Mathematics for Quantum Computing

A Structured Reference from Lecture Notes

Sakinah Faiza Hussain

February 23, 2026

Contents

Chapter 1

Algebraic Structures

This chapter develops the hierarchy of algebraic structures — from the most primitive (groupoids) to the richest (fields) — that underpin the mathematics of quantum computing. Every structure is a non-empty set equipped with one or more binary operations satisfying progressively stronger axioms.

1.1 Binary Operations and Closure

Definition 1.1.1 (Binary Operation)**.** Let R be a non-empty set. A *binary operation* $*$ on R is a map

$$* : R \times R \longrightarrow R, \qquad (a, b) \mapsto a * b.$$

The operation is said to satisfy the *closure property* if

$$\forall\, a, b \in R \implies a * b \in R.$$

Remark 1.1.1. An algebraic structure $(R, *_1, *_2, \ldots)$ consists of a non-empty set R together with one or more binary operations. Closure is automatic by definition of a binary operation, but it is often stated explicitly for emphasis.

Example 1.1.1. Consider the integers $\mathbb{Z}$ under addition. For any $x \in \mathbb{Z}$ we have $1 \cdot x = x \in \mathbb{Z}$, confirming closure. The step-by-step justification that $2x + (y - x) = x + y$ uses commutativity, associativity, the distributive property, and the multiplicative identity:

$$\begin{aligned}
2x + (y - x) &= 2x + (y + (-x)) && \text{(additive inverse notation)} \\
&= 2x + ((-x) + y) && \text{(commutativity of $+$)} \\
&= (2x + (-x)) + y && \text{(associativity of $+$)} \\
&= (2x + (-1)x) + y && \text{(notation: $-x = (-1)x$)} \\
&= (2 + (-1))x + y && \text{(distributive property)} \\
&= 1x + y && \text{(closure in $\mathbb{Z}$)} \\
&= x + y. && \text{(multiplicative identity)} \quad \square
\end{aligned}$$

1.2 The Algebraic Hierarchy

The following definitions build on one another; each adds one axiom to the previous structure.

Definition 1.2.1 (Groupoid)**.** A non-empty set R with a binary operation $*$ satisfying closure is called a *groupoid*.

Definition 1.2.2 (Semigroup)**.** A groupoid $(R, *)$ that additionally satisfies

- **Associativity:** $\forall\, a, b, c \in R, \quad (a * b) * c = a * (b * c)$

is called a *semigroup*.

Definition 1.2.3 (Monoid)**.** A semigroup $(R, *)$ that additionally contains an *identity element* $e \in R$ satisfying

$$a \,\square\, e = e \,\square\, a = a \quad \forall\, a \in R$$

is called a *monoid*.

Definition 1.2.4 (Group)**.** A monoid $(R, *)$ in which every element has an *inverse*, i.e.,

$$\forall\, a \in R\; \exists\, a^{-1} \in R \text{ such that } a * a^{-1} = a^{-1} * a = e,$$

is called a *group*.

Definition 1.2.5 (Abelian (Commutative) Group)**.** A group $(R, *)$ satisfying

- **Commutativity:** $\forall\, a, b \in R, \quad a * b = b * a$

is called an *Abelian group*.

1.3 Rings

Definition 1.3.1 (Ring)**.** A triple $(R, +, \cdot)$ is a *ring* if $(R, +)$ is an Abelian group, multiplication $\cdot$ is associative and closed, and the distributive laws hold:

$$(a + b) \cdot c = a \cdot c + b \cdot c,$$
$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Concretely, the twelve axioms are:

1. **Closure under $+$:** $a, b \in R \Rightarrow a + b \in R$.
2. **Associativity of $+$:** $(a + b) + c = a + (b + c)$.
3. **Additive identity:** $\exists\, 0 \in R$ s.t. $a + 0 = 0 + a = a$.
4. **Additive inverse:** $\forall\, a \in R\; \exists\, {-a} \in R$ s.t. $a + (-a) = 0$.
5. **Commutativity of $+$:** $a + b = b + a$.
6. **Closure under $\cdot$:** $a, b \in R \Rightarrow a \cdot b \in R$.
7. **Associativity of $\cdot$:** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
8. **Multiplicative identity** (if present): $\exists\, 1 \in R$ s.t. $a \cdot 1 = 1 \cdot a = a$.
9. **Multiplicative inverse** (if present): $\forall\, a \neq 0\; \exists\, a^{-1}$ s.t. $a \cdot a^{-1} = 1$.

10. **Commutativity of** $\cdot$ (if present): $a \cdot b = b \cdot a$.
11. **Distributivity:** $(a+b)c = ac + bc$ and $a(b+c) = ab + ac$.
12. **Non-triviality:** $0 \neq 1$ (excludes the trivial ring; also forces uniqueness of identity and inverses).

Definition 1.3.2 (Ring with Unity)**.** A ring satisfying axiom 8 (multiplicative identity) is called a *ring with unity.*

Definition 1.3.3 (Commutative Ring with Unity)**.** A ring with unity that also satisfies axiom 10 (commutativity of $\cdot$) is called a *commutative ring with unity.*

1.4 Fields

Definition 1.4.1 (Field)**.** A *field* $(F, +, \cdot)$ is a set F with two binary operations satisfying all twelve ring axioms (including multiplicative identity, multiplicative inverses for non-zero elements, and commutativity of multiplication). Equivalently:

$$\text{Field} = \text{Abelian group under } + \ \cup \ \text{Abelian group under } \cdot \ \cup \ \text{Distributivity} \ \cup \ (0 \neq 1).$$

Example 1.4.1. The classical fields are:

$$\mathbb{R}\ (\mathbb{R} \setminus \{0\}), \quad \mathbb{C}\ (\mathbb{C} \setminus \{0\}), \quad \mathbb{Q}\ (\mathbb{Q} \setminus \{0\}).$$

1.4.1 Field Extensions

Definition 1.4.2 (Field Extension)**.** Let F and K be fields with $F \subseteq K$. Then K is an *extension field* of F, written K/F.

Example 1.4.2 ($\mathbb{Q}(\alpha)$)**.** Since $\sqrt{2} \notin \mathbb{Q}$, the smallest field containing both $\mathbb{Q}$ and $\sqrt{2}$ is

$$\mathbb{Q}(\sqrt{2}) = \{\, a + b\sqrt{2} : a, b \in \mathbb{Q} \,\}.$$

This is an *algebraic extension* of $\mathbb{Q}$ and forms an Abelian group under both $+$ and $\cdot$, satisfies distributivity, and has $0 \neq 1$.

Definition 1.4.3 (Extended Field $F(x)$)**.** Given a field F, the field of *rational functions* over F is

$$F(x) = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f, g \text{ polynomials with coefficients in } F,\ g \neq 0 \right\}.$$

In particular, $\mathbb{R}(i) = \mathbb{C}$ (extended reals via the imaginary unit $i = \sqrt{-1}$) and $\mathbb{C}(x)$ consists of rational functions with complex coefficients, e.g. $\dfrac{ix+3}{3-ix^3}$.

Remark 1.4.1. There are infinitely many extension fields of $\mathbb{Q}$, one for each algebraic (or transcendental) element adjoined.

Chapter 2

Linear Transformations and Systems of Equations

2.1 Systems of Linear Equations

A system of linear equations can have three qualitatively different solution sets, visualised geometrically as intersecting lines in $\mathbb{R}^2$:

1. **Unique solution** — lines intersect at exactly one point.
2. **No solution** — lines are parallel and distinct.
3. **Infinitely many solutions** — lines coincide.

