# Vecteurs et matrices

Vidéo ■ partie 4.1. Vecteurs
Vidéo ■ partie 4.2. Produit scalaire hermitien
Vidéo ■ partie 4.3. Produit tensoriel de vecteurs
Vidéo ■ partie 4.4. Matrices
Vidéo ■ partie 4.5. Matrice adjointe
Vidéo ■ partie 4.6. Matrice unitaire

*Un qubit est un vecteur et les opérations sur les qubits sont codées par des matrices. Nous étudions ici le calcul sur les vecteurs, les matrices et leur lien avec les qubits.*

## 1. Vecteurs

### 1.1. Vecteurs du plan

On commence par la notion de vecteur du plan. Un ***vecteur du plan*** est la donnée de deux nombres réels, noté :

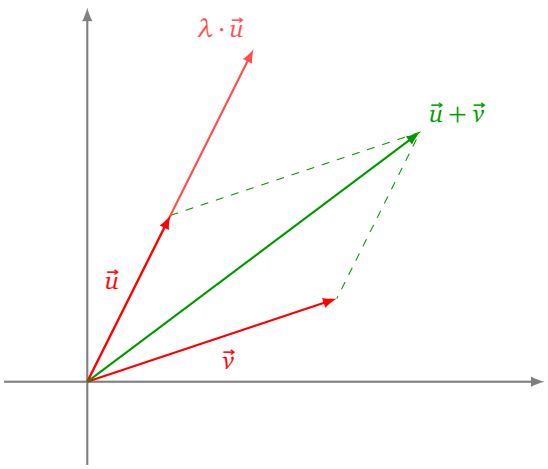
$$\vec{u} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \qquad \text{avec } x_1, x_2 \in \mathbb{R}.$$

On peut additionner deux vecteurs :

$$\vec{u} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \qquad \vec{v} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \qquad \text{alors} \quad \vec{u} + \vec{v} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \end{pmatrix}.$$

On peut multiplier un vecteur par un coefficient réel $\lambda$ :

$$\vec{u} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \qquad \lambda \cdot \vec{v} = \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \end{pmatrix}.$$



Le ***vecteur nul*** a toutes ses coordonnées nulles :

$$\vec{0} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

La ***norme*** (ou ***longueur***) d'un vecteur est :

$$\|\vec{u}\| = \sqrt{x_1^2 + x_2^2}$$

## 1.2. Vecteurs à coefficients complexes

Nous généralisons la notion précédente : le nombre $n$ de coefficients n'est pas limité à 2 et ceux-ci sont maintenant des nombres complexes (et non plus des nombres réels).
Notons $\mathbb{K}$ un corps, qui pour nous sera $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$. Fixons $n \geqslant 1$ un entier. Un ***vecteur*** de taille $n$ à coefficients dans $\mathbb{K}$ s'écrit :

$$u = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \quad \text{avec } x_1, x_2, \ldots, x_n \in \mathbb{K}.$$

Noter qu'à partir de maintenant on n'utilise plus la notation avec une flèche au-dessus du nom du vecteur.
L'addition de deux vecteurs :

$$u = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \qquad v = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \qquad \text{alors } u + v = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix}.$$

Le ***vecteur nul*** est :

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Nous allons voir plusieurs multiplications associées à des vecteurs. Pour l'instant on définit seulement la multiplication par un scalaire $\lambda \in \mathbb{K}$ :

$$u = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \qquad \lambda \cdot u = \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \\ \vdots \\ \lambda x_n \end{pmatrix}.$$

*Rappels.* Pour un nombre complexe $x$, on note $x^*$ son conjugué. Si $x$ est un nombre réel alors $x^* = x$.
Le ***vecteur dual*** d'un vecteur $u$ est un vecteur de même taille, dont les coefficients sont les conjugués de ceux de $u$, et qui est écrit sous la forme d'un vecteur ligne :

$$u = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \qquad u^* = \begin{pmatrix} x_1^* & x_2^* & \cdots & x_n^* \end{pmatrix}.$$

**Exemple.**

$$u = \begin{pmatrix} 1+\mathrm{i} \\ \mathrm{i} \\ 2 \\ 3-4\mathrm{i} \end{pmatrix} \qquad u^* = \begin{pmatrix} 1-\mathrm{i} & -\mathrm{i} & 2 & 3+4\mathrm{i} \end{pmatrix}.$$

### 1.3. Qubit sous forme de vecteur

Un qubit est un vecteur, ses coefficients sont des nombres complexes et sa taille est toujours une puissance de 2. Un 1-qubit est un vecteur de taille 2 :

$$|\psi\rangle = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \qquad \text{avec } x_1, x_2 \in \mathbb{C}.$$

On note $|0\rangle = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ (qui n'est pas le vecteur nul !) et $|1\rangle = \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$ les deux 1-qubits de base.
Plus généralement un $n$-qubit est un vecteur de taille $2^n$ :

$$|\psi\rangle = \begin{pmatrix} x_1 \\ \vdots \\ x_{2^n} \end{pmatrix} \qquad \text{avec } x_1, \ldots, x_{2^n} \in \mathbb{C}.$$

Le dual du vecteur $|\psi\rangle$ sera noté $\langle\psi|$ :

$$\boxed{\langle\psi| = |\psi\rangle^* = \begin{pmatrix} x_1^* & x_2^* & \cdots & x_{2^n}^* \end{pmatrix}}$$

On rappelle que la notation $|\psi\rangle$ se lit « ket psi ». La notation $\langle\psi|$ se lit « bra psi ».

## 2. Produit scalaire

### 2.1. Produit scalaire hermitien

Nous allons définir une opération qui, à partir de deux vecteurs, donne un scalaire (c'est-à-dire un nombre complexe si $\mathbb{K} = \mathbb{C}$ ou un nombre réel si $\mathbb{K} = \mathbb{R}$).
Soient

$$u = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \qquad v = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}.$$

Le ***produit scalaire hermitien*** des deux vecteurs $u$ et $v$ est défini par :

$$\boxed{\langle u|v\rangle = \sum_{i=1}^{n} x_i^* \cdot y_i}$$

Autrement dit :

$$\langle u|v\rangle = x_1^* \cdot y_1 + x_2^* \cdot y_2 + \cdots + x_n^* \cdot y_n.$$

**Proposition 1.**
*Le produit scalaire hermitien est linéaire par rapport au terme de droite et anti-linéaire par rapport au terme de gauche :*

$$\langle u|v_1+v_2\rangle = \langle u|v_1\rangle + \langle u|v_2\rangle \qquad \langle u_1+u_2|v\rangle = \langle u_1|v\rangle + \langle u_2|v\rangle$$

*et pour $\lambda \in \mathbb{C}$ :*

$$\boxed{\langle u|\lambda v\rangle = \lambda \langle u|v\rangle \quad et \quad \langle \lambda u|v\rangle = \lambda^* \langle u|v\rangle}$$

*Enfin :*

$$\boxed{\langle v|u\rangle = \langle u|v\rangle^*}$$

Notez bien le coefficient $\lambda^*$ obtenu par anti-linéarité par rapport au terme de gauche.

