathbf{C}$ sont de degré 1 : on a donc $P = X - \alpha$, ce qui entraîne $\alpha \in \mathbf{C}$ et donc $L = \mathbf{C}$.
7. Si on note, pour $P \in \mathbf{Q}[X] \setminus \{0\}$,

$$Z(P) = \left\{ z \in \mathbf{C} \,\middle|\, P(z) = 0 \right\},$$

on a par définition

$$\overline{\mathbf{Q}} = \bigcup_{P \in \mathbf{Q}[X] \setminus \{0\}} Z(P),$$

ce qui écrit $\overline{\mathbf{Q}}$ comme une union dénombrable d'ensembles finis et qui entraîne la dénombrabilité de $\overline{\mathbf{Q}}$.

Exercice 2.

(a) Les polynômes X^2-2 et X^3-2 sont irréductibles sur $\mathbf{Q}$ en vertu du critère d'Eisenstein. Ce sont donc les polynômes minimaux de $\sqrt{2}$ et $\sqrt[3]{2}$ sur $\mathbf{Q}$. On a donc

$$\begin{aligned}\left[\mathbf{Q}\left[\sqrt{2}\right]:\mathbf{Q}\right] &= 2 \text{ et une } \mathbf{Q}\text{-base de } \mathbf{Q}\left[\sqrt{2}\right] \text{ est } \left(1, \sqrt{2}\right)\\ \left[\mathbf{Q}\left[\sqrt[3]{2}\right]:\mathbf{Q}\right] &= 3 \text{ et une } \mathbf{Q}\text{-base de } \mathbf{Q}\left[\sqrt[3]{2}\right] \text{ est } \left(1, \sqrt[3]{2}, \sqrt[3]{4}\right)\end{aligned}$$

Le corps $\mathbf{Q}\left[\sqrt{2}, \sqrt[3]{2}\right]$ est évidemment inclus dans $\mathbf{Q}\left[\sqrt[6]{2}\right]$. Puisqu'en outre

$$\sqrt[6]{2} = \frac{\sqrt{2}}{\sqrt[3]{2}} = \frac{\sqrt{2}\cdot\sqrt[3]{4}}{2},$$

on a bien $\mathbf{Q}\left[\sqrt{2}, \sqrt[3]{2}\right] = \mathbf{Q}\left[\sqrt[6]{2}\right]$. Le polynôme X^6-2 étant irréductible sur $\mathbf{Q}$ d'après le critère d'Eisenstein, on a

$$\left[\mathbf{Q}\left[\sqrt{2}, \sqrt[3]{2}\right]:\mathbf{Q}\right] = 6 \text{ et une } \mathbf{Q}\text{-base de } \mathbf{Q}\left[\sqrt{2}, \sqrt[3]{2}\right] \text{ est } (1, 2^{1/6}, 2^{2/6} = \sqrt[3]{2}, 2^{3/6} = \sqrt{2}, 2^{4/6} = \sqrt[3]{4}, 2^{5/6}).$$

On voit en particulier que $\mathbf{Q}\left[\sqrt{2}\right] \cap \mathbf{Q}\left[\sqrt[3]{2}\right] = \mathrm{Vect}_{\mathbf{Q}}\left(1, \sqrt{2}\right) \cap \mathrm{Vect}_{\mathbf{Q}}\left(1, \sqrt[3]{2}, \sqrt[3]{4}\right) = \mathrm{Vect}_{\mathbf{Q}}(1) = \mathbf{Q}$. En particulier, on voit que X^2-2 n'a pas de racine dans $\mathbf{Q}\left[\sqrt[3]{2}\right]$ et que X^3-2 n'a pas de racine dans $\mathbf{Q}\left[\sqrt{2}\right]$. Puisque l'on a affaire à des polynômes de degré au plus 3, cela entraîne leur irréductibilité. Le polynôme X^2-2 est donc le polynôme minimal de $\sqrt{2}$ sur $\mathbf{Q}\left[\sqrt[3]{2}\right]$ et X^3-2 est le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbf{Q}\left[\sqrt{2}\right]$. On a donc

$$\begin{aligned}\left[\mathbf{Q}\left[\sqrt{2}, \sqrt[3]{2}\right]:\mathbf{Q}\left[\sqrt[3]{2}\right]\right] &= 2 \text{ et une } \mathbf{Q}\left[\sqrt[3]{2}\right]\text{-base de } \mathbf{Q}\left[\sqrt{2}, \sqrt[3]{2}\right] \text{ est } \left(1, \sqrt{2}\right)\\ \left[\mathbf{Q}\left[\sqrt{2}, \sqrt[3]{2}\right]:\mathbf{Q}\left[\sqrt{2}\right]\right] &= 3 \text{ et une } \mathbf{Q}\left[\sqrt{2}\right]\text{-base de } \mathbf{Q}\left[\sqrt{2}, \sqrt[3]{2}\right] \text{ est } \left(1, \sqrt[3]{2}, \sqrt[3]{4}\right)\end{aligned}$$

Notons qu'on aurait pu appliquer la deuxième question de l'exercice précédent, les degrés de $\sqrt{2}$ et $\sqrt[3]{2}$ sur $\mathbf{Q}$ étant premiers entre eux.

(b) Les nombres $\sqrt{2}$ et $\sqrt{3}$ sont tous les deux algébriques de degré 2 sur $\mathbf{Q}$, de polynômes minimaux X^2-2 et X^2-3, respectivement. Puisque ce sont des polynômes de degré 2, pour montrer que X^2-2 (resp. X^2-3) reste irréductible sur $\mathbf{Q}\left[\sqrt{3}\right]$ (resp. $\mathbf{Q}\left[\sqrt{2}\right]$), il s'agit de montrer que 2 (resp. 3) n'est pas un carré dans $\mathbf{Q}\left[\sqrt{3}\right]$ (resp. $\mathbf{Q}\left[\sqrt{2}\right]$). C'est assez facile :

$$\begin{aligned}2 \text{ est un carré dans } \mathbf{Q}\left[\sqrt{3}\right] &\Leftrightarrow \exists (a,b) \in \mathbf{Q} : \left(a + b\sqrt{3}\right)^2 = 2\\ &\Leftrightarrow \exists (a,b) \in \mathbf{Q} : a^2 + 3b^2 = 2 \text{ et } 2ab = 0\\ &\Leftrightarrow \exists a \in \mathbf{Q} : a^2 = 2 \text{ ou } \exists b \in \mathbf{Q} : b^2 = 2/3,\end{aligned}$$

ce qui est impossible (l'autre cas ne pose pas plus de problème). Cela entraîne que

$$\begin{aligned}\left[\mathbf{Q}\left[\sqrt{2}, \sqrt{3}\right]:\mathbf{Q}\left[\sqrt{3}\right]\right] &= 2 \text{ et une } \mathbf{Q}\left[\sqrt{3}\right]\text{-base de } \mathbf{Q}\left[\sqrt{2}, \sqrt{3}\right] \text{ est } \left(1, \sqrt{2}\right)\\ \left[\mathbf{Q}\left[\sqrt{2}, \sqrt{3}\right]:\mathbf{Q}\left[\sqrt{2}\right]\right] &= 2 \text{ et une } \mathbf{Q}\left[\sqrt{2}\right]\text{-base de } \mathbf{Q}\left[\sqrt{2}, \sqrt{3}\right] \text{ est } \left(1, \sqrt{3}\right)\end{aligned}$$

