Correction du TD 3 – Extension de corps

Exercice 1. Par hypothèse le K-espace vectoriel M est fini. Il en est donc de même pour le Kespace vectoriel L. L'extension L/K est donc finie. Soit $(e_1, ..., e_n)$ une K-base de M. Pour tout $\lambda_1, ..., \lambda_n \in L$ on a $\lambda_1 e_1 + ... + \lambda_n e_n \in M$ et donc $(e_1, ..., e_n)$ est une L-famille génératrice de M. L'extension M/L est donc finie.

Exercice 2. Soient p et q des nombres premiers. Posons $P = X^2 - p$ et $Q = X^3 - q$. En utilisant le critère d'Eisenstein, on obtient que P et Q sont irréductibles. Les extensions $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ et $\mathbb{Q}(\sqrt[3]{q})/\mathbb{Q}$ sont de degrés repspectifs $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}]$ et $[\mathbb{Q}(\sqrt[3]{q}) : \mathbb{Q}]$ repsectivement. Supposons $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\sqrt[3]{q})$. On a alors

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

ce qui est impossible. Donc aucunes valeurs des premiers p et q permet d'avoir $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\sqrt[3]{q})$.

Exercice 3. Soit $P = X^n + \sum_{i=0}^{n-1} a_i X^i$ le polynôme minimal de α. De $P(\alpha) = 0$, on obtient

$$\alpha^n + \sum_{i=0}^{n-1} a_i \alpha^i = \alpha \left(\alpha^{n-1} + \sum_{i=1}^{n-1} a_i \alpha^{i-1} \right) + a_0 = 0.$$

Comme $\alpha \neq 0$, on a $P(X) \neq X$. De plus X ne peut pas divisze P, car il est irréductible. On obtient donc $a_0 \neq 0$. On obtient donc

$$\alpha^{-1} = -\frac{\alpha^{n-1} + \sum_{i=1}^{n-1} a_i \alpha^{i-1}}{a_0}.$$

Exercice 4. Le polynôme $X^3 - 2$ est irréductible par le critère d'Eisenstein avec $p = 2$.

a. L'élément y est inversible car non nul. Son inverse est dans $L = \mathbb{Q}(x) = \mathbb{Q}[x]$ car x est algébrique. Le polynôme minimal est $X^3 - 2$ qui est de degré 3 est donc L est le $\mathbb{Q}$-espace vectoriel de base $(1, x, x^2)$. Il existe donc des rationnels a, b et c tel que $y^{-1} = ax^2 + bx + c$. L'équation $yy^{-1} = 1$ devient alors

$$(x^2 + 2x + 3)(ax^2 + bx + c) = 1,$$

qui donne

$$ax^4 + (2a + b)x^3 + (3a + 2b + c)x^2 + (3b + 2c)x + 3c = 1.$$

De $P(x) = 0$, on obtient $x^3 = 2$ et donc l'équation précédente devient :

$$(3a + b + c)x^2 + (2a + 3b + 2c)x + (4a + 2b + 3c) = 1.$$

Comme la famille $(1, x, x^2)$ est libre on obtient le système

$$\begin{cases} 3a + 2b + c &= 0, \\ 2a + 3b + 2c &= 0, \\ 4a + 2b + 3c &= 1. \end{cases}$$

Après résolution, on obtient $a = \frac{1}{11}$, $b = -\frac{4}{11}$ et $c = \frac{5}{11}$. D'où $y^{-1} = \frac{1}{11}x^2 - \frac{4}{11}x + \frac{5}{11}$.

b. Comme y est dans L, son polynôme minimal est de degré au plus 3.
On calcule d'abord y^2 :

$$\begin{aligned} y^2 &= (x^2+2x+3)^2 = x^4+4x^3+10x^2+12x+9 \\ &= 10x^2+14x+17 \end{aligned}$$

Ensuite on calcule y^3 :

$$\begin{aligned} y^3 &= (10x^2+14x+17)(x^2+2x+3) = 10x^4+34x^3+75x^2+76x+51 \\ &= 75x^2+96x+119 \end{aligned}$$