> **Exemple.**
>
> $\langle (1+\mathrm{i})u_1 + (4+2\mathrm{i})u_2 | \mathrm{i}v_1 + (1-2\mathrm{i})v_2\rangle$
> $= \mathrm{i}\,\langle (1+\mathrm{i})u_1 + (4+2\mathrm{i})u_2 | v_1\rangle + (1-2\mathrm{i})\,\langle (1+\mathrm{i})u_1 + (4+2\mathrm{i})u_2 | v_2\rangle$ linéarité à droite
> $= \mathrm{i}(1-\mathrm{i})\,\langle u_1|v_1\rangle + \mathrm{i}(4-2\mathrm{i})\,\langle u_2|v_1\rangle + (1-2\mathrm{i})(1-\mathrm{i})\,\langle u_1|v_2\rangle + (1-2\mathrm{i})(4-2\mathrm{i})\,\langle u_2|v_2\rangle$ anti-linéarité à gauche

## 2.2. Norme

La *norme* du vecteur $u = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, notée $\|u\|$, est définie par :

$$\boxed{\|u\| = \sqrt{\sum_{i=1}^{n} |x_i|^2}}$$

Autrement dit :

$$\|u\|^2 = |x_1|^2 + |x_2|^2 + \cdots + |x_n|^2.$$

C'est un nombre réel positif.
On rappelle que $|z|$, le module du nombre complexe $z = a + \mathrm{i}b$, est un nombre réel positif, et que :

$$|z|^2 = a^2 + b^2 = z^* \cdot z.$$

On peut donc récrire la norme à l'aide du produit scalaire hermitien :

$$\|u\| = \sqrt{\langle u|u\rangle}.$$

On retient aussi :

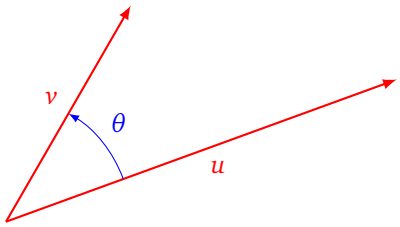
$$\boxed{\|u\|^2 = \langle u|u\rangle}$$

## 2.3. Vecteurs orthogonaux

**Rappel sur le produit scalaire réel.** Pour deux vecteurs du plan, le produit scalaire correspond à une mesure de l'angle entre les deux vecteurs. En effet, on a la formule :

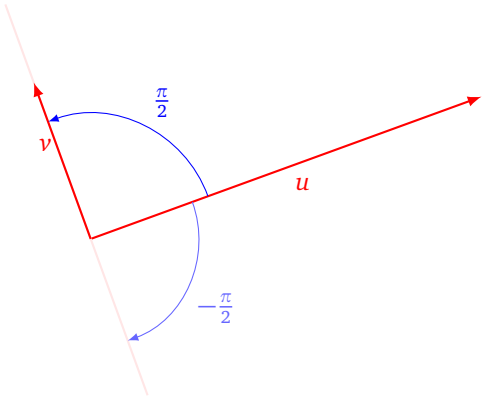
$$\langle u|v\rangle = \|u\| \cdot \|v\| \cdot \cos(\theta)$$

où $\theta$ est l'angle entre les vecteurs $u$ et $v$.




On dit que deux vecteurs du plan sont ***orthogonaux*** si $\theta = \pm\frac{\pi}{2} \pmod{2\pi}$. Ainsi deux vecteurs du plan sont orthogonaux si et seulement si leur produit scalaire est nul :

$$\langle u|v\rangle = 0.$$




**Cas général.** On utilise le produit scalaire hermitien pour définir la notion d'orthogonalité pour des vecteurs quelconques. Deux vecteurs $u$ et $v$ de $\mathbb{K}^n$ sont ***orthogonaux*** si leur produit scalaire hermitien est nul :

$$\langle u|v\rangle = 0.$$

Exemple : le qubit $|0\rangle = \binom{1}{0}$ et le qubit $|1\rangle = \binom{0}{1}$ sont des qubits orthogonaux.

**Qubits orthogonaux et sphère de Bloch.** Considérons deux qubits $|\psi\rangle$ et $|\psi'\rangle$ écrits sous forme normalisée

$$|\psi\rangle \equiv \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\phi}|1\rangle = \begin{pmatrix}\cos\left(\frac{\theta}{2}\right)\\ \sin\left(\frac{\theta}{2}\right)e^{i\phi}\end{pmatrix}$$

$$|\psi'\rangle \equiv \cos\left(\frac{\theta'}{2}\right)|0\rangle + \sin\left(\frac{\theta'}{2}\right)e^{i\phi'}|1\rangle = \begin{pmatrix}\cos\left(\frac{\theta'}{2}\right)\\ \sin\left(\frac{\theta'}{2}\right)e^{i\phi'}\end{pmatrix}$$

Sous quelles conditions ces qubits sont-ils orthogonaux ? On exclut le cas $\theta = 0$, qui correspond au qubit $|0\rangle$, car le seul qubit orthogonal à $|0\rangle$ est $|1\rangle$ (à équivalence près). Pour la même raison on exclut le cas $\theta = \pi$, qui correspond au qubit $|1\rangle$. Ainsi on a

$$0 < \theta, \theta' < \pi \quad \text{et} \quad -\pi < \phi, \phi' \leqslant \pi.$$

On calcule leur produit scalaire hermitien :

$$\begin{aligned}\langle\psi|\psi'\rangle &= \cos\left(\frac{\theta}{2}\right)\cdot\cos\left(\frac{\theta'}{2}\right) + \sin\left(\frac{\theta}{2}\right)e^{-i\phi}\cdot\sin\left(\frac{\theta'}{2}\right)e^{i\phi'}\\ &= \cos\left(\frac{\theta}{2}\right)\cos\left(\frac{\theta'}{2}\right) + \sin\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta'}{2}\right)e^{i(\phi'-\phi)}\end{aligned}$$

Avant d'être nul, ce produit scalaire doit être un nombre réel. Bien sûr, les sinus et les cosinus sont des nombres réels, mais il faut aussi que $e^{i(\phi'-\phi)}$ soit un nombre réel. Or

$$e^{i(\phi'-\phi)} \in \mathbb{R} \iff \phi'-\phi \equiv 0 \pmod{2\pi} \text{ ou } \phi'-\phi \equiv \pi \pmod{2\pi}.$$

En effet, on a $e^{i\alpha} = 1$ si et seulement si $\alpha \equiv 0 \pmod{2\pi}$, et $e^{i\alpha} = -1$ si et seulement si $\alpha \equiv \pi \pmod{2\pi}$.
Premier cas : $\phi'-\phi \equiv 0 \pmod{2\pi}$. Alors $\phi = \phi'$, et

