Lecture 8

Structure of mathematical text. Proof techniques

Structures in a mathematical text

Structure of mathematical texts

Structure of mathematical texts

In any mathematical text (article, monograph, textbook, etc.)

Structure of mathematical texts

In any mathematical text (article, monograph, textbook, etc.) one can trace common elements which help to see the structure of the text.

Structure of mathematical texts

In any mathematical text (article, monograph, textbook, etc.) one can trace common elements which help to see the structure of the text.

These common elements are:

Structure of mathematical texts

In any mathematical text (article, monograph, textbook, etc.) one can trace common elements which help to see the structure of the text.

These common elements are:
motivations, definitions, axioms, theorems (statements, propositions, claims, lemmas, corollaries), proofs of theorems, examples, exercises, etc.

Structure of mathematical texts

In any mathematical text (article, monograph, textbook, etc.) one can trace common elements which help to see the structure of the text.

These common elements are:
motivations, definitions, axioms, theorems (statements, propositions, claims, lemmas, corollaries), proofs of theorems, examples, exercises, etc.

Besides, each mathematical text contains introductions, list of literature, acknowledgements, history remarks, expositions, authors' opinions, and many other not that essential details.

Structure of mathematical texts

In any mathematical text (article, monograph, textbook, etc.) one can trace common elements which help to see the structure of the text.

These common elements are:
motivations, definitions, axioms, theorems (statements, propositions, claims, lemmas, corollaries), proofs of theorems, examples, exercises, etc.

Besides, each mathematical text contains introductions, list of literature, acknowledgements, history remarks, expositions, authors' opinions, and many other not that essential details.

Rarely one reads a mathematical text from the very beginning to the very end and understands everything at once.

Structure of mathematical texts

In any mathematical text (article, monograph, textbook, etc.) one can trace common elements which help to see the structure of the text.

These common elements are:
motivations, definitions, axioms, theorems (statements, propositions, claims, lemmas, corollaries), proofs of theorems, examples, exercises, etc.

Besides, each mathematical text contains introductions, list of literature, acknowledgements, history remarks, expositions, authors' opinions, and many other not that essential details.

Rarely one reads a mathematical text from the very beginning to the very end and understands everything at once. Usually a work with a mathematical text involves several rounds (approaches, periods).

Structure of mathematical texts

In any mathematical text (article, monograph, textbook, etc.) one can trace common elements which help to see the structure of the text.

These common elements are:
motivations, definitions, axioms, theorems (statements, propositions, claims, lemmas, corollaries), proofs of theorems, examples, exercises, etc.

Besides, each mathematical text contains introductions, list of literature, acknowledgements, history remarks, expositions, authors' opinions, and many other not that essential details.

Rarely one reads a mathematical text from the very beginning to the very end and understands everything at once. Usually a work with a mathematical text involves several rounds (approaches, periods). Each round contributes to the overall understanding.

Structure of mathematical texts

In any mathematical text (article, monograph, textbook, etc.) one can trace common elements which help to see the structure of the text.

These common elements are:
motivations, definitions, axioms, theorems (statements, propositions, claims, lemmas, corollaries), proofs of theorems, examples, exercises, etc.

Besides, each mathematical text contains introductions, list of literature, acknowledgements, history remarks, expositions, authors' opinions, and many other not that essential details.

Rarely one reads a mathematical text from the very beginning to the very end and understands everything at once. Usually a work with a mathematical text involves several rounds (approaches, periods). Each round contributes to the overall understanding.

An experienced reader starts with determining the **structure** of the text and sorting out its elements.

Structure of mathematical texts

In any mathematical text (article, monograph, textbook, etc.) one can trace common elements which help to see the structure of the text.

These common elements are:
motivations, definitions, axioms, theorems (statements, propositions, claims, lemmas, corollaries), proofs of theorems, examples, exercises, etc.

Besides, each mathematical text contains introductions, list of literature, acknowledgements, history remarks, expositions, authors' opinions, and many other not that essential details.

Rarely one reads a mathematical text from the very beginning to the very end and understands everything at once. Usually a work with a mathematical text involves several rounds (approaches, periods). Each round contributes to the overall understanding.

An experienced reader starts with determining the **structure** of the text and sorting out its elements.

The second round is to focus on the **primary** parts of the text:
definitions and statements of theorems.

Structure of mathematical texts

In any mathematical text (article, monograph, textbook, etc.) one can trace common elements which help to see the structure of the text.

These common elements are:
motivations, definitions, axioms, theorems (statements, propositions, claims, lemmas, corollaries), proofs of theorems, examples, exercises, etc.

Besides, each mathematical text contains introductions, list of literature, acknowledgements, history remarks, expositions, authors' opinions, and many other not that essential details.

Rarely one reads a mathematical text from the very beginning to the very end and understands everything at once. Usually a work with a mathematical text involves several rounds (approaches, periods). Each round contributes to the overall understanding.

An experienced reader starts with determining the **structure** of the text and sorting out its elements.

The second round is to focus on the **primary** parts of the text:
definitions and statements of theorems.

Next come examples and **detailed** reading of proofs.

Let us read!

Let us read!

Let's try to read an excerpt from a math textbook.

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics,*

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text:*

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

A number $\alpha \in \mathbb{C}$ is said to be *algebraic over a field* $\mathbb{F} \subseteq \mathbb{C}$ if there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that α is a zero of $f(x)$.

For each field $\mathbb{F}$, every number α in $\mathbb{F}$ is algebraic over $\mathbb{F}$
because α is a zero of the polynomial $f(x) = x - \alpha \in \mathbb{F}[x]$.
This implies that e and π are algebraic over $\mathbb{R}$,
though they are not algebraic over $\mathbb{Q}$ as we will prove later.

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

What is this?

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

What is this? Promises,

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

What is this? Promises, planning.

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

A number $\alpha \in \mathbb{C}$ is said to be *algebraic over a field* $\mathbb{F} \subseteq \mathbb{C}$ if there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that α is a zero of $f(x)$.

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

A number $\alpha \in \mathbb{C}$ is said to be *algebraic over a field* $\mathbb{F} \subseteq \mathbb{C}$ if there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that α is a zero of $f(x)$.
What is this?

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

A number $\alpha \in \mathbb{C}$ is said to be *algebraic over a field* $\mathbb{F} \subseteq \mathbb{C}$ if there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that α is a zero of $f(x)$.
What is this? Definition.

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

A number $\alpha \in \mathbb{C}$ is said to be *algebraic over a field* $\mathbb{F} \subseteq \mathbb{C}$ if there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that α is a zero of $f(x)$.
What is this? Definition. Definition of what?

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

A number $\alpha \in \mathbb{C}$ is said to be *algebraic over a field* $\mathbb{F} \subseteq \mathbb{C}$ if there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that α is a zero of $f(x)$.

For each field $\mathbb{F}$, every number α in $\mathbb{F}$ is algebraic over $\mathbb{F}$

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

A number $\alpha \in \mathbb{C}$ is said to be *algebraic over a field* $\mathbb{F} \subseteq \mathbb{C}$ if there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that α is a zero of $f(x)$.

For each field $\mathbb{F}$, every number α in $\mathbb{F}$ is algebraic over $\mathbb{F}$
What is this?

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

A number $\alpha \in \mathbb{C}$ is said to be *algebraic over a field* $\mathbb{F} \subseteq \mathbb{C}$ if there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that α is a zero of $f(x)$.

For each field $\mathbb{F}$, every number α in $\mathbb{F}$ is algebraic over $\mathbb{F}$
What is this? Theorem.

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

A number $\alpha \in \mathbb{C}$ is said to be *algebraic over a field* $\mathbb{F} \subseteq \mathbb{C}$ if there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that α is a zero of $f(x)$.

For each field $\mathbb{F}$, every number α in $\mathbb{F}$ is algebraic over $\mathbb{F}$

What is this? Theorem. Probably very simple, because it is not called Theorem.

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

A number $\alpha \in \mathbb{C}$ is said to be *algebraic over a field* $\mathbb{F} \subseteq \mathbb{C}$ if there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that α is a zero of $f(x)$.

For each field $\mathbb{F}$, every number α in $\mathbb{F}$ is algebraic over $\mathbb{F}$
because α is a zero of the polynomial $f(x) = x - \alpha \in \mathbb{F}[x]$.

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

A number $\alpha \in \mathbb{C}$ is said to be *algebraic over a field* $\mathbb{F} \subseteq \mathbb{C}$ if there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that α is a zero of $f(x)$.

For each field $\mathbb{F}$, every number α in $\mathbb{F}$ is algebraic over $\mathbb{F}$
because α is a zero of the polynomial $f(x) = x - \alpha \in \mathbb{F}[x]$.
What is this?

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

A number $\alpha \in \mathbb{C}$ is said to be *algebraic over a field* $\mathbb{F} \subseteq \mathbb{C}$ if there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that α is a zero of $f(x)$.

For each field $\mathbb{F}$, every number α in $\mathbb{F}$ is algebraic over $\mathbb{F}$
because α is a zero of the polynomial $f(x) = x - \alpha \in \mathbb{F}[x]$.
What is this? This is a proof.

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

A number $\alpha \in \mathbb{C}$ is said to be *algebraic over a field* $\mathbb{F} \subseteq \mathbb{C}$ if there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that α is a zero of $f(x)$.

For each field $\mathbb{F}$, every number α in $\mathbb{F}$ is algebraic over $\mathbb{F}$
because α is a zero of the polynomial $f(x) = x - \alpha \in \mathbb{F}[x]$.
This implies that e and π are algebraic over $\mathbb{R}$,

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

A number $\alpha \in \mathbb{C}$ is said to be *algebraic over a field* $\mathbb{F} \subseteq \mathbb{C}$ if there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that α is a zero of $f(x)$.

For each field $\mathbb{F}$, every number α in $\mathbb{F}$ is algebraic over $\mathbb{F}$
because α is a zero of the polynomial $f(x) = x - \alpha \in \mathbb{F}[x]$.
This implies that e and π are algebraic over $\mathbb{R}$,
What is this?

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

A number $\alpha \in \mathbb{C}$ is said to be *algebraic over a field* $\mathbb{F} \subseteq \mathbb{C}$ if there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that α is a zero of $f(x)$.

For each field $\mathbb{F}$, every number α in $\mathbb{F}$ is algebraic over $\mathbb{F}$
because α is a zero of the polynomial $f(x) = x - \alpha \in \mathbb{F}[x]$.
This implies that e and π are algebraic over $\mathbb{R}$,
What is this? Corollary, with a proof.

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

A number $\alpha \in \mathbb{C}$ is said to be *algebraic over a field* $\mathbb{F} \subseteq \mathbb{C}$ if there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that α is a zero of $f(x)$.

For each field $\mathbb{F}$, every number α in $\mathbb{F}$ is algebraic over $\mathbb{F}$
because α is a zero of the polynomial $f(x) = x - \alpha \in \mathbb{F}[x]$.
This implies that e and π are algebraic over $\mathbb{R}$,
though they are not algebraic over $\mathbb{Q}$ as we will prove later.

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

A number $\alpha \in \mathbb{C}$ is said to be *algebraic over a field* $\mathbb{F} \subseteq \mathbb{C}$ if there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that α is a zero of $f(x)$.

For each field $\mathbb{F}$, every number α in $\mathbb{F}$ is algebraic over $\mathbb{F}$
because α is a zero of the polynomial $f(x) = x - \alpha \in \mathbb{F}[x]$.
This implies that e and π are algebraic over $\mathbb{R}$,
though they are not algebraic over $\mathbb{Q}$ as we will prove later.
What is this?

Let us read!

Let's try to read an excerpt from a math textbook. We do **not** *intend to understand the mathematics, nonetheless we should be able to analyze the structure of the text: detect and distinguish definitions, notations, theorems, proofs, examples, exercises, etc. in the text.*

As the first step towards classifying the lengths which can be constructed by straightedge and compass, this chapter introduces the concept of an algebraic number. Each such number will satisfy many polynomial equations and our immediate goal is to choose the simplest one.

A number $\alpha \in \mathbb{C}$ is said to be *algebraic over a field* $\mathbb{F} \subseteq \mathbb{C}$ if there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that α is a zero of $f(x)$.

For each field $\mathbb{F}$, every number α in $\mathbb{F}$ is algebraic over $\mathbb{F}$
because α is a zero of the polynomial $f(x) = x - \alpha \in \mathbb{F}[x]$.
This implies that e and π are algebraic over $\mathbb{R}$,
though they are not algebraic over $\mathbb{Q}$ as we will prove later.
What is this? This is a promise, planning.

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

In order to show that a number is algebraic, we look for a suitable polynomial having that number as zero. Try to prove that $1 + \sqrt{3}$ is algebraic over $\mathbb{Q}$.

It is useful to be able to recognize the definition of "algebraic over a field $\mathbb{F}$" when it appears in different guises: a number $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{F} \subseteq \mathbb{C}$ if and only if there is a positive integer n such that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n\}$ are linearly dependent over $\mathbb{F}$.

Indeed, if $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{F} \subseteq \mathbb{C}$ then there exists a polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, whose coefficients $a_0, a_1, \ldots, a_n$ all belong to $\mathbb{F}$, at least one of these coefficients is nonzero, and $f(\alpha) = 0$, that is

$$a_0 + a_1\alpha + a_2\alpha^2 \cdots + a_{n-1}\alpha^{n-1} + a_n\alpha^n = 0. \qquad (*)$$

Let us read!

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

What is this?

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

What is this? *Example.*

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

In order to show that a number is algebraic, we look for a suitable polynomial having that number as zero.

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

In order to show that a number is algebraic, we look for a suitable polynomial having that number as zero.
What is this?

