Lecture 3

Welcome to MAT 250!

Brightspace for MAT 250.01 contains the course information:
Syllabus, Handouts, Announcements, etc.

Gradescope is the class homework and test platform.
Register for Gradescope using entry code **N2ZPJJ**

Activities: lectures
quizzes
homeworks (through Gradescope)
exams (two midterms and final)

Grading:

Midterm 1	20%
Midterm 2	25%
Final (5/14)	35%
HW	15%
Quizzes	5%

The **final grade** is the **maximum** of the score for final exam and the total grade calculated according to the scheme discribed above.

What we have learned so far

A **proposition** is a sentence that is either true or false.
We call true and false **truth values** or **Boolean values** and denote by T or F. A proposition with parameters (free variables) is called a **predicate**.

Propositions and predicates are called **statements**.

Statements may be combined into a new statement using **Boolean functions**
i.e., functions of Boolean variables taking Boolean values

$$\underbrace{\{\mathsf{F},\mathsf{T}\}\times\cdots\times\{\mathsf{F},\mathsf{T}\}}_{n\,\text{times}}\to\{\mathsf{F},\mathsf{T}\}\,.$$

The simplest Boolean functions are five **connectives**:

$\neg$ **negation** $\wedge$ **conjunction** $\vee$ **disjunction** $\Longrightarrow$ **implication** $\Longleftrightarrow$ **equivalence**

The connectives are defined by the **truth tables**:

P	Q	$P\wedge Q$	$P\vee Q$	$P\Longrightarrow Q$	$P\Longleftrightarrow Q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	T	T	F
F	F	F	F	T	T

P	$\neg P$
T	F
F	T

Boolean functions vs. propositional forms

Boolean functions allow to build new statements as compositions
of old statements with a Boolean function P, Q, $\dots \mapsto \Phi(P,Q,\dots)$.

An expression formed of **Boolean variables** and **connectives**
is called **a propositional form.**

A propositional form represents a Boolean function.
Propositional forms look like formulas for elementary functions in Calculus.

Fundamental differense:
In Calculus many functions cannot be expressed in elementary functions,
while any Boolean function of finitely many variables
can be presented by a propositional form.

Moreover, there are two **canonical** ways for this:
disjunctive and conjunctive normal forms.

In Calculus their counterparts are **polynomials**.

4 / 46

Disjunctive normal forms

A **disjuncive normal form** is a disjunction of
several conjuctions of variables and their negations.

Example. $(P \wedge \neg Q) \vee (\neg P \wedge Q) \vee \neg Q$.

Theorem. Any Boolean function of finitely many variable which is not identiacally false has a full disjunctive normal form.

Conjunction and disjunction are involved in a few simple relations,
which allow to simplify a disjunctive normal form.

5 / 46

What are implications for?

The connectives $\neg$, $\wedge$ and $\vee$ do **a great job!**

Any non-trivial Boolean function has been **canonically** presented as
a propositional form involving only these three connectives.

Do we need any other connectives? Do we need $\Longrightarrow$ and $\Longleftrightarrow$?

If yes, then what is their **purpose**?

In order to answer, we need to study $\Longrightarrow$ and $\Longleftrightarrow$.

Modus ponence

$P \wedge (P \Longrightarrow Q)$ is equivalent to $P \wedge Q$.

Proof.

$$
\begin{aligned}
& P \wedge (P \Longrightarrow Q) \\
\Longleftrightarrow\ & P \wedge (\neg P \vee Q) \\
\Longleftrightarrow\ & (P \wedge \neg P) \vee (P \wedge Q) \\
\Longleftrightarrow\ & \mathbb{T} \vee (P \wedge Q) \\
\Longleftrightarrow\ & P \wedge Q \,.
\end{aligned}
$$

□

Context: building a theory

Logic is used in the context of a **theory**.
Some statements in a theory are accepted to be true (and called **axioms**).
Some statements are deduced from axioms and have become **theorems**.

What does it mean, to prove a proposition P?

Say, let $A_1, \ldots, A_n$ be the list of axioms.

