# VALEURS PROPRES DE MATRICES SYMÉTRIQUES RATIONNELLES

G.BERHUY

Table des matières

1. Introduction . . . . . 1
2. Matrices compagnons . . . . . 5
3. La méthode générale . . . . . 6
4. Démonstration du théorème . . . . . 9
Annexe A. Démonstration du théorème des quatre carrés . . . . . 16
Annexe B. Tout ce qui vous a été caché... . . . . 17
Références . . . . . 22

## 1. Introduction

Cet article est une version abrégée de [1], et adaptée au niveau L2.

Le point de départ de cet article est le suivant. Soit $M \in \mathrm{M}_n(\mathbb{R})$ une matrice symétrique réelle. Le théorème spectral nous dit que toutes les valeurs propres de $M$ sont réelles et que $M$ est diagonalisable. Inversement, un réel arbitraire est valeur propre d'une matrice symétrique réelle, puisqu'il suffit de prendre une matrice diagonale appropriée.

Ainsi, l'ensemble des réels qui sont valeurs propres d'une matrice symétrique réelle est exactement $\mathbb{R}$, ce qui n'est pas un résultat très passionnant en soi. Néanmoins, pour corser un peu l'affaire, on peut se demander ce qu'il se passe si l'on remplace $\mathbb{R}$ par $\mathbb{Q}$.

Autrement dit, on peut se poser la question suivante : quels sont les nombres complexes $\alpha \in \mathbb{C}$ qui sont valeurs propres d'une matrice symétrique à coefficients rationnels ?

Pour donner un élément de réponse à cette question, notons qu'une matrice symétrique à coefficients rationnels peut se voir comme une matrice symétrique à coefficients réels. En particulier, elle est diagonalisable sur $\mathbb{R}$, et son polynôme minimal est donc scindé sur $\mathbb{R}$, sans racines multiples. Cela conduit à la définition suivante.

*Date*: 27 novembre 2021.

**Définition 1.1.** On dit qu'un nombre complexe $\alpha \in \mathbb{C}$ est *totalement réel* s'il existe un polynôme unitaire $f \in \mathbb{Q}[X]$ scindé sur $\mathbb{R}$ (i.e. dont toutes les racines sont réelles) sans racines multiples tel que $f(\alpha) = 0$.

**Exemple 1.2.** Si $d \in \mathbb{Q}$ est un rationnel strictement positif, $\sqrt{d}$ est totalement réel, puisqu'il est racine de $X^2 - d = (X - \sqrt{d})(X + \sqrt{d})$.

Les valeurs propres de matrices symétriques à coefficients dans $\mathbb{Q}$ sont donc à chercher parmi les nombres totalement réels.

La première question à se poser est de savoir si tout réel est totalement réel. Le résultat suivant, dont le lecteur pourra passer la démonstration sans que cela nuise à sa compréhension, montre que la réponse est négative.

**Proposition 1.3.** *Soit $d \in \mathbb{Q}$ un rationnel positif. On suppose que $d$ n'est pas le cube d'un rationnel. Alors, le réel $\alpha = \sqrt[3]{d}$ n'est pas totalement réel. en particulier, $\alpha$ n'est pas valeur propre d'une matrice symétrique à coefficients rationnels.*

*Démonstration.* Intéressons-nous aux polynômes de $\mathbb{Q}[X]$ s'annulant en $\alpha$. Soit $f \in \mathbb{Q}[X]$ tel que $f(\alpha) = 0$. Effectuons la division euclidienne de $f$ par $X^3 - d$, si bien que $f = (X^3 - d)Q + a_0 + a_1X + a_2X^2,\ a_i \in \mathbb{Q}$. En évaluant en $\alpha$, puisque $\alpha^3 = d$, on obtient

$$f(\alpha) = 0 = a_0 + a_1\alpha + a_2\alpha^2.$$

Nous allons démontrer par l'absurde que $a_0 = a_1 = a_2 = 0$.

Supposons tout d'abord que $a_2 \neq 0$. On a donc $\alpha^2 = u + v\alpha$, avec $u, v \in \mathbb{Q}$. En multipliant par $\alpha$, on obtient donc

$$d = \alpha^3 = u\alpha + v\alpha^2 = u\alpha + v(u + v\alpha) = uv + (u + v^2)\alpha.$$

Si $u + v^2 = 0$, on obtient $d = -v^3 = (-v)^3$, d'où une contradiction avec l'hypothèse sur $d$. Si $u + v^2 \neq 0$, on obtient que $\alpha \in \mathbb{Q}$. En élevant au cube, on obtient encore que $d$ est le cube d'un rationnel, d'où une contradiction.

Ainsi, $a_2 = 0$, et on a $a_0 + a_1\alpha = 0$. Si $a_1 \neq 0$, on obtient encore que $\alpha \in \mathbb{Q}$, et on conclut comme précédemment. Par conséquent, $a_1 = 0$, puis finalement $a_0 = 0$.

Il s'ensuit que $f = (X^3 - d)Q$. Mais alors, $j\alpha$ est une racine complexe non réelle de $f$, puisque $(j\alpha)^3 - d = j^3\alpha^3 = d - d = 0$.

Nous avons donc démontré que si $f \in \mathbb{Q}[X]$ annulait $\alpha$, alors $f$ possède une racine complexe non réelle. Ainsi, $\alpha$ n'est pas totalement réel, et ne peut donc être valeur propre d'une matrice symétrique à coefficients rationnels. □

**Notation.** Dans la suite, $\mathscr{S}_n(\mathbb{Q})$ désignera l'ensemble des matrices symétriques de $\mathrm{M}_n(\mathbb{Q})$.

Revenons à notre problème initial. La question soulevée précédemment est la suivante : tout nombre totalement réel est-il valeur propre d'une matrice symétrique à coefficients rationnels ?

Pour bien faire comprendre la difficulté de la question, commençons par étudier brièvement le cas de $\sqrt{d}$. Si $d$ est le carré d'un rationnel, $\sqrt{d}$ est

rationnel, et $\sqrt{d}$ est bien entendu valeur propre de la matrice $(\sqrt{d})$ de taille 1.

On suppose dorénavant que $d$ n'est pas le carré d'un rationnel. Pour essayer de déterminer si $\sqrt{d}$ est valeur propre d'une matrice symétrique à coefficients rationnels, on peut commencer par examiner le cas des matrices de taille 2.

Soit $M = \begin{pmatrix} u & v \\ v & w \end{pmatrix} \in \mathrm{M}_2(\mathbb{Q})$. Supposons que $\sqrt{d}$ soit valeur propre de $M$. Alors, la matrice réelle $M - \sqrt{d}I_2$ n'est pas inversible, donc est de déterminant nul. On a donc

$$(u - \sqrt{d})(w - \sqrt{d}) - v^2 = uw - v^2 + d - (u + w)\sqrt{d} = 0.$$

Si $u + w \neq 0$, on obtient $\sqrt{d} \in \mathbb{Q}$, puis que $d$ est le carré d'un rationnel, d'où une contradiction. Ainsi, $u + w = 0$, et donc $-u^2 - v^2 + d = 0$.

Ainsi, $d$ est somme de deux carrés dans $\mathbb{Q}$. Réciproquement, si $d = u^2 + v^2,\ u, v \in \mathbb{Q}$, alors il est facile de voir que le polynôme caractéristique de la matrice symétrique $\begin{pmatrix} u & -v \\ -v & -u \end{pmatrix}$ est $X^2 - d$, ce qui démontre que $\sqrt{d}$ est valeur propre d'une matrice de $\mathrm{M}_2(\mathbb{Q})$. On a donc démontré le résultat suivant.

**Proposition 1.4.** *Soit $d \in \mathbb{Q}$ un rationnel positif. On suppose que $d$ n'est pas le carré d'un rationnel.*

*Alors, $\sqrt{d}$ est valeur propre d'une matrice de $\mathscr{S}_2(\mathbb{Q})$ si, et seulement si, $d$ est une somme de deux carrés dans $\mathbb{Q}$.*

**Exemple 1.5.** Le résultat précédent montre que $\sqrt{3}$ n'est pas valeur propre d'une matrice de $\mathscr{S}_2(\mathbb{Q})$.

Il suffit en effet de se convaincre que 3 n'est pas somme de deux carrés dans $\mathbb{Q}$.

Supposons au contraire que $3 = u^2 + v^2,\ u, v \in \mathbb{Q}$. En réduisant au même dénominateur, et en multipliant par le carré d'un dénominateur commun, on obtient que $3c^2 = a^2 + b^2,\ a, b, c \in \mathbb{Z}, c \neq 0$. Si $a$ et $b$ sont tous deux divisibles par 3, alors $3^2 \mid 3c^2$. Mais alors, $3 \mid c^2$, puis $3 \mid c$ et enfin $3^2 \mid c$. Quitte à diviser $a, b, c$ par 3 suffisamment de fois, on peut donc supposer que $3 \nmid a$ par exemple. En réduisant modulo 3, on obtient $a^2 + b^2 \equiv 0\ [3]$.

Puisque $a$ n'est pas égal à 0 modulo 3, on a $a \equiv \pm 1\ [3]$, et ainsi $b^2 \equiv -1\ [3]$. Or, cette égalité ne peut avoir lieu, comme on le constate en remplaçant $b$ par $0, 1$ et 2.