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

In order to show that a number is algebraic, we look for a suitable polynomial having that number as zero.

What is this? Explanation, advice.

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

In order to show that a number is algebraic, we look for a suitable polynomial having that number as zero. Try to prove that $1 + \sqrt{3}$ is algebraic over $\mathbb{Q}$.

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

In order to show that a number is algebraic, we look for a suitable polynomial having that number as zero. Try to prove that $1 + \sqrt{3}$ is algebraic over $\mathbb{Q}$.
What is this?

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

In order to show that a number is algebraic, we look for a suitable polynomial having that number as zero. Try to prove that $1 + \sqrt{3}$ is algebraic over $\mathbb{Q}$.
What is this? Exercise.

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

In order to show that a number is algebraic, we look for a suitable polynomial having that number as zero. Try to prove that $1 + \sqrt{3}$ is algebraic over $\mathbb{Q}$.

It is useful to be able to recognize the definition of "algebraic over a field $\mathbb{F}$" when it appears in different guises:

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

In order to show that a number is algebraic, we look for a suitable polynomial having that number as zero. Try to prove that $1 + \sqrt{3}$ is algebraic over $\mathbb{Q}$.

It is useful to be able to recognize the definition of "algebraic over a field $\mathbb{F}$" when it appears in different guises:
What is this?

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

In order to show that a number is algebraic, we look for a suitable polynomial having that number as zero. Try to prove that $1 + \sqrt{3}$ is algebraic over $\mathbb{Q}$.

It is useful to be able to recognize the definition of "algebraic over a field $\mathbb{F}$" when it appears in different guises:

What is this? Motivation

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

In order to show that a number is algebraic, we look for a suitable polynomial having that number as zero. Try to prove that $1 + \sqrt{3}$ is algebraic over $\mathbb{Q}$.

It is useful to be able to recognize the definition of "algebraic over a field $\mathbb{F}$" when it appears in different guises: a number $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{F} \subseteq \mathbb{C}$ if and only if there is a positive integer n such that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n\}$ are linearly dependent over $\mathbb{F}$.

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

In order to show that a number is algebraic, we look for a suitable polynomial having that number as zero. Try to prove that $1 + \sqrt{3}$ is algebraic over $\mathbb{Q}$.

It is useful to be able to recognize the definition of "algebraic over a field $\mathbb{F}$" when it appears in different guises: a number $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{F} \subseteq \mathbb{C}$ if and only if there is a positive integer n such that $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}, \alpha^n\}$ are linearly dependent over $\mathbb{F}$.
What is this?

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

In order to show that a number is algebraic, we look for a suitable polynomial having that number as zero. Try to prove that $1 + \sqrt{3}$ is algebraic over $\mathbb{Q}$.

It is useful to be able to recognize the definition of "algebraic over a field $\mathbb{F}$" when it appears in different guises: a number $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{F} \subseteq \mathbb{C}$ if and only if there is a positive integer n such that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n\}$ are linearly dependent over $\mathbb{F}$.
What is this? Theorem, test for algebraicity.

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

In order to show that a number is algebraic, we look for a suitable polynomial having that number as zero. Try to prove that $1 + \sqrt{3}$ is algebraic over $\mathbb{Q}$.

It is useful to be able to recognize the definition of "algebraic over a field $\mathbb{F}$" when it appears in different guises: a number $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{F} \subseteq \mathbb{C}$ if and only if there is a positive integer n such that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n\}$ are linearly dependent over $\mathbb{F}$.

Indeed, if $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{F} \subseteq \mathbb{C}$ then there exists a polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, whose coefficients $a_0, a_1, \ldots, a_n$ all belong to $\mathbb{F}$, at least one of these coefficients is nonzero, and $f(\alpha) = 0$, that is

$$a_0 + a_1\alpha + a_2\alpha^2 \cdots + a_{n-1}\alpha^{n-1} + a_n\alpha^n = 0. \qquad (*)$$

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

In order to show that a number is algebraic, we look for a suitable polynomial having that number as zero. Try to prove that $1 + \sqrt{3}$ is algebraic over $\mathbb{Q}$.

It is useful to be able to recognize the definition of "algebraic over a field $\mathbb{F}$" when it appears in different guises: a number $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{F} \subseteq \mathbb{C}$ if and only if there is a positive integer n such that $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}, \alpha^n\}$ are linearly dependent over $\mathbb{F}$.

Indeed, if $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{F} \subseteq \mathbb{C}$ then there exists a polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, whose coefficients $a_0, a_1, \dots, a_n$ all belong to $\mathbb{F}$, at least one of these coefficients is nonzero, and $f(\alpha) = 0$, that is

$$a_0 + a_1\alpha + a_2\alpha^2 \cdots + a_{n-1}\alpha^{n-1} + a_n\alpha^n = 0. \qquad (*)$$

What is this?

Let us read!

The number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is zero of the polynomial $f(x) = x^2 - 2$, which is nonzero and has coefficients in $\mathbb{Q}$.

In order to show that a number is algebraic, we look for a suitable polynomial having that number as zero. Try to prove that $1 + \sqrt{3}$ is algebraic over $\mathbb{Q}$.

It is useful to be able to recognize the definition of "algebraic over a field $\mathbb{F}$" when it appears in different guises: a number $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{F} \subseteq \mathbb{C}$ if and only if there is a positive integer n such that $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}, \alpha^n\}$ are linearly dependent over $\mathbb{F}$.

Indeed, if $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{F} \subseteq \mathbb{C}$ then there exists a polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, whose coefficients $a_0, a_1, \dots, a_n$ all belong to $\mathbb{F}$, at least one of these coefficients is nonzero, and $f(\alpha) = 0$, that is

$$a_0 + a_1\alpha + a_2\alpha^2 \cdots + a_{n-1}\alpha^{n-1} + a_n\alpha^n = 0. \qquad (*)$$

What is this? Proof.

Let us read!

Since $\mathbb{F}$ is a subfield of $\mathbb{C}$, we can regard $\mathbb{C}$ as a vector space over $\mathbb{F}$.
The numbers $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n$ are all elements in $\mathbb{C}$, and hence can be regarded as vectors in the vector space $\mathbb{C}$ over $\mathbb{F}$.

The coefficients $a_0, a_1, a_2, \ldots, a_{n-1}, a_n$, on the other hand, are all in $\mathbb{F}$ so we can regard them as scalars. Thus, the equality $(*)$ can be interpreted as a linear dependence of vectors $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n$ in $\mathbb{C}$.

You will often meet the terms "algebraic number" and "transcendental number" where no field is specified.
In such cases the field is taken to be $\mathbb{Q}$.
We formalize this as follows.

A complex number is said to be an *algebraic number* if it is algebraic over $\mathbb{Q}$;
a *transcendental number* if it is not algebraic over $\mathbb{Q}$.

Let us read!

Since $\mathbb{F}$ is a subfield of $\mathbb{C}$, we can regard $\mathbb{C}$ as a vector space over $\mathbb{F}$.

Let us read!

Since $\mathbb{F}$ is a subfield of $\mathbb{C}$, we can regard $\mathbb{C}$ as a vector space over $\mathbb{F}$.

Reminding

Let us read!

Since $\mathbb{F}$ is a subfield of $\mathbb{C}$, we can regard $\mathbb{C}$ as a vector space over $\mathbb{F}$.
Reminding about relation between the notions of subfield and vector space.

Let us read!

Since $\mathbb{F}$ is a subfield of $\mathbb{C}$, we can regard $\mathbb{C}$ as a vector space over $\mathbb{F}$.
The numbers $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n$ are all elements in $\mathbb{C}$, and hence can be regarded as vectors in the vector space $\mathbb{C}$ over $\mathbb{F}$.

Let us read!

Since $\mathbb{F}$ is a subfield of $\mathbb{C}$, we can regard $\mathbb{C}$ as a vector space over $\mathbb{F}$.
The numbers $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n$ are all elements in $\mathbb{C}$, and hence can be regarded as vectors in the vector space $\mathbb{C}$ over $\mathbb{F}$.
Reminding

Let us read!

Since $\mathbb{F}$ is a subfield of $\mathbb{C}$, we can regard $\mathbb{C}$ as a vector space over $\mathbb{F}$.
The numbers $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n$ are all elements in $\mathbb{C}$, and hence can be regarded as vectors in the vector space $\mathbb{C}$ over $\mathbb{F}$.
Reminding about relation between complex numbers and vectors.

Let us read!

Since $\mathbb{F}$ is a subfield of $\mathbb{C}$, we can regard $\mathbb{C}$ as a vector space over $\mathbb{F}$.
The numbers $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n$ are all elements in $\mathbb{C}$, and hence can be regarded as vectors in the vector space $\mathbb{C}$ over $\mathbb{F}$.

The coefficients $a_0, a_1, a_2, \ldots, a_{n-1}, a_n$, on the other hand, are all in $\mathbb{F}$ so we can regard them as scalars. Thus, the equality $(*)$ can be interpreted as a linear dependence of vectors $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n$ in $\mathbb{C}$.

Let us read!

Since $\mathbb{F}$ is a subfield of $\mathbb{C}$, we can regard $\mathbb{C}$ as a vector space over $\mathbb{F}$.
The numbers $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n$ are all elements in $\mathbb{C}$, and hence can be regarded as vectors in the vector space $\mathbb{C}$ over $\mathbb{F}$.

The coefficients $a_0, a_1, a_2, \ldots, a_{n-1}, a_n$, on the other hand, are all in $\mathbb{F}$ so we can regard them as scalars. Thus, the equality $(*)$ can be interpreted as a linear dependence of vectors $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n$ in $\mathbb{C}$.

You will often meet the terms "algebraic number" and "transcendental number" where no field is specified.
In such cases the field is taken to be $\mathbb{Q}$.

Let us read!

Since $\mathbb{F}$ is a subfield of $\mathbb{C}$, we can regard $\mathbb{C}$ as a vector space over $\mathbb{F}$.
The numbers $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n$ are all elements in $\mathbb{C}$, and hence can be regarded as vectors in the vector space $\mathbb{C}$ over $\mathbb{F}$.

The coefficients $a_0, a_1, a_2, \ldots, a_{n-1}, a_n$, on the other hand, are all in $\mathbb{F}$ so we can regard them as scalars. Thus, the equality $(*)$ can be interpreted as a linear dependence of vectors $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n$ in $\mathbb{C}$.

You will often meet the terms “algebraic number” and “transcendental number” where no field is specified.
In such cases the field is taken to be $\mathbb{Q}$.
Motivation and informal definition.

Let us read!

Since $\mathbb{F}$ is a subfield of $\mathbb{C}$, we can regard $\mathbb{C}$ as a vector space over $\mathbb{F}$.
The numbers $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n$ are all elements in $\mathbb{C}$, and hence can be regarded as vectors in the vector space $\mathbb{C}$ over $\mathbb{F}$.

The coefficients $a_0, a_1, a_2, \ldots, a_{n-1}, a_n$, on the other hand, are all in $\mathbb{F}$ so we can regard them as scalars. Thus, the equality $(*)$ can be interpreted as a linear dependence of vectors $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n$ in $\mathbb{C}$.

You will often meet the terms "algebraic number" and "transcendental number" where no field is specified.
In such cases the field is taken to be $\mathbb{Q}$.
We formalize this as follows.

A complex number is said to be an *algebraic number* if it is algebraic over $\mathbb{Q}$;
a *transcendental number* if it is not algebraic over $\mathbb{Q}$.

Let us read!

Since $\mathbb{F}$ is a subfield of $\mathbb{C}$, we can regard $\mathbb{C}$ as a vector space over $\mathbb{F}$.
The numbers $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n$ are all elements in $\mathbb{C}$, and hence can be regarded as vectors in the vector space $\mathbb{C}$ over $\mathbb{F}$.

The coefficients $a_0, a_1, a_2, \ldots, a_{n-1}, a_n$, on the other hand, are all in $\mathbb{F}$ so we can regard them as scalars. Thus, the equality $(*)$ can be interpreted as a linear dependence of vectors $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n$ in $\mathbb{C}$.

You will often meet the terms “algebraic number” and “transcendental number” where no field is specified.
In such cases the field is taken to be $\mathbb{Q}$.
We formalize this as follows.

A complex number is said to be an *algebraic number* if it is algebraic over $\mathbb{Q}$;
a *transcendental number* if it is not algebraic over $\mathbb{Q}$.
These are definitions.

Proofs

Basic schemes of proof

Basic schemes of proof

In this lecture we will discuss basic proof techniques:

Basic schemes of proof

In this lecture we will discuss basic proof techniques:

- Direct proof

Basic schemes of proof

In this lecture we will discuss basic proof techniques:

- Direct proof
- Proof by contraposition

Basic schemes of proof

In this lecture we will discuss basic proof techniques:

- Direct proof
- Proof by contraposition
- Proof by contradiction

Basic schemes of proof

In this lecture we will discuss basic proof techniques:

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Proof by exhaustion (proof by cases)

Direct proof (to prove $P \implies Q$)

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P.

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P. Then ...

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P. Then ... Then ...

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P. Then ... Then ... Therefore, Q.

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P. Then ... Then ... Therefore, Q.

Example 1. Prove that if an integer n is odd, then n^2 is odd.

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P. Then ... Then ... Therefore, Q.

Example 1. Prove that if an integer n is odd, then n^2 is odd.

Proof.

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P . Then ... Then ... Therefore, Q .

Example 1. Prove that if an integer n is odd, then n^2 is odd.

Proof. We have to prove that

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P . Then ... Then ... Therefore, Q .