D'après le théorème de la base télescopique, on obtient en outre

$$\left[\mathbf{Q}\left[\sqrt{2},\sqrt{3}\right]:\mathbf{Q}\right]=4 \text{ et une } \mathbf{Q}\text{-base de } \mathbf{Q}\left[\sqrt{2},\sqrt{3}\right] \text{ est } \left(1,\sqrt{2},\sqrt{3},\sqrt{6}\right).$$

Évidemment, $\mathbf{Q}\left[\sqrt{2}+\sqrt{3}\right]\subseteq\mathbf{Q}\left[\sqrt{2},\sqrt{3}\right]$ donc $\sqrt{2}+\sqrt{3}$ doit être algébrique de degré divisant 4. Or, les éléments

$$1,\sqrt{2}+\sqrt{3} \text{ et } \left(\sqrt{2}+\sqrt{3}\right)^2=5+2\sqrt{6}$$

sont $\mathbf{Q}$-libres (il suffit de regarder leurs coordonnées dans la base $(1,\sqrt{2},\sqrt{3},\sqrt{6})$). Le nombre $\sqrt{2}+\sqrt{3}$ n'est donc pas algébrique de degré ≤ 2, ce qui entraîne qu'il est algébrique de degré 4. $\mathbf{Q}\left[\sqrt{2}+\sqrt{3}\right]\subseteq\mathbf{Q}\left[\sqrt{2},\sqrt{3}\right]$ est donc de $\mathbf{Q}$-dimension 4, ce qui entraîne $\mathbf{Q}\left[\sqrt{2}+\sqrt{3}\right]=\mathbf{Q}\left[\sqrt{2},\sqrt{3}\right]$.

D'après ce qui précède, le polynôme minimal de $\sqrt{2}+\sqrt{3}$ est l'unique polynôme unitaire de degré 4 qui l'annule. Cherchons-le. On remarque d'abord que $\left(\sqrt{2}+\sqrt{3}\right)^2=5+2\sqrt{6}$ est un élément de $\mathbf{Q}\left[\sqrt{6}\right]$: il doit donc être annulé par un polynôme de degré 2. En effet,

$$\left(5+2\sqrt{6}\right)^2=49+20\sqrt{6}=10\left(5+2\sqrt{6}\right)-1.$$

Le polynôme minimal de $\sqrt{2}+\sqrt{3}$ est donc $\mathrm{X}^4-10\mathrm{X}^2+1$.

(c) j est une racine primitive troisième de l'unité donc $j^2+j+1=0$. Le polynôme $\mathrm{X}^2+\mathrm{X}+1$ est irréductible sur $\mathbf{Q}$ (et même sur $\mathbf{R}$) donc

$$[\mathbf{Q}[j]:\mathbf{Q}]=2 \text{ et une } \mathbf{Q}\text{-base de } \mathbf{Q}[j] \text{ est } (1,j).$$

Remarquons que si l'on a deux extensions quadratiques $\mathbf{Q}[\alpha]/\mathbf{Q}$ et $\mathbf{Q}[\beta]/\mathbf{Q}$, $\alpha\in\mathbf{Q}[\beta]$ si et seulement si $\beta\in\mathbf{Q}[\alpha]$, car les deux propriétés sont équivalentes à l'égalité $\mathbf{Q}[\alpha]=\mathbf{Q}[\beta]$ (par égalité des dimensions).

Ainsi, puisque $j\notin\mathbf{Q}[\sqrt{3}]\subseteq\mathbf{R}$, on a $\sqrt{3}\notin\mathbf{Q}[j]$. Et puisque $j=-\dfrac{1}{2}+\dfrac{\sqrt{3}}{2}i\notin\mathbf{Q}[i]$ (car $\sqrt{3}\notin\mathbf{Q}$), on a $i\notin\mathbf{Q}[j]$.

(d) On a évidemment $\mathbf{Q}\left[\sqrt{3},j\right],\mathbf{Q}\left[\sqrt{3},i\right]\subseteq\mathbf{Q}\left[\sqrt{3},i,j\right]$. En fait, ces inclusions sont des égalités :

$$j=-\frac{1}{2}+\frac{\sqrt{3}}{2}i\in\mathbf{Q}\left[i,\sqrt{3}\right] \text{ donc } \mathbf{Q}\left[\sqrt{3},i,j\right]=\mathbf{Q}\left[\sqrt{3},i\right]$$
$$i=\frac{2j+1}{\sqrt{3}}\in\mathbf{Q}\left[j,\sqrt{3}\right] \text{ donc } \mathbf{Q}\left[\sqrt{3},i,j\right]=\mathbf{Q}\left[\sqrt{3},j\right].$$

Par ailleurs, on a vu que $\sqrt{3}\notin\mathbf{Q}[j]$, donc $\sqrt{3}$ est algébrique de degré 2 sur $\mathbf{Q}[j]$. Si on note $\mathrm{K}=\mathbf{Q}\left[\sqrt{3},j\right]=\mathbf{Q}\left[\sqrt{3},i\right]=\mathbf{Q}\left[\sqrt{3},i,j\right]$, on a donc, par le théorème de la base télescopique,

$$[\mathrm{K}:\mathbf{Q}]=[\mathrm{K}:\mathbf{Q}[j]]\cdot[\mathbf{Q}[j]:\mathbf{Q}]=4 \text{ et une } \mathbf{Q}\text{-base de K est } \left(1,\sqrt{3},j,\sqrt{3}j\right).$$

(e) $\cos\dfrac{2\pi}{3}=-\dfrac{1}{2}$ donc $\mathbf{Q}\left[\cos\dfrac{2\pi}{3}\right]=\mathbf{Q}$.

$\sin\dfrac{2\pi}{3}=\dfrac{\sqrt{3}}{2}$ donc $\mathbf{Q}\left[\sin\dfrac{2\pi}{3}\right]=\mathbf{Q}\left[\sqrt{3}\right]$, extension de degré 2 sur $\mathbf{Q}$, de $\mathbf{Q}$-base $\left(1,\sqrt{3}\right)$.

