Complex numbers
Algebra and Geometry

Ananda Dasgupta

MA211, Lecture 2

The algebra of complex numbers

- Consider the set $\mathbb{C}$ of ordered pairs of real numbers :

$$\mathbb{C} = \{(a, b) | a, b \in \mathbb{R}\}$$

The algebra of complex numbers

- Consider the set $\mathbb{C}$ of ordered pairs of real numbers :

$$\mathbb{C} = \{(a, b) | a, b \in \mathbb{R}\}$$

- Define the binary operation, *addition*, $+ : \mathbb{C} \to \mathbb{C}$ by

$$(a, b) + (c, d) = (a + c, b + d)$$

The algebra of complex numbers

- Consider the set $\mathbb{C}$ of ordered pairs of real numbers :

$$\mathbb{C} = \{(a, b) | a, b \in \mathbb{R}\}$$

- Define the binary operation, *addition*, $+ : \mathbb{C} \to \mathbb{C}$ by

$$(a, b) + (c, d) = (a + c, b + d)$$

- $\{\mathbb{C}, +\}$ is an Abelian group (?), with $(0, 0)$ being the additive identity.

The algebra of complex numbers

- Define *product* $*: \mathbb{C} \to \mathbb{C}$ by
$$(a, b) * (c, d) = (ac - bd, ad + bc)$$

The algebra of complex numbers

- Define *product* $*: \mathbb{C} \to \mathbb{C}$ by

$$(a, b) * (c, d) = (ac - bd, ad + bc)$$

  - $*$ is commutative.

The algebra of complex numbers

- Define *product* $* : \mathbb{C} \to \mathbb{C}$ by

$$(a, b) * (c, d) = (ac - bd, ad + bc)$$

  - $*$ is commutative.
  - $*$ is associative.

The algebra of complex numbers

- Define *product* $*:\mathbb{C}\to\mathbb{C}$ by

$$(a,b)*(c,d)=(ac-bd,ad+bc)$$

  - $*$ is commutative.
  - $*$ is associative.
  - $*$ distributes over $+$ (?).

The algebra of complex numbers

- Define *product* $* : \mathbb{C} \to \mathbb{C}$ by

$$(a, b) * (c, d) = (ac - bd, ad + bc)$$

  - $*$ is commutative.
  - $*$ is associative.
  - $*$ distributes over $+$ (▸ ?).
  - $(1, 0) \in \mathbb{C}$ is an identity element for $*$ (▸ ?).

The algebra of complex numbers

- Define *product* $* : \mathbb{C} \to \mathbb{C}$ by

$$(a, b) * (c, d) = (ac - bd, ad + bc)$$

  - $*$ is commutative.
  - $*$ is associative.
  - $*$ distributes over $+$ (?).
  - $(1, 0) \in \mathbb{C}$ is an identity element for $*$ (?).
- $\{\mathbb{C}, +, *\}$ is a commutative ring (?) with identity.

The algebra of complex numbers

- Every nonzero element of $\mathbb{C}$ has a multiplicative inverse.

The algebra of complex numbers

- Every nonzero element of $\mathbb{C}$ has a multiplicative inverse.
  - Proof by construction :
    Let (x, y) be the inverse of (a, b).

The algebra of complex numbers

- Every nonzero element of $\mathbb{C}$ has a multiplicative inverse.
  - Proof by construction :
    Let (x, y) be the inverse of (a, b).
  - Then

$$\begin{aligned} ax - by &= 1 \\ ay + bx &= 0 \end{aligned}$$

The algebra of complex numbers

- Every nonzero element of $\mathbb{C}$ has a multiplicative inverse.
  - Proof by construction :
    Let (x, y) be the inverse of (a, b).
  - Then

$$\begin{aligned} ax - by &= 1 \\ ay + bx &= 0 \end{aligned}$$

  - Which is satisfied by :

$$x = \frac{a}{a^2 + b^2}, \quad y = -\frac{b}{a^2 + b^2}$$

for $(a, b) \neq (0, 0)$.

The algebra of complex numbers

- Every nonzero element of $\mathbb{C}$ has a multiplicative inverse.
  - Proof by construction :
    Let (x, y) be the inverse of (a, b).
  - Then

$$\begin{aligned} ax - by &= 1 \\ ay + bx &= 0 \end{aligned}$$

  - Which is satisfied by :

$$x = \frac{a}{a^2 + b^2}, \quad y = -\frac{b}{a^2 + b^2}$$

    for $(a, b) \neq (0, 0)$.
  - Thus, $\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$ is the multiplicative inverse of (a, b).

The algebra of complex numbers

- Every nonzero element of $\mathbb{C}$ has a multiplicative inverse.
  - Proof by construction :
    Let (x, y) be the inverse of (a, b).
  - Then

$$\begin{aligned} ax - by &= 1 \\ ay + bx &= 0 \end{aligned}$$

  - Which is satisfied by :

$$x = \frac{a}{a^2 + b^2}, \quad y = -\frac{b}{a^2 + b^2}$$

    for $(a, b) \neq (0, 0)$.
  - Thus, $\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$ is the multiplicative inverse of (a, b).
- $\mathbb{C} \setminus \{(0, 0)\}$ is an Abelian group under $*$.

The algebra of complex numbers

- Every nonzero element of $\mathbb{C}$ has a multiplicative inverse.
  - Proof by construction :
    Let (x, y) be the inverse of (a, b).
  - Then

$$
\begin{aligned}
ax - by &= 1 \\
ay + bx &= 0
\end{aligned}
$$

  - Which is satisfied by :

$$
x = \frac{a}{a^2 + b^2}, \quad y = -\frac{b}{a^2 + b^2}
$$

    for $(a, b) \neq (0, 0)$.
  - Thus, $\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$ is the multiplicative inverse of (a, b).
- $\mathbb{C} \setminus \{(0, 0)\}$ is an Abelian group under $*$.
- $\{\mathbb{C}, +, *\}$ is a *field*(▸ ?).

- Consider the subset $R = \{(r, 0)\} \subset \mathbb{C}$.

The algebra of complex numbers

The reals

- Consider the subset $R = \{(r, 0)\} \subset \mathbb{C}$.
- Addition : $(r_1, 0) + (r_2, 0) = (r_1 + r_2, 0)$

The algebra of complex numbers

The reals

- Consider the subset $R = \{(r, 0)\} \subset \mathbb{C}$.
- Addition : $(r_1, 0) + (r_2, 0) = (r_1 + r_2, 0)$
- Multiplication : $(r_1, 0) * (r_2, 0) = (r_1 r_2, 0)$

- Consider the subset $R = \{(r, 0)\} \subset \mathbb{C}$.
- Addition : $(r_1, 0) + (r_2, 0) = (r_1 + r_2, 0)$
- Multiplication : $(r_1, 0) * (r_2, 0) = (r_1 r_2, 0)$
- The map $\vartheta : R \to \mathbb{R}$; $(r, 0) \mapsto r$ is a field isomorphism!

- Consider the subset $R = \{(r, 0)\} \subset \mathbb{C}$.
- Addition : $(r_1, 0) + (r_2, 0) = (r_1 + r_2, 0)$
- Multiplication : $(r_1, 0) * (r_2, 0) = (r_1 r_2, 0)$
- The map $\vartheta : R \longrightarrow \mathbb{R};\ (r, 0) \mapsto r$ is a field isomorphism!
- $\mathbb{C}$ has a subset, R, that is isomorphic to $\mathbb{R}$.

- Consider the subset $R = \{(r, 0)\} \subset \mathbb{C}$.
- Addition : $(r_1, 0) + (r_2, 0) = (r_1 + r_2, 0)$
- Multiplication : $(r_1, 0) * (r_2, 0) = (r_1 r_2, 0)$
- The map $\vartheta : R \longrightarrow \mathbb{R};\ (r, 0) \mapsto r$ is a field isomorphism!
- $\mathbb{C}$ has a subset, R, that is isomorphic to $\mathbb{R}$.
- We will henceforth denote $(r, 0)$ by r.

The algebra of complex numbers

Where is $\imath$?

- Consider $(0, 1) \in \mathbb{C}$.

The algebra of complex numbers

Where is $\imath$?

- Consider $(0, 1) \in \mathbb{C}$.
- Now,
  $(0, 1) * (0, 1)$

The algebra of complex numbers

Where is i?

- Consider $(0, 1) \in \mathbb{C}$.
- Now,
  $(0, 1) * (0, 1)$

The algebra of complex numbers

Where is $\imath$?

- Consider $(0,1) \in \mathbb{C}$.
- Now,
  $(0,1)*(0,1) = (0\cdot 0 - 1\cdot 1, 0\cdot 1 + 1\cdot 0)$

The algebra of complex numbers

Where is $\imath$?

- Consider $(0, 1) \in \mathbb{C}$.
- Now,
  $(0, 1) * (0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0)$

The algebra of complex numbers

Where is $\imath$?

- Consider $(0,1) \in \mathbb{C}$.
- Now,
  $(0,1)*(0,1) = (0\cdot 0 - 1\cdot 1, 0\cdot 1 + 1\cdot 0) = (-1,0)$!
- $(0,1)$ is the square root of -1!

The algebra of complex numbers

Where is $\imath$?

- Consider $(0,1) \in \mathbb{C}$.
- Now,
  $(0,1)*(0,1) = (0\cdot 0 - 1\cdot 1, 0\cdot 1 + 1\cdot 0) = (-1,0)$!
- $(0,1)$ is the square root of -1!
- Denoting $(0,1)$ by $\imath$, we have

The algebra of complex numbers
Where is $\imath$?

- Consider $(0, 1) \in \mathbb{C}$.
- Now,
  $(0, 1) * (0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0)$!
- $(0, 1)$ is the square root of -1!
- Denoting $(0, 1)$ by $\imath$, we have

The algebra of complex numbers

Where is $\mathfrak{i}$?

- Consider $(0, 1) \in \mathbb{C}$.
- Now,
  $(0, 1) * (0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0)$!
- $(0, 1)$ is the square root of -1!
- Denoting $(0, 1)$ by $\mathfrak{i}$, we have

$$(a, b) = (a, 0) * (1, 0) + (b, 0) * (0, 1)$$

The algebra of complex numbers

Where is $\mathfrak{i}$?

- Consider $(0,1) \in \mathbb{C}$.
- Now,
  $(0,1)*(0,1) = (0\cdot 0 - 1\cdot 1, 0\cdot 1 + 1\cdot 0) = (-1,0)$!
- $(0,1)$ is the square root of -1!
- Denoting $(0,1)$ by $\mathfrak{i}$, we have

$$(a,b) = (a,0)*(1,0) + (b,0)*(0,1) \equiv a + \mathfrak{i}b.$$

The algebra of complex numbers

Some useful definitions :

Given $z = (x, y) \equiv x + \imath y \in \mathbb{C}$

- Real part of z, $\Re(z) = x$.

The algebra of complex numbers

Some useful definitions :

Given $z = (x, y) \equiv x + \imath y \in \mathbb{C}$

- Real part of z, $\Re(z) = x$.
- Imaginary part of z, $\Im(z) = y$.

The algebra of complex numbers

Some useful definitions :

Given $z = (x, y) \equiv x + \imath y \in \mathbb{C}$

- Real part of z, $\Re(z) = x$.
- Imaginary part of z, $\Im(z) = y$.
- Complex conjugate of z, $\bar{z} \equiv (x, -y) \equiv x - \imath y$.

The algebra of complex numbers

Some useful definitions :

Given $z = (x, y) \equiv x + \imath y \in \mathbb{C}$

- Real part of z, $\Re(z) = x$.
- Imaginary part of z, $\Im(z) = y$.
- Complex conjugate of z, $\bar{z} \equiv (x, -y) \equiv x - \imath y$.
- Magnitude of z, $|z| = \sqrt{x^2 + y^2} = \sqrt{z\bar{z}}$.

The algebra of complex numbers

Some useful definitions :

Given $z = (x, y) \equiv x + \imath y \in \mathbb{C}$

- Real part of z, $\Re(z) = x$.
- Imaginary part of z, $\Im(z) = y$.
- Complex conjugate of z, $\bar{z} \equiv (x, -y) \equiv x - \imath y$.
- Magnitude of z, $|z| = \sqrt{x^2 + y^2} = \sqrt{z\bar{z}}$.
- Argument of z, $\arg(z) = \tan^{-1}\left(\frac{y}{x}\right)$, with $\cos(\arg(z)) = \frac{x}{|z|}, \sin(\arg(z)) = \frac{y}{|z|}$

The algebra of complex numbers

Some useful definitions :

Given $z = (x, y) \equiv x + \imath y \in \mathbb{C}$

- Real part of z, $\Re(z) = x$.
- Imaginary part of z, $\Im(z) = y$.
- Complex conjugate of z, $\bar{z} \equiv (x, -y) \equiv x - \imath y$.
- Magnitude of z, $|z| = \sqrt{x^2 + y^2} = \sqrt{z\bar{z}}$.
- Argument of z, $\arg\,(z) = \tan^{-1}\left(\frac{y}{x}\right)$, with $\cos(\arg\,(z)) = \frac{x}{|z|}, \sin(\arg\,(z)) = \frac{y}{|z|}$
- If $|z| = r$ and $\arg(z) = \theta$, we can write

$$z = r(\cos\theta + \imath\sin\theta) = r\angle\theta = re^{\imath\theta}$$

Some properties of complex conjugation

- $\overline{(z_1 + z_2)} = \overline{z_1} + \overline{z_2}$

Some properties of complex conjugation

- $\overline{(z_1 + z_2)} = \overline{z_1} + \overline{z_2}$
- $\overline{z_1 z_2} = \overline{z_1}\ \overline{z_2}$

Some properties of complex conjugation

- $\overline{(z_1 + z_2)} = \overline{z_1} + \overline{z_2}$
- $\overline{z_1 z_2} = \overline{z_1}\ \overline{z_2}$
- Hence, for any polynomial $P(z)$ with **real** coefficients, $\overline{P(z)} = P(\overline{z})$.

