Where are definitions coming from?

Example. We use **integers** every day and apply operations like addition without even thinking. But let's slow down and examine what's really happening when we do something familiar.

• It takes no time to compute $57 + 39 + 71$, just observe that
$57 + 39 + 71 = 57 + (39 + 71) = 57 + 110 = 167$.

The underlying property that makes this possible is called *associativity*:

$(a + b) + c = a + (b + c)$ for any integers a, b, c.

• There's also one special integer that plays a unique role: 0. It's an integer which is neutral with respect to addition. It's called the *additive identity* because adding it to any integer leaves the number unchanged: $a + 0 = 0 + a = a$.

• Each integer also has its *inverse*, or opposite – a number that cancels it out:
$a + (-a) = (-a) + a = 0$.

Not only integers

As we've seen, addition of integers has the following properties:

• Associativity: $(a + b) + c = a + (b + c)$ for all integers a, b, c
• Identity element: There exists a neutral element 0 such that $a + 0 = 0 + a = a$
• Inverses: Every integer a has an additive inverse $-a$ such that $a + (-a) = 0$

These properties are not unique to addition of integers.
Other sets with other operations may share the same structure.

Example. The set $\mathbb{R} \setminus \{0\}$ (nonzero real numbers) under multiplication.

• Associativity: $(ab)c = a(bc)$ for all $a, b, c \in \mathbb{R} \setminus \{0\}$
• Identity element: The number 1 acts as the neutral element for multiplication:
$1 \cdot a = a \cdot 1 = a$ for any $a \in \mathbb{R} \setminus \{0\}$
• Inverses: Every nonzero real number a has a multiplicative inverse $\frac{1}{a}$: $a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$

Don't take properties for granted

• Not all operations are associative.

For example, neither subtraction nor division is associative:

$$\underbrace{(3-2)-1}_{0} \neq \underbrace{3-(2-1)}_{2}, \quad \underbrace{(6\div 3)\div 2}_{1} \neq \underbrace{6\div(3\div 2)}_{4}.$$

• A set may lack an identity element.

For example, the set $\mathbb{N} = \{1, 2, 3, \dots\}$ of natural numbers (positive integers) does not include an additive identity: 0 is missing.

• Not every element in a set is necessarily invertible.

For example, 0 has no multiplicative inverse in the set of real numbers $\mathbb{R}$.

Invertible matrices

Many sets with an operation share the same three key properties:
associativity, an identity element, and inverses.

Example 1. Consider the set $GL(n, \mathbb{R})$ of invertible $n \times n$ matrices with real entries, under matrix multiplication.

• Associativity: Matrix multiplication is associative:
$(AB)C = A(BC)$ for all $A, B, C \in GL(n, \mathbb{R})$.

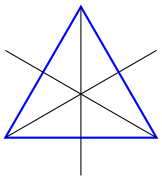
• Identity element: The identity matrix I acts as the neutral element: $AI = IA = A$ for any $A \in GL(n, \mathbb{R})$.

• Inverses: Every matrix $A \in GL(n, \mathbb{R})$ has an inverse $A^{-1} \in GL(n, \mathbb{R})$ such that $AA^{-1} = A^{-1}A = I$.

Notice how this example is very different from the previous ones:
Here we are working with matrices under multiplication,
not numbers under addition or multiplication. Yet, the same three properties hold.

Symmetries of triangle

Example 2. Consider an equilateral triangle and all of its **symmetries**. There are exactly six symmetries:
– three clockwise **rotations** by $120°$, $240°$, $360°$ (which is the identity transformation, or rotation by $0°$),
– and three **reflections**, each across a line of symmetry through a vertex and the midpoint of the opposite side.



The **composition** of any two of these symmetries is again a symmetry (you can verify this). We say that the set of symmetries is *closed* under composition.

The fact that every symmetry of the triangle is one of these six or a composition of them requires proof.

Now observe the familiar structure:

- Associativity: Composition of symmetries is associative, just like any composition of functions.
- Identity element: The identity transformation (rotation by $0°$) acts as a neutral element.
- Inverses: Every symmetry has an inverse that undoes its effect.

5 / 19

Group them all!

The properties we've seen in various sets with operations – namely:

- Associativity
- Existence of an identity element (a neutral element for the operation)
- Existence of inverses for all elements

– are surprisingly common.

It's natural, then, to group all such sets under a single mathematical concept.

This leads to the definition of a *group*.