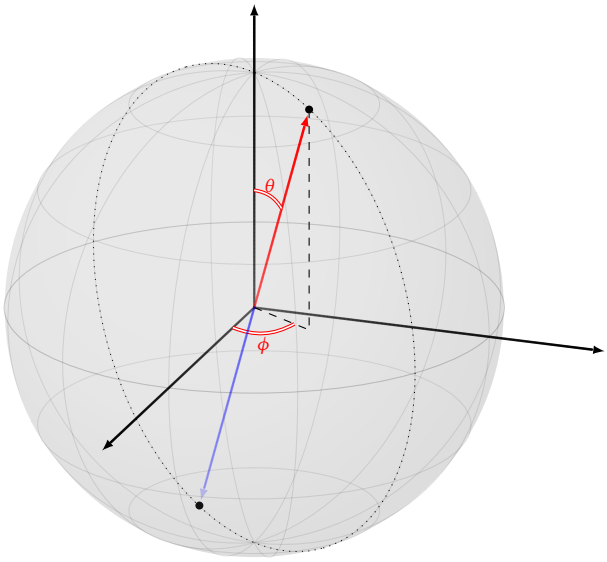
$$\begin{aligned}
\langle\psi|\psi'\rangle = 0 &\iff \cos\left(\frac{\theta}{2}\right)\cos\left(\frac{\theta'}{2}\right) + \sin\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta'}{2}\right) = 0 \\
&\iff \cos\left(\frac{\theta}{2} - \frac{\theta'}{2}\right) = 0 \\
&\iff \frac{\theta}{2} - \frac{\theta'}{2} = \frac{\pi}{2} \pmod{\pi} \\
&\iff \theta - \theta' = \pi \pmod{2\pi}
\end{aligned}$$

Mais cette dernière égalité est impossible car $0 < \theta < \pi$ et $0 < \theta' < \pi$, donc $-\pi < \theta - \theta' < \pi$. Le premier cas ne conduit donc à aucune solution.
Second cas : $\phi'-\phi \equiv \pi \pmod{2\pi}$. Alors $\phi' = \phi + \pi \pmod{2\pi}$, et alors

$$\begin{aligned}
\langle\psi|\psi'\rangle = 0 &\iff \cos\left(\frac{\theta}{2}\right)\cos\left(\frac{\theta'}{2}\right) - \sin\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta'}{2}\right) = 0 \\
&\iff \cos\left(\frac{\theta}{2} + \frac{\theta'}{2}\right) = 0 \\
&\iff \frac{\theta}{2} + \frac{\theta'}{2} = \frac{\pi}{2} \pmod{\pi} \\
&\iff \theta' = \pi - \theta \pmod{2\pi}
\end{aligned}$$

Nous avons obtenu une solution : le qubit de représentation $(\theta', \phi') = (\pi - \theta, \phi + \pi)$ est orthogonal au qubit de représentation $(\theta, \phi)$. Géométriquement le qubit $|\psi'\rangle$ est antipodal au qubit $|\psi\rangle$ sur la sphère de Bloch. Autrement dit, l'un s'obtient de l'autre par la symétrie centrale centrée à l'origine. Noter que c'est aussi valide pour $|0\rangle$ et $|1\rangle$.
On retient :

| Deux 1-qubits sont orthogonaux si, et seulement si, ils sont antipodaux sur la sphère de Bloch. |
|---|



### 2.4. Inégalité de Cauchy-Schwarz

Terminons par l'énoncé d'une inégalité importante.

**Théorème 1** (Inégalité de Cauchy-Schwarz)**.**

$$\boxed{|\langle u|v\rangle| \leqslant \|u\| \cdot \|v\|}$$

## 3. Produit tensoriel de vecteurs

### 3.1. Définition

Soient

$$u = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n \qquad \text{et} \qquad v = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix} \in \mathbb{K}^m.$$

Le *produit tensoriel* de $u$ par $v$, noté $u \otimes v$, est le vecteur de $\mathbb{K}^{nm}$ défini par :

$$u \otimes v = \begin{pmatrix} x_1 \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} \\ x_2 \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} \\ \vdots \\ x_n \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} \end{pmatrix} = \begin{pmatrix} x_1 y_1 \\ \vdots \\ x_1 y_m \\ x_2 y_1 \\ \vdots \\ x_2 y_m \\ \vdots \\ \vdots \\ x_n y_1 \\ \vdots \\ x_n y_m \end{pmatrix}$$

Autrement dit, on prend des copies du vecteur $v$, et chaque copie est multipliée par une coordonnée du vecteur $u$.

Par exemple :

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a \begin{pmatrix} c \\ d \end{pmatrix} \\ b \begin{pmatrix} c \\ d \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$$

En général $u \otimes v \neq v \otimes u$ :

$$\begin{pmatrix} 1 \\ 2 \end{pmatrix} \otimes \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \\ 5 \\ 6 \\ 8 \\ 10 \end{pmatrix} \qquad \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 3 \\ 6 \\ 4 \\ 8 \\ 5 \\ 10 \end{pmatrix}$$

## 3.2. Propriétés

**Proposition 2.**
*Le produit tensoriel est linéaire à gauche et à droite :*

$$(\lambda u)\otimes v = \lambda(u\otimes v) = u\otimes(\lambda v) \qquad \lambda\in\mathbb{C}$$
$$(u_1+u_2)\otimes v = u_1\otimes v \;+\; u_2\otimes v$$
$$u\otimes(v_1+v_2) = u\otimes v_1 \;+\; u\otimes v_2$$

**Exemple.**
On développe l'expression $(u_1+u_2)\otimes(v_1+v_2)$ en deux temps :

$$\begin{aligned}(u_1+u_2)\otimes(v_1+v_2) &= u_1\otimes(v_1+v_2) \;+\; u_2\otimes(v_1+v_2) \quad \text{linéarité à gauche}\\ &= u_1\otimes v_1 \;+u_1\otimes v_2 \;+\; u_2\otimes v_1 + \; u_2\otimes v_2 \quad \text{linéarité à droite}\end{aligned}$$

## 3.3. Produit de qubits

Si $|\phi\rangle$ est un $n$-qubit et $|\psi\rangle$ est un $m$-qubit, alors le ***produit*** de $|\phi\rangle\cdot|\psi\rangle$ est défini par le produit tensoriel :

$$\boxed{|\phi\rangle\cdot|\psi\rangle = |\phi\rangle\otimes|\psi\rangle}$$

Le produit $|\phi\rangle\cdot|\psi\rangle$ est un $(n+m)$-qubit (un vecteur de taille $2^n\cdot 2^m = 2^{n+m}$).
On rappelle que

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \qquad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

Ainsi :

$$|0.0\rangle = |0\rangle\cdot|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \qquad |0.1\rangle = |0\rangle\cdot|1\rangle = \begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$|1.0\rangle = |1\rangle\cdot|0\rangle = \begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \qquad |1.1\rangle = |1\rangle\cdot|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

**Exemple.**
Voyons comment calculer le produit $|\phi\rangle\cdot|\psi\rangle$ dans le cas où :

$$|\phi\rangle = (1+2\mathrm{i})\,|0\rangle + \mathrm{i}\,|1\rangle \qquad |\psi\rangle = 2\,|0\rangle + (3-4\mathrm{i})\,|1\rangle$$