To prove a proposition P means
to prove that $(A_1 \wedge \cdots \wedge A_n) \Longrightarrow P$ is a tautology.
By Modus Ponence,
$(A_1 \wedge \cdots \wedge A_n) \wedge (A_1 \wedge \cdots \wedge A_n \Longrightarrow P)$ is equivalent to $(A_1 \wedge \cdots \wedge A_n) \wedge P$.
As soon as we proved P,
P can be adjoined to the set of axioms (and used in the forthcoming proofs).

This is how a math theory **grows**.

Conclusion. the connective $\Longrightarrow$ is needed for **growth** of theories.

8 / 46

Objectives

In this lecture we'll explore the following questions:

- What **is** a definition?
- What are definitions **for**?
- Where do definitions **come from**?
- What is the **structure** of a definition?
- Why is it important to **remember** definitions?
- How can we **work with** definitions?
- How should we **read** a mathematical text?

9 / 46

The nature of a mathematical definition

Mathematics is an exact science.
All statements must be **precise** - to be understood in a unique way.
This precision is achieved through careful use of definitions.

Definitions introduce new terms
and ensure clarity and consistency in mathematical language.
A definition gives an exact, unambiguous meaning to a **term** –
a word or phrase being defined.

A definition is an agreement on how a term will be used.
It specifies what qualifies as the term - and what does not.

Let us illustrate the nature of a mathematical definition
using the definition of a rational number.

10 / 46

Definition of a rational number

Definition. A number is called **rational number**
if it can be presented as a quotient of two integers.

This definition contains three essential parts:
– The **term** (word or phrase) to be defined - "rational number".

– The **class** it belongs to - "numbers".

– The **distinguishing characteristic** -
"can be presented as a quotient of two integers".

Each time we say "rational number,"
we must mean exactly what the definition says - no more, no less.

The definition is clear and unambiguous, but to fully understand it,
we must know what an integer is and what a quotient means.

The definition also explains which number is not rational:
any number that cannot be written as a quotient of two integers is not rational.

11 / 46

Three essentials

The definition of a rational number can be stated in slightly different formats:

A number is said to be **rational**

if it can be presented as a quotient of two integers.

A number is a rational number

if it can be presented as a quotient of two integers.

A rational number is a number that can be presented

as a quotient of two integers.

Regardless the way a definition is written,
it should contain three essential elements:

– the term being defined,

– the class it belongs to

– its distinguishing characteristic.

12 / 46

Definitions as biconditional sentences

Formally, the definition of a rational number is a **conditional** sentence:
A number is a rational number

if it can be presented as a quotient of two integers.

This definition actually means the following:
– If a number is rational, then it can be written as a quotient of two integers.
– If a number can be written as a quotient of two integers, then it is rational.

☞ It is a custom to write definitions as **conditional** sentences,
though they are always understood as **biconditional**,
because they establish an **if and only if** relationship

between the term and its defining characteristic:

A number is a rational number

iff it can be presented as a quotient of two integers.

Compare with another format of the same definition:
A rational number is a number that can be presented

as a quotient of two integers.

13 / 46

Rational or not?

How do we use the definition of a rational number?

- $2/3$ is a rational number since it is a quotient of two integers 2 and 3.
- $1.3/2.3$ is also a rational number, although is not written as a quotient of two integers. But it can be presented as such a quotient: $1.3/2.3 = 13/23$.
- $\sqrt{9}$ is a rational number, although it is not given as a quotient of two integers. But it can be presented as such a quotient: $\sqrt{9} = 3 = 3/1$.
- $\sqrt{2}$ is not a rational number. It is not given as a quotient of two integers - but as we seen above, some numbers can be rewritten in that form. The claim that $\sqrt{2}$ cannot be expressed as such a quotient is not obvious - it requires a proof. Only after proving this can we state with certainty that $\sqrt{2}$ is not rational.

14 / 46

Example is <u>not</u> a definition

– What's a rational number?

– That's easy! Like $\frac{2}{3}$ or $-\frac{7}{5}$.