Example 2.1.1.

$$\begin{cases} x + y = 6 \\ 2x - y = 3 \end{cases} \xrightarrow{\text{subtract}} -x = 3 \implies x = -3,\ y = 9.$$

Unique solution. □

2.2 Matrix Notation (Cayley)

A system of m equations in n unknowns is written compactly as

$$A\mathbf{x} = \mathbf{b},$$

where A is an $m \times n$ matrix, $\mathbf{x}$ is the $n \times 1$ column of unknowns, and $\mathbf{b}$ is the $m \times 1$ right-hand-side vector.

Example 2.2.1.

$$\begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 6 \\ 4 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 1 \\ 1 & -3 & 1 \\ 2 & -1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \\ 5 \end{pmatrix}.$$

The matrix is *responsible for the transformation* of the solution space.

2.3 Linear Transformations

Definition 2.3.1 (Linear Transformation)**.** Let V and W be vector spaces over the same field F. A map $T : V \to W$ is a *linear transformation* if it preserves the vector space structure:

$$T(\mathbf{u}+\mathbf{v}) = T(\mathbf{u}) + T(\mathbf{v}) \qquad \forall\, \mathbf{u},\mathbf{v} \in V, \tag{2.1}$$

$$T(\gamma\,\mathbf{u}) = \gamma\, T(\mathbf{u}) \qquad \forall\, \mathbf{u} \in V,\ \gamma \in F. \tag{2.2}$$

Example 2.3.1 (Geometric transformations on $\mathbb{R}^2$)**.** Define

$$T(x,y) = (x,y), \qquad T(x,y) = (x+y,\ 2x-y).$$

The second map sends integer-lattice points to a *tilted* lattice — a square grid becomes a tilted rectangle. This geometric distortion is the hallmark of a non-trivial linear transformation.

2.3.1 Reflections as Linear Transformations

Example 2.3.2. Define the two maps $G, H : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$G(x,y) = (x,\ -y), \qquad H(x,y) = (y,\ -x).$$

Their matrix representations are

$$G = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad H = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

The composition GH satisfies

$$(GH)(x,y) = G(H(x,y)) = G(y,-x) = (y,x),$$

so

$$GH = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x \end{pmatrix}.$$

Verification: $GH(1,2)$: first $H(1,2) = (2,-1)$, then $G(2,-1) = (2,1)$. □

2.4 Composition of Linear Transformations as Matrix Multiplication

Proposition 2.4.1 (Matrix multiplication encodes composition)**.** *If $T_1 : \mathbb{R}^2 \to \mathbb{R}^2$ has matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and T_2 has matrix $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$, then $(T_2 \circ T_1)$ has matrix*

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} Aa+Bc & Ab+Bd \\ Ca+Dc & Cb+Dd \end{pmatrix}.$$

Proof. Let $x' = Ax+By$, $y' = Cx+Dy$ and $x = ax_0+by_0$, $y = cx_0+dy_0$. Substituting:

$$x' = A(ax_0+by_0) + B(cx_0+dy_0) = (Aa+Bc)x_0 + (Ab+Bd)y_0,$$
$$y' = C(ax_0+by_0) + D(cx_0+dy_0) = (Ca+Dc)x_0 + (Cb+Dd)y_0. \quad \square$$

□

2.5 Abstract Formalism: Linear Transformations on $\mathbb{R}^2$

Let $(a, b), (c, d) \in \mathbb{R}^2$ (a 2-dimensional plane, i.e. a *space*). The scalar field $\gamma \in \mathbb{R}$ (or $\mathbb{C}$) specifies the number of components. A map $T : \mathbb{R}^2 \to \mathbb{R}^2$ is linear if and only if

$$T\Big[(a, b) + (c, d)\Big] = T(a, b) + T(c, d), \qquad T\Big(\gamma(a, b)\Big) = \gamma T(a, b). \tag{2.3}$$

Remark 2.5.1. A vector space with *infinitely many dimensions* is called a **Hilbert Space** (see Chapter 6).

Chapter 3

Complex Numbers

Complex numbers are the native number system of quantum mechanics. Every quantum amplitude is complex, and the modulus-squared gives a probability.

3.1 Definition and the Argand Plane

Definition 3.1.1 (Imaginary Unit)**.** The *imaginary unit* is the number i satisfying $i^2 = -1$, i.e. $i = \sqrt{-1}$.

Definition 3.1.2 (Complex Number)**.** A *complex number* is an expression of the form

$$z = x + iy, \qquad x, y \in \mathbb{R},$$

where $x = \mathrm{Re}(z)$ is the *real part* and $y = \mathrm{Im}(z)$ is the *imaginary part*.

The set $\mathbb{C}$ of all complex numbers is visualised on the **Argand plane** (complex plane), with the real axis horizontal and the imaginary axis vertical.

3.2 Polar Form and Euler's Formula

Definition 3.2.1 (Polar Form)**.** Any $z = x + iy \in \mathbb{C}$ can be written in *polar form*

$$z = r(\cos\theta + i\sin\theta),$$

where $r = |z| = \sqrt{x^2 + y^2}$ is the *modulus* and $\theta = \arg(z)$ is the *argument*.

Theorem 3.2.1 (Euler's Formula)**.**

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

Hence the polar form simplifies to $z = re^{i\theta}$.

Corollary 3.2.2 (Euler's Identity)**.** *Setting $\theta = \pi$:*

$$\boxed{e^{i\pi} + 1 = 0.}$$

Proposition 3.2.3 (Product of complex numbers)**.** *If $z_1 = r_1 e^{i\theta_1}$ and $z_2 = r_2 e^{i\theta_2}$, then*

$$z_1 z_2 = r_1 r_2\, e^{i(\theta_1 + \theta_2)}.$$

Multiplication adds arguments *and* multiplies moduli.

3.3 Complex Conjugate

Definition 3.3.1 (Complex Conjugate)**.** The *complex conjugate* of $z = x+iy$ is $z^* = x-iy$. Geometrically, z^* is the reflection of z through the real axis (angle $-\theta$).

Proposition 3.3.1 (Modulus via conjugate)**.**

$$zz^* = (x+iy)(x-iy) = x^2 + y^2 = |z|^2.$$

Hence $|z| = \sqrt{zz^*}$.

Proof. Using Euler's form:

$$zz^* = (re^{i\theta})(re^{-i\theta}) = r^2 e^0 = r^2. \quad \square$$

$\square$

Remark 3.3.1 (Dual number system)*.* The pair (z, z^*) forms a *dual number system*: for every $z \in \mathbb{C}$ there exists a unique z^*, so that $\forall z\ \exists!\ z^*$.

3.4 Phase Factor

Definition 3.4.1 (Phase Factor)**.** A *phase factor* is a complex number of unit modulus:

$$z = e^{i\theta} = \cos\theta + i\sin\theta, \qquad |z| = 1.$$

Phase factors are ubiquitous in quantum mechanics: quantum states often differ only by a phase, and this phase carries physical information (e.g. interference).

Remark 3.4.1*.* In quantum calculations we work freely in $\mathbb{C}$, but the *final answer must be real* — probabilities and expectation values of Hermitian observables are always real numbers.

3.5 Complex Vector Space

Definition 3.5.1 (Complex Vector Space)**.** A *complex vector space* $V(\mathbb{C})$ is a vector space over the field $\mathbb{C}$ of scalars. This is the setting for quantum mechanics, where we take $F = \mathbb{C}$.

The complex conjugate of the scalar field $\mathbb{C}$ is $\mathbb{C}^*$; the dual vector space $V^*(\mathbb{C}^*)$ is the *complex conjugate vector space*.

Chapter 4

Vector Spaces

4.1 What is "Space" in Mathematics?

In everyday language, *space* is physical. In mathematics, a *space* is a non-empty set equipped with a **mathematical structure** — a collection of axioms, theorems, and definitions that constrain the set's behaviour.