Example 1. Prove that if an integer n is odd, then n^2 is odd.

Proof. We have to prove that $\forall\, n \in \mathbb{Z}\, (n \text{ is odd} \implies n^2 \text{ is odd})$

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P. Then ... Then ... Therefore, Q.

Example 1. Prove that if an integer n is odd, then n^2 is odd.

Proof. We have to prove that $\forall\, n \in \mathbb{Z}\, (\underbrace{n \text{ is odd}}_{P} \implies \underbrace{n^2 \text{ is odd}}_{Q})$

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P. Then ... Then ... Therefore, Q.

Example 1. Prove that if an integer n is odd, then n^2 is odd.

Proof. We have to prove that $\forall\, n \in \mathbb{Z}\, (\underbrace{n \text{ is odd}}_{\substack{P \\ \text{(given)}}} \implies \underbrace{n^2 \text{ is odd}}_{\substack{Q \\ \text{(to prove)}}})$

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P. Then ... Then ... Therefore, Q.

Example 1. Prove that if an integer n is odd, then n^2 is odd.

Proof. We have to prove that $\forall\, n \in \mathbb{Z}\, (\underbrace{n \text{ is odd}}_{\substack{P \\ \text{(given)}}} \implies \underbrace{n^2 \text{ is odd}}_{\substack{Q \\ \text{(to prove)}}})$

Let n be odd.

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P. Then ... Then ... Therefore, Q.

Example 1. Prove that if an integer n is odd, then n^2 is odd.

Proof. We have to prove that $\forall\, n \in \mathbb{Z}\, (\underbrace{n \text{ is odd}}_{\substack{P \\ \text{(given)}}} \implies \underbrace{n^2 \text{ is odd}}_{\substack{Q \\ \text{(to prove)}}})$

Let n be odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$.

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P. Then ... Then ... Therefore, Q.

Example 1. Prove that if an integer n is odd, then n^2 is odd.

Proof. We have to prove that $\forall\, n \in \mathbb{Z}\, (\underbrace{n \text{ is odd}}_{\substack{P \\ \text{(given)}}} \implies \underbrace{n^2 \text{ is odd}}_{\substack{Q \\ \text{(to prove)}}})$

Let n be odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. Therefore,

$n^2 = (2k+1)^2$

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P. Then ... Then ... Therefore, Q.

Example 1. Prove that if an integer n is odd, then n^2 is odd.

Proof. We have to prove that $\forall\, n \in \mathbb{Z}\, (\underbrace{n \text{ is odd}}_{\substack{P \\ \text{(given)}}} \implies \underbrace{n^2 \text{ is odd}}_{\substack{Q \\ \text{(to prove)}}})$

Let n be odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. Therefore,

$n^2 = (2k+1)^2 = 4k^2 + 4k + 1$

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P. Then ... Then ... Therefore, Q.

Example 1. Prove that if an integer n is odd, then n^2 is odd.

Proof. We have to prove that $\forall\, n \in \mathbb{Z}\, (\underbrace{n \text{ is odd}}_{\substack{P \\ \text{(given)}}} \implies \underbrace{n^2 \text{ is odd}}_{\substack{Q \\ \text{(to prove)}}})$

Let n be odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. Therefore,

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P. Then ... Then ... Therefore, Q.

Example 1. Prove that if an integer n is odd, then n^2 is odd.

Proof. We have to prove that $\forall\, n \in \mathbb{Z}\, (\underbrace{n \text{ is odd}}_{\substack{P \\ \text{(given)}}} \implies \underbrace{n^2 \text{ is odd}}_{\substack{Q \\ \text{(to prove)}}})$

Let n be odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. Therefore,

$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P. Then ... Then ... Therefore, Q.

Example 1. Prove that if an integer n is odd, then n^2 is odd.

Proof. We have to prove that $\forall\, n \in \mathbb{Z}\, (\underbrace{n \text{ is odd}}_{\substack{P \\ \text{(given)}}} \implies \underbrace{n^2 \text{ is odd}}_{\substack{Q \\ \text{(to prove)}}})$

Let n be odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. Therefore,

$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd, as required.

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P. Then ... Then ... Therefore, Q.

Example 1. Prove that if an integer n is odd, then n^2 is odd.

Proof. We have to prove that $\forall\, n \in \mathbb{Z}\, (\underbrace{n \text{ is odd}}_{\substack{P \\ \text{(given)}}} \implies \underbrace{n^2 \text{ is odd}}_{\substack{Q \\ \text{(to prove)}}})$

Let n be odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. Therefore,

$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd, as required.

qed

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called *modus ponens*.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P . Then ... Then ... Therefore, Q .

Example 1. Prove that if an integer n is odd, then n^2 is odd.

Proof. We have to prove that $\forall\, n \in \mathbb{Z}\, (\underbrace{n \text{ is odd}}_{P} \implies \underbrace{n^2 \text{ is odd}}_{Q})$

(given) (to prove)

Let n be odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. Therefore,

$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd, as required.

qed

(quod erat demonstrandum)

Arithmetic mean and geometric mean

Arithmetic mean and geometric mean

Example 2. Show that $\dfrac{a+b}{2} \geq \sqrt{ab}$ for any non-negative real numbers a, b.

Arithmetic mean and geometric mean

Example 2. Show that $\dfrac{a+b}{2} \geq \sqrt{ab}$ for any non-negative real numbers a, b.

Remark. $\dfrac{a+b}{2}$ is called the *arithmetic mean* (AM) of numbers a, b.

Arithmetic mean and geometric mean

Example 2. Show that $\dfrac{a+b}{2} \geq \sqrt{ab}$ for any non-negative real numbers a, b.

Remark. $\dfrac{a+b}{2}$ is called the *arithmetic mean* (AM) of numbers a, b.

$\sqrt{ab}$ is called the *geometric mean* (GM) of numbers a, b.

Arithmetic mean and geometric mean

Example 2. Show that $\frac{a+b}{2} \geq \sqrt{ab}$ for any non-negative real numbers a, b.

Remark. $\frac{a+b}{2}$ is called the *arithmetic mean* (AM) of numbers a, b.

$\sqrt{ab}$ is called the *geometric mean* (GM) of numbers a, b.

Discussion. We have to prove that $\forall\, a, b \in \mathbb{R}\, (a, b \geq 0 \implies \frac{a+b}{2} \geq \sqrt{ab})$.

Arithmetic mean and geometric mean

Example 2. Show that $\frac{a+b}{2} \geq \sqrt{ab}$ for any non-negative real numbers a, b.

Remark. $\frac{a+b}{2}$ is called the *arithmetic mean* (AM) of numbers a, b.

$\sqrt{ab}$ is called the *geometric mean* (GM) of numbers a, b.

Discussion. We have to prove that $\forall\, a, b \in \mathbb{R}\, (a, b \geq 0 \implies \frac{a+b}{2} \geq \sqrt{ab})$.

It's difficult to get $\frac{a+b}{2} \geq \sqrt{ab}$ directly from $a, b \geq 0$, though.

Arithmetic mean and geometric mean

Example 2. Show that $\dfrac{a+b}{2} \geq \sqrt{ab}$ for any non-negative real numbers a, b.

Remark. $\dfrac{a+b}{2}$ is called the *arithmetic mean* (AM) of numbers a, b.

$\sqrt{ab}$ is called the *geometric mean* (GM) of numbers a, b.

Discussion. We have to prove that $\forall\, a, b \in \mathbb{R}\ (a, b \geq 0 \implies \dfrac{a+b}{2} \geq \sqrt{ab})$.

It's difficult to get $\dfrac{a+b}{2} \geq \sqrt{ab}$ directly from $a, b \geq 0$, though.

Let us work "backwards":

Arithmetic mean and geometric mean

Example 2. Show that $\dfrac{a+b}{2} \geq \sqrt{ab}$ for any non-negative real numbers a, b.

Remark. $\dfrac{a+b}{2}$ is called the *arithmetic mean* (AM) of numbers a, b.

$\sqrt{ab}$ is called the *geometric mean* (GM) of numbers a, b.

Discussion. We have to prove that $\forall\ a, b \in \mathbb{R}\ (a, b \geq 0 \implies \dfrac{a+b}{2} \geq \sqrt{ab})$.

It's difficult to get $\dfrac{a+b}{2} \geq \sqrt{ab}$ directly from $a, b \geq 0$, though.

Let us work "backwards":

$$\frac{a+b}{2} \geq \sqrt{ab}$$

Arithmetic mean and geometric mean

Example 2. Show that $\dfrac{a+b}{2} \geq \sqrt{ab}$ for any non-negative real numbers a, b.

Remark. $\dfrac{a+b}{2}$ is called the *arithmetic mean* (AM) of numbers a, b.

$\sqrt{ab}$ is called the *geometric mean* (GM) of numbers a, b.

Discussion. We have to prove that $\forall\, a, b \in \mathbb{R}\; (a, b \geq 0 \implies \dfrac{a+b}{2} \geq \sqrt{ab})$.

It's difficult to get $\dfrac{a+b}{2} \geq \sqrt{ab}$ directly from $a, b \geq 0$, though.

Let us work "backwards":

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a + b \geq 2\sqrt{ab}$$

Arithmetic mean and geometric mean

Example 2. Show that $\dfrac{a+b}{2} \geq \sqrt{ab}$ for any non-negative real numbers a, b.

Remark. $\dfrac{a+b}{2}$ is called the *arithmetic mean* (AM) of numbers a, b.

$\sqrt{ab}$ is called the *geometric mean* (GM) of numbers a, b.

Discussion. We have to prove that $\forall\ a, b \in \mathbb{R}\ (a, b \geq 0 \implies \dfrac{a+b}{2} \geq \sqrt{ab})$.

It's difficult to get $\dfrac{a+b}{2} \geq \sqrt{ab}$ directly from $a, b \geq 0$, though.

Let us work "backwards":

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a+b \geq 2\sqrt{ab} \underset{\substack{\uparrow \\ a,b \geq 0}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

Arithmetic mean and geometric mean

Example 2. Show that $\dfrac{a+b}{2} \geq \sqrt{ab}$ for any non-negative real numbers a, b.

Remark. $\dfrac{a+b}{2}$ is called the *arithmetic mean* (AM) of numbers a, b.

$\sqrt{ab}$ is called the *geometric mean* (GM) of numbers a, b.

Discussion. We have to prove that $\forall\ a, b \in \mathbb{R}\ (a, b \geq 0 \implies \dfrac{a+b}{2} \geq \sqrt{ab})$.

It's difficult to get $\dfrac{a+b}{2} \geq \sqrt{ab}$ directly from $a, b \geq 0$, though.

Let us work "backwards":

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a+b \geq 2\sqrt{ab} \underset{\underset{a,b\geq 0}{\uparrow}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\implies (\sqrt{a} - \sqrt{b})^2 \geq 0\,.$$

Arithmetic mean and geometric mean

Example 2. Show that $\dfrac{a+b}{2} \geq \sqrt{ab}$ for any non-negative real numbers a, b.

Remark. $\dfrac{a+b}{2}$ is called the *arithmetic mean* (AM) of numbers a, b.

$\sqrt{ab}$ is called the *geometric mean* (GM) of numbers a, b.

Discussion. We have to prove that $\forall\ a, b \in \mathbb{R}\ (a, b \geq 0 \implies \dfrac{a+b}{2} \geq \sqrt{ab})$.

It's difficult to get $\dfrac{a+b}{2} \geq \sqrt{ab}$ directly from $a, b \geq 0$, though.

Let us work "backwards":

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a+b \geq 2\sqrt{ab} \underset{\substack{\uparrow \\ a,b\geq 0}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\implies (\sqrt{a} - \sqrt{b})^2 \geq 0\,.$$

Is this a proof?

Arithmetic mean and geometric mean

Example 2. Show that $\frac{a+b}{2} \geq \sqrt{ab}$ for any non-negative real numbers a, b.

Remark. $\frac{a+b}{2}$ is called the *arithmetic mean* (AM) of numbers a, b.

$\sqrt{ab}$ is called the *geometric mean* (GM) of numbers a, b.

Discussion. We have to prove that $\forall\ a, b \in \mathbb{R}\ (a, b \geq 0 \implies \frac{a+b}{2} \geq \sqrt{ab})$.

It's difficult to get $\frac{a+b}{2} \geq \sqrt{ab}$ directly from $a, b \geq 0$, though.

Let us work "backwards":

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a+b \geq 2\sqrt{ab} \underset{\substack{\uparrow \\ a,b\geq 0}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\implies (\sqrt{a} - \sqrt{b})^2 \geq 0\,.$$

Is this a proof? NO !

Arithmetic mean and geometric mean

Example 2. Show that $\dfrac{a+b}{2} \geq \sqrt{ab}$ for any non-negative real numbers a, b.

Remark. $\dfrac{a+b}{2}$ is called the *arithmetic mean* (AM) of numbers a, b.

$\sqrt{ab}$ is called the *geometric mean* (GM) of numbers a, b.

Discussion. We have to prove that $\forall\ a, b \in \mathbb{R}\ (a, b \geq 0 \implies \dfrac{a+b}{2} \geq \sqrt{ab})$.

It's difficult to get $\dfrac{a+b}{2} \geq \sqrt{ab}$ directly from $a, b \geq 0$, though.

Let us work "backwards":

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a+b \geq 2\sqrt{ab} \underset{\substack{\uparrow \\ a,b \geq 0}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\implies (\sqrt{a} - \sqrt{b})^2 \geq 0\,.$$

Is this a proof? NO ! Can we reverse the implications?

Arithmetic mean and geometric mean

Example 2. Show that $\dfrac{a+b}{2} \geq \sqrt{ab}$ for any non-negative real numbers a, b.