Some properties of complex conjugation

- $\overline{(z_1 + z_2)} = \overline{z_1} + \overline{z_2}$
- $\overline{z_1 z_2} = \overline{z_1}\ \overline{z_2}$
- Hence, for any polynomial $P(z)$ with **real** coefficients, $\overline{P(z)} = P(\overline{z})$.
- For more general polynomials, we have $\overline{P(z)} = \bar{P}(\overline{z})$, where $\bar{P}$ is the polynomial we obtain by replacing each coeffient of P by its complex conjugate.

Some properties of complex conjugation

- $\overline{(z_1 + z_2)} = \overline{z_1} + \overline{z_2}$
- $\overline{z_1 z_2} = \overline{z_1}\ \overline{z_2}$
- Hence, for any polynomial $P(z)$ with **real** coefficients, $\overline{P(z)} = P(\overline{z})$.
- For more general polynomials, we have $\overline{P(z)} = \bar{P}(\overline{z})$, where $\bar{P}$ is the polynomial we obtain by replacing each coeffient of P by its complex conjugate.
- This extends to general functions!

Arg and arg

- $\arg(z)$ is multiple valued.

Arg and arg

- $\arg(z)$ is multiple valued.
- If θ is an argument of z, so is $\theta + 2n\pi$, with $n \in \mathbb{Z}$.

Arg and arg

- $\arg(z)$ is multiple valued.
- If θ is an argument of z, so is $\theta + 2n\pi$, with $n \in \mathbb{Z}$.
- $\mathrm{Arg}(z)$, the principle argument of z, is defined by restricting θ to a particular 2π interval.

Arg and arg

- $\arg(z)$ is multiple valued.
- If θ is an argument of z, so is $\theta + 2n\pi$, with $n \in \mathbb{Z}$.
- $\mathrm{Arg}(z)$, the principle argument of z, is defined by restricting θ to a particular 2π interval.
- Usually, $0 \leq \mathrm{Arg}(z) < 2\pi$, though $-\pi \leq \mathrm{Arg}(z) < \pi$ is also used.

The algebra of complex numbers

Another construction :

- The set of all polynomials (▸ ?) with real coefficients, $\mathbb{R}[X]$ is a ring.

The algebra of complex numbers

Another construction :

- The set of all polynomials (▸ ?) with real coefficients, $\mathbb{R}[X]$ is a ring.
- Given a fixed polynomial $K \in \mathbb{R}[X]$, we define a relation $\sim$ by

$$P \sim Q \text{ if } \exists S \in \mathbb{R}[X] : P - Q = SK$$

The algebra of complex numbers

Another construction :

- The set of all polynomials (?) with real coefficients, $\mathbb{R}[X]$ is a ring.
- Given a fixed polynomial $K \in \mathbb{R}[X]$, we define a relation $\sim$ by

$$P \sim Q \text{ if } \exists S \in \mathbb{R}[X] : P - Q = SK$$

  - $\sim$ is reflexive : $P \sim P, \forall P \in \mathbb{R}[X]$.

The algebra of complex numbers

Another construction :

- The set of all polynomials (▸ ?) with real coefficients, $\mathbb{R}[X]$ is a ring.
- Given a fixed polynomial $K \in \mathbb{R}[X]$, we define a relation $\sim$ by

$$P \sim Q \text{ if } \exists S \in \mathbb{R}[X] : P - Q = SK$$

  - $\sim$ is reflexive : $P \sim P, \forall P \in \mathbb{R}[X]$.
  - $\sim$ is symmetric : $P \sim Q \implies Q \sim P, \forall P, Q \in \mathbb{R}[X]$.

The algebra of complex numbers

Another construction :

- The set of all polynomials (?) with real coefficients, $\mathbb{R}[X]$ is a ring.
- Given a fixed polynomial $K \in \mathbb{R}[X]$, we define a relation $\sim$ by

$$P \sim Q \text{ if } \exists S \in \mathbb{R}[X] : P - Q = SK$$

  - $\sim$ is reflexive : $P \sim P, \forall P \in \mathbb{R}[X]$.
  - $\sim$ is symmetric : $P \sim Q \implies Q \sim P, \forall P, Q \in \mathbb{R}[X]$.
  - $\sim$ is transitive : $P \sim Q$ and $Q \sim R \implies P \sim R, \forall P, Q, R \in \mathbb{R}[X]$.

The algebra of complex numbers

Another construction :

- The set of all polynomials (?) with real coefficients, $\mathbb{R}[X]$ is a ring.
- Given a fixed polynomial $K \in \mathbb{R}[X]$, we define a relation $\sim$ by

$$P \sim Q \text{ if } \exists S \in \mathbb{R}[X] : P - Q = SK$$

  - $\sim$ is reflexive : $P \sim P, \forall P \in \mathbb{R}[X]$.
  - $\sim$ is symmetric : $P \sim Q \implies Q \sim P, \forall P, Q \in \mathbb{R}[X]$.
  - $\sim$ is transitive : $P \sim Q$ and $Q \sim R \implies P \sim R, \forall P, Q, R \in \mathbb{R}[X]$.
- $\sim$ is an equivalence relation.

The algebra of complex numbers

- Define the equivalence class

$$[P] = \{Q \in \mathbb{R}[x] : Q \sim P\}.$$

The algebra of complex numbers

- Define the equivalence class

$$[P] = \{Q \in \mathbb{R}[x] : Q \sim P\}.$$

- We denote the set of all the equivalence classes by $\mathbb{R}[X]/K$.

The algebra of complex numbers

- Define the equivalence class

$$[P] = \{Q \in \mathbb{R}[x] : Q \sim P\}.$$

- We denote the set of all the equivalence classes by $\mathbb{R}[X]/K$.
- Define addition on $\mathbb{R}[X]/K$ by

$$[P] + [Q] = [P + Q].$$

The algebra of complex numbers

- Define the equivalence class
$$[P] = \{Q \in \mathbb{R}[x] : Q \sim P\}.$$
- We denote the set of all the equivalence classes by $\mathbb{R}[X]/K$.
- Define addition on $\mathbb{R}[X]/K$ by
$$[P] + [Q] = [P + Q].$$
- $+$ as defined above is well defined on $\mathbb{R}[X]/K$ (?).

The algebra of complex numbers

- Define the equivalence class
$$[P] = \{Q \in \mathbb{R}[x] : Q \sim P\}.$$
- We denote the set of all the equivalence classes by $\mathbb{R}[X]/K$.
- Define addition on $\mathbb{R}[X]/K$ by
$$[P] + [Q] = [P + Q].$$
- $+$ as defined above is well defined on $\mathbb{R}[X]/K$ (?).
- Define multiplication on $\mathbb{R}[X]/K$ by
$$[P][Q] = [PQ].$$

The algebra of complex numbers

- Given $P \in \mathbb{R}[X]$, there exists unique polynomials $S, R \in \mathbb{R}[X]$ such that

$$P(X) = S(X)K(X) + R(X), \qquad \deg(R) < \deg(K)$$

The algebra of complex numbers

- Given $P \in \mathbb{R}[X]$, there exists unique polynomials $S, R \in \mathbb{R}[X]$ such that

$$P(X) = S(X)K(X) + R(X), \qquad \deg(R) < \deg(K)$$

- Every polynomial is equivalent under $\sim$ to a unique polynomial of degree lower than K.

The algebra of complex numbers

- Given $P \in \mathbb{R}[X]$, there exists unique polynomials $S, R \in \mathbb{R}[X]$ such that

$$P(X) = S(X)K(X) + R(X), \qquad \deg(R) < \deg(K)$$

- Every polynomial is equivalent under $\sim$ to a unique polynomial of degree lower than K.
- If K is a quadratic polynomial, all polynomials are equivalent to a linear polynomial.

$$P(X) \sim a + bX$$

The algebra of complex numbers

- Given $P \in \mathbb{R}[X]$, there exists unique polynomials $S, R \in \mathbb{R}[X]$ such that

$$P(X) = S(X)K(X)+R(X), \qquad \deg(R) < \deg(K)$$

- Every polynomial is equivalent under $\sim$ to a unique polynomial of degree lower than K.
- If K is a quadratic polynomial, all polynomials are equivalent to a linear polynomial.

$$P(X) \sim a + bX$$

- We can label elements of $\mathbb{R}[X]/K$ by linear polynomials $a + bX$.

The algebra of complex numbers

- $[P] + [Q] = [P + Q] \implies$
  $[a + bX] + [c + dX] = [(a + c) + (b + d)X]$

The algebra of complex numbers

- $[P] + [Q] = [P + Q] \implies [a + bX] + [c + dX] = [(a + c) + (b + d)X]$
- $[a + bX][c + dX] = [(a + bX)(c + dX)] = [ac + (bc + ad)X + bdX^2]$

The algebra of complex numbers

- $[P] + [Q] = [P + Q] \implies [a + bX] + [c + dX] = [(a + c) + (b + d)X]$
- $[a + bX][c + dX] = [(a + bX)(c + dX)] = [ac + (bc + ad)X + bdX^2]$
- Choose $K(X) = 1 + X^2$.

The algebra of complex numbers

- $[P] + [Q] = [P + Q] \implies$ $[a + bX] + [c + dX] = [(a + c) + (b + d)X]$
- $[a + bX][c + dX] = [(a + bX)(c + dX)] =$ $[ac + (bc + ad)X + bdX^2]$
- Choose $K(X) = 1 + X^2$.
- Then, $1 + X^2 \sim 0$, so that $ac+(bc+ad)X+bdX^2 \sim (ac-bd)+(bc+ad)X$

The algebra of complex numbers

- $[P] + [Q] = [P + Q] \implies$
  $[a + bX] + [c + dX] = [(a + c) + (b + d)X]$
- $[a + bX][c + dX] = [(a + bX)(c + dX)] =$
  $[ac + (bc + ad)X + bdX^2]$
- Choose $K(X) = 1 + X^2$.
- Then, $1 + X^2 \sim 0$, so that
  $ac + (bc + ad)X + bdX^2 \sim (ac - bd) + (bc + ad)X$
- $[a + bX][c + dX] = [(ac - bd) + (bc + ad)X]$

The algebra of complex numbers

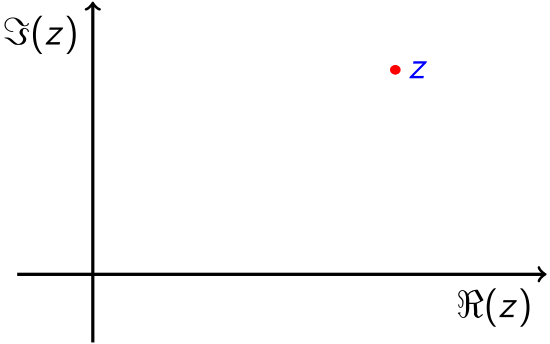
- $[P] + [Q] = [P + Q] \implies [a + bX] + [c + dX] = [(a + c) + (b + d)X]$
- $[a + bX][c + dX] = [(a + bX)(c + dX)] = [ac + (bc + ad)X + bdX^2]$
- Choose $K(X) = 1 + X^2$.
- Then, $1 + X^2 \sim 0$, so that $ac + (bc + ad)X + bdX^2 \sim (ac - bd) + (bc + ad)X$
- $[a + bX][c + dX] = [(ac - bd) + (bc + ad)X]$
- $\mathbb{R}[X]/\left(X^2 + 1\right)$ is isomorphic to $\mathbb{C}$!

The geometry of complex numbers

- There is an obvious set bijection between $\mathbb{C}$ to $\mathbb{R}^2$.
- We can use the same geometric representation for both!

