Quantum Computing

Lecture $|01\rangle$

A review of complex linear algebra

Paolo Zuliani

zuliani@di.uniroma1.it

Outline

- Complex numbers
- Vectors and matrices (of complex numbers)
- Eigenvectors and eigenvalues

Why Complex Numbers

- The set of the ***natural numbers***

$$\mathrm{N} = \{1, 2, 3, \dots\}$$

is the most fundamental object in mathematics.

- Note that the simple equation

$$x + 21 = 7$$

has <u>no solution</u> in the naturals!

- However, if we allow '***negative***' numbers we can solve and obtain $x = 7 - 21 = -14$

Why Complex Numbers

- Therefore, we get the set of the ***integers***

$$Z = \{\dots, -3, -2, -1, 0, 1, 2, \dots\}$$

- Note:
  - $x + a = b$ can now be solved for *any* integers a, b
  - The solution $x = b - a$ is always an integer!

Why Complex Numbers

- Hold on! How about solving

$$22x + 7 = 0$$

Does it have integer solutions?

- In general, no. We must introduce ***rational*** numbers

$$x = \frac{-7}{22}$$

Why Complex Numbers

- Therefore, we get the set of the ***rationals***

$$\mathrm{Q} = \{\dots, -\frac{2}{3}, -2, \dots, -\frac{1}{3}, -\frac{1}{2}, -1, 0, 1, \frac{1}{2}, \frac{1}{3}, \dots, 2, \frac{2}{3}, \dots\}$$

- Note:
  - $ax + b = 0$ can now be solved for *any* rationals a, b (except $a = 0$)
  - The solution $x = -\frac{b}{a}$ is always a rational!

Why Complex Numbers

- Now consider:

$$ax^2 + bx + c = 0 \qquad \text{where } a \neq 0, b, c \text{ are } \textit{integers}$$

- The solutions are:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \quad \text{as long as } \Delta = (b^2 - 4ac) \geq 0$$

  - If Δ is the square of an integer, then solutions are rational
  - However, solutions may be *irrational* (e.g., $\Delta = 2$)

Why Complex Numbers

- How about when $(b^2 - 4ac) < 0$?? (A legitimate question!)
- Square root of a negative number?!

$$\sqrt{-4} = \sqrt{4}\sqrt{-1} = 2\sqrt{-1} = 2i$$

where $i = \sqrt{-1}$ is an ***imaginary number*** (note $i^2 = -1$)

- ***Complex number***: $a + ib$ where a, b are reals
  - Example: $3.17 - i5$ is a complex number

Do We Need More Numbers?

- How about solving

$$4x^5 + x^4 + 3.44x^2 + x - 7 = 0$$

- Thankfully, complex numbers are enough!
- [***Fundamental Theorem of Algebra***]:

