Philosophical discussion about numbers

Q In what sense is \(-1\) a number? **DISCUSS**

Q Is \(\sqrt{-1}\) a number?

A from your Kindergarten teacher Not a REAL number.

Why not then a non-real number? After all, \(\sqrt{-1}\) exists as an expression, and as such it pops up all the time when you solve enough equations **EVEN IF** you are only interested in REAL numbers (see later).

OK. Let's extend our number system by pretending \(\sqrt{-1}\) is a number which we'll denote as usual by \(i\), and see what happens.
Q In what sense is $-1$ a number? DISCUSS
Q In what sense is $-1$ a number? DISCUSS

Q Is $\sqrt{-1}$ a number?
Q In what sense is \(-1\) a number? DISCUSS

Q Is \(\sqrt{-1}\) a number?

A from your Kindergarten teacher
Q In what sense is $-1$ a number? DISCUSS

Q Is $\sqrt{-1}$ a number?

A from your Kindergarten teacher Not a REAL number.
Philosophical discussion about numbers

Q In what sense is $-1$ a number? DISCUSS

Q Is $\sqrt{-1}$ a number?

A from your Kindergarten teacher Not a REAL number.

Why not then a non-real number?
Q In what sense is $-1$ a number? DISCUSS

Q Is $\sqrt{-1}$ a number?

A from your Kindergarten teacher Not a REAL number.

Why not then a non-real number? After all, $\sqrt{-1}$ exists as an expression, and as such it pops up all the time when you solve enough equations.
Q In what sense is $-1$ a number? DISCUSS

Q Is $\sqrt{-1}$ a number?

A from your Kindergarten teacher Not a REAL number.

Why not then a non-real number? After all, $\sqrt{-1}$ exists as an expression, and as such it pops up all the time when you solve enough equations EVEN IF you are only interested in REAL numbers (see later).
Philosophical discussion about numbers

Q In what sense is $-1$ a number? DISCUSS

Q Is $\sqrt{-1}$ a number?

A from your Kindergarten teacher Not a REAL number.

Why not then a non-real number? After all, $\sqrt{-1}$ exists as an expression, and as such it pops up all the time when you solve enough equations EVEN IF you are only interested in REAL numbers (see later).

OK. Let’s extend our number system by pretending $\sqrt{-1}$ is a number which we’ll denote as usual by $i$, and see what happens.
Thought experiment concerning $i$

Well if $i$ is a number, then surely so is $3i$ and $2 + 3i$.

In fact, for any $a, b, c, d \in \mathbb{R}$, $a + bi, c + di$ are numbers too, surely.

But then $(a + bi) + (c + di)$ is a number!

That’s OK, it must be one we’ve seen before $(a + c) + (b + d)i$.

But also $(a + bi)(c + di)$ is a number(??).

I guess it ought to be $(a + bi)(c + di) = ac - bd + (bc + ad)i$ since $i^2 = -1$.

We’ve seen this number before.

Q When does $a + bi = c + di$?

A Then $(a - c)^2 = (d - b)^2$ $i^2 = -1$ which occurs precisely when $a = c$ and $b = d$. (WHY?)

Major Question

If we keep playing this game blindly, using our usual rules of arithmetic, will we ever end up proving absurd statements like $1 = 0$?
Well if $i$ is a number, then surely so is $3i$. In fact, for any $a, b, c, d \in \mathbb{R}$, $a + bi, c + di$ are numbers too, surely. But then $(a + bi) + (c + di)$ is a number! That's OK, it must be one we've seen before $(a + c) + (b + d)i$. But also $(a + bi)(c + di)$ is a number. I guess it ought to be $(a + bi)(c + di) = ac + bci + ad + bdi^2 = (ac - bd) + (bc + ad)i$ since $i^2 = -1$. We've seen this number before. 

**When does** $a + bi = c + di$? **Then** $(a - c)^2 = (d - b)^2 i^2 = -(d - b)^2$ which occurs precisely when $a = c$ and $b = d$. (WHY?)

**Major Question** If we keep playing this game blindly, using our usual rules of arithmetic, will we ever end up proving absurd statements like $1 = 0$?
Thought experiment concerning \( i \)

- Well if \( i \) is a number, then surely so is \( 3i \) and \( 2 + 3i \).
Thought experiment concerning $i$

- Well if $i$ is a number, then surely so is $3i$ and $2 + 3i$.
- In fact, for any $a, b, c, d \in \mathbb{R}$, $a + bi, c + di$ are numbers too, surely.
Thought experiment concerning $i$

- Well if $i$ is a number, then surely so is $3i$ and $2 + 3i$.
- In fact, for any $a, b, c, d \in \mathbb{R}$, $a + bi, c + di$ are numbers too, surely.
- But then $(a + bi) + (c + di)$ is a number!

We've seen this number before. $a + bi = c + di$ when $(a - c)^2 = (d - b)^2 \implies a = c$ and $b = d$. (WHY?)

Major Question
If we keep playing this game blindly, using our usual rules of arithmetic, will we ever end up proving absurd statements like $1 = 0$?
Thought experiment concerning $i$

- Well if $i$ is a number, then surely so is $3i$ and $2 + 3i$.
- In fact, for any $a, b, c, d \in \mathbb{R}$, $a + bi, c + di$ are numbers too, surely.
- But then $(a + bi) + (c + di)$ is a number! That’s OK, it must be one we’ve seen before $(a + c) + (b + d)i$.
Thought experiment concerning $i$

- Well if $i$ is a number, then surely so is $3i$ and $2 + 3i$.
- In fact, for any $a, b, c, d \in \mathbb{R}$, $a + bi, c + di$ are numbers too, surely.
- But then $(a + bi) + (c + di)$ is a number! That’s OK, it must be one we’ve seen before $(a + c) + (b + d)i$.
- But also $(a + bi)(c + di)$ is a number(??).

Daniel Chan (UNSW)

Chapter 3: Complex Numbers

Semester 1 2019
Thought experiment concerning $i$

- Well if $i$ is a number, then surely so is $3i$ and $2 + 3i$.
- In fact, for any $a, b, c, d \in \mathbb{R}$, $a + bi, c + di$ are numbers too, surely.
- But then $(a + bi) + (c + di)$ is a number! That’s OK, it must be one we’ve seen before $(a + c) + (b + d)i$.
- But also $(a + bi)(c + di)$ is a number(??).

I guess it ought to be

$$(a + bi)(c + di) = ac + bci + adi + bdi^2 = (ac - bd) + (bc + ad)i$$
Thought experiment concerning $i$

- Well if $i$ is a number, then surely so is $3i$ and $2 + 3i$.
- In fact, for any $a, b, c, d \in \mathbb{R}$, $a + bi, c + di$ are numbers too, surely.
- But then $(a + bi) + (c + di)$ is a number! That’s OK, it must be one we’ve seen before $(a + c) + (b + d)i$.
- But also $(a + bi)(c + di)$ is a number(??).

I guess it ought to be

$$(a + bi)(c + di) = ac + bci + adi + bdi^2 = (ac - bd) + (bc + ad)i$$

since $i^2 = -1$. 

Thought experiment concerning $i$

- Well if $i$ is a number, then surely so is $3i$ and $2 + 3i$.
- In fact, for any $a, b, c, d \in \mathbb{R}$, $a + bi$, $c + di$ are numbers too, surely.
- But then $(a + bi) + (c + di)$ is a number! That’s OK, it must be one we’ve seen before $(a + c) + (b + d)i$.
- But also $(a + bi)(c + di)$ is a number(??).

I guess it ought to be

$$(a + bi)(c + di) = ac + bci + adi + bdi^2 = (ac - bd) + (bc + ad)i$$

since $i^2 = -1$. We’ve seen this number before.
Thought experiment concerning $i$

- Well if $i$ is a number, then surely so is $3i$ and $2 + 3i$.
- In fact, for any $a, b, c, d \in \mathbb{R}$, $a + bi, c + di$ are numbers too, surely.
- But then $(a + bi) + (c + di)$ is a number! That’s OK, it must be one we’ve seen before $(a + c) + (b + d)i$.
- But also $(a + bi)(c + di)$ is a number(??).

I guess it ought to be

$$(a + bi)(c + di) = ac + bci + adi + bdi^2 = (ac - bd) + (bc + ad)i$$

since $i^2 = -1$. We’ve seen this number before.

Q When does $a + bi = c + di$?
Thought experiment concerning \( i \)

- Well if \( i \) is a number, then surely so is \( 3i \) and \( 2 + 3i \).
- In fact, for any \( a, b, c, d \in \mathbb{R} \), \( a + bi, c + di \) are numbers too, surely.
- But then \((a + bi) + (c + di)\) is a number! That’s OK, it must be one we’ve seen before \((a + c) + (b + d)i\).
- But also \((a + bi)(c + di)\) is a number(??).

I guess it ought to be

\[
(a + bi)(c + di) = ac + bci + adi + bdi^2 = (ac - bd) + (bc + ad)i
\]

since \( i^2 = -1 \). We’ve seen this number before.

**Q** When does \( a + bi = c + di \)?

**A** Then \((a - c)^2 = (d - b)^2 i^2 = -(d - b)^2 \) which occurs precisely when \( a = c \) and \( b = d \). (WHY?)
Thought experiment concerning $i$

- Well if $i$ is a number, then surely so is $3i$ and $2 + 3i$.
- In fact, for any $a, b, c, d \in \mathbb{R}$, $a + bi, c + di$ are numbers too, surely.
- But then $(a + bi) + (c + di)$ is a number! That’s OK, it must be one we’ve seen before $(a + c) + (b + d)i$.
- But also $(a + bi)(c + di)$ is a number(??).

I guess it ought to be

$$(a + bi)(c + di) = ac + bci + adi + bdi^2 = (ac - bd) + (bc + ad)i$$

since $i^2 = -1$. We’ve seen this number before.

**Q** When does $a + bi = c + di$?

**A** Then $(a - c)^2 = (d - b)^2 i^2 = -(d - b)^2$ which occurs precisely when $a = c$ and $b = d$. (WHY?)

**Major Question**

If we keep playing this game blindly, using our usual rules of arithmetic, will we ever end up proving absurd statements like $1 = 0$?
Our new number system should satisfy the “usual rules of arithmetic”, and we need to formalise what this means. This uses the following
Our new number system should satisfy the “usual rules of arithmetic”, and we need to formalise what this means. This uses the following

**Definition**

A *field* is the data consisting of a non-empty set $\mathbb{F}$ together with
Fields

Our new number system should satisfy the “usual rules of arithmetic”, and we need to formalise what this means. This uses the following

Definition

A field is the data consisting of a non-empty set $\mathbb{F}$ together with

- an addition rule $+$, which assigns to any $x, y \in \mathbb{F}$ an element $x + y \in \mathbb{F}$.
Our new number system should satisfy the “usual rules of arithmetic”, and we need to formalise what this means. This uses the following

**Definition**

A *field* is the data consisting of a non-empty set $\mathbb{F}$ together with

- an *addition rule* $+$, which assigns to any $x, y \in \mathbb{F}$ an element $x + y \in \mathbb{F}$.
- a *multiplication rule*, which assigns to any $x, y \in \mathbb{F}$ an element $xy \in \mathbb{F}$. 
Our new number system should satisfy the “usual rules of arithmetic”, and we need to formalise what this means. This uses the following

**Definition**

A *field* is the data consisting of a non-empty set \( \mathbb{F} \) together with

- an *addition rule* \(+\), which assigns to any \( x, y \in \mathbb{F} \) an element \( x + y \in \mathbb{F} \).
- a *multiplication rule*, which assigns to any \( x, y \in \mathbb{F} \) an element \( xy \in \mathbb{F} \).

such that the axioms on the following page hold.
Field axioms

1. **Associative Law of Addition**: \((x + y) + z = x + (y + z)\) for all \(x, y, z \in F\).

2. **Commutative Law of Addition**: \(x + y = y + x\) for all \(x, y \in F\).

3. **Existence of a Zero**: There exists an element of \(F\) (usually written as 0 & called zero) such that 0 + \(x\) = \(x\) + 0 = \(x\) for all \(x \in F\).

4. **Existence of a Negative**: For each \(x \in F\), there exists an element \(w \in F\) (usually written as \(-x\) & called the negative of \(x\)) such that \(x + w = w + x = 0\).

5. **Associative Law of Multiplication**: \(x(yz) = (xy)z\) for all \(x, y, z \in F\).

6. **Commutative Law of Multiplication**: \(xy = yx\) for all \(x, y \in F\).

7. **Existence of a One**: There exists a non-zero element of \(F\) (usually written as 1 & called the multiplicative identity) such that \(x 1 = 1 x = x\) for all \(x \in F\).

8. **Existence of an Inverse for Multiplication**: For each non-zero \(x \in F\), there exists an element \(w \in F\) (usually written as \(1/x\) or \(x^{-1}\) & called the multiplicative inverse of \(x\)) such that \(xw = wx = 1\).

9. **Distributive Law**: \(x(y + z) = xy + xz\) for all \(x, y, z \in F\).

10. **Distributive Law**: \((x + y)z = xz + yz\), for all \(x, y, z \in F\).
Field axioms

1. **Associative Law of Addition.** \((x + y) + z = x + (y + z)\) for all \(x, y, z \in \mathbb{F}\).
1. **Associative Law of Addition.** \((x + y) + z = x + (y + z)\) for all \(x, y, z \in F\).

2. **Commutative Law of Addition.** \(x + y = y + x\) for all \(x, y \in F\).
Field axioms

1. **Associative Law of Addition.** \((x + y) + z = x + (y + z)\) for all \(x, y, z \in \mathbb{F}\).

2. **Commutative Law of Addition.** \(x + y = y + x\) for all \(x, y \in \mathbb{F}\).

3. **Existence of a Zero.** There exists an element of \(\mathbb{F}\) (usually written as 0 & called *zero*) such that \(0 + x = x + 0 = x\) for all \(x \in \mathbb{F}\).
Field axioms

1. **Associative Law of Addition.** \((x + y) + z = x + (y + z)\) for all \(x, y, z \in \mathbb{F}\).

2. **Commutative Law of Addition.** \(x + y = y + x\) for all \(x, y \in \mathbb{F}\).

3. **Existence of a Zero.** There exists an element of \(\mathbb{F}\) (usually written as 0 & called zero) such that \(0 + x = x + 0 = x\) for all \(x \in \mathbb{F}\).

4. **Existence of a Negative.** For each \(x \in \mathbb{F}\), there exists an element \(w \in \mathbb{F}\) (usually written as \(-x\) & called the negative of \(x\)) such that \(x + w = w + x = 0\).
Field axioms

1. **Associative Law of Addition.** \((x + y) + z = x + (y + z)\) for all \(x, y, z \in \mathbb{F}\).

2. **Commutative Law of Addition.** \(x + y = y + x\) for all \(x, y \in \mathbb{F}\).

3. **Existence of a Zero.** There exists an element of \(\mathbb{F}\) (usually written as 0 & called zero) such that \(0 + x = x + 0 = x\) for all \(x \in \mathbb{F}\).

4. **Existence of a Negative.** For each \(x \in \mathbb{F}\), there exists an element \(w \in \mathbb{F}\) (usually written as \(-x\) & called the negative of \(x\)) such that \(x + w = w + x = 0\).

5. **Associative Law of Multiplication.** \(x(yz) = (xy)z\) for all \(x, y, z \in \mathbb{F}\).
Field axioms

1. **Associative Law of Addition.** \((x + y) + z = x + (y + z)\) for all \(x, y, z \in \mathbb{F}\).

2. **Commutative Law of Addition.** \(x + y = y + x\) for all \(x, y \in \mathbb{F}\).

3. **Existence of a Zero.** There exists an element of \(\mathbb{F}\) (usually written as 0 & called zero) such that \(0 + x = x + 0 = x\) for all \(x \in \mathbb{F}\).

4. **Existence of a Negative.** For each \(x \in \mathbb{F}\), there exists an element \(w \in \mathbb{F}\) (usually written as \(-x\) & called the negative of \(x\)) such that \(x + w = w + x = 0\).

5. **Associative Law of Multiplication.** \(x(yz) = (xy)z\) for all \(x, y, z \in \mathbb{F}\).

6. **Commutative Law of Multiplication.** \(xy = yx\) for all \(x, y \in \mathbb{F}\).
Field axioms

1. **Associative Law of Addition.** \((x + y) + z = x + (y + z)\) for all \(x, y, z \in \mathbb{F}\).

2. **Commutative Law of Addition.** \(x + y = y + x\) for all \(x, y \in \mathbb{F}\).

3. **Existence of a Zero.** There exists an element of \(\mathbb{F}\) (usually written as 0 & called zero) such that \(0 + x = x + 0 = x\) for all \(x \in \mathbb{F}\).

4. **Existence of a Negative.** For each \(x \in \mathbb{F}\), there exists an element \(w \in \mathbb{F}\) (usually written as \(-x\) & called the negative of \(x\)) such that \(x + w = w + x = 0\).

5. **Associative Law of Multiplication.** \(x(yz) = (xy)z\) for all \(x, y, z \in \mathbb{F}\).

6. **Commutative Law of Multiplication.** \(xy = yx\) for all \(x, y \in \mathbb{F}\).

7. **Existence of a One.** There exists a non-zero element of \(\mathbb{F}\) (usually written as 1 & called the multiplicative identity) such that \(x1 = 1x = x\) for all \(x \in \mathbb{F}\).