L'exemple ci-dessus montre seulement que $\sqrt{3}$ n'est pas valeur propre d'une matrice de $\mathscr{S}_2(\mathbb{Q})$. Il n'exclut pas la possibilité que $\sqrt{3}$ soit racine d'une matrice de $\mathscr{S}_n(\mathbb{Q})$ avec $n > 2$. D'ailleurs, on peut vérifier que le polynôme caractéristique de la matrice $\begin{pmatrix} 0 & 1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ est égal à $X(X^2 - 3)$, ce qui démontre que $\sqrt{3}$ est valeur propre d'une matrice de $\mathscr{S}_3(\mathbb{Q})$.

Bref, ce n'est pas si simple...

Pour mettre tout de suite fin à ce suspense insoutenable, donnons tout de suite la réponse au problème initial : tout nombre totalement réel est effectivement valeur propre d'une matrice symétrique à coefficients rationnels. Pour énoncer un résultat plus précis, introduisons une définition commode.

**Définition 1.6.** Soit $\alpha \in \mathbb{C}$ un nombre totalement réel. Le *degré* de $\alpha$ est le degré minimal d'un polynôme de $\mathbb{Q}[X]$ non nul (non nécessairement scindé sur $\mathbb{R}$) annulant $\alpha$.

**Exemples 1.7.** Soit $\alpha$ un nombre totalement réel.

(1) $\alpha$ est de degré 1 si, et seulement si, $\alpha \in \mathbb{Q}$.

En effet, si $\alpha$ est de degré 1, il est annulé par un polynôme unitaire de degré 1 de $\mathbb{Q}[X]$. Ce polynôme est nécessairement $X - \alpha$, et ainsi $\alpha \in \mathbb{Q}$. La réciproque est claire.

(2) Soit $\alpha = \sqrt{d}$. Si $d$ n'est pas le carré d'un rationnel, alors $\alpha$ est de degré 2.

En effet, il est de degré $\leq 2$, puisque $X^2 - d \in \mathbb{Q}[X]$ annule $\alpha$, et il ne peut être de degré 1, puisque l'hypothèse sur $d$ entraîne que $\alpha$ n'est pas rationnel.

Dans cet article, nous démontrerons le résultat suivant.

**Théorème 1.8.** *Tout nombre totalement réel de degré $n \geq 1$ sur $\mathbb{Q}$ est valeur propre d'une matrice de $\mathscr{S}_{4n}(\mathbb{Q})$.*

**Remarque 1.9.** Le cas de $\sqrt{3}$ montre que ce résultat n'est pas optimal. Nous reviendrons sur ce point ultérieurement.

Le but de cet article est de donner une explication conceptuelle aux résultats précédents.

Nous allons en fait nous intéresser à un problème un tout petit peu différent, mais néanmoins lié : étant donné un polynôme unitaire $f \in \mathbb{Q}[X]$, à quelles conditions $f$ est-il le polynôme minimal d'une matrice symétrique à coefficients rationnels ?

Résoudre cette question nous permettra de répondre à la question initiale. En effet, rappelons que le polynôme minimal et le polynôme caractéristique d'une matrice ont mêmes racines. [1] En particulier, l'ensemble des valeurs propres des matrices symétriques à coefficients dans $\mathbb{Q}$ sont exactement l'ensemble des racines des polynômes minimaux de telles matrices.

Nous commençons nous intéresser à la question suivante, beaucoup plus simple : étant donné un corps $k$ et un polynôme unitaire $f \in k[X]$, peut-on trouver une matrice à coefficients dans $k$ (non nécessairement symétrique) de polynôme minimal $f$ ?

1. On peut en fait démontrer qu'ils ont mêmes facteurs irréductibles, mais nous n'en aurons pas besoin ici.

## 2. Matrices compagnons

Dans ce paragraphe, $k$ est un corps arbitraire. Nous commençons par définir notre objet d'étude.

**Définition 2.1.** Soit $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in k[X]$ un polynôme unitaire de degré $n \geq 1$. La *matrice compagnon associée à* $f$ est la matrice $C_f \in \mathrm{M}_n(k)$ définie par

$$C_f = \begin{pmatrix} 0 & 0 & & 0 & -a_0 \\ 1 & 0 & & & -a_1 \\ 0 & 1 & & & -a_2 \\ & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}.$$

Notons que si $n = 1$, on a simplement $C_f = (-a_0)$.

L'intérêt de cette matrice compagnon est donné par le résultat suivant.

**Lemme 2.2.** *Soit $f \in k[X]$ un polynôme unitaire de degré $n \geq 1$. Alors, le polynôme minimal et le polynôme caractéristique de $C_f \in \mathrm{M}_n(k)$ sont tous deux égaux à $f$.*

*Démonstration.* On commence par remarquer le fait suivant. Si $(\varepsilon_1, \ldots, \varepsilon_n)$ est la base canonique de $k^n$, alors

$$C_f\varepsilon_1 = \varepsilon_2, C_f\varepsilon_2 = \varepsilon_3, \ldots, C_f\varepsilon_{n-1} = \varepsilon_n,$$

ainsi que

$$C_f\varepsilon_n = -(a_0\varepsilon_1 + a_1\varepsilon_2 + \cdots + a_{n-1}\varepsilon_n).$$

En particulier, on a $C_f^{j-1}\varepsilon_1 = \varepsilon_j$ pour tout $j \in [\![1, n]\!]$, et

$$C_f^n\varepsilon_1 = C_f\varepsilon = -(a_0I_n + a_1C_f + \cdots + a_{n-1}C_f^{n-1})\varepsilon_1.$$

Cette dernière égalité se récrit $f(C_f)\varepsilon_1 = 0$. Mais alors, pour tout $j \in [\![1, n]\!]$, on a

$$f(C_f)\varepsilon_j = f(C_j)C_f^{j-1}\varepsilon_1 = C_f^{j-1}(f(C_f)\varepsilon_1) = 0.$$

Or, $f(C_f)\varepsilon_j$ est la $j$-ième colonne de $f(C_f)$. On en déduit donc que $f(C_f) = 0$. Ainsi, $f$ annule $C_f$. Il reste à se convaincre que $f$ est de degré minimal parmi les polynômes annulateurs de $C_f$.

Soit $P = b_{n-1}X^{n-1} + \cdots + b_1X + b_0 \in k[X]$ un polynôme de degré $\leq n-1$ annulant $C_f$. On a alors en particulier

$$P(C_f)\varepsilon_1 = 0 = b_{n-1}C_f^{n-1}\varepsilon_1 + \cdots + b_1C_f\varepsilon_1 + b_0\varepsilon_1 = b_{n-1}\varepsilon_n + \cdots + b_1\varepsilon_2 + b_0\varepsilon_1.$$

Comme $(\varepsilon_1, \ldots, \varepsilon_n)$ est une base de $k^n$, on en déduit que tous les $b_i$ sont nuls, c'est-à-dire $P = 0$.

Cela démontre qu'aucun polynôme non nul de degré $< n$ n'annule $C_f$. Ainsi, on a bien $\mu_{C_f} = f$. Mais alors, $\mu_{C_f}$ et $\chi_{C_f}$ sont tous deux unitaires de degré $n$. Comme $\mu_{C_f} \mid \chi_{C_f}$, on en déduit que $\chi_{C_f} = \mu_{C_f}$, d'où le résultat. □

## 3. La méthode générale

Nous allons maintenant expliquer la méthode générale que nous utiliserons dans la suite.

Rappelons tout d'abord une notation utile. Soit $k$ un corps arbitraire. Si $C \in \mathrm{M}_n(k)$, on pose

$$k[C] = \{P(C) \mid P \in k[X]\}.$$

Les propriétés des polynômes de matrices montrent que $k[C]$ est un sous-espace vectoriel de $\mathrm{M}_n(k)$, stable par produit, et que la restriction du produit matriciel est $k$-bilinéaire, associative et commutative. [2]

On a alors le lemme suivant.

**Lemme 3.1. ??** *Soit $k$ un corps, et soit $C \in \mathrm{M}_n(k)$. Soit $d$ le degré du polynôme minimal de $C$. Alors, la famille $(I_n, C, \ldots, C^{d-1})$ est une $k$-base de $k[C]$.*

*En particulier,* $\dim_k(k[C]) = \deg(\mu_C)$.

*Démonstration.* Soit $P \in k[X]$. Une division euclidienne de $P$ par $\mu_C$ donne l'existence d'un polynôme $Q \in k[X]$ et de scalaires $a_0, \ldots, a_{d-1}$ tels que

$$P = Q\mu_C + a_0 + a_1X + \ldots + a_{d-1}X^{d-1}.$$

En évaluant en $C$, on obtient $P(C) = a_0I_n + a_1M + \ldots + a_{d-1}C^{d-1}$, ce qui démontre que $(I_n, C, \ldots, \ldots, C^{d-1})$ engendre $k[C]$.

Il reste à voir que cette famille est libre. Soient $a_0, \ldots, a_{d-1} \in k$ tels que $a_0 + a_1C + \ldots + a_{d-1}C^{d-1}$. Alors, $R = a_{d-1}X^{d-1} + \ldots + a_1X + a_0$ est un polynôme annulateur de $M$, de degré $< d$. Par conséquent, $R = 0$, c'est-à-dire $a_0 = \cdots = a_{d-1} = 0$, ce qui fallait démontrer. □

L'idée qui va tout faire fonctionner est due à Bender [3] (cf. [2]), et part d'un constat très simple.