Le nombre complexe $\zeta_5=\cos\dfrac{2\pi}{5}+\sin\dfrac{2\pi}{5}i$ est, comme son nom l'indique, une racine cinquième primitive de l'unité. On a donc

$$0=1+\zeta_5+\zeta_5^2+\zeta_5^3+\zeta_5^4$$

Puisque

$$\text{Ré}\,\zeta_5 = \text{Ré}\,\zeta_5^4 = \cos\frac{2\pi}{5} \text{ et } \text{Ré}\,\zeta_5^2 = \text{Ré}\,\zeta_5^3 = \cos\frac{4\pi}{5} = 2\cos^2\frac{2\pi}{5} - 1,$$

le nombre $\cos\dfrac{2\pi}{5}$ est annulé par $2\left(2\mathrm{X}^2-1\right)+2\mathrm{X}+1 = 4\mathrm{X}^2+2\mathrm{X}-1$, et on a

$$\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}.$$

Donc $\mathbf{Q}\left[\cos\dfrac{2\pi}{5}\right] = \mathbf{Q}\left[\sqrt{5}\right]$, extension de degré 2 de $\mathbf{Q}$, de $\mathbf{Q}$-base $\left(1,\sqrt{5}\right)$.

On a

$$s = \sin\frac{2\pi}{5} = \sqrt{1-\cos^2\frac{2\pi}{5}} = \sqrt{1-\left(\frac{\sqrt{5}-1}{4}\right)^2} = \frac{\sqrt{10+2\sqrt{5}}}{4}.$$

On en déduit

$$\begin{aligned} s^2 &= \frac{5+\sqrt{5}}{8} \\ s^4 &= \left(\frac{5+\sqrt{5}}{8}\right)^2 = \frac{15+5\sqrt{5}}{32} = \frac{5}{4}s^2 - \frac{5}{16}. \end{aligned}$$

Le nombre $s = \sin\dfrac{2\pi}{5}$ est donc annulé par le polynôme $16\mathrm{X}^4-20\mathrm{X}^2+5$, qui est irréductible (en vertu du critère d'Eisenstein pour $p=5$ et du fait que le polynôme est primitif).

On a donc

$$\left[\mathbf{Q}\left[\sin\frac{2\pi}{5}\right] : \mathbf{Q}\right] = 4 \text{ et une } \mathbf{Q}\text{-base de } \mathbf{Q}\left[\sin\frac{2\pi}{5}\right] \text{ est } \left(1, \sin\frac{2\pi}{5}, \sin^2\frac{2\pi}{5}, \sin^3\frac{2\pi}{5}\right).$$

Remarquons que les coefficients disgracieux apparaissant dans les polynômes minimaux du cosinus et du sinus de $2\pi/5$ disparaîtraient si on considérait plutôt $2\cos\dfrac{2\pi}{5}$ et $2\sin\dfrac{2\pi}{5}$.

Exercice 3.

1. Le polynôme $\mathrm{P} = \mathrm{X}^3+2\mathrm{X}+2 \in \mathbf{Q}[\mathrm{X}]$ est irréductible en vertu du critère d'Eisenstein ($p=2$).
2. La relation $a^3+2a+2=0$ fournit immédiatement $a\cdot\left(a^2+2\right) = -2$ donc $\dfrac{1}{a} = -\left(\dfrac{a^2}{2}+1\right)$.

   Le deuxième calcul est plus pénible : on peut le faire
   - par identification des coefficients : les relations $a^3 = -2a-2$ et $a^4 = -2a^2-2a$ permettent de développer

     $$(a^2+a+1)(xa^2+ya+z) = (-x+y+z)a^2+(-4x-y+z)a+(-2x-2y+z)$$

     donc

     $$(a^2+a+1)(xa^2+ya+z) = 1 \Leftrightarrow \begin{cases} -x+y+z=0 \\ -4x-y+z=0 \\ -2x-2y+y=1 \end{cases} \Leftrightarrow \begin{cases} x = 2/7 \\ y = -3/7 \\ z = 5/7. \end{cases}$$

   - par l'algorithme d'Euclide :

     $$\begin{aligned} \mathrm{X}^3+2\mathrm{X}+2 &= (\mathrm{X}^2+\mathrm{X}+1)(\mathrm{X}-1)+(2\mathrm{X}+3) \\ \mathrm{X}^2+\mathrm{X}+1 &= (2\mathrm{X}+3)(1/2\mathrm{X}-1/4)+7/4 \end{aligned}$$

donc on obtient la relation de Bézout

$$\begin{aligned}1&=\frac{4}{7}\left((X^2+X+1)-(2X+3)(1/2X-1/4)\right)\\&=\frac{1}{7}\left[4(X^2+X+1)-(2X-1)\left((X^3+2X+2)-(X-1)(X^2+X+1)\right)\right]\\&=\frac{1}{7}\left((X^2+X+1)(2X^2-3X+5)-(X^3+2X+2)(2X-1)\right)\end{aligned}$$

donc X^2+X+1 et $(2X^2-3X+5)/7$ sont inverses modulo X^3+2X+2.
Dans les deux cas, on obtient

$$\frac{1}{a^2+a+1}=\frac{2a^2-3a+5}{7}.$$

Pour l'expression de u, on peut simplement effectuer la division euclidienne de $X^6+3X^4+2X^3+6X$ par X^3+2X+2 ou calculer méthodiquement en partant de l'expression de a^3, a^4, a^5 et a^6 en fonction de 1, a et a^2. Dans les deux cas on obtient

$$u=-2a^2+4a.$$

3. L'élément u appartient à $\mathbf{Q}(a)$, extension de $\mathbf{Q}$ de degré 3. C'est donc un élément algébrique sur $\mathbf{Q}$ de degré divisant 3. Comme en outre il n'appartient pas à $\mathbf{Q}$ (cela se voit dans sa décomposition sur la base $(1,a,a^2)$), il est de degré exactement 3. Il s'agit donc de chercher une relation de liaison entre 1, u, u^2 et u^3.
On peut toujours écrire la division euclidienne de

$$(-2X^2+4X)^3+\lambda(-2X^2+4X)^2+\mu(-2X^2+4X)+\nu$$

par (X^3+2X+2) :

$$\begin{aligned}-8X^6+48X^5+(4\lambda-96)X^4+(64-16\lambda)X^3+(16\lambda-2\mu)X^2+4\mu X+\nu&\\=(X^3+2X+2)\left[-8X^3+48X^2+(4\lambda-80)X-16-16\lambda\right]&\\+X^2\left(8\lambda-2\mu+64\right)+X\left(4\mu+24\lambda+192\right)+(32\lambda+\nu)&\end{aligned}$$