Remark. $\dfrac{a+b}{2}$ is called the *arithmetic mean* (AM) of numbers a, b.

$\sqrt{ab}$ is called the *geometric mean* (GM) of numbers a, b.

Discussion. We have to prove that $\forall\ a, b \in \mathbb{R}\ (a, b \geq 0 \implies \dfrac{a+b}{2} \geq \sqrt{ab})$.

It's difficult to get $\dfrac{a+b}{2} \geq \sqrt{ab}$ directly from $a, b \geq 0$, though.

Let us work "backwards":

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a+b \geq 2\sqrt{ab} \underset{\substack{\uparrow \\ a,b \geq 0}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\implies (\sqrt{a} - \sqrt{b})^2 \geq 0 .$$

Is this a proof? NO ! Can we reverse the implications? Yes!

AM-GM inequality

Recall backwards arguments:

AM-GM inequality

Recall backwards arguments:

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a+b \geq 2\sqrt{ab} \underset{\substack{\uparrow \\ a,b\geq 0}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\implies (\sqrt{a} - \sqrt{b})^2 \geq 0\,.$$

AM-GM inequality

Recall backwards arguments:

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a+b \geq 2\sqrt{ab} \underset{\substack{\uparrow \\ a,b\geq 0}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\implies (\sqrt{a} - \sqrt{b})^2 \geq 0\,.$$

Theorem. *The arithmetic mean of two non-negative numbers is greater than or equal to their geometric mean.*

AM-GM inequality

Recall backwards arguments:

$$\frac{a+b}{2} \ge \sqrt{ab} \implies a+b \ge 2\sqrt{ab} \underset{\substack{\uparrow \\ a,b\ge 0}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \ge 0$$

$$\implies (\sqrt{a} - \sqrt{b})^2 \ge 0\,.$$

Theorem. *The arithmetic mean of two non-negative numbers is greater than or equal to their geometric mean.*

Proof. Take any non-negative real numbers a and b. Then

AM-GM inequality

Recall backwards arguments:

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a+b \geq 2\sqrt{ab} \underset{\underset{a,b\geq 0}{\uparrow}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\implies (\sqrt{a}-\sqrt{b})^2 \geq 0\,.$$

Theorem. *The arithmetic mean of two non-negative numbers is greater than or equal to their geometric mean.*

Proof. Take any non-negative real numbers a and b. Then

$$(\sqrt{a}-\sqrt{b})^2 \geq 0$$

AM-GM inequality

Recall backwards arguments:

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a+b \geq 2\sqrt{ab} \underset{\substack{\uparrow \\ a,b\geq 0}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\implies (\sqrt{a}-\sqrt{b})^2 \geq 0\,.$$

Theorem. *The arithmetic mean of two non-negative numbers is greater than or equal to their geometric mean.*

Proof. Take any non-negative real numbers a and b. Then

$$(\sqrt{a}-\sqrt{b})^2 \geq 0 \implies a - 2\sqrt{a}\sqrt{b} + b \geq 0$$

AM-GM inequality

Recall backwards arguments:

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a+b \geq 2\sqrt{ab} \underset{\overset{\uparrow}{a,b\geq 0}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\implies (\sqrt{a} - \sqrt{b})^2 \geq 0\,.$$

Theorem. *The arithmetic mean of two non-negative numbers is greater than or equal to their geometric mean.*

Proof. Take any non-negative real numbers a and b. Then

$$(\sqrt{a} - \sqrt{b})^2 \geq 0 \implies a - 2\sqrt{a}\sqrt{b} + b \geq 0 \implies a + b \geq 2\sqrt{ab}$$

AM-GM inequality

Recall backwards arguments:

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a+b \geq 2\sqrt{ab} \underset{\overset{\uparrow}{a,b\geq 0}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\implies (\sqrt{a}-\sqrt{b})^2 \geq 0\,.$$

Theorem. *The arithmetic mean of two non-negative numbers is greater than or equal to their geometric mean.*

Proof. Take any non-negative real numbers a and b. Then

$$(\sqrt{a}-\sqrt{b})^2 \geq 0 \implies a - 2\sqrt{a}\sqrt{b} + b \geq 0 \implies a+b \geq 2\sqrt{ab} \implies \frac{a+b}{2} \geq \sqrt{ab}$$

AM-GM inequality

Recall backwards arguments:

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a+b \geq 2\sqrt{ab} \underset{\underset{a,b\geq 0}{\uparrow}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\implies (\sqrt{a}-\sqrt{b})^2 \geq 0 \,.$$

Theorem. *The arithmetic mean of two non-negative numbers is greater than or equal to their geometric mean.*

Proof. Take any non-negative real numbers a and b. Then

$$(\sqrt{a}-\sqrt{b})^2 \geq 0 \implies a - 2\sqrt{a}\sqrt{b} + b \geq 0 \implies a+b \geq 2\sqrt{ab} \implies \frac{a+b}{2} \geq \sqrt{ab}\,,$$

as required.

AM-GM inequality

Recall backwards arguments:

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a+b \geq 2\sqrt{ab} \underset{\substack{\uparrow \\ a,b\geq 0}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\implies (\sqrt{a}-\sqrt{b})^2 \geq 0\,.$$

Theorem. *The arithmetic mean of two non-negative numbers is greater than or equal to their geometric mean.*

Proof. Take any non-negative real numbers a and b. Then

$$(\sqrt{a}-\sqrt{b})^2 \geq 0 \implies a - 2\sqrt{a}\sqrt{b} + b \geq 0 \implies a+b \geq 2\sqrt{ab} \implies \frac{a+b}{2} \geq \sqrt{ab}\,,$$

as required.

Corollary. $AM(a,b) = GM(a,b)$ iff $a = b$.

AM-GM inequality

Recall backwards arguments:

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a+b \geq 2\sqrt{ab} \underset{\substack{\uparrow \\ a,b \geq 0}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\implies (\sqrt{a} - \sqrt{b})^2 \geq 0\,.$$

Theorem. *The arithmetic mean of two non-negative numbers is greater than or equal to their geometric mean.*

Proof. Take any non-negative real numbers a and b. Then

$$(\sqrt{a} - \sqrt{b})^2 \geq 0 \implies a - 2\sqrt{a}\sqrt{b} + b \geq 0 \implies a+b \geq 2\sqrt{ab} \implies \frac{a+b}{2} \geq \sqrt{ab}\,,$$

as required.

Corollary. $AM(a,b) = GM(a,b)$ iff $a = b$.

Proof.

AM-GM inequality

Recall backwards arguments:

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a+b \geq 2\sqrt{ab} \underset{\substack{\uparrow \\ a,b\geq 0}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\implies (\sqrt{a}-\sqrt{b})^2 \geq 0\,.$$

Theorem. *The arithmetic mean of two non-negative numbers is greater than or equal to their geometric mean.*

Proof. Take any non-negative real numbers a and b. Then

$$(\sqrt{a}-\sqrt{b})^2 \geq 0 \implies a - 2\sqrt{a}\sqrt{b} + b \geq 0 \implies a+b \geq 2\sqrt{ab} \implies \frac{a+b}{2} \geq \sqrt{ab}\,,$$

as required.

Corollary. $AM(a,b) = GM(a,b)$ iff $a = b$.

Proof. Let $a, b \geq 0$.

AM-GM inequality

Recall backwards arguments:

$$\frac{a+b}{2} \geq \sqrt{ab} \Longrightarrow a+b \geq 2\sqrt{ab} \underset{\substack{\uparrow \\ a,b \geq 0}}{\Longrightarrow} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\Longrightarrow (\sqrt{a} - \sqrt{b})^2 \geq 0\,.$$

Theorem. *The arithmetic mean of two non-negative numbers is greater than or equal to their geometric mean.*

Proof. Take any non-negative real numbers a and b. Then

$$(\sqrt{a} - \sqrt{b})^2 \geq 0 \Longrightarrow a - 2\sqrt{a}\sqrt{b} + b \geq 0 \Longrightarrow a+b \geq 2\sqrt{ab} \Longrightarrow \frac{a+b}{2} \geq \sqrt{ab}\,,$$

as required.

Corollary. $AM(a,b) = GM(a,b)$ iff $a = b$.

Proof. Let $a, b \geq 0$. Then $a = b \iff (\sqrt{a} - \sqrt{b})^2 = 0 \iff a - 2\sqrt{a}\sqrt{b} + b = 0$

AM-GM inequality

Recall backwards arguments:

$$\frac{a+b}{2} \geq \sqrt{ab} \Longrightarrow a+b \geq 2\sqrt{ab} \underset{\substack{\uparrow \\ a,b\geq 0}}{\Longrightarrow} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\Longrightarrow (\sqrt{a}-\sqrt{b})^2 \geq 0\,.$$

Theorem. *The arithmetic mean of two non-negative numbers is greater than or equal to their geometric mean.*

Proof. Take any non-negative real numbers a and b. Then

$$(\sqrt{a}-\sqrt{b})^2 \geq 0 \Longrightarrow a - 2\sqrt{a}\sqrt{b} + b \geq 0 \Longrightarrow a+b \geq 2\sqrt{ab} \Longrightarrow \frac{a+b}{2} \geq \sqrt{ab}\,,$$

as required.

Corollary. $AM(a,b) = GM(a,b)$ iff $a = b$.

Proof. Let $a, b \geq 0$. Then $a = b \Longleftrightarrow (\sqrt{a}-\sqrt{b})^2 = 0 \Longleftrightarrow a - 2\sqrt{a}\sqrt{b} + b = 0$

$$\Longleftrightarrow \frac{a+b}{2} = \sqrt{ab}$$

AM-GM inequality

Recall backwards arguments:

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a+b \geq 2\sqrt{ab} \underset{\substack{\uparrow \\ a,b\geq 0}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\implies (\sqrt{a}-\sqrt{b})^2 \geq 0\,.$$

Theorem. *The arithmetic mean of two non-negative numbers is greater than or equal to their geometric mean.*

Proof. Take any non-negative real numbers a and b. Then

$$(\sqrt{a}-\sqrt{b})^2 \geq 0 \implies a - 2\sqrt{a}\sqrt{b} + b \geq 0 \implies a+b \geq 2\sqrt{ab} \implies \frac{a+b}{2} \geq \sqrt{ab}\,,$$

as required.

Corollary. $AM(a,b) = GM(a,b)$ iff $a = b$.

Proof. Let $a,b \geq 0$. Then $a = b \iff (\sqrt{a}-\sqrt{b})^2 = 0 \iff a - 2\sqrt{a}\sqrt{b} + b = 0$

$$\iff \frac{a+b}{2} = \sqrt{ab} \iff AM(a,b) = GM(a,b)$$

AM-GM inequality

Recall backwards arguments:

$$\frac{a+b}{2} \geq \sqrt{ab} \implies a+b \geq 2\sqrt{ab} \underset{\substack{\uparrow \\ a,b\geq 0}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0$$

$$\implies (\sqrt{a}-\sqrt{b})^2 \geq 0 \,.$$

Theorem. *The arithmetic mean of two non-negative numbers is greater than or equal to their geometric mean.*

Proof. Take any non-negative real numbers a and b. Then

$$(\sqrt{a}-\sqrt{b})^2 \geq 0 \implies a - 2\sqrt{a}\sqrt{b} + b \geq 0 \implies a+b \geq 2\sqrt{ab} \implies \frac{a+b}{2} \geq \sqrt{ab}\,,$$

as required.

Corollary. $AM(a,b) = GM(a,b)$ iff $a=b$.

Proof. Let $a,b\geq 0$. Then $a=b \iff (\sqrt{a}-\sqrt{b})^2 = 0 \iff a-2\sqrt{a}\sqrt{b}+b=0$

$$\iff \frac{a+b}{2} = \sqrt{ab} \iff AM(a,b) = GM(a,b)\,,$$

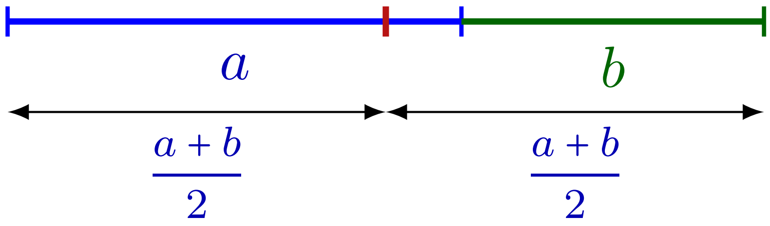
as required.