6 / 19

Definition of a group

Definition. A *group* $(G, *)$ is a set G equipped with an operation $*$, satisfying the following properties:

- **Closure**: G is **closed** with respect to $*$. That is, for all $a, b \in G$, the result $a * b \in G$.
- **Associativity**: $*$ is **associative**: $(a * b) * c = a * (b * c)$ for any $a, b, c \in G$.
- **Identity element**: There exists an element $e \in G$ such that $a * e = e * a = a$ for any $a \in G$. It is called the *identity element*.
- **Inverses**: For any $a \in G$, there exists its *inverse* a^{-1} such that $a * a^{-1} = a^{-1} * a = e$.

These four conditions are known as the **group axioms**.

- **Commutativity** (optional): If, additionally, $*$ satisfies $a * b = b * a$ for any $a, b \in G$, then G is called a *commutative* (or *abelian*) group.

7 / 19

Examples of groups

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are all **abelian groups**. In each case:
- the group operation $*$ is $+$ (addition),
- the identity element e is 0,
- the inverse of an element a is its opposite, $-a$.

The inverse element axiom, $\forall a \in G \ \exists\, a^{-1}$ such that $a * a^{-1} = a^{-1} * a = e$, takes the form: $\forall a \ \exists (-a)$ such that $a + (-a) = (-a) + a = 0$.

2. $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$ are also **abelian groups** but with multiplication as the operation. Here, the identity element is 1, and the inverse of a is $\frac{1}{a}$.

3. The *general linear group* $GL(n, \mathbb{R})$. This is the set of all invertible $n \times n$ matrices with real entries, using matrix multiplication as the operation.

4. The *symmetry group* of an equilateral triangle, denoted by D_3, and called *dihedral group of order* 6. It consists of all rotations and reflections that map the triangle onto itself.

5. The group $(\mathbb{Z}_n, +)$ of **integers modulo** n, using using addition modulo n. We will study this in more detail later in the course.

8 / 19

How to use the definition of a group

Let us see how the definition of a group is used in the proof of a theorem.

Theorem. In any group G, the identity element is unique.

Proof. Let us assume that there are two identity elements, e and e'. We need to prove that $e = e'$.

Since e is an identity, we have $a * e = a$ for any $a \in G$.
Let's take e' as a. Then $e' * e = e'$.

On the other hand, e' is also an identity, that is $e' * b = b$ for any $b \in G$. Let's take e as b. Then $e' * e = e$.

Therefore, $e = e'$ since both are equal to $e' * e$.

We obtained that any two identity elements are equal. Therefore, the identity element is unique, as required.

9 / 19

Definition of ring

Definition. A *ring* R is a set with two operations, addition and multiplication, denoted by $+$ and $\cdot$, satisfying the following properties:

1. $\forall\, a, b \in R \quad a + b \in R$ (R is **closed** with respect to $+$)
2. $\forall\, a, b \in R \quad a \cdot b \in R$ (R is **closed** with respect to $\cdot$)
3. $\forall\, a, b, c \in R \quad (a + b) + c = a + (b + c)$ ($+$ is **associative**)
4. $\forall\, a, b \in R \quad a + b = b + a$ ($+$ is **commutative**)
5. $\exists\, 0 \in R \quad \forall\, a \in R \quad a + 0 = a$ (there exists an **additive identity** in R)
6. $\forall\, a \in R \;\; \exists\, -a \in R \;\; a + (-a) = 0$ (each element in R has an **additive inverse**)
7. $\forall\, a, b, c \in R \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$ ($\cdot$ is **associative**)
8. $\forall\, a, b, c \in R \quad a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$
(multiplication **distributes** over addition)

• If, additionally, $\forall\, a, b \in R \quad a \cdot b = b \cdot a$ ($\cdot$ is **commutative**),
then R is called a *commutative* ring.

• If, additionally, $\exists\, 1 \in R \quad \forall\, a \in R \quad 1 \cdot a = a \cdot 1 = a$
(there exists a **multiplicative identity**), then R is called a ring with *unity*.

The properties are called the *axioms* of a ring.

10 / 19

Examples of rings

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are commutative rings with unity.

2. $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ is a ring of even integers (Commutative? With unity?)

3. $\mathbb{Z}[x]$, polynomials in variable x with integer coefficients, form a ring. (Commutative? With unity?)

4. $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{Z}[x, y]$, etc. are rings of polynomials.

5. $M_n(R)$, square $n \times n$ matrices with coefficients from a ring R form a ring. (Commutative? With unity?)

6. $\mathbb{Z}/m$, residues modulo m (to be discussed later in the course) form a ring.

7. $\mathcal{F} = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$, real valued functions with the operations of addition $(f + g)(x) = f(x) + g(x)$ and multiplication $(f \cdot g)(x) = f(x) \cdot g(x)$ form a ring.

Important: To prove that each of the listed above objects is a ring, we have to verify all ring axioms.

How to use the definition of ring

Let us see how the definition of ring is used in the proof of a theorem.