8. **Distributive Law.** \(x(y + z) = xy + xz\), for all \(x, y, z \in \mathbb{F}\).
**Field axioms**

1. **Associative Law of Addition.** \((x + y) + z = x + (y + z)\) for all \(x, y, z \in \mathbb{F}\).

2. **Commutative Law of Addition.** \(x + y = y + x\) for all \(x, y \in \mathbb{F}\).

3. **Existence of a Zero.** There exists an element of \(\mathbb{F}\) (usually written as 0 & called zero) such that \(0 + x = x + 0 = x\) for all \(x \in \mathbb{F}\).

4. **Existence of a Negative.** For each \(x \in \mathbb{F}\), there exists an element \(w \in \mathbb{F}\) (usually written as \(-x\) & called the negative of \(x\)) such that \(x + w = w + x = 0\).

5. **Associative Law of Multiplication.** \(x(yz) = (xy)z\) for all \(x, y, z \in \mathbb{F}\).

6. **Commutative Law of Multiplication.** \(xy = yx\) for all \(x, y \in \mathbb{F}\).

7. **Existence of a One.** There exists a non-zero element of \(\mathbb{F}\) (usually written as 1 & called the multiplicative identity) such that \(x1 = 1x = x\) for all \(x \in \mathbb{F}\).

8. **Existence of an Inverse for Multiplication.** For each non-zero \(x \in \mathbb{F}\), there exists an element \(w\) of \(\mathbb{F}\) (usually written as \(1/x\) or \(x^{-1}\) & called the multiplicative inverse of \(x\)) such that \(xw = wx = 1\).
Field axioms

1. **Associative Law of Addition.** $(x + y) + z = x + (y + z)$ for all $x, y, z \in F$.

2. **Commutative Law of Addition.** $x + y = y + x$ for all $x, y \in F$.

3. **Existence of a Zero.** There exists an element of $F$ (usually written as $0$ & called *zero*) such that $0 + x = x + 0 = x$ for all $x \in F$.

4. **Existence of a Negative.** For each $x \in F$, there exists an element $w \in F$ (usually written as $-x$ & called the *negative* of $x$) such that $x + w = w + x = 0$.

5. **Associative Law of Multiplication.** $x(yz) = (xy)z$ for all $x, y, z \in F$.

6. **Commutative Law of Multiplication.** $xy = yx$ for all $x, y \in F$.

7. **Existence of a One.** There exists a non-zero element of $F$ (usually written as $1$ & called the *multiplicative identity*) such that $x1 = 1x = x$ for all $x \in F$.

8. **Existence of an Inverse for Multiplication.** For each non-zero $x \in F$, there exists an element $w$ of $F$ (usually written as $1/x$ or $x^{-1}$ & called the *multiplicative inverse* of $x$) such that $xw = wx = 1$.

9. **Distributive Law.** $x(y + z) = xy + xz$ for all $x, y, z \in F$. 
### Field axioms

1. **Associative Law of Addition.** \((x + y) + z = x + (y + z)\) for all \(x, y, z \in \mathbb{F}\).

2. **Commutative Law of Addition.** \(x + y = y + x\) for all \(x, y \in \mathbb{F}\).

3. **Existence of a Zero.** There exists an element of \(\mathbb{F}\) (usually written as 0 & called zero) such that \(0 + x = x + 0 = x\) for all \(x \in \mathbb{F}\).

4. **Existence of a Negative.** For each \(x \in \mathbb{F}\), there exists an element \(w \in \mathbb{F}\) (usually written as \(-x\) & called the *negative* of \(x\)) such that \(x + w = w + x = 0\).

5. **Associative Law of Multiplication.** \(x(yz) = (xy)z\) for all \(x, y, z \in \mathbb{F}\).

6. **Commutative Law of Multiplication.** \(xy = yx\) for all \(x, y \in \mathbb{F}\).

7. **Existence of a One.** There exists a non-zero element of \(\mathbb{F}\) (usually written as 1 & called the *multiplicative identity*) such that \(x1 = 1x = x\) for all \(x \in \mathbb{F}\).

8. **Existence of an Inverse for Multiplication.** For each non-zero \(x \in \mathbb{F}\), there exists an element \(w\) of \(\mathbb{F}\) (usually written as \(1/x\) or \(x^{-1}\) & called the *multiplicative inverse* of \(x\)) such that \(xw = wx = 1\).

9. **Distributive Law.** \(x(y + z) = xy + xz\) for all \(x, y, z \in \mathbb{F}\).

10. **Distributive Law.** \((x + y)z = xz + yz\), for all \(x, y, z \in \mathbb{F}\).
Field axioms

1. **Associative Law of Addition.** \((x + y) + z = x + (y + z)\) for all \(x, y, z \in \mathbb{F}\).

2. **Commutative Law of Addition.** \(x + y = y + x\) for all \(x, y \in \mathbb{F}\).

3. **Existence of a Zero.** There exists an element of \(\mathbb{F}\) (usually written as 0 & called zero) such that \(0 + x = x + 0 = x\) for all \(x \in \mathbb{F}\).

4. **Existence of a Negative.** For each \(x \in \mathbb{F}\), there exists an element \(w \in \mathbb{F}\) (usually written as \(-x\) & called the negative of \(x\)) such that \(x + w = w + x = 0\).

5. **Associative Law of Multiplication.** \(x(yz) = (xy)z\) for all \(x, y, z \in \mathbb{F}\).

6. **Commutative Law of Multiplication.** \(xy = yx\) for all \(x, y \in \mathbb{F}\).

7. **Existence of a One.** There exists a non-zero element of \(\mathbb{F}\) (usually written as 1 & called the multiplicative identity) such that \(x1 = 1x = x\) for all \(x \in \mathbb{F}\).

8. **Existence of an Inverse for Multiplication.** For each non-zero \(x \in \mathbb{F}\), there exists an element \(w\) of \(\mathbb{F}\) (usually written as \(1/x\) or \(x^{-1}\) & called the multiplicative inverse of \(x\)) such that \(xw = wx = 1\).

9. **Distributive Law.** \(x(y + z) = xy + xz\) for all \(x, y, z \in \mathbb{F}\).

10. **Distributive Law.** \((x + y)z = xz + yz\), for all \(x, y, z \in \mathbb{F}\).
Examples

E.g. fields $F = R, Q$ are fields when endowed with the usual addition and multiplication of numbers for the addition and multiplication rule.

E.g. the field with 2 elements

Let $F = \{\text{even}, \text{odd}\}$.

Define the addition rule by $	ext{even} + \text{even} = \text{even}$, $	ext{even} + \text{odd} = \text{odd}$, ....

and the multiplication rule by $	ext{even} \times \text{even} = \text{even}$, $	ext{even} \times \text{odd} = \text{even}$, ....

You can check all field axioms are satisfied.

Remark This field is very important in coding theory.
**Examples**

**E.g.** $\mathbb{F} = \mathbb{R}, \mathbb{Q}$ are fields when endowed with the usual addition and multiplication of numbers for the addition and multiplication rule.

**Remark**
This field is very important in coding theory.
Examples

E.g. \( \mathbb{F} = \mathbb{R}, \mathbb{Q} \) are fields when endowed with the usual addition and multiplication of numbers for the addition and multiplication rule.

E.g. the field with 2 elements Let \( \mathbb{F} = \{ \text{even, odd} \} \).
Examples

E.g. $\mathbb{F} = \mathbb{R}, \mathbb{Q}$ are fields when endowed with the usual addition and multiplication of numbers for the addition and multiplication rule.

E.g. the field with 2 elements Let $\mathbb{F} = \{\text{even, odd}\}$. Define the addition rule by

$$\text{even} + \text{even} = \text{even}, \quad \text{even} + \text{odd} = \text{odd}, \ldots.$$
**Examples**

**E.g.** \( F = \mathbb{R}, \mathbb{Q} \) are fields when endowed with the usual addition and multiplication of numbers for the addition and multiplication rule.

**E.g. the field with 2 elements** Let \( F = \{ \text{even}, \text{odd} \} \). Define the addition rule by

\[
\text{even} + \text{even} = \text{even}, \quad \text{even} + \text{odd} = \text{odd}, \ldots.
\]

and the multiplication rule by

\[
\text{even} \times \text{even} = \text{even}, \quad \text{even} \times \text{odd} = \text{even}, \ldots.
\]
E.g. $\mathbb{F} = \mathbb{R}, \mathbb{Q}$ are fields when endowed with the usual addition and multiplication of numbers for the addition and multiplication rule.

E.g. the field with 2 elements Let $\mathbb{F} = \{\text{even}, \text{odd}\}$. Define the addition rule by

\[
even + even = even, \quad even + odd = odd, \ldots.
\]

and the multiplication rule by

\[
even \times even = even, \quad even \times odd = even, \ldots.
\]

You can check all field axioms are satisfied.

Remark This field is very important in coding theory.
Examples

E.g. $\mathbb{F} = \mathbb{R}, \mathbb{Q}$ are fields when endowed with the usual addition and multiplication of numbers for the addition and multiplication rule.

E.g. the field with 2 elements Let $\mathbb{F} = \{\text{even}, \text{odd}\}$. Define the addition rule by

\[
\text{even } + \text{ even } = \text{ even}, \quad \text{even } + \text{ odd } = \text{ odd}, \quad \text{....}
\]

and the multiplication rule by

\[
\text{even } \times \text{ even } = \text{ even}, \quad \text{even } \times \text{ odd } = \text{ even}, \quad \text{....}
\]

You can check all field axioms are satisfied.

Remark This field is very important in coding theory.
What’s subtraction and division?

The point of the axioms, is that this is the minimal set of assumptions to ensure you can do all the usual arithmetic in the usual way.
What’s subtraction and division?

The point of the axioms, is that this is the minimal set of assumptions to ensure you can do all the usual arithmetic in the usual way.

In particular, you can subtract and divide (by non-zero field elements). To do this you need

Fact
In a field $F$, the zero, negative, one and multiplicative inverse are unique. (What’s this mean?)

The proof (omitted) is not hard, but many of you might find it strange.

Hence for $x, y \in F$ we can define:

$$x - y = x + (-y)$$

and if $y \neq 0$,

$$xy = xy - 1.$$

E.g. Simplify the following expression in a field

$$x(y + z) - yx.$$
What’s subtraction and division?

The point of the axioms, is that this is the minimal set of assumptions to ensure you can do all the usual arithmetic in the usual way.

In particular, you can subtract and divide (by non-zero field elements). To do this you need

Fact

In a field $\mathbb{F}$, the zero, negative, one and multiplicative inverse are unique. (What’s this mean?)

E.g. Simplify the following expression in a field $x(y + z) - yx$. 

Daniel Chan (UNSW)
Chapter 3: Complex Numbers
Semester 1 2019
What’s subtraction and division?

The point of the axioms, is that this is the minimal set of assumptions to ensure you can do all the usual arithmetic in the usual way.

In particular, you can subtract and divide (by non-zero field elements). To do this you need

**Fact**

In a field $\mathbb{F}$, the zero, negative, one and multiplicative inverse are unique. (What’s this mean?)

The proof (omitted) is not hard, but many of you might find it strange.
What’s subtraction and division?

The point of the axioms, is that this is the minimal set of assumptions to ensure you can do all the usual arithmetic in the usual way.

In particular, you can subtract and divide (by non-zero field elements). To do this you need

**Fact**

In a field $\mathbb{F}$, the zero, negative, one and multiplicative inverse are unique. (What’s this mean?)

The proof (omitted) is not hard, but many of you might find it strange. Hence for $x, y \in \mathbb{F}$ we can define: $x - y = x + (-y)$
What’s subtraction and division?

The point of the axioms, is that this is the minimal set of assumptions to ensure you can do all the usual arithmetic in the usual way.

In particular, you can subtract and divide (by non-zero field elements). To do this you need

Fact

In a field $\mathbb{F}$, the zero, negative, one and multiplicative inverse are unique. (What’s this mean?)

The proof (omitted) is not hard, but many of you might find it strange. Hence for $x, y \in \mathbb{F}$ we can define: $x - y = x + (-y)$ and if $y \neq 0$, $\frac{x}{y} = xy^{-1}$. 

E.g. Simplify the following expression in a field $\mathbb{F}$

$$x(y + z) - yx$$
What’s subtraction and division?

The point of the axioms, is that this is the minimal set of assumptions to ensure you can do all the usual arithmetic in the usual way.

In particular, you can subtract and divide (by non-zero field elements). To do this you need

**Fact**

In a field $\mathbb{F}$, the zero, negative, one and multiplicative inverse are unique. (What’s this mean?)

The proof (omitted) is not hard, but many of you might find it strange. Hence for $x, y \in \mathbb{F}$ we can define: $x - y = x + (-y)$ and if $y \neq 0$, $\frac{x}{y} = xy^{-1}$.

**E.g.** Simplify the following expression in a field

$$x(y + z) - yx$$
Our thought experiment suggests the following

**Definition**

A complex number is a formal expression of the form \( a + bi \) for some \( a, b \in \mathbb{R} \). In particular, two such numbers \( a + bi, a' + b'i \) are equal iff \( a = a' \), \( b = b' \) as real numbers.

**Remarks**

1. Formal means in particular, that the + is just a symbol, it doesn’t mean addition (yet).
2. We often write \( a \) for \( a + 0i \) and \( bi \) for \( 0 + bi \).
Complex numbers

Our thought experiment suggests the following

**Definition**

A *complex number* is a formal expression of the form $a + bi$ for some $a, b \in \mathbb{R}$. In particular, two such numbers $a + bi, a' + b'i$ are equal iff $a = a', b = b'$ as real numbers.
Our thought experiment suggests the following

Definition

A complex number is a formal expression of the form $a + bi$ for some $a, b \in \mathbb{R}$. In particular, two such numbers $a + bi, a' + b'i$ are equal iff $a = a', b = b'$ as real numbers.
The real part of $a + bi$ is $\text{Re}(a + bi) = a$
Complex numbers

Our thought experiment suggests the following

Definition

A complex number is a formal expression of the form $a + bi$ for some $a, b \in \mathbb{R}$. In particular, two such numbers $a + bi, a' + b'i$ are equal iff $a = a', b = b'$ as real numbers.

The real part of $a + bi$ is $\text{Re}(a + bi) = a$ and the imaginary part is $\text{Im}(a + bi) = b$. 
Our thought experiment suggests the following

**Definition**

A *complex number* is a formal expression of the form $a + bi$ for some $a, b \in \mathbb{R}$. In particular, two such numbers $a + bi, a' + b'i$ are equal iff $a = a', b = b'$ as real numbers.

The *real part* of $a + bi$ is $\text{Re}(a + bi) = a$ and the *imaginary part* is $\text{Im}(a + bi) = b$.

**Remarks** 1. Formal means in particular, that the + is just a symbol, it doesn’t mean addition (yet).
Our thought experiment suggests the following

**Definition**

A *complex number* is a formal expression of the form $a + bi$ for some $a, b \in \mathbb{R}$. In particular, two such numbers $a + bi, a' + b'i$ are equal iff $a = a', b = b'$ as real numbers.

The *real part* of $a + bi$ is $\text{Re}(a + bi) = a$ and the *imaginary part* is $\text{Im}(a + bi) = b$.

**Remarks**

1. Formal means in particular, that the $+$ is just a symbol, it doesn’t mean addition (yet).
2. We often write $a$ for $a + 0i$ and $bi$ for $0 + bi$. 
Arithmetic of complex numbers

Definition

Given complex numbers $a + bi, a' + b'i$ as above, we define addition and multiplication by

$$(a + bi) + (a' + b'i) = (a + a') + (b + b')i$$

$$(a + bi)(a' + b'i) = (aa' - bb') + (ab' + a'b)i$$

Warning

There are two clashes of notation. What's $a + bi$ mean?

We're OK.

Theorem

The set $\mathbb{C}$ of complex numbers with the above addition and multiplication rule is a field.

Proof.

Is long and tedious but elementary. Note zero is $0 + 0i$. This means we can perform complex number arithmetic as usual.

N.B. $\mathbb{C}$ extends the real number system since complex numbers of form $a + 0i$ add and multiply just like real numbers.
Arithmetic of complex numbers

Definition

Given complex numbers \( a + bi, a' + b'i \) as above, we define addition and multiplication by

\[
(a + bi) + (a' + b'i) = (a + a') + (b + b')i
\]

\[
(a + bi)(a' + b'i) = (aa' - bb') + (ab' + a'b)i
\]

Warning

There are two clashes of notation. What's \( a + bi \) mean? We're OK.

Theorem

The set \( \mathbb{C} \) of complex numbers with the above addition and multiplication rule is a field.

Proof.

Is long and tedious but elementary. Note zero is \( 0 + 0i \).

This means we can perform complex number arithmetic as usual.

N.B.

