Étude de cas 3°
Formalisation dans $\mathsf{L}_{\textsf{esp\_vect\_réels}}$

« Théorème de Pythagore »[1]

11 et 18 mai 2004

Preuve « mathématique »

Montrons que deux vecteurs $\vec{u}$ et $\vec{v}$ sont orthogonaux si et seulement si $\|\vec{u}+\vec{v}\|^2 = \|\vec{u}\|^2 + \|\vec{v}\|^2$.

– Considérons le développement suivant

$$\begin{aligned}\|\vec{u}+\vec{v}\|^2 &= (\vec{u}+\vec{v})\cdot(\vec{u}+\vec{v})\\ &= \vec{u}\cdot(\vec{u}+\vec{v})+\vec{v}\cdot(\vec{u}+\vec{v})\\ &= \vec{u}\cdot\vec{u}+\vec{u}\cdot\vec{v}+\vec{v}\cdot\vec{u}+\vec{v}\cdot\vec{v}\\ &= \|\vec{u}\|^2+\|\vec{v}\|^2+2\vec{u}\cdot\vec{v}\end{aligned}$$

– L'égalité $\|\vec{u}+\vec{v}\|^2 = \|\vec{u}\|^2 + \|\vec{v}\|^2$ est donc respectée à la seule condition que $2\vec{u}\cdot\vec{v} = 0 \Leftrightarrow \vec{u}\cdot\vec{v} = 0 \Leftrightarrow \vec{u},\vec{v}$ orthogonaux.

[1] preuve « mathématique » tirée du cours Algèbre linéaire, EPFL, 2003 et fournie par Philippe Suter

