

Le théorème de Frobenius

Marc Lorenzi

18 août 2026

1 Introduction

Une $\mathbb{R}$ -algèbre est un sextuplet $(\mathbb{K}, +, \times, \cdot, 0, 1)$ vérifiant les propriétés suivantes.

- $(\mathbb{K}, +, \times, 0, 1)$ est un anneau.
- $(\mathbb{K}, +, \cdot, 0)$ est un $\mathbb{R}$ -espace vectoriel.
- Pour tout $\lambda \in \mathbb{R}$ et tous $x, y \in \mathbb{K}$, $\lambda.(x \times y) = (\lambda.x) \times y = x \times (\lambda.y)$.

Une sous-algèbre de $\mathbb{K}$ est une partie A de $\mathbb{K}$ telle $(A, +, \times, \cdot, 0, 1)$ soit une $\mathbb{R}$ -algèbre.

L'ensemble $\mathbb{R}' = \{\lambda 1 : \lambda \in \mathbb{R}\}$ est une sous-algèbre de $\mathbb{K}$ isomorphe à $\mathbb{R}$. Nous identifierons désormais $\mathbb{R}'$ et $\mathbb{R}$. Avec cette identification, $\mathbb{R} \subseteq \mathbb{K}$. Cette identification rend inutile la loi de composition externe et la troisième propriété d'algèbre nous dit que pour tout $\lambda \in \mathbb{R}$, pour tous $x, y \in \mathbb{K}$,

$$\lambda \times (x \times y) = (\lambda \times x) \times y = x \times (\lambda \times y)$$

Autrement dit, la multiplication $\times$ est associative (ce que l'on savait déjà par la structure d'anneau de $\mathbb{K}$), mais surtout, les réels *commutent* avec les éléments de $\mathbb{K}$.

Dans toute la suite, on se donne une $\mathbb{R}$ -algèbre $(\mathbb{K}, +, \times, \cdot, 0, 1)$ de dimension finie. On suppose que les éléments non nuls de $\mathbb{K}$ sont inversibles.

Notons que, techniquement, $\mathbb{K}$ n'est pas un corps car la multiplication n'est pas supposée commutative. On parle parfois de *corps non commutatif*, les anglo-saxons utilisent les termes *division ring* et *division algebra*.

Deux exemples immédiats de telles algèbres sont le corps $\mathbb{R}$ des réels, qui est une $\mathbb{R}$ -algèbre de dimension 1, et le corps $\mathbb{C}$ des nombres complexes, qui est une $\mathbb{R}$ -algèbre de dimension 2.

2 On suppose que $\mathbb{R} \subsetneq \mathbb{K}$

Supposons $\mathbb{K} \neq \mathbb{R}$. Donnons-nous $a \in \mathbb{K} \setminus \mathbb{R}$.

Proposition 1. *Il existe $P \in \mathbb{R}[X]$ irréductible de degré 2 tel que $P(a) = 0$.*

Démonstration. Soit $n = \dim K$. La famille $(1, a, a^2, \dots, a^n)$ est une famille d'éléments de $\mathbb{K}$ de cardinal $n + 1 > \dim \mathbb{K}$. Cette famille est donc liée : il existe $\lambda_0, \dots, \lambda_n \in \mathbb{K}$ pas tous nuls tels que

$$\sum_{k=0}^n \lambda_k a^k = 0$$

Soit m le plus grand entier $k \in \llbracket 0, n \rrbracket$ tel que $\lambda_k \neq 0$.

Soit

$$Q = \sum_{k=0}^m \lambda_k X^k$$

On a $\deg Q = m$. Le polynôme Q se factorise dans $\mathbb{R}[X]$ sous la forme

$$Q = P_1 \dots P_r P'_1 \dots P'_s$$

où les P_i sont des polynômes de degré 1 et les P'_i sont irréductibles de degré 2. On a $Q(a) = 0$ et donc, par l'intégrité de $\mathbb{K}$, l'un des facteurs de Q s'annule en a . Ce n'est pas l'un des P_i car $a \notin \mathbb{R}$. Il existe donc $i \in \llbracket 1, s \rrbracket$ tel que $P'_i(a) = 0$. $\square$

Il existe ainsi $p, q \in \mathbb{R}$ tels que $p^2 - 4q < 0$ et $a^2 + pa + q = 0$.