Every equation

$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$

with $a_n \neq 0$ and all a_i's complex has <u>exactly</u> n complex solutions

Complex Numbers

- The set of complex numbers is denoted by *C*

$$C = \{a + ib, \quad \text{where } a, b \text{ are real}\}$$

- Given a complex $\mathrm{z} = a + ib$ we define

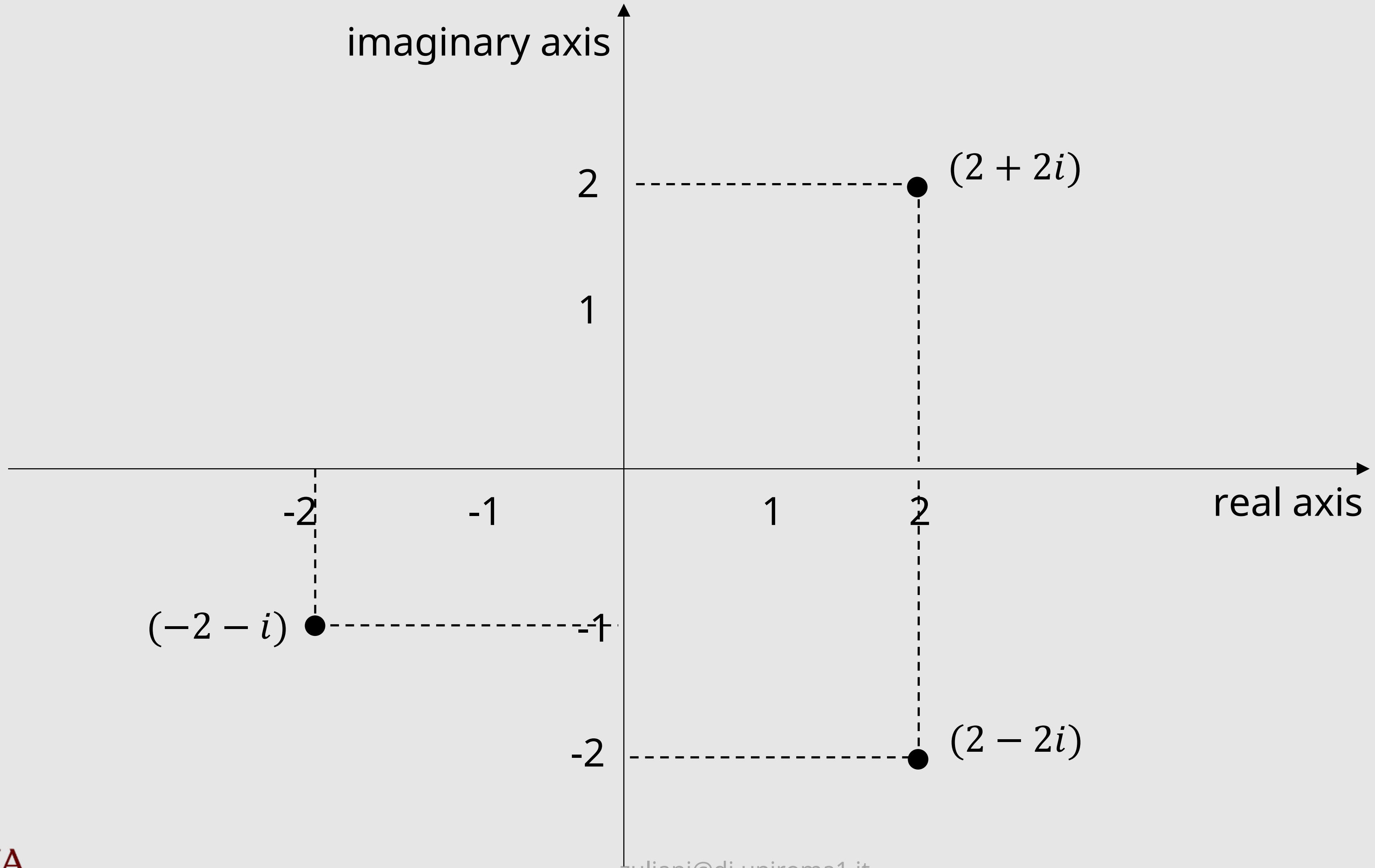
Re(*z*) = *a* (the *real* part of *z*)

Im(*z*) = *b* (the *imaginary* part of *z*)

Note: the imaginary part of a complex number is a real number!

zuliani@di.uniroma1.it

Complex Numbers: How to Plot Them



Complex Numbers: Basic Operations

$(a + ib) + (c + id) = (a + c) + i(b + d)$
$(a + ib) * (c + id) = (ac - bd) + i(ad + bc)$