Example 4.1.1. $A = \{1, 2, 3\}$ is an *ordinary* (simple) set with no additional structure. By contrast, $(\mathbb{R}, +)$ follows the axioms of an Abelian group and is therefore a *space*.

4.2 Definition of a Vector Space

Definition 4.2.1 (Vector Space)**.** A *vector space* over a field F is a non-empty set V together with two operations:

- **Vector addition:** $+ : V \times V \to V$,
- **Scalar multiplication:** $\cdot : F \times V \to V$,

satisfying the following nine axioms for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ and $a, b \in F$:

VS1. $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ (commutativity of $+$)

VS2. $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$ (associativity of $+$)

VS3. $\exists\, \mathbf{0} \in V$ such that $\mathbf{0} + \mathbf{u} = \mathbf{u} + \mathbf{0} = \mathbf{u}$ (additive identity)

VS4. $\forall\, \mathbf{u} \in V\ \exists\, (-\mathbf{u}) \in V$ such that $\mathbf{u} + (-\mathbf{u}) = \mathbf{0}$ (additive inverse)

VS5. $1 \cdot \mathbf{u} = \mathbf{u}$ (scalar identity)

VS6. $a \cdot (b \cdot \mathbf{u}) = (ab) \cdot \mathbf{u}$ (compatibility of scalar multiplication)

VS7. $(a + b)\mathbf{u} = a\mathbf{u} + b\mathbf{u}$ (distributivity over scalar addition)

VS8. $a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$ (distributivity over vector addition)

VS9. $\exists\, \mathbf{0} \in V$ such that $\mathbf{u} \cdot \mathbf{0} = \mathbf{0}$ (zero vector)

Remark 4.2.1. Axioms VS1–VS4 make $(V, +)$ an Abelian group. The scalar multiplication axioms VS5–VS8 couple the field structure to the group structure.

4.3 Examples of Vector Spaces

Example 4.3.1. The following are all vector spaces over appropriate fields:

1. **Polynomials of degree ≤ 1:** $u = x + 1$, $v = 2x - 3$; then $u + v = 3x - 2$ and $5u = 5x + 5$, both first-degree polynomials. ✓

2. 2×2 **matrices:** $u = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 3 \end{smallmatrix}\right)$, $v = \left(\begin{smallmatrix} -1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$; addition and scalar multiplication are component-wise. ✓

3. **Indefinite integrals:** $u = \int f(x)\,dx$, $v = \int g(x)\,dx$; $u + v = \int (f + g)(x)\,dx$. ✓

4. **Derivatives:** $u = \frac{d}{dx} f(x)$, $v = \frac{d}{dx} g(x)$. ✓

5. **Real scalars:** $u = 1$, $v = 2$. ✓

4.4 Subspaces

Definition 4.4.1 (Subspace)**.** Let $V(F)$ be a vector space. A non-empty subset $W \subseteq V$ is a *subspace* of V if W is itself a vector space over F under the same operations. Equivalently, W is a subspace if and only if:

1. $\mathbf{0} \in W$,

2. $\mathbf{u}, \mathbf{v} \in W \Rightarrow \mathbf{u} + \mathbf{v} \in W$,

3. $a \in F$, $\mathbf{u} \in W \Rightarrow a\mathbf{u} \in W$.

4.5 Metric Spaces

Definition 4.5.1 (Metric Space)**.** Let X be a non-empty set. A function $d : X \times X \to \mathbb{R}$ is a *metric* (distance function) on X if, for all $x, y, z \in X$:

(i) $d(x, y) \geq 0$ and $d(x, y) = 0 \iff x = y$,

(ii) $d(x, y) = d(y, x)$ (symmetry),

(iii) $d(x, z) \leq d(x, y) + d(y, z)$ (triangle inequality).

The pair (X, d) is then called a *metric space*.

Example 4.5.1. On $X = \mathbb{R}$, the function $d(x, y) = |x - y|$ is a metric (the standard Euclidean distance). Any x and y satisfying the three conditions above define a metric space — they need not be numbers.

4.6 Key Group-Theoretic Theorems

Theorem 4.6.1 (Uniqueness of Identity)**.** *If $(G, *)$ is a group, then the identity element e is unique.*

Proof. Suppose e and e' are both identities. Then $e = e * e' = e'$, since e' is an identity for e and e is an identity for e'. □ □

Theorem 4.6.2 (Uniqueness of Inverses)**.** *In a group $(G, *)$, every element has a unique inverse.*

Proof. Let b and c both be inverses of a. Then $b = b * e = b * (a * c) = (b * a) * c = e * c = c$. □ □

4.7 Internal and External Compositions

Definition 4.7.1 (Internal Composition)**.** A composition $*$ on a non-empty set V is *internal* if

$$\forall\, \alpha, \beta \in V \implies \alpha * \beta \in V.$$

The result is uniquely determined.

Definition 4.7.2 (External Composition)**.** Let F be a field (of scalars) and V a non-empty set. A composition $\circ : F \times V \to V$ is *external* if

$$\forall\, a \in F,\ \alpha \in V \implies a \circ \alpha \in V,$$

and the result is unique.

Remark 4.7.1. Vector addition is an *internal* composition on V; scalar multiplication is an *external* composition from F into V. Both are required to define a vector space.

Chapter 5

Normed Spaces and Inner Product Spaces

The progression **Vector Space** $\subset$ **Normed Space** $\subset$ **Inner Product Space** $\subset$ **Hilbert Space** adds richer geometric structure at each step.

5.1 Normed Spaces

A vector space has no built-in notion of length or distance. A norm supplies both.

Definition 5.1.1 (Norm)**.** Let V be a vector space over $F \in \{\mathbb{R}, \mathbb{C}\}$. A *norm* on V is a function $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ satisfying, for all $\mathbf{u}, \mathbf{v} \in V$ and $a \in F$:

N1. Non-negativity: $\|\mathbf{u}\| \geq 0$, and $\|\mathbf{u}\| = 0 \iff \mathbf{u} = \mathbf{0}$.

N2. Homogeneity: $\|a\mathbf{u}\| = |a|\,\|\mathbf{u}\|$.

N3. Triangle inequality: $\|\mathbf{u} + \mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\|$.

The pair $(V, \|\cdot\|)$ is a *normed space.*

Remark 5.1.1. The norm assigns a non-negative real number to each vector (its "length"), but without an inherent notion of actual physical distance or angle between vectors. The norm also induces a metric:

$$d(\mathbf{u}, \mathbf{v}) := \|\mathbf{u} - \mathbf{v}\|.$$

5.2 Inner Product Spaces

Definition 5.2.1 (Inner Product)**.** Let V be a vector space over F. An *inner product* is a map $\langle \cdot, \cdot \rangle : V \times V \to F$ (producing only non-negative real outputs when both arguments coincide) satisfying:

IP1. Linearity in the first argument: $\langle ax_1 + bx_2,\, y\rangle = a\langle x_1, y\rangle + b\langle x_2, y\rangle$.

IP2. Conjugate symmetry: $\langle x, y\rangle = \overline{\langle y, x\rangle}$.

IP3. Positive definiteness: $\langle x, x\rangle \geq 0$, and $\langle x, x\rangle = 0 \iff x = 0$.

The pair $(V, \langle \cdot, \cdot \rangle)$ is an *inner product space* (IPS).

Remark 5.2.1. Geometrically, the inner product $\langle x, y \rangle$ encodes how much x "points in the direction of" y and how their magnitudes contribute to their alignment. In physics it is often written $\vec{A} \cdot \vec{B} = |\vec{A}||\vec{B}| \cos\theta$.