1. *Calcul tensoriel.* Nous revenons à la définition vectorielle des qubits.

$$\begin{aligned}|\phi\rangle\otimes|\psi\rangle &= \left((1+2\mathrm{i})\begin{pmatrix}1\\0\end{pmatrix} + \mathrm{i}\begin{pmatrix}0\\1\end{pmatrix}\right)\otimes\left(2\begin{pmatrix}1\\0\end{pmatrix} + (3-4\mathrm{i})\begin{pmatrix}0\\1\end{pmatrix}\right)\\ &= (1+2\mathrm{i})\begin{pmatrix}1\\0\end{pmatrix}\otimes 2\begin{pmatrix}1\\0\end{pmatrix} + (1+2\mathrm{i})\begin{pmatrix}1\\0\end{pmatrix}\otimes(3-4\mathrm{i})\begin{pmatrix}0\\1\end{pmatrix} + \mathrm{i}\begin{pmatrix}0\\1\end{pmatrix}\otimes 2\begin{pmatrix}1\\0\end{pmatrix} + \mathrm{i}\begin{pmatrix}0\\1\end{pmatrix}\otimes(3-4\mathrm{i})\begin{pmatrix}0\\1\end{pmatrix}\\ &= 2(1+2\mathrm{i})\,|0.0\rangle + (1+2\mathrm{i})(3-4\mathrm{i})\,|0.1\rangle + 2\mathrm{i}\,|1.0\rangle + (4+3\mathrm{i})\,|1.1\rangle\end{aligned}$$

2. *Calcul formel.* C'est la technique vue dans le chapitre « Découverte de l'informatique quantique ». C'est en fait le même calcul que précédemment, mais sans revenir aux vecteurs :

$$\begin{aligned}|\phi\rangle \otimes |\psi\rangle &= \big((1+2\mathrm{i})\,|0\rangle + \mathrm{i}\,|1\rangle\big) \otimes \big(2\,|0\rangle + (3-4\mathrm{i})\,|1\rangle\big) \\ &= (1+2\mathrm{i})\,|0\rangle \otimes 2\,|0\rangle + (1+2\mathrm{i})\,|0\rangle \otimes (3-4\mathrm{i})\,|1\rangle + \mathrm{i}\,|1\rangle \otimes 2\,|0\rangle + \mathrm{i}\,|1\rangle \otimes (3-4\mathrm{i})\,|1\rangle \\ &= 2(1+2\mathrm{i})\,|0.0\rangle + (1+2\mathrm{i})(3-4\mathrm{i})\,|0.1\rangle + 2\mathrm{i}\,|1.0\rangle + (4+3\mathrm{i})\,|1.1\rangle\end{aligned}$$

On note l'intérêt de la notation $|\cdot\rangle$ qui permet d'écrire les calculs de façon condensée, mais il faut bien comprendre que la justification théorique qui nous permet cette écriture est le calcul tensoriel sur les vecteurs.

## 3.4. Intrication quantique

**Définition.**

- Un 2-qubit $|\phi\rangle$ est ***non intriqué*** s'il existe deux 1-qubits $|\psi_1\rangle$ et $|\psi_2\rangle$ tels que :
$$|\phi\rangle = |\psi_1\rangle \cdot |\psi_2\rangle\,.$$
- S'il n'existe aucun $|\psi_1\rangle$ et $|\psi_2\rangle$ tels que $|\phi\rangle = |\psi_1\rangle \cdot |\psi_2\rangle$, alors le qubit $|\phi\rangle$ est dit ***intriqué***.

**Exemple.**
Le 2-qubit $|\phi\rangle$ suivant n'est pas intriqué :
$$|\phi\rangle = |0.0\rangle - |0.1\rangle + |1.0\rangle - |1.1\rangle\,.$$
En effet si on pose :
$$|\psi_1\rangle = |0\rangle + |1\rangle \qquad |\psi_2\rangle = |0\rangle - |1\rangle$$
alors
$$|\psi_1\rangle \cdot |\psi_2\rangle = (|0\rangle + |1\rangle) \cdot (|0\rangle - |1\rangle) = |0.0\rangle - |0.1\rangle + |1.0\rangle - |1.1\rangle = |\phi\rangle\,.$$

**Exemple.**
L'état de Bell $\left|\Phi^+\right\rangle$ est intriqué :
$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\,|0.0\rangle + \frac{1}{\sqrt{2}}\,|1.1\rangle$$
*Preuve.* Supposons par l'absurde que $\left|\Phi^+\right\rangle$ ne soit pas intriqué, alors il existerait $|\psi_1\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ et $|\psi_2\rangle = \alpha'\,|0\rangle + \beta'\,|1\rangle$ tels que $\left|\Phi^+\right\rangle = |\psi_1\rangle \cdot |\psi_2\rangle$, où $\alpha$, $\beta$, $\alpha'$, $\beta'$ sont des nombres complexes.
D'une part, on aurait :
$$\left|\Phi^+\right\rangle = |\psi_1\rangle \cdot |\psi_2\rangle = \alpha\alpha'\,|0.0\rangle + \alpha\beta'\,|0.1\rangle + \beta\alpha'\,|1.0\rangle + \beta\beta'\,|1.1\rangle\,.$$
Mais d'autre part $\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\,|0.0\rangle + \frac{1}{\sqrt{2}}\,|1.1\rangle$. Par identification des coefficients on obtient :
$$\begin{cases} \alpha\alpha' &= \frac{1}{\sqrt{2}} \\ \beta\beta' &= \frac{1}{\sqrt{2}} \end{cases} \quad \text{et} \quad \begin{cases} \alpha\beta' &= 0 \\ \beta\alpha' &= 0 \end{cases}.$$
Les équations de gauche impliquent que $\alpha$, $\beta$, $\alpha'$ et $\beta'$ sont tous non nuls, ce qui contredit les équations de droite. Ainsi notre hypothèse de départ est nécessairement fausse, ce qui implique qu'il ne peut exister de tels $|\psi_1\rangle$ et $|\psi_2\rangle$, c'est-à-dire que le qubit $\left|\Phi^+\right\rangle$ est intriqué.

# 4. Matrices

Nous allons voir les notions de base concernant les matrices. Nous nous concentrons en particulier sur les matrices de taille $2 \times 2$.