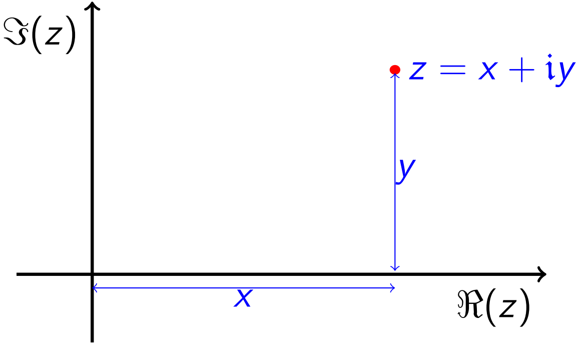
The geometry of complex numbers

- There is an obvious set bijection between $\mathbb{C}$ to $\mathbb{R}^2$.
- We can use the same geometric representation for both!



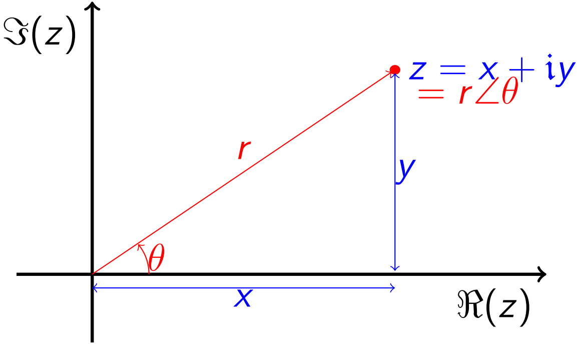
The geometry of complex numbers

- There is an obvious set bijection between $\mathbb{C}$ to $\mathbb{R}^2$.
- We can use the same geometric representation for both!



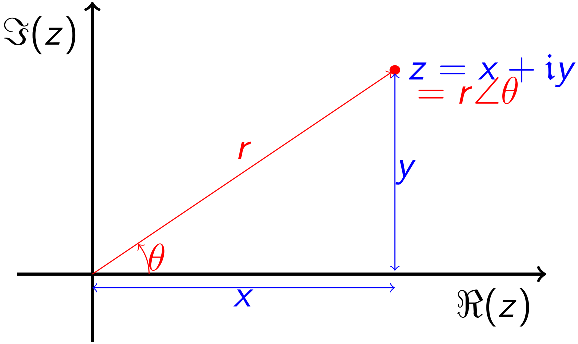
The geometry of complex numbers

- There is an obvious set bijection between $\mathbb{C}$ to $\mathbb{R}^2$.
- We can use the same geometric representation for both!



The geometry of complex numbers

- There is an obvious set bijection between $\mathbb{C}$ to $\mathbb{R}^2$.
- We can use the same geometric representation for both!



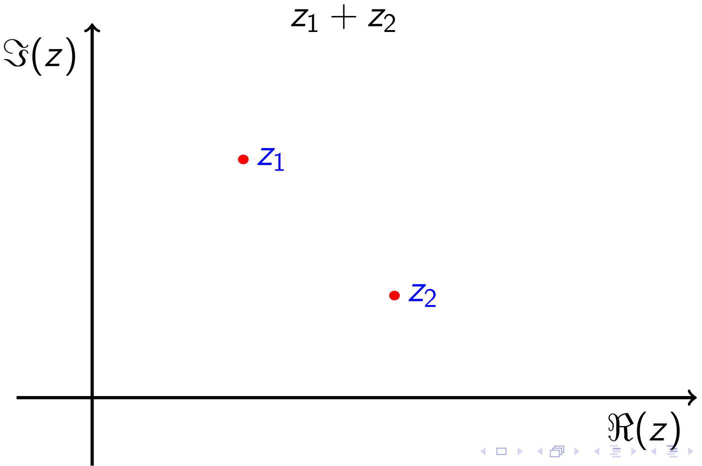
$$z = x + \imath y = r\cos\theta + \imath r\sin\theta = r\angle\theta$$

The geometry of addition

The addition of complex numbers is the same as addition of vectors in two dimensions!

The geometry of addition

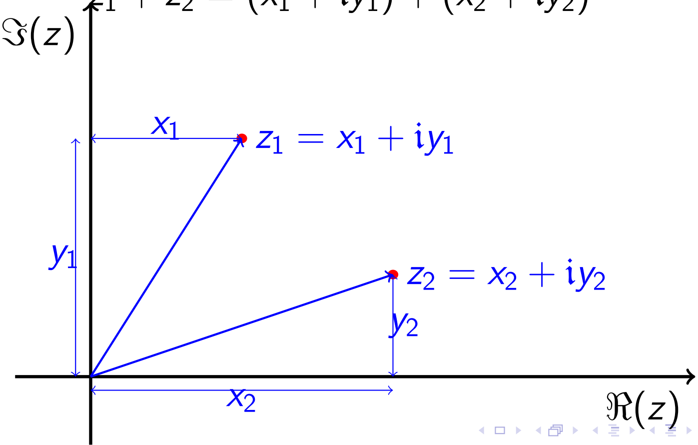
The addition of complex numbers is the same as addition of vectors in two dimensions!



The geometry of addition

The addition of complex numbers is the same as addition of vectors in two dimensions!

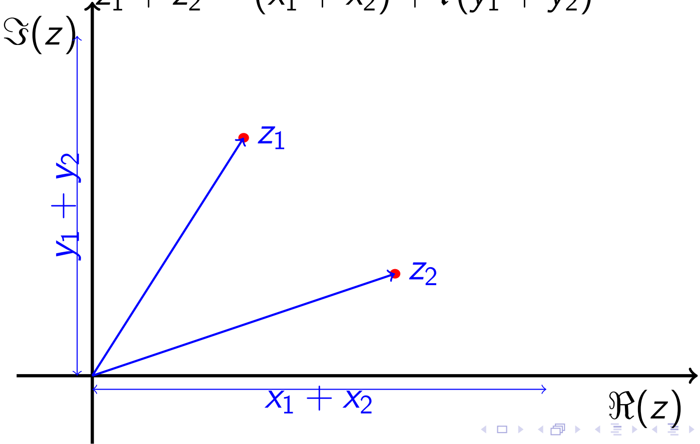
$$z_1 + z_2 = (x_1 + \imath y_1) + (x_2 + \imath y_2)$$



The geometry of addition

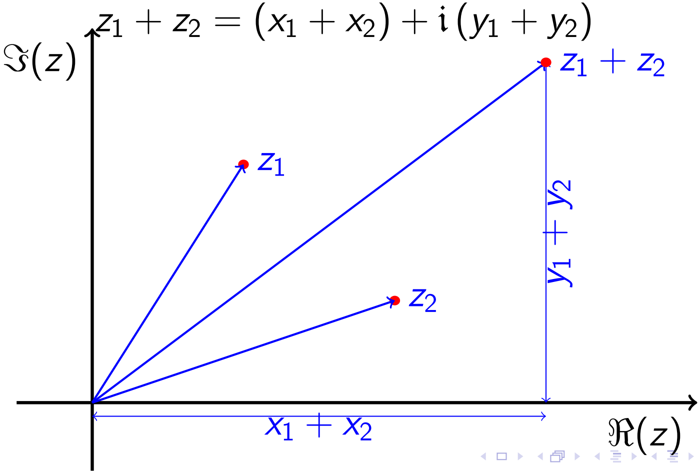
The addition of complex numbers is the same as addition of vectors in two dimensions!

$$z_1 + z_2 = (x_1 + x_2) + \mathrm{i}\,(y_1 + y_2)$$



The geometry of addition

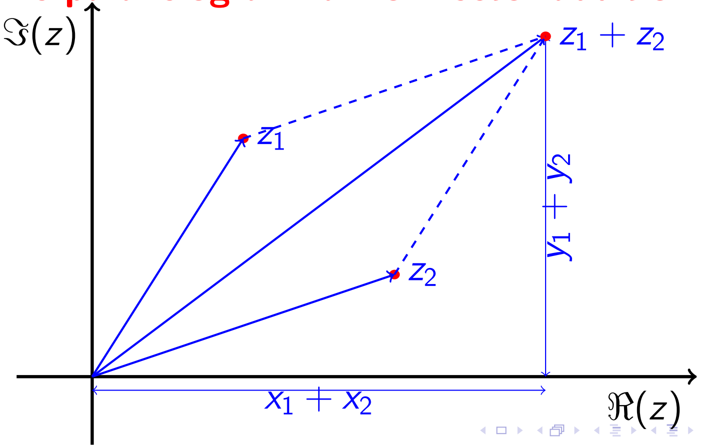
The addition of complex numbers is the same as addition of vectors in two dimensions!



The geometry of addition

The addition of complex numbers is the same as addition of vectors in two dimensions!

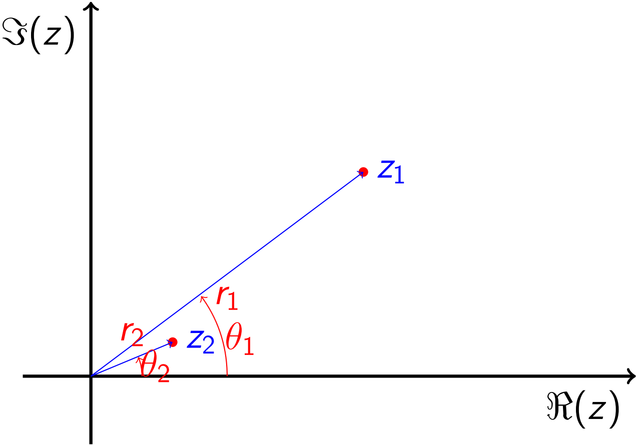
The parallelogram law of vector addition!



Geometry of multiplication

It helps to use the polar representation!

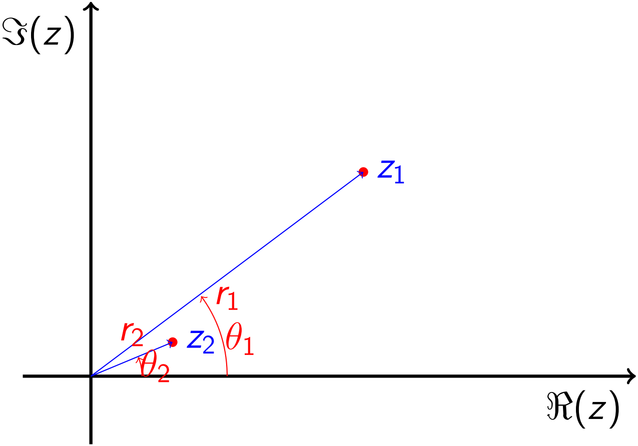
$$z_1 z_2 \;=\; r_1\angle\theta_1 \cdot r_2\angle\theta_2$$



Geometry of multiplication

It helps to use the polar representation!

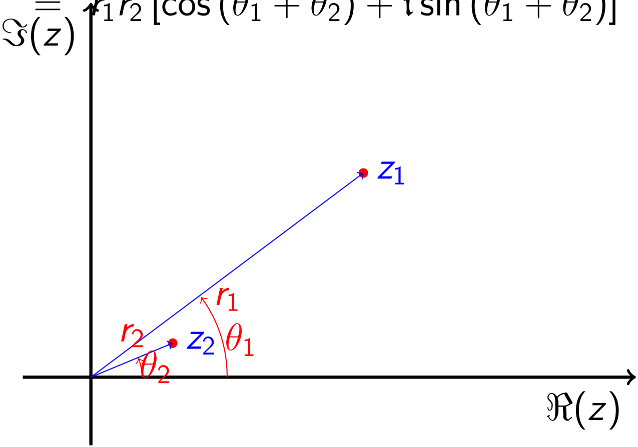
$$z_1 z_2 \;=\; r_1\left(\cos\theta_1 + \mathfrak{i}\sin\theta_1\right)\cdot r_2\left(\cos\theta_2 + \mathfrak{i}\sin\theta_2\right)$$



Geometry of multiplication

It helps to use the polar representation!

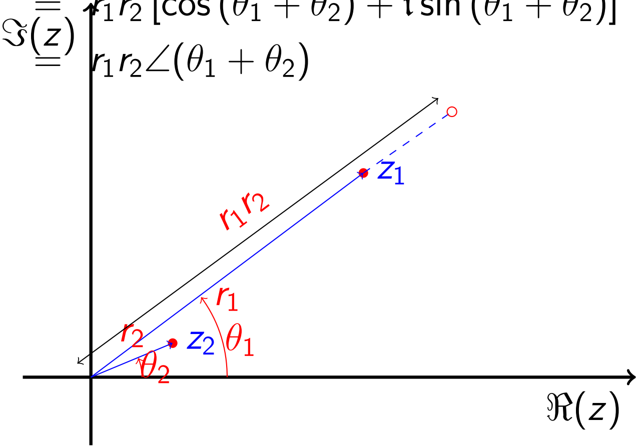
$$\begin{aligned} z_1 z_2 &= r_1 (\cos\theta_1 + \mathfrak{i}\sin\theta_1) \cdot r_2 (\cos\theta_2 + \mathfrak{i}\sin\theta_2) \\ &= r_1 r_2 [\cos(\theta_1 + \theta_2) + \mathfrak{i}\sin(\theta_1 + \theta_2)] \end{aligned}$$



Geometry of multiplication

It helps to use the polar representation!