Soit $C \in M_n(k)$. Alors, pour tout $x \in k[C]$, l'application

$$\begin{array}{rccc} \ell_x \colon & k[C] & \longrightarrow & k[C] \\ & y & \longmapsto & xy \end{array}$$

est $k$-linéaire, et pour toute forme linéaire $s : k[C] \longrightarrow k$, on a

$$s(\ell_x(y_1)y_2) = s(xy_1y_2) = s(y_1(xy_2)) = s(y_1\ell_x(y_2)) \quad \text{pour tous } y_1, y_2 \in k[C].$$

Or, on a le résultat bien connu d'algèbre bilinéaire suivant.

**Lemme 3.2.** *Soit $b : V \times V \longrightarrow k$ une forme bilinéaire symétrique, où $V$ est un $k$-espace vectoriel de dimension finie. Supposons que $V$ possède une base $\mathscr{B} = (e_1, \ldots, e_m)$ $b$-orthonormée.*

*Soit $u \in \mathscr{L}(V)$ un endomorphisme vérifiant*

$$b(u(x), y) = b(x, u(y)) \quad \textit{pour tous } x, y \in V.$$

*Alors,* $\mathrm{Mat}(u; \mathscr{B}) \in \mathrm{M}_m(k)$ *est symétrique.*

2. Autrement dit, $k[C]$ est une sous-algèbre commutative de $\mathrm{M}_n(k)$.
3. Le mathématicien américain, pas le robot de Futurama !

*Démonstration.* Gardons les notations de l'énoncé. Pour tout $x \in V$, on note $[x]_{\mathscr{B}} \in k^m$ le vecteur des coordonnées de $x$ dans la base $\mathscr{B}$. Puisque $\mathscr{B}$ est $b$-orthonormée, on a

$$b(x,y) = [x]_{\mathscr{B}}^t [y]_{\mathscr{B}} \quad \text{pour tous } x, y \in V.$$

Soit $M = \mathrm{Mat}(u; \mathscr{B})$, et soient $x, y \in V$. On a

$$b(u(x), y) = [u(x)]_{\mathscr{B}}^t [y]_{\mathscr{B}} = (M[x]_{\mathscr{B}})^t [y]_{\mathscr{B}} = [x]_{\mathscr{B}}^t M^t [y]_{\mathscr{B}}$$

d'une part, ainsi que

$$b(x, u(y)) = [x]_{\mathscr{B}}^t [u(y)]_{\mathscr{B}} = [x]_{\mathscr{B}}^t M [y]_{\mathscr{B}}$$

d'autre part. On a donc

$$[x]_{\mathscr{B}}^t M^t [y]_{\mathscr{B}} = [x]_{\mathscr{B}}^t M [y]_{\mathscr{B}} \quad \text{pour tous } x, y \in V.$$

En remarquant que $[e_i]_{\mathscr{B}}$ est le $i$-ème vecteur de la base canonique de $k^n$, en appliquant cette égalité à $x = e_i$ et $y = e_j$ pour tous $i, j \in [\![1, m]\!]$, on en déduit que $M = M^t$, d'où le résultat souhaité. □

L'idée est donc de trouver une matrice $C \in \mathrm{M}_n(\mathbb{Q})$ et une forme linéaire $s : \mathbb{Q}[C] \longrightarrow \mathbb{Q}$ telles que $E$ possède une base orthonormée $\mathscr{B}$ pour la forme bilinéaire symétrique

$$\begin{array}{rccc} b_s \colon & \mathbb{Q}[C] \times \mathbb{Q}[C] & \longrightarrow & \mathbb{Q} \\ & (x, y) & \longmapsto & s(xy). \end{array}$$

Si de plus $\mathbb{Q}[C]$ contient un élément $x$ tel que le polynôme minimal de $\ell_x$ soit égal à $f$, alors $\mathrm{Mat}(\ell_x; \mathscr{B})$ sera une matrice symétrique de polynôme minimal $f$.

Un bon candidat pour $C$ est la matrice $C_f$. En effet, on a le lemme suivant.

**Lemme 3.3.** *Soit $k$ un corps arbitraire, et soit $f \in k[X]$ un polynôme unitaire de degré $n \geq 1$.*

*Alors, le polynôme minimal de $\ell_{C_f} \in \mathscr{L}(k[C_f])$ est $f$.*

*Démonstration.* On commence par constater que $\ell_{C_f}$ et $C_f$ ont même ensemble de polynômes annulateurs. En effet, de simples calculs montrent les deux propriétés suivantes :

(i) pour tout $x \in k[C_f]$, on a $\ell_x = 0$ si, et seulement si, $x = 0$ ;

(ii) pour tout $P \in k[X]$, on a $\ell_{P(x)} = P(\ell_x)$.

Pour tout $P \in k[X]$, on a alors

$$P(\ell_x) = 0 \iff \ell_{P(x)} = 0 \iff P(x) = 0,$$

ce qui démontre que $\ell_{C_f}$ et $C_f$ ont même polynôme minimal. On conclut alors en utilisant le lemme 2.2. □

**Notation.** Si $f \in k[X]$ est un polynôme unitaire de degré $n \geq 1$, on note $k[f] = k[C_f]$.

Résumons : si l'on trouve une $\mathbb{Q}$-forme linéaire $s : \mathbb{Q}[C_f] \longrightarrow \mathbb{Q}$ telle que $\mathbb{Q}[C_f]$ possède une $b_s$-orthonormée $\mathscr{B}$, alors la matrice $\mathrm{Mat}(\ell_{C_f}; \mathscr{B})$ sera symétrique, de polynôme minimal $f$.

Hélas, cela n'est pas possible en général. En effet, si l'on pouvait appliquer les considérations précédentes avec $f = X^2 - 3 \in \mathbb{Q}[X]$, on obtiendrait une matrice de $\mathscr{S}_2(\mathbb{Q})$ de polynôme minimal $X^2 - 3$. En particulier, $\sqrt{3}$ serait valeur propre d'une matrice de $\mathscr{S}_2(\mathbb{Q})$. Mais c'est impossible d'après l'exemple 1.5.

Néanmoins, on a le résultat suivant, que l'on énonce pour un corps arbitraire, étant donné que cela ne coûte pas plus cher.

**Proposition 3.4.** *Soit $k$ un corps arbitraire, et soit $f_1, \dots, f_r \in k[X]$ des polynômes unitaires de degrés respectifs $n_1, \dots, n_r \geq 1$. Enfin, soit $E = k[f_1] \times \cdots \times k[f_r]$. On suppose qu'il existe une forme linéaire $s : E \longrightarrow k$ telle que $E$ possède une base $\mathscr{B}$ qui est orthonormée pour la forme bilinéaire symétrique*

$$\begin{aligned} b_s \colon E \times E &\longrightarrow k \\ (x, y) &\longmapsto s(xy). \end{aligned}$$

*Si $x = (C_{f_1}, \dots, C_{f_r})$, la matrice $M = \mathrm{Mat}(\ell_x; \mathscr{B}) \in \mathrm{M}_n(k)$ est symétrique, de polynôme minimal $\mathrm{ppcm}(f_1, \dots, f_r)$, où $n = n_1 + \cdots + n_r$.*

*Démonstration.* Gardons les notations de l'énoncé. Des calculs similaires à ceux faits précédemment montrent que l'on a

$$b_s(\ell_x(y_1), y_2) = b_s(y_1, \ell_x(y_2)) \quad \text{pour tous } y_1, y_2 \in E.$$

Le lemme 3.2 montre alors que la matrice $M$ est symétrique. Il reste à calculer le polynôme minimal de $\ell_x$. Pour déterminer ce dernier, remarquons que pour tout $P \in k[X]$, on a

$$\begin{aligned} P(\ell_x) = (P(\ell_{C_{f_1}}), \dots, P(\ell_{C_{f_r}})) = 0 \quad &\iff \quad P(\ell_{C_{f_j}}) = 0 \ \text{ pour tout } j \in [\![1, r]\!] \\ &\iff \quad f_j \mid P \text{ pour tout } j \in [\![1, r]\!] \\ &\iff \quad \mathrm{ppcm}(f_1, \dots, f_r) \mid P, \end{aligned}$$

la deuxième équivalence découlant du fait que le polynôme minimal de $C_{f_i}$ est $f_i$ d'après le lemme 3.3.

Ainsi, les polynômes annulateurs de $\ell_x$ sont exactement les multiples du ppcm de $f_1, \dots, f_r$. Comme ce dernier est bien unitaire et de degré minimal parmi les polynômes annulateurs non nuls, ceci achève la démonstration. □

Dans la suite, nous appliquerons la proposition précédente avec $E = \mathbb{Q}[f]^4$ et $x = (C_f, \dots, C_f)$.

Finissons ce paragraphe par quelques remarques calculatoires.

**Remarque 3.5.** Soit $k$ un corps arbitraire. On commence par remarquer le fait suivant. Soit $\mathscr{B}_0 = (I_2, C_f, \dots, C_f^{n-1})$, alors $\mathrm{Mat}(\ell_{C_f}; \mathscr{B}_0) = C_f$.