Theorem. In any ring R, $a \cdot 0 = 0$ for all $a \in R$.

Proof.

$a \cdot 0 = a \cdot 0 + 0$ by axiom **5** ($a + 0 = a$)

$= a \cdot 0 + (a + (-a)) \cdot 0)$ by axiom **6** $(a + (-a) = 0)$

$= a \cdot 0 + a \cdot 0 + (-a) \cdot 0$ by axiom **8** distributiivity

$= (a \cdot 0 + a \cdot 0) + (-a \cdot 0)$ by axiom **3**

$= a \cdot (0 + 0) + (-a \cdot 0)$ by axiom **8** associativity

$= a \cdot 0 + (-a \cdot 0)$ by axiom **5**

$= 0$ by axiom **6**

Definition of limit

Definition. Let $f(x)$ be a function, a and L be real numbers.
L is called a *limit* of f as x approaches a if

$$\forall\, \varepsilon > 0 \quad \exists\, \delta > 0 \quad \forall\, x \qquad 0 < |x - a| < \delta \implies |f(x) - L| < \varepsilon\,.$$

Notations: $L = \lim\limits_{x \to a} f(x)$ or $f(x) \underset{x \to a}{\longrightarrow} L$.

Why does this definition appear to be difficult?

– Unknown letters: ε, δ from **Greek alphabet**:

$\alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon,\ \zeta,\ \eta,\ \theta,\ \iota,\ \kappa,\ \lambda,\ \mu,\ \nu,\ \xi,\ o,\ \pi,\ \rho,\ \sigma,\ \tau,\ \upsilon,\ \varphi,\ \chi,\ \psi,\ \omega$
$\mathrm{A},\ \mathrm{B},\ \Gamma,\ \Delta,\ \mathrm{E},\ \mathrm{Z},\ \mathrm{H},\ \Theta,\ \mathrm{I},\ \mathrm{K},\ \Lambda,\ \mathrm{M},\ \mathrm{N},\ \Xi,\ \mathrm{O},\ \Pi,\ \mathrm{P},\ \Sigma,\ \mathrm{T},\ \Upsilon,\ \Phi,\ \mathrm{X},\ \Psi,\ \Omega$

– Three quantifiers

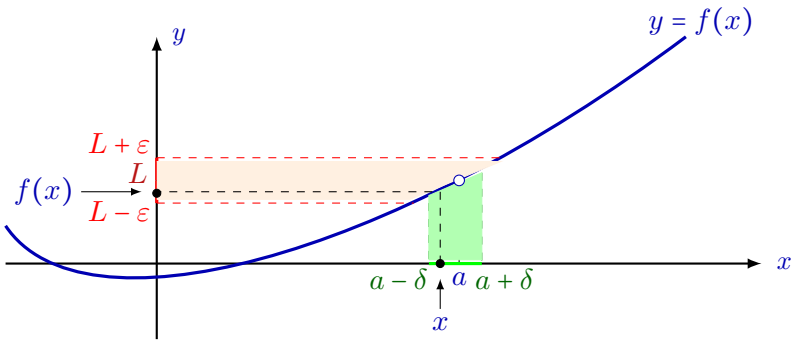
– Two inequalities

– One implication

Understanding the definition of limit

How to understand what **exactly** the definition says?

$$L = \lim_{x \to a} f(x) \;:=\; \forall\, \varepsilon > 0 \quad \exists\, \delta > 0 \quad \forall\, x \qquad 0 < |x - a| < \delta \implies |f(x) - L| < \varepsilon\,.$$



For any x such that $x \in (a - \delta, a + \delta)$, we have $f(x) \in (L - \varepsilon, L + \varepsilon)$.

Limit by definition

Exercise. Use the definition of limit to prove that $\lim\limits_{x\to 3}(2x+1)=7$.

Solution. We have to use the following definition:

$$L=\lim_{x\to a} f(x) \iff \forall\,\varepsilon>0 \quad \exists\,\delta>0 \quad \forall\, x \qquad 0<|x-a|<\delta \implies |f(x)-L|<\varepsilon.$$

In our case, $f(x)=2x+1$, $\quad a=3 \quad$ and $\quad L=7$. What is required?

For **any** given positive number ε, we need to find some positive number δ (δ is expected to depend on ε), such that we'll get $|(2x+1)-7|<\varepsilon$ for **all** x for which $0<|x-3|<\delta$.

Let's see for which x is the inequality $|(2x+1)-7|<\varepsilon$ satisfied.

$$|(2x+1)-7|<\varepsilon \iff |2x-6|<\varepsilon \iff 2|x-3|<\varepsilon \iff |x-3|<\frac{\varepsilon}{2}.$$

Therefore, the condition $|x-3|<\frac{\varepsilon}{2}$ will ensure the inequality $|(2x+1)-7|<\varepsilon$.