et résoudre un système linéaire pour obtenir l'annulation du reste

$$(X^3+2X+2)\text{ divise }(-2X^2+4X)^3+\lambda(-2X^2+4X)^2+\mu(-2X^2+4X)+\nu\Leftrightarrow\begin{cases}8\lambda-2\mu+64=0\\4\mu+24\lambda+192=0\\32\lambda+\nu=0\end{cases}$$

$$\Leftrightarrow\begin{cases}\lambda=-8\\\mu=0\\\nu=224\end{cases}$$

Mais il est sans doute plus simple de développer les puissances de u dans la base $(1,a,a^2)$:

$$\begin{array}{rcrcrcr}1&=&&&&&1\\u&=&-2a^2&+&4a&&\\u^2&=&8a^2&+&24a&+&32\\u^3&=&64a^2&+&192a&+&32\end{array}$$

et de chercher une relation de liaison :

$$u^3+\lambda u^2+\mu u+\nu=0 \Leftrightarrow \begin{cases} 32\lambda & & & + & \nu & = & -32 \\ 24\lambda & + & 4\mu & & & = & -192 \\ 8\lambda & - & 2\mu & & & = & -64 \end{cases} \Leftrightarrow \begin{cases} \lambda=-8 \\ \mu=0 \\ \nu=224 \end{cases}$$

Dans tous les cas, le polynôme minimal de u est X^3-8X^2+224.

Exercice 4.

1. Si L est un K-espace vectoriel fini et que $\alpha \in L$, le morphisme

$$\begin{aligned} \text{év}_\alpha : K[X] &\to L \\ P &\mapsto P(\alpha) \end{aligned}$$

ne peut pas être injectif ($\dim_K K[X]=\infty$) ; le nombre α est donc algébrique sur K. Le raisonnement étant valable pour tout $\alpha \in L$, l'extension L/K est algébrique.

2. Par définition, L/K est algébrique si et seulement si tout $\alpha \in L$ est algébrique sur K. Il s'ensuit que L/K est algébrique si et seulement si tous les $K[\alpha]/K$, $\alpha \in L$ le sont. Il s'agit donc de montrer qu'une extension du type $K[\alpha]/K$ (on parle d'*extension monogène*) est finie si et seulement si elle est algébrique.

   Le sens direct vient de la question précédente : une extension finie est algébrique. Réciproquement, si α est algébrique, $K[\alpha]$ est l'image du morphisme

$$\begin{aligned} \text{év}_\alpha : K[X] &\to L \\ P &\mapsto P(\alpha), \end{aligned}$$

   dont le noyau est (μ_α), l'idéal engendré par le polynôme minimal de α. On a donc un isomorphisme $K[\alpha] \simeq K[X]/(\mu_\alpha)$ et $K[\alpha]$ est un K-espace vectoriel de dimension $\deg \mu_\alpha$: $K[\alpha]/K$ est une extension finie.

3. Commençons par remarquer que le résultat est facile pour une extension L/K finie : un morphisme $f : L \to L$ est injectif en tant que morphisme de corps, et, s'agissant d'une application K-linéaire entre deux K-espaces vectoriels de même dimension, l'injectivité entraîne la bijectivité.

   Supposons maintenant simplement L/K algébrique. Le morphisme $f : L \to L$ est toujours injectif. Remarquons que si $\alpha_1, \dots, \alpha_n \in L$, le sous-anneau $K[\alpha_1, \dots, \alpha_n]$ est un sous-corps de L et l'extension $K[\alpha_1, \dots, \alpha_n]/K$ est finie. (Par récurrence sur n : le cas $n=1$ vient par exemple de la question précédente et, puisque α_n est algébrique sur K, il l'est aussi sur $K[\alpha_1, \dots, \alpha_{n-1}]$, donc $K[\alpha_1, \dots, \alpha_n]$ est un sous-corps de L et $K[\alpha_1, \dots, \alpha_n]/K[\alpha_1, \dots, \alpha_{n-1}]$ est une extension finie. Par le théorème de la base télescopique, le résultat est démontré).

   Soit donc $\alpha \in L$. Soit $\alpha_1=\alpha, \alpha_2, \dots, \alpha_n$ les racines dans L du polynôme minimal $\mu_\alpha \in K[X]$. Le morphisme K-linéaire $f : L \to L$ vérifie nécessairement

$$P(f(\alpha_i))=f(P(\alpha_i))=0 \text{ donc } \exists j \in [\![1,n]\!] : f(\alpha_i)=\alpha_j.$$

   Ainsi, f se restreint en un morphisme $K[\alpha_1, \dots, \alpha_n] \to K[\alpha_1, \dots, \alpha_n]$, qui est un isomorphisme d'après la première partie de la question. En particulier, il existe $\beta \in K[\alpha_1, \dots, \alpha_n] \subseteq L$ tel que $f(\beta)=\alpha$. Le morphisme f est donc bien un automorphisme.

4. Si $a \in K''$ est algébrique sur K', $K'[a]$ est un K'-espace vectoriel de dimension finie. Si K'/K est une extension finie, cela conclut : d'après le théorème de la base télescopique, $K'[a]$ sera

alors un K-espace vectoriel de dimension finie et $K[a] \subseteq K'[a]$ également, ce qui entraîne que a est algébrique sur K.

Dans le cas général, soit $\beta_1, \dots, \beta_n$ les coefficients du polynôme minimal $\mu_a^{K'} \in K'[X]$ de a sur K'. L'élément $a \in K''$ est alors algébrique sur le corps $K[\beta_1, \dots, \beta_n]$, qui est une extension finie de K car, comme K'/K est algébrique, les β_i sont algébriques sur K. On se ramène donc au cas précédent et $a \in K''$ est bien algébrique sur K.

5. Si $e+\pi$ et $e\pi$ étaient algébriques sur $\mathbf{Q}$, le polynôme $X^2 - (e+\pi)X + e\pi$ serait à coefficients dans $\overline{\mathbf{Q}}$. Les nombres $e, \pi \in \mathbf{C}$, racines de ce polynôme, seraient donc algébriques sur $\overline{\mathbf{Q}}$. La question précédente (appliquée à $K = \mathbf{Q}$, $K' = \overline{\mathbf{Q}}$ et $K'' = \mathbf{C}$) entraînerait donc que e et π soient algébriques sur $\mathbf{Q}$, ce qui est exclu par les théorèmes de Hermite et Lindemann.

Exercice 5.

1. Le morphisme
$$\begin{aligned} \text{év}_X : K[T] &\to K(X) \\ P(T) &\mapsto P(X) \end{aligned}$$
est évidemment injectif (son image est $K[X] \subseteq K(X)$) donc X est transcendant sur K.