– Is $\sum_{n=0}^{\infty}(-1)^n \frac{\pi^{2n+1}}{6^{2n+1}(2n+1)!}$ a rational number?

– Umm... maybe?

– Then what is a rational number, really?
Give a **definition**, not just an example!

15 / 46

Not only in math

A definition specifies properties that uniquely characterize the term.
The shorter and more precise the list of properties, the better the definition.

Definition (chemistry). An **acid** is a molecule that can donate a hydrogen ion.

Definition (medicine). A **diabetes** is a chronic condition when the body either doesn't produce enough insulin or can't effectively use the insulin it produces.

Definition (astronomy). A **star** is a luminous spherical celestial body of plasma held together by self-gravity.

Definition (political science). A **democracy** is a system of government in which power is held by the people through elected representatives.

Definition (biology). A **bird** is an animal having feathers.

Definition (music). A **counterpoint** is the technique of combining several independent musical lines that are harmonically dependent.

16 / 46

Remarks on necessary, but not sufficient

Problem 3 in the midterm.
Necessary, but not sufficient condition for triangle to be isosceles (or equilateral.)

Solution: the sum of all inner angles is 180? Sufficient? No, Necessary?

Is every trivial predicate a necessary condition for everything?
Yes! By definition.
We forgot to request non-trivial.

With this requirement, is this an easy question?

In the case of equilateral. Isosceles is a good answer.

For isosceles?

Try A.I.

17 / 46

Structure of a definition

In mathematics, a definition often has the following structure:

Definition. Let _____ (description of universes, objects, variables).

_____ (object) is called / is said to be / is _____ (term)

if ← if always means iff in definitions

_____ (distinguishing characteristic).

18 / 46

Divisibilty

Definition. Let d and n be **integers** and $d \neq 0$. One says that
d **divides** n (or, equivalently, n is **divisible** by d)
if $n = d \cdot k$ for some integer k.
In this case d is called a **divisor** of n.

Notation: $d \mid n$

Remarks. 1. Variables d and n are free.

2. Here is this definition written symbolically:
Let $d, n \in \mathbb{Z} \ \wedge \ d \neq 0$.
$d \mid n \iff \exists k \in \mathbb{Z} \quad n = d \cdot k$.

3. The definition of divisibility is made in terms of multiplication, not division. Why?

4. Why $d \neq 0$? Why we can't divide by 0?

19 / 46

Warning

Consider two conditional sentences:

Two lines on a coordinate plane are parallel (*if*) *they don't intersect each other.*

Two lines on a coordinate plane are parallel (*if*) *they have the same slope.*

One of them can be used as a definition; the other cannot.
Which is which?

The definition is the first sentence.
We can replace (if) by (iff) without loosing the meaning:

Two lines on a coordinate plane are parallel (*iff*) *they don't intersect each other.*

The second sentence is not biconditional. It is not true that

Two lines on a coordinate plane are parallel (*iff*) *they have the same slope.*

Vertical lines are parallel, but they have undefined slopes.

Quantifiers in definitions

In definitions, a variable for the term is always free (without a quantifier),
all other variables should be appropriately quantified.
Quantification is crucial for understanding the exact meaning of the definition.

Consider the definition of an even function.

Definition. A function $f : \mathbb{R} \to \mathbb{R}$ is called **even** if $f(-x) = f(x)$ for all $x \in \mathbb{R}$.

Here, there are two variables, f and x.
f denotes the term "even function", and it is free.
x denotes a variable, and it stands under universal quantifier:
$f : \mathbb{R} \to \mathbb{R}$ is an **even function** $\iff \forall\, x \in \mathbb{R}\ f(-x) = f(x)$.

What happens if we omit the universal quantifier $\forall$?
The statement $f(-x) = f(x)$ becomes ambiguous:

for which values of x does this hold?

What happens if we change universal to existential quantifier?
This gives a statement with a different meaning: $f(-x) = f(x)$ for some $x \in \mathbb{R}$.