Résolvons le système $y^3+ay^2+by+c=0$:

$$\begin{cases} 75+10a+b & =0 \\ 96+14a+2b & =0 \\ 119+17a+3b+c & =0 \end{cases} \Leftrightarrow \begin{cases} 10a+b & =-75 \\ 14a+2b & =-96 \\ 17a+3b+c & =-119 \end{cases}$$

Après résolution, on trouve $a=-9$, $b=15$ et $c=-11$. L'élément y est donc racine du polynôme $Q=X^3-9X^2+15X-11$. Le polynôme $\overline{Q}$ n'ayant pas de racines dans $\mathbb{F}_7$ il est irréductible et donc Q est irréductible dans $\mathbb{Q}[X]$. On obtient donc $\mathrm{Irr}(y,\mathbb{Q})=Q$.

c. Soit $\alpha \in L \setminus \mathbb{Q}$. On a donc $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(x) = L$. Comme L/Q est finie, on a

$$3 = [L:\mathbb{Q}] = [L:\mathbb{Q}(\alpha)] \times [\mathbb{Q}(\alpha):\mathbb{Q}],$$

ainsi $[\mathbb{Q}(\alpha):\mathbb{Q}]$ vaut 1 ou 3. Si elle vaut alors $\mathrm{Irr}(\alpha,\mathbb{Q}) = X-\alpha$ et donc $\alpha \in \mathbb{Q}$, ce qui est impossible par hypothèse. Ainsi $\mathbb{Q}(\alpha)/\mathbb{Q}]$ est de degré 3 et donc algébrique.

Exercice 5.

a. Comme tout élément de $\mathbb{Q}$ est algébrique sur $\mathbb{Q}$, on a $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$. En particulier $\overline{\mathbb{Q}}$ contient 1 et est donc non vide. Soit a, b dans $\overline{\mathbb{Q}}$. Les éléments a et b sont donc algébrique sur $\mathbb{Q}$. Les éléments $x+y$ et xy sont aussi algébriques et donc dans $\overline{\mathbb{Q}}$. Notons $P(X)$ le polynôme minimal de a. Le polynôme $Q(X)=P(-X)$ est irréductible et admet $-a$ comme racine. Il en suit que $-a$ est algébrique et donc dans $\overline{\mathbb{Q}}$. L'ensemble $\overline{\mathbb{Q}}$ est donc un sous-anneau de $\mathbb{C}$. Par l'exercice 3, c'est un sous-corps.

b. Soit a un élément de $\mathbb{C}$ algébrique que $\overline{\mathbb{Q}}$. Comme l'extension $\overline{\mathbb{Q}}/\mathbb{Q}$ est algébrique a est algébrique sur $\mathbb{Q}$. L'élément a est donc dans $\overline{\mathbb{Q}}$. Il en suit que $\overline{\mathbb{Q}}$ est algébriquement clos.

Exercice 6. Notons m l'application de L dans $\mathrm{End}_K(L)$ qui à x associe m_x.

a. Soient x, y, z des élément de L . On a

$$m(x+y)(z) = m_{x+y}(z) = (x+y)\cdot z = tx\cdot z + y\cdot z = m_x(z)+m_y(z).$$

On obtient ainsi $m(x+y) = \lambda m_x + m_y$. De même, on a

$$m(x\cdot y)(z) = (x\cdot y)\cdot z = x\cdot(y\cdot z) = m_x(m_y(z)) = (m_x\circ m_y)(z).$$

De plus $m_1(z) = 1\cdot z = 1_{\mathrm{End}_K(L)}(z)$ et donc $m(1) = 1_{\mathrm{End}_K(L)}$. L'application m est donc un morphisme unitaire d'anneau.

b. Soit $P = \sum_{i=0}^{n} a_i X^i$ le polynôme caractéristique de m_x. Par le théorème de Hamilton-Cayley, on a $P(m_x) = 0$. On a donc $\sum_{i=0}^{n} a_i \cdot m_x^i = 0_{\mathrm{End}_K(L)}$. En évaluant cette endomorphisme en 1 on obtient

$$0 = P(m_x)(1) = \left(\sum_{i=0}^{n} a_i m_x^i\right)(1) = \sum_{i=0}^{n} a_i m_x^i(1) = \sum_{i=0}^{n} a_i x^i = P(x).$$

