

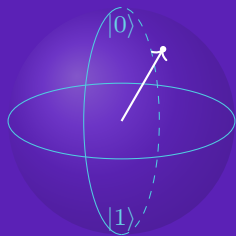
COMPUTACIÓN CUÁNTICA • UNA INTRODUCCIÓN

Capítulo 2

Fundamentos Matemáticos

Alcides Montoya Cañola

Universidad Nacional de Colombia • Sede Medellín | 2026-II



El andamiaje matemático que necesitamos

► Estados como vectores

amplitudes complejas y regla de Born

► Álgebra lineal

matrices, Dirac, producto interno

► Autovalores y observables

Pauli, Stern–Gerlach, espectral

► Hermíticas y unitarias

lo que medimos vs. lo que hacemos

► Producto tensorial

el origen del crecimiento 2^n

► Espacio de Hilbert

la arena de la mecánica cuántica

Meta del capítulo

Toda la mecánica cuántica vive en *espacios vectoriales complejos*. Aquí forjamos ese lenguaje.

Del bit clásico a la moneda en el aire

Un **bit** distingue dos estados: 0 o 1. Los codificamos como vectores:

$$\text{cara} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \text{sello} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Mientras la moneda gira, nuestra *ignorancia* se resume en un vector de probabilidad:

$$\frac{1}{2} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{1}{2} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix}$$

Cuidado

Esto es una *mezcla estadística clásica*: la moneda *siempre* tiene un valor definido; el vector solo codifica lo que no sabemos.

Las componentes son *probabilidades* y suman 1.

El hábito conceptual más importante

Mezcla clásica

El sistema *sí* tiene un valor definido; solo lo ignoramos.

Componentes = **probabilidades**

$$p_0 + p_1 = 1$$

Superposición cuántica

El sistema *no* tiene valor definido antes de medir.

Componentes = **amplitudes** complejas

$$|\alpha|^2 + |\beta|^2 = 1$$

Confundirlas es el error más común en las divulgaciones de lo cuántico.

Por qué la Naturaleza exige números complejos

En la **doble rendija**, sin observar por cuál pasa el electrón, surge un patrón de *interferencia*:

Amplitudes que se cancelan

$$P = |\psi_1 + \psi_2|^2 = |\psi_1|^2 + |\psi_2|^2 + \underbrace{2 \operatorname{Re}[\psi_1^* \psi_2]}_{\text{interferencia}}$$

El último término *no existe* en la probabilidad clásica.



Cancelación (destructiva) y refuerzo (constructiva)
según la *fase*.

? Pausa socrática #1 — probabilidad vs. amplitud

- ▶ ¿Por qué la Naturaleza “elevaría al cuadrado” una amplitud para darnos una probabilidad?
- ▶ Si dos caminos pueden *cancelarse*, ¿en qué sentido el electrón “recorrió” alguno?
- ▶ ¿Podrías construir un mundo con amplitudes *reales* negativas, sin números complejos? ¿Qué perderías?



La regla de Born — el puente a lo medible

Densidad de probabilidad

$$P(x) = |\psi(x)|^2 = \psi^*(x) \psi(x) \geq 0, \quad \int_{\mathbb{R}^3} |\psi|^2 dV = 1$$

- ▶ $|\psi|^2$ es real y no negativo, aunque ψ sea complejo.
- ▶ Para un qubit $\alpha|0\rangle + \beta|1\rangle$: se mide $|0\rangle$ con prob. $|\alpha|^2$, $|1\rangle$ con $|\beta|^2$.

La clave algorítmica

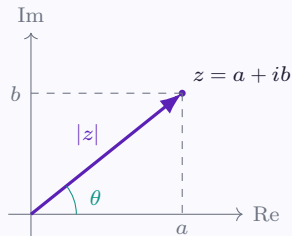
Las *fases* de α, β no se ven en una medición, pero gobiernan la *interferencia* que amplifica las respuestas correctas.

Repaso exprés: números complejos

Tres formas del mismo número

$$z = a + ib = r(\cos \theta + i \sin \theta) = r e^{i\theta}$$

- Unidad imaginaria: $i^2 = -1$ (Descartes la llamó “imaginaria”).
- Fórmula de Euler: $e^{i\theta} = \cos \theta + i \sin \theta$.
- Módulo: $|z| = \sqrt{a^2 + b^2} = r$, $|z|^2 = z z^*$.