## 4.1. Définition

Une ***matrice*** est un tableau de nombres représenté de la manière suivante :

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,j} & \dots & a_{1,p} \\ a_{2,1} & a_{2,2} & \dots & a_{2,j} & \dots & a_{2,p} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{i,1} & a_{i,2} & \dots & a_{i,j} & \dots & a_{i,p} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n,1} & a_{n,2} & \dots & a_{n,j} & \dots & a_{n,p} \end{pmatrix} \quad \text{ou} \quad A = \left(a_{i,j}\right)_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}} \quad \text{ou} \quad \left(a_{i,j}\right).$$

Les $a_{i,j}$ seront pour nous des nombres réels ou des nombres complexes. On note $M_{n,p}(\mathbb{K})$ les matrices de taille $n \times p$ à coefficients dans $\mathbb{K}$.
Par exemple :

$$A = \begin{pmatrix} 1+\mathrm{i} & -2\mathrm{i} & 5 \\ \mathrm{i} & 0 & 1+7\mathrm{i} \end{pmatrix} \in M_{2,3}(\mathbb{C}),$$

$A$ est une matrice $2 \times 3$ à coefficients complexes.
Si $n = p$ (même nombre de lignes que de colonnes), la matrice est dite ***matrice carrée***. On note $M_n(\mathbb{K})$ au lieu de $M_{n,n}(\mathbb{K})$. Dans ce cas les éléments $a_{1,1}, a_{2,2}, \dots, a_{n,n}$ forment la ***diagonale principale*** de la matrice :

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{pmatrix}.$$

On retrouve des cas particuliers déjà rencontrés.

- Une matrice qui n'a qu'une seule ligne ($n = 1$) est appelée ***matrice ligne*** ou ***vecteur ligne***. On la note
$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,p} \end{pmatrix}.$$
- De même, une matrice qui n'a qu'une seule colonne ($p = 1$) est appelée ***matrice colonne*** ou ***vecteur colonne***. On la note
$$A = \begin{pmatrix} a_{1,1} \\ a_{2,1} \\ \vdots \\ a_{n,1} \end{pmatrix}.$$

**Définition** (Somme de deux matrices)**.**
Soient $A$ et $B$ deux matrices ayant la même taille $n \times p$. Leur ***somme*** $C = A + B$ est la matrice de taille $n \times p$ définie par

$$c_{ij} = a_{ij} + b_{ij}$$

pour $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant p$.

En d'autres termes, on somme coefficients à coefficients.
Remarque : on note indifféremment $a_{ij}$ ou $a_{i,j}$ pour les coefficients de la matrice $A$.

$$\text{Si} \quad A = \begin{pmatrix} 3+\mathrm{i} & -2 \\ 1 & 7\mathrm{i} \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} -2 & 5+2\mathrm{i} \\ 3\mathrm{i} & -\mathrm{i} \end{pmatrix} \quad \text{alors} \quad A+B = \begin{pmatrix} 1+\mathrm{i} & 3+2\mathrm{i} \\ 1+3\mathrm{i} & 6\mathrm{i} \end{pmatrix}.$$

La matrice de taille $n \times p$ dont tous les coefficients sont des zéros est appelée la ***matrice nulle*** et est notée $0_{n,p}$ ou plus simplement 0. Dans le calcul matriciel, la matrice nulle joue le rôle du nombre 0 pour les réels, c'est l'élément neutre pour l'addition.

## 4.2. Produit de matrices

**Définition** (Produit de deux matrices)**.**
Soient $A = (a_{ij})$ une matrice $n \times p$ et $B = (b_{ij})$ une matrice $p \times q$. Alors le produit $C = AB$ est une matrice $n \times q$ dont les coefficients $c_{ij}$ sont définis par :

$$\boxed{c_{ij} = \sum_{k=1}^{p} a_{ik} b_{kj}}$$

où $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant q$.

On peut écrire le coefficient général de façon plus développée, à savoir :

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ik}b_{kj} + \cdots + a_{ip}b_{pj}.$$

Il est commode de disposer les calculs de la façon suivante :

$$\begin{pmatrix} & \times & \\ & \times & \\ & \times & \\ & \times & \end{pmatrix} \leftarrow B$$

$$A \rightarrow \begin{pmatrix} & & & \\ \times & \times & \times & \times \\ & & & \end{pmatrix} \quad \begin{pmatrix} & | & \\ & | & \\ - & - & - \\ & c_{ij} & \end{pmatrix} \leftarrow AB$$

Avec cette disposition, on considère d'abord la ligne de la matrice $A$ située à gauche du coefficient que l'on veut calculer (ligne numéro $i$ représentée par des $\times$ dans $A$) et aussi la colonne de la matrice $B$ située au-dessus du coefficient que l'on veut calculer (colonne numéro $j$ représentée par des $\times$ dans $B$). On calcule le produit du premier coefficient de la ligne par le premier coefficient de la colonne ($a_{i1} \times b_{1j}$), que l'on ajoute au produit du deuxième coefficient de la ligne par le deuxième coefficient de la colonne ($a_{i2} \times b_{2j}$), que l'on ajoute au produit du troisième…

## 4.3. Exemples

**Exemple.**

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 2 \\ -1 & 1 \\ 1 & 1 \end{pmatrix}$$

On dispose d'abord le produit correctement (à gauche) : la matrice obtenue est de taille $2 \times 2$. Puis on calcule chacun des coefficients, en commençant par le premier coefficient $c_{11} = 1 \times 1 + 2 \times (-1) + 3 \times 1 = 2$ (au milieu), puis les autres (à droite).

$$\begin{pmatrix} 1 & 2 \\ -1 & 1 \\ 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 \\ -1 & 1 \\ 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 \\ -1 & 1 \\ 1 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{pmatrix} \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{pmatrix} \begin{pmatrix} 2 & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{pmatrix} \begin{pmatrix} 2 & 7 \\ 3 & 11 \end{pmatrix}$$

La matrice carrée suivante s'appelle la ***matrice identité*** :

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Ses éléments diagonaux sont égaux à 1 et tous ses autres éléments sont égaux à 0. Elle se note $I_n$ ou simplement $I$. Dans le calcul matriciel, la matrice identité joue un rôle analogue à celui du nombre 1 pour les réels. C'est l'élément neutre pour la multiplication. En d'autres termes :

**Proposition 3.**
*Si $A$ est une matrice $n \times p$, alors*

$$I_n \cdot A = A \qquad \text{et} \qquad A \cdot I_p = A.$$

## 4.4. Matrice inverse, déterminant

**Définition** (Matrice inverse)**.**
Soit $A$ une matrice carrée de taille $n \times n$. S'il existe une matrice carrée $B$ de taille $n \times n$ telle que

$$AB = I \qquad \text{et} \qquad BA = I,$$

on dit que $A$ est ***inversible***. On appelle $B$ l'***inverse de $A$*** et on la note $A^{-1}$.

Considérons le cas d'une matrice $2 \times 2$ : $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

**Proposition 4.**
*Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Si $ad - bc \neq 0$, alors $A$ est inversible et*

$$\boxed{A^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}}$$

Le nombre $ad - bc \in \mathbb{K}$ s'appelle le ***déterminant*** de la matrice $A \in M_2(\mathbb{K})$.
Plus généralement pour une matrice carrée $A \in M_n(\mathbb{K})$, il existe un scalaire $\det(A) \in \mathbb{K}$, appelé ***déterminant*** de $A$ tel que :

- si $\det(A) \neq 0$ alors la matrice $A$ est inversible ;
- $\det(AB) = \det(A) \cdot \det(B)$ ;
- $\det(I) = 1$ ;
- $\det(A^{-1}) = 1/\det(A)$, si $A$ est inversible.