\( \mathbb{C} \) extends the real number system since complex numbers of form \( a + 0i \) add and multiply just like real numbers.
Arithmetic of complex numbers

Definition

Given complex numbers $a + bi, a' + b'i$ as above, we define addition and multiplication by

\[
(a + bi) + (a' + b'i) = (a + a') + (b + b')i \\
(a + bi)(a' + b'i) = (aa' - bb') + (ab' + a'b)i
\]
Arithmetic of complex numbers

**Definition**

Given complex numbers $a + bi$, $a' + b'i$ as above, we define addition and multiplication by

\[
(a + bi) + (a' + b'i) = (a + a') + (b + b')i
\]

\[
(a + bi)(a' + b'i) = (aa' - bb') + (ab' + a'b)i
\]

**Warning** There are two clashes of notation. What’s $a + bi$ mean?
Arithmetic of complex numbers

Definition

Given complex numbers $a + bi, a' + b'i$ as above, we define addition and multiplication by

$$\begin{align*}
(a + bi) + (a' + b'i) &= (a + a') + (b + b')i \\
(a + bi)(a' + b'i) &= (aa' - bb') + (ab' + a'b)i
\end{align*}$$

Warning There are two clashes of notation. What’s $a + bi$ mean? We’re OK.
Arithmetic of complex numbers

Definition

Given complex numbers $a + bi, a' + b'i$ as above, we define addition and multiplication by

\[
(a + bi) + (a' + b'i) = (a + a') + (b + b')i
\]

\[
(a + bi)(a' + b'i) = (aa' - bb') + (ab' + a'b)i
\]

Warning There are two clashes of notation. What’s $a + bi$ mean? We’re OK.

Theorem

The set $\mathbb{C}$ of complex numbers with the above addition and multiplication rule is a field.
Arithmetic of complex numbers

**Definition**

Given complex numbers \( a + bi \), \( a' + b'i \) as above, we define addition and multiplication by

\[
(a + bi) + (a' + b'i) = (a + a') + (b + b')i
\]
\[
(a + bi)(a' + b'i) = (aa' - bb') + (ab' + a'b)i
\]

**Warning** There are two clashes of notation. What’s \( a + bi \) mean? We’re OK.

**Theorem**

The set \( \mathbb{C} \) of complex numbers with the above addition and multiplication rule is a field.

**Proof.** Is long and tedious but elementary. Note zero is \( 0 + 0i \).
Arithmetic of complex numbers

**Definition**
Given complex numbers $a + bi, a' + b'i$ as above, we define addition and multiplication by

$$(a + bi) + (a' + b' i) = (a + a') + (b + b')i$$
$$(a + bi)(a' + b' i) = (aa' - bb') + (ab' + a'b)i$$

**Warning** There are two clashes of notation. What’s $a + bi$ mean? We’re OK.

**Theorem**
The set $\mathbb{C}$ of complex numbers with the above addition and multiplication rule is a field.

**Proof.** Is long and tedious but elementary. Note zero is $0 + 0i$. This means we can perform complex number arithmetic as usual.
Arithmetic of complex numbers

**Definition**
Given complex numbers \(a + bi, a' + b'i\) as above, we define addition and multiplication by

\[
(a + bi) + (a' + b'i) = (a + a') + (b + b')i
\]

\[
(a + bi)(a' + b'i) = (aa' - bb') + (ab' + a'b)i
\]

**Warning** There are two clashes of notation. What’s \(a + bi\) mean? We’re OK.

**Theorem**
The set \(\mathbb{C}\) of complex numbers with the above addition and multiplication rule is a field.

**Proof.** Is long and tedious but elementary. Note zero is \(0 + 0i\).
This means we can perform complex number arithmetic as usual.

**N.B.** \(\mathbb{C}\) extends the real number system since complex numbers of form \(a + 0i\) add and multiply just like real numbers.
Examples of complex arithmetic

Eg  What's the negative of $a + bi$?

Eg  $(5 - 7i) - (6 + i)$?

Eg  Simplify $(2 + i)(1 - 3i) - 1 + 3i$
Examples of complex arithmetic

Eg What’s the negative of $a + bi$?
Examples of complex arithmetic

**Eg** What’s the negative of $a + bi$?

**Eg** $(5 - 7i) - (6 + i)$?
Examples of complex arithmetic

Eg What’s the negative of $a + bi$?

Eg $(5 - 7i) - (6 + i)$?

Eg Simplify $(2 + i)(1 - 3i) - 1 + 3i$
Division

To get the inverse we need a cool formula. Let $z = a + bi \in \mathbb{C}$ (with $a, b \in \mathbb{R}$ of course). We define the conjugate of $z$ to be $\overline{z} = a - bi$.

$z \overline{z} = a^2 + b^2 \in \mathbb{R} \geq 0$.

This gives the multiplicative inverse of $z$ as $z^{-1} = \frac{\overline{z}}{a^2 + b^2}$.

This is all we need since we know inverses of real numbers. Usually though, we divide as follows.

E.g.

Daniel Chan (UNSW)  Chapter 3: Complex Numbers  Semester 1 2019  11 / 48
Division

To get the inverse we need

**Cool Formula**

Let \( z = a + bi \in \mathbb{C} \) (with \( a, b \in \mathbb{R} \) of course). We define the conjugate of \( z \) to be \( \bar{z} = a - bi \). 

\[
\bar{z} \cdot z = a^2 + b^2 \in \mathbb{R} \geq 0.
\]

This gives the multiplicative inverse of \( z \) as \( z^{-1} = \frac{\bar{z}}{a^2 + b^2} \).

This is all we need since we know inverses of real numbers.

Usually though, we divide as follows

E.g.
Division

To get the inverse we need

**Cool Formula**

Let $z = a + bi \in \mathbb{C}$ (with $a, b \in \mathbb{R}$ of course). We define the *conjugate of* $z$ to be $\bar{z} = a - bi$.

$$z\bar{z} = a^2 + b^2 \in \mathbb{R}_{\geq 0}.$$
Division

To get the inverse we need

Cool Formula

Let $z = a + bi \in \mathbb{C}$ (with $a, b \in \mathbb{R}$ of course). We define the conjugate of $z$ to be $\overline{z} = a - bi$.

$$z\overline{z} = a^2 + b^2 \in \mathbb{R}_{\geq 0}.$$  

This gives the multiplicative inverse of $z$ as

$$z^{-1} = \frac{\overline{z}}{a^2 + b^2}.$$
To get the inverse we need

Cool Formula

Let $z = a + bi \in \mathbb{C}$ (with $a, b \in \mathbb{R}$ of course). We define the conjugate of $z$ to be $\bar{z} = a - bi$.

$$z\bar{z} = a^2 + b^2 \in \mathbb{R}_{\geq 0}.$$

This gives the multiplicative inverse of $z$ as

$$z^{-1} = \frac{\bar{z}}{a^2 + b^2}.$$

This is all we need since we know inverses of real numbers.
To get the inverse we need

**Cool Formula**

Let \( z = a + bi \in \mathbb{C} \) (with \( a, b \in \mathbb{R} \) of course). We define the *conjugate of \( z \)* to be \( \bar{z} = a - bi \).

\[
z\bar{z} = a^2 + b^2 \in \mathbb{R}_{\geq 0}.
\]

This gives the multiplicative inverse of \( z \) as

\[
z^{-1} = \frac{\bar{z}}{a^2 + b^2}.
\]

This is all we need since we know inverses of real numbers.

Usually though, we divide as follows
Division

To get the inverse we need

**Cool Formula**

Let \( z = a + bi \in \mathbb{C} \) (with \( a, b \in \mathbb{R} \) of course). We define the *conjugate of \( z \)* to be \( \bar{z} = a - bi \).

\[
z \bar{z} = a^2 + b^2 \in \mathbb{R}_{\geq 0}.
\]

This gives the multiplicative inverse of \( z \) as

\[
z^{-1} = \frac{\bar{z}}{a^2 + b^2}.
\]

This is all we need since we know inverses of real numbers.

Usually though, we divide as follows

E.g.
Cartesian form

A complex number \( z \) written in the form \( a + bi \) with \( a, b \in \mathbb{R} \) is called the cartesian form (Later we'll meet the polar form).

Q Express \( 1 + i \) in cartesian form.
A complex number $z$ written in the form $a + bi$ with $a, b \in \mathbb{R}$ is called the **cartesian form** (Later we’ll meet the polar form).
A complex number $z$ written in the form $a + bi$ with $a, b \in \mathbb{R}$ is called the *cartesian form* (Later we’ll meet the polar form).

**Q** Express $\frac{1+i}{1-i} - \frac{1-i}{1+i}$ in cartesian form.
Properties of conjugation

Proposition 1
\( z \) is real iff (i.e., if and only if) \( z = \overline{z} \).

Proposition 2
\( \overline{z} = z \).

Proposition 3
\( z + w = \overline{z} + \overline{w} \) and \( z - w = \overline{z} - \overline{w} \).

Proposition 4
\( zw = \overline{z} \overline{w} \) and \( (zw) \overline{z} = \overline{z} \overline{w} \).

Proposition 5
\( \text{Re}(z) = \frac{1}{2}(z + \overline{z}) \) and \( \text{Im}(z) = \frac{1}{2}i(\overline{z} - z) \).

Proof.
Easy. Write both sides out e.g. Show that for any \( z \in \mathbb{C} \), \( (i + 5)z - (i - 5)\overline{z} \) is real.
Properties of conjugation

Proposition

1. $z$ is real iff (if and only if) $\overline{z} = z$.

Proof. Easy. Write both sides out e.g. Show that for any $z \in \mathbb{C}$, $(i + 5)z - (i - 5)z$ is real.
Properties of conjugation

Proposition

1. $z$ is real iff (= if and only if) $\bar{z} = z$.

2. $\bar{\bar{z}} = z$. 

Proof.

Easy. Write both sides out e.g.

E.g. Show that for any $z \in \mathbb{C}$, $(i + 5)z - (i - 5)z$ is real.

Daniel Chan (UNSW)

Chapter 3: Complex Numbers

Semester 1 2019
Properties of conjugation

Proposition

1. \( z \) is real iff \( (= \) if and only if) \( \overline{z} = z \).
2. \( \overline{\overline{z}} = z \).
3. \( \overline{z + w} = \overline{z} + \overline{w} \) and \( \overline{z - w} = \overline{z} - \overline{w} \).
Properties of conjugation

**Proposition**

1. \( z \) is real iff \( \bar{z} = z \).
2. \( \bar{\bar{z}} = z \).
3. \( \bar{z + w} = \bar{z} + \bar{w} \) and \( \bar{z - w} = \bar{z} - \bar{w} \).
4. \( \bar{zw} = \bar{z} \bar{w} \) and \( \frac{\bar{z}}{\bar{w}} = \frac{\bar{z}}{\bar{w}} \).

**Proof.** Easy. Write both sides out e.g. Show that for any \( z \in \mathbb{C} \), \( (i + 5)z - (i - 5)\bar{z} \) is real.
Properties of conjugation

Proposition

1. $z$ is real iff $= \text{ if and only if } \bar{z} = z$.
2. $\bar{\bar{z}} = z$.
3. $z + w = \bar{z} + \bar{w}$ and $z - w = \bar{z} - \bar{w}$.
4. $\bar{zw} = \bar{z} \bar{w}$ and $\frac{z}{w} = \frac{\bar{z}}{\bar{w}}$.
5. $\text{Re}(z) = \frac{1}{2}(z + \bar{z})$ and $\text{Im}(z) = \frac{1}{2i}(z - \bar{z})$.

Proof. Easy. Write both sides out e.g. Show that for any $z \in \mathbb{C}$, $(i + 5)z - (i - 5)z$ is real.
Properties of conjugation

**Proposition**

1. $z$ is real iff ($=$ if and only if) $\overline{z} = z$.
2. $\overline{\overline{z}} = z$.
3. $\overline{z + w} = \overline{z} + \overline{w}$ and $\overline{z - w} = \overline{z} - \overline{w}$.
4. $\overline{zw} = \overline{z} \overline{w}$ and $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$.
5. $\text{Re}(z) = \frac{1}{2}(z + \overline{z})$ and $\text{Im}(z) = \frac{1}{2i}(z - \overline{z})$.

**Proof.** Easy. Write both sides out e.g.
Properties of conjugation

Proposition

1. \( z \) is real iff \((= \text{if and only if}) \) \( \overline{z} = z \).
2. \( \overline{z} = z \).
3. \( \overline{z + w} = \overline{z} + \overline{w} \) and \( \overline{z - w} = \overline{z} - \overline{w} \).
4. \( \overline{zw} = \overline{z} \overline{w} \) and \( \overline{\left( \frac{z}{w} \right)} = \frac{\overline{z}}{\overline{w}} \).
5. \( \text{Re}(z) = \frac{1}{2}(z + \overline{z}) \) and \( \text{Im}(z) = \frac{1}{2i}(z - \overline{z}) \).

Proof. Easy. Write both sides out e.g.

E.g. Show that for any \( z \in \mathbb{C} \), \((i + 5)z - (i - 5)\overline{z} \) is real.
The Argand diagram

Just as real numbers can be represented by points on the real number line, complex numbers can be represented on the complex plane (or Argand diagram) as follows. 

\[ z = a + bi \]
is represented by the point with coords \((a, b) = (\text{Re} z, \text{Im} z)\).

The axes though are called the real and imaginary axes.

Adding complex numbers is by adding real and imaginary parts, i.e. coordinatewise so is represented geometrically by the addition of vectors. Similarly for subtraction.
The Argand diagram

Just as real numbers can be represented by points on the real number line, complex numbers can be represented on the complex plane (or Argand diagram) as follows.

\[ z = a + bi \]

is represented by the point with coords \((a, b) = (\text{Re}z, \text{Im}z)\).

The axes though are called the real and imaginary axes.

Adding complex numbers is by adding real and imaginary parts, i.e. coordinatewise so is represented geometrically by the addition of vectors. Similarly for subtraction.
The Argand diagram

Just as real numbers can be represented by points on the real number line, complex numbers can be represented on the complex plane (or Argand diagram) as follows.

\[ z = a + bi \] is represented by the point with coords \((a, b) = (\text{Re} z, \text{Im} z)\).

The axes though are called the *real* and *imaginary* axes.
The Argand diagram

Just as real numbers can be represented by points on the real number line, complex numbers can be represented on the complex plane (or Argand diagram) as follows.

\[ z = a + bi \] is represented by the point with coords \((a, b) = (\text{Re}z, \text{Im}z)\).

The axes though are called the real and imaginary axes.

Adding complex numbers is by adding real and imaginary parts, i.e. coordinatewise so is represented geometrically by the addition of vectors. Similarly for subtraction.
Polar form

Writing a complex number as $z = x + yi$, $x, y \in \mathbb{R}$ is called the cartesian form of $z$. It corresponds to rectilinear coordinates.

Suppose the polar coordinates for $z$ are given by $(r, \theta)$ as above.

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

**Definition**

1. The modulus of $z$ is defined to be $|z| = r = \sqrt{x^2 + y^2}$ so $\overline{z}z = |z|^2$. 

2. If $z \neq 0$, an argument for $z$ is any $\theta = \arg z$ as above i.e. so that $\tan \theta = \frac{y}{x}$ and $\cos \theta, \Re z$ have the same sign. 

$\theta =: \Arg z$ is the principal argument if further $-\pi < \theta \leq \pi$. 

Daniel Chan (UNSW)
Polar form

Writing a complex number as $z = x + yi, x, y \in \mathbb{R}$ is called the \textit{cartesian form} of $z$. It corresponds to rectilinear coordinates.
Polar form

Writing a complex number as $z = x + yi, x, y \in \mathbb{R}$ is called the *cartesian form* of $z$. It corresponds to rectilinear coordinates.

Suppose the polar coordinates for $z$ are given by $(r, \theta)$ as above.

The modulus of $z$ is defined to be $|z| = r = \sqrt{x^2 + y^2}$ so $z \bar{z} = |z|^2$.

If $z \neq 0$, an argument for $z$ is any $\theta = \arg z$ as above i.e. so that $\tan \theta = \frac{y}{x}$ and $\cos \theta, \Re z$ have the same sign.

$\theta =: \Arg z$ is the principal argument if further $-\pi < \theta \leq \pi$. 
Polar form

Writing a complex number as $z = x + yi, x, y \in \mathbb{R}$ is called the \textit{cartesian form} of $z$. It corresponds to rectilinear coordinates.

Suppose the polar coordinates for $z$ are given by $(r, \theta)$ as above.

$$z = r \cos \theta + (r \sin \theta)i.$$
Polar form

Writing a complex number as \( z = x + yi, x, y \in \mathbb{R} \) is called the \textit{cartesian form} of \( z \). It corresponds to rectilinear coordinates.

Suppose the polar coordinates for \( z \) are given by \((r, \theta)\) as above.

\[
z = r \cos \theta + (r \sin \theta)i.
\]

\textbf{Definition}

Let \( z = x + iy, x, y \in \mathbb{R} \).
Writing a complex number as $z = x + yi, x, y \in \mathbb{R}$ is called the \textit{cartesian form} of $z$. It corresponds to rectilinear coordinates.

Suppose the polar coordinates for $z$ are given by $(r, \theta)$ as above.

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

**Definition**

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

1. The \textit{modulus of $z$} is defined to be $|z| = r = \sqrt{x^2 + y^2}$ so $z\bar{z} = |z|^2$. 
Polar form

Writing a complex number as \( z = x + yi, x, y \in \mathbb{R} \) is called the *cartesian form* of \( z \). It corresponds to rectilinear coordinates.

Suppose the polar coordinates for \( z \) are given by \((r, \theta)\) as above.

\[
z = r \cos \theta + (r \sin \theta)i.
\]

**Definition**

Let \( z = x + iy, x, y \in \mathbb{R} \).

1. The *modulus of \( z \)* is defined to be \(|z| = r = \sqrt{x^2 + y^2}\) so \( z\bar{z} = |z|^2 \).
2. If \( z \neq 0 \), an *argument for \( z \)* is any \( \theta = \arg z \) as above i.e. so that \( \tan \theta = \frac{y}{x} \) and \( \cos \theta, \Re z \) have the same sign.
Polar form

Writing a complex number as \( z = x + yi, x, y \in \mathbb{R} \) is called the \textit{cartesian form} of \( z \). It corresponds to rectilinear coordinates.