En effet, pour tout $j \in [\![0, n-2]\!]$, on a

$$\ell_{C_f}(C_f^j) = C_f^{j+1}.$$

De plus, si $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X = a_0$, on a $f(C_f) = 0$, puisque $f$ annule $C_f$, et ainsi

$$\ell_{C_f}(C_f^{n-1}) = C_f^n = -a_0 I_n - a_1 C_f - \cdots - a_{n-1} C_f^{n-1}.$$

Par conséquent, on a

$$\mathrm{Mat}(\ell_{C_f};\mathscr{B}_0)=\begin{pmatrix}0&0&&0&-a_0\\1&0&&&-a_1\\0&1&&&-a_2\\&&\ddots&&\vdots\\0&0&\cdots&1&-a_{n-1}\end{pmatrix}=C_f.$$

Reprenons maintenant les notations de la proposition 3.4. Alors la famille

$$\mathscr{E}=((I_{n_1},0,\dots,0),\dots,(C_{f_1}^{n_1-1},0,\dots,0),\dots,(0,\dots,0,I_{n_r}),\dots,(0,\dots,0,C_{f_r}^{n_r-1}))$$

est une base de $E$, et on a

$$\mathrm{Mat}(\ell_x;\mathscr{E})=\begin{pmatrix}C_{f_1}&&\\&\ddots&\\&&C_{f_r}\end{pmatrix}$$

Si $P$ est la matrice des vecteurs de $\mathscr{B}$ dans la base $\mathscr{E}$, une matrice symétrique de $\mathrm{M}_n(k)$ de polynôme minimal $\mathrm{ppcm}(f_1,\dots,f_r)$ est donc

$$M=\mathrm{Mat}(\ell_x;\mathscr{B})=P^{-1}\begin{pmatrix}C_{f_1}&&\\&\ddots&\\&&C_{f_r}\end{pmatrix}P.$$

## 4. Démonstration du théorème

Nous commençons par énoncer les résultats principaux que nous démontrerons dans ce paragraphe (cf. [3]).

**Théorème 4.1.** *Soit $f\in\mathbb{Q}[X]$ un polynôme unitaire de degré $n\geq 1$ scindé sur $\mathbb{R}$ sans racines multiples. Alors, $f$ est le polynôme minimal d'une matrice de $\mathscr{S}_{4n}(\mathbb{Q})$.*

**Corollaire 4.2.** *Soit $\alpha$ un nombre totalement réel de degré $n\geq 1$. Alors, $\alpha$ est valeur propre d'une matrice de $\mathscr{S}_{4n}(\mathbb{Q})$.*

**Remarque 4.3.** Notons que c'est Krakowski qui a démontré le premier qu'un nombre totalement réel est valeur propre d'une matrice symétrique à coefficients rationnels (cf. [5]). Néanmoins, la taille de la matrice en question est exponentielle par rapport au degré du nombre considéré. Le corollaire précédent est donc bien meilleur, et on peut encore faire mieux, comme on le verra plus loin.

La démonstration du théorème 4.1 s'appuiera sur le théorème des quatre carrés, que l'on énonce seulement dans le cas rationnel, et dont nous reléguons la démonstration à la fin de cet article (cf. Annexe A).

**Théorème 4.4.** *Tout entier rationnel positif est somme de quatre carrés de rationnels.*

Nous allons en déduire le résultat d'algèbre bilinéaire suivant.

**Théorème 4.5.** *Soit $b : V \times V \longrightarrow \mathbb{Q}$ une forme bilinéaire symétrique, où $V$ est un $\mathbb{Q}$-espace vectoriel de dimension finie. On suppose que $b(x,x) > 0$ pour tout $x \in V$ non nul.*

*Alors, $V^4$ possède une base orthonormée pour la forme bilinéaire symétrique*

$$\begin{aligned} \theta_b : \quad V^4 \times V^4 &\longrightarrow \mathbb{Q} \\ ((x_1,x_2,x_3,x_4),(y_1,y_2,y_3,y_4)) &\longmapsto \sum_{i=1}^{4} b(x_i,y_i). \end{aligned}$$

*Démonstration.* Soit $(e_1,\dots,e_n)$ une base $b$-orthogonale de $V$ fixée, et soit $r_i = b(e_i,e_i)$. Il est alors facile de voir que la famille

$$\mathscr{B} = ((e_1,0,0,0),(0,e_1,0,0),(0,0,e_1,0),(0,0,0,e_1),\dots,(0,0,0,e_n))$$

est une base $\theta$-orthogonale de $V^4$, et que la matrice représentative de $\theta_b$ dans cette base est

$$M = \begin{pmatrix} r_1 I_4 & & \\ & \ddots & \\ & & r_n I_4 \end{pmatrix}.$$

Nous allons exhiber une matrice $P \in \mathrm{GL}_{4n}(\mathbb{Q})$ inversible telle que $P^t M P = I_{4n}$. Cela suffira à démontrer le théorème. En effet, si $\mathscr{B}' = (f_1,\dots,f_{4n})$ est la base dont la matrice des vecteurs coordonnées dans la base $\mathscr{B}$ est $P$, alors la formule de changement de base pour les matrices représentatives de formes bilinéaires montre que $\mathrm{Mat}(\theta_b,\mathscr{B}') = P^t M P = I_{4n}$, ce qui démontre que $\mathscr{B}'$ est $\theta_b$-orthonormée.

Il suffit en fait de montrer que pour tout rationnel $r > 0$, il existe $Q \in \mathrm{GL}_4(\mathbb{Q})$ telle que $rQ^tQ = I_4$. En effet, par hypothèse sur $b$, chaque $r_i$ est $> 0$. Si $Q_i \in \mathrm{GL}_4(\mathbb{Q})$ vérifie $r_i Q_i^t Q_i = I_4$, il est alors aisé de voir que la matrice $P = \begin{pmatrix} P_1 & & \\ & \ddots & \\ & & P_n \end{pmatrix}$ convient.

Soit donc $r > 0$ un rationnel strictement positif. D'après le théorème 4.4, il existe $a,b,c,d \in \mathbb{Q}$ tels que $r = a^2+b^2+c^2+d^2$.

Supposons tout d'abord que $c^2+d^2 = 0$, i.e. $r = a^2+b^2$. On vérifie alors que la matrice

$$Q = \frac{1}{r}\begin{pmatrix} a & b & 0 & 0 \\ b & -a & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & b & -a \end{pmatrix}$$

satisfait $rQ^tQ = I_4$. Supposons maintenant que $c^2+d^2 \neq 0$. Cette fois, on vérifie que la matrice

$$Q = \frac{1}{r}\begin{pmatrix} a & b & c & d \\ b & -a & d & -c \\ c & d & \dfrac{-ac^2+ad^2-2bcd}{c^2+d^2} & \dfrac{-2acd+bc^2-bd^2}{c^2+d^2} \\ d & -c & \dfrac{-2acd+bc^2-bd^2}{c^2+d^2} & \dfrac{ac^2-ad^2+2bcd}{c^2+d^2} \end{pmatrix}$$

satisfait $rQ^tQ = I_4$. Ceci achève la démonstration. □

L'idée est donc d'appliquer le théorème 4.5 à une forme bilinéaire $b$ bien choisie. Supposons un instant que nous ayons à disposition une forme linéaire $t : \mathbb{Q}[f] \longrightarrow \mathbb{Q}$ telle que $b_t(x,x) = t(x^2) > 0$ pour tout $x \in \mathbb{Q}[f]$ non nul, et soit $s : \mathbb{Q}[f]^4 \longrightarrow \mathbb{Q}$ la forme linéaire définie par

$$s((x_1,x_2,x_3,x_4)) = \sum_{i=1}^{4} t(x_i).$$

Alors, la forme bilinéaire $b_s$ est exactement la forme bilinéaire $\theta_{b_t}$. En effet, pour tous $(x_1,x_2,x_3,x_4),(y_1,y_2,y_3,y_4) \in \mathbb{Q}[f]^4$, on a

$$\begin{aligned} b_s((x_1,x_2,x_3,x_4),(y_1,y_2,y_3,y_4)) &= s((x_1,x_2,x_3,x_4)(y_1,y_2,y_3,y_4)) \\ &= s((x_1y_1,x_2y_2,x_3y_3,x_4,y_4)) \\ &= \sum_{i=1}^{4} t(x_iy_i) \\ &= \sum_{i=1}^{4} b_t(x_i,y_i) \\ &= \theta_{b_t}((x_1,x_2,x_3,x_4),(y_1,y_2,y_3,y_4)). \end{aligned}$$

Mais alors, le théorème 4.5 montre que $\mathbb{Q}[f]^4$ possède une base $b_s$-orthonormée. Une application de la proposition 3.4 à $E = \mathbb{Q}[f]^4$ et $x = (C_f,\dots,C_f)$ montre alors que $f$ est le polynôme minimal d'une matrice symétrique de $\mathrm{M}_{4n}(\mathbb{Q})$.

Il reste donc à exhiber une forme linéaire $t : \mathbb{Q}[f] \longrightarrow \mathbb{Q}$ telle que $t(x^2) > 0$ pour tout $x \in \mathbb{Q}[f]$ non nul, ce qui est le but du lemme suivant.

**Lemme 4.6.** *Soit $f \in \mathbb{Q}[X]$ un polynôme unitaire de degré $n \geq 1$ scindé sur $\mathbb{R}$ sans racines multiples. Alors, la forme linéaire*

$$\begin{array}{rcl} t\colon \mathbb{Q}[f] & \longrightarrow & \mathbb{Q} \\ x & \longmapsto & \mathrm{tr}(x) \end{array}$$

*vérifie $t(x^2) > 0$ pour tout $x \in \mathbb{Q}[f]$ non nul.*

*Démonstration.* Rappelons que $(I_n, C_f, \dots, C_f^{n-1})$ est une $\mathbb{Q}$-base de $\mathbb{Q}[f]$. En particulier, un élément $x \in \mathbb{Q}[f]$ s'écrit sous la forme $x = P(C_f)$, où $P \in \mathbb{Q}[X]$ est un polynôme de degré $\leq n-1$.

