Intro QC - 2 - Rappels mathématiques

JM.Torres - IBM Quantum Ambassador

16 avril 2023

Structures algébriques

- Un ensemble M muni d'une loi de composition interne ($M \times M \to M$), notée $\star$ est un monoïde si et seulement si, pour tout $a, b, c \in M$:
  - $a \star (b \star c) = (a \star b) \star c$: associativité
  - il existe $e \in M$, tel que $e \star a = a \star e = a$: élément neutre

- Un ensemble E muni d'une loi de composition interne ($E \times E \to E$), notée $\star$ est un groupe si et seulement si, pour tout $a, b, c \in E$:
  - $a \star (b \star c) = (a \star b) \star c$: associativité
  - il existe $e \in E$, tel que $e \star a = a \star e = a$: élément neutre
  - pour tout a il existe a' tel que $a \star a' = a' \star a = e$: inverse (ou opposé).

  Si de plus $a \star b = b \star a$ alors le groupe est commutatif ou abélien

- Un ensemble A qui est un groupe pour la loi de composition $+$, peut être muni d'une seconde loi de composition interne, notée $\times$. Alors $(A, +, \times)$ est un anneau si et seulement si pour tout $a, b, c \in A$:
  - associativité $a \times (b \times c) = (a \times b) \times c$
  - il existe $u \in A$, tel que $u \times a = a \times u = a$: élément neutre pour $\times$
  - $a \times (b + c) = (a \times b) + (a \times c)$ distributivité à gauche de $\times$ sur $+$ (et distributivité à droite).

  Si de plus $a \times b = b \times a$ alors l'anneau est commutatif

- Un ensemble K doté d'une structure d'anneau pour $+$ et $\times$ est un corps si tout élément de K sauf l'élément neutre de $+$ admet un inverse pour $\times$

Espaces Vectoriels

Vecteur

Un vecteur est "quelque chose" qui peut :

1. être multiplié par un scalaire,
2. être additionné à un autre vecteur,

Espace vectoriel

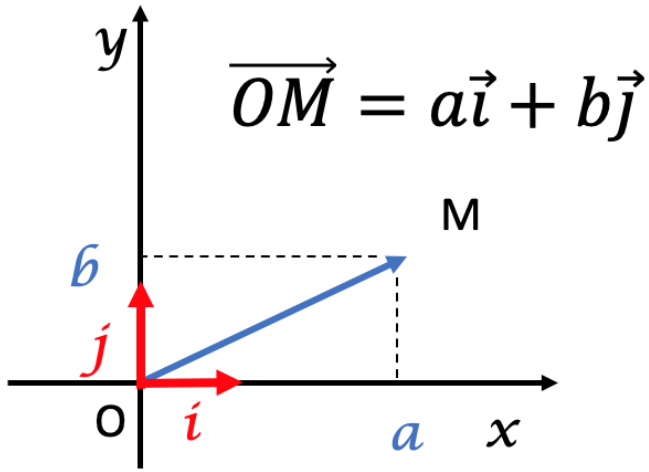
Un espace vectoriel est un ensemble dont les éléments (vecteurs) satisfont aux axiomes suivants, il est associé à un ensemble de scalaires (corps dans notre cadre).

u, v, w... sont des éléments quelconques de E, $\alpha, \beta, \gamma...$ sont des éléments quelconques du corps.

- $\alpha(u + v) = \alpha u + \alpha v$
- $u + v = v + u$
- il existe un vecteur nul (0) tel que : $v + 0 = v$
- pour tout u on a $-1 \times u$, tel que $u - u = 0$

Exemple : l'espace vectoriel associé au plan euclidien

On définit ensuite des familles libres (non liées par des relation linéaires), des bases, des coordonnées, un produit scalaire ($E \times E \to K$), pour utiliser des espaces vectoriels de manière moins abstraite, ce qui sera (presque) le cas dans le cadre du calcul quantique.
Et on arrive à cette situation bien connue :



Corps des nombres complexes

Il existe de nombreuses manières de définir les nombres complexes, la plus simple :

$\mathbb{C}$ est l'ensemble des $z = a + i.b$ avec $(a, b) \in \mathbb{R}^2$ et $i^2 = -1$