Suppose the polar coordinates for \( z \) are given by \((r, \theta)\) as above.

\[ z = r \cos \theta + (r \sin \theta)i. \]

Definition

Let \( z = x + iy, x, y \in \mathbb{R} \).

1. The \textit{modulus of} \( z \) is defined to be \( |z| = r = \sqrt{x^2 + y^2} \) so \( z\overline{z} = |z|^2 \).

2. If \( z \neq 0 \), an \textit{argument for} \( z \) is any \( \theta = \arg z \) as above i.e. so that \( \tan \theta = \frac{y}{x} \) and \( \cos \theta, \Re z \) have the same sign. \( \theta =: \Arg z \) is the \textit{principal} argument if further \(-\pi < \theta \leq \pi\).
Examples: modulus and argument

E.g. Find the modulus and principal argument of $1 - \sqrt{3}i$.

E.g. Find the modulus and principal argument of $-5 - 12i$.

E.g. Find the complex number with modulus 3 and argument $\pi/4$. 
E.g. Find the modulus and principal argument of $1 - \sqrt{3}i$. 
Examples: modulus and argument

E.g. Find the modulus and principal argument of $1 - \sqrt{3}i$.

E.g. Find the modulus and principal argument of $-5 - 12i$. 
Examples: modulus and argument

E.g. Find the modulus and principal argument of $1 - \sqrt{3}i$.

E.g. Find the modulus and principal argument of $-5 - 12i$.

E.g. Find the complex number with modulus 3 and argument $\pi/4$. 
Euler’s formula

Definition (Euler’s formula)
For \( \theta \in \mathbb{R} \), we define
\[ e^{i\theta} = \cos(\theta) + i\sin(\theta). \]
This is reasonable by

1. \( e^{i(\theta_1 + \theta_2)} = e^{i\theta_1} e^{i\theta_2} \) (De Moivre’s thm)
2. For \( n \in \mathbb{Z} \), \( (e^{i\theta})^n = e^{in\theta} \)
3. \( \frac{d}{d\theta}(e^{i\theta}) = ie^{i\theta} \).

Proof. 2) & 3) easy omitted. We only check 1).

\[
(e^{i\theta_1}) (e^{i\theta_2}) = (\cos\theta_1 + i\sin\theta_1) (\cos\theta_2 + i\sin\theta_2)
= \cos\theta_1 \cos\theta_2 - \sin\theta_1 \sin\theta_2 + i(\cos\theta_1 \sin\theta_2 + \sin\theta_1 \cos\theta_2)
= \cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2).
\]

Challenge Q
What’s \( i^i \)?
Euler’s formula

Definition (Euler’s formula)

For $\theta \in \mathbb{R}$, we define $e^{i\theta} = \cos \theta + i \sin \theta$. 
Euler’s formula

Definition (Euler’s formula)

For $\theta \in \mathbb{R}$, we define $e^{i\theta} = \cos \theta + i \sin \theta$.

This is reasonable by
Euler’s formula

Definition (Euler’s formula)
For $\theta \in \mathbb{R}$, we define $e^{i\theta} = \cos \theta + i \sin \theta$.

This is reasonable by

Formulas

1. $e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$. 

Challenge Q
What's $i^i$?
Euler’s formula

**Definition (Euler’s formula)**

For \( \theta \in \mathbb{R} \), we define \( e^{i\theta} = \cos \theta + i \sin \theta \).

This is reasonable by

**Formulas**

1. \( e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1 + \theta_2)} \).
2. (De Moivre’s thm) For \( n \in \mathbb{Z} \), \( (e^{i\theta})^n = e^{in\theta} \).
Euler’s formula

Definition (Euler’s formula)

For $\theta \in \mathbb{R}$, we define $e^{i\theta} = \cos \theta + i \sin \theta$.

This is reasonable by

Formulas

1. $e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1 + \theta_2)}$.
2. (De Moivre’s thm) For $n \in \mathbb{Z}$, $(e^{i\theta})^n = e^{in\theta}$.
3. $\frac{d}{d\theta}(e^{i\theta}) = ie^{i\theta}$.
Euler’s formula

Definition (Euler’s formula)

For $\theta \in \mathbb{R}$, we define $e^{i\theta} = \cos \theta + i \sin \theta$.

This is reasonable by

Formulas

1. $e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1 + \theta_2)}$.
2. (De Moivre’s thm) For $n \in \mathbb{Z}$, $(e^{i\theta})^n = e^{in\theta}$.
3. $\frac{d}{d\theta}(e^{i\theta}) = ie^{i\theta}$.

Proof. 2) & 3) easy omitted. We only check 1).
Euler’s formula

Definition (Euler’s formula)
For $\theta \in \mathbb{R}$, we define $e^{i\theta} = \cos \theta + i \sin \theta$.

This is reasonable by

Formulas
1. $e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1 + \theta_2)}$.
2. (De Moivre’s thm) For $n \in \mathbb{Z}$, $(e^{i\theta})^n = e^{in\theta}$.
3. $\frac{d}{d\theta} (e^{i\theta}) = ie^{i\theta}$.

Proof. 2) & 3) easy omitted. We only check 1).

\[
(\cos \theta_1 + i \sin \theta_1) \times (\cos \theta_2 + i \sin \theta_2) \\
= \cos \theta_1 \cos \theta_2 - \sin \theta_1 \sin \theta_2 + i(\cos \theta_1 \sin \theta_2 + \sin \theta_1 \cos \theta_2) \\
= \cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2).
\]
Euler’s formula

**Definition (Euler’s formula)**

For $\theta \in \mathbb{R}$, we define $e^{i\theta} = \cos \theta + i \sin \theta$.

This is reasonable by

**Formulas**

1. $e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$.
2. (De Moivre’s thm) For $n \in \mathbb{Z}$, $(e^{i\theta})^n = e^{in\theta}$.
3. $\frac{d}{d\theta}(e^{i\theta}) = ie^{i\theta}$.

**Proof.** 2) & 3) easy omitted. We only check 1).

\[
(cos \theta_1 + i \sin \theta_1) \times (cos \theta_2 + i \sin \theta_2)
\]

\[
= \cos \theta_1 \cos \theta_2 - \sin \theta_1 \sin \theta_2 + i(\cos \theta_1 \sin \theta_2 + \sin \theta_1 \cos \theta_2)
\]

\[
= \cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2).
\]

**Challenge Q** What’s $i^i$?
Arithmetic of polar forms

The polar form of $z$ is $z = re^{i\theta}$ where $r = |z|$ and $\theta$ is an argument of $z$.

Our formulas above give

$$r_1e^{i\theta_1}r_2e^{i\theta_2} = (r_1r_2)e^{i(\theta_1+\theta_2)},$$

$$re^{i\theta} - 1 = r - 1e^{-i\theta}.$$

Geometrically, this says that when you multiply complex numbers, you multiply the moduli and add the arguments.

Inverting inverts the modulus and negates the argument.

$$|z_1z_2| = |z_1||z_2|,$$

$$|z_1|^{-1} = |z_1|^{-1},$$

$$\text{Arg}(z_1z_2) = \text{Arg}(z_1) + \text{Arg}(z_2) + 2k\pi,$$

$$\text{Arg}z_1^{-1} = -\text{Arg}z_1$$ unless where $k \in \mathbb{Z}$ is chosen so that

E.g. Find the exact value of $\text{Arg}(1+i)(1+\sqrt{3}i)$.
Arithmetic of polar forms

The polar form of $z$ is $z = re^{i\theta}$ where $r = |z|$ and $\theta$ is an argument of $z$. 

Our formulas above give $r_1 e^{i\theta_1} \cdot r_2 e^{i\theta_2} = (r_1 r_2) e^{i(\theta_1 + \theta_2)}$, $(re^{i\theta})^{-1} = r^{-1}e^{-i\theta}$. 

Geometrically, this says that when you multiply complex numbers, you multiply the moduli and add the arguments. 

Inverting inverts the modulus and negates the argument.

$|z_1 z_2| = |z_1| |z_2|$ 

$|z_1^{-1}| = |z_1|$ 

$\text{Arg}(z_1 z_2) = \text{Arg}(z_1) + \text{Arg}(z_2) + 2k\pi$, $\text{Arg}(z_1^{-1}) = -\text{Arg}(z_1)$ unless 

where $k \in \mathbb{Z}$ is chosen so that 

E.g. Find the exact value of $\text{Arg}(1 + i (1 + \sqrt{3}i))$. 

Daniel Chan (UNSW) 

Chapter 3: Complex Numbers 

Semester 1 2019 18 / 48
Arithmetic of polar forms

The polar form of $z$ is $z = re^{i\theta}$ where $r = |z|$ and $\theta$ is an argument of $z$. Our formulas above give

$$r_1 e^{i\theta_1} r_2 e^{i\theta_2} = (r_1 r_2) e^{i(\theta_1 + \theta_2)}, \quad (re^{i\theta})^{-1} = r^{-1} e^{-i\theta}.$$
Arithmetic of polar forms

The polar form of $z$ is $z = re^{i\theta}$ where $r = |z|$ and $\theta$ is an argument of $z$. Our formulas above give

$$r_1 e^{i\theta_1} r_2 e^{i\theta_2} = (r_1 r_2) e^{i(\theta_1 + \theta_2)} \quad , \quad (re^{i\theta})^{-1} = r^{-1} e^{-i\theta}.$$  

Geometrically, this says that when you multiply complex numbers, you **multiply the moduli** and **add the arguments**.
The polar form of $z$ is $z = re^{i\theta}$ where $r = |z|$ and $\theta$ is an argument of $z$. Our formulas above give

$$r_1 e^{i\theta_1} r_2 e^{i\theta_2} = (r_1 r_2) e^{i(\theta_1 + \theta_2)} , \quad (re^{i\theta})^{-1} = r^{-1} e^{-i\theta}.$$ 

Geometrically, this says that when you multiply complex numbers, you multiply the moduli and add the arguments. Inverting inverts the modulus and negates the argument.
The polar form of $z$ is $z = re^{i\theta}$ where $r = |z|$ and $\theta$ is an argument of $z$. Our formulas above give

$$r_1 e^{i\theta_1} r_2 e^{i\theta_2} = (r_1 r_2)e^{i(\theta_1+\theta_2)}, \quad (re^{i\theta})^{-1} = r^{-1}e^{-i\theta}.$$  

Geometrically, this says that when you multiply complex numbers, you **multiply the moduli** and **add the arguments**. Inverting inverts the modulus and negates the argument.

$$|z_1 z_2| = |z_1||z_2| \quad |z^{-1}| = |z|^{-1}$$

$$\text{Arg}(z_1 z_2) = \text{Arg}(z_1) + \text{Arg}(z_2) + 2k\pi,$$  

$$\text{Arg}z^{-1} = -\text{Arg}z \text{ unless }$$
The polar form of $z$ is $z = re^{i\theta}$ where $r = |z|$ and $\theta$ is an argument of $z$. Our formulas above give

$$r_1 e^{i\theta_1} r_2 e^{i\theta_2} = (r_1 r_2) e^{i(\theta_1 + \theta_2)}, \quad (re^{i\theta})^{-1} = r^{-1} e^{-i\theta}.$$

Geometrically, this says that when you multiply complex numbers, you **multiply the moduli** and **add the arguments**. Inverting inverts the modulus and negates the argument.

$$|z_1 z_2| = |z_1| |z_2|$$

$$\text{Arg}(z_1 z_2) = \text{Arg}(z_1) + \text{Arg}(z_2) + 2k\pi,$$

$$|z^{-1}| = |z|^{-1}$$

$$\text{Arg}z^{-1} = -\text{Arg}z \text{ unless }$$

where $k \in \mathbb{Z}$ is chosen so that
The polar form of $z$ is $z = re^{i\theta}$ where $r = |z|$ and $\theta$ is an argument of $z$. Our formulas above give

$$r_1 e^{i\theta_1} r_2 e^{i\theta_2} = (r_1 r_2) e^{i(\theta_1 + \theta_2)}, \quad (re^{i\theta})^{-1} = r^{-1} e^{-i\theta}.$$ 

Geometrically, this says that when you multiply complex numbers, you multiply the moduli and add the arguments. Inverting inverts the modulus and negates the argument.

$$|z_1 z_2| = |z_1| |z_2|, \quad |z^{-1}| = |z|^{-1}$$

$$\text{Arg}(z_1 z_2) = \text{Arg}(z_1) + \text{Arg}(z_2) + 2k\pi, \quad \text{Arg}z^{-1} = -\text{Arg}z \text{ unless }$$

where $k \in \mathbb{Z}$ is chosen so that

**E.g.** Find the exact value of $\text{Arg}\frac{1+i}{1+\sqrt{3}i}$. 

Let $z \in \mathbb{C}$ have $|z| = 1$. Show that $w = i - z + iz$ is purely imaginary in the sense that $\text{Re} \, w = 0$. Interpret the result geometrically.
Q Let $z \in \mathbb{C}$ have $|z| = 1$. Show that $w = \frac{i - z}{i + z}$ is purely imaginary in the sense that $\text{Re}w = 0$. Interpret the result geometrically.
Square roots of complex numbers

E.g. Find the complex square roots $\pm z$ of $16 - 30i$.
E.g. Find the complex square roots \( \pm z \) of \( 16 - 30i \)
Quadratic formula

E.g.

Solve \(z^2 + (1 + i)z + (-4 + 8i) = 0\).
E.g. Solve $z^2 + (1 + i)z + (-4 + 8i) = 0$. 
Cubic formula

In the 16th century Ferro, Tartaglia, Cardano, ... discovered how to solve cubics.

Formula \( z^3 + pz = q \) has solutions

\[
z = \sqrt[3]{q^2 + \sqrt{q^2 + 4p^3}} - \sqrt[3]{q^2 + \sqrt{q^2 + 4p^3}}.
\]

Let's use this to solve \( z^3 - z = 0 \) (which we know has solutions ...)

Bizarre fact

If there are 3 real roots, then the formula above ALWAYS involves non-real numbers.

Moral to this story

Even if you only ever cared about real numbers, complex numbers naturally arise.

Daniel Chan (UNSW)
In the 16th century Ferro, Tartaglia, Cardano, . . . , discovered how to solve cubics.

The cubic formula is:

\[ z^3 + pz = q \]

has solutions

\[ z = \sqrt[3]{q^2 + \sqrt{q^4 - 4p^3}} - \sqrt[3]{q^2 - \sqrt{q^4 - 4p^3}} \]

Let's use this to solve

\[ z^3 - z = 0 \] (which we know has solutions ???)

Bizarre fact

If there are 3 real roots, then the formula above ALWAYS involves non-real numbers.

Moral to this story

Even if you only ever cared about real numbers, complex numbers naturally arise.
In the 16th century Ferro, Tartaglia, Cardano, . . . , discovered how to solve cubics.

Formula

\[ z^3 + pz = q \] has solutions

\[
z = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.
\]
In the 16th century Ferro, Tartaglia, Cardano, . . . , discovered how to solve cubics.

**Formula**

\[ z^3 + pz = q \]

has solutions

\[
z = 
\sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + 
\sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}
\]

**Q** Let’s use this to solve \( z^3 - z = 0 \) (which we know has solns ???)
In the 16th century Ferro, Tartaglia, Cardano, . . . , discovered how to solve cubics.

Formula

\[ z^3 + pz = q \] has solutions

\[ z = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q^2}{4} + \frac{p^3}{27}\right)}} + \sqrt[3]{\frac{q}{2} - \sqrt{\left(\frac{q^2}{4} + \frac{p^3}{27}\right)}}. \]

Q Let’s use this to solve \( z^3 - z = 0 \) (which we know has solns ???)

Bizarre fact If there are 3 real roots, then the formula above ALWAYS involves non-real numbers.
In the 16th century Ferro, Tartaglia, Cardano,..., discovered how to solve cubics.