Proposition 2. $\mathcal{C} = \text{Vect}(1, a)$ est une sous-algèbre de $\mathbb{K}$ de dimension 2.

Démonstration. Comme $a \notin \mathbb{R}$, la famille $(1, a)$ est libre, donc $\text{Vect}(1, a)$ est un sous-espace vectoriel de $\mathbb{K}$ de dimension 2. On a évidemment $1 \in \mathcal{C}$. Il reste à montrer la stabilité de $\mathcal{C}$ pour la multiplication.

Soient $z, z' \in \mathcal{C}$. Soient x, y, x', y' tels que $z = x + ay$ et $z' = x' + ay'$. On a

$$\begin{aligned} zz' &= xx' + a(xy' + x'y) + a^2 yy' \\ &= xx' + a(xy' + x'y) - (pa + q)yy' \\ &= (xx' - qyy') + a(xy' + x'y - pyy') \end{aligned}$$

Ainsi, $zz' \in \mathcal{C}$. $\square$

Proposition 3. Il existe $i' \in \mathcal{C}$ tel que $i'^2 = -1$.

Démonstration. L'égalité $a^2 + pa + q = 0$ s'écrit

$$\left(a + \frac{p}{2}\right)^2 = -\frac{4q - p^2}{4}$$

Remarquons que $4q - p^2 > 0$. Soit $\delta = \sqrt{4q - p^2}$. On a donc

$$\left(a + \frac{p}{2}\right)^2 = -\frac{\delta^2}{4}$$

ou encore

$$\left(\frac{2a + p}{\delta}\right)^2 = -1$$

d'où le résultat en posant $i' = (2a + p)/\delta$. $\square$

Proposition 4. $\mathcal{C} = \text{Vect}(1, i')$.

Démonstration. $i' \notin \mathbb{R}$ puisque $i'^2 < 0$. La famille $(1, i')$ est donc une famille libre de $\mathcal{C}$. Cette famille est de cardinal $2 = \dim \mathcal{C}$, donc elle est une base de $\mathcal{C}$. $\square$

Proposition 5. $\mathcal{C}$ est une $\mathbb{R}$ -algèbre isomorphe à $\mathbb{C}$.

Démonstration. Soit $f : \mathcal{C} \rightarrow \mathbb{C}$ définie par $f(x + i'y) = x + iy$. On vérifie facilement que f est un isomorphisme d'algèbres. $\square$

Dorénavant, nous identifions $\mathcal{C}$ et $\mathbb{C}$ via l'isomorphisme f . Avec cette identification, on a donc $i' = i$ et $\mathbb{C} \subseteq \mathbb{K}$.

Proposition 6. Pour tout $x \in \mathbb{K}$, $ix = xi$ si et seulement si $x \in \mathbb{C}$.

Démonstration. Si $x \in \mathbb{C}$, on a évidemment $ix = xi$. Inversement, supposons que x et i commutent. On a alors pour tout $y \in \mathbb{C}$, $xy = yx$. Si $x \in \mathbb{R}$, alors $x \in \mathbb{C}$. Sinon, en reprenant les idées de la preuve de la proposition 1, il existe $P \in \mathbb{R}[X]$ irréductible de degré 2 tel que $P(x) = 0$. On a $P = c(X - \alpha)(X - \beta)$ où $c \in \mathbb{R}^*$ et $\alpha, \beta \in \mathbb{C} \setminus \mathbb{R}$ sont conjugués. Comme x commute avec les nombres complexes, on a

$$0 = P(x) = c(x - \alpha)(x - \beta)$$

Par l'intégrité de $\mathbb{K}$, $x = \alpha$ ou $x = \beta$, et donc $x \in \mathbb{C}$. $\square$

Proposition 7. Si $\mathbb{K}$ est une $\mathbb{R}$ -algèbre commutative, alors $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$.