Comme $f$ est le polynôme minimal de $C_f$ d'après le lemme 2.2, et que $f$ est scindé sur $\mathbb{R}$ sans racines multiples, $C_f$ est diagonalisable sur $\mathbb{R}$. Ainsi, il existe $Q \in \mathrm{GL}_n(\mathbb{R})$ telle que

$$C_f = Q^{-1} \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_n \end{pmatrix} Q,$$

où $\alpha_1, \dots, \alpha_n \in \mathbb{R}$ sont les racines de $f$. Mais alors, on a

$$x^2 = Q^{-1} \begin{pmatrix} P(\alpha_1)^2 & & \\ & \ddots & \\ & & P(\alpha_n)^2 \end{pmatrix} Q,$$

et par conséquent,

$$t(x^2) = \sum_{j=1}^{n} P(\alpha_i)^2 \geq 0.$$

Soit maintenant $x \in \mathbb{Q}[f]$ tel que $t(x^2) = 0$, et montrons que $x = 0$. Si $x = P(C_f)$, avec $\deg(P) \leq n-1$, et si $t(x^2) = 0$, on a donc

$$P(\alpha_1) = \cdots = P(\alpha_n) = 0.$$

Comme $\alpha_1, \dots, \alpha_n$ sont des réels deux à deux distincts par hypothèse sur $f$, $P$ est un polynôme de degré $\leq n-1$ possédant au moins $n$ racines distinctes. Par conséquent, $P = 0$, et donc $x = 0$. □

Nous avons donc établi le théorème 4.1.

Soit $\alpha$ un nombre totalement réel. Pour pouvoir appliquer le théorème 4.1 afin d'en déduire le corollaire 4.2, il faut se convaincre qu'un polynôme $f \in \mathbb{Q}[X]$ unitaire scindé sur $\mathbb{R}$ de degré minimal annulant $\alpha$ est nécessairement sans racines multiples. Ce n'est pas si évident a priori, puisque pour calculer le degré d'un nombre algébrique $\alpha$, on doit considérer **tous** les polynômes de $\mathbb{Q}[X]$ annulant $\alpha$, y compris ceux qui ont des racines multiples.

Le lemme suivant montre que c'est bien le cas.

**Lemme 4.7.** *Soit $\alpha$ est un nombre totalement réel, et soit $f \in \mathbb{Q}[X]$ un polynôme unitaire scindé sur $\mathbb{R}$ annulant $\alpha$.*

*Alors, $g = \dfrac{f}{\operatorname{pcgd}(f, f')} \in \mathbb{Q}[X]$ est un polynôme unitaire scindé sur $\mathbb{R}$ sans racines multiples, annulant $\alpha$.*

*En particulier, un polynôme $f \in \mathbb{Q}[X]$ unitaire scindé sur $\mathbb{R}$ annulant $\alpha$ de degré minimal est nécessairement sans racines multiples.*

*Démonstration.* Écrivons $f = (X-\alpha_1)^{m_1} \cdots (X-\alpha_r)^{m_r}$, où $r \geq 1, \alpha_1, \dots, \alpha_r \in \mathbb{R}$ sont des réels deux à deux distincts, et $m_1, \dots, m_r \geq 1$.

Notons tout d'abord que le pgcd de $f$ et $f'$, que l'on voie ces polynômes comme des éléments de $\mathbb{Q}[X]$ ou de $\mathbb{R}[X]$, est le même, puisque les divisions euclidiennes utilisées dans l'algorithme d'Euclide sont les mêmes. De plus, $g$ est bien un polynôme de $\mathbb{Q}[X]$, comme quotient de deux polynômes de $\mathbb{Q}[X]$.

Fixons $i \in [\![1, r]\!]$. On a donc $f = (X - \alpha_i)^{m_i} h_i$, avec $h_i(\alpha_i) \neq 0$. Mais alors, on a

$$f' = m_i(X - \alpha_i)^{m_i - 1} h_i + (X - \alpha_i)^{m_i} h_i' = (X - m_i)^{m_i - 1} \tilde{h}_i,$$

avec $\tilde{h}_i = m_i h_i + (X - \alpha_i) h_i'$. Or, $\tilde{h}_i(\alpha_i) = m_i h_i(\alpha_i) \neq 0$, car $m_i \geq 1$ et $h_i(\alpha_i) \neq 0$.

Ainsi, si $(X-\alpha_i)^{m_i}$ divise exactement $f$ dans $\mathbb{R}[X]$, alors $(X-\alpha_i)^{m_i-1}$ divise exactement $f'$. On a donc $\mathrm{pgcd}(f,f') = (X-\alpha_1)^{m_1-1}\cdots(X-\alpha_r)^{m_r-1}$, et donc

$$g = (X-\alpha_1)\cdots(X-\alpha_r).$$

Remarquons à présent que si $f$ a une racine multiple, on a $\deg(g) < \deg(f)$. Par conséquent, un polynôme $f \in \mathbb{Q}[X]$ unitaire scindé sur $\mathbb{R}$ annulant $\alpha$ de degré minimal est nécessairement sans racines multiples, car sinon $g$ serait tel polynôme de degré strictement plus petit. Ceci achève la démonstration. □

**Remarque 4.8.** Ce lemme montre qu'un nombre complexe est totalement réel si, et seulement si, il est annulé par un polynôme unitaire $f \in \mathbb{Q}[X]$ scindé sur $\mathbb{R}$.

Autrement dit, on peut se passer de l'hypothèse « sans racines multiples » dans la définition 1.1.

Le corollaire 4.2 se déduit alors du théorème 4.1, appliqué à un polynôme $f \in \mathbb{Q}[X]$ unitaire scindé sur $\mathbb{R}$ annulant $\alpha$ de degré minimal, qui est scindé sur $\mathbb{R}$ et sans racines multiples d'après le lemme 4.7.

Ce résultat est très loin d'être optimal. Si $d \in \mathbb{Q}$ est une somme de deux carrés de rationnels, mais pas le carré d'un rationnel, alors $\sqrt{d}$ est totalement réel de degré 2 sur $\mathbb{Q}$ d'après l'exemple 1.7 (2). Le corollaire 4.2 montre alors que $\sqrt{d}$ est valeur propre d'une matrice de $\mathscr{S}_8(\mathbb{Q})$. Néanmoins, comme $d$ est somme de deux carrés, la proposition 1.4 montre que $\sqrt{d}$ est valeur propre d'une matrice de $\mathscr{S}_2(\mathbb{Q})$.

Le même phénomène se produit pour $\sqrt{3}$. Le corollaire 4.2 fournit l'existence d'une matrice de $\mathscr{S}_8(\mathbb{Q})$ dont $\sqrt{3}$ est valeur propre, alors que l'introduction fournit une matrice de $\mathscr{S}_3(\mathbb{Q})$ dont $\sqrt{3}$ est valeur propre. Notons au passage que ce dernier résultat est optimal pour $\sqrt{3}$, puisque $\sqrt{3}$ n'est pas valeur propre d'une matrice de $\mathscr{S}_2(\mathbb{Q})$.

En fait, nous avons le théorème quasi-optimal suivant, dont la démonstration est extrêmement difficile et utilise des outils très sophistiqués (cf. [2]).

**Théorème 4.9** (Bender)**.** *Soit $\alpha$ un nombre totalement réel de degré $n \geq 1$ sur $\mathbb{Q}$.*

(1) *Si $n$ est impair, $\alpha$ est valeur propre d'une matrice de $\mathscr{S}_n(\mathbb{Q})$.*

(2) *Si $n$ est pair, $\alpha$ est valeur propre d'une matrice de $\mathscr{S}_{n+1}(\mathbb{Q})$.*

**Remarque 4.10.** À l'heure actuelle, on ne sait pas caractériser les nombres totalement réels de degré $n$ pair qui ne sont pas valeur propre d'une matrice de $\mathscr{S}_n(\mathbb{Q})$.

Nous nous proposons maintenant de retrouver les résultats de l'introduction en utilisant le point de vue exposé dans cet article.

Soit $d = u^2 + v^2$. On suppose que $d$ n'est pas le carré d'un rationnel, si bien que l'on peut supposer que $v \neq 0$. Soit $f = X^2 - d$, et soit $s : \mathbb{Q}[f] \longrightarrow \mathbb{Q}$

l'unique forme linéaire telle que

$$s(I_2) = 1 \text{ et } s(C_f) = u.$$

Il est alors facile de voir que la famille $\mathscr{B} = (I_2, v^{-1}(uI_2 - C_f))$ est une base $b_s$-orthonormée de $\mathbb{Q}[f]$. La matrice de changement de base est donc $P = \begin{pmatrix} 1 & v^{-1}u \\ 0 & -v^{-1} \end{pmatrix}$. La remarque 3.5 montre alors que

$$\mathrm{Mat}(\ell_{C_f}; \mathscr{B}) = P^{-1}C_f P = \begin{pmatrix} u & v^{-1}(u^2 - d) \\ -v & -u \end{pmatrix},$$

et puisque $d = u^2 + v^2$, on a $\mathrm{Mat}(\ell_{C_f}; \mathscr{B}) = \begin{pmatrix} u & -v \\ -v & -u \end{pmatrix}$, qui est la matrice donnée dans l'introduction.