**Formula**

\[ z^3 + pz = q \] has solutions

\[ z = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \]

**Q** Let’s use this to solve \( z^3 - z = 0 \) (which we know has solns ???)

**Bizarre fact** If there are 3 real roots, then the formula above ALWAYS involves non-real numbers.

**Moral to this story** Even if you only ever cared about real numbers, complex numbers naturally arise.
Proof of the cubic formula

Recall the Binomial Theorem:

\[(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\]

where \(\binom{n}{k} = \frac{n!}{k!(n-k)!}\)

We use Vieta's substitution:

\[x = w - \frac{p}{3}w = w^3 - 3w^2p + 3wp^2 - \frac{p^3}{27}w + \frac{p}{3}(w - \frac{p}{3}w)\]

This is equivalent to the quadratic in \(w^3\) which has roots:

\[w^3 = \frac{1}{2}(q \pm \sqrt{q^2 + 4p^3/27})\]

Substituting back into \(x = w - \frac{p}{3}w\) gives the formula.
Proof of the cubic formula

Recall the Binomial Thm \((a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\)
Proof of the cubic formula

Recall the **Binomial Thm** \((a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\) where \(\binom{n}{k} = \frac{n!}{k!(n-k)!}\)
Proof of the cubic formula

Recall the **Binomial Thm** \((a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\) where \(\binom{n}{k} = \frac{n!}{k!(n-k)!}\)

We use Vieta’s substitution \(x = w - \frac{p}{3w}\)
Proof of the cubic formula

Recall the **Binomial Thm** \((a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\) where \(\binom{n}{k} = \frac{n!}{k!(n-k)!}\)

We use Vieta’s substitution \(x = w - \frac{p}{3w}\)

\[
q = \left( w^3 - 3w^2 \frac{p}{3w} + 3w \frac{p^2}{9w^2} - \frac{p^3}{27w^3} \right) + p \left( w - \frac{p}{3w} \right) \\
= w^3 - \frac{p^3}{27w^3}
\]
Proof of the cubic formula

Recall the **Binomial Thm** \((a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\) where \(\binom{n}{k} = \frac{n!}{k!(n-k)!}\)

We use Vieta’s substitution \(x = w - \frac{p}{3w}\)

\[
q = \left( w^3 - 3w^2 \frac{p}{3w} + 3w \frac{p^2}{9w^2} - \frac{p^3}{27w^3} \right) + p(w - \frac{p}{3w})
\]

\[
= w^3 - \frac{p^3}{27w^3}
\]

This is equivalent to the quadratic in \(w^3\)

\[
0 = w^6 - qw^3 - \frac{p^3}{27}
\]
Proof of the cubic formula

Recall the Binomial Thm \((a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\) where \(\binom{n}{k} = \frac{n!}{k!(n-k)!}\)

We use Vieta’s substitution \(x = w - \frac{p}{3w}\)

\[
q = \left( w^3 - 3w^2 \frac{p}{3w} + 3w \frac{p^2}{9w^2} - \frac{p^3}{27w^3} \right) + p\left( w - \frac{p}{3w} \right)
\]

\[
= w^3 - \frac{p^3}{27w^3}
\]

This is equivalent to the quadratic in \(w^3\)

\[
0 = w^6 - qw^3 - \frac{p^3}{27}
\]

which has roots

\[
w^3 = \frac{1}{2} \left( q \pm \sqrt{q^2 + \frac{4p^3}{27}} \right).
\]
Proof of the cubic formula

Recall the **Binomial Thm** \((a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\) where \(\binom{n}{k} = \frac{n!}{k!(n-k)!}\)

We use Vieta’s substitution \(x = w - \frac{p}{3w}\)

\[
q = \left( w^3 - 3w^2 \frac{p}{3w} + 3w \frac{p^2}{9w^2} - \frac{p^3}{27w^3} \right) + p\left( w - \frac{p}{3w} \right) \\
= w^3 - \frac{p^3}{27w^3}
\]

This is equivalent to the quadratic in \(w^3\)

\[0 = w^6 - qw^3 - \frac{p^3}{27}\]

which has roots

\[w^3 = \frac{1}{2} \left( q \pm \sqrt{q^2 + \frac{4p^3}{27}} \right).\]

Substituting back into \(x = w - \frac{p}{3w}\) gives the formula.
Powers of complex numbers

Polar form allows us to find $n$-th powers and $n$-th roots of a complex number. 

E.g. Find $w = (1 + i)^{18}$.

[Dumb way: multiply out $(1 + i)(1 + i)\ldots(1 + i)$]
Powers of complex numbers

Polar form allows us to find \( n \)-th powers and \( n \)-th roots of a complex number.

E.g. Find \( w = (1 + i)^{18} \).

Dumb way: multiply out \((1 + i)(1 + i)\ldots(1 + i)\).
Powers of complex numbers

Polar form allows us to find $n$-th powers and $n$-th roots of a complex number.

**E.g.** Find $w = (1 + i)^{18}$. 
Powers of complex numbers

Polar form allows us to find $n$-th powers and $n$-th roots of a complex number.

**E.g.** Find $w = (1 + i)^{18}$.
[Dumb way: multiply out $(1 + i)(1 + i) \ldots (1 + i)$]
More interestingly, polar forms allow easy computation of roots.
More interestingly, polar forms allow easy computation of roots.

**E.g.** Solve $z^4 = i$. 
The geometry of complex $n$-th roots

This example shows something that is true more generally. Suppose that $0 \neq z_0 \in \mathbb{C}$ is given and $n \in \mathbb{Z}^+$. Then the equation $z^n = z_0$ has exactly $n$ solutions. These all lie equally spaced on the circle centred at the origin with radius $|z_0|^{1/n}$. One solution has argument $\text{Arg}(z_0)^n$, and from this you can see where the remaining solutions lie.
This example shows something that is true more generally.

Suppose that $0 \neq z_0 \in \mathbb{C}$ is given and $n \in \mathbb{Z}^+$. Then the equation $z^n = z_0$ has exactly $n$ solutions. These all lie equally spaced on the circle centred at the origin with radius $|z_0|^{1/n}$. One solution has argument $\text{Arg}(z_0)^n$, and from this you can see where the remaining solutions lie.
This example shows something that is true more generally.

Suppose that $0 \neq z_0 \in \mathbb{C}$ is given and $n \in \mathbb{Z}^+$. Then the equation $z^n = z_0$ has exactly $n$ solutions. These all lie equally spaced on the circle centred at the origin with radius $|z_0|^{1/n}$. One solution has argument $\text{Arg}(z_0)^n$, and from this you can see where the remaining solutions lie.
The geometry of complex $n$-th roots

This example shows something that is true more generally. Suppose that $0 \neq z_0 \in \mathbb{C}$ is given and $n \in \mathbb{Z}^+$. Then the equation

$$z^n = z_0$$

has exactly $n$ solutions.
This example shows something that is true more generally.

Suppose that \( 0 \neq z_0 \in \mathbb{C} \) is given and \( n \in \mathbb{Z}^+ \). Then the equation

\[
z^n = z_0
\]

has exactly \( n \) solutions. These all lie equally spaced on the circle centred at the origin with radius \( |z_0|^{1/n} \).
The geometry of complex $n$-th roots

This example shows something that is true more generally.

Suppose that $0 \neq z_0 \in \mathbb{C}$ is given and $n \in \mathbb{Z}^+$. Then the equation

$$z^n = z_0$$

has exactly $n$ solutions. These all lie equally spaced on the circle centred at the origin with radius $|z_0|^{1/n}$.

One solution has argument $\frac{\text{Arg}(z_0)}{n}$, and from this you can see where the remaining solutions lie.
A number theoretic result

A sum of squares is an integer of the form $a^2 + b^2$ where $a, b \in \mathbb{Z}$.

E.g. $6$?

Theorem

The product of two sums of squares is itself a sum of squares.

Proof.

We have to show given integers $a, b, c, d$, that $(a^2 + b^2)(c^2 + d^2)$ is a sum of two squares.

Note

Using an extension of complex numbers called hypercomplex numbers or quaternions, one can show that every non-negative integer is the sum of 4 squares!
A number theoretic result

A *sum of squares* is an integer of the form $a^2 + b^2$ where $a, b \in \mathbb{Z}$.

Theorem

The product of two sums of squares is itself a sum of squares.

Proof.

We have to show given integers $a, b, c, d$, that $(a^2 + b^2)(c^2 + d^2)$ is a sum of two squares.

Note

Using an extension of complex numbers called *hypercomplex numbers* or *quaternions*, one can show that every non-negative integer is the sum of 4 squares!
A number theoretic result

A *sum of squares* is an integer of the form $a^2 + b^2$ where $a, b \in \mathbb{Z}$. E.g. 6??

**Theorem**
The product of two sums of squares is itself a sum of squares.

**Proof.** We have to show given integers $a, b, c, d$, that $(a^2 + b^2)(c^2 + d^2)$ is a sum of two squares.

Just note that $(a^2 + b^2)(c^2 + d^2) = \ldots$

Note Using an extension of complex numbers called *hypercomplex numbers* or *quaternions*, one can show that every non-negative integer is the sum of 4 squares!
A sum of squares is an integer of the form $a^2 + b^2$ where $a, b \in \mathbb{Z}$. E.g. 6?

**Theorem**

The product of two sums of squares is itself a sum of squares.
A number theoretic result

A sum of squares is an integer of the form $a^2 + b^2$ where $a, b \in \mathbb{Z}$. E.g. 6??

Theorem

The product of two sums of squares is itself a sum of squares.

Proof. We have to show given integers $a, b, c, d$, that $(a^2 + b^2)(c^2 + d^2)$ is a sum of two squares.
A number theoretic result

A *sum of squares* is an integer of the form $a^2 + b^2$ where $a, b \in \mathbb{Z}$. E.g. 6??

**Theorem**

The product of two sums of squares is itself a sum of squares.

**Proof.** We have to show given integers $a, b, c, d$, that $(a^2 + b^2)(c^2 + d^2)$ is a sum of two squares. Just note that

$$(a^2 + b^2)(c^2 + d^2) =$$
A sum of squares is an integer of the form $a^2 + b^2$ where $a, b \in \mathbb{Z}$. E.g. 6??

**Theorem**

The product of two sums of squares is itself a sum of squares.

**Proof.** We have to show given integers $a, b, c, d$, that $(a^2 + b^2)(c^2 + d^2)$ is a sum of two squares. Just note that

$$(a^2 + b^2)(c^2 + d^2) =$$

**Note** Using an extension of complex numbers called *hypercomplex numbers* or *quaternions*, one can show that every non-negative integer is the sum of 4 squares!
Expressing trigonometric polynomials as polynomials in \( \cos \theta, \sin \theta \)
Expressing trigonometric polynomials as polynomials in $\cos \theta$, $\sin \theta$

A **trigonometric polynomial** is a linear combination of functions of the form $\cos n\theta$, $\sin n\theta$.

Example:

Use De Moivre’s theorem to show $\cos(3\theta) = 4 \cos^3\theta - 3 \cos \theta$.

$$
\begin{align*}
\cos 3\theta &= \Re(e^{i3\theta}) \\
&= \Re(\cos \theta + i\sin \theta)^3 \\
&= \Re(\cos^3 \theta + 3i\cos^2 \theta \sin \theta - 3\cos \theta \sin^2 \theta - i\sin^3 \theta) \\
&= \cos^3 \theta - 3\cos \theta \sin^2 \theta \\
&= 4 \cos^3 \theta - 3 \cos \theta.
\end{align*}
$$
Expressing trigonometric polynomials as polynomials in $\cos \theta$, $\sin \theta$

A *trigonometric polynomial* is a linear combination of functions of the form $\cos n\theta, \sin n\theta$.

**Example:** Use De Moivre’s thm to show $\cos(3\theta) = 4 \cos^3 \theta - 3 \cos \theta$.

$$\cos 3\theta = \Re (e^{i3\theta})$$

$$= \Re (\cos \theta + i \sin \theta)^3$$

$$= \Re (\cos^3 \theta + 3i \cos^2 \theta \sin \theta - 3 \cos \theta \sin^2 \theta - i \sin^3 \theta)$$

$$= \cos^3 \theta - 3 \cos \theta \sin^2 \theta$$

$$= \cos^3 \theta - 3 \cos \theta (1 - \cos^2 \theta)$$

$$= 4 \cos^3 \theta - 3 \cos \theta.$$
Application to solving cubics

We use the substitution \( x = r \cos \theta \) so \( r^3 \cos^3 \theta - 3r \cos \theta = 1 \).

Pick \( r = 2 \) so ratio of co-efficients matches with \( 4 \cos^3 \theta - 3 \cos \theta \).

Divide the eqn by \( r = 2 \) to obtain \( \frac{1}{2} = 4 \cos^3 \theta - 3 \cos \theta = \cos 3\theta \).

Hence \( 3\theta = \frac{\pi}{3} + 2k \pi \) for \( k \in \mathbb{Z} \).

The roots are thus \( x = 2 \cos \frac{\pi}{9}, 2 \cos \frac{7\pi}{9}, 2 \cos \frac{-5\pi}{9} \).

Challenge Q

Show that if a cubic \( x^3 - px - q \) has 3 real roots, then this method always works.
Application to solving cubics

Q Solve $x^3 - 3x = 1$

We use the substitution $x = r \cos \theta$ so $r^3 \cos^3 \theta - 3r \cos \theta = 1$.

Pick $r = 2$ so ratio of co-efficients matches with $4 \cos 3\theta - 3 \cos \theta$.

Divide the eqn by $r = 2$ to obtain $\frac{1}{2} = 4 \cos 3\theta - 3 \cos \theta = \cos 3\theta$.

Hence $3\theta = \frac{\pi}{3} + 2k\pi$ for $k \in \mathbb{Z}$. The roots are thus $x = 2 \cos \frac{\pi}{9}, 2 \cos \frac{7\pi}{9}, 2 \cos \frac{-5\pi}{9}$.

Challenge Q Show that if a cubic $x^3 - px - q$ has 3 real roots, then this method always works.
Q Solve $x^3 - 3x = 1$

A We use the substitution $x = r \cos \theta$ so

$$r^3 \cos^3 \theta - 3r \cos \theta = 1.$$ 

Pick $r = 2$ so ratio of co-efficients matches $4 \cos^3 \theta - 3 \cos \theta = \cos 3\theta$. 

Divide the eqn by $r = 2$ to obtain 

$$\frac{1}{2} = 4 \cos^3 \theta - 3 \cos \theta = \cos 3\theta.$$ 

Hence $3\theta = \pi/3 + 2k\pi$ for $k \in \mathbb{Z}$. The roots are thus 

$$x = 2 \cos \pi/9, 2 \cos 7\pi/9, 2 \cos -5\pi/9.$$ 

Challenge Q Show that if a cubic $x^3 - px - q$ has 3 real roots, then this method always works.
Q Solve $x^3 - 3x = 1$

A We use the substitution $x = r \cos \theta$ so

$$r^3 \cos^3 \theta - 3r \cos \theta = 1.$$
Application to solving cubics

**Q** Solve $x^3 - 3x = 1$

**A** We use the substitution $x = r \cos \theta$ so

$$r^3 \cos^3 \theta - 3r \cos \theta = 1.$$ 

Pick $r = 2$ so ratio of co-efficients matches with $4 \cos^3 \theta - 3 \cos \theta$.

Challenge **Q** Show that if a cubic $x^3 - px - q$ has 3 real roots, then this method always works.
Q Solve \( x^3 - 3x = 1 \)

A We use the substitution \( x = r \cos \theta \) so

\[
    r^3 \cos^3 \theta - 3r \cos \theta = 1.
\]

Pick \( r = 2 \) so ratio of co-efficients matches with \( 4 \cos^3 \theta - 3 \cos \theta \).

Divide the eqn by \( r = 2 \) to obtain

\[
    \frac{1}{2} = 4 \cos^3 \theta - 3 \cos \theta = \cos 3\theta.
\]
Application to solving cubics

Q Solve $x^3 - 3x = 1$

A We use the substitution $x = r \cos \theta$ so

$$r^3 \cos^3 \theta - 3r \cos \theta = 1.$$ 

Pick $r = 2$ so ratio of co-efficients matches with $4 \cos^3 \theta - 3 \cos \theta$.

Divide the eqn by $r = 2$ to obtain

$$\frac{1}{2} = 4 \cos^3 \theta - 3 \cos \theta = \cos 3\theta.$$ 

Hence $3\theta = \frac{\pi}{3} + 2k\pi$ for $k \in \mathbb{Z}$. The roots are thus
Application to solving cubics

Q Solve $x^3 - 3x = 1$

A We use the substitution $x = r \cos \theta$ so

$$r^3 \cos^3 \theta - 3r \cos \theta = 1.$$

Pick $r = 2$ so ratio of co-efficients matches with $4 \cos^3 \theta - 3 \cos \theta$.

Divide the eqn by $r = 2$ to obtain

$$\frac{1}{2} = 4 \cos^3 \theta - 3 \cos \theta = \cos 3\theta.$$ 

Hence $3\theta = \frac{\pi}{3} + 2k\pi$ for $k \in \mathbb{Z}$. The roots are thus

$$x = 2 \cos \frac{\pi}{9}, 2 \cos \frac{7\pi}{9}, 2 \cos \frac{-5\pi}{9}.$$
**Application to solving cubics**

**Q** Solve $x^3 - 3x = 1$

**A** We use the substitution $x = r \cos \theta$ so

$$r^3 \cos^3 \theta - 3r \cos \theta = 1.$$ 

Pick $r = 2$ so ratio of co-efficients matches with $4 \cos^3 \theta - 3 \cos \theta$.

Divide the eqn by $r = 2$ to obtain

$$\frac{1}{2} = 4 \cos^3 \theta - 3 \cos \theta = \cos 3\theta.$$ 

Hence $3\theta = \frac{\pi}{3} + 2k\pi$ for $k \in \mathbb{Z}$. The roots are thus

$$x = 2 \cos \frac{\pi}{9}, \ 2 \cos \frac{7\pi}{9}, \ 2 \cos \frac{-5\pi}{9}.$$ 

**Challenge Q** Show that if a cubic $x^3 - px - q$ has 3 real roots, then this method always works.
Remark on solving higher order equations

Cardano's formula for the cubic can be used to solve the general cubic. There's a similar formula for the quartic (i.e. degree 4). There is no similar formula for degree 5 and higher. Abel and Galois proved this in the 18th century. This is taught in our 3rd/4th year course Galois theory.

Our solution to the cubic via trigonometric functions can be extended to quintics if you use fancier functions called elliptic functions.
Remark on solving higher order equations

- Cardano’s formula for the cubic can be used to solve the general cubic.
Remark on solving higher order equations

- Cardano’s formula for the cubic can be used to solve the general cubic.
- There’s a similar formula for the quartic (i.e. degree 4).
Remark on solving higher order equations

- Cardano’s formula for the cubic can be used to solve the general cubic.
- There’s a similar formula for the quartic (i.e. degree 4).
- There is no similar formula for degree 5 and higher. Abel and Galois proved this in the 18th century. This is taught in our 3rd/4th year course Galois theory.