Operaciones que usaremos sin cesar

- ▶ Conjugado: $z^* = a - ib = r e^{-i\theta}$
- ▶ Producto (polar):
 $(r e^{i\theta})(r' e^{i\theta'}) = r r' e^{i(\theta+\theta')}$
- ▶ Módulo al cuadrado: $|z|^2 = z z^*$
- ▶ Inverso: $\frac{1}{z} = \frac{z^*}{|z|^2}$
- ▶ De Moivre: $z^n = |z|^n [\cos(n\theta) + i \sin(n\theta)]$

Puente con la IA. El producto en forma polar dice que multiplicar por $e^{i\theta}$ es *rotar*.^{AI} Toda la computación cuántica es una coreografía de rotaciones de fase — el análogo de mover vectores en el espacio de *embeddings* de un modelo moderno.

? Pausa socrática #2 — la fase escondida

Una fase global $e^{i\theta}$ no cambia ninguna probabilidad $|z|^2$.



- ▶ Entonces, ¿es la fase “real” o un artefacto matemático?
- ▶ Si nunca puedo medir una fase global, ¿por qué las fases *relativas* sí importan?
- ▶ ¿Qué tiene la Naturaleza que prefiere el círculo ($e^{i\theta}$) y no la recta?

Sección 2.2

Álgebra Lineal — el Lenguaje

Matrices: conjugada, transpuesta y adjunta

► Conjugada: $(A^*)_{ij} = (A_{ij})^*$

► Transpuesta: $(A^T)_{ij} = A_{ji}$

► **Adjunta (daga):** $A^\dagger = (A^*)^T$

► $(A^T)^T = A$, $(MN)^T = N^T M^T$

► $(MN)^\dagger = N^\dagger M^\dagger$

► Si $M^T = M$: *simétrica*; si $M^T = -M$: *antisimétrica*.

Ejemplo 2×2

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}^\dagger = \begin{bmatrix} a_{11}^* & a_{21}^* \\ a_{12}^* & a_{22}^* \end{bmatrix}$$

La daga $\dagger$ se reserva *siempre* para la adjunta — de matrices y de operadores.

Multiplicación de matrices — y la no conmutatividad

Producto fila por columna

$$C_{ik} = \sum_{j=1}^m A_{ij} B_{jk} \quad (\text{columnas de } A = \text{filas de } B)$$

Asociativa, distributiva, pero en general:

$$AB \neq BA$$

Física escondida

La *no conmutatividad* de los observables está en el corazón de las relaciones de incertidumbre. No es un estorbo: es física.

Notación de Dirac: bra y ket

- ▶ **Ket** $|\psi\rangle$: vector columna (estado).
- ▶ **Bra** $\langle\psi| = |\psi\rangle^\dagger$: vector fila conjugado.
- ▶ **Producto interno** $\langle\phi|\psi\rangle \in \mathbb{C}$: *amplitud* de transición.

$$\langle u|v\rangle = \sum_i a_i^* b_i, \quad |\langle\phi|\psi\rangle|^2 = \text{probabilidad}$$

Puente con la IA. $\langle\phi|\psi\rangle$ es un *producto punto*: mide cuánto se parecen dos estados — la misma operación de “similitud” que puntúa consultas contra claves en la *atención* de un Transformer.

? Pausa socrática #3 — el producto interno

$\langle \phi | \psi \rangle$ es la amplitud de que un sistema en $|\psi\rangle$ “se encuentre” en $|\phi\rangle$. ?

- ▶ Si $\langle \phi | \psi \rangle = 0$, ¿qué relación física tienen los dos estados?
- ▶ ¿Por qué el bra lleva conjugado y el ket no? ¿Qué se rompería si no?
- ▶ ¿Puede una amplitud ser mayor que 1? ¿Y una probabilidad?

El qubit en notación de Dirac

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \quad \langle\psi| = \alpha^* \langle 0| + \beta^* \langle 1|$$

Normalización

$$\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$$

- ▶ Norma: $\| |v\rangle \| = \sqrt{\langle v|v\rangle}$.
- ▶ Ortogonalidad: $\langle u|v\rangle = 0$.
- ▶ Cauchy-Schwarz:
 $|\langle u|v\rangle| \leq \| |u\rangle \| \| |v\rangle \|$.