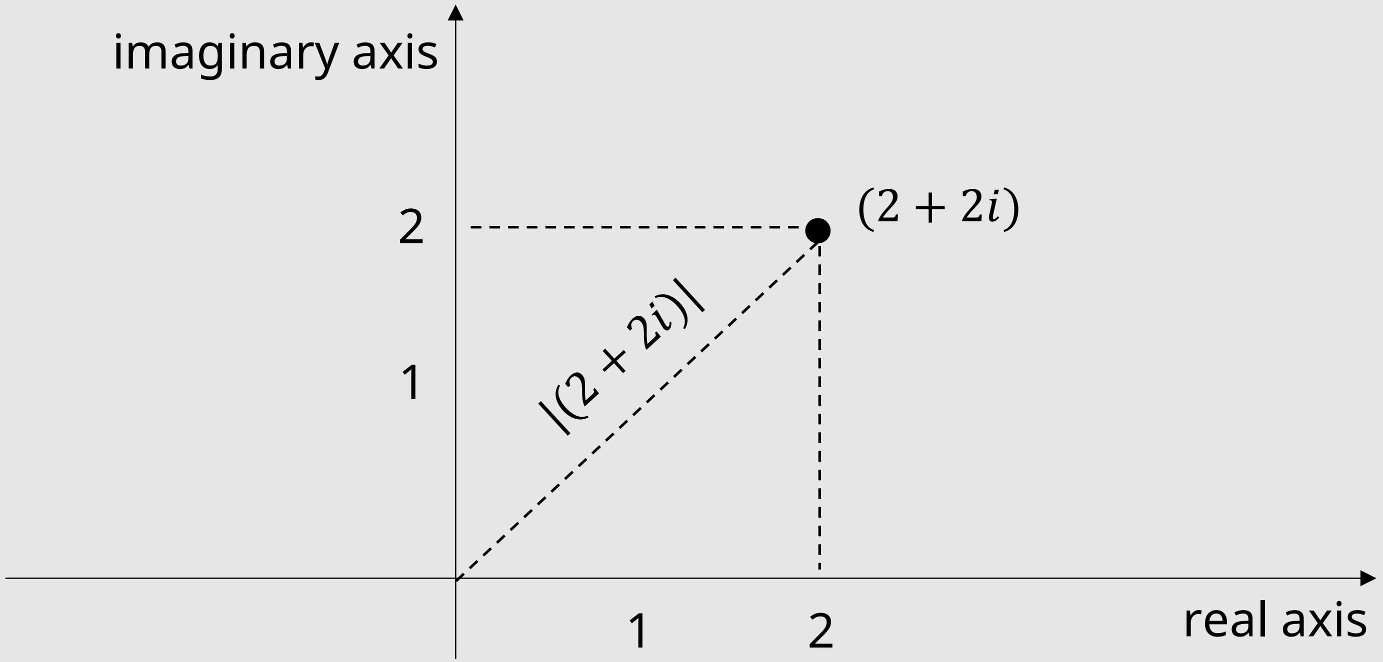
The ***<u>conjugate</u>*** of $z = (a + ib)$ is $\bar{z} = \overline{(a + ib)} = (a - ib)$

The ***<u>modulus</u>*** of $z = (a + ib)$ is $|z| = \sqrt{a^2 + b^2}$

- $|z|$ is real!

Note that $|zw| = |z||w|$ and $|z| = \sqrt{z\bar{z}}$ (exercise)

