CSCE 785 — Quantum Computer Science

"Linear Algebra Done Right"

Quantum Mechanics

Niels Bohr — H atom

equiv. { Heisenberg — Matrix mechanics
Schrödinger — wave mechanics }

Dirac — amalgamation

Feynman — quantum computer to simulate quantum system

Benioff, Deutsch — Quantum Turing machine (QTM)

Bennett & Brassard 1984: Quantum cryptographic key distribution

Bernstein & Vazirani — universal QTM exists — quantum computational complexity

Peter Shor: Factoring integers is "easy" on a quantum computer.

Shor, Steane — Good quantum error-correcting codes exist.

Q computation can be implemented fault-tolerantly

Threshold theorem (D. Aharonov, et al.)

Quantum Circuit Model — stand. way to describe quantum algos.

Grover (~1996) — searching an unstructured database of n items target item takes $\sqrt{n}$ queries to the database with a quantum algo.

Besides Shor, Grover, main apps of Q computer:

quantum machine learning:
- simulating quantum systems
- optimization (variational algorithms) ⟺ hybrid quantum/classical
- phase estimation (related to the above)

Quantum Fourier Transform (QFT)

IBM, Amazon, Microsoft, Quantinuum, Rigetti, . . .

Quantum hardware implementations
- superconducting (most popular) IBM, Rigetti
- ion traps (neutral atom traps) (IonQ, . . .)
- NMR (nuclear magnetic resonance) (out of favor)
- photonic/optical

Current era — NISQ era (noisy intermediate-scale quantum)

Qubits, quantum gates are noisy, decohering quickly

Future (to be hoped) EC era (error correction)

Complex numbers:

$\mathbb{C} = \{x + iy : x, y \in \mathbb{R}\}$

$(i^2 = -1)$

$z = x + iy$

$x = \mathrm{Re}(z)$

$y = \mathrm{Im}(z)$

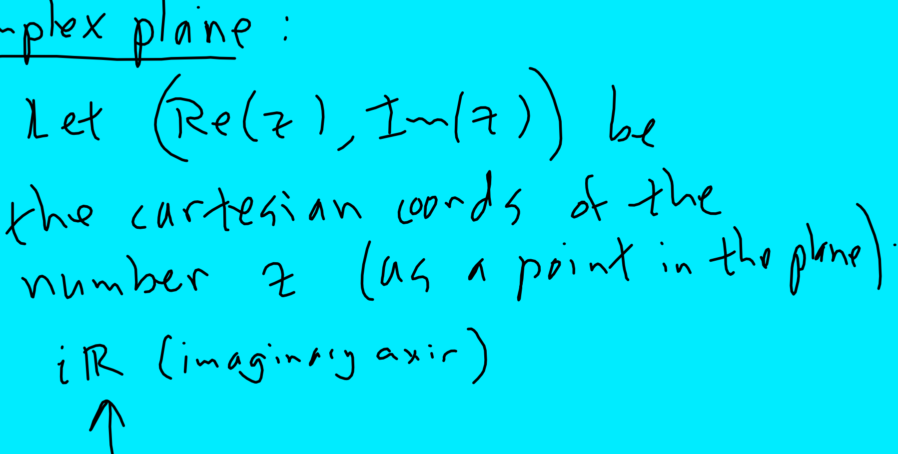
Addition & multiplication are what you would expect, except $i^2 = -1$

complex conjugate

$$z = x + iy$$
$$z^* = \bar{z} = x - iy$$

complex plane:

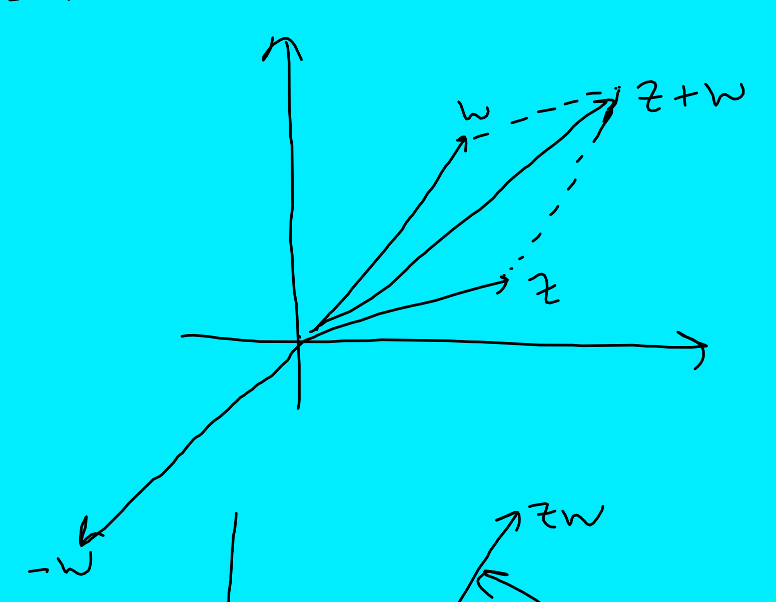
Let $(\mathrm{Re}(z), \mathrm{Im}(z))$ be the cartesian coords of the number z (as a point in the plane):