Exercice 7. Le polynôme P est irréductible par le critère d'Eisenstein. Les racines de P sont $\sqrt[3]{2}$, $\sqrt[3]{2}j$ et $\sqrt[3]{2}j^2$ avec $j = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Pour simplifier posons $x = \sqrt[3]{2}j$ et $\sqrt[3]{2}j^2$. Remarquons la relation $x' = \overline{x}$

a. On a $x + x' = 2\,\mathrm{Re}(x) = -\sqrt[3]{2}$ et $x - x' = 2\,\mathrm{Im}(x)i = \sqrt[3]{2}\sqrt{3}i$. On a donc

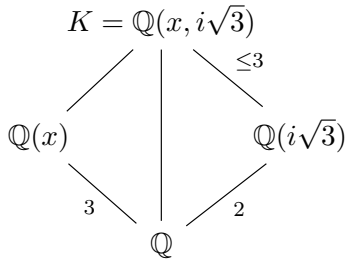
$$i\sqrt{3} = \frac{x' - x}{x + x'} \in K.$$

b. De $i\sqrt{3} \in K$. On obtient $\mathbb{Q}(x, i\sqrt{3}) \subseteq K$. De la relation précédente on obtient

$$x' = \frac{x \times (1 - i\sqrt{3})}{1 + i\sqrt{3}} \in \mathbb{Q}(x, i\sqrt{3}),$$

et donc $K = \mathbb{Q}(x, x') \subseteq \mathbb{Q}(x, i\sqrt{3})$. Il en résulte $K = \mathbb{Q}(x, i\sqrt{3})$.

c. Le polynôme P étant de degré 3 on a $[\mathbb{Q}(x) : \mathbb{Q}] = 3$. C' est aussi un polynôme annulateur de x sur $\mathbb{Q}(i\sqrt{3})$, c'est donc un multiple de $\mathrm{Irr}(x, \mathbb{Q}(i\sqrt{3}))$. On a donc $[\mathbb{Q}(x, i\sqrt{3}) : \mathbb{Q}(i\sqrt{3})] \leq 3$. Le polynôme minimal de $i\sqrt{3}$ est $X^2 - 3$ (critère d'Eisenstein), on a donc $[\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}] = 2$. On obtient donc le diagramme suivant :



Le degré de $[K : \mathbb{Q}]$ doit dont être multiple de 2 et 3 et inférieur ou égale à 6 et donc $[K : \mathbb{Q}] = 6$.

d.

i. Par calculs directs ou avec `Maxima` par exemple.

ii. Par calculs directs ou avec `Maxima` par exemple.

iii. Par calculs directs ou avec `Maxima` par exemple.

iv. Supposons que Q soit le produit de deux polynômes F et G de degré ≥ 1. C'est alors aussi le cas dans $\mathbb{F}_p$. Ainsi par **ii.** F est de degré 3 tandis que par **iii.** il doit être de degré 2 ou 4. Le polynôme Q est donc irréductible.

v. Les éléments y et $i\sqrt{3}$ étant dans K, on a $z \in \mathbb{K}$ et donc $\mathbb{Q}(z) \subseteq K$. De

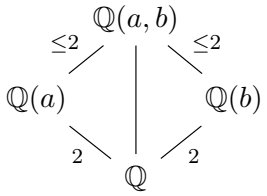
$$6 = [\mathbb{Q}(z) : \mathbb{Q}] = \deg(Q) = [K : \mathbb{Q}],$$

on obtient alors $K = \mathbb{Q}(z)$.

Exercice 8.

a. Posons $a = \sqrt{2}$ et $b = \sqrt{3}$. On a $\mathrm{Irr}(a, \mathbb{Q}) = X^2 - 2$ et $\mathrm{Irr}(b, \mathbb{Q}) = X^2 - 3$ (on montre que c'est polynôme sont irréductibles avec le critère d'Eisensetein). De plus $X^2 - 2$ et $X^2 - 3$ sont des polynômes anulateur de a et b sur $\mathbb{Q}(b)$ et $\mathbb{Q}(a)$ respectivement.