2. Évidemment, les éléments de K sont algébriques sur K. Réciproquement, soit $\alpha = f(X)/g(X) \in L$ une fraction rationnelle (on suppose $f, g \in K[X]$ premiers entre eux) que l'on suppose algébrique sur K et soit $P \in K[T]$ son polynôme minimal. Si on écrit $P(T) = \sum_{k=0}^{d} a_k T^k$ (avec a_d non nul), la relation $P(\alpha) = 0$ devient
$$\sum_{k=0}^{d} a_k f(X)^k g(X)^{n-k} = 0.$$
En outre, P étant irréductible, on a $a_0 \neq 0$. Le polynôme $f(X)$ divise tous les $(f(X)^k g(X)^{n-k})_{k\geq 1}$ donc il doit diviser $a_0 g(X)^n$. Mais $a_0 \neq 0$ et on a supposé f et g premiers entre eux : la seule solution est que $f(X)$ doit être inversible (donc constant). De même, $g(X)$ divise tous les $(f(X)^k g(X)^{n-k})_{k<d}$ donc doit diviser $a_d f(X)^d$ et être constant. Finalement, f et g sont constants donc $\alpha \in K$.

3. Si $\beta \in L \setminus K$, β s'écrit $f(X)/g(X)$, où les polynômes $f(X), g(X)$ sont premiers entre eux et où au moins l'un des deux n'est pas constant. L'élément $X \in L$ est alors annulé par le polynôme non constant
$$f(T) - \frac{f(X)}{g(X)} g(T) \in K(\beta)[T]$$
et est donc algébrique sur $K(\beta)$. Comme l'ensemble des éléments de L algébriques sur $K(\beta)$ forme un corps contenant $K(\beta)$ et que l'on vient de voir qu'il contenait également X, on a que tout élément de K(X) est algébrique sur $K(\beta) : K(X)/K(\beta)$ est algébrique.

Exercice 6. Supposons que P ait une racine α dans une extension L/K de degré 2. Si $\alpha \in K$, P a une racine dans K et n'y est donc pas irréductible. Sinon, α est un algébrique de degré 2 sur K, et son polynôme minimal $\mu_\alpha \in K[X]$, de degré 2, divise P, qui n'est donc pas irréductible.
Réciproquement, supposons que P soit réductible. Le facteur de plus bas degré P_1 dans une décomposition non triviale de P est alors de degré 1 ou 2. Dans le premier cas, P_1 (et donc P) a une racine $\alpha \in K$. Dans le second, $K[X]/(P_1(X))$ est une extension de degré 2 de K dans lequel P_1 a une racine (la classe de X) donc P également. Dans les deux cas, P a une racine dans une extension de degré ≤ 2.

Remarquons que ce critère se généralise comme suit (avec la même preuve) : *un polynôme de degré n sur* K *est irréductible si et seulement s'il n'a aucune racine dans une extension* L/K *de degré* $\leq n/2$.

Exercice 7. Le polynôme X^3-2 est irréductible sur $\mathbf{Q}$ en vertu du critère d'Eisenstein ($p=2$) et annule β : c'est le polynôme minimal (sur $\mathbf{Q}$) de β et le corps $\mathbf{Q}[\beta]\subseteq\mathbf{C}$ est donc isomorphe à $\mathbf{Q}[X]/(X^3-2)$.
Le même raisonnement peut parfaitement être tenu en remplaçant β par $\alpha=\sqrt[3]{2}$. En particulier, on a un isomorphisme de corps $\varphi:\mathbf{Q}[\beta]\to\mathbf{Q}[\alpha]\subseteq\mathbf{R}$. Cela conclut : si $x_1,\dots,x_n$ étaient des éléments de $\mathbf{Q}[\beta]$ tels que $x_1^2+\cdots+x_n^2=-1$, on aurait

$$\varphi(x_1)^2+\cdots+\varphi(x_n)^2=\varphi(x_1^2+\cdots+x_n^2)=\varphi(-1)=-1.$$

Mais les $\varphi(x_i)^2$ sont des réels positifs : on obtient une contradiction.
Remarque. Un corps dans lequel -1 n'est pas une somme de carrés s'appelle un corps *formellement réel*. D'après un théorème dû à Emil Artin et Otto Schreier, ce sont exactement les corps qui peuvent être munis d'un ordre total compatible avec la structure de corps.
En ces termes plus savants, on vient donc de montrer que $\mathbf{Q}(\beta)$ était formellement réel en exhibant un morphisme $\mathbf{Q}(\beta)\to\mathbf{R}$. Dans la lancée du théorème d'Artin-Schreier, on peut montrer une forme de réciproque : étant donné une extension algébrique K/$\mathbf{Q}$, K est formellement réel si et seulement s'il existe un morphisme $K\to\mathbf{R}$ (cf. par exemple Milnor et Husemoller, *Symmetric Bilinear Forms*, ch. III, §. 2).

Exercice 8.