Preuve formelle

1	$\forall(x\in\mathbb{R})\forall(y\in\mathbb{R})(x+y\in\mathbb{R})$	ax 1
2	$\forall(x\in\mathbb{R})\forall(y\in\mathbb{R})\forall(z\in\mathbb{R})(x+(y+z)=(x+y)+z)$	ax 2
3	$\forall(x\in\mathbb{R})\forall(y\in\mathbb{R})(x+y=y+x)$	ax 3
4	$\forall(x\in\mathbb{R})(x+0=x)$	ax 4
5	$\forall(x\in\mathbb{R})\exists(-x\in\mathbb{R})(x+(-x)=0)$	ax 5
6	$\forall(x\in\mathbb{R})\forall(y\in\mathbb{R})(x{\cdot}y\in\mathbb{R})$	ax 6
7	$\forall(x\in\mathbb{R})\forall(y\in\mathbb{R})\forall(z\in\mathbb{R})(x{\cdot}(y{\cdot}z)=(x{\cdot}y){\cdot}z)$	ax 7
8	$\forall(x\in\mathbb{R})\forall(y\in\mathbb{R})(x{\cdot}y=y{\cdot}x)$	ax 8
9	$\forall(x\in\mathbb{R})(x{\cdot}1=x)$	ax 9
10	$\forall(x\in\mathbb{R}\setminus\{0\})\exists(x^{-1}\in\mathbb{R}\setminus\{0\})(x{\cdot}x^{-1}=1)$	ax 10
11	$\forall(x\in\mathbb{R})\forall(y\in\mathbb{R})\forall(z\in\mathbb{R})(x{\cdot}(y+z)=x{\cdot}y+x{\cdot}z)$	ax 11
12	$\forall(n\in\mathbb{N})\forall(\vec{x}\in\mathbb{R}^n)\forall(\vec{y}\in\mathbb{R}^n)(\vec{x}+\vec{y}\in\mathbb{R}^n)$	ax 12
13	$\forall(n\in\mathbb{N})\forall(\vec{u}\in\mathbb{R}^n)\forall(\vec{v}\in\mathbb{R}^n)(\vec{u}\cdot\vec{v}=\vec{v}\cdot\vec{u})$	ax 13
14	$\forall(n\in\mathbb{N})\forall(\vec{u}\in\mathbb{R}^n)\forall(\vec{v}\in\mathbb{R}^n)\forall(\vec{w}\in\mathbb{R}^n)(\vec{u}\cdot(\vec{v}+\vec{w})=\vec{u}\cdot\vec{v}+\vec{u}\cdot\vec{w})$	ax 14
15	$\forall(n\in\mathbb{N})\forall(\vec{u}\in\mathbb{R}^n)\forall(\vec{v}\in\mathbb{R}^n)(\vec{u},\vec{v}\ \texttt{sont orth.}\Leftrightarrow\vec{u}\cdot\vec{v}=0)$	ax déf
16	$\forall(n\in\mathbb{N})\forall(\vec{u}\in\mathbb{R}^n)(\|\vec{u}\|^2=\vec{u}\cdot\vec{u})$	ax déf
17	$\forall(x\in\mathbb{R})\forall(y\in\mathbb{R})\forall(z\in\mathbb{R}\setminus\{0\})(x=y\Leftrightarrow z{\cdot}x=z{\cdot}y))$	lem 1
18	$\forall(x\in\mathbb{R})\forall(y\in\mathbb{R})\forall(z\in\mathbb{R})(x=y\Leftrightarrow z+x=z+y))$	lem 2
19	$\forall(x\in\mathbb{R})(x{\cdot}0=0)$	lem 3
20	$\forall(x\in\mathbb{R})(2{\cdot}x=x+x)$	lem 4
21	$n\in\mathbb{N}\wedge\vec{u}\in\mathbb{R}^n\wedge\vec{v}\in\mathbb{R}^n$	hyp
22	$\vec{u},\vec{v}\ \texttt{sont orth.}\Leftrightarrow\vec{u}\cdot\vec{v}=0$	21, 15
	$\Leftrightarrow 2{\cdot}(\vec{u}\cdot\vec{v})=2{\cdot}0$	17
	$\Leftrightarrow 2{\cdot}(\vec{u}\cdot\vec{v})=0$	19
	$\Leftrightarrow(\|\vec{u}\|^2+\|\vec{v}\|^2)+2{\cdot}(\vec{u}\cdot\vec{v})=(\|\vec{u}\|^2+\|\vec{v}\|^2)+0$	18
	$\Leftrightarrow(\|\vec{u}\|^2+\|\vec{v}\|^2)+2{\cdot}(\vec{u}\cdot\vec{v})=\|\vec{u}\|^2+\|\vec{v}\|^2$	4
	$\Leftrightarrow(\|\vec{u}\|^2+\|\vec{v}\|^2)+(\vec{u}\cdot\vec{v}+\vec{u}\cdot\vec{v})=\|\vec{u}\|^2+\|\vec{v}\|^2$	20
	$\Leftrightarrow(\vec{u}\cdot\vec{u}+\vec{v}\cdot\vec{v})+(\vec{u}\cdot\vec{v}+\vec{u}\cdot\vec{v})=\|\vec{u}\|^2+\|\vec{v}\|^2$	21, 16
	$\Leftrightarrow(\vec{u}\cdot\vec{u}+\vec{v}\cdot\vec{v})+(\vec{u}\cdot\vec{v}+\vec{v}\cdot\vec{u})=\|\vec{u}\|^2+\|\vec{v}\|^2$	21, 13
	$\Leftrightarrow(\vec{u}\cdot\vec{u}+\vec{u}\cdot\vec{v})+(\vec{v}\cdot\vec{u}+\vec{v}\cdot\vec{v})=\|\vec{u}\|^2+\|\vec{v}\|^2$	2, 3
	$\Leftrightarrow\vec{u}\cdot(\vec{u}+\vec{v})+\vec{v}\cdot(\vec{u}+\vec{v})=\|\vec{u}\|^2+\|\vec{v}\|^2$	21, 14
	$\Leftrightarrow(\vec{u}+\vec{v})\cdot(\vec{u}+\vec{v})=\|\vec{u}\|^2+\|\vec{v}\|^2$	21, 14
	$\Leftrightarrow\|\vec{u}+\vec{v}\|^2=\|\vec{u}\|^2+\|\vec{v}\|^2$	21, 16
23	$(n\in\mathbb{N}\wedge\vec{u}\in\mathbb{R}^n\wedge\vec{v}\in\mathbb{R}^n)\Rightarrow(\vec{u},\vec{v}\ \texttt{sont orth.}\Leftrightarrow\|\vec{u}+\vec{v}\|^2=\|\vec{u}\|^2+\|\vec{v}\|^2)$	21, 22
24	$\forall(n\in\mathbb{N})\forall(\vec{u}\in\mathbb{R}^n)\forall(\vec{v}\in\mathbb{R}^n)(\vec{u},\vec{v}\ \texttt{sont orth.}\Leftrightarrow\|\vec{u}+\vec{v}\|^2=\|\vec{u}\|^2+\|\vec{v}\|^2))$	23