Nous allons maintenant expliquer comme nous avons obtenu la matrice de $\mathscr{S}_3(\mathbb{Q})$ de polynôme caractéristique égal à $X(X^2 - 3)$. Soit $f = X^2 - 3$. Reprenons la forme linéaire $t : \mathbb{Q}[f] \longrightarrow \mathbb{Q}$ du lemme 4.6. De simples calculs montrent que l'on a

$$\mathrm{Mat}(b_t; \mathscr{B}_0) = \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix}.$$

Notons maintenant que, si $b : V \times V \longrightarrow k$ est une forme bilinéaire symétrique, et si $V$ possède une une base $b$-orthonormée, alors le déterminant de n'importe quelle matrice représentative de $b$ est un carré d'un élément non nul de $k$. En effet, si $\mathscr{B}$ est une base $b$-orthonormée, on a $\mathrm{Mat}(b; \mathscr{B}) = I_n$. Si maintenant $\mathscr{B}'$ est une base arbitraire de $V$, et si $P$ est la matrice des vecteurs de $\mathscr{B}'$ dans la base $\mathscr{B}$, on a $\mathrm{Mat}(b; \mathscr{B}') = P^t P$, qui est de déterminant $\det(P)^2$.

L'idée sous-jacente est donc de compléter la matrice précédente en une matrice symétrique $3 \times 3$ dont le déterminant est un carré, et espérer que la forme bilinéaire symétrique qu'elle représente admette une base orthonormée. Pour concrétiser cette idée fort vague, nous allons utiliser la proposition 3.4, avec $r = 2, f_1 = X$ et $f_2 = f = X^2 - 3$. Notons que $\mathbb{Q}[C_X]$ n'est rien d'autre que $\mathbb{Q}$ (car c'est un $\mathbb{Q}$-espace vectoriel de dimension 1).

Pour appliquer cette proposition, il faut donc trouver une forme linéaire $s : \mathbb{Q} \times \mathbb{Q}[f] \longrightarrow \mathbb{Q}$ appropriée. Afin de poursuivre l'idée précédente, il semble donc tout indiqué de poser

$$s((r, x)) = 3r + t(x) = 3r + \mathrm{tr}(x) \text{ pour tout } (r, x) \in \mathbb{Q} \times \mathbb{Q}[f].$$

En effet, si on prend la base $\mathscr{E}$ de la remarque 3.5, on voit facilement que l'on a

$$B = \mathrm{Mat}(b_s; \mathscr{E}) = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix},$$

qui est de déterminant $6^2$.

Pour alléger un peu la rédaction, nous allons maintenant introduire une notation commode.

Si $k$ est un corps, $M_1, M_2 \in \mathrm{M}_n(k)$, et si $P \in \mathrm{GL}_n(k)$, on note $M_1 \underset{P}{\sim} M_2$ si $P^t M_1 P = M_2$.

Afin de pouvoir faire les calculs, on va utiliser l'identité suivante. Si $d \in \mathbb{Q}$, et si $r = a^2 + db^2$, on a

$$\begin{pmatrix} r & 0 \\ 0 & rd \end{pmatrix} \underset{Q}{\sim} \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}, \text{ avec } Q = r^{-1} \begin{pmatrix} a & db \\ b & -a \end{pmatrix}.$$

On a alors successivement :

(1) $B \underset{P_1}{\sim} B_2 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 6 \end{pmatrix}$, avec $P_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

(2) $B_2 \underset{P_2}{\sim} B_3 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$, avec $P_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & \frac{2}{3} \\ 0 & \frac{1}{3} & -\frac{1}{3} \end{pmatrix}$

(3) $B_3 \underset{P_1}{\sim} B_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$

(4) $B_4 \underset{P_3}{\sim} I_3$, avec $P_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} \end{pmatrix}$

En recollant les morceaux, on a donc $P^t M P = I_3$, avec

$$P = P_1 P_2 P_1 P_3 = \frac{1}{6} \begin{pmatrix} 2 & 2 & -2 \\ 0 & 3 & 3 \\ 2 & -1 & 1 \end{pmatrix}.$$

La matrice $P$ est alors la matrice des vecteurs d'une base $\mathscr{B}$ dans la base $\mathscr{E}$, et c'est la base $b_s$-orthonormée recherchée.

La remarque 3.5 montre alors qu'une matrice symétrique de polynôme minimal $\mathrm{ppcm}(X, X^2 - 3) = X(X^2 - 3)$ est donnée par

$$M = P^{-1} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 3 \\ 0 & 1 & 0 \end{pmatrix} P = \begin{pmatrix} 0 & 1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

**Remarque 4.11.** Les diverses démonstrations et calculs qui précèdent peuvent paraître un peu miraculeux. En particulier, le théorème 4.5 et sa démonstration peuvent sembler un peu sortis de nulle part aux yeux d'un lecteur non-spécialiste d'algèbre bilinéaire, et ce, à juste titre.

Cet état de fait découle directement du parti pris que nous avons choisi, à savoir essayer de limiter l'introduction de nouveaux concepts au strict minimum, et de ne pas dépasser le niveau L2 dans l'exposition. Néanmoins, pour le lecteur curieux de comprendre un peu plus en profondeur, nous révélons tout ce qui a été caché soigneusement sous le tapis dans l'annexe B.

## Annexe A. Démonstration du théorème des quatre carrés

Nous démontrons ici la version rationnelle du théorème des quatre carrés de Lagrange (cf. théorème 4.4), à savoir que tout rationnel positif est somme de quatre carrés de rationnels.

Notons tout d'abord qu'il suffit de démontrer ce résultat dans le cas des entiers positifs. En effet, supposons que cela soit le cas, et soit $x \in \mathbb{Q}$ un rationnel positif. On peut alors toujours écrire $x = \dfrac{a}{b}$, où $a, b$ sont des entiers positifs et $b$ est non nul. Mais alors, $ab = u_1^2 + u_2^2 + u_3^2 + u_4^2,\ u_i \in \mathbb{Q}$, et on a

$$x = \frac{ab}{b^2} = \frac{u_1^2 + u_2^2 + u_3^2 + u_4^2}{b^2} = x_1^2 + x_2^2 + x_3^2 + x_4^2,$$

avec $x_i = b^{-1}u_i$.

Il suffit donc de démontrer que tout entier $n \geq 0$ est somme de quatre carrés de rationnels. Les cas de 0 et 1 étant triviaux, on peut toujours supposer $n \geq 2$.

Nous utiliserons plusieurs fois, l'identité suivante (due à Euler), un peu effrayante au fond [4], mais qui se démontre aisément en développant tout :

$$\begin{array}{rcl}(x_1^2+y_1^2+z_1^2+t_1^2)(x_2^2+y_2^2+z_2^2+t_2^2) & = & (x_1x_2+y_1y_2+z_1z_2+t_1t_2)^2+(x_1y_2-y_1x_2+t_1z_2-z_1t_2)^2 \\ & + & (x_1z_2-z_1x_2+y_1t_2-t_1y_2)^2+(x_1t_2-t_1x_2+z_1y_2-y_1z_2)^2.\end{array}$$

pour tous $x_1, x_2, y_1, y_2, z_1, z_2, t_1, t_2 \in \mathbb{Q}$.

Autrement dit, un produit de deux sommes de quatre carrés de rationnels est encore une somme de quatre carrés de rationnels.

On suppose maintenant que l'ensemble des entiers $n \geq 2$ qui ne s'écrivent pas comme somme de quatre carrés de rationnels est non vide, et soit $p$ le plus petit élément de cet ensemble. Alors, $p$ est premier. Sinon, on aurait $p = n_1n_2$, avec $2 \leq n_1, n_2 \leq p-1$. Par minimalité de $p$, $n_1$ et $n_2$ sont des sommes de quatre carrés de rationnels, et il est en alors de même de $p$ d'après l'identité d'Euler. Remarquons aussi que $p$ est impair, puisque $2 = 1^2 + 1^2 + 0^2 + 0^2$.

On commence par établir le fait suivant.

**Fait.** Pour tout nombre premier impair $p$, il existe des entiers $a, b \geq 0$ et un entier $n \in [\![1, p-1]\!]$ tels que $np = 1 + a^2 + b^2$.

*Démonstration du fait.* Remarquons que pour tous $x, y \in \left[\!\left[0, \frac{p-1}{2}\right]\!\right]$, on a

$$x^2 \equiv y^2\ [p] \Longrightarrow x = y.$$

En effet, si $x^2 \equiv y^2\ [p]$, alors $(x-y)(x+y) \equiv 0\ [p]$, soit $p \mid (x-y)(x+y)$. Comme $p$ est premier, $p \mid (x-y)$ ou $p \mid (x+y)$. Mais, on a

$$|x \pm y| \leq |x| + |y| \leq p - 1 < p.$$

Ainsi, $x \pm y$ est un multiple de $p$ strictement compris entre $-p$ et $p$, c'est-à-dire 0. On a donc soit $x = y$, soit $x = -y$. Comme $x, y \geq 0$, le second cas implique $x = 0 = y$. Bref, dans les deux cas, $x = y$.

4. Ce qui nous fait dire que le fond d'Euler effraie...

Les $\dfrac{p+1}{2}$ entiers $a^2$, $a \in \left[\!\left[0, \frac{p-1}{2}\right]\!\right]$ sont donc deux à deux non congrus modulo $p$. De même, les $\dfrac{p+1}{2}$ entiers $-b^2-1$, $b \in \left[\!\left[0, \frac{p-1}{2}\right]\!\right]$ sont deux à deux non congrus modulo $p$. Par le principe des tiroirs, il existe donc $a, b \in \left[\!\left[0, \frac{p-1}{2}\right]\!\right]$ tels que $a^2$ et $-b^2-1$ sont congrus modulo $p$, c'est-à-dire pour lesquels $a^2+b^2+1 = np$, avec $n \in \mathbb{Z}$. Notons que $1 \leq np \leq \dfrac{(p-1)^2}{2}+1 < p^2$, et donc que $n \in [\![1, p-1]\!]$.