5.2.1 Norm Induced by the Inner Product

Proposition 5.2.1. *Every inner product induces a norm by*

$$\|x\| := \sqrt{\langle x, x \rangle}.$$

Example 5.2.1. For $\vec{A}$ pointing along itself, $\vec{A} \cdot \vec{A} = |\vec{A}|^2 \cos 0 = |\vec{A}|^2$, so $|\vec{A}| = \sqrt{\vec{A} \cdot \vec{A}}$.

5.3 Orthogonality, Normalization, and Orthonormality

Definition 5.3.1 (Orthogonality)**.** Two vectors $|A\rangle$ and $|B\rangle$ in an IPS are *orthogonal* if $\langle A|B \rangle = 0$. Orthogonal vectors are linearly independent.

Definition 5.3.2 (Normalization)**.** A vector $|A\rangle$ is *normalized* (a unit vector) if $\langle A|A \rangle = 1$.

Definition 5.3.3 (Orthonormality)**.** A set of vectors $\{|A\rangle, |B\rangle, \ldots\}$ is *orthonormal* if

$$\langle A|B \rangle = \delta_{AB} = \begin{cases} 0 & A \neq B, \\ 1 & A = B. \end{cases}$$

5.4 Topological Properties of Spaces

Definition 5.4.1 (Topological Space)**.** A *topological space* is the most general type of space: a set X together with a *topology* (a collection $\mathcal{T}$ of "open" subsets of X) satisfying:

1. The union of *any* collection of open sets is open.
2. The intersection of a *finite* number of open sets is open.

Examples: function spaces, polynomial spaces.

Three key properties of topological spaces relevant to quantum mechanics:

Definition 5.4.2 (Connectedness)**.** A space is *connected* if it cannot be split into two non-overlapping, disjoint, non-empty open sets.

Definition 5.4.3 (Continuity)**.** A function f between topological spaces is *continuous* (smooth) if small changes in the input produce only small changes in the output.

Definition 5.4.4 (Compactness)**.** A space is *compact* if it is both bounded and closed, making it well-behaved for convergence and containment. For example, the open interval (a, b) is *not* compact; the closed interval $[a, b]$ *is* compact.

5.5 Unit Vectors and Normalization

Definition 5.5.1 (Unit Vector)**.** A vector $|\psi\rangle$ with $\||\psi\rangle\| = 1$ is a *unit vector*.

Proposition 5.5.1 (Normalization)**.** *Any non-zero vector $|\psi\rangle$ can be converted to a unit vector by dividing by its norm:*

$$\widehat{\psi} = \frac{1}{\||\psi\rangle\|} |\psi\rangle .$$

Example 5.5.1. Let $|\psi\rangle = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$. Then $\||\psi\rangle\| = \sqrt{9+1} = \sqrt{10}$, and

$$\text{unit vector} = \frac{1}{\sqrt{10}} \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 3/\sqrt{10} \\ 1/\sqrt{10} \end{pmatrix}, \qquad \left\| \begin{pmatrix} 3/\sqrt{10} \\ 1/\sqrt{10} \end{pmatrix} \right\| = \sqrt{\tfrac{9}{10} + \tfrac{1}{10}} = 1. \quad \checkmark$$

Chapter 6

Hilbert Spaces

A *Hilbert space* is the mathematical arena of quantum mechanics. It combines the algebraic richness of an inner product space with the analytical property of completeness.

6.1 Cauchy Sequences and Convergence

Definition 6.1.1 (Cauchy Sequence)**.** A sequence $\{x_n\}$ in a metric space (X, d) (or normed space) is a *Cauchy sequence* if

$$\forall \varepsilon > 0 \;\; \exists N \in \mathbb{N} \;\text{ such that }\; \forall m, n \geq N : \quad |x_m - x_n| < \varepsilon.$$

Intuitively, consecutive terms cluster arbitrarily tightly as $n \to \infty$.

Example 6.1.1. $\left\{\frac{1}{n}\right\}_{n=1}^{\infty} = 1, \frac{1}{2}, \frac{1}{3}, \ldots$ is Cauchy: for any $\varepsilon > 0$ choose $N > 2/\varepsilon$, then for $m, n \geq N$,

$$|x_m - x_n| \leq |x_m| + |x_n| < \tfrac{2}{N} < \varepsilon.$$

Definition 6.1.2 (Convergent Sequence)**.** A sequence $\{x_n\}$ *converges* to a limit L if

$$\lim_{n\to\infty} x_n = L, \quad \text{i.e.,} \quad \forall \varepsilon > 0 \, \exists N : \; n \geq N \Rightarrow |x_n - L| < \varepsilon.$$

Every convergent sequence is Cauchy, but the converse requires completeness.

Definition 6.1.3 (Dart-board analogy)**.** Think of convergence as a dart game: every throw lands strictly closer to the bull's-eye than the previous throw. The sequence of positions is Cauchy; the bull's-eye is the limit.

6.2 Completeness

Definition 6.2.1 (Complete Normed Space (Banach Space))**.** A normed space X is *complete* if every Cauchy sequence in X has a limit *within* X. A complete normed space is called a **Banach space**.

Example 6.2.1 (Incompleteness of $\mathbb{Q}$)**.** Consider the sequence in $\mathbb{Q}$ defined by $x_n = \sum_{k=0}^{n} \frac{1}{k!}$. It is Cauchy, but its limit $e = 2.71828\ldots$ is irrational, hence $e \notin \mathbb{Q}$. Therefore $(\mathbb{Q}, |\cdot|)$ is *not* complete.

Example 6.2.2 (Motivation from physics)**.** The sequence of hydrogen energy levels $E_n = -13.6\,\mathrm{eV}/n^2$. As $n \to \infty$, $E_n \to 0$. Completeness requires that 0 be in the same space as the E_n, which it is (the continuum of unbound states).

6.3 Hilbert Space

Definition 6.3.1 (Hilbert Space)**.** A **Hilbert space** $\mathcal{H}$ is a *complete inner product space* (a complete IPS):

$$\mathcal{H} = \underbrace{\text{IPS}}_{\text{properties}} + \underbrace{\text{completeness}}_{\text{every Cauchy seq. converges in } \mathcal{H}}.$$

6.3.1 Quantum Mechanical Interpretation

1. **States.** The state of a quantum particle is represented by a vector (ket) $|\psi\rangle \in \mathcal{H}$.
2. **Infinite dimension.** $\mathcal{H}$ is generically infinite-dimensional, encoding the infinite complexity of states available to a particle. A particle's state is a superposition of infinitely many basis states.
3. **Finite vs. infinite.** In quantum *computing* (qubits, spin), finite-dimensional Hilbert spaces suffice (2 or 3 dimensions). In full quantum *mechanics* (position, momentum, energy), we need infinite-dimensional $\mathcal{H}$.
4. **Many particles.** For a system of many particles, the total Hilbert space is the tensor product of individual Hilbert spaces:

$$\mathcal{H}_{\text{total}} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots$$

   The space grows very large, but each individual factor remains infinite-dimensional.
5. **Physical examples.**
   - Spin of an electron, polarisation of a photon $\longrightarrow$ 2 or 3 dimensions.
   - Position, energy, momentum $\longrightarrow \infty$ dimensions.

6.4 L^2 Space

Definition 6.4.1 (L^2 Space)**.** The space of *square-integrable functions* is

$$L^2(\mathbb{R}) = \left\{ f : \mathbb{R} \to \mathbb{C} \;\middle|\; \int_{-\infty}^{\infty} |f(x)|^2 \, dx < \infty \right\}.$$

This is an infinite-dimensional Hilbert space. Functions in L^2 are the natural setting for quantum wavefunctions.

Remark 6.4.1. In L^2, the vector $|v\rangle = c_1 |e_1\rangle + c_2 |e_2\rangle + \cdots$ has basis elements $|e_i\rangle$ and coefficients c_i that tell how much each basis element contributes to reconstruct the original "vector" (function). This is directly analogous to Fourier series coefficients.