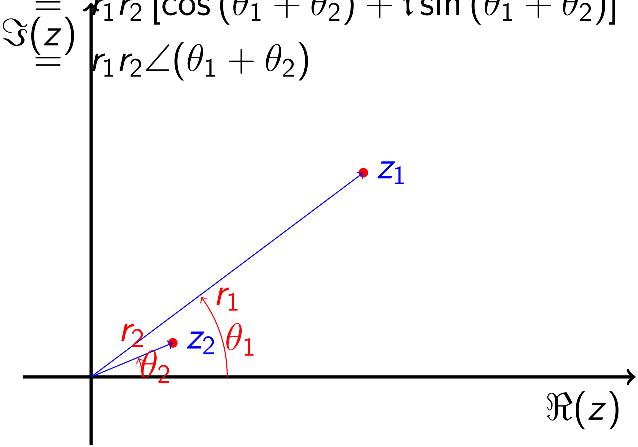
$$\begin{aligned} z_1 z_2 &= r_1 (\cos\theta_1 + \mathfrak{i}\sin\theta_1) \cdot r_2 (\cos\theta_2 + \mathfrak{i}\sin\theta_2) \\ &= r_1 r_2 [\cos(\theta_1+\theta_2) + \mathfrak{i}\sin(\theta_1+\theta_2)] \\ &= r_1 r_2 \angle(\theta_1+\theta_2) \end{aligned}$$



Geometry of multiplication

It helps to use the polar representation!

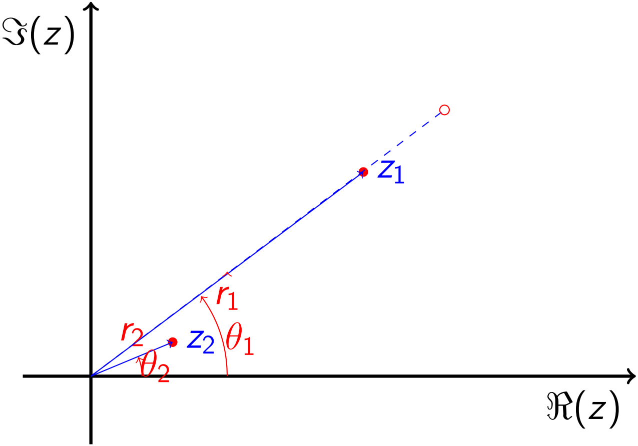
$$\begin{aligned} z_1 z_2 &= r_1 (\cos\theta_1 + \mathfrak{i}\sin\theta_1) \cdot r_2 (\cos\theta_2 + \mathfrak{i}\sin\theta_2) \\ &= r_1 r_2 \left[\cos(\theta_1 + \theta_2) + \mathfrak{i}\sin(\theta_1 + \theta_2)\right] \\ &= r_1 r_2 \angle(\theta_1 + \theta_2) \end{aligned}$$



Geometry of multiplication

It helps to use the polar representation!

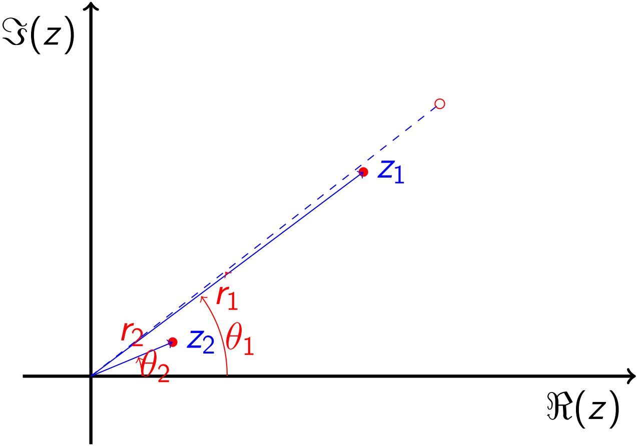
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

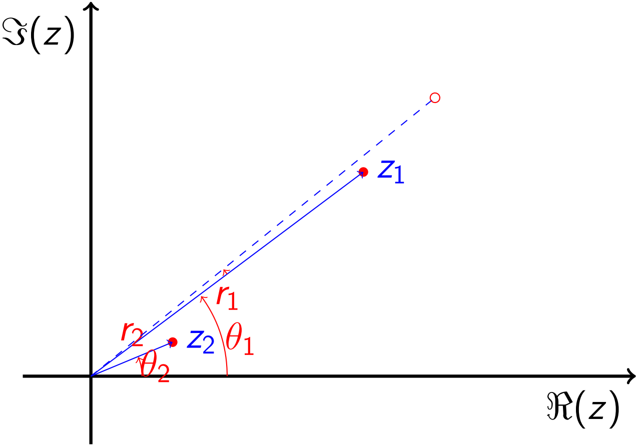
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

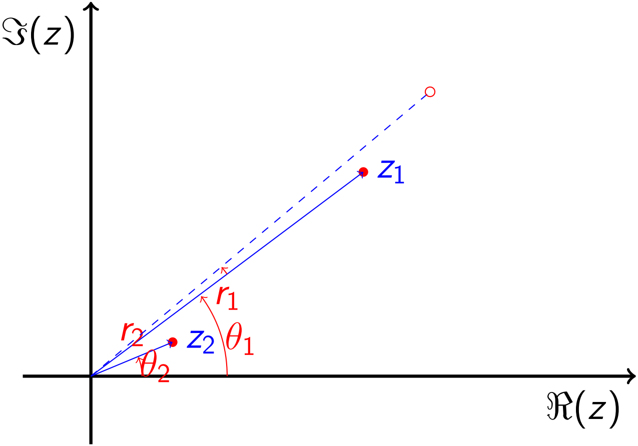
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

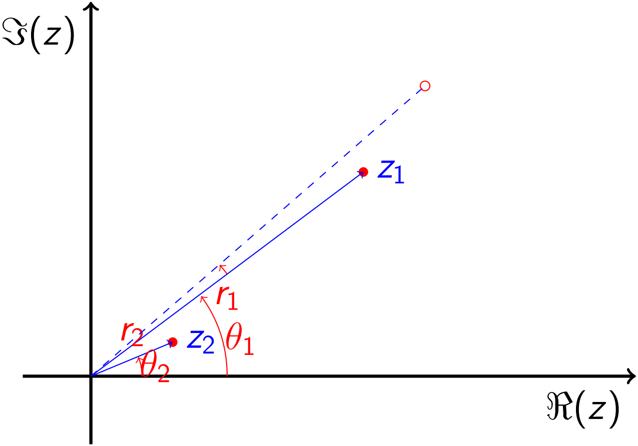
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

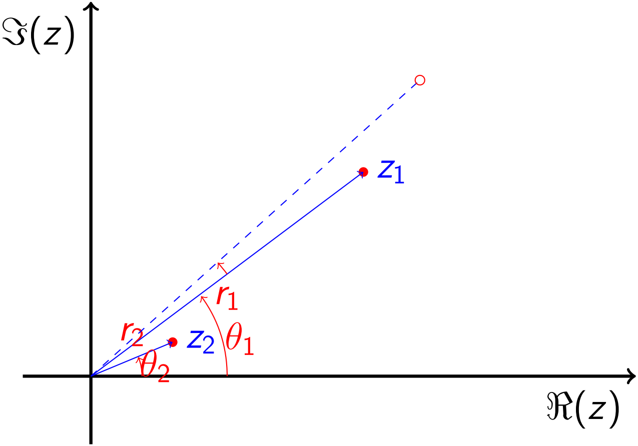
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

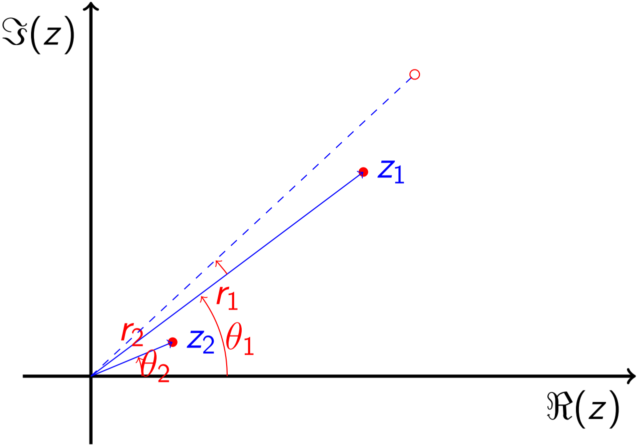
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

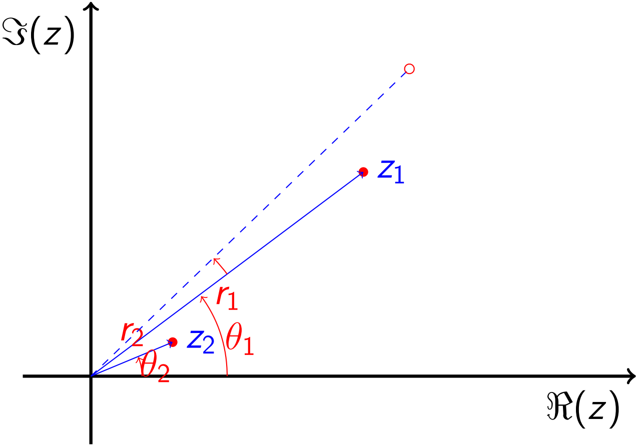
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

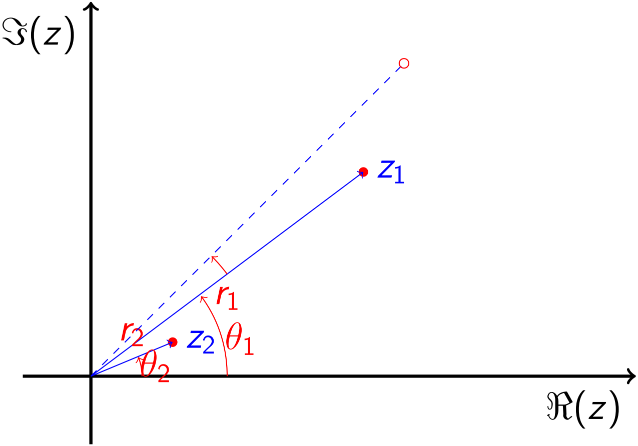
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

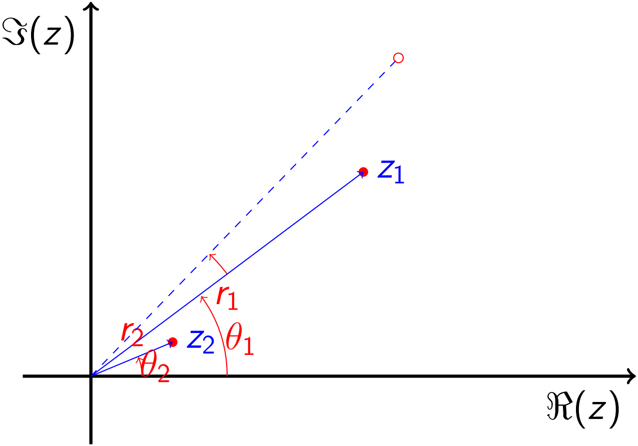
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

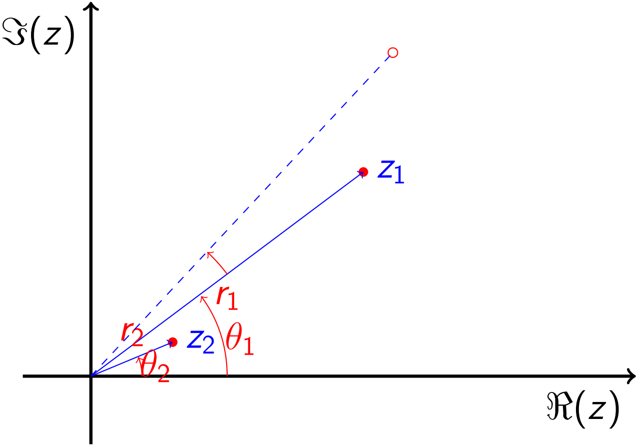
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

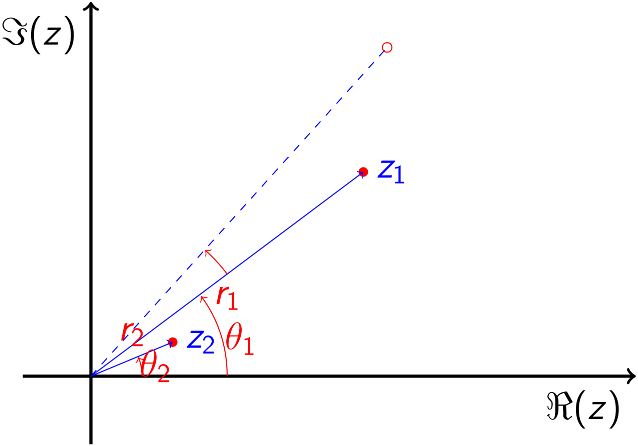
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