On a donc $\mathrm{Irr}(a, \mathbb{Q}(b)) \leq 2$ et $\mathrm{Irr}(b, \mathbb{Q}(a)) \leq 2$.On alors le diagramme suivant

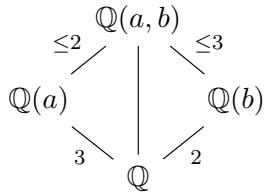


Si $\mathbb{Q}(a) = \mathbb{Q}(b)$ alors il existe des rationnels s et t tels qu'on ait $a = s + tb$. Et donc $2 = a^2 = s^2 + 2stb + 3$. Ce qui donne $b = (-1 - s^2)/(2st) \in \mathbb{Q}$ ce qui est impossible. On a donc $[\mathbb{Q}(a, b) : \mathbb{Q}(a)] = [\mathbb{Q}(a, b) : \mathbb{Q}(b)] = 2$ puis $[\mathbb{Q}(a, b) : \mathbb{Q}] = 4$.
La famille $\mathcal{F} = \{1, a, b, ab\}$ est une famille $\mathbb{Q}$-génératrice et donc une $\mathbb{Q}$-base de $\mathbb{Q}(a, b)$. On a $m_{a+b}(1) = a + b$, $m_{a+b}(a) = a^2 + ab = 2 \cdot 1 + ab$, $m_{a+b}(b) = ab + b^2 = 3 \cdot 1 + ab$ et $m_{a+b}(ab) = a^2b + ab^2 = 2 \cdot a + 3 \cdot b$. La matrice de m_{a+b} relativement à la base $\mathcal{F}$ est

$$A = \begin{bmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 2 \\ 1 & 0 & 0 & 3 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

Le polynôme $\chi_A(X) = X^4 - 10X^2 + 1$ est donc annulateur de $\sqrt{2} + \sqrt{3} = a + b$. On montre qu'il est irréductible et donc $\mathrm{Irr}(\sqrt{2} + \sqrt{3}, \mathbb{Q}) = X^4 - 10X^2 + 1$ (En réduisant modulo 3 on montre qu'il n'a pas de facteur de degré 1, on montre ensuite qu'on ne peut pas le factoriser comme produit de polynômes de degré 2 dans $\mathbb{Z}[X]$ et donc dans $\mathbb{Q}[X]$).

b. On pose $a = \sqrt[3]{7}$ et $b = \sqrt{2}$. On a $\mathrm{Irr}(a, \mathbb{Q}) = X^3 - 7$ et $\mathrm{Irr}(b, \mathbb{Q}) = X^2 - 2$, encore par Einsenstein. Comme précédemment on a



L'extension $[\mathbb{Q}(a, b) : \mathbb{Q}]$ doit donc être de degré multiple de 6 et inférieur à 6. Elle est donc de degré 6. La famille $\mathcal{F} = \{1, a, a^2, b, ab, a^2b\}$ est une famille $\mathbb{Q}$-génératrice et donc une $\mathbb{Q}$-base de $\mathbb{Q}(a, b)$. La matrice de m_{a+b} relativement à la famille $\mathcal{F}$ est

$$\begin{bmatrix} 0 & 0 & 7 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & 0 & 0 & 7 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix},$$

et son polynôme caractéristique est

$$\chi_A(X) = X^6 - 6X^4 - 14X^3 + 12X^2 - 84X + 41.$$

On commence par montrer que se polynôme n'a pas de racine en considérant sa réduction modulo 3. Il faut ensuite montre qu'il ne peut pas avoir de facteur de degré 2 ni de degré 3 dans $\mathbb{Z}[X]$.

c. On trouve $\mathrm{Irr}(i + j, \mathbb{Q}) = X^4 + 2X^3 + 5X^2 + 4X + 1$.

d. On trouve $\mathrm{Irr}(j\sqrt{2}, \mathbb{Q}) = X^4 + 2X^2 + 4$.