Our solution to the cubic via trigonometric functions can be extended to quintics if you use fancier functions called elliptic functions.
Remark on solving higher order equations

- Cardano’s formula for the cubic can be used to solve the general cubic.
- There’s a similar formula for the quartic (i.e. degree 4).
- There is no similar formula for degree 5 and higher. Abel and Galois proved this in the 18th century. This is taught in our 3rd/4th year course Galois theory.
- Our solution to the cubic via trigonometric functions can be extended to quintics if you use fancier functions called *elliptic functions*. 
cos \theta, \sin \theta in terms of exponentials
Since

\[ e^{i\theta} = \cos \theta + i \sin \theta \]
\[ e^{-i\theta} = \cos(-\theta) + i \sin(-\theta) \]
\[ = \cos \theta - i \sin \theta \]
\[ = e^{i\theta} \]
cos \theta, \sin \theta \text{ in terms of exponentials}

Since

\[ e^{i\theta} = \cos \theta + i \sin \theta \]
\[ e^{-i\theta} = \cos(-\theta) + i \sin(-\theta) = \cos \theta - i \sin \theta = \overline{e^{i\theta}} \]

we have

\[ \cos \theta = \frac{e^{i\theta} + e^{-i\theta}}{2}, \quad \text{and} \quad i \sin \theta = \frac{e^{i\theta} - e^{-i\theta}}{2}. \]
Expressing \( \cos^n \theta, \sin^n \theta \) as trig polynomials

E.g.

Prove that

\[
\sin 4\theta = \frac{1}{8} \cos 4\theta - \frac{1}{2} \cos 2\theta + \frac{3}{8}.
\]

\[
\sin 4\theta = \left( e^{i\theta} - e^{-i\theta} \right)^4 = \sum e^{i k \theta} = \sum e^{i k \theta} \frac{1}{2^{k/2}} \binom{4}{k}.
\]

Thus

\[
\int \sin 4\theta \, d\theta = \frac{1}{8} \cos 4\theta - \frac{1}{2} \cos 2\theta + \frac{3}{8}.
\]
Expressing $\cos^n \theta$, $\sin^n \theta$ as trig polynomials

E.g. Prove that $\sin^4 \theta = \frac{1}{8} \cos 4\theta - \frac{1}{2} \cos 2\theta + \frac{3}{8}$. 
Expressing $\cos^n \theta$, $\sin^n \theta$ as trig polynomials

E.g. Prove that $\sin^4 \theta = \frac{1}{8} \cos 4\theta - \frac{1}{2} \cos 2\theta + \frac{3}{8}$.

$$
\sin^4 \theta = \left(\frac{e^{i\theta} - e^{-i\theta}}{2i}\right)^4
$$

$$
= \frac{e^{4i\theta} - 4e^{2i\theta} + 6 - 4e^{-2i\theta} + e^{-4i\theta}}{16}
$$

$$
= \frac{e^{4i\theta} + e^{-4i\theta}}{16} - 4 \frac{e^{2i\theta} + e^{-2i\theta}}{16} + \frac{6}{16}
$$

$$
= \frac{1}{8} \cos 4\theta - \frac{1}{2} \cos 2\theta + \frac{3}{8}.
$$
Expressing \( \cos^n \theta, \sin^n \theta \) as trig polynomials

**E.g.** Prove that \( \sin^4 \theta = \frac{1}{8} \cos 4\theta - \frac{1}{2} \cos 2\theta + \frac{3}{8} \).

\[
\sin^4 \theta = \left( \frac{e^{i\theta} - e^{-i\theta}}{2i} \right)^4
\]

\[
= \frac{e^{i4\theta} - 4e^{i2\theta} + 6 - 4e^{-i2\theta} + e^{-i4\theta}}{16}
\]

\[
= \frac{e^{i4\theta} + e^{-i4\theta}}{16} - 4 \frac{e^{i2\theta} + e^{-i2\theta}}{16} + \frac{6}{16}
\]

\[
= \frac{1}{8} \cos 4\theta - \frac{1}{2} \cos 2\theta + \frac{3}{8}.
\]

Thus \( \int \sin^4 \theta \, d\theta = \)
Trigonometric sums

Consider the sum of a geometric progression $S = e^{i\theta} + e^{i2\theta} + \ldots + e^{in\theta} = e^{i(n+1)\theta} - e^{i\theta} - 1$.

Then $\Sigma = \text{Re} S = S_1 + S_2 = \frac{1}{2}(e^{in\theta/2} - e^{-in\theta/2}) e^{i\theta/2} = \cos((n+1)\theta/2)\sin(n\theta/2)\sin(\theta/2)$, which has real part $\Sigma = \cos((n+1)\theta/2)\sin(n\theta/2)\sin(\theta/2)$.
Q Find $\Sigma = \cos \theta + \cos 2\theta + \ldots + \cos n\theta$. 

Consider the sum of a geometric progression $S$:

$$S = e^{i\theta} + e^{i2\theta} + \ldots + e^{in\theta} = e^{i(n+1)\theta} - e^{i\theta} - 1.$$ 

Then

$$\Sigma = \text{Re} S = S + S^2 = \frac{1}{2}$$

which has real part $\Sigma = \cos \left( \frac{(n+1)\theta}{2} \right) \sin \frac{n\theta}{2} \sin \frac{\theta}{2}$. 

Daniel Chan  (UNSW)  
Chapter 3: Complex Numbers  
Semester 1 2019  33 / 48
Q Find $\Sigma = \cos \theta + \cos 2\theta + \ldots + \cos n\theta$.

A Consider the sum of a geometric progression

$$S := e^{i\theta} + e^{i2\theta} + \ldots + e^{in\theta} = \frac{e^{i(n+1)\theta} - e^{i\theta}}{e^{i\theta} - 1}.$$
Q Find $\Sigma = \cos \theta + \cos 2\theta + \ldots + \cos n\theta$.

A Consider the sum of a geometric progression

$$S := e^{i\theta} + e^{i2\theta} + \ldots + e^{in\theta} = \frac{e^{i(n+1)\theta} - e^{i\theta}}{e^{i\theta} - 1}.$$ 

Then

$$\Sigma = \Re S = \frac{S + \overline{S}}{2} = \frac{1}{2} \left( \frac{e^{i(n+1)\theta} - e^{i\theta}}{e^{i\theta} - 1} + \frac{e^{-i(n+1)\theta} - e^{-i\theta}}{e^{-i\theta} - 1} \right) = \ldots$$
Trigonometric sums

Q Find $\Sigma = \cos \theta + \cos 2\theta + \ldots + \cos n\theta$.

A Consider the sum of a geometric progression

$$S := e^{i\theta} + e^{i2\theta} + \ldots + e^{in\theta} = \frac{e^{i(n+1)\theta} - e^{i\theta}}{e^{i\theta} - 1}.$$ 

Then

$$\Sigma = \text{Re}\, S = \frac{S + \bar{S}}{2} = \frac{1}{2} \left( \frac{e^{i(n+1)\theta} - e^{i\theta}}{e^{i\theta} - 1} + \frac{e^{-i(n+1)\theta} - e^{-i\theta}}{e^{-i\theta} - 1} \right) = \ldots$$

OR note

$$S = e^{i\theta} \frac{e^{in\theta} - 1}{e^{i\theta} - 1} = e^{i\theta} \frac{e^{in\theta/2}(e^{in\theta/2} - e^{-in\theta/2})}{e^{i\theta/2}(e^{i\theta/2} - e^{-i\theta/2})} = e^{i(n+1)\theta/2} \frac{\sin n\theta/2}{\sin \theta/2}$$
Q Find $\Sigma = \cos \theta + \cos 2\theta + \ldots + \cos n\theta$.

A Consider the sum of a geometric progression

$$S := e^{i\theta} + e^{i2\theta} + \ldots + e^{in\theta} = \frac{e^{i(n+1)\theta} - e^{i\theta}}{e^{i\theta} - 1}.$$ 

Then

$$\Sigma = \text{Re}S = \frac{S + \overline{S}}{2} = \frac{1}{2} \left( \frac{e^{i(n+1)\theta} - e^{i\theta}}{e^{i\theta} - 1} + \frac{e^{-i(n+1)\theta} - e^{-i\theta}}{e^{-i\theta} - 1} \right) = \ldots$$

OR note

$$S = e^{i\theta} \frac{e^{in\theta} - 1}{e^{i\theta} - 1} = e^{i\theta} \frac{e^{in\theta/2}(e^{in\theta/2} - e^{-in\theta/2})}{e^{i\theta/2}(e^{i\theta/2} - e^{-i\theta/2})} = e^{i(n+1)\theta/2} \frac{\sin n\theta/2}{\sin \theta/2}$$

which has real part $\Sigma = \cos \left( (n + 1)\theta/2 \right) \frac{\sin n\theta/2}{\sin \theta/2}$.
Describing domains in the complex plane

If $z$ and $w$ are complex numbers then $|z - w|$ is the distance from $w$ to $z$, and $\text{Arg}(z - w)$ is the "direction" from $w$ to $z$.

Thus $S = \{ z \in \mathbb{C} : |z - i| \leq 3 \}$ is the disk centred at $i = (0,1)$ with radius 3.

The set $T = \{ z \in \mathbb{C} : 0 \leq \text{Arg}(z - 1 + i) \leq \pi/2 \}$ is the set of all the points $z$ for which the direction from $1 - i$ lies between 0 and $\pi/2$.

[For the pedants: $1 - i \not\in T$]
Describing domains in the complex plane

If $z$ and $w$ are complex numbers then $|z - w|$ is the distance from $w$ to $z$, and $\text{Arg}(z - w)$ is the "direction" from $w$ to $z$.

Thus $S = \{ z \in \mathbb{C} : |z - i| \leq 3 \}$ is the disk centred at $i = (0, 1)$ with radius 3.

The set $T = \{ z \in \mathbb{C} : 0 \leq \text{Arg}(z - 1 + i) \leq \pi/2 \}$ is the set of all the points $z$ for which the direction from $1 - i$ lies between 0 and $\pi/2$.

[For the pedants: $1 - i \not\in T$]
Describing domains in the complex plane

If $z$ and $w$ are complex numbers then $|z - w|$ is the distance from $w$ to $z$, and $\text{Arg}(z - w)$ is the “direction” from $w$ to $z$. 

$S = \{ z \in \mathbb{C} : |z - i| \leq 3 \}$ is the disk centred at $i = (0, 1)$ with radius 3.

$T = \{ z \in \mathbb{C} : 0 \leq \text{Arg}(z - 1 + i) \leq \pi/2 \}$ is the set of all the points $z$ for which the direction from $1 - i$ lies between 0 and $\pi/2$.

[For the pedants: $1 - i \not\in T$]
Describing domains in the complex plane

If \( z \) and \( w \) are complex numbers then \( |z - w| \) is the distance from \( w \) to \( z \), and \( \text{Arg}(z - w) \) is the “direction” from \( w \) to \( z \). Thus

\[
S = \{ z \in \mathbb{C} : |z - i| \leq 3 \}
\]

is the disk centred at \( i = (0, 1) \) with radius 3.
Describing domains in the complex plane

If \( z \) and \( w \) are complex numbers then \( |z - w| \) is the distance from \( w \) to \( z \), and \( \text{Arg}(z - w) \) is the “direction” from \( w \) to \( z \). Thus

\[
S = \{ z \in \mathbb{C} : |z - i| \leq 3 \}
\]

is the disk centred at \( i = (0, 1) \) with radius 3.

The set

\[
T = \{ z \in \mathbb{C} : 0 \leq \text{Arg}(z - 1 + i) \leq \pi/2 \}
\]

is the set of all the points \( z \) for which the direction from \( 1 - i \) lies between 0 and \( \pi/2 \).

[For the pedants: \( 1 - i \not\in T \)]
Example: domain in the complex plane

\[ \{ z \in \mathbb{C} \mid \text{Re} \, z < 1, \text{Arg} \, (z + 1) \leq \pi/3 \} \]

\[ \{ z \in \mathbb{C} \mid 0 \leq \text{Arg} \, z \leq \pi/3 \} \]
Example: domain in the complex plane

Sketch the set \( \{ z \in \mathbb{C} \mid \text{Re}z < 1, \text{Arg}(z + 1) \leq \pi/3 \} \).
Example: domain in the complex plane

Q Sketch the set \( \{ z \in \mathbb{C} \mid \text{Re}z < 1, \text{Arg}(z + 1) \leq \pi/3 \} \).

Q Sketch the set \( \{ z \in \mathbb{C} \mid 0 \leq \text{Arg}z^3 \leq \pi/3 \} \).
Loci in the complex plane

Sketch the set \( \{ z \in \mathbb{C} | \text{Im} z = |z - i| \} \).
Q Sketch the set \( \{ z \in \mathbb{C} \mid \text{Im} z = |z - i| \} \).
Triangle inequality

The name comes from the following geometric interpretation.
Triangle inequality

\[|z + w|^2 = (z + w)(\overline{z} + \overline{w})\]
\[= (z + w)(\overline{z} + \overline{w})\]
\[= z\overline{z} + z\overline{w} + w\overline{z} + w\overline{w}\]
\[= |z|^2 + z\overline{w} + w\overline{z} + |w|^2\]
\[= |z|^2 + 2\text{Re}(z\overline{w}) + |w|^2\]
\[\leq |z|^2 + 2|z\overline{w}| + |w|^2\]
\[= (|z| + |w|)^2\]
Triangle inequality

\[ |z + w|^2 = (z + w)(\overline{z + w}) \]
\[ = (z + w)(\overline{z} + \overline{w}) \]
\[ = z\overline{z} + z\overline{w} + w\overline{z} + w\overline{w} \]
\[ = |z|^2 + z\overline{w} + \overline{z}w + |w|^2 \]
\[ = |z|^2 + 2\text{Re}(z\overline{w}) + |w|^2 \]
\[ \leq |z|^2 + 2|z\overline{w}| + |w|^2 \]
\[ = (|z| + |w|)^2 \]

Triangle Inequality

\[ |z + w| \leq |z| + |w| \]
Triangle inequality

\[ |z + w|^2 = (z + w)(\bar{z} + \bar{w}) \]
\[ = (z + w)(\bar{z} + \bar{w}) \]
\[ = z\bar{z} + z\bar{w} + \bar{z}w + \bar{w}w \]
\[ = |z|^2 + z\bar{w} + \bar{z}w + |w|^2 \]
\[ = |z|^2 + 2\text{Re}(z\bar{w}) + |w|^2 \]
\[ \leq |z|^2 + 2|z\bar{w}| + |w|^2 \]
\[ = (|z| + |w|)^2 \]

Triangle Inequality

\[ |z + w| \leq |z| + |w| \]

The name comes from the following geometric interpretation.
Complex polynomials

**Definition**
A function $p : \mathbb{C} \rightarrow \mathbb{C}$ of the form
$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$$
(with coefficients $a_n, \ldots, a_0 \in \mathbb{C}$) is called a (complex) polynomial.

The **degree** of $p$, written $\text{deg}(p)$, is the highest power with a non-zero coefficient. If $n$ above is the degree, then $a_n$ is called the **leading coefficient**.
A function $p : \mathbb{C} \to \mathbb{C}$ of the form

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$$

is called a (complex) polynomial.

The degree of $p$, written $\deg(p)$, is the highest power with a non-zero coefficient.

If $n$ above is the degree, then $a_n$ is called the leading coefficient.
Complex polynomials

Definition

A function $p : \mathbb{C} \to \mathbb{C}$ of the form

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$$

(with coefficients $a_n, \ldots, a_0 \in \mathbb{C}$) is called a (complex) polynomial.
Complex polynomials

Definition

A function \( p : \mathbb{C} \to \mathbb{C} \) of the form

\[
p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0
\]

(with coefficients \( a_n, \ldots, a_0 \in \mathbb{C} \)) is called a (complex) polynomial.
The degree of \( p \), written \( \text{deg}(p) \), is the highest power with a non-zero coefficient.
Complex polynomials

Definition

A function $p : \mathbb{C} \to \mathbb{C}$ of the form

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$$

(with coefficients $a_n, \ldots, a_0 \in \mathbb{C}$) is called a (complex) polynomial.

The degree of $p$, written $\deg(p)$, is the highest power with a non-zero coefficient. If $n$ above is the degree, then $a_n$ is called the leading coefficient.
The fundamental theorem of algebra

A root of a polynomial $p$ is any $\alpha \in \mathbb{C}$ such that $p(\alpha) = 0$.

Theorem (Gauss) Every complex polynomial of degree at least one has a root $\alpha \in \mathbb{C}$.

Note: It does not give any formula for the roots (unlike the quadratic and cubic formula).

About the proofs
You will see a proof in your 2nd year complex analysis course. There is another proof via Galois theory. Gauss himself gave several proofs, including the following below which requires algebraic topology to make rigorous.
The fundamental theorem of algebra

A (complex) root of a polynomial \( p \) is any \( \alpha \in \mathbb{C} \) such that \( p(\alpha) = 0 \).
The fundamental theorem of algebra

A (complex) root of a polynomial $p$ is any $\alpha \in \mathbb{C}$ such that $p(\alpha) = 0$.