Producto interno: sesquilineal y completitud

► **Lineal en el ket:**

$$\langle u | c_1 v_1 + c_2 v_2 \rangle = c_1 \langle u | v_1 \rangle + c_2 \langle u | v_2 \rangle$$

► **Antilineal en el bra:** las constantes salen conjugadas $\Rightarrow$ forma *sesquilineal*.

► **Simetría hermítica:** $\langle u | v \rangle = \langle v | u \rangle^*$.

Base ortonormal y completitud

$$\langle e_i | e_j \rangle = \delta_{ij}, \quad \sum_i |e_i\rangle \langle e_i| = I$$

La relación de completitud deja *insertar identidades* I a voluntad — el truco de cálculo más usado.

Bases: estándar y computacional

Base **computacional** de $\mathbb{C}^2$ (etiquetas desde 0):

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Base **de Hadamard** (diagonal):

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad |-\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

Idea clave

Un mismo estado tiene *muchas* representaciones — una por base. Cambiar de base es cambiar la *pregunta* que le hacemos al sistema.

Para n qubits la base tiene 2^n elementos $|i\rangle$.

Producto externo y proyectores

El **producto externo** $|\phi\rangle \langle\psi|$ es una *matriz* (un operador):

$$(|\phi\rangle \langle\psi|) |\chi\rangle = \langle\psi|\chi\rangle |\phi\rangle$$

Proyector

$$P = |\psi\rangle \langle\psi|, \quad P^2 = P \text{ (idempotente)}$$

► $P^2 = |\psi\rangle \underbrace{\langle\psi|\psi\rangle}_{=1} \langle\psi| = P.$

- Los proyectores *modelan la medición*:
dejan el sistema en $P|\chi\rangle$ con prob.
 $|\langle\psi|\chi\rangle|^2.$

Se formaliza en los postulados del Capítulo 3.

? Pausa socrática #4 — medir es proyectar

Si medir es aplicar un proyector $P = |\psi\rangle \langle\psi|$ y renormalizar:



- ▶ ¿Por qué la medición *no* es reversible, si casi todo lo demás en cuántica sí lo es?
- ▶ Tras medir y obtener $|\psi\rangle$, medir de nuevo da lo mismo. ¿Dónde se “fue” la superposición?
- ▶ ¿Quién o qué decide *cuándo* ocurre una medición?

Sección 2.3

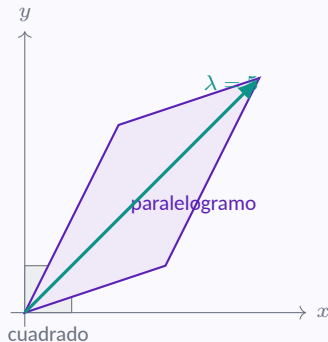
Autovalores, Hermíticas y Unitarias

Autovalores y autovectores — la intuición

Un **autovector** no cambia de dirección bajo la matriz; solo se escala por el **autovalor**:

$$A|v\rangle = \lambda|v\rangle$$

Ejemplo: $A = \begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix}$ lleva el cuadrado a un paralelogramo, pero $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ solo se dilata $\times 5$.



Cómo hallarlos: el polinomio característico

Ecuación característica

$$\det(A - \lambda I) = 0 \quad \Rightarrow \quad p(\lambda) = \lambda^2 - \lambda \operatorname{tr}(A) + \det(A) \quad (2 \times 2)$$

- ▶ Los autovectores resuelven $(A - \lambda_k I) |v\rangle = 0$.
- ▶ Toda matriz compleja $n \times n$ tiene al menos un autovalor (teorema fundamental del álgebra).

Por qué nos importa

En física, los autovalores son los *posibles resultados* de una medición, y los autovectores, los *estados* asociados.

? Pausa socrática #5 — resultados discretos

La medición solo puede arrojar un *autovalor*.



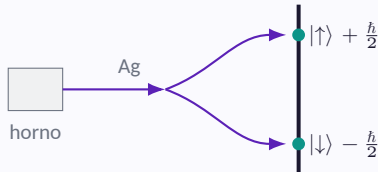
- ▶ ¿Por qué la Naturaleza “elige” un conjunto discreto de resultados y no un continuo?
- ▶ ¿Qué significa que un estado *no* sea autovector del observable que medimos?
- ▶ Si los autovalores deben ser reales, ¿qué le exige eso a la matriz?