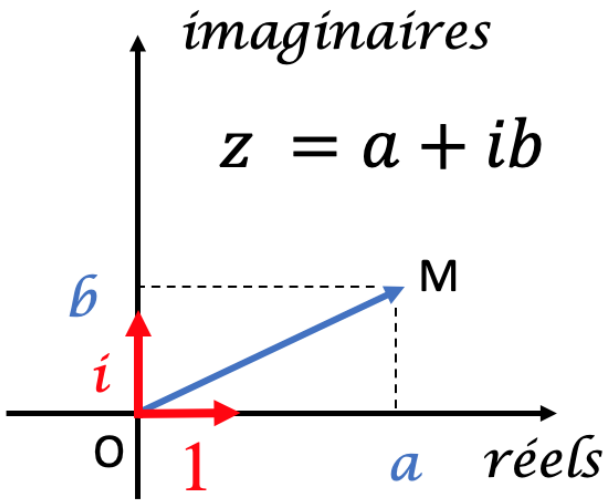
- On appelle partie réelle de z et l'on note $\Re(z)$ le nombre réel a
- On appelle partie imaginaire de z et l'on note $\Im(z)$ le nombre réel b
- On appelle nombre complexe conjugué $\bar{z}$ du nombre complexe z, on a :
  - $z + \bar{z} = 2a = 2\Re(z)$ et $z - \bar{z} = 2b = 2\Im(z)$
  - On appelle module de z et l'on note $|z|$: $|z| = \sqrt{z\bar{z}}$
  - Il est facile de constater que : $z\bar{z} = a^2 + b^2$ et donc $|z| = \sqrt{a^2 + b^2}$

Méthode plus formelle (et surtout permettant de ne pas sortir i d'un chapeau et encore moins de parler de racine carrée d'un nombre négatif) :

- soient les (a, b) de $\mathbb{R}^2$
- munis de l'addition : $(a, b) + (a', b') = (a + a', b + b')$
- munis de la multiplication définie comme suit : $(a, b) \times (a', b') = (a.a' - b.b', a.b' + a'.b)$
- alors on appelle on appelle $1 = (1, 0)$ et $i = (0, 1)$, tout le reste en découle, en particulier $i^2 = -1$, et on vérifie "facilement" que l'on a bien construit un corps (et il est algébriquement clôt)