Constructive definitions

The scheme of a constructive definition looks as follows:

<description of objects>
<formula> is called <name>.

Example.

Let X, Y and Z be sets, and let $f : X \to Y$, $g : Y \to Z$ be maps.

Then the map $g \circ f : X \to Z$ defined by formula $g \circ f(x) = g(f(x))$ is called the **composition** of f and g.

22 / 46

Reformulations

Given a definition "X is called <name> if $P(X)$", a statement

"X is <name> $\iff Q(X)$"

is called a **reformulation of the definition**.

Why are reformulations useful?

Example.

Definition: A triangle is said to be **right**, if it has a right angle.

Reformulation. A triangle is right

iff the lengths of its sides are a, b, c such that $a^2 + b^2 = c^2$.

It's a matter of choice and convinience what is definition and and what is reformulation.

In a good textbook definitions come with lots of reformulations.

Give examples.

23 / 46

Even function

Exercise. Using the definition of even function, show that $f(x) = x^2$ is an even function, while $g(x) = x + 1$ is not.

Solution. To show that f is even, we need to prove that $\forall\, x \in \mathbb{R}\ \ f(-x) = f(x)$.

If we simply write $f(-x) = (-x)^2 = x^2 = f(x)$, this wouldn't suffice:
it's unclear for which x this calculation is valid. For some special x or for all x? This makes difference!
Here is correct proof:
$\forall\, x \in \mathbb{R}\quad f(-x) = (-x)^2 = x^2 = f(x)$. Therefore, f is even.

Let us show now that $g(x) = x + 1$ is not even.

What does it mean that g is not even? It means that $g(-x) \neq g(x)$ for some x. To prove this, it would suffice to find such x. Take, for example, $x = 1$.
Then $g(-1) = -1 + 1 = 0$ and $g(1) = 1 + 1 = 2$, so $g(-1) \neq g(1)$.
So there exists x, namely $x = 1$ such that $g(-x) \neq g(x)$.
Therefore, g is not even.

How to use definition in a proof

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

Theorem. Let a, b and c be integers, and $a \neq 0$.
If a divides both b and c, then a divides $b + c$.

Proof. Since $a \,|\, b$, then, by definition of divisibility, $b = a \cdot k$ for some integer k. Since $a \,|\, c$, then $c = a \cdot l$ for some integer l. Therefore,

$$b + c = ak + al = a(k + l).$$

So there exists an integer, namely $k + l$, such that $b + c = a(k + l)$.
Therefore, a divides $b + c$, as required.

Exercise. Is the converse statement true? That is,
if $a \,|\, (b + c)$, then $a \,|\, b$ and $a \,|\, c$?
Prove the statement if true; otherwise, give a counterexample.

Solution. This is not true. Take, for example $a = 3$, $b = 4$, $c = 5$.
Then $3 \,|\, \underbrace{(4 + 5)}_{9}$, but it is not true that $3 \,|\, 4$ and it is not true that $3 \,|\, 5$.

Definition of a prime number

Definition. Let $p > 1$ be an integer.
p is called **prime** if it has only two positive divisors: 1 and p.

Exercise. Write down the definition in symbolic form.
Solution. Any integer greater than 1 has at least two positive divisors:
1 and itself. The integer is called prime if these are its only positive divisors.
That is, there are no other positive divisors.
This means that any positive divisor of a prime number p must be either 1 or p:

$$k \mid p \implies k = 1 \vee k = p\,.$$

Let us complete this statement by specifying the universe and quantifier for k:

$$\forall k \in \mathbb{Z}^+ \ (k \mid p \implies k = 1 \vee k = p)\,.$$

Add the universe for p to get a complete symbolic form of the definition:
Let $p \in \mathbb{Z}$ and $p > 1$.

$$p \text{ is prime} \iff \forall k \in \mathbb{Z}^+ \ (k \mid p \implies k = 1 \vee k = p)\,.$$

There is no special notation for a prime number,
so there are words in the symbolic form of the definition.