Geometric interpretation of AM-GM inequality

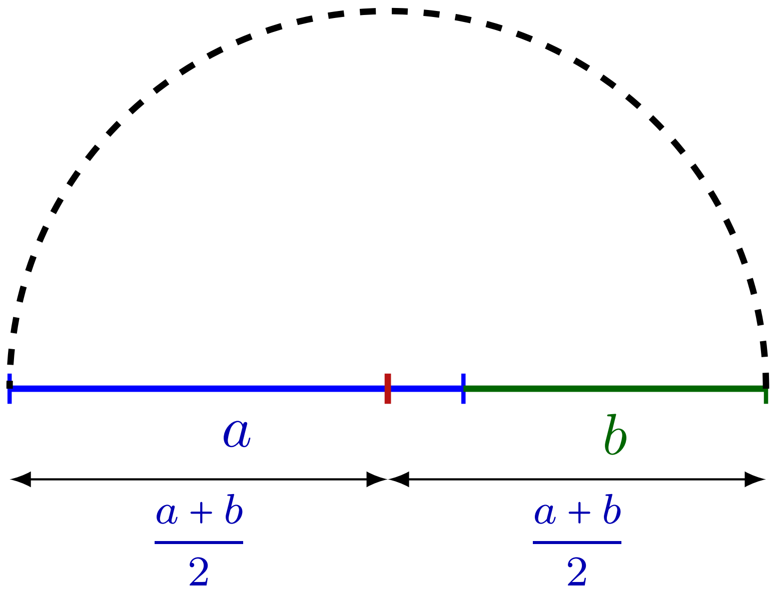
Geometric interpretation of AM-GM inequality

Geometric interpretation of AM-GM inequality

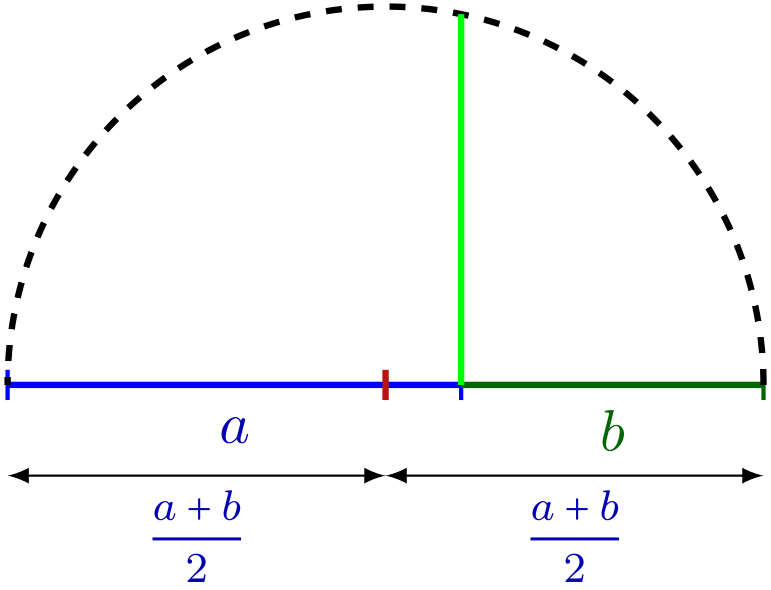
Geometric interpretation of AM-GM inequality



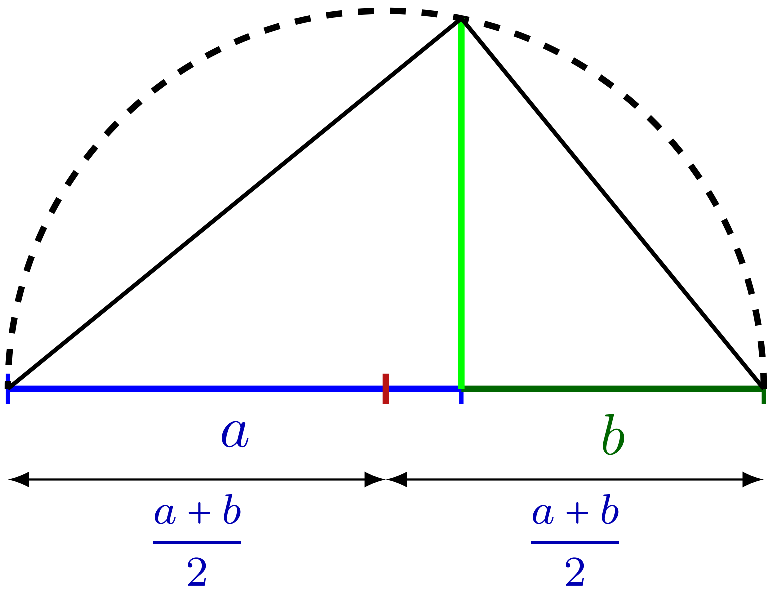
Geometric interpretation of AM-GM inequality



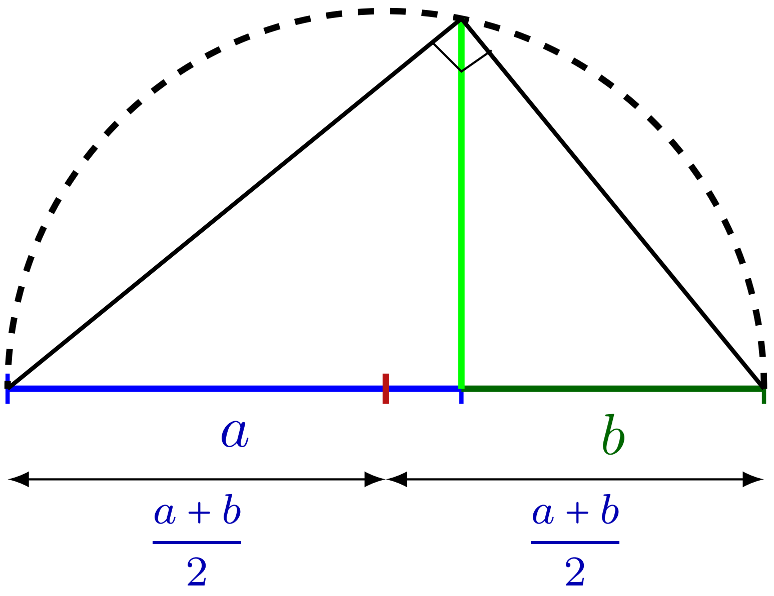
Geometric interpretation of AM-GM inequality



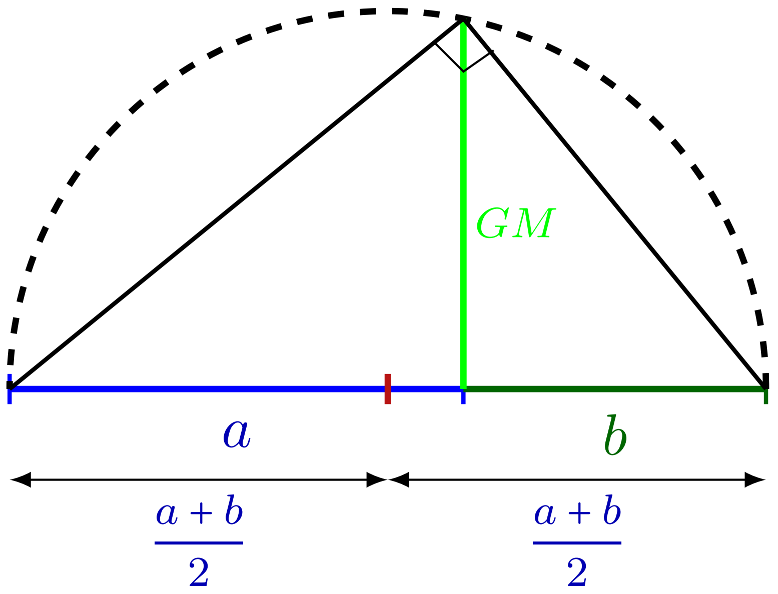
Geometric interpretation of AM-GM inequality



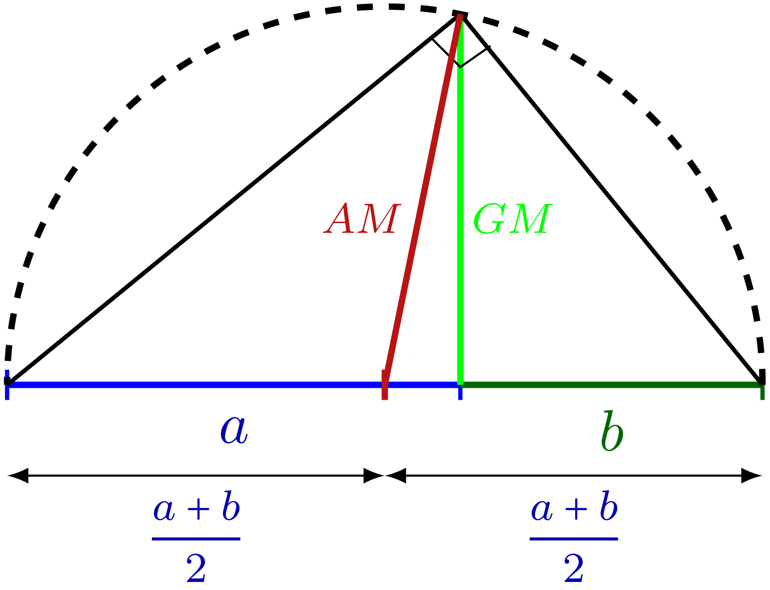
Geometric interpretation of AM-GM inequality



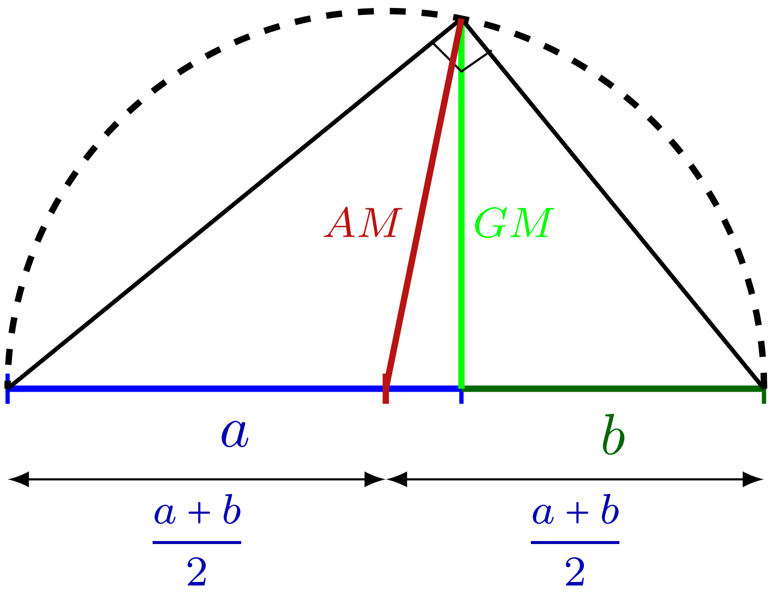
Geometric interpretation of AM-GM inequality



Geometric interpretation of AM-GM inequality



Geometric interpretation of AM-GM inequality

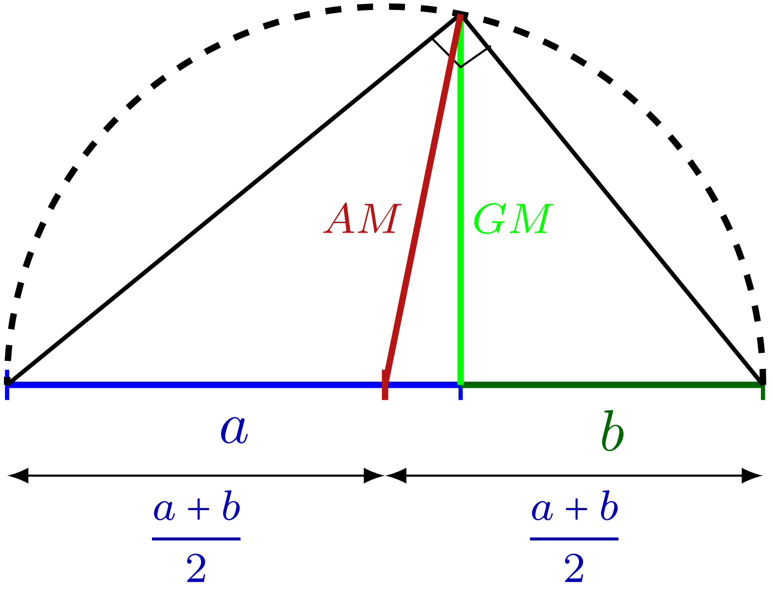


$$AM = \frac{a+b}{2}$$

$$GM = \sqrt{ab}$$

$$AM \geq GM$$

Geometric interpretation of AM-GM inequality



$$AM = \frac{a+b}{2}$$

$$GM = \sqrt{ab}$$

$$AM \geq GM$$

$$AM = GM \iff a = b$$

Differentiability implies continuity

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point,

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Discussion.

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Discussion. Given:

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Discussion. Given: function f,

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Discussion. Given: function f,
point a in its domain,

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Discussion. Given: function f,
point a in its domain,
differentiability of f at a.

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Discussion. Given: function f,
point a in its domain,
differentiability of f at a. What does it mean exactly?

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Discussion. Given: function f,
point a in its domain,
differentiability of f at a. What does it mean exactly?

Definition.

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point,
then it is continuous at this point.

Discussion. Given: function f,
point a in its domain,
differentiability of f at a. What does it mean exactly?

Definition. A function f is differentiable at point a if there exists $f'(a)$,

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Discussion. Given: function f,
point a in its domain,
differentiability of f at a. What does it mean exactly?

Definition. A function f is differentiable at point a if there exists $f'(a)$,

that is, there exists the limit $\lim\limits_{h\to 0} \dfrac{f(a+h)-f(a)}{h}$.

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Discussion. Given: function f,
point a in its domain,
differentiability of f at a. What does it mean exactly?

Definition. A function f is differentiable at point a if there exists $f'(a)$,

that is, there exists the limit $\lim\limits_{h\to 0} \dfrac{f(a+h)-f(a)}{h}$.

Have to prove:

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Discussion. Given: function f,
point a in its domain,
differentiability of f at a. What does it mean exactly?

Definition. A function f is differentiable at point a if there exists $f'(a)$,

that is, there exists the limit $\lim\limits_{h\to 0} \dfrac{f(a+h)-f(a)}{h}$.

Have to prove: f is continuous at a.

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Discussion. Given: function f,
point a in its domain,
differentiability of f at a. What does it mean exactly?

Definition. A function f is differentiable at point a if there exists $f'(a)$,

that is, there exists the limit $\lim_{h\to 0} \dfrac{f(a+h)-f(a)}{h}$.