Nous admettons ces propriétés et nous n'expliquons pas ici comment calculer le déterminant en général.

# 5. Matrice adjointe

Une matrice adjointe est la version complexe d'une matrice transposée.

## 5.1. La transposition

On commence par rappeler que la transposition est une opération qui transforme une matrice : les lignes de $A$ deviennent les colonnes de $A^T$.
Voici une matrice $A$ de taille $n \times p$ et sa ***matrice transposée*** notée $A^T$ qui est de taille $p \times n$ :

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1p} \\ a_{21} & a_{22} & \dots & a_{2p} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{np} \end{pmatrix} \qquad A^T = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \vdots & \vdots & & \vdots \\ a_{1p} & a_{2p} & \dots & a_{np} \end{pmatrix}.$$

Autrement dit : le coefficient à la place $(i, j)$ de $A^T$ est $a_{ji}$.

## 5.2. Matrice adjointe

Nos matrices ont des coefficients complexes, la matrice adjointe s'obtient par transposition et conjugaison complexe. On rappelle que si $a \in \mathbb{C}$, alors $a^*$ est le conjugué.

**Définition.**
On appelle ***matrice adjointe*** de $A$, de taille $n \times p$, la matrice $A^*$ de taille $p \times n$ définie par :

$$A^* = \begin{pmatrix} a_{11}^* & a_{21}^* & \dots & a_{n1}^* \\ a_{12}^* & a_{22}^* & \dots & a_{n2}^* \\ \vdots & \vdots & & \vdots \\ a_{1p}^* & a_{2p}^* & \dots & a_{np}^* \end{pmatrix}.$$

> **Exemple.**
>
> $$A = \begin{pmatrix} 1+\mathrm{i} & 2+\mathrm{i} \\ 3+\mathrm{i} & 4+\mathrm{i} \\ 5+\mathrm{i} & 6+\mathrm{i} \end{pmatrix} \qquad A^* = \begin{pmatrix} 1-\mathrm{i} & 3-\mathrm{i} & 5-\mathrm{i} \\ 2-\mathrm{i} & 4-\mathrm{i} & 6-\mathrm{i} \end{pmatrix}$$

Nous avons déjà vu le cas des vecteurs : l'adjoint d'un vecteur colonne est un vecteur ligne, et réciproquement.

$$u = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \qquad u^* = \begin{pmatrix} x_1^* & \cdots & x_n^* \end{pmatrix}$$

$$v = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} \qquad v^* = \begin{pmatrix} x_1^* \\ \vdots \\ x_n^* \end{pmatrix}$$

**Proposition 5.**
*Pour deux matrices $A$ et $B$ de tailles respectives $n \times p$ et $p \times m$ :*

$$\boxed{(A^*)^* = A \qquad (AB)^* = B^* A^*}$$

La relation $(A^*)^* = A$ signifie que l'adjointe de l'adjointe est la matrice elle-même. C'est déjà le cas pour la transposition et aussi la conjugaison complexe.
On va prouver la seconde assertion $(AB)^* = B^*A^*$. Notez bien l'inversion de l'ordre, que l'on rencontre déjà pour les inverses $(AB)^{-1} = B^{-1}A^{-1}$. On rappelle aussi que l'ordre d'un produit de matrices est important, car en général $AB \neq BA$.

*Démonstration.* On va faire la preuve pour les matrices $2 \times 2$ uniquement. Soient :

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

Alors

$$AB = \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix} \qquad (AB)^* = \begin{pmatrix} a^*\alpha^* + b^*\gamma^* & c^*\alpha^* + d^*\gamma^* \\ a^*\beta^* + b^*\delta^* & c^*\beta^* + d^*\delta^* \end{pmatrix}.$$

Et d'autre part

$$A^* = \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix} \qquad B^* = \begin{pmatrix} \alpha^* & \gamma^* \\ \beta^* & \delta^* \end{pmatrix} \qquad B^*A^* = \begin{pmatrix} a^*\alpha^* + b^*\gamma^* & c^*\alpha^* + d^*\gamma^* \\ a^*\beta^* + b^*\delta^* & c^*\beta^* + d^*\delta^* \end{pmatrix}$$

On a bien $(AB)^* = B^*A^*$. □

## 5.3. Notation bra-ket

On rappelle la notation « ket » $|\psi\rangle$ et la notation « bra » $\langle\phi|$. En posant :

$$|\psi\rangle = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \qquad \text{et} \qquad |\phi\rangle = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

alors

$$\langle\phi| = |\phi\rangle^* = \begin{pmatrix} x_1^* & \cdots & x_n^* \end{pmatrix}.$$

Calculons le produit de matrices $\langle\phi| \times |\psi\rangle$ :

$$\langle\phi| \times |\psi\rangle = \begin{pmatrix} x_1^* & \cdots & x_n^* \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = x_1^* y_1 + \cdots x_n^* y_n = \langle\phi|\psi\rangle.$$

C'est le produit d'un vecteur ligne par un vecteur colonne qui donne une matrice de taille $1 \times 1$, qu'on identifie à un nombre complexe.
Ce calcul justifie la notation « bra-ket » : le produit $\langle\phi| \times |\psi\rangle$ correspond au produit scalaire hermitien $\langle\phi|\psi\rangle$. Ainsi la notation « bra-ket » est un jeu de mots associé au « bracket » du produit scalaire hermitien (*bracket* signifie crochet).

## 5.4. Produit scalaire hermitien

**Proposition 6.**

$$\boxed{\langle Au|v\rangle = \langle u|A^*v\rangle}$$

*Démonstration.* Nous faisons la preuve uniquement pour les matrices de taille $2 \times 2$.

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad A^* = \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix} \qquad u = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \qquad v = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

$$Au = \begin{pmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \end{pmatrix} \qquad \langle Au|v\rangle = (ax_1 + bx_2)^* y_1 + (cx_1 + dx_2)^* y_2$$

$$A^*v = \begin{pmatrix} a^*y_1 + c^*y_2 \\ b^*y_1 + d^*y_2 \end{pmatrix} \qquad \langle u|A^*v\rangle = x_1^*(a^*y_1 + c^*y_2) + x_2^*(b^*y_1 + d^*y_2)$$

Ainsi

$$\langle Au|v\rangle = a^*x_1^*y_1 + b^*x_2^*y_1 + c^*x_1^*y_2 + d^*x_2^*y_2 = \langle u|A^*v\rangle\,.$$

□

# 6. Matrice unitaire

On travaille souvent avec des qubits de norme 1. Les portes logiques transforment les qubits, mais doivent tout de même transformer un qubit $|\phi\rangle$ de norme 1 en un qubit $|\psi\rangle$ de norme 1.
Lorsque cette transformation est linéaire et s'écrit $A|\phi\rangle = |\psi\rangle$, la matrice $A$ est d'un type particulier : c'est une matrice unitaire. Dans ce chapitre les exemples seront des matrices $2 \times 2$. On retrouvera le cas général dans le chapitre « Portes quantiques ».