Chapter 7

Bra-Ket (Dirac) Notation

Dirac's bra-ket notation is the standard language of quantum mechanics. It provides an elegant, basis-independent way to express vectors, dual vectors, inner products, and operators.

7.1 Notation Table

Symbol	Name	Meaning
z	Complex scalar	$z \in \mathbb{C}$
z^*	Complex conjugate	$z^* \in \mathbb{C}^*$
$\|\psi\rangle$	Ket vector	$\|\psi\rangle \in V(\mathbb{C})$, the complex vector space
$\langle\psi\|$	Bra vector	$\langle\psi\| \in V^*(\mathbb{C}^*)$, the dual (conjugate) space
$\langle\phi\|\psi\rangle$	Inner product	A number (generally $\in \mathbb{C}$)
$\|\phi\rangle \otimes \|\psi\rangle$	Tensor product	A vector in $V \otimes V$
A^*	Complex conjugate of matrix A	Element-wise conjugation
A^T	Transpose	$(A^T)_{ij} = A_{ji}$
$A^\dagger$	Hermitian conjugate	$A^\dagger = (A^T)^* = (\bar{A})^T$

7.2 Ket Vectors — Axioms

Let $V(\mathbb{C})$ be a complex vector space. A ket $|\psi\rangle \in V(\mathbb{C})$ represents the *state of a quantum particle*. Ket vectors satisfy the following seven axioms (for $|\psi\rangle, |\phi\rangle, |\chi\rangle \in V$ and $z, w \in \mathbb{C}$):

K1. $|\psi\rangle + |\phi\rangle \in V$ (closure under +)

K2. $|\psi\rangle + |\phi\rangle = |\phi\rangle + |\psi\rangle$ (commutativity)

K3. $|\psi\rangle + (|\phi\rangle + |\chi\rangle) = (|\psi\rangle + |\phi\rangle) + |\chi\rangle$ (associativity)

K4. $|\psi\rangle + |0\rangle = |\psi\rangle$ (additive identity)

K5. $|\psi\rangle + (-|\psi\rangle) = |0\rangle$ (additive inverse)

K6. $z\,|\psi\rangle = z\,|\psi\rangle \in V$ (scalar multiplication by $\mathbb{C}$)

K7. $z(|A\rangle + |B\rangle) = z\,|A\rangle + z\,|B\rangle, \quad (z+w)\,|A\rangle = z\,|A\rangle + w\,|A\rangle$ (linearity)

A function $A(x)$ that is continuous and complex-valued, closed under addition and complex-scalar multiplication, and satisfies the above axioms is a ket vector.

Example 7.2.1 (Column vector ket)**.**

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}, \qquad |\psi\rangle + |\phi\rangle = \begin{pmatrix} \alpha_1 + \beta_1 \\ \alpha_2 + \beta_2 \end{pmatrix}, \qquad z\,|\psi\rangle = \begin{pmatrix} z\alpha_1 \\ z\alpha_2 \end{pmatrix}.$$

7.3 Bra Vectors (Dual Space)

Definition 7.3.1 (Bra Vector)**.** For every ket $|a\rangle \in V$ there exists a unique *bra* $\langle a| \in V^*$ in the dual space (complex conjugate vector space):

$$|a\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} \quad \longleftrightarrow \quad \langle a| = \begin{pmatrix} \alpha_1^* & \alpha_2^* & \cdots & \alpha_n^* \end{pmatrix}.$$

Proposition 7.3.1 (Duality under scaling)**.** *If* $z\,|A\rangle = |B\rangle$*, then* $\langle A|\,z^* = \langle B|$*, i.e.,* $z\,|A\rangle \Rightarrow \langle A|\,z^*$*.*

Remark 7.3.1. Bra vectors also satisfy the seven axioms above (they live in the dual complex-conjugate space $V^*(\mathbb{C}^*)$), and $\forall\ |a\rangle \in V\ \exists!\ \langle a| \in V^*$.

7.4 Inner Product in Bra-Ket Notation

Definition 7.4.1. The inner product of $|\phi\rangle$ and $|\psi\rangle$ is

$$\langle\phi|\psi\rangle \in \mathbb{C}.$$

Properties:

1. **Linearity:** $\langle\psi|\,(|\phi\rangle + |\chi\rangle) = \langle\psi|\phi\rangle + \langle\psi|\chi\rangle$.
2. **Conjugate property:** $\langle A|B\rangle = \langle B|A\rangle^*$.
3. **Reality of self-inner-product:** $\langle A|A\rangle \in \mathbb{R}_{\geq 0}$ (with some exceptions involving complex phases).

7.5 Length of a Vector in Bra-Ket Notation

For $z = x + iy$,

$$zz^* = (x + iy)(x - iy) = x^2 + y^2,$$

so the norm of $|\psi\rangle = (\alpha_1, \alpha_2, \alpha_3)^T$ is

$$\| \, |\psi\rangle \, \| = \sqrt{\alpha_1^2 + \alpha_2^2 + \alpha_3^2}.$$

A vector of length 1 is a **unit vector**.

Example 7.5.1 (Standard basis kets for a qubit)**.**

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

$$|\rightarrow\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \quad |\leftarrow\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

$$|\nearrow\rangle = \begin{pmatrix} 1/2 \\ -\sqrt{3}/2 \end{pmatrix}, \quad |\swarrow\rangle = \begin{pmatrix} \sqrt{3}/2 \\ 1/2 \end{pmatrix}.$$

These all have unit norm. The standard basis $\{|\uparrow\rangle, |\downarrow\rangle\}$ is used for the spin of an electron.

7.6 Basis, Linear Combination, and Linear Dependence

Definition 7.6.1 (Basis)**.** A set $\{|i\rangle\}$ of vectors in $V(F)$ is a *basis* if it

1. **Spans** V (every vector in V is a linear combination of basis vectors), and
2. is **linearly independent**.

An *orthonormal basis* additionally satisfies $\langle i|j\rangle = \delta_{ij}$.

Theorem 7.6.1 (Expansion in an orthonormal basis)**.** *If $\{|i\rangle\}$ is an orthonormal basis of $V(F)$, then any $|A\rangle \in V$ can be written*

$$|A\rangle = \sum_i \langle i|A\rangle \, |i\rangle,$$

where the coefficient $\langle i|A\rangle$ is the component *of $|A\rangle$ along $|i\rangle$.*

Proof. Write $|A\rangle = \sum_i \alpha_i |i\rangle$. Apply $\langle j|$ to both sides:

$$\langle j|A\rangle = \sum_i \alpha_i \langle j|i\rangle = \sum_i \alpha_i \, \delta_{ji} = \alpha_j. \quad \square$$

□

Definition 7.6.2 (Linear Dependence and Independence)**.** A set of vectors $\{|v_1\rangle, \ldots, |v_n\rangle\}$ is *linearly dependent* if there exist scalars $c_1, \ldots, c_n$, not all zero, such that

$$c_1 |v_1\rangle + c_2 |v_2\rangle + \cdots + c_n |v_n\rangle = 0.$$

If the only solution is $c_1 = c_2 = \cdots = c_n = 0$, the set is *linearly independent.*

Proposition 7.6.2 (Dimension)**.** *Any two linearly independent sets that span V have the same cardinality, which defines the* dimension *of V. In quantum computing, Hilbert spaces are finite-dimensional; in quantum mechanics, infinite-dimensional.*

7.7 Probability Amplitudes

For an infinite-dimensional expansion

$$|\Psi\rangle = \sum_n a_n |b_n\rangle ,$$

the *probability amplitude* that $|\Psi\rangle$ "jumps" to state $|b_k\rangle$ upon measurement is $\langle b_k|\Psi\rangle$, and the probability is

$$P(\text{outcome } k) = |\langle b_k|\Psi\rangle|^2 = \langle b_k|\Psi\rangle \langle\Psi|b_k\rangle .$$

Chapter 8

Matrices

A matrix is a rectangular array of numbers. In quantum mechanics, linear operators on finite-dimensional Hilbert spaces are represented by matrices.