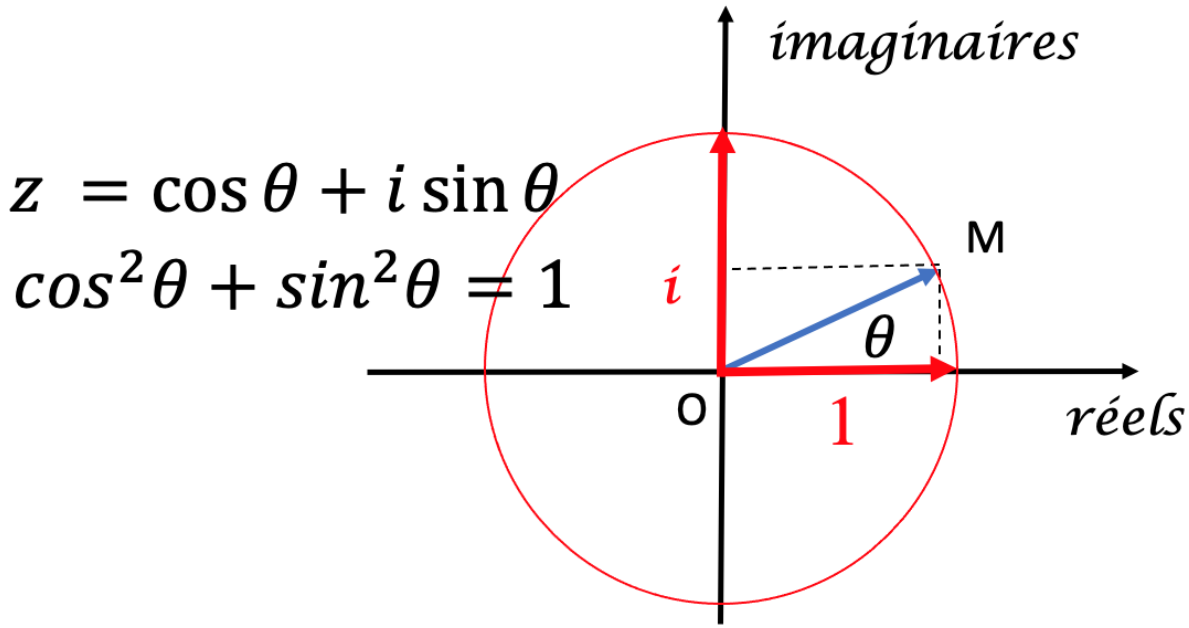
Complexes, suite

Il est courant de représenter les nombres complexes dans un plan, en identifiant z à un point M de coordonnées (a,b) si le plan est construit sur la base d'une droite d'abscisse sur laquelle tous les points sont des réels "purs" (leur partie imaginaire est nulle) et d'une droite d'ordonnée sur laquelle les points sont des nombres imaginaires "purs" (leur partie réelle est nulle), le dessin suivant explique ce concept :



Coordonnées polaires

Le point M a pour coordonnées (a, b), mais on peut aussi le repérer en coordonnées dites "polaires" avec (r, θ) où r est la distance à l'origine (et il s'agit du module tel que vu ci-dessus $(r = \sqrt{a^2 + b^2})$, et où θ est l'angle entre l'axe des abcisse et $\overrightarrow{OM}$, on a alors :
$z = a + i.b = r(cos\theta + i.sin\theta)$
que l'on peut également noter (formule d'Euler) :
$z = r.e^{i.\theta}$



Pourquoi la notation $e^{i\theta}$? (justification de la formule d'Euler)

- Formule de Taylor-Young au voisinage de 0 :
  Soit une fonction d'une variable réelle f de classe C^n :

$$f(x) = f(0) + x.f'(0)x + \frac{x^2}{2!}f''(0) + \frac{x^3}{3!}f'''(0) + .. + \frac{x^n}{n!}f^{(n)} + x^n\epsilon(x)$$

  avec $lim_{x\to 0}\epsilon(x) = 0$

- Fonction exponentielle : $exp(x)$, aussi notée e^x peut être définie comme la fonction telle qu'en tout point : $f'(x) = f(x)$ et $f(0) = 1$
  Son développement est le suivant (on voit qu'il vérifie $f'(x) = f(x)$)

$$exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + .. + \frac{x^n}{n!} + x^n\epsilon(x)$$

$$exp(x) = \sum_{x=0}^{x=n} \frac{x^n}{n!} + x^{n+1}\epsilon(x)$$

  (on admet que $0! = 1$)

Pourquoi la notation $e^{i\theta}$? (justification de la formule d'Euler)

- Développement des fonctions $\cos(x)$ et $\sin(x)$ autour de 0
  la dérivée de $\cos(x)$ est la fonction $-\sin(x)$, la dérivée de la fonction $\sin(x)$ est la fonction $\cos(x)$.
  Alors :

$$\cos(x) = \cos(0) - x\sin(0) - \frac{x^2}{2!}\cos(0) + \frac{x^3}{3!}\sin(0) + .. + \frac{x^n}{n!}f^{(n)} + x^n\epsilon(x)$$

  Il reste (avec $\cos(0) = 1$, et $\sin(0) = 0$) :

$$\cos(x) = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + .. + (-1)^n f^{(2n)}\frac{x^{2n}}{(2n)!} + x^{2n+2}\epsilon(x)$$

- Fonction *sinus* :

$$\sin(x) = \sin(0) + x\cos(0) - \frac{x^2}{2!}\sin(0) - \frac{x^3}{3!}\cos(0) + .. + (-1)^n\frac{x^{2n+1}}{(2n+1)!} + x^{2n+1}\epsilon(x)$$

  Il reste (avec $\cos(0) = 1$, et $\sin(0) = 0$) :

$$\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} + .. + (-1)^n f^{(2n)}\frac{x^{2n}}{2n!} + x^{2n+2}\epsilon(x)$$

Pourquoi la notation $e^{i\theta}$? (justification de la formule d'Euler)