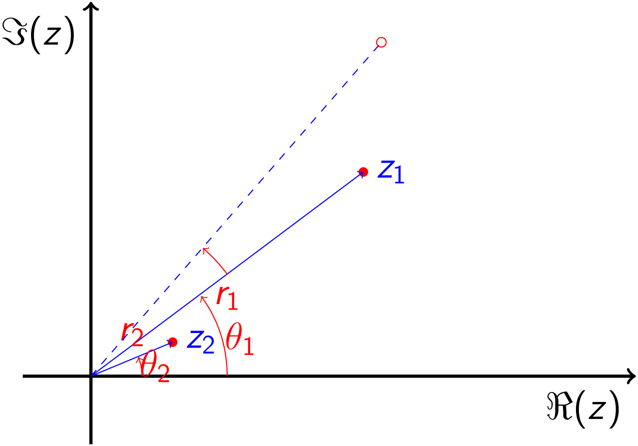
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

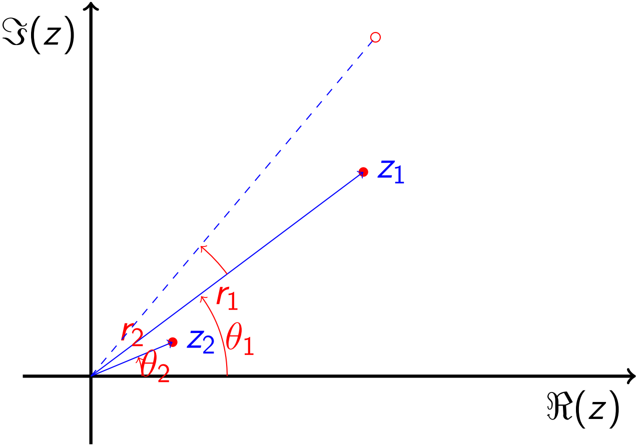
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

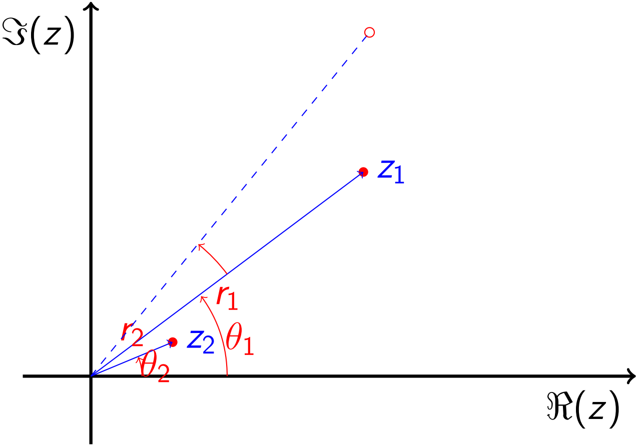
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

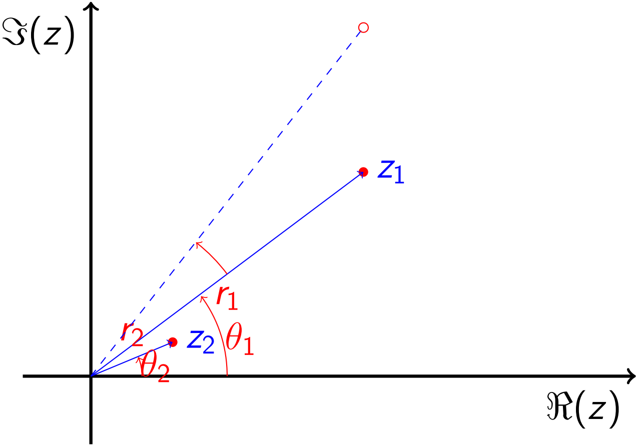
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

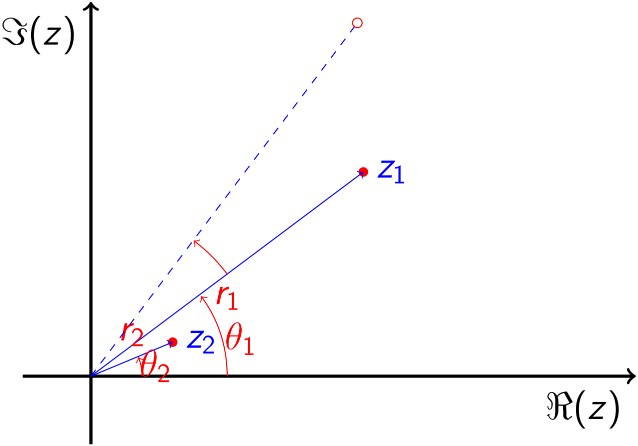
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

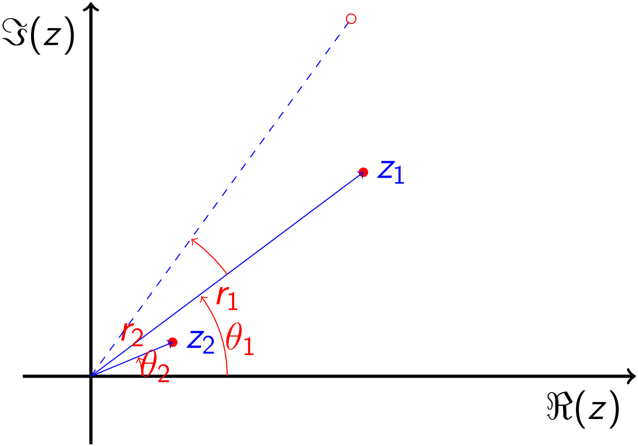
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

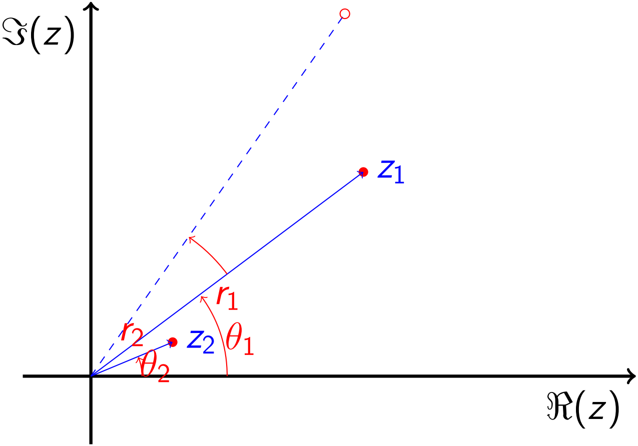
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

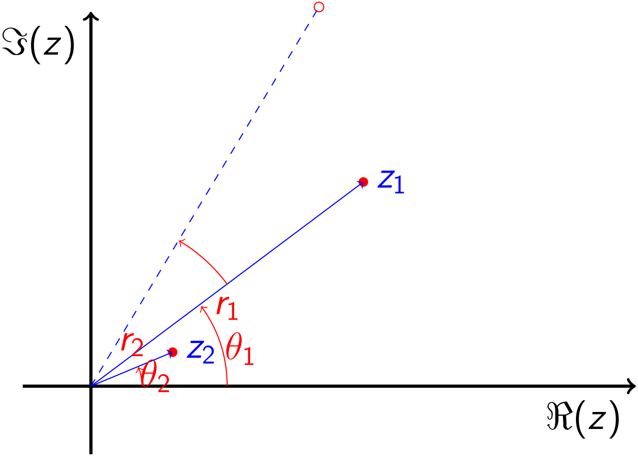
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

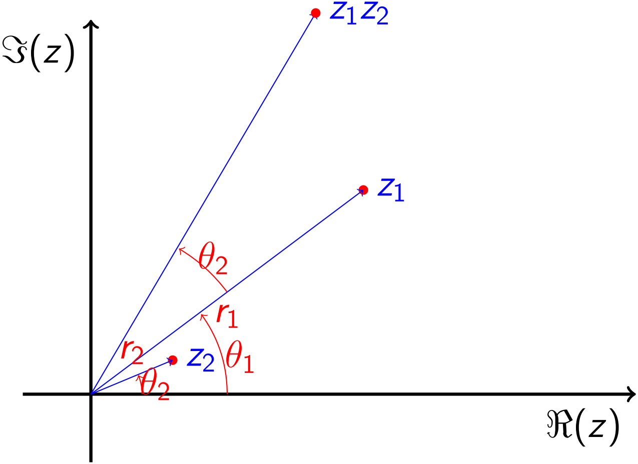
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

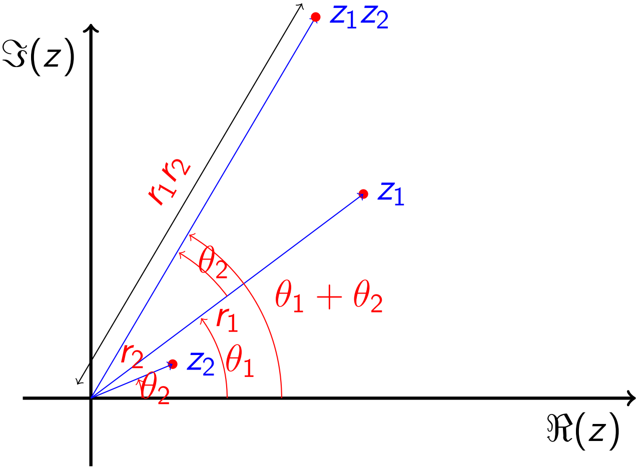
$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$



Geometry of multiplication

It helps to use the polar representation!

$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$

Multiplying several complex numbers :

$z_1 z_2 \dots z_n$

Geometry of multiplication

It helps to use the polar representation!

$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$

Multiplying several complex numbers :

$$z_1 z_2 \ldots z_n = r_1 r_2 \ldots r_n \angle(\theta_1 + \theta_2 + \ldots \theta_n)$$

Geometry of multiplication

It helps to use the polar representation!

$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$

Multiplying several complex numbers :

$$z_1 z_2 \ldots z_n = r_1 r_2 \ldots r_n \angle(\theta_1 + \theta_2 + \ldots \theta_n)$$

Powers of complex numbers :

$$z^n$$

Geometry of multiplication

It helps to use the polar representation!

$$z_1 z_2 = r_1 r_2 \angle(\theta_1 + \theta_2)$$

Multiplying several complex numbers :

$$z_1 z_2 \ldots z_n = r_1 r_2 \ldots r_n \angle(\theta_1 + \theta_2 + \ldots \theta_n)$$

Powers of complex numbers :

$$z^n = r^n \angle n\theta$$

Geometry behind Euler's roots of unity

A reminder :

The roots of $z^n = 1$ *lie on the vertices of a regular n-sided polygon inscribed inside a unit circle.*

- *Euler*

Geometry behind Euler's roots of unity

A reminder :

> *The roots of $z^n = 1$ lie on the vertices of a regular n-sided polygon inscribed inside a unit circle.*
>
> \- *Euler*

The vertices $z_m,\ m \in \{0, 1, 2, \ldots, n-1\}$ are at $z_m = 1\angle\left(\frac{2\pi m}{n}\right)$.

Geometry behind Euler's roots of unity

A reminder :

The roots of $z^n = 1$ lie on the vertices of a regular n-sided polygon inscribed inside a unit circle.

- Euler

The vertices $z_m,\ m \in \{0, 1, 2, \ldots, n-1\}$ are at $z_m = 1\angle\left(\frac{2\pi m}{n}\right)$.

Thus

$$(z_m)^n$$

Geometry behind Euler's roots of unity

A reminder :

> *The roots of $z^n = 1$ lie on the vertices of a regular n-sided polygon inscribed inside a unit circle.*
>
> \- *Euler*

The vertices $z_m,\ m \in \{0, 1, 2, \ldots, n-1\}$ are at $z_m = 1\angle\left(\frac{2\pi m}{n}\right)$.
Thus

$$(z_m)^n = 1^n \angle n\left(\frac{2\pi m}{n}\right)$$

Geometry behind Euler's roots of unity

A reminder :

The roots of $z^n = 1$ lie on the vertices of a regular n-sided polygon inscribed inside a unit circle.

- *Euler*

The vertices $z_m, \; m \in \{0, 1, 2, \ldots, n-1\}$ are at $z_m = 1\angle\left(\frac{2\pi m}{n}\right)$.

Thus

$$(z_m)^n = 1^n \angle n\left(\frac{2\pi m}{n}\right) = 1\angle 2\pi$$

Geometry behind Euler's roots of unity

A reminder :

The roots of $z^n = 1$ lie on the vertices of a regular n-sided polygon inscribed inside a unit circle.