Démonstration. Nous avons vu que si $\mathbb{K} \neq \mathbb{R}$, alors $\mathbb{C} \subseteq \mathbb{K}$. Supposons que $\mathbb{K}$ est commutative. Tous les éléments de $\mathbb{K}$ commutent avec i et donc, par la proposition précédente, appartiennent à $\mathbb{C}$. Ainsi, $\mathbb{C} \subseteq \mathbb{K}$. Les deux inclusions prouvent que $\mathbb{K} = \mathbb{C}$. $\square$

3 On suppose que $\mathbb{C} \subsetneq \mathbb{K}$

Supposons dans la suite que $\mathbb{K}$ est une $\mathbb{R}$ algèbre non commutative. On a donc $\mathbb{C} \subsetneq \mathbb{K}$. Soit $y \in \mathbb{K} \setminus \mathbb{C}$. Posons $z = iy - yi$.

Proposition 8. $iz = -zi$ et $iz^2 = z^2i$.

Démonstration. $iz = i(iy - yi) = -y - iyi$ et $zi = (iy - yi)i = iyi + i$, donc $iz = -zi$. Également,

$$iz^2 = izz = -ziz = -z(-zi) = z^2i$$

$\square$

Proposition 9. $z^2 \in \mathbb{R}_-^*$.

Démonstration. i et z^2 commutent, donc $z^2 \in \mathbb{C}$. Soit $\mathbb{C}' = \text{Vect}(1, z)$. Comme $iz \neq zi$, $z \notin \mathbb{C}$ et a fortiori, $z \notin \mathbb{R}$. On montre comme plus haut que $\mathbb{C}'$ est une sous-algèbre de $\mathbb{K}$ de dimension 2 isomorphe à $\mathbb{C}$. Remarquons que $\mathbb{C} \cap \mathbb{C}'$ est un sous-espace vectoriel de $\mathbb{C}$ et de $\mathbb{C}'$. Comme $z \notin \mathbb{C}$, ce sous-espace vectoriel est différent de $\mathbb{C}$. Il est donc de dimension 0 ou 1. Mais $\mathbb{R} \subseteq \mathbb{C} \cap \mathbb{C}'$, donc $\mathbb{C} \cap \mathbb{C}'$ est de dimension 1. De là, $\mathbb{C} \cap \mathbb{C}' = \mathbb{R}$. Or, $z^2 \in \mathbb{C}$ et $\mathbb{C}'$ étant stable pour la multiplication, $z^2 \in \mathbb{C}'$. Ainsi, $z^2 \in \mathbb{C} \cap \mathbb{C}'$, d'où $z^2 \in \mathbb{R}$.

On ne peut pas avoir $z^2 \in \mathbb{R}_+$, car sinon $z \in \mathbb{R}$. Donc, $z^2 \in \mathbb{R}_-^*$. $\square$

Posons $z^2 = -\alpha$ où $\alpha \in \mathbb{R}_+^*$. Posons ensuite $j = z/\sqrt{\alpha}$.

Proposition 10. $j^2 = -1$ et $ij = -ji$.

Démonstration. Immédiat, à partir de $z^2 = -\alpha$ et $iz = -zi$. $\square$

Posons $k = ij$. On a $ji = -ij = -k$, $ik = i^2j = -j$, $ki = iji = -i^2j = j$, $jk = jij = -j^2i = i$, $kj = ij^2 = -i$ et $k^2 = iji^2j = -i^2j^2 = -1$.

Proposition 11. $\mathbb{H}' = \text{Vect}(1, i, j, k)$ est une $\mathbb{R}$ -algèbre de dimension 4 isomorphe à la $\mathbb{R}$ -algèbre $\mathbb{H}$ des quaternions.

Le lecteur ne connaissant pas les quaternions pourra consulter l'annexe de cet article.