En repartant du développement de e^x, en considérant le paramètre ix pour la fonction exponentielle (et bien sûr : $i^2 = -1$, $i^3 = -i$, $i^4 = 1$)

$$exp(ix) = 1+ix-\frac{x^2}{2!}-i\frac{x^3}{3!}+\frac{x^4}{4!}+i\frac{x^5}{5!}+...+\frac{x^{4n}}{(4n)!}+i\frac{x^{4n+1}}{(4n+1)!}-\frac{x^{4n+2}}{(4n+2)!}-i\frac{x^{4n+3}}{(4n+3)!}+\frac{x^{4(n+1)}}{(4(n+1))!}...$$

en séparant les termes réels des termes complexes :

$$exp(ix) = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} + ... + \frac{x^{4n}}{(4n)!} - \frac{x^{4n+2}}{(4n+2)!} + \frac{x^{4(n+1)}}{(4(n+1))!} + ...$$

$$+i(x - \frac{x^3}{3!} + \frac{x^5}{5!} + ... + \frac{x^{4n+1}}{(4n+1)!} - \frac{x^{4n+3}}{(4n+3)!} + ...)$$

on retrouve les développements de $\cos(x)$ et $\sin(x)$, ce qui permet de justifier la notation :

$$\exp(ix) = e^{ix} = \cos(x) + i\sin(x)$$

NB : il y a aussi cette surprenante explication géométrique du développement en série de $\sin x$ (et $\cos x$) : `https://www.youtube.com/watch?v=x09IsbVZeXo` , qui donne bien entendu le même résultat que Taylor-Young, mais sans l'idée de polynôme approché et de dérivée, du moins en apparence.

Par exemple dans le plan (mais aussi en plus grandes dimensions), on définit des transformations (qui à un vecteur associent un autre vecteur), à ces transformations on peut faire correspondre des matrices.
On considère un vecteur $\vec{u}$ de coordonnées (α, β)

Une matrice M à valeurs dans $\mathbb{K}$: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ permet de représenter les transformations linéaires de E (linéaires veut dire : $f(u+v) = f(u) + f(v)$ et $f(\lambda u) = \lambda f(u)$).

Alors le résultat de la transformation de matrice M sur le vecteur $\vec{u}$ est le vecteur $\vec{v} = M\vec{u}$:

$$\vec{v} = M\vec{u} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha a + \beta b \\ \alpha c + \beta d \end{pmatrix}$$

Exemples

- l'idendité, notée I_2 (en dim 2) de matrice : $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, on vérifie facilement que $M\vec{u} = \vec{u}$.
- la matrice $D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ transforme le vecteur de coordonnées (α, β) en un vecteur de coordonnées (β, α), il s'agit d'une symétrie autour de la première diagonale.
- la matrice $X = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ transforme le vecteur de coordonnées (α, β) en un vecteur de coordonnées $(\alpha, -\beta)$, il s'agit d'une symétrie par rapport à l'axe x
- tandis que celle-ci $Y = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, transforme le vecteur de coordonnées (α, β) en un vecteur de coordonnées $(-\alpha, \beta)$, il s'agit d'une symétrie par rapport à l'axe y
- enfin $C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, transforme le vecteur de coordonnées (α, β) en un vecteur de coordonnées $(-\alpha, -\beta)$, il s'agit d'une symétrie de centre O
- la matrice $P = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ transforme (α, β) en $(\alpha, 0)$, c'est la projection sur l'axe x
- la matrice $R(\theta) = \begin{pmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{pmatrix}$, produit une rotation d'angle θ

Produit de matrices

Si A et B sont deux matrices, correspondant aux transformations $\mathcal{A}$ et $\mathcal{B}$, alors le produit BA correspond à la composition des transformations $\mathcal{A}$ et $\mathcal{B}$ (dans cet ordre).

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

alors :

$$BA = \begin{pmatrix} a_{11}b_{11} + a_{21}b_{12} & a_{12}b_{11} + a_{22}b_{12} \\ a_{11}b_{21} + a_{21}b_{22} & a_{12}b_{21} + a_{22}b_{22} \end{pmatrix}$$

Nous en restons là à ce stade. Nous continuerons avec certaines propriétés des matrices dont nous aurons besoin pour les modèles de qubit et de circuit (inversible, unitaire, hermitienne...)