## 6.1. Définition

**Définition.**
Une matrice $A \in M_n$ est ***unitaire*** si :

$$\boxed{A^*A = I}$$

On note $U_n$ l'ensemble des matrices unitaires de taille $n \times n$.

Si $A$ est une matrice unitaire alors on a

$$A^{-1} = A^* \qquad \text{et} \qquad AA^* = I.$$

> **Exemple.**
> Les matrices de Pauli sont les matrices unitaires suivantes :
> $$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
> Vérifier que l'on a bien $A^*A = I$. De plus pour ces exemples on a $A^* = A$.

La propriété fondamentale des matrices unitaires est qu'elles préservent le produit scalaire hermitien.

**Proposition 7.**
*Si $A$ est une matrice unitaire alors*

$$\boxed{\langle Au|Av\rangle = \langle u|v\rangle}$$

En termes de vecteurs du plan, cela signifie que l'angle entre deux vecteurs est préservé par l'action d'une matrice unitaire.


*Démonstration.*

$$\langle Au|Av\rangle = \langle u|A^*Av\rangle = \langle u|v\rangle$$

□

## 6.2. Matrice unitaire de dimension 2

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de taille $2 \times 2$. Notons cette matrice à l'aide de ses vecteurs colonnes :

$$A = \begin{pmatrix} u & v \end{pmatrix} \qquad \text{avec} \qquad u = \begin{pmatrix} a \\ c \end{pmatrix}, \quad v = \begin{pmatrix} b \\ d \end{pmatrix}.$$

**Proposition 8.**
*La matrice $A$ est unitaire si et seulement si les vecteurs $(u, v)$ forment une base orthonormale, c'est-à-dire satisfont les conditions :*

$$\|u\| = 1, \quad \|v\| = 1 \qquad \textit{et} \qquad \langle u|v\rangle = 0.$$

*Démonstration.*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad A^* = \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix}$$

$$A^*A = \begin{pmatrix} aa^* + cc^* & ba^* + dc^* \\ ab^* + cd^* & bb^* + dd^* \end{pmatrix}$$

Si $A$ est une matrice unitaire alors

$$A^*A = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

On identifie les coefficients :

$$\begin{cases} aa^* + cc^* = 1 \\ bb^* + dd^* = 1 \\ a^*b + c^*d = 0 \end{cases} \qquad \text{donc} \qquad \begin{cases} \|u\|^2 = |a|^2 + |c|^2 = 1 \\ \|v\|^2 = |b|^2 + |d|^2 = 1 \\ \langle u|v\rangle = a^*b + c^*d = 0 \end{cases}$$

On n'utilise pas l'égalité $ab^* + cd^* = 0$ qui est en fait $(a^*b + c^*d)^* = 0$.
Réciproquement, si on a les égalités $\|u\| = 1$, $\|v\| = 1$ et $\langle u|v\rangle = 0$, alors les coefficients de $A^*A$ sont les coefficients de l'identité. □

**Exemple.**
La matrice suivante est unitaire :

$$U(\theta, \phi, \lambda) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) e^{i\lambda} \\ \sin\left(\frac{\theta}{2}\right) e^{i\phi} & \cos\left(\frac{\theta}{2}\right) e^{i(\phi+\lambda)} \end{pmatrix}.$$

On vérifie que les deux vecteurs verticaux formant cette matrice sont de norme 1 et orthogonaux.

Cette transformation est disponible sous la forme d'une porte quantique.

$$\boxed{U_3(\theta,\phi,\lambda)}$$

**Proposition 9.**
*L'ensemble des matrices unitaires forme un groupe pour la multiplication. En particulier si $A,B \in U_n$ alors $AB \in U_n$ et $A^{-1} \in U_n$.*

*Démonstration.* Soient $A,B \in U_n$.

$$(AB)^*(AB) = (B^*A^*)(AB) = B^*(A^*A)B = B^*IB = B^*B = I.$$

De même, comme $A^{-1} = A^*$ :

$$(A^{-1})^*A^{-1} = (A^*)^*A^* = AA^* = I.$$

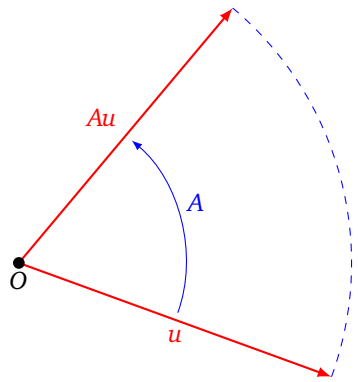
□

## 6.3. Longueur préservée

Une matrice unitaire préserve les longueurs, autrement dit si $A$ est une matrice unitaire et $u$ un vecteur alors $\|Au\| = \|u\|$. En fait cette particularité caractérise les matrices unitaires.

**Proposition 10.**
*Soit $A \in M_2$. La matrice $A$ est unitaire si et seulement pour tout vecteur $u$, on a*

$$\|Au\| = \|u\|.$$




*Démonstration.*

- Sens $\Rightarrow$.
$$\|Au\|^2 = \langle Au|Au\rangle = \langle u|A^*Au\rangle = \langle u|u\rangle = \|u\|^2.$$
- Sens $\Leftarrow$.
Notons la matrice $A$ sous la forme de ses vecteurs colonnes $A = \begin{pmatrix} u & v \end{pmatrix}$ et supposons qu'elle préserve les longueurs. Nous allons utiliser la caractérisation de la proposition 8.
  — Comme $A\binom{1}{0} = u$ et que $A$ préserve les longueurs alors
  $$\left\|A\binom{1}{0}\right\| = \left\|\binom{1}{0}\right\| \qquad \text{donc} \qquad \|u\| = 1.$$
  — De même $A\binom{0}{1} = v$, donc $\|v\| = 1$.

— D'une part $A\begin{pmatrix}1\\1\end{pmatrix} = u+v$, donc $\|u+v\| = \sqrt{2}$. Ainsi :

$$\begin{aligned}\|u+v\|^2 = 2 &\implies \langle u+v|u+v\rangle = 2\\ &\implies \langle u|u+v\rangle + \langle v|u+v\rangle = 2\\ &\implies \langle u|u\rangle + \langle u|v\rangle + \langle v|u\rangle + \langle v|v\rangle = 2\\ &\implies \|u\|^2 + \langle u|v\rangle + (\langle u|v\rangle)^* + \|v\|^2 = 2 \quad \text{mais } \|u\|^2 = 1 \text{ et } \|v\|^2 = 1\\ &\implies 2\,\mathrm{Re}\big(\langle u|v\rangle\big) = 0 \quad \text{sachant que } z+z^* = 2\,\mathrm{Re}(z)\end{aligned}$$