Stern-Gerlach (1922): el espín se cuantiza

- ▶ Un haz de átomos de plata cruza un campo magnético *no uniforme*.
- ▶ Clásicamente: una mancha *continua*. El experimento: **dos** manchas discretas.
- ▶ Interpretación (1925): **espín** $\pm \hbar/2$ — un grado de libertad puramente cuántico.

El prototipo del qubit

El espacio de estados de dos niveles $\{|\uparrow\rangle, |\downarrow\rangle\}$ es el qubit.



Las matrices de Pauli

Tres observables de espín (en unidades de $\hbar/2$)

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- ▶ Son **hermíticas**: $\sigma_k = \sigma_k^\dagger$.
- ▶ Autovalores ± 1 : los dos resultados de medir espín.
- ▶ Junto con $\sigma_0 = I$ generan *toda* matriz hermítica 2×2 .
- ▶ Reaparecen como compuertas X, Y, Z .

Ejemplo resuelto: autovectores de σ_y

Aplicando $\sigma_y |\psi\rangle = \lambda |\psi\rangle$ a $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$:

$$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} -i\beta \\ i\alpha \end{bmatrix} = \lambda \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$p(\lambda) = \lambda^2 - 1 \Rightarrow \lambda = \pm 1$. Resolviendo cada caso:

$$|+i\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix}, \quad |-i\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \end{bmatrix}$$

Verificación de la teoría

Autovalores *reales* (± 1) y autovectores *ortogonales*:

$$\langle +i | -i \rangle = \frac{1}{2}(1 - 1) = 0$$

justo lo que garantiza la hermiticidad.

Cada Pauli define una base del qubit

Matriz	Autovalor +1	Autovalor -1	Nombres
σ_x	$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$	$ +\rangle, -\rangle$
σ_y	$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix}$	$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \end{bmatrix}$	$ +i\rangle, -i\rangle$
σ_z	$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$ 0\rangle, 1\rangle$

Cada par es una base ortonormal de $\mathbb{C}^2$; la de σ_z es la base computacional.

? Pausa socrática #6 — tres direcciones incompatibles



$\sigma_x, \sigma_y, \sigma_z$ *no* conmutan entre sí.

- ▶ ¿Qué significa físicamente que no compartan autovectores?
- ▶ Si mido el espín en z y luego en x , ¿por qué “pierdo” la información de z ?
- ▶ ¿Es la incertidumbre una limitación del aparato, o de la Naturaleza misma?

Matrices hermíticas: dos teoremas centrales

Definición

$$A = A^\dagger \quad (\text{hermítica})$$

1. **Autovalores reales:** de $A|v\rangle = \lambda|v\rangle$,
 $\lambda = \langle v|Av\rangle = \lambda^*$.
2. **Autovectores ortogonales** si $\lambda_m \neq \lambda_n$:
 $(\lambda_m - \lambda_n) \langle \phi_n | \phi_m \rangle = 0$.

Por qué observables = hermíticos

Toda medición física da un *número real*. La hermiticidad *garantiza* autovalores reales. Los dos teoremas trabajan juntos.

Normales, teorema espectral y la esfera de Pauli

Matriz normal

$$AA^\dagger = A^\dagger A$$

Teorema espectral: una matriz admite base ortonormal de autovectores *si y solo si* es normal.
(Hermíticas y unitarias lo son.)

Hermíticas 2×2 = espacio real 4D

$$H = h_0\sigma_0 + h_x\sigma_x + h_y\sigma_y + h_z\sigma_z$$

$$\text{con } h_0, h_x, h_y, h_z \in \mathbb{R}$$

Base de los hamiltonianos y compuertas de un qubit.

Matrices unitarias — lo que podemos *hacer*

Definición

$$UU^\dagger = U^\dagger U = I \quad \Longleftrightarrow \quad U^{-1} = U^\dagger$$

- ▶ **Preservan el producto interno** y la norma:
 $\|U|v\rangle\| = \||v\rangle\|.$
- ▶ Autovalores de módulo 1: $e^{i\theta}$.
- ▶ Producto de unitarias es unitario $\Rightarrow$ un circuito entero es *una* unitaria.