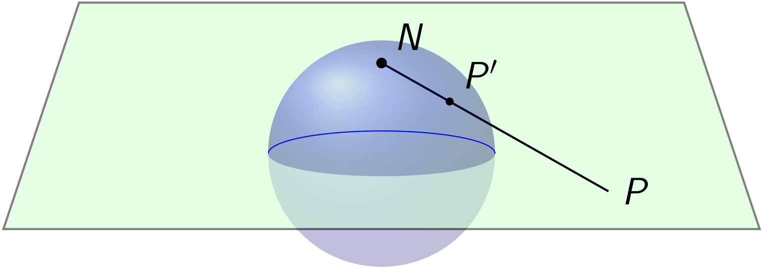
- Euler

The vertices $z_m,\ m \in \{0, 1, 2, \ldots, n-1\}$ are at $z_m = 1\angle\left(\frac{2\pi m}{n}\right)$.

Thus

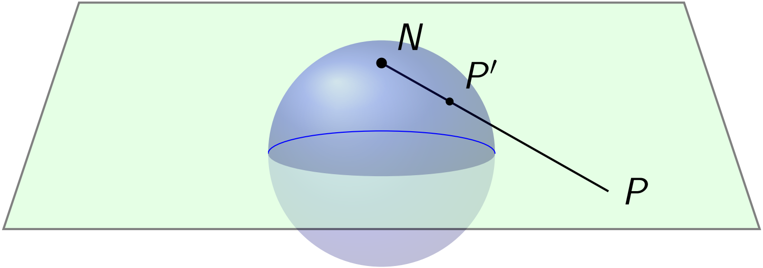
$$(z_m)^n = 1^n \angle n \left(\frac{2\pi m}{n}\right) = 1\angle 2\pi = 1 + \imath 0$$

The Riemann sphere



The Riemann sphere is an alternative geometric representation of complex numbers.

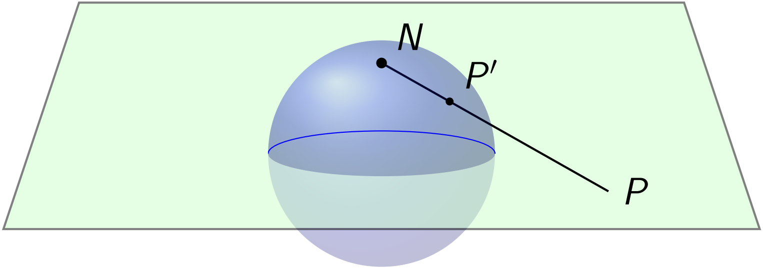
The Riemann sphere



The Riemann sphere is an alternative geometric representation of complex numbers.

The point P' where the straight line joining the "north pole" $N = (0, 0, 1)$ of the unit sphere centered at the origin to the point $P = (x, y, 0)$ represents the complex number $\zeta = x + iy$.

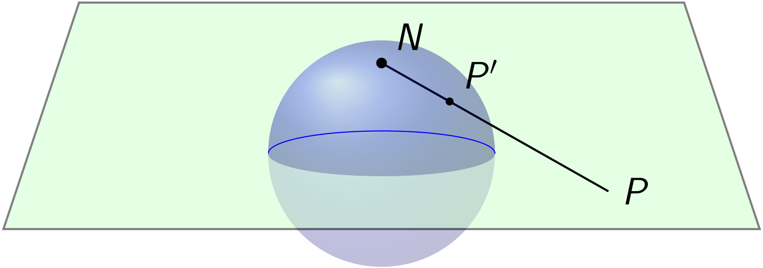
The Riemann sphere



The Riemann sphere is an alternative geometric representation of complex numbers.

Numbers inside the unit circle, $|\zeta| < 1$, are represented by the southern hemisphere.

The Riemann sphere

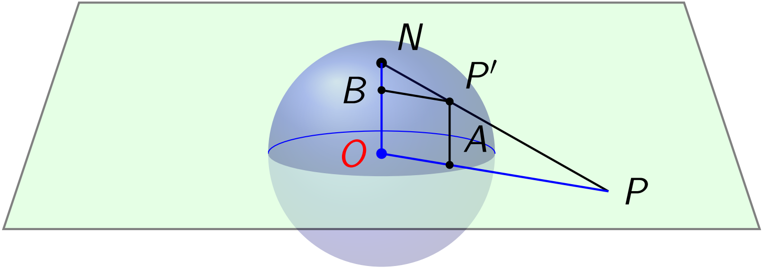


The Riemann sphere is an alternative geometric representation of complex numbers.

Numbers inside the unit circle, $|\zeta| < 1$, are represented by the southern hemisphere.

The north pole represents the *“point at infinity”!*

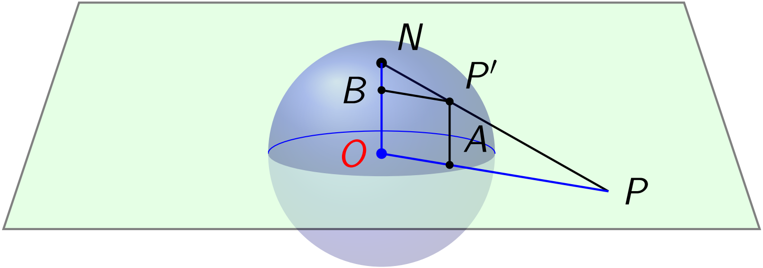
The Riemann sphere



$$O = (0,0,0), \quad N = (0,0,1), \quad P = (x,y,0)$$

$$P' = (x',y',z')\,, \quad A = (x',y',0) \quad B = (0,0,z')$$

The Riemann sphere

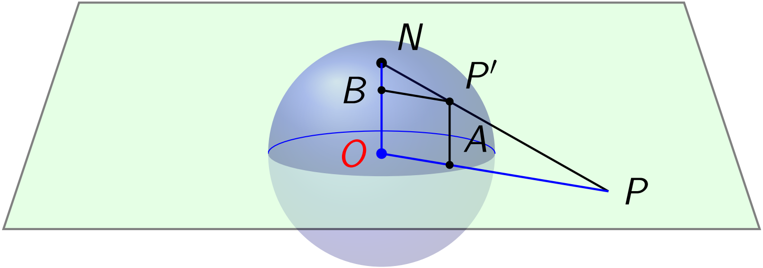


$$O = (0,0,0), \quad N = (0,0,1), \quad P = (x, y, 0)$$

$$P' = (x', y', z'), \quad A = (x', y', 0) \quad B = (0, 0, z')$$

The triangles $\Delta NPO, \Delta NP'B, \Delta P'PA$ are similar.

The Riemann sphere

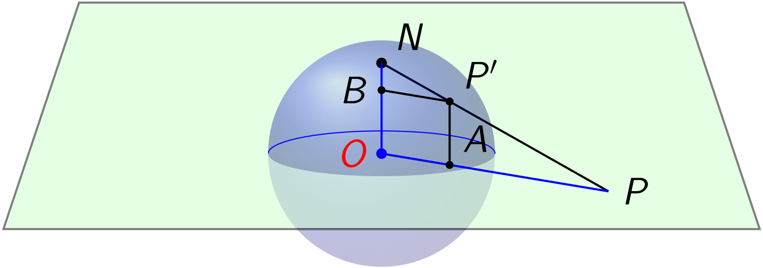


$$O = (0,0,0), \quad N = (0,0,1), \quad P = (x,y,0)$$

$$P' = (x', y', z'), \quad A = (x', y', 0) \quad B = (0,0,z')$$

$$\frac{\overline{OA}}{\overline{OP}} = \frac{\overline{NP'}}{\overline{NP}} = \frac{\overline{NB}}{\overline{NO}} = 1 - z'$$

The Riemann sphere

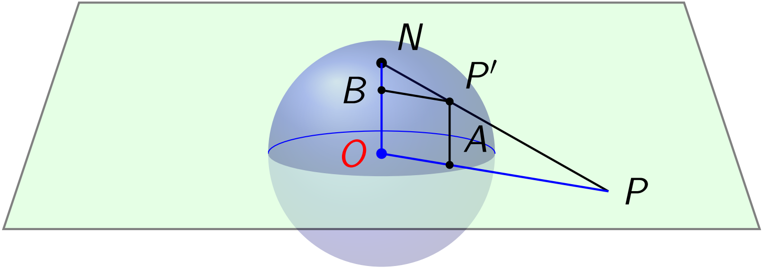


$$O = (0,0,0), \quad N = (0,0,1), \quad P = (x,y,0)$$

$$P' = (x',y',z'), \quad A = (x',y',0) \quad B = (0,0,z')$$

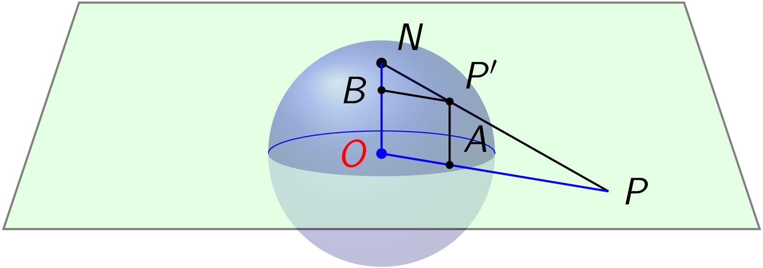
$$\frac{x'}{x} = \frac{y'}{y} = 1 - z'$$

The Riemann sphere



$$\frac{x'}{x} = \frac{y'}{y} = \frac{x' + \mathfrak{i}y'}{x + \mathfrak{i}y} = 1 - z'$$

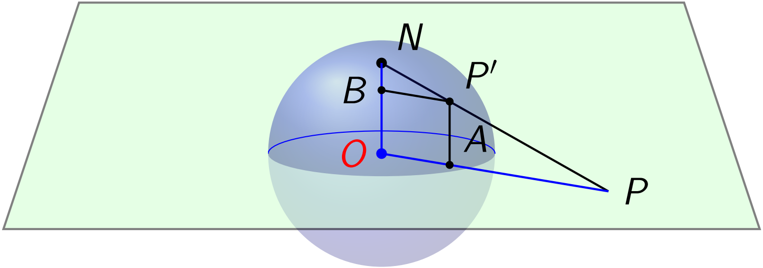
The Riemann sphere



$$\frac{x'}{x} = \frac{y'}{y} = \frac{x' + iy'}{x + iy} = 1 - z'$$

$$\zeta = x + iy = \frac{x' + iy'}{1 - z'}$$

The Riemann sphere

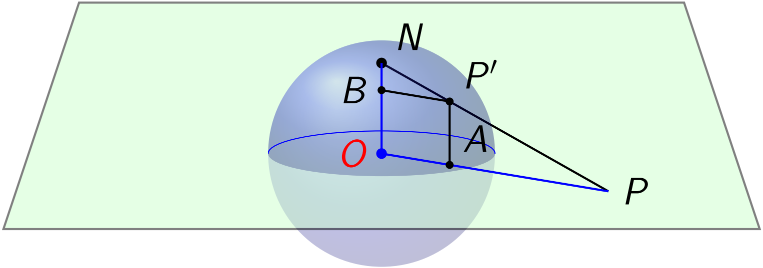


$$\frac{x'}{x} = \frac{y'}{y} = 1 - z'$$

$$\zeta = x + iy = \frac{x' + iy'}{1 - z'}$$

$$|\zeta|^2 = \frac{x'^2 + y'^2}{(1 - z')^2}$$

The Riemann sphere

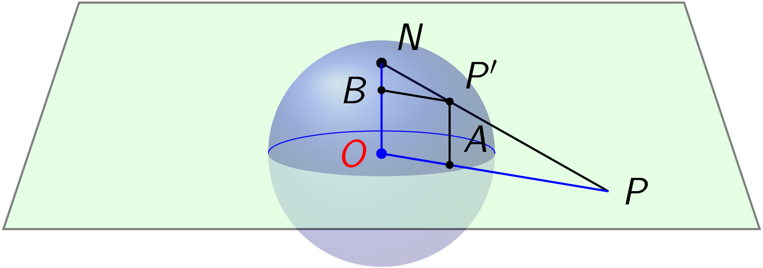


$$\frac{x'}{x} = \frac{y'}{y} = 1 - z'$$

$$\zeta = x + \mathrm{i}y = \frac{x' + \mathrm{i}y'}{1 - z'}$$

$$|\zeta|^2 = \frac{1 + z'}{1 - z'}$$

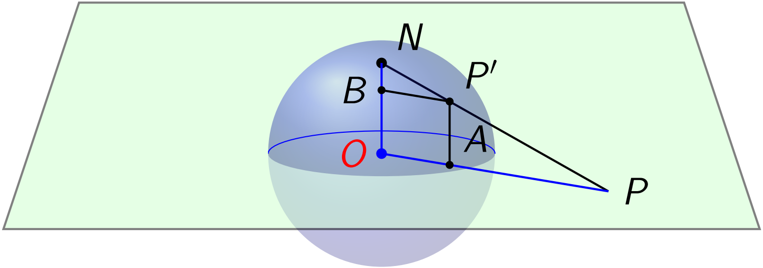
The Riemann sphere



$$\frac{x'}{x} = \frac{y'}{y} = 1 - z' = \frac{2}{|\zeta|^2 + 1}$$

$$|\zeta|^2 = \frac{1 + z'}{1 - z'}$$

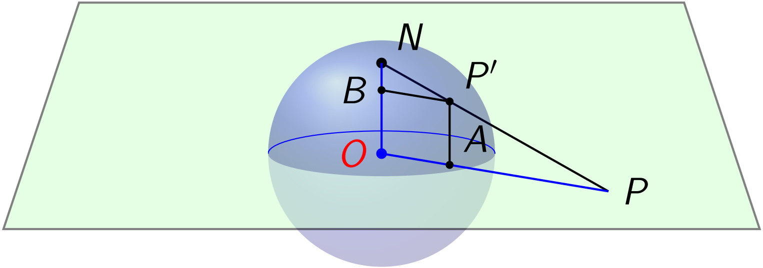
The Riemann sphere



$$\frac{x'}{x} = \frac{y'}{y} = 1 - z' = \frac{2}{|\zeta|^2 + 1}$$

$$x' = \frac{\zeta + \bar{\zeta}}{|\zeta|^2 + 1}, \qquad y' = -\mathrm{i}\,\frac{\zeta - \bar{\zeta}}{|\zeta|^2 + 1}, \qquad z' = \frac{|\zeta|^2 - 1}{|\zeta|^2 + 1}$$