Have to prove: f is continuous at a. What does it mean exactly?

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Discussion. Given: function f,
point a in its domain,
differentiability of f at a. What does it mean exactly?

Definition. A function f is differentiable at point a if there exists $f'(a)$,

that is, there exists the limit $\lim\limits_{h\to 0}\dfrac{f(a+h)-f(a)}{h}$.

Have to prove: f is continuous at a. What does it mean exactly?

Definition.

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Discussion. Given: function f,
point a in its domain,
differentiability of f at a. What does it mean exactly?

Definition. A function f is differentiable at point a if there exists $f'(a)$,

that is, there exists the limit $\lim_{h \to 0} \dfrac{f(a+h) - f(a)}{h}$.

Have to prove: f is continuous at a. What does it mean exactly?

Definition. A function f is *continuous* at point a if $\lim_{x \to a} f(x) = f(a)$.

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Discussion. Given: function f,
point a in its domain,
differentiability of f at a. What does it mean exactly?

Definition. A function f is differentiable at point a if there exists $f'(a)$,

that is, there exists the limit $\lim\limits_{h\to 0} \dfrac{f(a+h)-f(a)}{h}$.

Have to prove: f is continuous at a. What does it mean exactly?

Definition. A function f is *continuous* at point a if $\lim\limits_{x\to a} f(x) = f(a)$.

What does the phrase $\lim\limits_{x\to a} f(x) = f(a)$ say exactly?

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Discussion. Given: function f,
point a in its domain,
differentiability of f at a. What does it mean exactly?

Definition. A function f is differentiable at point a if there exists $f'(a)$,

that is, there exists the limit $\lim\limits_{h\to 0} \dfrac{f(a+h)-f(a)}{h}$.

Have to prove: f is continuous at a. What does it mean exactly?

Definition. A function f is *continuous* at point a if $\lim\limits_{x\to a} f(x) = f(a)$.

What does the phrase $\lim\limits_{x\to a} f(x) = f(a)$ say exactly?

1. $\exists \lim\limits_{x\to a} f(x)$

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Discussion. Given: function f,
point a in its domain,
differentiability of f at a. What does it mean exactly?

Definition. A function f is differentiable at point a if there exists $f'(a)$,

that is, there exists the limit $\lim\limits_{h\to 0} \dfrac{f(a+h)-f(a)}{h}$.

Have to prove: f is continuous at a. What does it mean exactly?

Definition. A function f is *continuous* at point a if $\lim\limits_{x\to a} f(x) = f(a)$.

What does the phrase $\lim\limits_{x\to a} f(x) = f(a)$ say exactly?

1. $\exists \lim\limits_{x\to a} f(x)$

2. $f(x)$ is defined at $x = a$

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Discussion. Given: function f,
point a in its domain,
differentiability of f at a. What does it mean exactly?

Definition. A function f is differentiable at point a if there exists $f'(a)$,

that is, there exists the limit $\lim_{h\to 0} \dfrac{f(a+h)-f(a)}{h}$.

Have to prove: f is continuous at a. What does it mean exactly?

Definition. A function f is *continuous* at point a if $\lim_{x\to a} f(x) = f(a)$.

What does the phrase $\lim_{x\to a} f(x) = f(a)$ say exactly?

1. $\exists \lim_{x\to a} f(x)$

2. $f(x)$ is defined at $x = a$

3. $\lim_{x\to a} f(x) = f(a)$.

Differentiability implies continuity

We have to prove the implication

Differentiability implies continuity

We have to prove the implication

$$\exists \lim_{h\to 0} \frac{f(a+h)-f(a)}{h} \implies \lim_{x\to a} f(x) = f(a)$$

Differentiability implies continuity

We have to prove the implication

$$\underbrace{\exists \lim_{h\to 0} \frac{f(a+h)-f(a)}{h}}_{\text{given}} \implies \underbrace{\lim_{x\to a} f(x) = f(a)}_{\text{to prove}}$$

Differentiability implies continuity

We have to prove the implication

$$\underbrace{\exists \lim_{h\to 0} \frac{f(a+h)-f(a)}{h}}_{\text{given}} \implies \underbrace{\lim_{x\to a} f(x) = f(a)}_{\text{to prove}}$$

Let us prove that $\lim_{x\to a} f(x) - f(a) = 0$:

Differentiability implies continuity

We have to prove the implication

$$\underbrace{\exists \lim_{h\to 0} \frac{f(a+h)-f(a)}{h}}_{\text{given}} \implies \underbrace{\lim_{x\to a} f(x) = f(a)}_{\text{to prove}}$$

Let us prove that $\lim_{x\to a} f(x) - f(a) = 0$:

$$\lim_{x\to a} f(x) - \quad f(a) \quad =$$

Differentiability implies continuity

We have to prove the implication

$$\underbrace{\exists \lim_{h\to 0}\frac{f(a+h)-f(a)}{h}}_{\text{given}} \implies \underbrace{\lim_{x\to a} f(x) = f(a)}_{\text{to prove}}$$

Let us prove that $\lim_{x\to a} f(x) - f(a) = 0$:

$$\lim_{x\to a} f(x) - \underbrace{f(a)}_{\text{constant}} =$$

Differentiability implies continuity

We have to prove the implication

$$\underbrace{\exists \lim_{h\to 0} \frac{f(a+h)-f(a)}{h}}_{\text{given}} \Longrightarrow \underbrace{\lim_{x\to a} f(x) = f(a)}_{\text{to prove}}$$

Let us prove that $\lim_{x\to a} f(x) - f(a) = 0$:

$$\lim_{x\to a} f(x) - \underbrace{f(a)}_{\text{constant}} = \lim_{x\to a}(f(x) - f(a))$$

Differentiability implies continuity

We have to prove the implication

$$\underbrace{\exists \lim_{h\to 0}\frac{f(a+h)-f(a)}{h}}_{\text{given}} \implies \underbrace{\lim_{x\to a} f(x) = f(a)}_{\text{to prove}}$$

Let us prove that $\lim_{x\to a} f(x) - f(a) = 0$:

$$\lim_{x\to a} f(x) - \underbrace{f(a)}_{\text{constant}} = \lim_{x\to a}(f(x) - f(a)) \underbrace{=}_{\substack{x \neq a \\ \text{by def. of } \lim}} \lim_{x\to a}\left(\frac{f(x)-f(a)}{x-a}\cdot(x-a)\right)$$

Differentiability implies continuity

We have to prove the implication

$$\underbrace{\exists \lim_{h\to 0} \frac{f(a+h)-f(a)}{h}}_{\text{given}} \Longrightarrow \underbrace{\lim_{x\to a} f(x) = f(a)}_{\text{to prove}}$$

Let us prove that $\lim_{x\to a} f(x) - f(a) = 0$:

$$\lim_{x\to a} f(x) - \underbrace{f(a)}_{\text{constant}} = \lim_{x\to a}(f(x) - f(a)) \underbrace{=}_{\substack{x \neq a \\ \text{by def. of lim}}} \lim_{x\to a}\left(\frac{f(x)-f(a)}{x-a}\cdot(x-a)\right)$$

$$\underbrace{=}_{\text{let } h=x-a}$$

Differentiability implies continuity

We have to prove the implication

$$\underbrace{\exists \lim_{h\to 0} \frac{f(a+h)-f(a)}{h}}_{\text{given}} \Longrightarrow \underbrace{\lim_{x\to a} f(x) = f(a)}_{\text{to prove}}$$

Let us prove that $\lim_{x\to a} f(x) - f(a) = 0$:

$$\lim_{x\to a} f(x) - \underbrace{f(a)}_{\text{constant}} = \lim_{x\to a}(f(x)-f(a)) \underbrace{=}_{\substack{x\neq a\\ \text{by def. of } \lim}} \lim_{x\to a}\left(\frac{f(x)-f(a)}{x-a}\cdot(x-a)\right)$$

$$\underbrace{=}_{\text{let } h=x-a} \lim_{h\to 0}\left(\frac{f(a+h)-f(a)}{h}\cdot h\right)$$

Differentiability implies continuity

We have to prove the implication

$$\underbrace{\exists \lim_{h\to 0} \frac{f(a+h)-f(a)}{h}}_{\text{given}} \implies \underbrace{\lim_{x\to a} f(x) = f(a)}_{\text{to prove}}$$

Let us prove that $\lim_{x\to a} f(x) - f(a) = 0$:

$$\lim_{x\to a} f(x) - \underbrace{f(a)}_{\text{constant}} = \lim_{x\to a}(f(x)-f(a)) \underbrace{=}_{\substack{x \neq a \\ \text{by def. of lim}}} \lim_{x\to a}\left(\frac{f(x)-f(a)}{x-a}\cdot(x-a)\right)$$

$$\underbrace{=}_{\text{let } h=x-a} \lim_{h\to 0}\left(\frac{f(a+h)-f(a)}{h}\cdot h\right) \underbrace{=}_{\substack{\text{since both} \\ \text{lims exist}}} \lim_{h\to 0}\frac{f(a+h)-f(a)}{h}\cdot \lim_{h\to 0} h$$

Differentiability implies continuity

We have to prove the implication

$$\underbrace{\exists \lim_{h\to 0} \frac{f(a+h)-f(a)}{h}}_{\text{given}} \implies \underbrace{\lim_{x\to a} f(x) = f(a)}_{\text{to prove}}$$

Let us prove that $\lim_{x\to a} f(x) - f(a) = 0$:

$$\lim_{x\to a} f(x) - \underbrace{f(a)}_{\text{constant}} = \lim_{x\to a}(f(x)-f(a)) \underbrace{=}_{\substack{x\neq a \\ \text{by def. of lim}}} \lim_{x\to a}\left(\frac{f(x)-f(a)}{x-a}\cdot(x-a)\right)$$

$$\underbrace{=}_{\text{let } h=x-a} \lim_{h\to 0}\left(\frac{f(a+h)-f(a)}{h}\cdot h\right) \underbrace{=}_{\substack{\text{since both} \\ \text{lims exist}}} \lim_{h\to 0}\frac{f(a+h)-f(a)}{h}\cdot \lim_{h\to 0} h$$

$$= f'(a)\cdot 0$$

Differentiability implies continuity

We have to prove the implication

$$\underbrace{\exists \lim_{h\to 0} \frac{f(a+h)-f(a)}{h}}_{\text{given}} \implies \underbrace{\lim_{x\to a} f(x) = f(a)}_{\text{to prove}}$$

Let us prove that $\lim_{x\to a} f(x) - f(a) = 0$:

$$\lim_{x\to a} f(x) - \underbrace{f(a)}_{\text{constant}} = \lim_{x\to a}(f(x)-f(a)) \underbrace{=}_{\substack{x \neq a \\ \text{by def. of } \lim}} \lim_{x\to a}\left(\frac{f(x)-f(a)}{x-a}\cdot(x-a)\right)$$

$$\underbrace{=}_{\text{let } h=x-a} \lim_{h\to 0}\left(\frac{f(a+h)-f(a)}{h}\cdot h\right) \underbrace{=}_{\substack{\text{since both} \\ \lim\text{s exist}}} \lim_{h\to 0}\frac{f(a+h)-f(a)}{h}\cdot \lim_{h\to 0} h$$

$$= f'(a)\cdot 0 \quad = 0$$

Differentiability implies continuity

We have to prove the implication

$$\underbrace{\exists \lim_{h\to 0} \frac{f(a+h)-f(a)}{h}}_{\text{given}} \implies \underbrace{\lim_{x\to a} f(x) = f(a)}_{\text{to prove}}$$

Let us prove that $\lim_{x\to a} f(x) - f(a) = 0$:

$$\lim_{x\to a} f(x) - \underbrace{f(a)}_{\text{constant}} = \lim_{x\to a}(f(x)-f(a)) \underbrace{=}_{\substack{x\neq a \\ \text{by def. of } \lim}} \lim_{x\to a}\left(\frac{f(x)-f(a)}{x-a}\cdot(x-a)\right)$$

$$\underbrace{=}_{\text{let } h=x-a} \lim_{h\to 0}\left(\frac{f(a+h)-f(a)}{h}\cdot h\right) \underbrace{=}_{\substack{\text{since both} \\ \lim\text{s exist}}} \lim_{h\to 0}\frac{f(a+h)-f(a)}{h}\cdot\lim_{h\to 0} h$$

$= f'(a)\cdot 0 \;\; = 0$, as required.

Differentiability implies continuity

Let us clear our work off unnecessary ”educational” bells and whistles:

Differentiability implies continuity

Let us clear our work off unnecessary ”educational” bells and whistles:

Theorem. *Let* f *be a function defined in a neighborhood of a point* a *.*

Differentiability implies continuity

Let us clear our work off unnecessary "educational" bells and whistles:

Theorem. *Let* f *be a function defined in a neighborhood of a point* a *.*

If f *is differentiable at* a *, then* f *is continuous at* a *.*

Differentiability implies continuity

Let us clear our work off unnecessary "educational" bells and whistles:

Theorem. *Let* f *be a function defined in a neighborhood of a point* a *.*

If f *is differentiable at* a *, then* f *is continuous at* a *.*

Proof.

