Math for Quantum

Hans Halvorson

1 The complex numbers

By definition, we let $i^2 = -1$, and we define $\mathbb{C}$ to be all numbers of the form $a + ib$, where $a, b \in \mathbb{R}$. The number a is called the **real part** of $a + ib$, and the number b is called the **imaginary part** of b. That is, $\mathrm{Re}(a+ib) = a$ and $\mathrm{Im}(a + ib) = b$. We then define addition and multiplication on $\mathbb{C}$ by

$$\begin{aligned} (a+ib)+(c+id) &= (a+c)+i(b+d), \\ (a+ib)\cdot(c+id) &= (ac-bd)+i(bc+ad). \end{aligned}$$

We define **complex conjugation** by

$$\overline{a+bi} = a - bi.$$

Note that $\frac{1}{2}(z + \overline{z}) = \mathrm{Re}(z)$ and $\frac{1}{2}(z - \overline{z}) = \mathrm{Im}(z)$.

Fact. Addition and multiplication on $\mathbb{C}$ are commutative and associative, and multiplication distributes over addition. Every nonzero complex number z has a unique multiplicative inverse, i.e. a complex number z^{-1} such that $zz^{-1} = z^{-1}z = 1$.

Exercise 1. Show that $\overline{\overline{z}} = z$, and $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$, and $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$.

For a complex number z, we say that $z \in \mathbb{R}$ when the imaginary part of z is zero.

Exercise 2. Show that $\overline{z} = z$ iff $z \in \mathbb{R}$, and $\overline{z} = -z$ iff $z = ib$ for some $b \in \mathbb{R}$.

Exercise 3. Show that $\overline{z}z = a^2 + b^2$ when $z = a + ib$.

Definition. We define the **modulus** of a complex number by $|z| = \sqrt{z\overline{z}}$.

Exercise 4. Show that $|z_1 \cdot z_2| = |z_2| \cdot |z_2|$. Show that $|z| = 0$ iff $z = 0$.

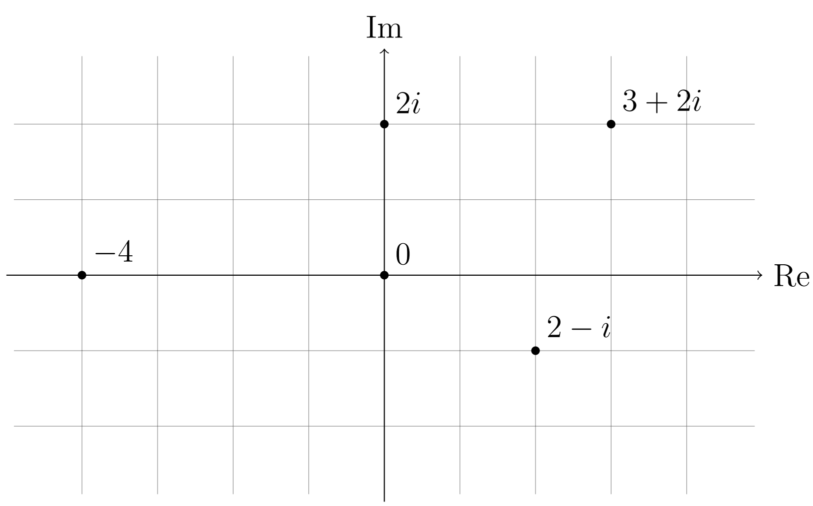
For any complex number $z = a + bi$, if we define $\theta = \tan(\frac{b}{a})^{-1}$, then

$$z = |z| (\cos\theta + i \sin\theta) .$$

This is referred to as the **polar representation** of z, and θ is called the **phase** of z. Defining $r = |z|$ and $e^{i\theta} = \cos\theta + i\sin\theta$, we can write $z = re^{i\theta}$. In polar form, multiplication of complex numbers has the following convenient representation:

$$(r_1 e^{i\theta_1}) \cdot (r_2 e^{i\theta_2}) \;=\; (r_1 r_2) e^{i(\theta_1+\theta_2)}.$$