26 / 46

Composite number

Definition. Let $n > 1$ be an integer.
n is called **composite** if it has more than two positive divisors.

Exercise. Is it true that if an integer greater than 1 is not prime,
then it is composite?

Solution. Let us construct a negation for the definition of prime:

$$p \text{ is prime} \iff \forall k \in \mathbb{Z}^+ \ (k \mid p \implies k = 1 \vee k = p)\,.$$

$$\begin{aligned} p \text{ is not prime} &\iff \neg(\forall k \in \mathbb{Z}^+ \ (k \mid p \implies k = 1 \vee k = p)) \\ &\iff \exists k \in \mathbb{Z}^+ \ \neg(k \mid p \implies k = 1 \vee k = p) \\ &\iff \exists k \in \mathbb{Z}^+ \ (k \mid p \wedge k \neq 1 \wedge k \neq p) \end{aligned}$$

In particular, this means that if an integer p is not prime,
then there exists its positive divisor different from both 1 and p.
Therefore, p has more than two positive divisors, so it is composite.

Answer: Yes, it is true that if a integer greater than 1 is not prime,
then it is composite.

27 / 46

Increasing function

We know that a function is called **increasing**

$\Longleftarrow$ if $f(x_1) < f(x_2)$ whenever $x_1 < x_2$.

Let us formulate a complete definition.
First of all, we have to describe what x_1, x_2 and f are.

Let $f : D \longrightarrow \mathbb{R}$ be a function defined on its domain $D \subset \mathbb{R}$. Let $x_1, x_2 \in D$.
f is called **increasing on** D if $x_1 < x_2 \implies f(x_1) < f(x_2)$.
Is this good as a definition? Almost ...

We have to specify for which x_1, x_2 the implication is valid,

that is we have to bind x_1, x_2 by quantifiers.

Definition. Let $f : D \longrightarrow \mathbb{R}$ be a function defined on its domain $D \subset \mathbb{R}$.
f is called **increasing on its domain** if $\forall\, x_1, x_2 \in D \;\; x_1 < x_2 \implies f(x_1) < f(x_2)$.
Symbolically:
f is **increasing on** $D \iff \forall\, x_1, x_2 \in D \;\; x_1 < x_2 \implies f(x_1) < f(x_2)$

In this definition, f is free, and x_1, x_2 are quantified.

Non-increasing function

Exercise. Given the definition of **increasing** function,

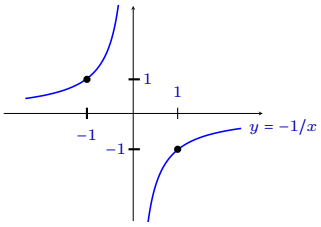
f is **increasing on** $D \iff \forall\, x_1, x_2 \in D \;\; \big(x_1 < x_2 \implies f(x_1) < f(x_2)\big)$,

formulate what it means that a function is **not** increasing.

Solution.

$$f \text{ is } \textbf{not increasing on } D \iff \neg\big(\forall\, x_1, x_2 \in D \;\; \big(x_1 < x_2 \implies f(x_1) < f(x_2)\big)\big)$$
$$\iff \exists\, x_1, x_2 \in D \;\; \big(x_1 < x_2 \wedge f(x_1) \geq f(x_2)\big)$$

Example 3. Is the function $f(x) = -\dfrac{1}{x}$ increasing on its domain?



The domain of f is $\mathbb{R} \setminus \{0\}$.
Take $x_1 = -1$ and $x_2 = 1$.
Then $x_1 < x_2$, but $\underbrace{f(x_1)}_{1} \geq \underbrace{f(x_2)}_{-1}$.
So $\exists x_1, x_2 \;\; \big(x_1 < x_2 \wedge f(x_1) \geq f(x_2)\big)$.
Therefore, f is **not** increasing on its domain.

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:
$a + (-a) = (-a) + a = 0$.

30 / 46

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 $\frac{1}{a}$: $a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$

31 / 46

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 $A, B, C \in GL(n, \mathbb{R})$.