Passons maintenant à la démonstration proprement dite. Le fait précédent montre en particulier l'ensemble des entiers $n \in [\![1, p-1]\!]$ tels que $np$ est somme de quatre carrés d'entiers est non vide. Si $n = 1$, on a une contradiction, puisque $p$ n'est pas somme de quatre carrés de rationnels. Ainsi, $n \geq 2$. Comme $n < p$, $n$ est donc somme de quatre carrés de rationnels par minimalité de $p$. Mais alors, $n^2 p = n(np)$ est somme de quatre carrés de rationnels d'après l'identité d'Euler, et il en est de même de $p = (n^2)^{-1}(n^2 p)$, d'où encore une contradiction avec le choix de $p$.

Ceci achève la démonstration.

## Annexe B. Tout ce qui vous a été caché...

Le but de cette annexe est donner un point de vue plus conceptuel, mais plus éclairant, des démonstrations présentes dans cet article.

La première notion à introduire est la notion d'isomorphisme entre formes bilinéaires.

**Définition B.1.** Soit $k$ un corps. Deux formes bilinéaires $b_1 : V_1 \times V_1 \longrightarrow k$ et $b_2 : V_2 \times V_2 \longrightarrow k$ sont dites *isomorphes* s'il existe un isomorphisme d'espaces vectoriels $u : V_1 \xrightarrow{\sim} V_2$ tel que

$$b_2(u(x), u(y)) = b_1(x, y) \quad \text{pour tous } x, y \in V_1.$$

On le note $(V_1, b_1) \simeq (V_2, b_2)$, voire $b_1 \simeq b_2$ s'il n 'y a pas de confusion possible.

En utilisant la définition, on voit facilement que, pour toutes formes bilinéaires $b : V \times V \longrightarrow k$, $b_i : V_i \times V_i \longrightarrow k, i \in [\![1, 3]\!]$, on a :

(1) $b \simeq b$

(2) Si $b_1 \simeq b_2$, alors $b_2 \simeq b_1$

(3) Si $b_1 \simeq b_2$ et $b_2 \simeq b_3$, alors $b_1 \simeq b_3$.

**Remarque B.2.** Si $V_1$ et $V_2$ sont de dimension finie, et si $(V_1, b_1) \simeq (V_2, b_2)$, alors $V_1$ et $V_2$ ont nécessairement même dimension.

En dimension finie, on a une caractérisation concrète en termes matriciels. Pour l'énoncer, introduisons une autre définition.

**Définition B.3.** Soit $k$ un corps. Deux matrices $M_1, M_2 \in \mathrm{M}_n(k)$ sont *congruentes* s'il existe $P \in \mathrm{GL}_n(k)$ telle que $P^t M_1 P = M_2$

On peut alors démontrer le résultat suivant.

**Lemme B.4.** *Soient deux formes bilinéaires $b_1 : V_1 \times V_1 \longrightarrow k$ et $b_2 : V_2 \times V_2 \longrightarrow k$. On suppose que $V_1$ et $V_2$ sont de dimension finie. Alors, les propriétés suivantes sont équivalentes :*

(1) $(V_1, b_1) \simeq (V_2, b_2)$
(2) *pour toute base $\mathscr{B}_1$ de $V_1$ et toute base $\mathscr{B}_2$ de $V_2$, les matrices représentatives* $\mathrm{Mat}(b_1, \mathscr{B}_1)$ *et* $\mathrm{Mat}(b_2, \mathscr{B}_2)$ *sont congruentes*
(3) *il existe une base $\mathscr{B}_1$ de $V_1$ et une base $\mathscr{B}_2$ de $V_2$ telles que les matrices représentatives* $\mathrm{Mat}(b_1, \mathscr{B}_1)$ *et* $\mathrm{Mat}(b_2, \mathscr{B}_2)$ *sont congruentes*
(4) *il existe une base $\mathscr{B}'_1$ de $V_1$ et une base $\mathscr{B}'_2$ de $V_2$ telles que* $\mathrm{Mat}(b_1, \mathscr{B}'_1) = \mathrm{Mat}(b_2, \mathscr{B}'_2)$.

**Notation.** Si $a_1, \ldots, a_n \in k$, on note $\langle a_1, \ldots, a_n \rangle$ l'unique forme bilinéaire sur $k^n$ dont la matrice représentative dans la base canonique est la matrice

$$\begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix}.$$

Autrement dit, c'est la forme bilinéaire symétrique

$$\begin{aligned} k^n \times k^n &\longrightarrow k \\ (x, y) &\longmapsto \sum_{i=1}^{n} a_i x_i y_i. \end{aligned}$$

Si $b : V \times V \longrightarrow k$ est une forme bilinéaire symétrique sur un $k$-espace vectoriel $V$ de dimension finie, il est bien connu qu'il existe une base de $V$ qui soit $b$-orthonormée (lorsque $2 \neq 0$ dans $k$). En termes d'isomorphisme, cela se retraduit commue suit : il existe $a_1, \ldots, a_n \in k$ tel que $b \simeq \langle a_1, \ldots, a_n \rangle$.

De même, on constate que $V$ possède une base $b$-orthonormée si, et seulement si, on a $b \simeq \langle 1, \ldots, 1 \rangle$.

**Remarque B.5.** Soient $a_1, \ldots, a_n \in k$. Pour toute permutation $\sigma$ de l'ensemble $[\![1, n]\!]$, on a

$$\langle a_1, \ldots, a_n \rangle \simeq \langle a_{\sigma(1)}, \ldots, a_{\sigma(n)} \rangle.$$

En effet, il suffit de faire la permutation appropriée sur les vecteurs de la base canonique pour s'en convaincre.

On continue en introduisant la notion de somme orthogonale de formes bilinéaires.

**Définition B.6.** Soient $b_i : V_i \times V_i \longrightarrow k, i \in [\![1, r]\!]$ $r$ formes bilinéaires. La *somme orthogonale* de $b_1, \ldots, b_r$, notée $(V_1, b_1) \perp \cdots \perp (V_r, b_r)$, ou plus sobrement $b_1 \perp \cdots \perp b_r$, est la forme bilinéaire sur $V_1 \times \cdots \times V_r$ définie par

$$\begin{aligned} (V_1 \times \cdots \times V_r) \times (V_1 \times \cdots \times V_r) &\longrightarrow k \\ ((x_1, \ldots, x_r), (y_1, \ldots, y_r)) &\longmapsto \sum_{i=1}^{r} b(x_i, y_i). \end{aligned}$$

La proposition suivante résume les principales propriétés de la somme orthogonale.

**Proposition B.7.** *Soient $b : V \times V \longrightarrow k$, $b_i : V_i \times V_i \longrightarrow k, i \in [\![1, r]\!]$ des formes bilinéaires. Alors :*

(1) *pour tout $j \in [\![1, r]\!]$, l'isomorphisme évident*

$$(V_1 \times \cdots \times V_j) \times (V_{j+1} \times \cdots \times V_r) \simeq V_1 \times \cdots \times V_r$$

*induit un isomorphisme*

$$(b_1 \perp \cdots \perp b_j) \perp (b_{j+1} \perp \cdots \perp b_r) \simeq b_1 \perp \cdots \perp b_r.$$

(2) *l'isomorphisme évident $V_1 \times V_2 \simeq V_2 \times V_1$ induit un isomorphisme*

$$b_1 \perp b_2 \simeq b_2 \perp b_1$$

(3) *si $b_1 \simeq b_2$, alors $b \perp b_1 \simeq b \perp b_2$*

(4) *si $V_1$ et $V_2$ sont de dimension finie, et si $\mathscr{B}_1 = (e_1, \ldots, e_n)$ et $\mathscr{B}_2 = (e'_1, \ldots, e'_m)$ sont des bases de $V_1$ et $V_2$ respectivement, alors la matrice représentative de $b_1 \perp b_2$, dans la base*

$$\mathscr{B} = ((e_1, 0), \ldots, (e_n, 0), (0, e'_1), \ldots, (0, e'_m))$$

*est*

$$\begin{pmatrix} \mathrm{Mat}(b_1; \mathscr{B}_1) & 0 \\ 0 & \mathrm{Mat}(b_2; \mathscr{B}_2). \end{pmatrix}$$

*En particulier, pour tous $a_1, \ldots, a_n, a'_1, \ldots, a'_m \in k$, on a*

$$\langle a_1, \ldots, a_n \rangle \perp \langle a'_1, \ldots, a'_m \rangle \simeq \langle a_1, \ldots, a_n, a'_1, \ldots, a'_m \rangle.$$

**Remarque B.8.** Le dernier point se généralise bien entendu à $r$ formes bilinéaires.

**Notation.** Si $r \geq 1$, la somme orthogonale $b \perp \cdots \perp b$ est notée simplement $r \times b$.

On constate alors que la forme bilinéaire symétrique $\theta_b$ du théorème 4.5 n'est rien d'autre que $4 \times b$. On peut alors récrire la démonstration de ce théorème comme suit.

Le choix d'une base $b$-orthogonale $(e_1, \ldots, e_n)$ de $V$ donne un isomorphisme $b \simeq \langle a_1, \ldots, a_n \rangle$. Comme les $a_i$ sont les valeurs $b(e_i, e_i)$, on a $a_i > 0$ pour tout $i \in [\![1, n]\!]$.