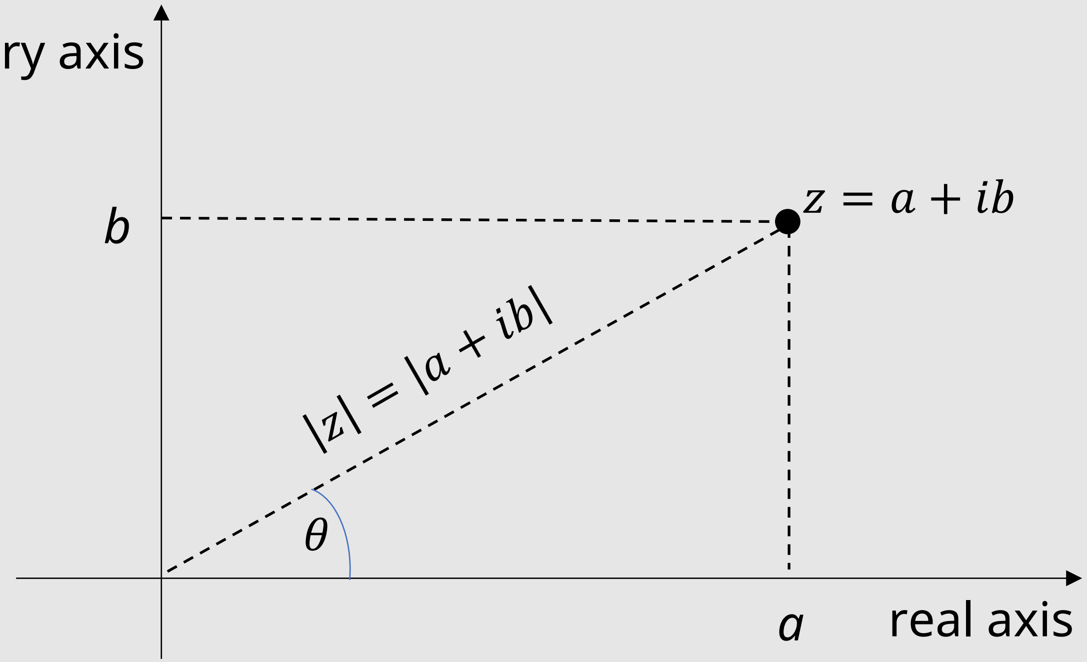
Complex Numbers: Basic Operations



- How about complex division $\frac{z}{w}$?
- Multiply both numerator and denominator by $\overline{w}$ …

Complex Numbers: Polar Coordinates

- Suppose $z = a + ib$ is non-zero, and so $|z| = \sqrt{a^2 + b^2}$
- Then there is a unique angle θ in the interval (-π, π] such that:

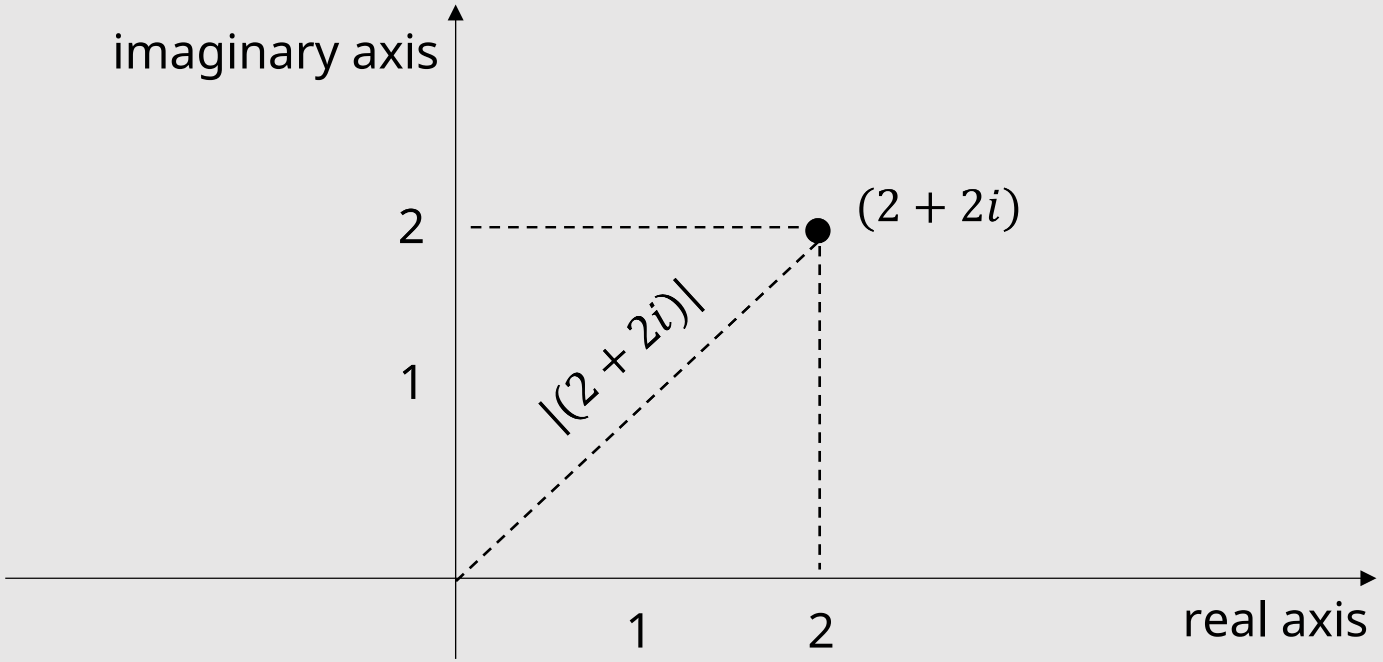


$$\cos\theta = \frac{a}{\sqrt{a^2 + b^2}} = \frac{a}{|z|} \qquad \sin\theta = \frac{b}{\sqrt{a^2 + b^2}} = \frac{b}{|z|}$$

- Thus, we can write

$$\boxed{z = |z|(\cos\theta + i\sin\theta)}$$

Complex Numbers: Polar Coordinates



For example: $(2+2i) = |2+2i|\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) = 2\sqrt{2}\left(\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}\right)$

Complex Numbers: Polar Coordinates

- We also define the exponential of an imaginary number

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

and we can thus write

$$z = |z|e^{i\theta}$$

- This form is handy when dealing with powers of complex numbers:

$$z^2 = (|z|e^{i\theta})^2 = |z|^2 e^{i2\theta}$$

$$\frac{1}{z} = z^{-1} = (|z|e^{i\theta})^{-1} = |z|^{-1} e^{-i\theta}$$

$$\sqrt{z} = (|z|e^{i\theta})^{\frac{1}{2}} = \sqrt{|z|}e^{i\frac{\theta}{2}}$$ (square root always exists!)

Vectors

- Simply, lists of (complex) numbers

$$v = \begin{pmatrix} 4 \\ i \\ 2+3i \end{pmatrix} \qquad w = \begin{pmatrix} 0 \\ 1 \\ i \end{pmatrix}$$

$$v + w = \begin{pmatrix} 4 \\ i \\ 2+3i \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ i \end{pmatrix} = \begin{pmatrix} 4 \\ 1+i \\ 2+4i \end{pmatrix}$$

summing vectors

$$v * 2i = 2i * \begin{pmatrix} 4 \\ i \\ 2+3i \end{pmatrix} = \begin{pmatrix} 8i \\ -2 \\ -6+4i \end{pmatrix}$$

scalar multiplication

Vectors

- The ***norm*** of a vector is its ‘size’
- Given a complex vector of dimension n:

$$v = (v_1, v_2, \dots, v_n)$$

The norm of v is $\|v\|$

$$\|v\| = \sqrt{|v_1|^2 + |v_2|^2 + \cdots + |v_n|^2} = \sqrt{\sum_{i=1}^{n} |v_i|^2}$$

Example: $\|(4, i, 2 + 3i)\| = \sqrt{16 + 1 + 13} = \sqrt{30}$

Matrices

- Essentially: tables of complex numbers, with a 'funky' multiplication rule
- A matrix has ***m* rows**, ***n* columns** (its dimensions are *m* x *n*)
- A 3 x 2 matrix: $\begin{bmatrix} 3 & i \\ 1+i & 0 \\ -4 & 2+3i \end{bmatrix}$
- A 2 x 2 matrix (when *m*=*n* we say the matrix is *square*)