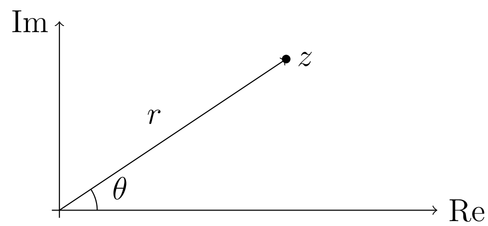
It is often convenient to represent the complex numbers on a plane, with the real numbers as the horizontal axis and the imaginary numbers as the vertical axis. In this case, the modulus r of $re^{i\theta}$ corresponds to its distance from the origin, and the phase θ corresponds to the angle that $re^{i\theta}$ makes with the real axis. What's more, we have $\overline{re^{i\theta}} = re^{i(-\theta)}$, so that complex conjugation corresponds to reflection in the real axis.



Definition. Let $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$. We say that $\mathbb{T}$ is the **complex unit circle**.

Each unit-length complex number is of the form $e^{i\theta} = \cos\theta + i\sin\theta$, and multiplication on $\mathbb{T}$ can be represented as $e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$. Hence $(e^{i\theta})^{-1} = e^{-i\theta}$. We also have the famous **Euler identity**:

$$e^{i\pi} \;=\; \cos\pi + i\sin\pi \;=\; -1.$$



2 Vector spaces

A **complex vector space** is a set V, equipped with

- a special **zero** element $\mathbf{0}$,
- an **addition** operation $+ : V \times V \to V$, and
- a **scalar multiplication** operation $\cdot : \mathbb{C} \times V \to V$,

such that for any $u, v, w \in V$ and $\alpha, \beta \in \mathbb{C}$,

$$\begin{array}{rcl} u + v &=& v + u \\ u + (v + w) &=& (u + v) + w \\ v + \mathbf{0} &=& v \\ 0 \cdot v &=& \mathbf{0} \\ 1 \cdot v &=& v \\ \alpha \cdot (\beta \cdot v) &=& (\alpha\beta) \cdot v \\ \alpha \cdot (u + v) &=& \alpha \cdot u + \alpha \cdot v \\ (\alpha + \beta) \cdot v &=& \alpha \cdot v + \beta \cdot v \end{array}$$

We will henceforth abbreviate scalar multiplication $\alpha \cdot v$ by αv.

Exercise 5. Show that $v + (-1)v = \mathbf{0}$.

Definition. A **basis** for V is a collection of vectors $v_i \in V$ such that any $v \in V$ can be expressed uniquely in the form $v = \sum_i \alpha_i v_i$. The **dimension** of vector space V is the smallest number n such that there exists a basis consisting of n vectors. We write $\dim V = n$.

Example.

Definition. A **subspace** of a vector space V is a nonempty subset $W \subseteq V$ that is closed under addition and scalar multiplication. In other words, W is itself a vector space inside of V such that $\dim W \leq \dim V$. In the finite-dimensional case, $\dim W = \dim V$ only if $W = V$.

Definition. Given a complex vector space V, an **inner product** is a binary operation $\langle -, - \rangle : V \times V \to \mathbb{C}$ such that for any $u, v, w \in V$ and $c \in \mathbb{C}$,

$$\begin{aligned} \langle u, v \rangle &= \overline{\langle v, u \rangle} \\ \langle u, v + w \rangle &= \langle u, v \rangle + \langle u, w \rangle \\ \langle u, cv \rangle &= c\langle u, v \rangle \\ \langle u, u \rangle &\geq 0 \end{aligned}$$

The **norm** of a vector v is defined to be $\|v\| = \sqrt{\langle v, v \rangle}$.

Proposition 1 (Cauchy-Schwartz inequality)**.** $|\langle u, v \rangle| \leq \langle u, u \rangle \cdot \langle v, v \rangle$.

Definition. Two vectors $u, v \in V$ are said to be **orthogonal** if $\langle u, v \rangle = 0$.

Definition. An **orthonormal** basis for V is a basis consisting entirely of vectors of norm 1, which are all orthogonal to one another.

Definition. A **finite-dimensional Hilbert space** is a finite-dimensional complex vector space equipped with an inner product.