1. (a) Soit $P\in K[X]$ un polynôme unitaire de degré 2. On peut l'écrire $P=X^2-p_1X+p_2$ avec $p_1,\ p_2\in K$. En posant $a=p_1/2$ et $b=p_1^2/4-p_2$ (ce qui est licite car K n'est pas de caractéristique 2), on a bien $P=(X-a)^2-b$.
   (b) Soit $\widetilde{\alpha}\in L\setminus K$. La famille $(1,\widetilde{\alpha})$ est donc une famille K-libre de L. C'en est donc une base. On peut ainsi écrire $\widetilde{\alpha}^2=\mu\widetilde{\alpha}+\lambda$ pour un certain couple $(\lambda,\mu)\in K^2$. Le polynôme minimal de $\widetilde{\alpha}$ est alors $\mu_{\widetilde{\alpha}}(X)=X^2-\mu X-\lambda$ (ce polynôme est en effet annulateur, et il est clairement de degré minimal pour cette propriété). D'après la question précédente, il existe a et b dans K tels que $\mu_{\widetilde{\alpha}}(X)=(X-a)^2-b$. Soit $\alpha=\widetilde{\alpha}-a$. On a évidemment $K(\alpha)=K(\widetilde{\alpha})=L$, et $\alpha^2=(\widetilde{\alpha}-a)^2=b\in K$.
   (c) Soit $\beta\in L$ tel que $L=K(\beta)$ et $\beta^2\in K$. On peut alors écrire $\beta=\lambda\alpha+\mu$, pour $(\lambda,\mu)\in K^2$. On obtient alors $\beta^2=(\lambda^2\alpha^2+\mu)^2+2\lambda\mu\alpha$. L'hypothèse $\beta^2\in K$ entraîne donc que $\lambda=0$ ou que $\mu=0$. Mais le premier cas est impossible car il entraînerait $\beta\in K$; on a donc $\mu=0$, c'est-à-dire que $\beta/\alpha\in K$.
2. (a) L'extension $\mathbf{Q}(\sqrt{p})/\mathbf{Q}$ est de degré 2. Le réel $\sqrt{q}$ est une racine de $X^2-q\in\mathbf{Q}(\sqrt{p})[X]$. On a donc $[\mathbf{Q}(\sqrt{p},\sqrt{q}):\mathbf{Q}(\sqrt{p})]\leq 2$. Plus précisément, soit $\sqrt{q}\in\mathbf{Q}(\sqrt{p})$, soit l'extension $\mathbf{Q}(\sqrt{p},\sqrt{q})/\mathbf{Q}(\sqrt{p})$ est de degré 2. Mais le premier cas est impossible : il entraînerait $\mathbf{Q}(\sqrt{p})=\mathbf{Q}(\sqrt{q})$ et, d'après la question précédente, $\sqrt{p/q}\in\mathbf{Q}$, ce qui n'est pas (par exemple, si p/q était le carré d'un rationnel, sa valuation p-adique serait paire). On a donc bien $[\mathbf{Q}(\sqrt{p},\sqrt{q}):\mathbf{Q}(\sqrt{p})]=2$. Le théorème de la base télescopique entraîne donc que $\mathbf{Q}(\sqrt{p},\sqrt{q})/\mathbf{Q}$ est de degré 4.
   (b) Soit $\beta\in\mathbf{Q}(\sqrt{p},\sqrt{q})$ tel que $\beta^2\in\mathbf{Q}$. Si $\beta\in\mathbf{Q}(\sqrt{p})$, la question 1.(c) appliquée à l'extension $\mathbf{Q}(\sqrt{p})/\mathbf{Q}$ entraîne $\beta\in\mathbf{Q}$ ou $\beta/\sqrt{p}\in\mathbf{Q}$. Dans le cas contraire, la même question appliquée à $\mathbf{Q}(\sqrt{p},\sqrt{q})/\mathbf{Q}(\sqrt{p})$ entraîne que $\beta/\sqrt{q}\in\mathbf{Q}(\sqrt{p})$. On obtient donc (car $(\beta/\sqrt{q})^2\in\mathbf{Q}$) que $\beta/\sqrt{q}$ est un multiple rationnel de 1 ou $\sqrt{p}$.
   (c) D'après le théorème de la base télescopique, une sous-extension $\mathbf{Q}\subseteq K\subseteq\mathbf{Q}(\sqrt{p},\sqrt{q})$ est de degré 1, 2 ou 4. Évidemment, la seule sous-extension de degré 1 est $\mathbf{Q}/\mathbf{Q}$ et la seule

de degré 4 est $\mathbf{Q}(\sqrt{p},\sqrt{q})/\mathbf{Q}$. Si le degré est 2, la première partie entraîne l'existence de $\beta \in \mathbf{Q}(\sqrt{p},\sqrt{q})$ tel que $\mathrm{K}=\mathbf{Q}(\beta)$ et $\beta^2 \in \mathrm{K}$. D'après la première question, β est un multiple rationnel de $\sqrt{p}$, $\sqrt{q}$ ou $\sqrt{pq}$ (le cas $\beta \in \mathbf{Q}$ est exclu car il entraînerait $[\mathbf{Q}(\beta):\mathbf{Q}]=1$). Les sous-extensions de degré 2 sont donc $\mathbf{Q}(\sqrt{p})/\mathbf{Q}$, $\mathbf{Q}(\sqrt{q})/\mathbf{Q}$ et $\mathbf{Q}(\sqrt{pq})/\mathbf{Q}$.

(d) $(\sqrt{p}+\sqrt{q})^2 = p+q+2\sqrt{pq}$ donc $\sqrt{p}+\sqrt{q}$ annule

$$\mathrm{P} = (\mathrm{X}^2-(p+q))^2 - 4pq = \mathrm{X}^4 - 2(p+q)\mathrm{X}^2 + (p-q)^2.$$

D'après le théorème de la base télescopique, la famille $(1,\sqrt{p},\sqrt{q},\sqrt{pq})$ est une $\mathbf{Q}$-base de $\mathbf{Q}(\sqrt{p},\sqrt{q})$. Cette base est en outre adaptée aux trois sous-extensions quadratiques de $\mathbf{Q}(\sqrt{p},\sqrt{q})$:

$$\mathbf{Q}\left(\sqrt{p}\right) = \underset{\mathbf{Q}}{\mathrm{Vect}}\left(1,\sqrt{p}\right) \qquad \mathbf{Q}\left(\sqrt{q}\right) = \underset{\mathbf{Q}}{\mathrm{Vect}}\left(1,\sqrt{q}\right) \qquad \mathbf{Q}\left(\sqrt{pq}\right) = \underset{\mathbf{Q}}{\mathrm{Vect}}\left(1,\sqrt{pq}\right).$$

L'élément $\sqrt{p}+\sqrt{q}$ n'appartient donc à aucune de ces extensions quadratiques, ce qui entraîne $\mathbf{Q}(\sqrt{p}+\sqrt{q}) = \mathbf{Q}(\sqrt{p},\sqrt{q})$. Cela entraîne que $\deg \mu_{\sqrt{p}+\sqrt{q}} = [\mathbf{Q}(\sqrt{p}+\sqrt{q}):\mathbf{Q}] = 4$. On a donc $\mu_{\sqrt{p}+\sqrt{q}} = \mathrm{P} = \mathrm{X}^4 - 2(p+q)\mathrm{X}^2 + (p-q)^2$.

Exercice 9.

1. Un polynôme de degré 2 ou 3 est irréductible si et seulement s'il n'a pas de racine. Sur $\mathbf{F}_2$, il faut et il suffit donc que le coefficient constant soit égal à 1 (0 n'est pas racine) et que le nombre de coefficients égaux à 1 soit impair (1 n'est pas racine). Ainsi, les polynômes de degré 2 ou 3 irréductibles sont

$$\mathrm{X}^2+\mathrm{X}+1, \qquad \mathrm{X}^3+\mathrm{X}+1 \qquad \text{et} \qquad \mathrm{X}^3+\mathrm{X}^2+1.$$

En degré 4, il faut aussi empêcher que le polynôme soit le produit de deux irréductibles de degré 2. Sur $\mathbf{F}_2$, cela n'exclut que $(\mathrm{X}^2+\mathrm{X}+1) = \mathrm{X}^4+\mathrm{X}^2+1$. Les polynômes irréductibles de degré 4 sont donc

$$\mathrm{X}^4+\mathrm{X}^3+\mathrm{X}^2+\mathrm{X}+1, \qquad \mathrm{X}^4+\mathrm{X}+1 \qquad \text{et} \qquad \mathrm{X}^4+\mathrm{X}^3+1.$$