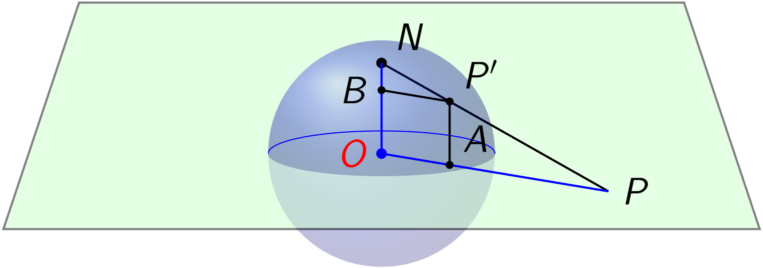
The Riemann sphere



Using spherical polar coordinates :

$$x' = \sin\theta\ \cos\phi, \qquad y' = \sin\theta\ \sin\phi, \qquad z' = \cos\theta$$

The Riemann sphere

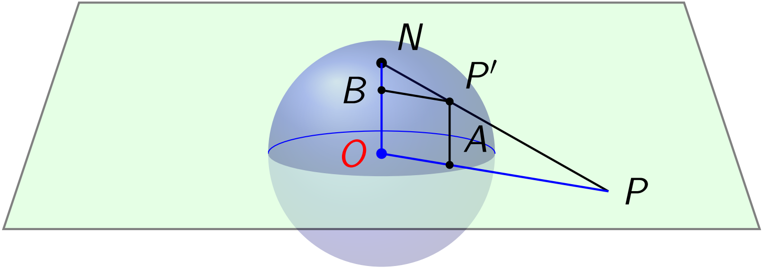


Using spherical polar coordinates :

$$x' = \sin\theta \;\; \cos\phi, \qquad y' = \sin\theta \;\; \sin\phi, \qquad z' = \cos\theta$$

$$\zeta = \frac{x' + \mathrm{i}y'}{1 - z'}$$

The Riemann sphere

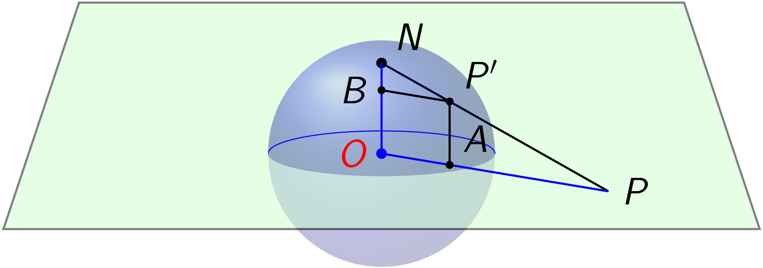


Using spherical polar coordinates :

$$x' = \sin\theta \ \cos\phi, \qquad y' = \sin\theta \ \sin\phi, \qquad z' = \cos\theta$$

$$\zeta = \frac{\sin\theta\,(\cos\phi + \imath \sin\phi)}{1 - \cos\theta}$$

The Riemann sphere



Using spherical polar coordinates :

$$x' = \sin\theta\ \cos\phi, \qquad y' = \sin\theta\ \sin\phi, \qquad z' = \cos\theta$$

$$\zeta = e^{\mathrm{i}\phi}\tan\frac{\theta}{2}$$

Some nice things about sterographic projections

- Stereographic projection maps straight lines in the plane into circles passing through the north pole.

Some nice things about sterographic projections

- Stereographic projection maps straight lines in the plane into circles passing through the north pole.
  - As the point $P \equiv \zeta$ moves in a straight line, the line $\overline{NP}$ traces out a plane.

Some nice things about sterographic projections

- Stereographic projection maps straight lines in the plane into circles passing through the north pole.
  - As the point $P \equiv \zeta$ moves in a straight line, the line $\overline{NP}$ traces out a plane.
  - The point P' traces out a locus, which is the intersection of the plane with the unit sphere.

Some nice things about sterographic projections

- Stereographic projection maps straight lines in the plane into circles passing through the north pole.
  - As the point $P \equiv \zeta$ moves in a straight line, the line $\overline{NP}$ traces out a plane.
  - The point P' traces out a locus, which is the intersection of the plane with the unit sphere.
- The projection maps circles in the plane into circles on the sphere!

Some nice things about sterographic projections

- Stereographic projection maps straight lines in the plane into circles passing through the north pole.
  - As the point $P \equiv \zeta$ moves in a straight line, the line $\overline{NP}$ traces out a plane.
  - The point P' traces out a locus, which is the intersection of the plane with the unit sphere.
- The projection maps circles in the plane into circles on the sphere!
  - Obvious for circles centered at the origin!

Some nice things about sterographic projections

- Stereographic projection maps straight lines in the plane into circles passing through the north pole.
  - As the point $P \equiv \zeta$ moves in a straight line, the line $\overline{NP}$ traces out a plane.
  - The point P' traces out a locus, which is the intersection of the plane with the unit sphere.
- The projection maps circles in the plane into circles on the sphere!
  - Obvious for circles centered at the origin!
- Intersecting straight lines map into circles that intersect at the same angle!

Some nice things about sterographic projections

- Stereographic projection maps straight lines in the plane into circles passing through the north pole.
  - As the point $P \equiv \zeta$ moves in a straight line, the line $\overline{NP}$ traces out a plane.
  - The point P' traces out a locus, which is the intersection of the plane with the unit sphere.
- The projection maps circles in the plane into circles on the sphere!
  - Obvious for circles centered at the origin!
- Intersecting straight lines map into circles that intersect at the same angle!
- This works for other curves too.

Some nice things about sterographic projections

- Stereographic projection maps straight lines in the plane into circles passing through the north pole.
  - As the point $P \equiv \zeta$ moves in a straight line, the line $\overline{NP}$ traces out a plane.
  - The point P' traces out a locus, which is the intersection of the plane with the unit sphere.
- The projection maps circles in the plane into circles on the sphere!
  - Obvious for circles centered at the origin!
- Intersecting straight lines map into circles that intersect at the same angle!
- This works for other curves too.
- Sterographic projections are **conformal**!

Groups : a reminder

- A group is a set G, along with a binary operation $\circ : G \times G \longrightarrow G$, with the following properties :

Groups : a reminder

- A group is a set G, along with a binary operation $\circ\ :\ G \times G \longrightarrow G$, with the following properties :
  - $\circ$ is associative : $(\forall a, b, c \in G),\ a \circ (b \circ c) = (a \circ b) \circ c$

Groups : a reminder

- A group is a set G, along with a binary operation $\circ : G \times G \longrightarrow G$, with the following properties :
  - $\circ$ is associative : $(\forall a, b, c \in G),\ a \circ (b \circ c) = (a \circ b) \circ c$
  - There exists an identity element $e \in G$, which satisfies $(\forall a \in G),\ a \circ e = e \circ a = a$.

Groups : a reminder

- A group is a set G, along with a binary operation $\circ \ : \ G \times G \longrightarrow G$, with the following properties :
  - $\circ$ is associative : $(\forall a, b, c \in G), \ a \circ (b \circ c) = (a \circ b) \circ c)$
  - There exists an identity element $e \in G$, which satisfies $(\forall a \in G), \ a \circ e = e \circ a = a$.
  - Every element of G has an inverse : $(\forall a \in G), \exists b \in G \ : \ a \circ b = b \circ a = e$. The inverse is usually denoted a^{-1}.

Groups : a reminder

- A group is a set G, along with a binary operation $\circ \ : \ G \times G \longrightarrow G$, with the following properties :
  - $\circ$ is associative : $(\forall a, b, c \in G), \ a \circ (b \circ c) = (a \circ b) \circ c)$
  - There exists an identity element $e \in G$, which satisfies $(\forall a \in G), \ a \circ e = e \circ a = a$.
  - Every element of G has an inverse : $(\forall a \in G), \exists b \in G \ : \ a \circ b = b \circ a = e$. The inverse is usually denoted a^{-1}.
- A group is called **Abelian** if $\circ$ is **commutative** : $(\forall a, b \in G) \ : \ a \circ b = b \circ a$.

Groups : a reminder

- A group is a set G, along with a binary operation $\circ \ : \ G \times G \longrightarrow G$, with the following properties :
  - $\circ$ is associative : $(\forall a, b, c \in G), \ a \circ (b \circ c) = (a \circ b) \circ c)$
  - There exists an identity element $e \in G$, which satisfies $(\forall a \in G), \ a \circ e = e \circ a = a$.
  - Every element of G has an inverse : $(\forall a \in G), \exists b \in G \ : \ a \circ b = b \circ a = e$. The inverse is usually denoted a^{-1}.
- A group is called **Abelian** if $\circ$ is **commutative** : $(\forall a, b \in G) \ : \ a \circ b = b \circ a$.
- In an Abelian group, usually

Groups : a reminder

- A group is a set G, along with a binary operation $\circ : G \times G \longrightarrow G$, with the following properties :
  - $\circ$ is associative : $(\forall a, b, c \in G),\ a \circ (b \circ c) = (a \circ b) \circ c)$
  - There exists an identity element $e \in G$, which satisfies $(\forall a \in G),\ a \circ e = e \circ a = a$.
  - Every element of G has an inverse : $(\forall a \in G), \exists b \in G\ :\ a \circ b = b \circ a = e$. The inverse is usually denoted a^{-1}.
- A group is called **Abelian** if $\circ$ is **commutative** : $(\forall a, b \in G)\ :\ a \circ b = b \circ a$.
- In an Abelian group, usually
  - the group operation is denoted by $+$.

Groups : a reminder

- A group is a set G, along with a binary operation $\circ \ : \ G \times G \longrightarrow G$, with the following properties :
  - $\circ$ is associative : $(\forall a, b, c \in G), \ a \circ (b \circ c) = (a \circ b) \circ c)$
  - There exists an identity element $e \in G$, which satisfies $(\forall a \in G), \ a \circ e = e \circ a = a$.
  - Every element of G has an inverse : $(\forall a \in G), \exists b \in G \ : \ a \circ b = b \circ a = e$. The inverse is usually denoted a^{-1}.
- A group is called **Abelian** if $\circ$ is **commutative** : $(\forall a, b \in G) \ : \ a \circ b = b \circ a$.
- In an Abelian group, usually
  - the group operation is denoted by $+$.
  - the identity is denoted by 0.

Groups : a reminder

- A group is a set G, along with a binary operation $\circ : G \times G \longrightarrow G$, with the following properties :
  - $\circ$ is associative : $(\forall a, b, c \in G),\ a \circ (b \circ c) = (a \circ b) \circ c)$
  - There exists an identity element $e \in G$, which satisfies $(\forall a \in G),\ a \circ e = e \circ a = a.$
  - Every element of G has an inverse : $(\forall a \in G), \exists b \in G\ :\ a \circ b = b \circ a = e.$ The inverse is usually denoted a^{-1}.
- A group is called **Abelian** if $\circ$ is **commutative** : $(\forall a, b \in G)\ :\ a \circ b = b \circ a.$
- In an Abelian group, usually
  - the group operation is denoted by $+$.
  - the identity is denoted by 0.
  - the inverse of a is usually denoted by $-a$.

Rings : a reminder

- A ring R is a set with two binary operations, $+$ and $\times$, with the following properties :

Rings : a reminder

- A ring R is a set with two binary operations, $+$ and $\times$, with the following properties :
  - $(R, +)$ is an Abelian group (▸ ?).

Rings : a reminder

- A ring R is a set with two binary operations, $+$ and $\times$, with the following properties :
  - $(R, +)$ is an Abelian group (▸ ?).
  - $\times$ is associative.