We use elements of a Hilbert space H to represent the so-called "pure" states of a quantum system. Unlike in the classical case, one cannot determine whether or not the system is in the state represented by v through a single measurement. The best one can do is find a measurement setup such that for any state v, the probability of a positive result is given by

$$\frac{|\langle v, w \rangle|^2}{\|v\|^2 \|w\|^2} \tag{1}$$

Hence, for any $\alpha \in \mathbb{C}$ and $\psi \in H$, the states represented by ψ and $\alpha\psi$ cannot be discriminated from one another; we therefore take them to be the same state. We use this freedom to stipulate that only the **unit norm** elements of a Hilbert space (those such that $\|v\| = 1$) will be used to represent states. Under this stipulation, the probability of a positive result in the "ψ-test" is then simply given by $|\langle \phi, \psi \rangle|^2$. Note that even with this stipulation, there are still multiple elements of H representing the same state: e.g., v and iv.

Example. Consider the two-dimensional vector space V. We can represent elements of V by ordered pairs (or by column vectors), and we can define an inner product on V by

$$\langle (a, b), (c, d) \rangle = a^* c + b^* d.$$

In this case, the pair $(1, 0)$ and $(0, 1)$ form an orthonormal basis for V.

3 Linear operators

Definition. Let V and W be a vector spaces over $\mathbb{C}$, and let $A : V \to W$ be a function. We say that A is **linear** just in case $A(v + w) = Av + Aw$ and $A(cv) = cAv$, for all $v, w \in V$ and all $c \in \mathbb{C}$. For the case where $A : V \to V$, we say that A is a **linear operator**.

You may well have seen linear operators before, but most likely under the name **matrices**. That's because matrices provide a particularly convenient way for representing linear operators on finite-dimensional vector spaces. Here an $n \times n$ matrix (over $\mathbb{C}$) is an array of n^2 complex numbers. For the most part, it will suffice for us to look at the simplest non-trivial case, i.e. 2×2 matrices. Let A be the matrix

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

Then the action of A on a vector $\begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$ can be computed as follows:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_{11}b_1 + a_{12}b_2 \\ a_{21}b_1 + a_{22}b_2 \end{pmatrix}.$$

We've already defined a product of linear operators in terms of composition. You can then verify (by a straightforward calculation) that this product yields the standard matrix multiplication rule:

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

Definition. A **linear functional** on V is a linear map from V to $\mathbb{C}$.

Interestingly, the linear functionals on a vector space V themselves form another vector space V^*. In particular, given linear functionals ρ and σ, define $\rho + \sigma$ pointwise, i.e. $(\rho + \sigma)(v) = \rho(v) + \sigma(v)$. Similarly, given a complex number c, define $(c\rho)(v) = c\rho(v)$. We call V^* the **dual space** of V.

Theorem 1 (Riesz representation)**.** *Let V be a finite-dimensional vector space, and let $\rho : V \to \mathbb{C}$ be a linear functional. Then there is a unique vector $w \in V$ such that $\rho(v) = \langle w, v \rangle$, for all $v \in W$.*

Proposition 2. *Let V be a finite-dimensonal vector space. If $A : V \to W$ is linear, then there is a unique linear operator $A^* : W \to V$ such that $\langle w, Av \rangle = \langle A^* w, v \rangle$, for all $v \in V$ and $w \in W$.*

Fact. In a matrix representation of linear operators, the matrix for the operator A^* is the conjugate transpose of the matrix for the operator A.

Definition. Let A be a linear operator. Then we define:

- A is **normal** if $A^*A = AA^*$.
- A is **self-adoint** if $A^* = A$.
- A is **unitary** if $A^*A = AA^* = I$.

Example (spin operators)**.** Consider the two-dimensional vector space V, whose elements we will represent by column vectors. We define the function $\sigma_x : V \to V$ to take (a, b) to $\frac{1}{2}(a, -b)$. Clearly σ_x is linear. In fact, σ_x can be represented as the matrix

$$\sigma_x = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

It's easy to see then that $\sigma_x^* = \sigma_x$, and $\sigma_x \sigma_x = 1$. Hence, σ_x is both self-adjoint and unitary.

4 Composite systems