Démonstration. Montrons que la famille $(1, i, j, k)$ est libre. Soient $a, b, c, d \in \mathbb{R}$. Supposons que

$$a + bi + cj + dk = 0$$

En multipliant par i à gauche, il vient

$$(1) \quad ai - b + ck - dj = 0$$

En multipliant par i à droite, on obtient

$$(2) \quad ai - b - ck + dj = 0$$

En additionnant (1) et (2), il vient $ai - b = 0$. Comme $(1, i)$ est une famille libre, $a = b = 0$. En soustrayant (1) et (2), il vient $ck - dj = 0$. En multipliant à gauche par k , on obtient $-c + di = 0$. Encore une fois, la liberté de $(1, i)$ montre que $c = d = 0$. Ainsi, $\dim \mathbb{H}' = 4$.

Considérons l'application $f : \mathbb{H}' \rightarrow \mathbb{H}$ définie par $f(a + bi + cj + dk) = a + bi + cj + dk$. On vérifie facilement que f est un isomorphisme d'algèbres. $\square$

Résumons-nous. Si $\mathbb{K} \neq \mathbb{R}$, alors $\mathbb{K}$ contient (une sous-algèbre isomorphe à) $\mathbb{C}$. Si $\mathbb{K} \neq \mathbb{C}$, alors $\mathbb{K}$ contient (une sous-algèbre isomorphe à) $\mathbb{H}$. Nous identifions évidemment cette sous-algèbre à $\mathbb{H}$.

4 On suppose $\mathbb{H} \subsetneq \mathbb{K}$

Dernière étape, supposons $\mathbb{H} \subsetneq \mathbb{K}$. Nous allons montrer que cette hypothèse amène une contradiction.

Soit $u \in \mathbb{K} \setminus \mathbb{H}$. Soit $v = ui - iu$. En procédant comme nous l'avons fait plus haut, on obtient $iv = -vi$ et $v^2 \in \mathbb{R}_-^*$. Puis, en posant $m = v/\sqrt{-v^2}$, on a $im = -mi$ et $m^2 = -1$. De là,

$$ijm = -jim = jmi$$

Ainsi, jm commute avec i , donc $jm \in \mathbb{C}$, donc $jm \in \mathbb{H}$. En multipliant par l'inverse de j (qui est $-j$), on en déduit que $m \in \mathbb{H}$ et donc $v \in \mathbb{H}$.

Soit enfin $w = ui + iu$. On a $wi = -u + iui = iw$. Comme w et i commutent, $w \in \mathbb{C}$. A fortiori, $w \in \mathbb{H}$. On a aussi $v = ui - iu \in \mathbb{H}$. En additionnant, $v + w = 2ui \in \mathbb{H}$ d'où, en multipliant à droite par $-i/2$, $u \in \mathbb{H}$. Contradiction. Ainsi, $\mathbb{K} = \mathbb{H}$.

5 Conclusion

Nous avons montré le résultat suivant.

Théorème 12. [FROBENIUS]

Il existe, à isomorphisme près, trois $\mathbb{R}$ -algèbres de dimension finie dont les éléments non nuls sont inversibles. Ces algèbres sont

- *Le corps $\mathbb{R}$ des nombres réels.*
- *Le corps $\mathbb{C}$ des nombres complexes.*
- *L'algèbre $\mathbb{H}$ des quaternions.*

6 Annexe - les quaternions

Pour tous $a, b \in \mathbb{C}$, posons

$$[a, b] = \begin{pmatrix} a & -b \\ \bar{b} & \bar{a} \end{pmatrix}$$

Soit

$$\mathbb{H} = \{[a, b] : a, b \in \mathbb{C}\}$$

Les éléments de $\mathbb{H}$ sont appelés les *quaternions*.

Proposition 13. $\mathbb{H}$ est une sous-algèbre de la $\mathbb{R}$ -algèbre $\mathcal{M}_2(\mathbb{C})$. De plus, les éléments non nuls de $\mathbb{H}$ sont inversibles (dans $\mathbb{H}$).