8.1 Fundamental Definitions

Definition 8.1.1 (Square Matrix)**.** An $n \times n$ matrix A with elements a_{ij} $(1 \leq i, j \leq n)$.

Definition 8.1.2 (Row Matrix (Bra))**.** A $1 \times n$ matrix: $\langle a| = \begin{bmatrix} a & b & c \end{bmatrix}$.

Definition 8.1.3 (Column Matrix (Ket))**.** An $n \times 1$ matrix: $|a\rangle = \begin{bmatrix} a \\ b \\ c \end{bmatrix}$.

Definition 8.1.4 (Identity Matrix)**.** The $n \times n$ identity matrix I has $I_{ij} = \delta_{ij}$:

$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Note $AI = A = IA$ for any $n \times n$ matrix A. In general $AB \neq BA$.

Definition 8.1.5 (Transpose)**.** The transpose A^T of A has $(A^T)_{ij} = A_{ji}$:

$$A = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \implies A^T = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix}.$$

Definition 8.1.6 (Trace)**.** The *trace* of a square matrix A is the sum of its diagonal elements: $\mathrm{Tr}(A) = \sum_i A_{ii}$.

8.2 Special Matrices

8.2.1 Symmetric Matrix

Definition 8.2.1. A is *symmetric* if $A^T = A$.

Example 8.2.1. $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $A^T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = A$. ✓

8.2.2 Hermitian Matrix

Definition 8.2.2. A is *Hermitian* (self-adjoint) if $A^\dagger = A$, where $A^\dagger = (\bar{A})^T$ is the Hermitian conjugate.

Remark 8.2.1. The *diagonal elements of a Hermitian matrix are always real*, since $(A^\dagger)_{ii} = \bar{A}_{ii} = A_{ii} \Rightarrow A_{ii} \in \mathbb{R}$.

Example 8.2.2.

$$A = \begin{pmatrix} 3 & 1-i \\ 1+i & -2 \end{pmatrix}, \quad \bar{A} = \begin{pmatrix} 3 & 1+i \\ 1-i & -2 \end{pmatrix}, \quad (\bar{A})^T = \begin{pmatrix} 3 & 1-i \\ 1+i & -2 \end{pmatrix} = A. \quad \checkmark$$

8.2.3 Orthogonal Matrix

Definition 8.2.3. A is *orthogonal* if $AA^T = I = A^T A$. The rows (and columns) of A form an orthonormal set.

Example 8.2.3 (Rotation matrix)**.**

$$A = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}, \quad A^T = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix},$$

$$AA^T = \begin{pmatrix} \cos^2\alpha + \sin^2\alpha & 0 \\ 0 & \sin^2\alpha + \cos^2\alpha \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I. \quad \checkmark$$

Example 8.2.4 (3×3 orthogonal matrix)**.**

$$A = \begin{pmatrix} 1/3 & 2/3 & -2/3 \\ -2/3 & 2/3 & 1/3 \\ 2/3 & 1/3 & 2/3 \end{pmatrix}, \qquad AA^T = I. \quad \checkmark$$

8.2.4 Unitary Matrix

Definition 8.2.4. A is *unitary* if $AA^\dagger = I = A^\dagger A$. Unitary matrices are the complex generalisation of orthogonal matrices; they preserve inner products.

Example 8.2.5.

$$A = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}, \quad A^\dagger = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}, \quad AA^\dagger = I. \quad \checkmark$$

8.3 Checking if a Set Forms an Orthonormal Basis

Proposition 8.3.1. *A set $\mathcal{A} = \{|b_i\rangle\}$ forms an orthonormal basis if and only if the matrix $[\langle b_i | b_j \rangle]_{i,j} = I$.*

Proof. In matrix form:

$$\underbrace{\begin{bmatrix} \langle b_1 | \\ \langle b_2 | \\ \vdots \\ \langle b_n | \end{bmatrix}}_{n \times 1} \underbrace{\begin{bmatrix} |b_1\rangle & |b_2\rangle & \cdots & |b_n\rangle \end{bmatrix}}_{1 \times n} = \begin{bmatrix} \langle b_1 | b_1 \rangle & \langle b_1 | b_2 \rangle & \cdots \\ \langle b_2 | b_1 \rangle & \langle b_2 | b_2 \rangle & \cdots \\ \vdots & & \ddots \end{bmatrix} = I. \quad \square$$

This is equivalent to checking: (i) normalization $\langle b_i|b_i\rangle = 1$, and (ii) orthogonality $A^\dagger A = I$. $\square$

Chapter 9

Linear Operators and Eigenvalues

9.1 Linear Operators

In quantum mechanics:

- **States** of a system are represented by vectors in a vector space (Hilbert space).
- **Physical observables** (energy, position, momentum, angular momentum) are represented by *linear operators* on that space.

Definition 9.1.1 (Linear Operator)**.** A map $M : V(F) \to V(F)$ is a *linear operator* if it satisfies (for all $|A\rangle, |B\rangle \in V$ and $z \in F$):

LO1. $M\Big(z\,|A\rangle\Big) = z\,M\,|A\rangle$,

LO2. $M\Big(|A\rangle + |B\rangle\Big) = M\,|A\rangle + M\,|B\rangle$.

Think of M as a machine: input goes in, output comes out. If no output is produced, M is not a linear operator.

Remark 9.1.1. Not every operator is linear. Linear operators are *associated with* a vector space but are not themselves vectors.

9.2 Matrix Representation of Linear Operators

Proposition 9.2.1. *Given an orthonormal basis $\{|i\rangle\}$ of V, a linear operator M is represented by the matrix with entries*

$$m_{ki} = \langle k \mid M \mid i\rangle.$$

The action $M\,|A\rangle = |B\rangle$ becomes

$$\begin{pmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}, \qquad \sum_i a_i\, m_{ki} = b_k.$$

Remark 9.2.1. The dimensions of the matrix M depend on the choice of basis. The relationship between vectors and operators is *independent* of basis in abstract notation but acquires a concrete matrix form once a basis is fixed.

Special operators.

- **Identity operator:** $I_V |v\rangle = |v\rangle, \quad |v\rangle \in V(F)$.
- **Zero operator:** $O |v\rangle = 0, \quad |v\rangle \in V(F)$.
- **Composition:** If $V : A \to B$ and $W : B \to C$ are linear, then $WV |a\rangle = W(V |a\rangle)$ is linear, and $AB(|v\rangle) = A(B |v\rangle)$.

9.3 Eigenvalues and Eigenvectors

Definition 9.3.1 (Eigenvalue / Eigenvector)**.** A non-zero vector $|\lambda\rangle$ is an *eigenvector* of M with *eigenvalue* $\lambda \in \mathbb{C}$ if

$$\boxed{M |\lambda\rangle = \lambda |\lambda\rangle .}$$

The operator M preserves the *direction* of $|\lambda\rangle$ (only scaling it by λ).

Remark 9.3.1. In general, a linear operator *changes* the direction of its input vector. Eigenvectors are special inputs for which only scaling occurs.

Example 9.3.1. Let $M = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$.