Differentiability implies continuity

Let us clear our work off unnecessary "educational" bells and whistles:

Theorem. *Let* f *be a function defined in a neighborhood of a point* a *.*

If f *is differentiable at* a *, then* f *is continuous at* a *.*

Proof. $$\lim_{x\to a} f(x) - f(a) = \lim_{x\to a}(f(x) - f(a)) = \lim_{x\to a}\left(\frac{f(x)-f(a)}{x-a}\cdot(x-a)\right) =$$
$$\lim_{h\to 0}\left(\frac{f(a+h)-f(a)}{h}\cdot h\right) = \lim_{h\to 0}\frac{f(a+h)-f(a)}{h}\cdot\lim_{h\to 0} h = f'(a)\cdot 0 = 0\,.$$

Differentiability implies continuity

Let us clear our work off unnecessary "educational" bells and whistles:

Theorem. *Let* f *be a function defined in a neighborhood of a point* a *.*

If f *is differentiable at* a *, then* f *is continuous at* a *.*

Proof. $\lim\limits_{x\to a} f(x) - f(a) = \lim\limits_{x\to a}(f(x) - f(a)) = \lim\limits_{x\to a}\left(\frac{f(x)-f(a)}{x-a}\cdot(x-a)\right) =$

$\lim\limits_{h\to 0}\left(\frac{f(a+h)-f(a)}{h}\cdot h\right) = \lim\limits_{h\to 0}\frac{f(a+h)-f(a)}{h}\cdot\lim\limits_{h\to 0} h = f'(a)\cdot 0 = 0$.

Therefore, $\lim\limits_{x\to a} f(x) = f(a)$,

Differentiability implies continuity

Let us clear our work off unnecessary "educational" bells and whistles:

Theorem. *Let* f *be a function defined in a neighborhood of a point* a*.*

If f *is differentiable at* a*, then* f *is continuous at* a*.*

Proof. $\lim\limits_{x\to a} f(x) - f(a) = \lim\limits_{x\to a}(f(x) - f(a)) = \lim\limits_{x\to a}\left(\dfrac{f(x)-f(a)}{x-a}\cdot(x-a)\right) =$
$\lim\limits_{h\to 0}\left(\dfrac{f(a+h)-f(a)}{h}\cdot h\right) = \lim\limits_{h\to 0}\dfrac{f(a+h)-f(a)}{h}\cdot\lim\limits_{h\to 0} h = f'(a)\cdot 0 = 0\,.$

Therefore, $\lim\limits_{x\to a} f(x) = f(a)$, and, by this, f is continuous at a

Differentiability implies continuity

Let us clear our work off unnecessary "educational" bells and whistles:

Theorem. *Let f be a function defined in a neighborhood of a point a.*

If f is differentiable at a, then f is continuous at a.

Proof. $\lim\limits_{x\to a} f(x) - f(a) = \lim\limits_{x\to a}(f(x) - f(a)) = \lim\limits_{x\to a}\left(\dfrac{f(x) - f(a)}{x - a} \cdot (x - a)\right) =$

$\lim\limits_{h\to 0}\left(\dfrac{f(a+h) - f(a)}{h} \cdot h\right) = \lim\limits_{h\to 0} \dfrac{f(a+h) - f(a)}{h} \cdot \lim\limits_{h\to 0} h = f'(a) \cdot 0 = 0$.

Therefore, $\lim\limits_{x\to a} f(x) = f(a)$, and, by this, f is continuous at a, as required.

Proof by contraposition

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

This rule of logical deduction $((P \implies Q) \wedge \neg Q) \implies \neg P$ is called *modus tollens*.

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

This rule of logical deduction $((P \implies Q) \wedge \neg Q) \implies \neg P$ is called *modus tollens*.

Method: Assume (let) $\neg Q$.

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

This rule of logical deduction $((P \implies Q) \wedge \neg Q) \implies \neg P$ is called *modus tollens*.

Method: Assume (let) $\neg Q$. Then ...

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

This rule of logical deduction $((P \implies Q) \wedge \neg Q) \implies \neg P$ is called *modus tollens*.

Method: Assume (let) $\neg Q$. Then ... Then ...

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

This rule of logical deduction $((P \implies Q) \wedge \neg Q) \implies \neg P$ is called *modus tollens*.

Method: Assume (let) $\neg Q$. Then ... Then ... Therefore, $\neg P$.

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

This rule of logical deduction $((P \implies Q) \wedge \neg Q) \implies \neg P$ is called *modus tollens*.

Method: Assume (let) $\neg Q$. Then ... Then ... Therefore, $\neg P$.

So $\neg Q \implies \neg P$.

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

This rule of logical deduction $((P \implies Q) \land \neg Q) \implies \neg P$ is called *modus tollens*.

Method: Assume (let) $\neg Q$. Then ... Then ... Therefore, $\neg P$.

So $\neg Q \implies \neg P$. By contraposition, $P \implies Q$.

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

This rule of logical deduction $((P \implies Q) \wedge \neg Q) \implies \neg P$ is called *modus tollens*.

Method: Assume (let) $\neg Q$. Then ... Then ... Therefore, $\neg P$.

So $\neg Q \implies \neg P$. By contraposition, $P \implies Q$.

Example 1.

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

This rule of logical deduction $((P \implies Q) \wedge \neg Q) \implies \neg P$ is called *modus tollens*.

Method: Assume (let) $\neg Q$. Then ... Then ... Therefore, $\neg P$.

So $\neg Q \implies \neg P$. By contraposition, $P \implies Q$.

Example 1. Let n be an integer.

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

This rule of logical deduction $((P \implies Q) \wedge \neg Q) \implies \neg P$ is called *modus tollens*.

Method: Assume (let) $\neg Q$. Then ... Then ... Therefore, $\neg P$.

So $\neg Q \implies \neg P$. By contraposition, $P \implies Q$.

Example 1. Let n be an integer. Prove that if n^2 is odd then n is odd.

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

This rule of logical deduction $((P \implies Q) \wedge \neg Q) \implies \neg P$ is called *modus tollens*.

Method: Assume (let) $\neg Q$. Then ... Then ... Therefore, $\neg P$.

So $\neg Q \implies \neg P$. By contraposition, $P \implies Q$.

Example 1. Let n be an integer. Prove that if n^2 is odd then n is odd.

Discussion.

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

This rule of logical deduction $((P \implies Q) \wedge \neg Q) \implies \neg P$ is called *modus tollens*.

Method: Assume (let) $\neg Q$. Then ... Then ... Therefore, $\neg P$.

So $\neg Q \implies \neg P$. By contraposition, $P \implies Q$.

Example 1. Let n be an integer. Prove that if n^2 is odd then n is odd.

Discussion. We have to prove that

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

This rule of logical deduction $((P \implies Q) \wedge \neg Q) \implies \neg P$ is called *modus tollens*.

Method: Assume (let) $\neg Q$. Then ... Then ... Therefore, $\neg P$.

So $\neg Q \implies \neg P$. By contraposition, $P \implies Q$.

Example 1. Let n be an integer. Prove that if n^2 is odd then n is odd.

Discussion. We have to prove that

$$\forall\, n \in \mathbb{Z} \quad \boxed{n^2 \text{ is odd}} \implies \boxed{n \text{ is odd}}$$

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

This rule of logical deduction $((P \implies Q) \wedge \neg Q) \implies \neg P$ is called *modus tollens*.

Method: Assume (let) $\neg Q$. Then ... Then ... Therefore, $\neg P$.

So $\neg Q \implies \neg P$. By contraposition, $P \implies Q$.

Example 1. Let n be an integer. Prove that if n^2 is odd then n is odd.

Discussion. We have to prove that

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \implies \boxed{n \text{ is odd}}$$

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

This rule of logical deduction $((P \implies Q) \land \neg Q) \implies \neg P$ is called *modus tollens*.

Method: Assume (let) $\neg Q$. Then ... Then ... Therefore, $\neg P$.

So $\neg Q \implies \neg P$. By contraposition, $P \implies Q$.

Example 1. Let n be an integer. Prove that if n^2 is odd then n is odd.

Discussion. We have to prove that

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \implies \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

This rule of logical deduction $((P \implies Q) \wedge \neg Q) \implies \neg P$ is called *modus tollens*.

Method: Assume (let) $\neg Q$. Then … Then … Therefore, $\neg P$.

So $\neg Q \implies \neg P$. By contraposition, $P \implies Q$.

Example 1. Let n be an integer. Prove that if n^2 is odd then n is odd.

Discussion. We have to prove that

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \implies \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

Why not to prove like this:

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

This rule of logical deduction $((P \implies Q) \wedge \neg Q) \implies \neg P$ is called *modus tollens*.

Method: Assume (let) $\neg Q$. Then ... Then ... Therefore, $\neg P$.

So $\neg Q \implies \neg P$. By contraposition, $P \implies Q$.

Example 1. Let n be an integer. Prove that if n^2 is odd then n is odd.

Discussion. We have to prove that

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \implies \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

Why not to prove like this: n^2 is odd $\implies$ $\sqrt{n^2} = n$ is odd?

What to choose: direct proof or proof by contraposition?

For a **direct** proof of

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \Longrightarrow \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

What to choose: direct proof or proof by contraposition?

For a **direct** proof of

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \Longrightarrow \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

we have to start with P.

What to choose: direct proof or proof by contraposition?

For a **direct** proof of

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \Longrightarrow \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

we have to start with P. But Q seems to be simpler than P.

What to choose: direct proof or proof by contraposition?

For a **direct** proof of

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \implies \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

we have to start with P. But Q seems to be simpler than P.

This suggests a proof by **contraposition**:

What to choose: direct proof or proof by contraposition?

For a **direct** proof of

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \Longrightarrow \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

we have to start with P. But Q seems to be simpler than P.

This suggests a proof by **contraposition**:

Let $\neg Q$,

What to choose: direct proof or proof by contraposition?

For a **direct** proof of

$$\forall\, n \in \mathbb{Z} \quad \underset{P}{\boxed{n^2 \text{ is odd}}} \Longrightarrow \underset{Q}{\boxed{n \text{ is odd}}}$$

we have to start with P. But Q seems to be simpler than P.

This suggests a proof by **contraposition**:

Let $\neg Q$, that is,

What to choose: direct proof or proof by contraposition?

For a **direct** proof of

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \Longrightarrow \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

we have to start with P. But Q seems to be simpler than P.

This suggests a proof by **contraposition**:

Let $\neg Q$, that is, let n be even

What to choose: direct proof or proof by contraposition?

For a **direct** proof of

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \Longrightarrow \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

we have to start with P. But Q seems to be simpler than P.

This suggests a proof by **contraposition**:

Let $\neg Q$, that is, let n be even, that is, $n = 2k$ for some integer k.

What to choose: direct proof or proof by contraposition?

For a **direct** proof of

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \Longrightarrow \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

we have to start with P. But Q seems to be simpler than P.

This suggests a proof by **contraposition**:

Let $\neg Q$, that is, let n be even, that is, $n = 2k$ for some integer k.

Then n^2

What to choose: direct proof or proof by contraposition?

For a **direct** proof of

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \Longrightarrow \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

we have to start with P. But Q seems to be simpler than P.

This suggests a proof by **contraposition**:

Let $\neg Q$, that is, let n be even, that is, $n = 2k$ for some integer k.

Then $n^2 = 4k^2$,

What to choose: direct proof or proof by contraposition?

For a **direct** proof of

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \Longrightarrow \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

we have to start with P. But Q seems to be simpler than P.

This suggests a proof by **contraposition**:

Let $\neg Q$, that is, let n be even, that is, $n = 2k$ for some integer k.

Then $n^2 = 4k^2$, which is even

What to choose: direct proof or proof by contraposition?

For a **direct** proof of

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \Longrightarrow \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

we have to start with P. But Q seems to be simpler than P.

This suggests a proof by **contraposition**:

Let $\neg Q$, that is, let n be even, that is, $n = 2k$ for some integer k.

Then $n^2 = 4k^2,$ which is even ($\neg P$).

What to choose: direct proof or proof by contraposition?

For a **direct** proof of

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \implies \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

we have to start with P. But Q seems to be simpler than P.

This suggests a proof by **contraposition**:

Let $\neg Q$, that is, let n be even, that is, $n = 2k$ for some integer k.

Then $n^2 = 4k^2,$ which is even ($\neg P$).

Therefore, $\neg Q \implies \neg P$,

What to choose: direct proof or proof by contraposition?

For a **direct** proof of

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \Longrightarrow \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

we have to start with P. But Q seems to be simpler than P.

This suggests a proof by **contraposition**:

Let $\neg Q$, that is, let n be even, that is, $n = 2k$ for some integer k.

Then $n^2 = 4k^2$, which is even ($\neg P$).

Therefore, $\neg Q \Longrightarrow \neg P$, or, equivalently, $P \Longrightarrow Q$.
Cast off crutches:

What to choose: direct proof or proof by contraposition?

For a **direct** proof of

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \implies \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

we have to start with P. But Q seems to be simpler than P.

This suggests a proof by **contraposition**:

Let $\neg Q$, that is, let n be even, that is, $n = 2k$ for some integer k.

Then $n^2 = 4k^2$, which is even ($\neg P$).

Therefore, $\neg Q \implies \neg P$, or, equivalently, $P \implies Q$.
Cast off crutches:
Proposition. *For any integer* n, *if* n^2 *is odd then* n *is odd.*

What to choose: direct proof or proof by contraposition?

For a **direct** proof of

$$\forall\, n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \implies \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

we have to start with P. But Q seems to be simpler than P.

This suggests a proof by **contraposition**:

Let $\neg Q$, that is, let n be even, that is, $n = 2k$ for some integer k.

Then $n^2 = 4k^2$, which is even ($\neg P$).

Therefore, $\neg Q \implies \neg P$, or, equivalently, $P \implies Q$.
Cast off crutches:
Proposition. *For any integer* n*, if* n^2 *is odd then* n *is odd.*

Proof. Let n be even. Then $n = 2k$ for some integer k. So $n^2 = 4k^2$, which is even. Therefore, by contraposition, if n^2 is odd then n is odd, as required.