Les propriétés de la somme orthogonale et de la relation d'isomorphisme entraînent alors la succession d'isomorphismes suinvante :

$$\begin{aligned} 4 \times b &\simeq \langle a_1, \ldots, a_n \rangle \perp \cdots \perp \langle a_1, \ldots, a_n \rangle \\ &\simeq \langle a_1, \ldots, a_n, \ldots, a_1, \ldots, a_n \rangle \\ &\simeq \langle a_1, a_1, a_1, a_1, \ldots, a_n, a_n, a_n, a_n \rangle \\ &\simeq \langle a_1, a_1, a_1, a_1 \rangle \perp \cdots \perp \langle a_n, a_n, a_n, a_n \rangle. \end{aligned}$$

Or, les calculs faits en fin de démonstration montrent alors que $\langle r, r, r, r \rangle \simeq \langle 1, 1, 1, 1 \rangle$ pour tout rationnel $r > 0$.

On a alors

$$4 \times b \simeq \langle 1,1,1,1\rangle \perp \cdots \perp \langle 1,1,1,1\rangle \simeq \langle 1,\ldots,1\rangle,$$

ce qui revient à dire que $V^4$ possède une base orthonormée pour la forme bilinéaire $4 \times b$.

Il reste à comprendre d'où peut bien sortir l'isomorphisme $\langle r,r,r,r\rangle \simeq \langle 1,1,1,1\rangle$.

Pour cela, nous allons introduire le concept de forme bilinéaire symétrique multiplicative. La définition que nous allons proposer est volontairement beaucoup plus restrictive que la définition officielle, mais elle suffira pour ce que l'on veut en faire.

**Notation.** Si $b : V \times V \longrightarrow k$ est une forme bilinéaire symétrique, et si $\lambda \in k^\times$, on note $\lambda b$ la forme bilinéaire symétrique

$$\begin{aligned} \lambda b\colon V \times V &\longrightarrow k \\ (x,y) &\longmapsto \lambda b(x,y). \end{aligned}$$

Rappelons qu'une forme bilinéaire $b : V \times V \longrightarrow k$ est *anisotrope* si $b(x,x) \neq 0$ pour tout $x \in V \setminus \{0\}$. On a alors la définition suivante.

**Définition B.9.** Soit $b : V \times V \longrightarrow k$ une forme bilinéaire symétrique anisotrope sur un $k$-espace vectoriel de dimension finie $V$ est dite *multiplicative* si elle vérifie les deux conditions suivantes :

(1) il existe $x_0 \in V$ tel que $b(x_0,x_0) = 1$

(2) pour tout $x \in V \setminus \{0\}$, on a $b \simeq b(x,x)b$.

**Remarque B.10.** L'expression « forme multiplicative » est justifiée par le constat suivant. Soit $x \in V \setminus \{0\}$, et soit $u_x : V \xrightarrow{\sim} V$ un isomorphisme tel que $b(x,x)b(y,z) = b(u_x(y),u_x(z))$ pour tous $y,z \in V$. En particulier, on a

$$b(x,x)b(y,y) = b(u_x(y),u_x(y)) \quad \text{pour tout } y \in V,$$

et l'ensemble $\{b(x,x) \mid x \in V \setminus \{0\}\}$ est stable par produit.

**Exemple B.11.** La forme $(k,\langle 1\rangle)$ est multiplicative. Elle est clairement anisotrope, $b(1,1) = 1$, et pour tout $x \in k^\times$, on a

$$x^2\langle 1\rangle 1 = \langle x^2\rangle \simeq \langle 1\rangle,$$

le dernier isomorphisme étant induit par la multiplication par $x$ dans $k$.

**Théorème B.12.** *Soit $b : V \times V \longrightarrow k$ une forme multiplicative, et soit $d \in k^\times$. Si $b \perp db$ est anisotrope, elle est multiplicative.*

**Remarque B.13.** Le lecteur pourra retrouver toutes les notions et résultats introduits ici dans [4], par exemple.

Si $k = \mathbb{Q}$, l'exemple et le théorème précédents appliqué à $b = \langle 1\rangle$ et à $d = 1$, montrent que $\langle 1,1\rangle$ est multiplicative. Une utilisation répétée de ce même théorème montre alors plus généralement que $b_m = 2^m \times \langle 1\rangle$ est multiplicative.

Comme les valeurs $b_m(x,x)$ sont exactement les sommes de $2^m$ carrés de rationnels, on en déduit que si $a$ est somme de $2^m$ carrés, alors

$$2^m \times \langle a \rangle = a(2^m \times \langle 1 \rangle) \simeq 2^m \times \langle 1 \rangle.$$

L'isomorphisme utilisé dans la démonstration du théorème 4.5 s'explique alors par le théorème de Lagrange et l'isomorphisme précédent pour $m = 2$. La multiplicativité de $b_m$ implique également que le produit de deux sommes de $2^m$ carrés est une somme de $2^m$ carrés, ce qui explique l'existence de l'identité d'Euler.

Nous finissons ce paragraphe en réinterprétant le calcul d'une matrice de $\mathscr{S}_3(\mathbb{Q})$ de polynôme minimal $X(X^2-3)$. Si $f = X^2-3$, et si $t : \mathbb{Q}[f] \longrightarrow \mathbb{Q}$ est la forme linéaire

$$\begin{array}{rccc} t\colon & \mathbb{Q}[f] & \longrightarrow & \mathbb{Q} \\ & x & \longmapsto & \mathrm{tr}(x), \end{array}$$

on a $b_t \simeq \langle 2, 6 \rangle$. Comme on l'a déjà constaté, si $V$ admet une base orthonormée pour une forme bilinéaire symétrique $b : V \times V \longrightarrow \mathbb{Q}$, alors le déterminant de la matrice représentative de $b$ dans n'importe quelle base de $V$ est un carré non nul. En particulier, si $\langle a_1, \ldots, a_n \rangle \simeq n \times \langle 1 \rangle$, alors $a_1 \cdots a_n$ est un carré non nul.

Or, il est facile de voir que si l'on considère $r$ formes linéaires $t_i : \mathbb{Q}[f_i] \longrightarrow \mathbb{Q}$, et si $(t_1 \oplus \cdots \oplus t_r) : \mathbb{Q}[f_1] \times \cdots \times \mathbb{Q}[f_r] \longrightarrow \mathbb{Q}$ est la forme linéaire définie par

$$(t_1 \oplus \cdots \oplus t_r)(x_1, \ldots, x_r) = \sum_{i=1}^{t} t_i(x_i) \quad \text{pour tout } x_i \in \mathbb{Q}[f_i],$$

alors $b_{t_1 \oplus \cdots \oplus t_r} = b_{t_1} \perp \cdots \perp b_{t_r}$.

Ceci explique le choix de la forme linéaire $s : \mathbb{Q} \times \mathbb{Q}[f] \longrightarrow \mathbb{Q}$. On a en fait pris $s = (3\mathrm{Id}_{\mathbb{Q}}) \oplus t$, afin d'obtenir

$$b_s = b_{3\mathrm{Id}_{\mathbb{Q}} \oplus t} = \langle 3 \rangle \perp b_t \simeq \langle 3 \rangle \perp \langle 2, 6 \rangle \simeq \langle 3, 2, 6 \rangle.$$

Remarquons que l'on a bien $3 \cdot 2 \cdot 6 = 6^2$. Notons que le théorème B.12 implique que pour tout rationnel $d > 0$, et pour tout $r \in \mathbb{Q}^\times$ de la forme $r = a^2 + db^2$, on a

$$\langle r, rd \rangle = r\langle 1, d \rangle \simeq \langle 1, d \rangle,$$

ce qui explique les égalités matricielles un peu sorties du chapeau dans le paragraphe 4.

Mais alors, on a

$$\begin{array}{rcl} \langle 3, 2, 6 \rangle & \simeq & \langle 2, 3, 6 \rangle \\ & \simeq & \langle 2 \rangle \perp (1^2 + 2 \cdot 1^2)\langle 1, 2 \rangle \\ & \simeq & \langle 2 \rangle \perp \langle 1, 2 \rangle \\ & \simeq & \langle 2, 1, 2 \rangle \\ & \simeq & \langle 1, 2, 2 \rangle \\ & \simeq & \langle 1 \rangle \perp (1^2 + 1^2)\langle 1, 1 \rangle \\ & \simeq & \langle 1 \rangle \perp \langle 1, 1 \rangle \\ & \simeq & \langle 1, 1, 1 \rangle. \end{array}$$

Ceci résume les calculs effectués à la fin du paragraphe 4 de manière plus conceptuelle. Notons néanmoins que ce point de vue ne donne pas une base orthonormée concrète. Pour en calculer une, il faut expliciter chaque isomorphisme, et c'est d'ailleurs exactement ce que l'on a fait.

## Références

[1] Berhuy, G., *Valeurs propres de matrices symétriques.* http://www-fourier.univ-grenoble-alpes.fr/~berhuy/fichiers/vpsymnew.pdf

[2] Bender, E.A., *Characteristic polynomials of symmetric matrices.* Pacific J. Math. **25** (1968), 433-431

[3] Bender, E.A., *The dimension of symmetric matrices with a given minimal polynomial.* Linear Alg. and Appl. **3** (1970), 115–123

[4] de Séguins Pazzis, C., *Invitation aux formes quadratiques.* Mathématiques en devenir **104**, Calvage et Mounet, 2010

[5] Krakowski, F., *Eigenwerte und Minimalpolynome symmetrischer Matrizen in kommutativen Körpen.* Comm. Math. Helv. **32** (1957), 224–240