1. $|v\rangle = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$: $M |v\rangle = \begin{pmatrix} 3 \\ 3 \end{pmatrix} = 3 |v\rangle$. Eigenvalue $\lambda = 3$. ✓
2. $|u\rangle = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$: $M |u\rangle = \begin{pmatrix} -1 \\ 1 \end{pmatrix} = -1 |u\rangle$. Eigenvalue $\lambda = -1$. ✓
3. Let $N = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $|u'\rangle = \begin{pmatrix} 1 \\ i \end{pmatrix}$: $N |u'\rangle = \begin{pmatrix} -i \\ 1 \end{pmatrix} = -i |u'\rangle$. Eigenvalue $\lambda = -i$. ✓

9.4 Hermitian Conjugate and Its Role in Quantum Mechanics

Proposition 9.4.1. *For a linear operator M, the map in dual space is given by:*

$$M |A\rangle = |B\rangle \quad \Longleftrightarrow \quad \langle A| M^\dagger = \langle B| ,$$

so $M^\dagger$ is the Hermitian conjugate (adjoint) of M. In matrix form,

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \implies M^\dagger = \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix} .$$

Derivation. Starting from $M |A\rangle = |B\rangle$, expand in orthonormal basis: $M \sum_i a_i |i\rangle = \sum_i b_i |i\rangle$. Apply $\langle j|$: $\sum_i a_i \langle j|M|i\rangle = b_j$, so m_{ji} are the matrix elements. In dual space with complex-conjugate coefficients, m^*_{ji} appear, giving $(M^\dagger)_{ij} = m^*_{ji} = (M^T)^*_{ij}$, i.e. $M^\dagger = (\bar{M})^T$. □ □

9.5 Observables and Hermitian Operators

Theorem 9.5.1 (Observables are Hermitian)**.** *Observables in quantum mechanics are represented by Hermitian operators ($M = M^\dagger$), and* all eigenvalues of a Hermitian operator are real.

Proof. Let $M|\lambda\rangle = \lambda|\lambda\rangle$. Since $M = M^\dagger$,

$$\langle\lambda| M^\dagger = \lambda^* \langle\lambda| .$$

Multiply $\langle\lambda|$ on the left of $M|\lambda\rangle = \lambda|\lambda\rangle$:

$$\langle\lambda|M|\lambda\rangle = \lambda \langle\lambda|\lambda\rangle .$$

Multiply $M|\lambda\rangle = \lambda|\lambda\rangle$ on the right with $\langle\lambda|$ and use $M = M^\dagger$:

$$\langle\lambda|M|\lambda\rangle = \lambda^* \langle\lambda|\lambda\rangle .$$

Subtracting: $0 = (\lambda^* - \lambda)\langle\lambda|\lambda\rangle$. Since $|\lambda\rangle \neq 0$ we have $\langle\lambda|\lambda\rangle > 0$, hence $\lambda^* = \lambda$, i.e. $\lambda \in \mathbb{R}$. □ □

Remark 9.5.1*.* This is physically essential: the outcome of any experiment is always a real number, and observables correspond to Hermitian operators precisely to guarantee this.

9.6 Cauchy–Schwarz Inequality

Theorem 9.6.1 (Cauchy–Schwarz Inequality)**.** *For any two vectors $|u\rangle, |v\rangle$ in a Hilbert space $\mathcal{H}$,*

$$|\langle u|v\rangle|^2 \leq \langle u|u\rangle\ \langle v|v\rangle .$$

Remark 9.6.1*.* The Cauchy–Schwarz inequality is fundamental to Hilbert space theory. It bounds how much any two vectors can “overlap” and is a key ingredient in proving the triangle inequality for the induced norm.

Chapter 10

Fourier Analysis

Fourier analysis is the mathematical heart of quantum mechanics. The Fourier transform is the mathematical heart of Heisenberg's uncertainty principle (Rajan Chopra). It decomposes functions into their constituent frequencies, exactly as an orthonormal basis decomposes vectors.

10.1 Motivation: Seeing Functions Differently

The Fourier transform is a way of viewing a function from a different perspective — the *frequency domain* instead of the *time domain*. Just as $\hat{\imath}, \hat{\jmath}, \hat{k}$ span all of 3D space, the exponential functions $e^{in\omega_0 t}$ span L^2 space.

10.2 Fourier Series

Definition 10.2.1 (Periodic Function)**.** A function $f : \mathbb{R} \to \mathbb{C}$ is *periodic* with period T if $f(t) = f(t + T)$ for all t.

Theorem 10.2.1 (Fourier Series)**.** *Any periodic function $f(t)$ with period T can be expressed as a sum of sines and cosines (each with its own amplitude and frequency):*

$$f(t) = a_0 + \sum_{n=1}^{\infty} \Big[\, a_n \sin(n\omega_0 t) + b_n \cos(n\omega_0 t) \Big],$$

where $\omega_0 = 2\pi/T$ is the fundamental angular frequency *and $\omega = 2\pi\nu$ (ν = frequency in waves per second). Sines and cosines act as the* basis functions*.*

Example 10.2.1. $f(t) = \sin\omega t + \frac{1}{2}\sin 2\omega t + \frac{3}{2}\cos\omega t$. Each term is one frequency component, so this function has been expressed in its "Fourier basis."

10.2.1 Why Use Sines and Cosines?

1. **Orthogonality:** Sine and cosine are mutually independent (like orthogonal vectors in a vector space).

2. **Completeness:** The set $\{\sin(n\omega_0 t), \cos(n\omega_0 t)\}$ is a complete set — it can generate a wide variety of functions, especially from L^2.

10.3 Complex Exponential Form

Using Euler's formula $e^{i\theta} = \cos\theta + i\sin\theta$:

$$\cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2}, \qquad \sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}.$$

Substituting into the Fourier series and collecting terms, one obtains the **complex exponential Fourier series**:

$$\boxed{f(t) = \sum_{n=-\infty}^{\infty} C_n \, e^{in\omega_0 t},} \tag{10.1}$$

where $C_n \in \mathbb{C}$ are the *complex Fourier coefficients.*

Why $e^{i\omega t}$? Three reasons:

1. **Orthogonality:** $e^{i\omega t}$, $e^{2i\omega t}, \ldots$ are all mutually independent.
2. **Completeness:** Any well-behaved function is a linear combination of $\{e^{in\omega_0 t}\}$.
3. **Periodic nature:** $e^{i\omega t}$ traces a circle in the complex plane as t varies.

10.4 Derivation of Fourier Coefficients

Theorem 10.4.1 (Fourier Coefficients)**.** *The n-th complex Fourier coefficient of a periodic function $f(t)$ with period T is*

$$\boxed{C_n = \frac{1}{T}\int_0^T f(t)\, e^{-in\omega_0 t}\, dt.}$$

Proof. Start from (10.1): $f(t) = \sum_{k=-\infty}^{\infty} C_k e^{ik\omega_0 t}$.

Step 1. Multiply both sides by $e^{-in\omega_0 t}$ (for a fixed integer n) and integrate over one period $[0, T]$:

$$\int_0^T e^{-in\omega_0 t} f(t)\, dt = \int_0^T e^{-in\omega_0 t} \sum_{k=-\infty}^{\infty} C_k e^{ik\omega_0 t}\, dt.$$

Step 2. Exchange sum and integral (Fubini's theorem):

$$= \sum_{k=-\infty}^{\infty} C_k \int_0^T e^{i(k-n)\omega_0 t}\, dt.$$

Step 3. Use orthogonality of complex exponentials: any two exponentials $e^{ik\omega_0 t}$ and $e^{in\omega_0 t}$ are orthogonal over one period (their inner product is zero if $k \neq n$). Explicitly, if $k \neq n$:

$$\begin{aligned}\int_0^T e^{i(k-n)\omega_0 t}\, dt &= \left[\frac{e^{i(k-n)\omega_0 t}}{i(k-n)\omega_0}\right]_0^T = \frac{e^{i(k-n)\cdot 2\pi} - 1}{i(k-n)\omega_0} \\ &= \frac{\cos 2\pi(k-n) + i\sin 2\pi(k-n) - 1}{i(k-n)\omega_0} = \frac{1+0-1}{i(k-n)\omega_0} = 0.\end{aligned}$$

Step 4. Only the $k = n$ term survives:

$$\int_0^T e^{-in\omega_0 t} f(t)\, dt = C_n \int_0^T 1\, dt = C_n T.$$

Step 5. Solve for C_n:

$$C_n = \frac{1}{T} \int_0^T f(t)\, e^{-in\omega_0 t}\, dt. \quad \square$$

$\square$

10.5 Fourier Transform

Definition 10.5.1 (Fourier Transform)**.** For a *non-periodic* function $f(t)$ (thought of as having a continuous spectrum of frequencies), the **Fourier transform** is

$$\boxed{\tilde{f}(\omega) = \int_{-\infty}^{\infty} f(t)\, e^{-i\omega t}\, dt.}$$

This transforms from the *time domain* to the *frequency domain.* $\tilde{f}(\omega)$ is the *amplitude* of the frequency component ω in the original function — it tells us how much $e^{i\omega t}$ contributes to $f(t)$.