— D'autre part $A\begin{pmatrix}1\\\mathrm{i}\end{pmatrix} = u+\mathrm{i}v$, donc $\|u+\mathrm{i}v\| = \sqrt{2}$. Ainsi :

$$\begin{aligned}\|u+\mathrm{i}v\|^2 = 2 &\implies \langle u+\mathrm{i}v|u+\mathrm{i}v\rangle = 2\\ &\implies \langle u|u+\mathrm{i}v\rangle + \langle \mathrm{i}v|u+\mathrm{i}v\rangle = 2\\ &\implies \langle u|u\rangle + \mathrm{i}\langle u|v\rangle - \mathrm{i}\langle v|u\rangle + \langle v|v\rangle = 2\\ &\implies \|u\|^2 + \mathrm{i}\langle u|v\rangle - \mathrm{i}(\langle u|v\rangle)^* + \|v\|^2 = 2\\ &\implies 2\mathrm{i}\,\mathrm{Im}\big(\langle u|v\rangle\big) = 0 \quad \text{sachant que } z-z^* = 2\,\mathrm{Im}(z)\end{aligned}$$

— On a prouvé que la partie réelle et la partie imaginaire de $\langle u|v\rangle$ sont nulles. Ainsi $\langle u|v\rangle = 0$.
— On a donc $\|u\| = 1$, $\|v\| = 1$ et $\langle u|v\rangle = 0$, alors par la proposition 8, la matrice $A = \begin{pmatrix}u & v\end{pmatrix}$ est unitaire.

□

## 6.4. Matrice spéciale unitaire

Parmi les matrices unitaires, celles dont le déterminant vaut 1 sont particulièrement intéressantes.

**Définition.**
Une matrice $A \in M_n$ est ***spéciale unitaire*** si elle est unitaire (c'est-à-dire $A^*A = I$) et de déterminant 1 :

$$\det(A) = 1.$$

On note $SU_n$ l'ensemble des matrices spéciales unitaires de taille $n \times n$.

*Exemple.* Les matrices de Pauli (voir l'exemple plus haut) ne sont *pas* spéciales unitaires car de déterminant $-1$, par contre en multipliant tous les coefficient par i, on obtient un déterminant $+1$, donc $\mathrm{i}X, \mathrm{i}Y, \mathrm{i}Z \in SU_2$.

**Proposition 11.**
*L'ensemble des matrices spéciales unitaires forme un groupe pour la multiplication. En particulier si $A, B \in SU_n$ alors $AB \in SU_n$ et $A^{-1} \in SU_n$.*

*Démonstration.* On sait déjà que $AB$ et $A^{-1}$ sont des matrices unitaires et que de plus $\det(AB) = \det(A)\det(B) = 1$ et $\det(A^{-1}) = \frac{1}{\det(A)} = 1$. □

Dans le cas de matrices de taille $2 \times 2$, nous décrivons l'ensemble des matrices de $SU_2$.

**Proposition 12.**
*Une matrice spéciale unitaire de taille $2 \times 2$, s'écrit sous la forme*

$$A = \begin{pmatrix}\alpha & -\beta^*\\ \beta & \alpha^*\end{pmatrix} \qquad \textit{avec } \alpha, \beta \in \mathbb{C} \textit{ tels que } |\alpha|^2 + |\beta|^2 = 1.$$

*Démonstration.* Tout d'abord comme $A \in SU_2$ alors en particulier $A \in U_2$. D'après la proposition 8, $A$ s'écrit sous la forme de ses vecteurs colonnes :

$$A = \begin{pmatrix}u & v\end{pmatrix} \qquad \|u\| = 1 \qquad \|v\| = 1 \qquad \langle u|v\rangle = 0.$$

Notons $u = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$. Comme $\|u\| = 1$ alors $|\alpha|^2 + |\beta|^2 = 1$. Notons $v = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$. Comme $u$ et $v$ sont orthogonaux, car $\langle u|v\rangle = 0$, alors $\alpha^*\gamma + \beta^*\delta = 0$. Cela implique $\alpha^*\gamma = -\beta^*\delta$. Si $\alpha \neq 0$, on pose $\lambda = \frac{\delta}{\alpha^*}$. On a alors $\gamma = -\frac{\delta\beta^*}{\alpha^*} = -\lambda\beta^*$ et $\delta = \lambda\alpha^*$. (Si $\alpha = 0$ alors on a nécessairement $\beta \neq 0$ donc $\delta = 0$ et on a encore une relation $\gamma = -\lambda\beta^*$ et $\delta = \lambda\alpha^*$ avec $\lambda = -\frac{\gamma}{\beta^*}$).
Donc la matrice $A$ s'écrit :

$$A = \begin{pmatrix} \alpha & -\lambda\beta^* \\ \beta & \lambda\alpha^* \end{pmatrix}.$$

Or

$$\det(A) = \lambda\alpha\alpha^* + \lambda\beta\beta^* = \lambda(|\alpha|^2 + |\beta|^2) = \lambda.$$

Comme $\det(A) = 1$, alors $\lambda = 1$. Ainsi :

$$A = \begin{pmatrix} \alpha & -\beta^* \\ \beta & \alpha^* \end{pmatrix} \qquad \text{avec } |\alpha|^2 + |\beta|^2 = 1.$$

□

Terminons par une propriété, dite de ***transitivité***. On peut transformer un vecteur en n'importe quel autre vecteur par une matrice spéciale unitaire, à condition ques ces deux vecteurs aient la même longueur.

**Proposition 13.**
*Soient $u \in \mathbb{C}^2$ et $v \in \mathbb{C}^2$ deux vecteurs avec $\|u\| = \|v\|$. Il existe une matrice $A \in SU_2$ telle que $Au = v$.*

Une telle matrice $A$ n'est pas unique.
*Application.* Si $|\phi\rangle$ et $|\psi\rangle$ sont de norme 1, alors il existe $A \in SU_2$ telle que $|\psi\rangle = A|\phi\rangle$.

*Démonstration.* Sans perte de généralité on suppose $\|u\| = \|v\| = 1$.
*Étape 1.* Il existe $B \in SU_2$ telle que $B\begin{pmatrix} 1 \\ 0 \end{pmatrix} = u$. En effet, si on note $u = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ avec $\alpha, \beta \in \mathbb{C}$. Alors posons :

$$B = \begin{pmatrix} \alpha & -\beta^* \\ \beta & \alpha^* \end{pmatrix}$$

Comme $\|u\|^2 = |\alpha|^2 + |\beta|^2 = 1$, c'est bien une matrice spéciale unitaire : $B \in SU_2$.
Comme $B \in SU_2$, alors $B^{-1} \in SU_2$ et vérifie $B^{-1}u = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.
*Étape 2.* On reprend la construction de la première étape pour construire cette fois $C \in SU_2$ telle que $C\begin{pmatrix} 1 \\ 0 \end{pmatrix} = v$.
*Étape 3.* La matrice $A = CB^{-1}$ convient. En effet, comme $B, C \in SU_2$ alors $CB^{-1} \in SU_2$ et

$$Au = (CB^{-1})u = C(B^{-1}u) = C\begin{pmatrix} 1 \\ 0 \end{pmatrix} = v.$$

□

*Note.* Certains passages de ce chapitre sont extraits du chapitre « Matrice » du livre « Algèbre » d'Exo7.