Exercice 9. Posons $\zeta = a + ib$.

a. Un polynôme annulateur de ζ est $X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1)$. Un a déjà montré que le polynôme $P = X^4 + X^3 + X^2 + X + 1$ est irréductible, on a donc $\mathrm{Irr}(\zeta, \mathbb{Q}) = P$.

b. Posons $\alpha = \zeta + \zeta^{-1}$. On a $\alpha = \zeta + \overline{\zeta} = 2\,\mathrm{Re}(\zeta) = 2a$. De plus $\zeta^2 + \zeta^3 = \zeta^2 + \overline{\zeta^2} = 2\,\mathrm{Re}(\zeta^2)$. Or $\zeta^2 = a^2 - b^2 + 2aib$. De $|\zeta| = 1$ on a $a^2 + b^2 = 1$ et donc $\mathrm{Re}(\zeta^2) = a^2 - (1 - a^2) = 2a^2 - 1$ et donc $\zeta^2 + \zeta^3 = 2a^2 - 1$. On obtient ainsi

$$0 = 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 1 + 2a + 4a^2 - 2 = 4a^2 + 2a - 1 = (2a)^2 + 2a - 1$$

Posons $Q = X^2 + X - 1$, on a $\Delta = 5$ et les racines de Q sont $\frac{-1-\sqrt{5}}{2}$ et $\frac{-1+\sqrt{5}}{2}$. On a donc $\mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(\sqrt{5})$.

c. On a $\zeta\alpha = \zeta(\zeta + \zeta^{-1}) = \zeta^2 + 1$ et donc ζ est racine de $R = X^2 - X\alpha + 1 \in K[X]$. De $4 = [\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : K] \times [K : \mathbb{Q}]$ on obtient $[\mathbb{Q}(\zeta) : K] = 2$ et donc R est irréductible sur $K[X]$.

Exercice 10.

a. Soit $x \in L \setminus K$. L'extension L/K étant finie, elle est algébrique et donc x est algébrique sur K. Comme L/K est quadratique, le polynôme $\mathrm{Irr}(x, K)$ est de dégré 1 ou 2. Il ne peut pas être de degré 1 car $x \notin K$. Il est denc de degré 2 et on a $L = \mathbb{Q}(x)$. On note $X^2 + aX + b$ le polynôme $\mathrm{Irr}(x, \mathbb{Q})$. On a

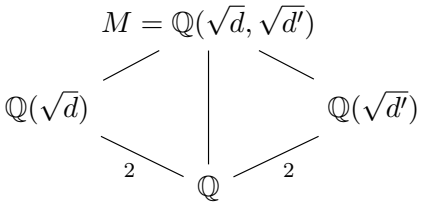
$$X^2 + aX + b = \left(X + \frac{a}{2}\right)^2 + b - \frac{a^2}{4} \quad \text{car } \mathrm{car}(K) \neq 2$$

Posons $d = \frac{a^2}{4} - b$, $Q = X^2 - d$ et $y = x + \frac{a}{2}$. On a alors $Q(y) = 0$. De $x \in L$, on a $y = x + \frac{a}{2} \in L$ et donc $\mathbb{Q}(y) \subset \mathbb{Q}(x) = L$. De même $x = y - \frac{a}{2} \in \mathbb{Q}(y)$ et $\mathbb{Q}(x) \subseteq \mathbb{Q}(y)$. On a donc $\mathbb{Q}(x) = \mathbb{Q}(y)$ avec $y^2 = d$. On a ainsi montrer $L = \mathbb{Q}(\sqrt{d})$. De plus Q est irréductible si et seulement si $\Delta = a^2 - 4b$ n'est pas un carré dans K et donc si etseulement si $d = \frac{a^2}{4} - b$ n'est pas un carré dans K. Comme d ne peut pas être nul on a $d \in K^* \setminus (K^*)^2$.

b. Soit $x \in L$. On a alors $\mathbb{Q}(x) \subseteq L$. Le dégré de $\mathbb{Q}(x)/\mathbb{Q}$ est donc 1 ou 2. Si le degré est 1, le polynôme irréductible de x est $X - x \in K[X]$ qui ne possède que x comme racine (avec $x \in K$). Sinon posons $\mathrm{Irr}(x, K) = X^2 + aX + b$. Soit $y \in \Omega$ une autre racine de $X^2 + aX + b$. On a alors $b = xy$ puis $y = \frac{b}{x} \in L$.