Commentaires

– pour fixer les idées, la preuve porte sur des vecteurs *réels*
– $\mathbb{R}^n$ désigne l'espace vectoriel de nombres réels et de dimension n
– $-x$ et x^{-1} sont considérés comme des *symboles*[2] (variables individuelles) et non pas comme des termes
– $\| \ \|^2$ représente un abus de notation pour un (seul) symbole fonctionnel
– l'axiome 1 dit que les nombres réels sont *clos sous l'opération d'addition*
– l'axiome 2 dit que l'addition de nombres réels est *associative*
– l'axiome 3 dit que l'addition de nombres réels est *commutative*
– l'axiome 4 dit que 0 désigne un *élément neutre à gauche* pour l'opération d'addition
– l'axiome 5 dit que pour tout nombre réel il existe un nombre *inverse* pour l'opération d'addition
– les axiomes 1–5 disent que l'ensemble des nombres réels forme un *groupe commutatif* pour l'opération d'addition
– l'axiome 6 dit que les nombres réels sont *clos sous l'opération de multiplication*
– l'axiome 7 dit que la multiplication de nombres réels est *associative*
– l'axiome 8 dit que la multiplication de nombres réels est *commutative*
– l'axiome 9 dit que 1 désigne un *élément neutre à gauche* pour l'opération de multiplication
– l'axiome 10 dit que pour tout nombre réel différent de zéro il existe un nombre *inverse* pour l'opération de multiplication
– les axiomes 6–10 disent que l'ensemble des nombres réels sans le nombre zéro forme un *groupe commutatif* pour l'opération de multiplication
– l'axiome 11 dit que la multiplication de nombres réels est *distributive* par rapport à l'addition de nombres réels
– les axiomes 1–4, 6–10 et 11 disent que l'ensemble des nombres réels forme un *corps* pour l'opération d'addition et de multiplication
– l'axiome 12 dit que l'ensemble des vecteurs réels est *clos sous l'opération d'addition*
– l'axiome 13 dit que le produit scalaire est *commutatif*
– l'axiome 14 dit que le produit scalaire est *distributif* par rapport à l'addition vectorielle
– le lemme 2 se montre de façon analogue au lemme 1
– le lemme 3 dit que la constante individuelle 0 désigne un *anihilateur à gauche* pour l'opération de multiplication
– le lemme 4 se montre par *induction*[3]

[2] au même titre qu'une variable primée x'
[3] sujet pas abordé dans ce cours

Lemme (1)

16.1	$x \in \mathbb{R}$	hyp
16.2	$y \in \mathbb{R}$	hyp
16.3	$z \in \mathbb{R} \setminus \{0\}$	hyp
16.4	$x = y$	hyp
16.5	$z \cdot x = z \cdot x$	théor
16.6	$z \cdot x = z \cdot y$	16.4, 16.5
16.7	$z \cdot x = z \cdot y$	hyp
16.8	$\exists (z^{-1} \in \mathbb{R} \setminus \{0\})(z \cdot z^{-1} = 1)$	16.3, 10
16.9	$z^{-1} \in \mathbb{R} \setminus \{0\} \wedge z \cdot z^{-1} = 1$	hyp
16.10	$x = x \cdot 1$	9
	$= x \cdot (z \cdot z^{-1})$	16.9
	$= (x \cdot z) \cdot z^{-1}$	7
	$= (z \cdot x) \cdot z^{-1}$	8
	$= (z \cdot y) \cdot z^{-1}$	16.7
	$= (y \cdot z) \cdot z^{-1}$	8
	$= y \cdot (z \cdot z^{-1})$	7
	$= y \cdot 1$	16.9
	$= y$	9
16.11	$x = y$	
16.12	$x = y \Leftrightarrow z \cdot x = z \cdot y$	
16.13	$z \in \mathbb{R} \setminus \{0\} \Rightarrow x = y \Leftrightarrow z \cdot x = z \cdot y$	
16.14	$\forall (z \in \mathbb{R} \setminus \{0\})(x = y \Leftrightarrow z \cdot x = z \cdot y)$	
16.15	$y \in \mathbb{R} \Rightarrow \forall (z \in \mathbb{R} \setminus \{0\})(x = y \Leftrightarrow z \cdot x = z \cdot y)$	
16.16	$\forall (y \in \mathbb{R}) \forall (z \in \mathbb{R} \setminus \{0\})(x = y \Leftrightarrow z \cdot x = z \cdot y)$	
16.17	$x \in \mathbb{R} \Rightarrow \forall (y \in \mathbb{R}) \forall (z \in \mathbb{R} \setminus \{0\})(x = y \Leftrightarrow z \cdot x = z \cdot y)$	
17	$\forall (x \in \mathbb{R}) \forall (y \in \mathbb{R}) \forall (z \in \mathbb{R} \setminus \{0\})(x = y \Leftrightarrow z \cdot x = z \cdot y)$	

Lemme (3)

18.1	$x \in \mathbb{R}$	hyp
18.2	$0 + 0 = 0$	4
18.3	$x{\cdot}0 = x{\cdot}(0 + 0)$	18.2
	$= x{\cdot}0 + x{\cdot}0$	11
18.4	$x{\cdot}0 + 0 = x{\cdot}0$	4
18.5	$x{\cdot}0 + 0 = x{\cdot}0 + x{\cdot}0$	18.3, 18.4
18.6	$0 = x{\cdot}0$	18.5, lem 2
18.7	$x{\cdot}0 = 0$	18.6
19	$\forall(x \in \mathbb{R})(x{\cdot}0 = 0)$	