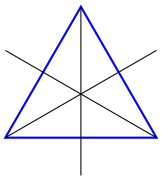
• Identity element: The identity matrix I acts as the neutral element: $AI = IA = A$ for any $A \in GL(n, \mathbb{R})$.

• 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.

34 / 46

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**.

35 / 46

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.

36 / 46

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 addition modulo n. We will study this in more detail later in the course.

37 / 46

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.

38 / 46

A definition from geometry

Definition. Let l be a line and α be a plane in the space. The line l is said to be **parallel** to the plane α, if either l doesn't intersect α or l lies on α.

Notation: $l \parallel \alpha$

Illustration:

Control question: What does it mean that a line is **not** parallel to a plane?

By definition, $l \parallel \alpha \iff \underbrace{l \cap \alpha = \varnothing}_{l \text{ doesn't intersect } \alpha} \vee \underbrace{l \subset \alpha}_{l \text{ lies on } \alpha}$

Therefore, $l \nparallel \alpha \iff \underbrace{l \cap \alpha \neq \varnothing}_{l \text{ intersects } \alpha} \wedge \underbrace{l \not\subset \alpha}_{l \text{ doesn't lies on } \alpha}$

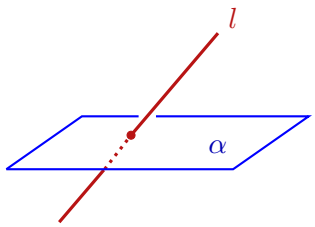
39 / 46

Non-parallel

$l \nparallel \alpha \iff \underbrace{l \cap \alpha \neq \varnothing}_{l \text{ intersects } \alpha} \wedge \underbrace{l \not\subset \alpha}_{l \text{ doesn't lies on } \alpha}$

In words:
A line l is **not** parallel to a plane α if l intersects α, but doesn't lie on α.

Illustration:



40 / 46

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

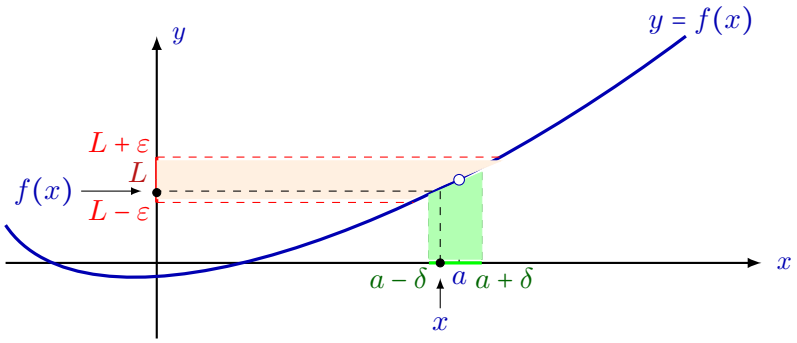
– One implication

41 / 46

Understanding the definition of limit

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

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



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

42 / 46

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, $f(x) = 2x+1$, $a = 3$ and $L = 7$. 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, $\delta = \frac{\varepsilon}{2}$.

43 / 46

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

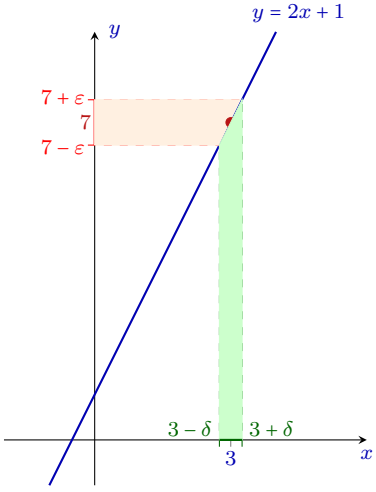
In symbols only, this is written as follows:

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

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

Geometric interpretation

Let us illustrate our proof of $\lim_{x\to 3}(2x+1) = 7$ 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,

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

Working with the definition of limit

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

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

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

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 $\lim\limits_{x \to 0} \left(\sin \dfrac{1}{x} \right) \neq 0$.

46 / 46