**Theorem (Gauss)**

Every complex polynomial of degree at least one has a root $\alpha \in \mathbb{C}$. 

Note: It does not give any formula for the roots (unlike the quadratic and cubic formula).

About the proofs:
You will see a proof in your 2nd year complex analysis course.
There is another proof via Galois theory.
Gauss himself gave several proofs, including the following below which requires algebraic topology to make rigorous.
A (complex) root of a polynomial $p$ is any $\alpha \in \mathbb{C}$ such that $p(\alpha) = 0$.

**Theorem (Gauss)**

Every complex polynomial of degree at least one has a root $\alpha \in \mathbb{C}$.

**Note** It does not give any formula for the roots (unlike the quadratic and cubic formula).
A \textit{(complex) root} of a polynomial $p$ is any $\alpha \in \mathbb{C}$ such that $p(\alpha) = 0$.

**Theorem (Gauss)**

Every complex polynomial of degree at least one has a root $\alpha \in \mathbb{C}$.

**Note** It does not give any formula for the roots (unlike the quadratic and cubic formula).

**About the proofs**

- You will see a proof in your 2nd year complex analysis course.
The fundamental theorem of algebra

A \textit{(complex) root} of a polynomial \( p \) is any \( \alpha \in \mathbb{C} \) such that \( p(\alpha) = 0 \).

**Theorem (Gauss)**

Every complex polynomial of degree at least one has a root \( \alpha \in \mathbb{C} \).

\textbf{Note} It does not give any formula for the roots (unlike the quadratic and cubic formula).

\textbf{About the proofs}

- You will see a proof in your 2nd year complex analysis course.
- There is another proof via Galois theory.
The fundamental theorem of algebra

A (complex) root of a polynomial $p$ is any $\alpha \in \mathbb{C}$ such that $p(\alpha) = 0$.  

Theorem (Gauss)  
Every complex polynomial of degree at least one has a root $\alpha \in \mathbb{C}$.  

Note It does not give any formula for the roots (unlike the quadratic and cubic formula).  

About the proofs

- You will see a proof in your 2nd year complex analysis course.
- There is another proof via Galois theory.
- Gauss himself gave several proofs, including the following below which requires algebraic topology to make rigorous.
Factorising polynomials

Let $p, q$ be complex polynomials of degree at least 1. Then $q$ is a factor of $p$ if there is a polynomial $r$ such that $p = qr$. We also say $q$ divides $p$.

**Example.** $z - 1$ is a factor of $z^3 - 1$ as $z^3 - 1 = (z - 1)(z^2 + z + 1)$.

**Theorem (Remainder and Factor).** Let $p$ be a complex polynomial of degree at least one. The remainder on dividing $p$ by $z - \alpha$ is $p(\alpha)$. In particular, $z - \alpha$ is a factor of $p(z)$ if and only if $\alpha$ is a root of $p$.

**Proof.** Use the long division algorithm for polynomial division to see that $p(z) = (z - \alpha)q(z) + r$ for some polynomial $q(z)$ and remainder $r$ which is constant since its degree must be less that $\deg(z - \alpha)$.

Then $p(\alpha) = r$ which is zero precisely when $\alpha$ is a root or equivalently, $z - \alpha$ is a factor.
Let \( p, q \) be complex polynomials of degree at least 1. Then \( q \) is a factor of \( p \) if there is a polynomial \( r \) such that \( p = qr \). We also say \( q \) divides \( p \).
Factorising polynomials

Let $p, q$ be complex polynomials of degree at least 1. Then $q$ is a factor of $p$ if there is a polynomial $r$ such that $p = qr$. We also say $q$ divides $p$.

eg. $z - 1$ is a factor of $z^3 - 1$ as $z^3 - 1 = (z - 1)(z^2 + z + 1)$. 
Factorising polynomials

Let \( p, q \) be complex polynomials of degree at least 1. Then \( q \) is a factor of \( p \) if there is a polynomial \( r \) such that \( p = qr \). We also say \( q \) divides \( p \).

eg. \( z - 1 \) is a factor of \( z^3 - 1 \) as \( z^3 - 1 = (z - 1)(z^2 + z + 1) \).

**Theorem (Remainder and Factor)**

Let \( p \) be a complex polynomial of degree at least one.
Factorising polynomials

Let $p, q$ be complex polynomials of degree at least 1. Then $q$ is a factor of $p$ if there is a polynomial $r$ such that $p = qr$. We also say $q$ divides $p$.

eg. $z - 1$ is a factor of $z^3 - 1$ as $z^3 - 1 = (z - 1)(z^2 + z + 1)$.

**Theorem (Remainder and Factor)**

Let $p$ be a complex polynomial of degree at least one. The remainder on dividing $p$ by $z - \alpha$ is $p(\alpha)$.
Factorising polynomials

Let \( p, q \) be complex polynomials of degree at least 1. Then \( q \) is a factor of \( p \) if there is a polynomial \( r \) such that \( p = qr \). We also say \( q \) divides \( p \).

eg. \( z - 1 \) is a factor of \( z^3 - 1 \) as \( z^3 - 1 = (z - 1)(z^2 + z + 1) \).

Theorem (Remainder and Factor)

Let \( p \) be a complex polynomial of degree at least one. The remainder on dividing \( p \) by \( z - \alpha \) is \( p(\alpha) \). In particular, \( z - \alpha \) is a factor of \( p(z) \) if and only if \( \alpha \) is a root of \( p \).
Factorising polynomials

Let $p, q$ be complex polynomials of degree at least 1. Then $q$ is a factor of $p$ if there is a polynomial $r$ such that $p = qr$. We also say $q$ divides $p$.

eg. $z - 1$ is a factor of $z^3 - 1$ as $z^3 - 1 = (z - 1)(z^2 + z + 1)$.

**Theorem (Remainder and Factor)**

Let $p$ be a complex polynomial of degree at least one. The remainder on dividing $p$ by $z - \alpha$ is $p(\alpha)$. In particular, $z - \alpha$ is a factor of $p(z)$ if and only if $\alpha$ is a root of $p$.

**Proof.** Use the long division algorithm for polynomial division to see that

$$p(z) = (z - \alpha)q(z) + r$$
Factorising polynomials

Let \( p, q \) be complex polynomials of degree at least 1. Then \( q \) is a factor of \( p \) if there is a polynomial \( r \) such that \( p = qr \). We also say \( q \) divides \( p \).

eg. \( z - 1 \) is a factor of \( z^3 - 1 \) as \( z^3 - 1 = (z - 1)(z^2 + z + 1) \).

Theorem (Remainder and Factor)

Let \( p \) be a complex polynomial of degree at least one. The remainder on dividing \( p \) by \( z - \alpha \) is \( p(\alpha) \). In particular, \( z - \alpha \) is a factor of \( p(z) \) if and only if \( \alpha \) is a root of \( p \).

Proof. Use the long division algorithm for polynomial division to see that \( p(z) = (z - \alpha)q(z) + r \) for some polynomial \( q(z) \) and remainder \( r \) which is constant since its degree must be less that \( \deg(z - \alpha) \).
Factorising polynomials

Let $p, q$ be complex polynomials of degree at least 1. Then $q$ is a factor of $p$ if there is a polynomial $r$ such that $p = qr$. We also say $q$ divides $p$.

eg. $z - 1$ is a factor of $z^3 - 1$ as $z^3 - 1 = (z - 1)(z^2 + z + 1)$.

Theorem (Remainder and Factor)

Let $p$ be a complex polynomial of degree at least one. The remainder on dividing $p$ by $z - \alpha$ is $p(\alpha)$. In particular, $z - \alpha$ is a factor of $p(z)$ if and only if $\alpha$ is a root of $p$.

Proof. Use the long division algorithm for polynomial division to see that $p(z) = (z - \alpha)q(z) + r$ for some polynomial $q(z)$ and remainder $r$ which is constant since its degree must be less that $\deg(z - \alpha)$. Then $p(\alpha) = r$ which is zero precisely when $\alpha$ is a root or equivalently, $z - \alpha$ is a factor.
Fundamental theorem of algebra (factor form)

Putting the Factor Theorem and the Fundamental Theorem of Algebra together says that if $p$ is a polynomial of degree $n$, then there exists $\alpha_1 \in \mathbb{C}$ such that $p(z) = (z - \alpha_1)g_1(z)$, where $g_1(z)$ has degree $n - 1$.

If $n - 1 \geq 1$ then there exists $\alpha_2 \in \mathbb{C}$ such that $p(z) = (z - \alpha_1)(z - \alpha_2)g_2(z)$.

Continuing, you get

Theorem Any degree $n$ complex polynomial has a factorisation of the form $p(z) = (z - \alpha_1)(z - \alpha_2)\ldots(z - \alpha_n)c$ with $\alpha_i, c \in \mathbb{C}$.

The terms $(z - \alpha_j)$ are called linear factors of $p$.

This factorisation is unique up to swapping factors around.

E.g. Factorise $p(z) = z^3 + z^2 - 2$ into linear factors.
Putting the Factor Theorem and the Fundamental Theorem of Algebra together says that if $p$ is a polynomial of degree $n$, 

$$p(z) = (z - \alpha_1)(z - \alpha_2)\ldots(z - \alpha_n)c$$

with $\alpha_i, c \in \mathbb{C}$. The terms $(z - \alpha_j)$ are called linear factors of $p$.

This factorisation is unique up to swapping factors around.

E.g. Factorise $p(z) = z^3 + z^2 - 2$ into linear factors.
Putting the Factor Theorem and the Fundamental Theorem of Algebra together says that if $p$ is a polynomial of degree $n$, then there exists $\alpha_1 \in \mathbb{C}$ such that $p(z) = (z - \alpha_1)g_1(z)$, where $g_1(z)$ has degree $n - 1$. 

Continuing, you get

**Theorem**

Any degree $n$ complex polynomial has a factorisation of the form

$$p(z) = (z - \alpha_1)(z - \alpha_2)\ldots(z - \alpha_n)c$$

with $\alpha_i, c \in \mathbb{C}$. The terms $(z - \alpha_j)$ are called linear factors of $p$. This factorisation is unique up to swapping factors around.

E.g. Factorise $p(z) = z^3 + z^2 - 2$ into linear factors.
Putting the Factor Theorem and the Fundamental Theorem of Algebra together says that if $p$ is a polynomial of degree $n$, then there exists $\alpha_1 \in \mathbb{C}$ such that $p(z) = (z - \alpha_1)g_1(z)$, where $g_1(z)$ has degree $n - 1$.

If $n - 1 \geq 1$ then there exists $\alpha_2 \in \mathbb{C}$ such that $p(z) = (z - \alpha_1)(z - \alpha_2)g_2(z)$. 

Continuing, you get

**Theorem**

Any degree $n$ complex polynomial has a factorisation of the form $p(z) = (z - \alpha_1)(z - \alpha_2)...(z - \alpha_n)c$ with $\alpha_i, c \in \mathbb{C}$.

The terms $(z - \alpha_j)$ are called linear factors of $p$.

This factorisation is unique up to swapping factors around.

E.g. Factorise $p(z) = z^3 + z^2 - 2$ into linear factors.
Putting the Factor Theorem and the Fundamental Theorem of Algebra together says that if \( p \) is a polynomial of degree \( n \), then there exists \( \alpha_1 \in \mathbb{C} \) such that \( p(z) = (z - \alpha_1)g_1(z) \), where \( g_1(z) \) has degree \( n - 1 \).

If \( n - 1 \geq 1 \) then there exists \( \alpha_2 \in \mathbb{C} \) such that \( p(z) = (z - \alpha_1)(z - \alpha_2)g_2(z) \).

Continuing, you get

**Theorem**

Any degree \( n \) complex polynomial has a factorisation of the form

\[
p(z) = (z - \alpha_1)(z - \alpha_2)\ldots(z - \alpha_n)c
\]

with \( \alpha_i, c \in \mathbb{C} \).
Putting the Factor Theorem and the Fundamental Theorem of Algebra together says that if \( p \) is a polynomial of degree \( n \), then there exists \( \alpha_1 \in \mathbb{C} \) such that 
\[
p(z) = (z - \alpha_1)g_1(z),
\]
where \( g_1(z) \) has degree \( n - 1 \).

If \( n - 1 \geq 1 \) then there exists \( \alpha_2 \in \mathbb{C} \) such that 
\[
p(z) = (z - \alpha_1)(z - \alpha_2)g_2(z).
\]
Continuing, you get

**Theorem**

Any degree \( n \) complex polynomial has a factorisation of the form

\[
p(z) = (z - \alpha_1)(z - \alpha_2)\ldots(z - \alpha_n)c
\]

with \( \alpha_i, c \in \mathbb{C} \). The terms \( (z - \alpha_j) \) are called *linear factors* of \( p \).
Putting the Factor Theorem and the Fundamental Theorem of Algebra together says that if \( p \) is a polynomial of degree \( n \), then there exists \( \alpha_1 \in \mathbb{C} \) such that \( p(z) = (z - \alpha_1)g_1(z) \), where \( g_1(z) \) has degree \( n - 1 \).

If \( n - 1 \geq 1 \) then there exists \( \alpha_2 \in \mathbb{C} \) such that \( p(z) = (z - \alpha_1)(z - \alpha_2)g_2(z) \). Continuing, you get

### Theorem

Any degree \( n \) complex polynomial has a factorisation of the form

\[
p(z) = (z - \alpha_1)(z - \alpha_2) \ldots (z - \alpha_n)c
\]

with \( \alpha_i, c \in \mathbb{C} \). The terms \( (z - \alpha_j) \) are called **linear factors** of \( p \). This factorisation is unique up to swapping factors around.
Putting the Factor Theorem and the Fundamental Theorem of Algebra together says that if $p$ is a polynomial of degree $n$, then there exists $\alpha_1 \in \mathbb{C}$ such that $p(z) = (z - \alpha_1)g_1(z)$, where $g_1(z)$ has degree $n - 1$.

If $n - 1 \geq 1$ then there exists $\alpha_2 \in \mathbb{C}$ such that $p(z) = (z - \alpha_1)(z - \alpha_2)g_2(z)$. Continuing, you get

**Theorem**

Any degree $n$ complex polynomial has a factorisation of the form

$$p(z) = (z - \alpha_1)(z - \alpha_2)\ldots(z - \alpha_n)c$$

with $\alpha_i, c \in \mathbb{C}$. The terms $(z - \alpha_j)$ are called *linear factors* of $p$. This factorisation is unique up to swapping factors around.

**E.g.** Factorise $p(z) = z^3 + z^2 - 2$ into linear factors.
In an example like \( p(z) = (z-3)^4(z-i)^2(z+1) \) where the linear factors are not distinct, we say that \( (z-3) \) is a factor of multiplicity 4, and that 3 is a root of multiplicity 4. Similarly, \( i \) is a root of multiplicity 2 and -1 is a root of multiplicity 1.

Find all cubic polynomials which have 2 as a root of multiplicity 3.
In an example like

\[ p(z) = (z - 3)^4(z - i)^2(z + 1) \]

where the linear factors are not distinct,

where the linear factors are not distinct,
In an example like

\[ p(z) = (z - 3)^4(z - i)^2(z + 1) \]

where the linear factors are not distinct, we say that \((z - 3)\) is a factor of \textit{multiplicity} 4, and that 3 is a \textit{root of multiplicity} 4.

Similarly, \(i\) is a root of multiplicity 2 and -1 is a root of multiplicity 1.
In an example like
\[ p(z) = (z - 3)^4(z - i)^2(z + 1) \]
where the linear factors are not distinct, we say that \((z - 3)\) is a factor of \textit{multiplicity} 4, and that 3 is a \textit{root of multiplicity} 4.
Similarly, \(i\) is a root of multiplicity 2 and -1 is a root of multiplicity 1.
In an example like

\[ p(z) = (z - 3)^4(z - i)^2(z + 1) \]

where the linear factors are not distinct, we say that \((z - 3)\) is a factor of multiplicity 4, and that 3 is a root of multiplicity 4. Similarly, \(i\) is a root of multiplicity 2 and \(-1\) is a root of multiplicity 1.

**Q** Find all cubic polynomials which have 2 as a root of multiplicity 3.
Proof of uniqueness of factorisation

Consider two factorisations

\[ p(z) = (z - \alpha_1)(z - \alpha_2)\ldots(z - \alpha_n) \]

\[ c = (z - \beta_1)(z - \beta_2)\ldots(z - \beta_n) \] \hspace{1cm} (1)

We need to show that we can re-order the \( \beta_i \)'s so that \( \alpha_1 = \beta_1,\ldots,\alpha_n = \beta_n, c = d \).

First note \( c = d \) since they are both the leading co-efficient of \( p \).

We argue by induction on \( n \). The case \( n = 0 \) already has been verified so assume \( n > 0 \).

Substitute in \( z = \alpha_1 \) to obtain

\[ 0 = (\alpha_1 - \beta_1)(\alpha_1 - \beta_2)\ldots(\alpha_1 - \beta_n) \]

One of the RHS factors, say \( \alpha_1 - \beta_i = 0 \).

Swap \( \beta_i, \beta_1 \) so \( \alpha_1 = \beta_1 \).