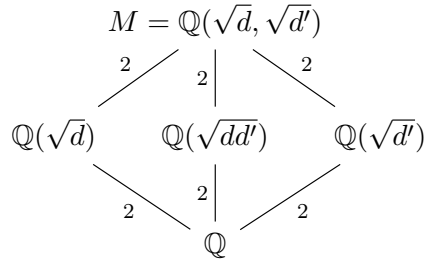
c. Soit $x \in K^*$ on alors $x^2 \in (K^*)^2 \subseteq (L^*)^2$, $x^2 \in K$, $dx^2 = (\sqrt{d}x)^2 \in (L^*)^2$ et $dx^2 \in K$. On obtient alors $(K^*)^2 \cup d(K^*)^2 \subseteq (L^*)^2 \cap K$. Réciproquement. Soit $y \in (L^*)^2 \cap K$. On a alors $y = x^2$ avec $x \in L^*$. Il existe donc $a, b \in K$ avec $a \neq 0$ ou $b \neq 0$ tel que $x = a + b\sqrt{d}$. On a $y = x^2 = (a^2 + bd^2) + 2ab\sqrt{d}$. De $y \in K$ on obtient $2ab = 0$ puis $ab = 0$ (car $\mathrm{car}(K) \neq 2$). Si $a = 0$ et donc $b \neq 0$ on a $x \in K^*$ et donc $y \in (K^*)^2$. Si $b = 0$ et donc $a \neq 0$, on a $y = db^2 \in d(K^*)^2$. On a donc $y \in (K^*)^2 \cup d(K^*)^2$ puis $(L^*)^2 \cap K \subseteq (K^*)^2 \cup d(K^*)^2$.

d. **i.** Supposons $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ de degré 1 on a alors $\sqrt{d} \in \mathbb{Q}$. Il existe alors $a, b \in \mathbb{Z}$ avec $b \neq 0$, $a \wedge b = 1$ tel que $\sqrt{d} = \frac{a}{b}$. On a alors $d = \frac{a^2}{b^2}$ puis $db^2 = a^2$. Si $a = \pm 1$ alors $d = \frac{1}{b^2} \in \mathbb{Z}$ et donc $b^2 = 1$ puis $d = 1$ impossible car 1 n'est pas divisible pas un carré ($1 = 1^2$). Supposons alors $a \neq \pm 1$. L'entier a est alors divisible par un premier p. On a donc p^2 divise db^2. Comme a et b sont premiers entre eux, b n'est pas divisible par p et donc p^2 divise d ce qui est impossbile par hypothèse.On a donc $\sqrt{d} \notin \mathbb{Q}$. L'extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ est donc de degré ≥ 2. Comme $X^2 - d \in \mathbb{Q}[X]$ est annulateur de $\sqrt{2}$ on a $\mathrm{Irr}(\sqrt{d}, \mathbb{Q})|(X^2 - d)$ et donc $\mathrm{Irr}(\sqrt{d}, \mathbb{Q}) = X^2 - d$ puis $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$. De même $[\mathbb{Q}(\sqrt{d'}) : \mathbb{Q}] = 2$. On a alors