Hermíticas vs. unitarias

Hermíticas = lo que *medimos* (observables).

Unitarias = lo que *hacemos* (evolución, compuertas).

? Pausa socrática #7 — conservar la probabilidad

Toda operación cuántica cerrada preserva la norma (la probabilidad total $= 1$). ?

- ▶ ¿Por qué la Naturaleza *insiste* en que nada se pierda hasta que medimos?
- ▶ Si toda compuerta es reversible ($U^{-1} = U^\dagger$), ¿cómo puede un algoritmo “borrar” respuestas incorrectas?
- ▶ ¿Es la irreversibilidad de la computación clásica un defecto o una comodidad?

Compuertas cuánticas = matrices unitarias

Hadamard — crea superposición

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$$

Pauli-X — el NOT cuántico

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} : |0\rangle \leftrightarrow |1\rangle$$

CNOT — enlaza dos qubits

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Si el control es $|1\rangle$, invierte el objetivo. Es la puerta que *crea entrelazamiento*.

Reversibilidad, no-clonación y evolución

Teorema de no-clonación

No existe una unitaria que copie un estado *desconocido* arbitrario (Wootters–Zurek, Dieks, 1982).

Da seguridad a BB84 y prohíbe “respaldar” estados intermedios.

Evolución temporal

$$|\psi(t)\rangle = U(t) |\psi(0)\rangle, \quad U(t) = e^{-iHt/\hbar}$$

Aquí se *encuentran* las dos familias: toda **hermítica** H genera, al exponenciar, una **unitaria** U .

Descomposición espectral

Toda matriz normal se descompone así

$$A = \sum_i \lambda_i |v_i\rangle \langle v_i|, \quad U^\dagger A U = D = \text{diag}(\lambda_1, \dots, \lambda_n)$$

Ejemplo: $H = \begin{bmatrix} 3 & 1 \\ 1 & 3 \end{bmatrix}$, $\lambda_1 = 4$, $\lambda_2 = 2$:

$$H = 4 |v_1\rangle \langle v_1| + 2 |v_2\rangle \langle v_2|$$

$$\text{con } |v_1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad |v_2\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}.$$

Interpretación física

λ_i = resultados posibles; $|v_i\rangle \langle v_i|$ = proyectores de la medición. Diagonalizar un hamiltoniano da las *energías* y los *estados estacionarios*.

? Pausa socrática #8 — cambiar de base lo aclara todo

En la base de autovectores, un operador solo *escala* cada componente. ?

- ▶ ¿Por qué “diagonalizar” se siente como *entender* el operador?
- ▶ Si $U(t) = e^{-iHt/\hbar}$, ¿qué le pasa a un autovector de H con el tiempo?
- ▶ ¿Existe siempre una base donde el problema sea trivial? ¿Cuándo no?

Producto tensorial — el origen del 2^n

Combinar dos qubits

$$\begin{bmatrix} x_0 \\ x_1 \end{bmatrix} \otimes \begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} x_0 y_0 \\ x_0 y_1 \\ x_1 y_0 \\ x_1 y_1 \end{bmatrix}$$

La raíz del poder — y del reto

n qubits $\Rightarrow$ espacio de dimensión 2^n .
Esa explosión es la ventaja cuántica y, a la vez, lo que hace intratable la simulación clásica.

- ▶ Las dimensiones se *multiplican*:
 $\mathbb{C}^n \otimes \mathbb{C}^m = \mathbb{C}^{nm}$.
- ▶ $|1\rangle \otimes |1\rangle \otimes |0\rangle = |110\rangle$ (se concatenan las etiquetas).

Entrelazamiento: cuando el todo no se factoriza

- ▶ No todo estado de $\mathbb{C}^4$ es un producto $|a\rangle \otimes |b\rangle$ de dos qubits.
- ▶ Los estados que *no* factorizan se llaman **entrelazados** — el recurso clave de muchos algoritmos.