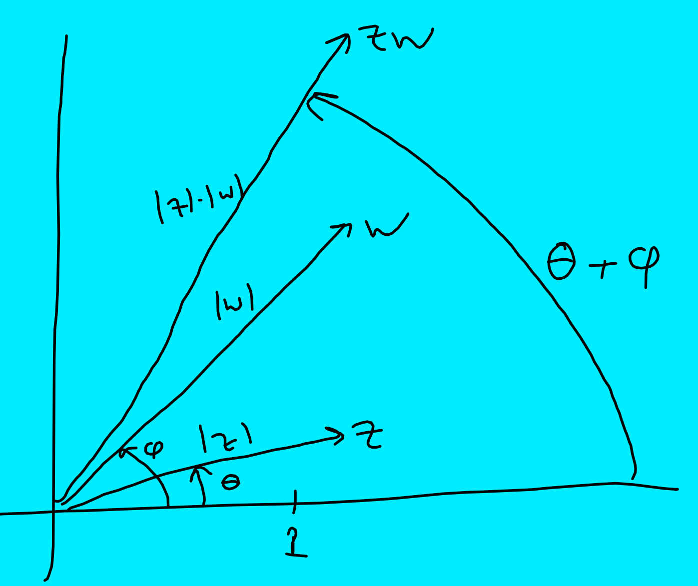
$$zz^* = (x+iy)(x-iy) = x^2 - (iy)^2$$
$$= x^2 - i^2y^2 = x^2 + y^2 = |z|^2$$

$|z| := \sqrt{zz^*}$

$z + w$

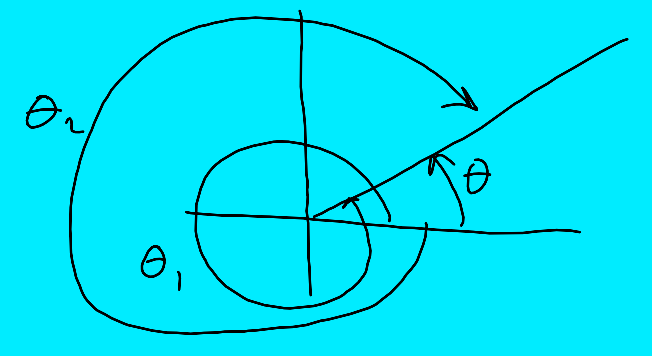


$|zw|$
$= |z| \cdot |w|$



<u>Def</u>:
$\arg(z) :=$ angle (in radians)
from the positive real axis
counterclockwise to z
(range $0 — 2\pi$)
$[\qquad)$

determined up to additive
multiples of 2π (complete
revolutions)



$\theta_1 = \theta + 2\pi$
$\theta_2 = \theta - 2\pi$

$\theta \equiv_{2\pi} \theta_1 \equiv_{2\pi} \theta_2$

$\arg(zw) \equiv_{2\pi} \arg(z) + \arg(w)$
$(z, w \neq 0)$
$\arg(0)$ is undef.

Exponential map: $z \in \mathbb{C}$

$$e^z := \sum_{j=0}^{\infty} \frac{z^j}{j!} = \lim_{n \to \infty} \left(1 + \frac{z}{n}\right)^n$$

$$z \neq 0 \Rightarrow z^{-1} = \frac{z^*}{|z|^2}$$

<u>Proof</u>: $z z^{-1} = \frac{z z^*}{|z|^2} = \frac{|z|^2}{|z|^2} = 1$

Euler's formula: $\theta \in \mathbb{R}$

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