Comme $X^2 - d'$ est en particulier un polynôme de $\mathbb{Q}(\sqrt{d})[X]$, on a que $\mathrm{Irr}(\sqrt{d'}, \mathbb{Q}(\sqrt{d})$ divise $X^2 - d'$ et donc l'extension $M/\mathbb{Q}(\sqrt{d})$ est de degré au plus 2. Si elle était de dégré 1 alors on aurait $\sqrt{d'} \in \mathbb{Q}(\sqrt{d})$ et donc $d' \in (\mathbb{Q}(\sqrt{d})^*)^2 \cap \mathbb{Q}$ qui est $(\mathbb{Q}^*)^2 \cup d(\mathbb{Q}^*)^2$. On aurait donc $d' \in (\mathbb{Q}^*)^2 \cup d(\mathbb{Q}^*)^2$. L'appartenance $d' \in (\mathbb{Q}^*)^2$ implique $\sqrt{d'} \in \mathbb{Q}^*$ et contredit $[\mathbb{Q}(\sqrt{d'} : \mathbb{Q}] = 2$. Tandis que $d' \in d(\mathbb{Q}^*)^2$ implique que d'/d soit un carré, ce qui est impossible par hypothèse. On a donc $[M : \mathbb{Q}(\sqrt{d})] = 2$ puis $[M : \mathbb{Q}] = 4$.

ii. Montrons que $\mathbb{Q}(\sqrt{dd'})/\mathbb{Q}$ est une extension quadratique. Si elles est de degré 1 alors $\sqrt{dd'}$ appartient à $\mathbb{Q}^*$ et donc $\sqrt{dd'} = \frac{a}{b}$ avec $a, b \in \mathbb{Z}$, $b \neq 0$, $a \wedge b = 1$ et donc $dd' = \frac{a^2}{b^2}$ puis $\frac{d'}{d} = \frac{a^2}{(bd)^2}$, ce qui est impossible par hypothèse. L'exstension $\mathbb{Q}(\sqrt{dd'})/\mathbb{Q}$ est donc de degré supérieur ou égale 2. Comme $\sqrt{dd'}$ est racine de $X^2 - dd' \in \mathbb{Q}[X]$ elle est quadratique.
Comme précédement supposons $\sqrt{dd'} \in \mathbb{Q}(\sqrt{d}) = L$. On a alors $dd' \in (L^*)^2 \cap \mathbb{Q} = (\mathbb{Q}^*)^2 \cup d(\mathbb{Q}^*)^2$. On ne peut pas avoir $dd' \in (\mathbb{Q}^*)^2$ car sinon $\mathbb{Q}(\sqrt{dd'})/\mathbb{Q}$ serait de degré 1. De même si $dd' \in d(\mathbb{Q}^*)^2$ alors $d' \in (\mathbb{Q}^*)^2$ et alors $\mathbb{Q}(\sqrt{d'})/\mathbb{Q}$ serait de degré 1. On a donc $\sqrt{dd'} \notin \mathbb{Q}(\sqrt{d})$ et donc $\mathbb{Q}(\sqrt{dd'}) \neq \mathbb{Q}(\sqrt{d})$ de même, $\mathbb{Q}(\sqrt{dd'}) \neq \mathbb{Q}(\sqrt{d'})$.



Soit $N \subseteq M$ tel que $N/\mathbb{Q}$ soit quadratique. Par le **a)**, il existe $e \in \mathbb{Q}^* \setminus (\mathbb{Q}^*)^2$ tel que $N = \mathbb{Q}(\sqrt{e})$. On a alors $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{e}) \subseteq M$. On ne peut avoir $\sqrt{d} \in \mathbb{Q}(\sqrt{e})$ et $\sqrt{d'} \in \mathbb{Q}(\sqrt{e})$ car sinon on aurait $M = \mathbb{Q}(\sqrt{e})$.
Supposons $\sqrt{d} \notin \mathbb{Q}(\sqrt{e})$. On a lors $M = \mathbb{Q}(\sqrt{e})(\sqrt{d})$ et en particulier $\sqrt{d'} \in \mathbb{Q}(\sqrt{e})(\sqrt{d})$ et donc d' est un carré (non nul) dans $\mathbb{Q}(\sqrt{e})(\sqrt{d})$. Le **c.** implique alors $d' \in \mathbb{Q}(\sqrt{e})^2 \cup d\mathbb{Q}(\sqrt{e})^2$. Si d' appartient à $\mathbb{Q}(\sqrt{e})^2$ alors $\sqrt{d'} \in \mathbb{Q}(\sqrt{e})$ et alors $\mathbb{Q}(\sqrt{e}) = \mathbb{Q}(\sqrt{d'})$. Supposons donc $d' \in d\mathbb{Q}(\sqrt{e})^2$.
Il existe alors $a, b \in \mathbb{Q}$ tels qu'on ait

$$d' = d(a + b\sqrt{e})^2 = d(a^2 + b^2 e + 2ab\sqrt{e}) = (da^2 + edb^2) + 2abd\sqrt{e}.$$