Démonstration. Notons bien que nous considérons la $\mathbb{R}$ -algèbre $\mathcal{M}_2(\mathbb{C})$ et **pas** la $\mathbb{C}$ -algèbre $\mathcal{M}_2(\mathbb{C})$. La dimension réelle de $\mathcal{M}_2(\mathbb{C})$ est $\dim_{\mathbb{R}} \mathcal{M}_2(\mathbb{C}) = 8$.

On a immédiatement les deux propriétés suivantes : pour tous $a, b \in \mathbb{C}$ et tout $\lambda \in \mathbb{R}$,

$$\lambda[a, b] = [\lambda a, \lambda b] \in \mathbb{H}$$

et pour tous $a, b, c, d \in \mathbb{C}$,

$$[a, b] + [c, d] = [a + c, b + d] \in \mathbb{H}$$

Ainsi, $\mathbb{H}$ est un sous-espace vectoriel du $\mathbb{R}$ -espace vectoriel $\mathcal{M}_2(\mathbb{C})$.

Le neutre pour la multiplication, qui est $I_2 = [1, 0]$, appartient à $\mathbb{H}$. Vérifions la stabilité pour la multiplication matricielle. Soient $a, b, c, d \in \mathbb{C}$. On a

$$\begin{aligned} [a, b] \times [c, d] &= \begin{pmatrix} a & -b \\ \bar{b} & \bar{a} \end{pmatrix} \begin{pmatrix} c & -d \\ \bar{d} & \bar{c} \end{pmatrix} \\ &= \begin{pmatrix} ac - b\bar{d} & -ad - b\bar{c} \\ \bar{b}c + \bar{a}\bar{d} & -\bar{b}d + \bar{a}\bar{c} \end{pmatrix} \\ &= [ac - b\bar{d}, ad + b\bar{c}] \in \mathbb{H} \end{aligned}$$

Montrons enfin l'inversibilité des éléments non nuls de $\mathbb{H}$. Soit $(a, b) \in \mathbb{C}^2$ différent de $(0, 0)$. On a

$$\det[a, b] = |a|^2 + |b|^2 \in \mathbb{R}_+^*$$

donc $[a, b]$ est inversible. De plus,

$$[a, b]^{-1} = \frac{1}{|a|^2 + |b|^2} \begin{pmatrix} \bar{a} & b \\ -\bar{b} & a \end{pmatrix} = \frac{1}{|a|^2 + |b|^2} [\bar{a}, -b] \in \mathbb{H}$$

□

Soient $a, b \in \mathbb{C}$. Écrivons $a = x + iy$ et $b = z + it$ où $x, y, z, t \in \mathbb{R}$. On a

$$[a, b] = [x + iy, z + it] = x[1, 0] + y[i, 0] + z[0, 1] + t[0, i]$$

Posons $1 = [1, 0]$, $i = [i, 0]$, $j = [0, 1]$ et $k = [0, i]$. La famille $(1, i, j, k)$ engendre $\mathbb{H}$. Montrons que cette famille est libre. Pour cela, calculons les produits des quaternions $1, i, j, k$ les uns avec les autres. Le tableau ci-dessous résume les résultats.

	1	i	j	k
1	1	i	j	k
i	1	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

Soient $x, y, z, t \in \mathbb{R}$. Supposons

$$(1) \quad x + iy + jz + kt = 0$$

En multipliant par i à gauche, on obtient

$$(2) \quad ix - y + kz - jt = 0$$

En multipliant par i à droite, on obtient

$$(3) \quad ix - y - kz + jt = 0$$

La combinaison (2) + (3) donne $ix - y = 0$. Clairement, la famille $(1, i)$ est libre, donc $x = y = 0$. En reportant dans (1), on obtient $jz + kt = 0$. La famille (j, k) est libre, donc $z = t = 0$. Ainsi, $(1, i, j, k)$ est une base de $\mathbb{H}$. Nous avons donc prouvé le résultat suivant.

Proposition 14. $\dim_{\mathbb{R}} \mathbb{H} = 4$.

Nous avons finalement montré que $\mathbb{H}$ est une $\mathbb{R}$ -algèbre de dimension 4 dont tous les éléments non nuls sont inversibles.