2. D'après ce qui précède, $\mathbf{F}_8 = \mathbf{F}_2[\mathrm{X}]/(\mathrm{X}^3+\mathrm{X}+1)$ est une extension de degré 3 de $\mathbf{F}_2$. Si on note ω la classe de X, on a donc

$$\mathbf{F}_8 = \{0,1,\omega,\omega+1,\omega^2,\omega^2+1,\omega^2+\omega,\omega^2+\omega+1\}$$

et ω vérifie $\omega^3 = \omega+1$. On aurait pu faire l'autre choix et construire $\mathbf{F}'_8 = \mathbf{F}_2[\mathrm{X}]/(\mathrm{X}^3+\mathrm{X}^2+1) = \mathbf{F}_2[\alpha]$, avec $\alpha^3 = \alpha^2+1$ mais on obtient ainsi un corps isomorphe. En effet,

$$(\omega+1)^3 = \omega^3+\omega^2+\omega+1 = \omega^2 = (\omega+1)^2+1.$$

Puisque $\omega+1 \notin \mathbf{F}_2 = \{0,1\}$, son polynôme minimal sur $\mathbf{F}_2$ est bien $\mathrm{X}^3+\mathrm{X}^2+1$ et l'application

$$\begin{aligned} \mathrm{év}_{\omega+1} : \mathbf{F}_2[\mathrm{X}] &\to \mathbf{F}_8 \\ \mathrm{P} &\mapsto \mathrm{P}(\omega+1) \end{aligned}$$

induit bien un isomorphisme $\varphi : \mathbf{F}'_8 = \mathbf{F}_2[\mathrm{X}]/(\mathrm{X}^3+\mathrm{X}^2+1) \to \mathbf{F}_8$ envoyant α sur $\omega+1$. On peut facilement calculer toutes les valeurs de φ :

$x \in \mathbf{F}'_8 \mapsto \psi(x) \in \mathbf{F}_8$	$x \in \mathbf{F}'_8 \mapsto \psi(x) \in \mathbf{F}_8$	$x \in \mathbf{F}'_8 \mapsto \psi(x) \in \mathbf{F}_8$	$x \in \mathbf{F}'_8 \mapsto \psi(x) \in \mathbf{F}_8$
$0 \mapsto 0$	$\alpha \mapsto \omega+1$	$\alpha^2 \mapsto \omega^2+1$	$\alpha^2+\alpha \mapsto \omega^2+\omega$
$1 \mapsto 1$	$\alpha+1 \mapsto \omega$	$\alpha^2+1 \mapsto \omega^2$	$\alpha^2+\alpha+1 \mapsto \omega^2+\omega+1.$

3. L'élément ω engendre $\mathbf{F}_8^\times$ (comme $\mathbf{F}_8^\times$ est un groupe d'ordre 7, tout élément de $\mathbf{F}_8^\times$ est un générateur).

$$\omega^0=1,\ \omega^1=\omega,\ \omega^2=\omega^2,\ \omega^3=\omega+1,\ \omega^4=\omega^2+\omega,\ \omega^5=\omega^2+\omega+1,\ \omega^6=\omega^2+1.$$

4. $\mathbf{F}_8/\mathbf{F}_2$ est une extension de degré 3 donc tous les éléments de $\mathbf{F}_8$ sont algébriques, d'un degré divisant 3, c'est-à-dire 1 ou 3. Il suffit donc, pour chaque élément de $\mathbf{F}_8 \setminus \mathbf{F}_2$ de déterminer lequel des deux polynômes irréductibles de degré 3 l'annule.

   Ainsi, 0 a pour polynôme minimal X, 1 a $X-1$; ω, ω^2 et $\omega^2+\omega$ ont X^3+X+1 et $\omega+1$, ω^2+1 et $\omega^2+\omega+1$ ont X^3+X+1.

5. Prenons $\mathbf{F}_{16}=\mathbf{F}_2[X]/(X^4+X+1)$ et appelons β la classe de X. On obtient que β est un générateur de $\mathbf{F}_{16}^\times$ (cette fois-ci, rien ne garantissait que ce soit le cas, puisqu'il y a des éléments de $\mathbf{F}_{16}^\times$, groupe cyclique d'ordre 15, qui ne l'engendrent pas, mais on est rassuré dès que l'on constate que β^3 et β^5 sont différents de 1) :

$$\begin{aligned}&\beta^0=1,\beta^1=\beta,\beta^2,\beta^3,\beta^4=\beta+1,\beta^5=\beta^2+\beta,\beta^6=\beta^3+\beta^2,\beta^7=\beta^3+\beta+1,\\&\beta^8=\beta^2+1,\beta^9=\beta^3+\beta,\beta^{10}=\beta^2+\beta+1,\beta^{11}=\beta^3+\beta^2+\beta,\beta^{12}=\beta^3+\beta^2+\beta+1,\\&\beta^{13}=\beta^3+\beta^2+1,\beta^{14}=\beta^3+1.\end{aligned}$$

   Maintenant, les éléments de $\mathbf{F}_{16}$ sont algébriques sur $\mathbf{F}_2$, de degré divisant 4. Il faut les répartir parmi les quatre polynômes minimaux possibles (le polynôme irréductible de degré 2 et les trois polynômes irréductibles de degré 4). Une remarque aide : comme $(X-1)(X^2+X+1)=X^3-1$ et $(X-1)(X^4+X^3+X^2+X+1)=X^5-1$ (évidemment, les $-$ sont aussi des $+$, mais il est plus facile de se souvenir de ces formules-ci), les éléments de $\mathbf{F}_{16}$ dont le polynôme minimal est X^2+X+1 (resp. $X^4+X^3+X^2+X+1$) sont les racines troisièmes (resp. cinquièmes) de l'unité différentes de 1, c'est-à-dire β^5 et β^{10} (resp. β^3, β^6, β^9 et β^{12}). Pour le reste des calculs (c'est-à-dire pour répartir les huit éléments restants entre les deux polynômes irréductibles X^4+X+1 et X^4+X^3+1) la table des puissances de β permet de mener les calculs relativement rapidement. Par exemple, $(\beta^3+\beta^2+\beta)^4+(\beta^3+\beta^2+\beta)^3+1=(\beta^{11})^4+(\beta^{11})^3+1=\beta^{44}+\beta^{33}+1=\beta^{14}+\beta^3+1=0$. On obtient ainsi les résultats suivants.
   – Le polynôme minimal de 0 est X ;
   – Le polynôme minimal de 1 est $X-1$;
   – Le polynôme minimal de $\beta^2+\beta$ et $\beta^2+\beta+1$ est X^2+X+1 ;
   – Le polynôme minimal de β^3, $\beta^3+\beta^2$, $\beta^3+\beta$ et $\beta^3+\beta^2+\beta+1$ est $X^4+X^3+X^2+X+1$;
   – Le polynôme minimal de β, $\beta+1$, β^2 et β^2+1 est X^4+X+1 ;
   – Le polynôme minimal de β^3+1, $\beta^3+\beta+1$, $\beta^3+\beta^2+1$ et $\beta^3+\beta^2+\beta$ est X^4+X^3+1.
   En particulier, on obtient ainsi des éléments de polynôme minimal X^4+X^3+1 et $X^4+X^3+X^2+X+1$, ce qui permet de trouver des morphismes de corps