De $d' \in \mathbb{Q}$ on obtient alors $2abd = 0$ puis $ab = 0$. Si on a $a = 0$ alors $d' = edb^2$ puis $dd' = ed^2b^2$ et donc $\sqrt{dd'} = bd\sqrt{e}$ il en suit $\mathbb{Q}(\sqrt{e}) = \mathbb{Q}(\sqrt{dd'})$. Si on a $b = 0$ alors $d' = da^2$ et donc $a^2 = d'/d$, ce qui est impossible par hypothèse sur d et d'.

iv. On pose $a = \sqrt{d}$ et $b = \sqrt{d'}$. La famille $\{1, a, b, ab\}$ est alors une base de M sur $\mathbb{Q}$. La matrice représentative de l'application m_{a+b} (multiplication par $\sqrt{d} + \sqrt{d'}$) est alors

$$\begin{bmatrix} 0 & d & d' & 0 \\ 1 & 0 & 0 & d' \\ 1 & 0 & 0 & d \\ 0 & 1 & 1 & 0 \end{bmatrix},$$

qui pour polynôme minimal $P = X^4 - 2(d + d')X^2 + (d - d')^2 = Q(X^2)$ avec $Q(X) = X^2 - 2(d + d')X + (d - d')^2$. Le discriminant de Q est

$$\begin{aligned} \Delta &= (-2(d + d'))^2 - 4(d - d')^2 = 4((d + d')^2 - (d - d')^2) \\ &= 4(d^2 + 2dd' + d'^2 - d^2 + 2dd' - d'^2) = 16dd'. \end{aligned}$$

On obtient alors $\sqrt{\Delta} = 4\sqrt{dd'}$ et les racines de Q sont

$$\begin{aligned} x_1 &= \frac{2(d + d') - 4\sqrt{dd'}}{2} = d + d' - 2\sqrt{dd'} \\ x_2 &= \frac{2(d + d') + 4\sqrt{dd'}}{2} = d + d' + 2\sqrt{dd'} \end{aligned}$$

Ainsi les racines de $P = \mathrm{Irr}(\sqrt{d} + \sqrt{d'}, \mathbb{Q})$ sont $\sqrt{x_1}, -\sqrt{x_1}, \sqrt{x_2}, -\sqrt{x_2}$. De $\sqrt{dd'} \notin \mathbb{Q}$ on obtient que P n'a pas de racines dans $\mathbb{Q}$. Supposons par l'absurde

$$P = (X^2 + aX + b)(X^2 + a'X + b') = X^4 + (a + a')X^3 + (aa' + b + b')X^2 + (ab' + a'b)X + bb',$$

on obtient alors le système

$$\begin{cases} a + a' & = 0 \\ aa' + b + b' & = -2(d + d') \\ ab' + a'b & = 0 \\ bb' & = (d - d')^2 \end{cases}$$

Ainsi on doit avoir $a = -a'$ puis $b - b' = 0$ et donc $b = b'$. On a donc $b = b' = \pm(d - d')$. Si $b = d - d'$ on a $aa' + b + b' = aa' + 2d - 2d' = -2d - 2d'$ et donc $aa' = 4d$ puis $a = \pm 2\sqrt{d}$ ce qui est impossible. De même si $b = d' - d$ on obtient $a = \pm 2\sqrt{d'}$ ce qui est aussi impossible. Le polynôme P étant irréductible, l'extension $\mathbb{Q}(\sqrt{d} + \sqrt{d'})/\mathbb{Q}$ est de degré 4 et on obtient $M = \mathbb{Q}(\sqrt{d} + \sqrt{d'})$.