Dividing (1) by \( z - \alpha_1 \) gives 2 factorisations of \( p(z) \)

\[ z - \alpha_1 = (z - \alpha_2)\ldots(z - \alpha_n) \]

\[ c = (z - \beta_2)\ldots(z - \beta_n) \]

By induction, we may assume also \( \alpha_2 = \beta_2,\ldots,\alpha_n = \beta_n, c = d \), so we've won.
Proof of uniqueness of factorisation

Consider two factorisations

\[ p(z) = (z - \alpha_1)(z - \alpha_2) \ldots (z - \alpha_n) c = (z - \beta_1)(z - \beta_2) \ldots (z - \beta_n) d. \quad (1) \]
Proof of uniqueness of factorisation

Consider two factorisations

\[ p(z) = (z - \alpha_1)(z - \alpha_2) \ldots (z - \alpha_n) c = (z - \beta_1)(z - \beta_2) \ldots (z - \beta_n) d. \quad (1) \]

We need to show that we can re-order the \( \beta_i \)'s so that

\[ \alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n, c = d. \]
Proof of uniqueness of factorisation

Consider two factorisations

\[ p(z) = (z - \alpha_1)(z - \alpha_2) \ldots (z - \alpha_n)c = (z - \beta_1)(z - \beta_2) \ldots (z - \beta_n)d. \quad (1) \]

We need to show that we can re-order the \( \beta_i \)'s so that
\[ \alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n, c = d. \]
First note \( c = d \) since they are both the leading co-efficient of \( p \).
Proof of uniqueness of factorisation

Consider two factorisations

\[ p(z) = (z - \alpha_1)(z - \alpha_2) \ldots (z - \alpha_n) \]
\[ \quad = (z - \beta_1)(z - \beta_2) \ldots (z - \beta_n) \]  \hspace{1cm} (1)

We need to show that we can re-order the \( \beta_i \)'s so that
\[ \alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n, c = d. \] First note \( c = d \) since they are both the leading co-efficient of \( p \).

We argue by induction on \( n \). The case \( n = 0 \) already has been verified so assume \( n > 0 \).
Proof of uniqueness of factorisation

Consider two factorisations

\[ p(z) = (z - \alpha_1)(z - \alpha_2) \ldots (z - \alpha_n) \]
\[ \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad c = (z - \beta_1)(z - \beta_2) \ldots (z - \beta_n) \]

(1)

We need to show that we can re-order the \( \beta_i \)'s so that
\[ \alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n, c = d. \]

First note \( c = d \) since they are both the leading co-efficient of \( p \).

We argue by induction on \( n \). The case \( n = 0 \) already has been verified so assume \( n > 0 \). Substitute in \( z = \alpha_1 \) to obtain

\[ 0 = (\alpha_1 - \beta_1)(\alpha_1 - \beta_2) \ldots (\alpha_1 - \beta_n)d. \]
Proof of uniqueness of factorisation

Consider two factorisations

\[ p(z) = (z - \alpha_1)(z - \alpha_2) \ldots (z - \alpha_n) c = (z - \beta_1)(z - \beta_2) \ldots (z - \beta_n) d. \]  \hspace{1cm} (1)

We need to show that we can re-order the \( \beta_i \)'s so that
\[ \alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n, c = d. \]

First note \( c = d \) since they are both the leading co-efficient of \( p \).

We argue by induction on \( n \). The case \( n = 0 \) already has been verified so assume \( n > 0 \). Substitute in \( z = \alpha_1 \) to obtain

\[ 0 = (\alpha_1 - \beta_1)(\alpha_1 - \beta_2) \ldots (\alpha_1 - \beta_n)d. \]

One of the RHS factors, say \( \alpha_1 - \beta_i = 0 \).
Proof of uniqueness of factorisation

Consider two factorisations

\[ p(z) = (z - \alpha_1)(z - \alpha_2) \ldots (z - \alpha_n) \quad c = (z - \beta_1)(z - \beta_2) \ldots (z - \beta_n) d. \tag{1} \]

We need to show that we can re-order the \( \beta_i \)'s so that
\[ \alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n, c = d. \]
First note \( c = d \) since they are both the leading co-efficient of \( p \).

We argue by induction on \( n \). The case \( n = 0 \) already has been verified so assume \( n > 0 \). Substitute in \( z = \alpha_1 \) to obtain

\[ 0 = (\alpha_1 - \beta_1)(\alpha_1 - \beta_2) \ldots (\alpha_1 - \beta_n)d. \]

One of the RHS factors, say \( \alpha_1 - \beta_i = 0 \). Swap \( \beta_i, \beta_1 \) so \( \alpha_1 = \beta_1 \).
Proof of uniqueness of factorisation

Consider two factorisations

\[ p(z) = (z - \alpha_1)(z - \alpha_2) \ldots (z - \alpha_n) \]
\[ \quad c = (z - \beta_1)(z - \beta_2) \ldots (z - \beta_n) \]  
\[ d. \quad (1) \]

We need to show that we can re-order the \( \beta_i \)'s so that
\[ \alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n, \quad c = d. \]
First note \( c = d \) since they are both the leading co-efficient of \( p \).

We argue by induction on \( n \). The case \( n = 0 \) already has been verified so assume \( n > 0 \). Substitute in \( z = \alpha_1 \) to obtain

\[ 0 = (\alpha_1 - \beta_1)(\alpha_1 - \beta_2) \ldots (\alpha_1 - \beta_n)d. \]

One of the RHS factors, say \( \alpha_1 - \beta_i = 0 \). Swap \( \beta_i, \beta_1 \) so \( \alpha_1 = \beta_1 \).

Dividing (1) by \( z - \alpha_1 \) gives 2 factorisations of

\[ \frac{p(z)}{z - \alpha_1} = (z - \alpha_2) \ldots (z - \alpha_n) \quad c = (z - \beta_2) \ldots (z - \beta_n) d. \]
Proof of uniqueness of factorisation

Consider two factorisations

\[ p(z) = (z - \alpha_1)(z - \alpha_2) \ldots (z - \alpha_n)c = (z - \beta_1)(z - \beta_2) \ldots (z - \beta_n)d. \quad (1) \]

We need to show that we can re-order the \( \beta_i \)'s so that
\[ \alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n, c = d. \]

First note \( c = d \) since they are both the leading co-efficient of \( p \).

We argue by induction on \( n \). The case \( n = 0 \) already has been verified so assume \( n > 0 \). Substitute in \( z = \alpha_1 \) to obtain

\[ 0 = (\alpha_1 - \beta_1)(\alpha_1 - \beta_2) \ldots (\alpha_1 - \beta_n)d. \]

One of the RHS factors, say \( \alpha_1 - \beta_i = 0 \). Swap \( \beta_i, \beta_1 \) so \( \alpha_1 = \beta_1 \).

Dividing (1) by \( z - \alpha_1 \) gives 2 factorisations of

\[ \frac{p(z)}{z - \alpha_1} = (z - \alpha_2) \ldots (z - \alpha_n)c = (z - \beta_2) \ldots (z - \beta_n)d. \]

By induction, we may assume also \( \alpha_2 = \beta_2, \ldots, \alpha_n = \beta_n, c = d \), so we’ve won.
Example: factorisation

E.g. Write $p(z) = z^4 + 1$ as a product of linear factors.

N.B. Here, the complex roots occur in complex conjugate pairs. This is a general phenomena for real polynomials.
**Example: factorisation**

**E.g** Write \( p(z) = z^4 + 1 \) as a product of linear factors.
Example: factorisation

**E.g** Write \( p(z) = z^4 + 1 \) as a product of linear factors.

**N.B.** Here, the complex roots occur in complex conjugate pairs. This is general phenomena for *real* polynomials.
A polynomial is real if the co-efficients are real.

**Theorem**

Suppose that $\alpha$ is a root of a real polynomial $p$. Then $\alpha$ is also a root of $p$.

**Proof.**

Note that in such a case $(z - \alpha)$ and $(z - \alpha)$ are both factors. If $\alpha \not\in \mathbb{R}$, then unique factorisation $\Rightarrow p(z)$ has a quadratic factor $(z - \alpha)(z - \alpha) = z^2 - (2\text{Re}\alpha)z + |\alpha|^2$, which is a real quadratic.
Roots of real polynomials

A polynomial is real if the co-efficients are real.
Roots of real polynomials

A polynomial is *real* if the co-efficients are real.

**Theorem**

Suppose that $\alpha$ is a root of a real polynomial $p$. Then $\overline{\alpha}$ is also a root of $p$.

Proof.

Note that in such a case, $(z - \alpha)$ and $(z - \alpha)$ are both factors. If $\alpha \not\in \mathbb{R}$, then unique factorisation $\implies p(z)$ has a quadratic factor $(z - \alpha)(z - \alpha) = z^2 - (\alpha + \alpha)z + \alpha \alpha = z^2 - (2 \text{Re} \alpha)z + |\alpha|^2$, which is a real quadratic.
Roots of real polynomials

A polynomial is *real* if the co-efficients are real.

**Theorem**

Suppose that \( \alpha \) is a root of a real polynomial \( p \). Then \( \overline{\alpha} \) is also a root of \( p \).

**Proof.**
A polynomial is *real* if the co-efficients are real.

**Theorem**

Suppose that \( \alpha \) is a root of a real polynomial \( p \). Then \( \bar{\alpha} \) is also a root of \( p \).

**Proof.**

Note that in such a case \((z - \alpha)\) and \((z - \bar{\alpha})\) are both factors.
A polynomial is *real* if the co-efficients are real.

**Theorem**

Suppose that $\alpha$ is a root of a real polynomial $p$. Then $\overline{\alpha}$ is also a root of $p$.

**Proof.**

Note that in such a case $(z - \alpha)$ and $(z - \overline{\alpha})$ are both factors. If $\alpha \notin \mathbb{R}$, then unique factorisation $\implies p(z)$ has a quadratic factor

$$(z - \alpha)(z - \overline{\alpha}) = z^2 - (\alpha + \overline{\alpha})z + \alpha \overline{\alpha}
= z^2 - (2\Re \alpha)z + |\alpha|^2.$$
A polynomial is *real* if the co-efficients are real.

**Theorem**

Suppose that $\alpha$ is a root of a real polynomial $p$. Then $\overline{\alpha}$ is also a root of $p$.

**Proof.**

Note that in such a case $(z - \alpha)$ and $(z - \overline{\alpha})$ are both factors. If $\alpha \notin \mathbb{R}$, then unique factorisation $\implies p(z)$ has a quadratic factor

$$(z - \alpha)(z - \overline{\alpha}) = z^2 - (\alpha + \overline{\alpha})z + \alpha\overline{\alpha}$$

$$= z^2 - (2\text{Re}\alpha)z + |\alpha|^2.$$

which is a real quadratic.
Factorising real polynomials

We say a real polynomial $p$ is irreducible over the reals if it can't be factored into a product of two real polynomials of positive degree.

E.g. $z^2 - 3z + 2$ is not irreducible but $z^2 + 1$ is.

Why?

Upshot

A real quadratic polynomial is irreducible over $\mathbb{R}$ iff it has non-real roots.

Using the the fundamental thm of algebra and the previous slide (and our old inductive argument) we see

Theorem

Any real polynomial can be factored into a product of real linear and real irreducible quadratic polynomials.
We say a real polynomial $p$ is *irreducible over the reals* if it can’t be factored into a product of two real polynomials of positive degree.

**Example:**
- $z^2 - 3z + 2$ is not irreducible but $z^2 + 1$ is.

**Upshot:** A real quadratic polynomial is irreducible over $\mathbb{R}$ iff it has non-real roots.

**Theorem:** Any real polynomial can be factored into a product of real linear and real irreducible quadratic polynomials.
We say a real polynomial $p$ is *irreducible over the reals* if it can’t be factored into a product of two real polynomials of positive degree.

**E.g.** $z^2 - 3z + 2$ is not irreducible but $z^2 + 1$ is.
We say a real polynomial $p$ is *irreducible over the reals* if it can’t be factored into a product of two real polynomials of positive degree.

**E.g.** $z^2 - 3z + 2$ is not irreducible but $z^2 + 1$ is.

**Why?**
We say a real polynomial $p$ is *irreducible over the reals* if it can't be factored into a product of two real polynomials of positive degree.

**E.g.** $z^2 - 3z + 2$ is not irreducible but $z^2 + 1$ is.

**Why?**

**Upshot** A real quadratic polynomial is irreducible over $\mathbb{R}$ iff it has non-real roots.
Factorising real polynomials

We say a real polynomial $p$ is *irreducible over the reals* if it can’t be factored into a product of two real polynomials of positive degree.

**E.g.** $z^2 - 3z + 2$ is not irreducible but $z^2 + 1$ is.

**Why?**

**Upshot** A real quadratic polynomial is irreducible over $\mathbb{R}$ iff it has non-real roots. Using the fundamental thm of algebra and the previous slide (and our old inductive argument) we see
We say a real polynomial $p$ is *irreducible over the reals* if it can’t be factored into a product of two real polynomials of positive degree.

**E.g.** $z^2 - 3z + 2$ is not irreducible but $z^2 + 1$ is.

**Why?**

**Upshot** A real quadratic polynomial is irreducible over $\mathbb{R}$ iff it has non-real roots. Using the fundamental theorem of algebra and the previous slide (and our old inductive argument) we see

**Theorem**

Any real polynomial can be factored into a product of real linear and real irreducible quadratic polynomials.
Example: factorisation of a real polynomial

Factorise $p(z) = z^6 - 1$ into real irreducible factors.

**Method 1**
Just try your luck with factorisation facts you know

$$z^6 - 1 = (z^2 - 1)(z^4 + z^2 + 1) = (z - 1)(z + 1)(z^2 + 1)(z^2 - 1)$$

**Method 2**
Factorise into complex linear factors first.

**Remark**
This is the first instance of common technique in mathematics, to answer a question involving real numbers, first answer it over the complex numbers and deduce your result accordingly.
Example: factorisation of a real polynomial

Q Factorise $p(z) = z^6 - 1$ into real irreducible factors.
Example: factorisation of a real polynomial

Q Factorise $p(z) = z^6 - 1$ into real irreducible factors.

**Method 1** Just try your luck with factorisation facts you know

\[
z^6 - 1 = (z^2 - 1)(z^4 + z^2 + 1) = (z - 1)(z + 1)((z^2 + 1)^2 - z^2) = (z - 1)(z + 1)(z^2 + z + 1)(z^2 - z + 1)
\]
Example: factorisation of a real polynomial

Q Factorise $p(z) = z^6 - 1$ into real irreducible factors.

Method 1 Just try your luck with factorisation facts you know

\[ z^6 - 1 = (z^2 - 1)(z^4 + z^2 + 1) = (z - 1)(z + 1)((z^2 + 1)^2 - z^2) = (z - 1)(z + 1)(z^2 + z + 1)(z^2 - z + 1) \]

OR Method 2 Factorise into complex linear factors first.
Example: factorisation of a real polynomial

Q Factorise \( p(z) = z^6 - 1 \) into real irreducible factors.

Method 1 Just try your luck with factorisation facts you know

\[
z^6 - 1 = (z^2 - 1)(z^4 + z^2 + 1) = (z - 1)(z + 1)((z^2 + 1)^2 - z^2) = (z - 1)(z + 1)(z^2 + z + 1)(z^2 - z + 1)
\]

OR Method 2 Factorise into complex linear factors first.

Remark This is the first instance of common technique in mathematics, to answer a question involving real numbers, first answer it over the complex numbers and deduce your result accordingly.
Sums and products of roots

Formula

Consider a degree \( n \) polynomial \( p(z) = a_0 + a_1 z + \ldots + a_n z^n \). Let \( \alpha_1, \ldots, \alpha_n \) be its roots (listed with multiplicity). Then

\[
\sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n}, \quad \prod_{i=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}.
\]

Why?

For example when \( n = 3 \), just expand

\[a_n(z - \alpha_1)(z - \alpha_2)(z - \alpha_3) = E \text{g} \]

Any real cubic of form

\[x^3 + a_2 x^2 + a_1 x - 1 \]

has a positive real root

Challenge Q

Express

\[\sum_{i=1}^{n} \alpha_i^2 \]

in terms of the coefficients.
Sums and products of roots

**Formula**

Consider a degree $n$ polynomial $p(z) = a_0 + a_1 z + \ldots + a_n z^n$. Let $\alpha_1, \ldots, \alpha_n$ be its roots (listed with multiplicity). Then

$$\sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n}, \quad \prod_{i=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}.$$  

**Why?** For example when $n = 3$, just expand

$$a_n(z - \alpha_1)(z - \alpha_2)(z - \alpha_3) =$$
Consider a degree \( n \) polynomial \( p(z) = a_0 + a_1 z + \ldots + a_n z^n \). Let \( \alpha_1, \ldots, \alpha_n \) be its roots (listed with multiplicity). Then

\[
\sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n}, \quad \prod_{i=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}.
\]

**Why?** For example when \( n = 3 \), just expand

\[a_n(z - \alpha_1)(z - \alpha_2)(z - \alpha_3) = \]

**Eg** Any real cubic of form \( x^3 + a_2 x^2 + a_1 x - 1 \) has a positive real root
Sums and products of roots

**Formula**

Consider a degree $n$ polynomial $p(z) = a_0 + a_1z + \ldots + a_nz^n$. Let $\alpha_1, \ldots, \alpha_n$ be its roots (listed with multiplicity). Then

$$
\sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n}, \quad \prod_{i=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}.
$$

**Why?** For example when $n = 3$, just expand

$$
a_n(z - \alpha_1)(z - \alpha_2)(z - \alpha_3) =
$$

**Eg** Any real cubic of form $x^3 + a_2x^2 + a_1x - 1$ has a positive real root

**Challenge Q** Express $\sum_i \alpha_i^2$ in terms of the co-efficients.