$$\varphi'=\text{év}_{\beta^3+1}:\mathbf{F}'_{16}=\mathbf{F}_2[X]/(X^4+X^3+1)\to\mathbf{F}_{16},\qquad \varphi''=\text{év}_{\beta^3}:\mathbf{F}''_{16}=\mathbf{F}_2[X]/(X^4+X^3+X^2+X+1)\to\mathbf{F}_{16}$$

   qui sont des isomorphismes par égalité des cardinaux (ou des $\mathbf{F}_2$-dimensions).

   On remarque que l'on obtient de la même façon un morphisme de corps

$$\iota=\text{év}_{\beta^2+\beta}:\mathbf{F}_4=\mathbf{F}_2[X]/(X^2+X+1)\to\mathbf{F}_{16}$$

   dont l'image est $\{0,1,\beta^2+\beta,\beta^2+\beta+1\}$.

Exercice 10. Commençons par remarquer que le fait que $\sqrt{3}+\sqrt{2}$ soit une racine du polynôme $P=X^4-10X^2+1$ n'a rien de spécifique au corps $\mathbf{Q}(\sqrt{2},\sqrt{3})$. Plus précisément, si K est un corps

contenant deux éléments d et t dont les carrés valent respectivement 2 et 3, on obtient

$$\begin{aligned}\mathrm{P}(d+t) &= (d+t)^4 - 10(d+t)^2 + 1 = d^4 + 4d^3t + 6d^2t^2 + 4dt^3 + t^4 - 10\left(d^2 + 2dt + t^2\right) + 1\\ &= 4 + 8dt + 36 + 12dt + 9 - 10(2 + 2dt + 3) + 1 = 0.\end{aligned}$$

Ainsi, le polynôme P a une racine dans tout corps dans lequel 2 et 3 sont des carrés.
Puisqu'on va commencer à se demander si 2 et 3 sont des carrés, il vaut mieux distinguer tout de suite le cas des caractéristiques 2 et 3 : cela ne pose pas de problème puisque

$$\begin{aligned}&\text{dans } \mathbf{F}_2 : \mathrm{X}^4 - 10\mathrm{X}^2 + 1 = \mathrm{X}^4 + 1 = (\mathrm{X}+1)^4\\ &\text{dans } \mathbf{F}_3 : \mathrm{X}^4 - 10\mathrm{X}^2 + 1 = \mathrm{X}^4 + 2\mathrm{X}^2 + 1 = (\mathrm{X}^2+1)^2\end{aligned}$$

sont évidemment réductibles.
On peut alors vouloir utiliser le critère vu à l'exercice 6. Plus précisément, le résultat suivant, couplé à ce critère, montre l'exercice.
Lemme. Soit $p \geq 5$ un nombre premier. Alors $\mathbf{F}_p$ admet une extension de degré 2 dans lequel 2 et 3 sont des carrés.
Preuve. On va utiliser le fait bien connu que les éléments de $\mathbf{F}_p^\times$ qui sont des carrés forment un sous-groupe d'indice 2 dans $\mathbf{F}_p^\times$.
Si 2 et 3 sont déjà des carrés modulo p, il suffit de prendre une extension quadratique quelconque (c'est-à-dire qu'on prend $q \in \mathbf{F}_p$ qui ne soit pas un carré et on considère l'extension $\mathbf{F}_p[\sqrt{q}] = \mathbf{F}_q[\mathrm{X}]/(\mathrm{X}^2 - q)$).
Si 2 est un carré modulo p mais que 3 ne l'est pas, il suffit de prendre l'extension quadratique $\mathbf{F}_p[\sqrt{3}] = \mathbf{F}_q[\mathrm{X}]/(\mathrm{X}^2 - 3)$; dualement, si 3 est un carré mais que 2 ne l'est pas, il suffit de prendre l'extension $\mathbf{F}_p[\sqrt{2}] = \mathbf{F}_q[\mathrm{X}]/(\mathrm{X}^2 - 2)$.
Enfin, si ni 2 ni 3 n'est un carré, le fait que les carrés forment un sous-groupe d'indice 2 montre que 6 est un carré modulo p. Dans l'extension $\mathbf{F}_p[\sqrt{2}] = \mathbf{F}_p[\mathrm{X}]/(\mathrm{X}^2 - 2)$, 2 devient un carré et 6 le reste, donc $3 = 6/2$ devient lui aussi un carré.
Cela conclut la preuve.
Remarques.

- Bien qu'on n'en ait pas eu besoin dans la preuve, un fait supplémentaire permet d'obtenir une image beaucoup plus claire de ce qui se passe : on sait en effet que $\mathbf{F}_p$ possède une unique extension quadratique, $\mathbf{F}_{p^2}$, qui s'obtient en ajoutant une racine à un nombre qui n'en avait pas. Ainsi, les arguments que l'on a utilisés prouvent en fait que dans $\mathbf{F}_{p^2}$, tous les éléments de $\mathbf{F}_p$ sont des carrés.
- En utilisant explicitement la factorisation fournie par le critère de l'exercice 6, il est possible de transformer cette preuve en une preuve plus élémentaire : une fois que l'on sait que les carrés forment un sous-groupe d'indice 2 dans $\mathbf{F}_p^\times$, on sait qu'au moins un élément parmi 2, 3 et 6 possède une racine dans $\mathbf{F}_p^\times$. Ainsi, si l'on note d, t et s ces racines putatives, au moins une des trois factorisations suivantes a lieu dans $\mathbf{F}_p$:

  $$\begin{aligned}\mathrm{X}^4 - 10\mathrm{X}^2 + 1 &= (\mathrm{X}^2 - 2d\mathrm{X} - 1)(\mathrm{X}^2 + 2d\mathrm{X} - 1),\\ \mathrm{X}^4 - 10\mathrm{X}^2 + 1 &= (\mathrm{X}^2 - 2t\mathrm{X} + 1)(\mathrm{X}^2 + 2t\mathrm{X} + 1),\\ \mathrm{X}^4 - 10\mathrm{X}^2 + 1 &= (\mathrm{X}^2 - (5+2s))(\mathrm{X}^2 + (5+2s)).\end{aligned}$$

  Mais en l'absence de tout contexte, cette preuve semble pour le moins parachutée.