Rings : a reminder

- A ring R is a set with two binary operations, $+$ and $\times$, with the following properties :
  - $(R, +)$ is an Abelian group (▸ ?).
  - $\times$ is associative.
  - $\times$ distributes over $+$:

$$(\forall a, b, c \in R) \ : \ a \times (b + c) = a \times b + a \times c, \quad (a + b) \times c = a \times c + b \times c$$

Rings : a reminder

- A ring R is a set with two binary operations, $+$ and $\times$, with the following properties :
  - $(R, +)$ is an Abelian group (?).
  - $\times$ is associative.
  - $\times$ distributes over $+$:

$$(\forall a, b, c \in R) \ : \ a \times (b + c) = a \times b + a \times c, \quad (a + b) \times c = a \times c + b \times c$$

- A ring R is called a "ring with identity" if

$$\exists 1 \in R \ : \ 1 \times a = a \times 1 = a, \ (\forall a \in R).$$

Rings : a reminder

- A ring R is a set with two binary operations, $+$ and $\times$, with the following properties :
  - $(R, +)$ is an Abelian group (▸ ?).
  - $\times$ is associative.
  - $\times$ distributes over $+$:

$$(\forall a, b, c \in R) \;:\; a \times (b + c) = a \times b + a \times c, \quad (a + b) \times c = a \times c + b \times c$$

- A ring R is called a "ring with identity" if

$$\exists 1 \in R \;:\; 1 \times a = a \times 1 = a, \; (\forall a \in R).$$

- A ring is called commutative if $a \times b = b \times a, (\forall a, b \in R)$.

Rings : a reminder

- A ring R is a set with two binary operations, $+$ and $\times$, with the following properties :
  - $(R, +)$ is an Abelian group (?).
  - $\times$ is associative.
  - $\times$ distributes over $+$:

$$(\forall a, b, c \in R) \;:\; a\times(b+c) = a\times b + a\times c, \quad (a+b)\times c = a\times c + b\times c$$

- A ring R is called a "ring with identity" if

$$\exists 1 \in R \;:\; 1 \times a = a \times 1 = a, \; (\forall a \in R).$$

- A ring is called commutative if $a \times b = b \times a, (\forall a, b \in R)$.
- *You can add, subtract and multiply in a ring, but not (necessarily) divide!*

Fields : a reminder

- A field F is a set with two binary operations, $+$ and $\times$, with the following properties :

Go Back!

Fields : a reminder

- A field F is a set with two binary operations, $+$ and $\times$, with the following properties :
  - $(F, +)$ is an Abelian group (?).

Go Back!

Fields : a reminder

- A field F is a set with two binary operations, $+$ and $\times$, with the following properties :
  - $(F, +)$ is an Abelian group (▸ ?).
  - $(F, \times)$ is a commutative ring with identity (▸ ?).

◂ Go Back!

Fields : a reminder

- A field F is a set with two binary operations, $+$ and $\times$, with the following properties :
  - $(F, +)$ is an Abelian group (?).
  - $(F, \times)$ is a commutative ring with identity (?).
  - $F^{\times} = F - 0$ is an Abelian group under $\times$.

Go Back!

Fields : a reminder

- A field F is a set with two binary operations, $+$ and $\times$, with the following properties :
  - $(F, +)$ is an Abelian group (▸ ?).
  - $(F, \times)$ is a commutative ring with identity (▸ ?).
  - $F^{\times} = F - 0$ is an Abelian group under $\times$.
  - *i.e.* $(\forall a \in F^{\times}), \exists a^{-1} \in F \ : \ a \times a^{-1} = 1$

◂ Go Back!

Fields : a reminder

- A field F is a set with two binary operations, $+$ and $\times$, with the following properties :
  - $(F, +)$ is an Abelian group (?).
  - $(F, \times)$ is a commutative ring with identity (?).
  - $F^{\times} = F - 0$ is an Abelian group under $\times$.
  - *i.e.* $(\forall a \in F^{\times}), \exists a^{-1} \in F \ : \ a \times a^{-1} = 1$
- *In a field, you can add, subtract, multiply and divide!*

Go Back!

Polynomials - a quick review

- Consider a commutative ring with identity, R.

Polynomials - a quick review

- Consider a commutative ring with identity, R.
- An infinite sequence of elements of R is a mapping $\mathbb{N} \to R$.

Polynomials - a quick review

- Consider a commutative ring with identity, R.
- An infinite sequence of elements of R is a mapping $\mathbb{N} \to R$.
- The mapping is determined by

$$f_0 = f(0),\ f_1 = f(1),\ \ldots,\ f_i = f(i),\ \ldots$$

and can be denoted by $(f_0, f_1, \ldots, f_i, \ldots)$.

Polynomials - a quick review

- Consider a commutative ring with identity, R.
- An infinite sequence of elements of R is a mapping $\mathbb{N} \to R$.
- The mapping is determined by

$$f_0 = f(0),\ f_1 = f(1),\ \ldots,\ f_i = f(i),\ \ldots$$

  and can be denoted by $(f_0, f_1, \ldots, f_i, \ldots)$.
- A finite sequence is an infinite sequence in which only a finite number of f_i are non-zero.

Polynomials - a quick review

- Consider a commutative ring with identity, R.
- An infinite sequence of elements of R is a mapping $\mathbb{N} \to R$.
- The mapping is determined by

$$f_0 = f(0),\ f_1 = f(1),\ \dots,\ f_i = f(i),\ \dots$$

  and can be denoted by $(f_0, f_1, \dots, f_i, \dots)$.
- A finite sequence is an infinite sequence in which only a finite number of f_i are non-zero.
- Denote by $S(R)$ the set of all finite sequences of elements of R.

Polynomials - a quick review

- Define binary operations
  $+ \ : \ S(R) \times S(R) \to S(R)$ and
  $* \ : \ S(R) \times S(R) \to S(R)$ by :

Go Back!

Polynomials - a quick review

- Define binary operations
  $+ \ : \ S(R) \times S(R) \to S(R)$ and
  $* \ : \ S(R) \times S(R) \to S(R)$ by :
- $(f_0, f_1, \ldots) + (g_0, g_1, \ldots) = (f_0 + g_0, f_1 + g_1, \ldots)$.

Go Back!

Polynomials - a quick review

- Define binary operations
  $+ \ : \ S(R) \times S(R) \to S(R)$ and
  $* \ : \ S(R) \times S(R) \to S(R)$ by :
- $(f_0, f_1, \ldots) + (g_0, g_1, \ldots) = (f_0 + g_0, f_1 + g_1, \ldots)$.
- $(f_0, f_1, \ldots) * (g_0, g_1, \ldots) = (h_0, h_1, \ldots)$ where
  $h_i = \sum_{j+k=i} f_j g_k$.

Go Back!

Polynomials - a quick review

- Define binary operations
  $+ \; : \; S(R) \times S(R) \to S(R)$ and
  $* \; : \; S(R) \times S(R) \to S(R)$ by :
- $(f_0, f_1, \ldots) + (g_0, g_1, \ldots) = (f_0 + g_0, f_1 + g_1, \ldots)$.
- $(f_0, f_1, \ldots) * (g_0, g_1, \ldots) = (h_0, h_1, \ldots)$ where
  $h_i = \sum_{j+k=i} f_j g_k$.
- $(S(R), +, *)$ is a ring.

Go Back!

Polynomials - a quick review

- Consider $X = (0, 1, 0, 0, \dots) \in S(R)$. Then

Go Back!

Polynomials - a quick review

- Consider $X = (0, 1, 0, 0, \ldots) \in S(R)$. Then
  - $X^2 = (0, 0, 1, 0, \ldots)$.

Polynomials - a quick review

- Consider $X = (0, 1, 0, 0, \ldots) \in S(R)$. Then
  - $X^2 = (0, 0, 1, 0, \ldots)$.
  - $X^3 = (0, 0, 0, 1, \ldots)$.

Go Back!

Polynomials - a quick review

- Consider $X = (0, 1, 0, 0, \ldots) \in S(R)$. Then
  - $X^2 = (0, 0, 1, 0, \ldots)$.
  - $X^3 = (0, 0, 0, 1, \ldots)$.
- We can write

$$(a_0, a_1, a_2, \ldots) = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n$$

where $a_n \neq 0$ and $a_k = 0$ for all $k > n$.

Polynomials - a quick review

- Consider $X = (0, 1, 0, 0, \ldots) \in S(R)$. Then
  - $X^2 = (0, 0, 1, 0, \ldots)$.
  - $X^3 = (0, 0, 0, 1, \ldots)$.
- We can write

$$(a_0, a_1, a_2, \ldots) = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n$$

where $a_n \neq 0$ and $a_k = 0$ for all $k > n$.

- X is called an *indeterminate*.

Polynomials - a quick review

- Consider $X = (0, 1, 0, 0, \ldots) \in S(R)$. Then
  - $X^2 = (0, 0, 1, 0, \ldots)$.
  - $X^3 = (0, 0, 0, 1, \ldots)$.
- We can write

$$(a_0, a_1, a_2, \ldots) = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n$$

  where $a_n \neq 0$ and $a_k = 0$ for all $k > n$.
- X is called an *indeterminate*.
- Each element of $S(R)$ is a polynomial in the indeterminate X with coefficients in the ring R.

Polynomials - a quick review

- Consider $X = (0, 1, 0, 0, \ldots) \in S(R)$. Then
  - $X^2 = (0, 0, 1, 0, \ldots)$.
  - $X^3 = (0, 0, 0, 1, \ldots)$.
- We can write

$$(a_0, a_1, a_2, \ldots) = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n$$

  where $a_n \neq 0$ and $a_k = 0$ for all $k > n$.
- X is called an *indeterminate*.
- Each element of $S(R)$ is a polynomial in the indeterminate X with coefficients in the ring R.
- $S(R)$ is usually denoted by $R[X]$.

Multiplication distributes over addition!

$$(a, b) \quad * \quad \{(c, d) + (e, f)\}$$

Multiplication distributes over addition!

$$(a, b) \quad * \quad \{(c, d) + (e, f)\} = (a, b) * (c + e, d + f)$$

Multiplication distributes over addition!

$$\begin{aligned}(a, b) &* \{(c, d) + (e, f)\} = (a, b) * (c + e, d + f) \\ &= (a[c + e] - b[d + f], a[d + f] + b[c + e])\end{aligned}$$

Multiplication distributes over addition!

$$\begin{aligned}
(a,b) \;*\; \{(c,d)+(e,f)\} &= (a,b)*(c+e,d+f) \\
&= (a[c+e]-b[d+f], a[d+f]+b[c+e]) \\
&= ([ac-bd]+[ae-bf], \\
&\quad [ad+bc]+[af+be])
\end{aligned}$$

Multiplication distributes over addition!

$$
\begin{aligned}
(a, b) &* \{(c, d) + (e, f)\} = (a, b) * (c + e, d + f) \\
&= (a[c + e] - b[d + f], a[d + f] + b[c + e]) \\
&= ([ac - bd] + [ae - bf], \\
&\quad [ad + bc] + [af + be]) \\
&= (a, b) * (c, d) + (a, b) * (e, f)
\end{aligned}
$$

Go Back!

The identity on C

$$(1, 0) * (a, b)$$

The identity on C

$$(1,0) * (a,b) = (1 \cdot a - 0 \cdot b, 1 \cdot b + 0 \cdot a)$$

The identity on C

$$(1,0) * (a,b) = (1 \cdot a - 0 \cdot b, 1 \cdot b + 0 \cdot a) = (a,b)$$

Go Back!

$+$ is well defined on $\mathbb{R}[X]/K$:

- If $P' \sim P$ and $Q' \sim Q$,

  $\exists S_1, S_2 \in \mathbb{R}[X] : P' - P = S_1 K, \quad Q' - Q = S_2 K$

$+$ is well defined on $\mathbb{R}[X]/K$:

- If $P' \sim P$ and $Q' \sim Q$,

  $$\exists S_1, S_2 \in \mathbb{R}[X] : P' - P = S_1 K, \quad Q' - Q = S_2 K$$

- Thus

  $$(P' + Q') - (P + Q) = (S_1 + S_2)K,$$

  $$\implies P' + Q' \sim P + Q$$

$+$ is well defined on $\mathbb{R}[X]/K$:

- If $P' \sim P$ and $Q' \sim Q$,

  $\exists S_1, S_2 \in \mathbb{R}[X] : P' - P = S_1 K, \quad Q' - Q = S_2 K$

- Thus

$$(P' + Q') - (P + Q) = (S_1 + S_2)K,$$

$$\implies P' + Q' \sim P + Q$$

- $\implies [P' + Q'] = [P + Q]$

Go Back!

$+$ is well defined on $\mathbb{R}[X]/K$:

- If $P' \sim P$ and $Q' \sim Q$,

  $\exists S_1, S_2 \in \mathbb{R}[X] : P' - P = S_1 K, \quad Q' - Q = S_2 K$
- Thus

$$(P' + Q') - (P + Q) = (S_1 + S_2)K,$$

$$\implies P' + Q' \sim P + Q$$

- $\implies [P' + Q'] = [P + Q]$
- Thus $+$ is well defined on $\mathbb{R}[X]/K$.

Go Back!