Definition 10.5.2 (Inverse Fourier Transform)**.** The original function is recovered by

$$\boxed{f(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \tilde{f}(\omega)\, e^{i\omega t}\, d\omega.}$$

This transforms from the *frequency domain* back to the *time domain.* The factor $\frac{1}{2\pi}$ is the normalizing factor.

Remark 10.5.1. A non-periodic function can be thought of as having a *continuous* spectrum of frequencies. It can be represented as a continuous sum (integral) of sines, cosines, or exponentials $e^{i\omega t}$, over (possibly) all frequencies.

Example 10.5.1 (Gaussian function)**.** Let $f(t) = e^{-t^2}$. Then

$$\tilde{f}(\omega) = \int_{-\infty}^{\infty} e^{-t^2} e^{-i\omega t}\, dt = \frac{1}{\sqrt{\pi}}\, e^{-\omega^2/4},$$

so

$$e^{-t^2} = \int_{-\infty}^{\infty} \underbrace{\frac{1}{\sqrt{\pi}} e^{-\omega^2/4}}_{\text{coeff.}} \underbrace{e^{i\omega t}}_{\text{basis}}\, d\omega.$$

A Gaussian in time is a Gaussian in frequency — a hallmark of the uncertainty principle.

10.6 Connection to Quantum Mechanics

The Fourier transform is the heart of **Heisenberg's Uncertainty Principle**.

- A sharply localized (narrow) wavepacket in position-space corresponds to a *spread-out* wavefunction in momentum-space, and vice versa.
- Mathematically: $\Delta x \, \Delta p \geq \hbar/2$.
- The Fourier transform relates the two representations.

The analogy with linear algebra is exact:

$$\underbrace{|v\rangle = \sum_i c_i \, |e_i\rangle}_{\text{vector expansion}} \quad \longleftrightarrow \quad \underbrace{f(t) = \int \tilde{f}(\omega) \, e^{i\omega t} \, d\omega}_{\text{Fourier expansion}},$$

with $e^{i\omega t}$ playing the role of the orthonormal basis functions and $\tilde{f}(\omega)$ playing the role of the expansion coefficients c_i.

Chapter 11

Outer Product, Completeness, and Projection Operators

11.1 Outer Product

Definition 11.1.1 (Outer Product)**.** The *outer product* of $|\psi\rangle \in \mathbb{R}^n$ and $|\phi\rangle \in \mathbb{R}^m$ is the $n \times m$ matrix

$$|\psi\rangle \langle\phi| \in \mathbb{R}^{n+m},$$

formed by

$$\underbrace{(\ \cdot\ )}_{n\times 1}\underbrace{(\ \cdot\ )}_{1\times m} = \underbrace{(\ \cdot\ )}_{n\times m}.$$

Remark 11.1.1. Contrast with the *inner product* $\langle\phi|\psi\rangle$, which collapses into a single number (scalar). The outer product $|\psi\rangle \langle\phi|$ preserves the full structure of both vectors and produces a matrix (higher-dimensional object).

Physical interpretation.

- Outer product $\Rightarrow$ **Projection operator** in quantum mechanics.
- $|\psi\rangle \langle\phi|$ is a way of "spreading out" the interaction between two vectors in a higher-dimensional space.
- Unlike the dot product (which collapses into a scalar), the outer product retains both vectors' properties.

Example 11.1.1. $(|\psi\rangle \langle\phi|)\,|\chi\rangle = |\psi\rangle \langle\phi|\chi\rangle$: first $\langle\phi|$ is projected onto $|\chi\rangle$ yielding a number $\langle\phi|\chi\rangle$, then $|\psi\rangle$ is scaled by that number. The projection operator thus performs *projection then scaling.*

11.2 Completeness Relation

Theorem 11.2.1 (Completeness Relation)**.** *Let* $\{|i\rangle\}$ *be an orthonormal basis of* $V(F)$*. Then*

$$\boxed{\sum_i |i\rangle \langle i| = I,}$$

the identity operator on V*.*

Proof. Let $|v\rangle \in V(F)$ be arbitrary. Since $\{|i\rangle\}$ is orthonormal, $|v\rangle = \sum_i v_i |i\rangle$ with $v_i = \langle i|v\rangle$. Therefore:

$$\left(\sum_i |i\rangle \langle i|\right) |v\rangle = \sum_i |i\rangle \langle i|v\rangle = \sum_i v_i |i\rangle = |v\rangle .$$

Since this holds for all $|v\rangle$, $\sum_i |i\rangle \langle i| = I$. $\square$ $\square$

Remark 11.2.1. The completeness relation is the outer-product analogue of the statement that any vector can be written as a linear combination of basis vectors. It is used constantly to insert resolutions of the identity in quantum mechanical calculations.

11.3 Representing Linear Operators as Outer Products

Theorem 11.3.1 (Outer Product Representation of a Linear Operator)**.** *Let $A : V \to W$ be a linear operator, with $\{|v_i\rangle\}$ an orthonormal basis of V and $\{|w_j\rangle\}$ an orthonormal basis of W. Then*

$$A = \sum_{i,j} |v_i\rangle \langle w_j| \ \langle v_i|A|w_j\rangle.$$

Equivalently, by inserting two completeness relations I_V and I_W:

$$A = I_V\, A\, I_W = \left(\sum_i |v_i\rangle \langle v_i|\right) A \left(\sum_j |w_j\rangle \langle w_j|\right) = \sum_{i,j} |v_i\rangle \ \underbrace{\langle v_i|A|w_j\rangle}_{\textit{matrix element}} \ \langle w_j| .$$

Remark 11.3.1. Linear operators can be represented in three equivalent ways:

1. **Abstract notation:** A
2. **Matrix notation:** $[A_{ij}]$ with $A_{ij} = \langle i|\, A\, |j\rangle$
3. **Outer product:** $A = \sum_{ij} |v_i\rangle \langle v_i|A|w_j\rangle \langle w_j|$

The choice depends on the calculation.

11.4 Cauchy–Schwarz Inequality (Inner Product Form)

Theorem 11.4.1 (Cauchy–Schwarz Inequality)**.** *For any $|u\rangle, |v\rangle$ in a Hilbert space $\mathcal{H}$:*

$$|\langle u|v\rangle|^2 \leq \langle u|u\rangle \cdot \langle v|v\rangle .$$

This bounds the squared inner product by the product of norms-squared.

Remark 11.4.1. The Cauchy–Schwarz inequality:

- Ensures the inner product is well-defined on $\mathcal{H}$.
- Is equivalent to the statement $|\cos\theta| \leq 1$ in geometry.
- Is a cornerstone of functional analysis and quantum mechanics.