A number δ which we are looking for, is, therefore, $\delta=\frac{\varepsilon}{2}$.

15 / 19

Limit by definition

Let's write our reasoning in a form suitable to be a proof of the fact

$$\lim_{x\to 3}(2x+1)=7.$$

For **any** $\varepsilon>0$, there exists δ, namely $\delta=\frac{\varepsilon}{2}$, such that if $|x-3|<\delta$,

then $|(2x+1)-7|=|2x-6|=2|x-3|<2\delta=2\,\frac{\varepsilon}{2}=\varepsilon$.

In symbols only, this is written as follows:

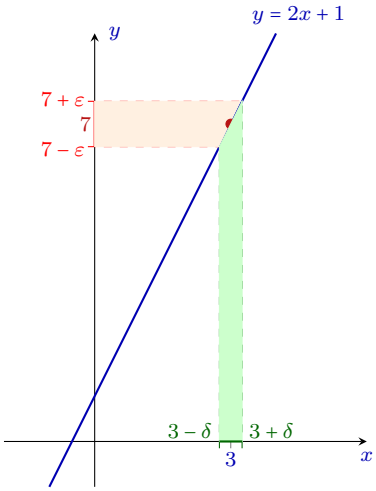
$$\forall\,\varepsilon>0 \quad \exists\,\delta=\frac{\varepsilon}{2} \quad \forall\, x \quad |x-3|<\delta \implies |(2x+1)-7|<\varepsilon.$$

Therefore, by definition of limit, $\lim\limits_{x\to 3}(2x+1)=7$.

16 / 19

Geometric interpretation

Let us illustrate our proof of $\lim\limits_{x\to 3}(2x+1) = 7$ geometrically.



Choose any $\varepsilon > 0$.

$\forall\, x \;\; x \in (3-\delta, 3+\delta) \implies f(x) \in (7-\varepsilon, 7+\varepsilon)$

Observe that

$x \in (3-\delta, 3+\delta) \iff 3-\delta < x < 3+\delta$

$\iff -\delta < x-3 < \delta \iff |x-3| < \delta$.

Similarly, $f(x) \in (7-\varepsilon, 7+\varepsilon) \iff |f(x)-7| < \varepsilon$.

Therefore,

$\forall\, \varepsilon > 0\ \exists\, \delta > 0\ \forall\, x\ |x-3| < \delta \implies |f(x)-7| < \varepsilon.$

It means, by definition of limit,

$7 = \lim\limits_{x\to 3} f(x)$, where $f(x) = 2x+1$.

17 / 19

Working with the definition of limit

What does it mean that $L \neq \lim\limits_{x\to a} f(x)$?

$$L = \lim_{x\to a} f(x) \;:=\; \forall\, \varepsilon > 0 \quad \exists\, \delta > 0 \quad \forall\, x \qquad 0 < |x-a| < \delta \implies |f(x)-L| < \varepsilon\,.$$

$$L \neq \lim_{x\to a} f(x) \iff \exists\, \varepsilon > 0 \quad \forall\, \delta > 0 \quad \exists\, x \qquad 0 < |x-a| < \delta \;\wedge\; |f(x)-L| \geq \varepsilon\,.$$

In words:

A number L is **not** a limit of a function $f(x)$ at a point a, if there exists a positive number ε, such that for any positive number δ one can find x, such that $0 < |x-a| < \delta$, but $|f(x)-L| \geq \varepsilon$.

Exercise. Use the definition of limit to prove that $\lim\limits_{x\to 0}\left(\sin\dfrac{1}{x}\right)$ **does not exist**.

18 / 19

Can one simplify the definition of limit?

Yes, at some cost. At the cost of an extra definition.

Let $a \in \mathbb{R}$, $\varepsilon \in \mathbb{R}$ and $\varepsilon > 0$. Then the interval $(a-\varepsilon, a+\varepsilon)$ is called the ε-**neighborhood** of a.

L is called a **limit** of f as x approaches a if
for any ε-neighborhood V of L there exists a δ-neighborhood U of a such that $f(U \setminus \{a\}) \subset V$.
Not easy enough? Then take one more definition:

Let $a \in \mathbb{R}$. A set U is a **neighborhood** of a iff
there exists $\varepsilon > 0$ such that U contains the ε-neighborhood of a. Now

L is a **limit** of f as x approaches a iff for each neighborhood V of L
$f^{-1}(V) \cup \{a\}$ is a neighborhood of a.

The notion of **limit** can be replaced by the notion of **continuity**:

A function f is said to be **continuous** at a if
the preimage $f^{-1}(U)$ of any neighborhood U of $f(a)$ is a neighborhood of a.