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

2 x 2 identity matrix

zuliani@di.uniroma1.it

Matrices: Sum

- Two matrices can be *summed* only if they have the ***same dimension***; the sum is element-wise (as for vectors)

$$\begin{bmatrix} 3 & i \\ 1+i & 0 \\ -4 & 2+3i \end{bmatrix} + \begin{bmatrix} 1 & i \\ i & 10 \\ -4 & 2-3i \end{bmatrix} = \begin{bmatrix} 4 & 2i \\ 1+2i & 10 \\ -8 & 4 \end{bmatrix}$$

- For any two matrices A, B with the same dimension

$A + B = B + A$ (matrix sum is *commutative*)

Matrices: Row-by-Column Product

- Two matrices *A*, *B*

  dim(*A*)=*m* x *n*   dim(*B*)=*p* x *q*

can be *multiplied* only if ***n* = *p***

the product *A*·*B* has dimension ***m* x *q***

$$\begin{bmatrix} \boxed{3 \quad i} \\ 1+i & 0 \\ -4 & 2+3i \end{bmatrix} \cdot \begin{bmatrix} 3 & \boxed{1} \\ 0 & \boxed{0} \end{bmatrix} = \begin{bmatrix} \boxed{9+i0} & 3+i0 \\ 3+3i+0 & 1+i+0 \\ -12+0 & -4 \end{bmatrix} = \begin{bmatrix} 9 & 3 \\ 3+3i & 1+i \\ -12 & -4 \end{bmatrix}$$

$\boxed{3 \text{ x } 2}$ $\boxed{2 \text{ x } 2}$ $\boxed{3 \text{ x } 2}$

Matrices: Row-by-Column Product

$$\begin{bmatrix} 3 & i \\ 1+i & 0 \\ -4 & 2+3i \end{bmatrix} \cdot \begin{bmatrix} i \\ 1 \end{bmatrix} = \begin{bmatrix} 3i+i \\ i+i^2 \\ -4i+2+3i \end{bmatrix} = \begin{bmatrix} 4i \\ -1+i \\ 2-i \end{bmatrix}$$

3 x 2 2 x 1 3 x 1

Scalar multiplication is *element-wise*:

$$\begin{bmatrix} 3 & i \\ 1+i & 0 \\ -4 & 2+3i \end{bmatrix} \cdot 2 = \begin{bmatrix} 6 & 2i \\ 2+2i & 0 \\ -8 & 4+6i \end{bmatrix}$$

Matrices: Row-by-Column Product

In general, matrix multiplication is **NOT** commutative:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$$

but

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$

This property is ***crucially important*** in quantum physics (and thus quantum computing!)

Matrices: Eigenvectors & Eigenvalues

A (non-zero) vector v is an ***eigenvector*** of matrix A with ***eigenvalue*** λ if

$$A \cdot v = \lambda \cdot v$$

Equivalently: $A \cdot v - \lambda \cdot v = 0$ iff $(A - \lambda I) \cdot v = 0$

Now, $(A - \lambda I) \cdot v = 0$ has non-zero v solutions iff $\det(A - \lambda I) = 0$

Matrices: Eigenvectors & Eigenvalues

Example: $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ has eigenvalues +1 and -1 with eigenvectors $\begin{bmatrix} 1 \\ i \end{bmatrix}$ and $\begin{bmatrix} 1 \\ -i \end{bmatrix}$, respectively. In fact, for eigenvalue +1:

$$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ i \end{bmatrix} = \begin{bmatrix} -i^2 \\ i \end{bmatrix} = \begin{bmatrix} 1 \\ i \end{bmatrix}$$

Exercise: prove the above.

Matrices: Eigenvectors & Eigenvalues

Note that:

- in general, both v and λ are complex;
- it is possible for an eigenvalue to be associated to *more than one* eigenvector [such eigenvectors form a linear subspace – more later]

Spoiler: quantum mechanics models physical measurements with certain linear operators (matrices) that always have *real* eigenvalues