Puente con la IA. El álgebra lineal de este capítulo es *exactamente* la maquinaria del aprendizaje profundo: vectores, productos internos, matrices. La diferencia es el tamaño del espacio — un modelo grande vive en $\mathbb{R}^d$ con d de miles; n qubits viven en $\mathbb{C}^{2^n}$, exponencial en n . AI

Operadores, conmutador y valor esperado

Conmutador

$$[\hat{A}, \hat{B}] \equiv \hat{A}\hat{B} - \hat{B}\hat{A}$$

$[\hat{B}, \hat{A}] = -[\hat{A}, \hat{B}]$,
 $[\hat{A}, \hat{B}\hat{C}] = [\hat{A}, \hat{B}]\hat{C} + \hat{B}[\hat{A}, \hat{C}]$. Si $[\hat{A}, \hat{B}] \neq 0$, los observables son *incompatibles*.

Valor esperado

$$\langle A \rangle = \langle \psi | \hat{A} | \psi \rangle$$

Es el promedio de resultados, pesado por sus probabilidades. Exigir $\langle A \rangle = \langle A \rangle^*$ para todo ψ define los operadores hermíticos.

? Pausa socrática #9 — el promedio de lo que nunca es promedio

El valor esperado $\langle A \rangle$ puede ser un número que *nunca* sale en una medición (p. ej. 0 para autovalores ± 1). ?

- ▶ ¿Qué significa entonces “el valor esperado”?
- ▶ ¿Cuántas mediciones (*shots*) necesito para estimarlo bien? (recuerda $\mathcal{O}(\epsilon^{-2})$).
- ▶ ¿Es el conmutador $[\hat{A}, \hat{B}]$ una propiedad de los operadores o del mundo?

Secciones 2.4–2.5

El Espacio de Hilbert

Espacio de Hilbert — la arena formal

Un espacio vectorial complejo con producto interno, y completo

Producto interno $\langle \cdot | \cdot \rangle : \mathcal{H} \times \mathcal{H} \rightarrow \mathbb{C}$ con: lineal en el ket, simetría hermítica $\langle x | y \rangle = \langle y | x \rangle^*$, y $\langle x | x \rangle \geq 0$ ($=0$ sii $x = 0$).

- ▶ Componentes *complejas* (no reales).
- ▶ “Completo”: toda sucesión de Cauchy converge — irrelevante en dimensión finita.

Hilbert (1912), von Neumann (1927–32) le dio la axiomática y acuñó el nombre; Dirac aportó el lenguaje bra-ket.

¿Por qué este espacio y no otro?

Cada rasgo de Hilbert responde a una necesidad física:

Amplitudes complejas → interferencia

Suma de vectores → superposición

Producto interno → regla de Born
 $|\langle \phi | \psi \rangle|^2$

Ortogonalidad → resultados excluyentes

Unitariedad → conserva la probabilidad

Operadores hermíticos → valores reales

Hilbert en computación cuántica

El espacio de n qubits

$$\mathcal{H} = \mathbb{C}^{2^n} \quad \text{dimensión} = 2^n$$

- ▶ 1 qubit $\rightarrow \mathbb{C}^2$; 2 qubits $\rightarrow \mathbb{C}^4$, base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.
- ▶ Compuerta de n qubits: unitaria $2^n \times 2^n$.

El álgebra de los circuitos

Todo el modelo de circuitos se reduce a *multiplicar matrices* en $\mathcal{H}$. La maquinaria de este capítulo es, literalmente, la herramienta de diseño de algoritmos.

Capítulo 2 — qué llevarse

- ▶ Mezcla clásica $\neq$ superposición: probabilidades vs. *amplitudes*.
- ▶ La notación de Dirac vuelve elegante todo el álgebra lineal.
- ▶ **Hermíticas** = observables (autovalores reales); **unitarias** = evolución (reversible).
- ▶ Pauli + Stern–Gerlach: donde la abstracción toca el laboratorio.
- ▶ El producto tensorial explica el crecimiento 2^n y el entrelazamiento.
- ▶ Todo vive en el **espacio de Hilbert** $\mathbb{C}^{2^n}$.

Preguntas para llevar al Capítulo 3

- ▶ Ya tenemos el *lenguaje*. ¿Qué *postulados* convierten estas matrices en física?
- ▶ Si la evolución es $U(t) = e^{-iHt/\hbar}$, ¿de dónde sale el hamiltoniano H de un sistema real?
- ▶ La medición rompe la unitariedad. ¿Es un postulado aparte, o algo más profundo?

¡Nos vemos en el Capítulo 3 — Mecánica Cuántica!