Parity

Parity

Let us collect our results about the parity.

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Proof. We have to prove that n and n^2 have the same parity,

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Proof. We have to prove that n and n^2 have the same parity, that is, both are even or both are odd.

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Proof. We have to prove that n and n^2 have the same parity, that is, both are even or both are odd. For this, it's enough to prove that

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Proof. We have to prove that n and n^2 have the same parity, that is, both are even or both are odd. For this, it's enough to prove that

$$n \text{ is even} \iff n^2 \text{ is even.}$$

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Proof. We have to prove that n and n^2 have the same parity, that is, both are even or both are odd. For this, it's enough to prove that

$$n \text{ is even } \iff n^2 \text{ is even.}$$

Indeed,

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Proof. We have to prove that n and n^2 have the same parity, that is, both are even or both are odd. For this, it's enough to prove that

$$n \text{ is even} \iff n^2 \text{ is even.}$$

Indeed, if n is even,

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Proof. We have to prove that n and n^2 have the same parity, that is, both are even or both are odd. For this, it's enough to prove that

$$n \text{ is even} \iff n^2 \text{ is even.}$$

Indeed, if n is even, then $n = 2k$ for some $k \in \mathbb{Z}$.

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Proof. We have to prove that n and n^2 have the same parity, that is, both are even or both are odd. For this, it's enough to prove that

$$n \text{ is even} \iff n^2 \text{ is even.}$$

Indeed, if n is even, then $n = 2k$ for some $k \in \mathbb{Z}$. In this case, $n^2 = 4k^2$, which is even.

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Proof. We have to prove that n and n^2 have the same parity, that is, both are even or both are odd. For this, it's enough to prove that

$$n \text{ is even} \iff n^2 \text{ is even.}$$

Indeed, if n is even, then $n = 2k$ for some $k \in \mathbb{Z}$. In this case, $n^2 = 4k^2$, which is even. So if n is even, then n^2 is also even.

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Proof. We have to prove that n and n^2 have the same parity, that is, both are even or both are odd. For this, it's enough to prove that

$$n \text{ is even } \iff n^2 \text{ is even.}$$

Indeed, if n is even, then $n = 2k$ for some $k \in \mathbb{Z}$. In this case, $n^2 = 4k^2$, which is even. So if n is even, then n^2 is also even.

To prove the converse (if n^2 is even, then n is even),

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Proof. We have to prove that n and n^2 have the same parity, that is, both are even or both are odd. For this, it's enough to prove that

$$n \text{ is even} \iff n^2 \text{ is even.}$$

Indeed, if n is even, then $n = 2k$ for some $k \in \mathbb{Z}$. In this case, $n^2 = 4k^2$, which is even. So if n is even, then n^2 is also even.

To prove the converse (if n^2 is even, then n is even), we use contaposition.

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Proof. We have to prove that n and n^2 have the same parity, that is, both are even or both are odd. For this, it's enough to prove that

$$n \text{ is even } \iff n^2 \text{ is even.}$$

Indeed, if n is even, then $n = 2k$ for some $k \in \mathbb{Z}$. In this case, $n^2 = 4k^2$, which is even. So if n is even, then n^2 is also even.

To prove the converse (if n^2 is even, then n is even), we use contaposition.

Let n be odd,

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Proof. We have to prove that n and n^2 have the same parity, that is, both are even or both are odd. For this, it's enough to prove that

$$n \text{ is even} \iff n^2 \text{ is even.}$$

Indeed, if n is even, then $n = 2k$ for some $k \in \mathbb{Z}$. In this case, $n^2 = 4k^2$, which is even. So if n is even, then n^2 is also even.

To prove the converse (if n^2 is even, then n is even), we use contaposition.

Let n be odd, that is $n = 2k + 1$ for some $k \in \mathbb{Z}$.

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Proof. We have to prove that n and n^2 have the same parity, that is, both are even or both are odd. For this, it's enough to prove that

$$n \text{ is even} \iff n^2 \text{ is even.}$$

Indeed, if n is even, then $n = 2k$ for some $k \in \mathbb{Z}$. In this case, $n^2 = 4k^2$, which is even. So if n is even, then n^2 is also even.

To prove the converse (if n^2 is even, then n is even), we use contaposition.

Let n be odd, that is $n = 2k + 1$ for some $k \in \mathbb{Z}$. Then $n^2 = 4k^2 + 4k + 1$,

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Proof. We have to prove that n and n^2 have the same parity, that is, both are even or both are odd. For this, it's enough to prove that

$$n \text{ is even } \iff n^2 \text{ is even.}$$

Indeed, if n is even, then $n = 2k$ for some $k \in \mathbb{Z}$. In this case, $n^2 = 4k^2$, which is even. So if n is even, then n^2 is also even.

To prove the converse (if n^2 is even, then n is even), we use contaposition.

Let n be odd, that is $n = 2k + 1$ for some $k \in \mathbb{Z}$. Then $n^2 = 4k^2 + 4k + 1$, which is odd.

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Proof. We have to prove that n and n^2 have the same parity, that is, both are even or both are odd. For this, it's enough to prove that

$$n \text{ is even} \iff n^2 \text{ is even.}$$

Indeed, if n is even, then $n = 2k$ for some $k \in \mathbb{Z}$. In this case, $n^2 = 4k^2$, which is even. So if n is even, then n^2 is also even.

To prove the converse (if n^2 is even, then n is even), we use contaposition.

Let n be odd, that is $n = 2k + 1$ for some $k \in \mathbb{Z}$. Then $n^2 = 4k^2 + 4k + 1$, which is odd. By contraposition, if n^2 is even, then n is even.

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Proof. We have to prove that n and n^2 have the same parity, that is, both are even or both are odd. For this, it's enough to prove that

$$n \text{ is even} \iff n^2 \text{ is even.}$$

Indeed, if n is even, then $n = 2k$ for some $k \in \mathbb{Z}$. In this case, $n^2 = 4k^2$, which is even. So if n is even, then n^2 is also even.

To prove the converse (if n^2 is even, then n is even), we use contaposition.

Let n be odd, that is $n = 2k + 1$ for some $k \in \mathbb{Z}$. Then $n^2 = 4k^2 + 4k + 1$, which is odd. By contraposition, if n^2 is even, then n is even.

qed

Divisibility

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof.

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove:

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $8 \nmid (n^2 - 1) \implies 2 | n$

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $\underbrace{8 \nmid (n^2 - 1)}_{P} \implies \underbrace{2 | n}_{Q}$

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $\underbrace{8 \nmid (n^2 - 1)}_{P} \Longrightarrow \underbrace{2 | n}_{Q}$

Which one is simpler, P or Q?

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $\underbrace{8 \nmid (n^2 - 1)}_{P} \implies \underbrace{2 | n}_{Q}$

Which one is simpler, P or Q? Q is simpler,

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $\underbrace{8 \nmid (n^2 - 1)}_{P} \Longrightarrow \underbrace{2 \mid n}_{Q}$

Which one is simpler, P or Q? Q is simpler, so we'll do contraposition:

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $\underbrace{8 \nmid (n^2 - 1)}_{P} \implies \underbrace{2 \mid n}_{Q}$

Which one is simpler, P or Q? Q is simpler, so we'll do contraposition:

Assume that $2 \nmid n$

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $\underbrace{8 \nmid (n^2 - 1)}_{P} \implies \underbrace{2 | n}_{Q}$

Which one is simpler, P or Q? Q is simpler, so we'll do contraposition:

Assume that $2 \nmid n$ $(\neg Q)$.

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $\underbrace{8 \nmid (n^2 - 1)}_{P} \implies \underbrace{2 | n}_{Q}$

Which one is simpler, P or Q? Q is simpler, so we'll do contraposition:

Assume that $2 \nmid n$ $(\neg Q)$. Then $n = 2k + 1$ for some integer k.

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $\underbrace{8 \nmid (n^2 - 1)}_{P} \Longrightarrow \underbrace{2 \,|\, n}_{Q}$

Which one is simpler, P or Q? Q is simpler, so we'll do contraposition:

Assume that $2 \nmid n$ $(\neg Q)$. Then $n = 2k + 1$ for some integer k.

Calculate $n^2 - 1$:

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $\underbrace{8 \nmid (n^2 - 1)}_{P} \implies \underbrace{2 | n}_{Q}$

Which one is simpler, P or Q? Q is simpler, so we'll do contraposition:

Assume that $2 \nmid n$ $(\neg Q)$. Then $n = 2k + 1$ for some integer k.

Calculate $n^2 - 1$:

$n^2 - 1$

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $\underbrace{8 \nmid (n^2 - 1)}_{P} \implies \underbrace{2 | n}_{Q}$

Which one is simpler, P or Q? Q is simpler, so we'll do contraposition:

Assume that $2 \nmid n$ $(\neg Q)$. Then $n = 2k + 1$ for some integer k.

Calculate $n^2 - 1$:

$n^2 - 1 = (2k + 1)^2 - 1$

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $\underbrace{8 \nmid (n^2 - 1)}_{P} \implies \underbrace{2 \mid n}_{Q}$

Which one is simpler, P or Q? Q is simpler, so we'll do contraposition:

Assume that $2 \nmid n$ $(\neg Q)$. Then $n = 2k + 1$ for some integer k.

Calculate $n^2 - 1$:

$$n^2 - 1 = (2k + 1)^2 - 1 = 4k^2 + 4k$$

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $\underbrace{8 \nmid (n^2 - 1)}_{P} \implies \underbrace{2 \mid n}_{Q}$

Which one is simpler, P or Q? Q is simpler, so we'll do contraposition:

Assume that $2 \nmid n$ $(\neg Q)$. Then $n = 2k + 1$ for some integer k.

Calculate $n^2 - 1$:

$$n^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k = 4 \ k(k+1)$$

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $\underbrace{8 \nmid (n^2 - 1)}_{P} \implies \underbrace{2 | n}_{Q}$

Which one is simpler, P or Q? Q is simpler, so we'll do contraposition:

Assume that $2 \nmid n$ $(\neg Q)$. Then $n = 2k + 1$ for some integer k.

Calculate $n^2 - 1$:

$$n^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k = 4 \underbrace{k(k+1)}_{\text{divisible by } 2}$$

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $\underbrace{8 \nmid (n^2 - 1)}_{P} \implies \underbrace{2 \mid n}_{Q}$

Which one is simpler, P or Q? Q is simpler, so we'll do contraposition:

Assume that $2 \nmid n$ $(\neg Q)$. Then $n = 2k + 1$ for some integer k.

Calculate $n^2 - 1$:

$$n^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k = 4\underbrace{k(k+1)}_{\text{divisible by } 2}$$ is divisible by 8 $(\neg P)$.

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $\underbrace{8 \nmid (n^2 - 1)}_{P} \implies \underbrace{2 | n}_{Q}$

Which one is simpler, P or Q? Q is simpler, so we'll do contraposition:

Assume that $2 \nmid n$ $(\neg Q)$. Then $n = 2k + 1$ for some integer k.

Calculate $n^2 - 1$:

$n^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k = 4 \underbrace{k(k+1)}_{\text{divisible by } 2}$ is divisible by 8 $(\neg P)$.

We have proved that $2 \nmid n \implies 8 | (n^2 - 1)$.

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $\underbrace{8 \nmid (n^2 - 1)}_{P} \implies \underbrace{2 | n}_{Q}$

Which one is simpler, P or Q? Q is simpler, so we'll do contraposition:

Assume that $2 \nmid n$ $(\neg Q)$. Then $n = 2k + 1$ for some integer k.

Calculate $n^2 - 1$:

$n^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k = 4 \underbrace{k(k+1)}_{\text{divisible by } 2}$ is divisible by 8 $(\neg P)$.

We have proved that $2 \nmid n \implies 8 | (n^2 - 1)$.

By contraposition, $8 \nmid (n^2 - 1) \implies 2 | n$,

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $\underbrace{8 \nmid (n^2 - 1)}_{P} \implies \underbrace{2 | n}_{Q}$

Which one is simpler, P or Q? Q is simpler, so we'll do contraposition:

Assume that $2 \nmid n$ $(\neg Q)$. Then $n = 2k + 1$ for some integer k.

Calculate $n^2 - 1$:

$n^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k = 4 \underbrace{k(k+1)}_{\text{divisible by } 2}$ is divisible by 8 $(\neg P)$.

We have proved that $2 \nmid n \implies 8 | (n^2 - 1)$.

By contraposition, $8 \nmid (n^2 - 1) \implies 2 | n$, as required.

Non-zero integral

Example 3. Let f be integrable on $[0,1]$.

Non-zero integral

Example 3. Let f be integrable on $[0, 1]$. Prove that

Non-zero integral

Example 3. Let f be integrable on $[0,1]$. Prove that

$$\text{if } \int_0^1 f(x)\,dx \neq 0, \text{ then } f(x) \neq 0 \text{ for some } x \in [0,1].$$

Non-zero integral

Example 3. Let f be integrable on $[0,1]$. Prove that

if $\int_0^1 f(x)\,dx \neq 0$, then $f(x) \neq 0$ for some $x \in [0,1]$.

Proof.

Non-zero integral

Example 3. Let f be integrable on $[0,1]$. Prove that

if $\int_0^1 f(x)\,dx \neq 0$, then $f(x) \neq 0$ for some $x \in [0,1]$.

Proof. Have to prove:

Non-zero integral

Example 3. Let f be integrable on $[0,1]$. Prove that

$$\text{if } \int_0^1 f(x)\,dx \neq 0\text{, then } f(x) \neq 0 \text{ for some } x \in [0,1].$$

Proof. Have to prove:

$$\int_0^1 f(x)\,dx \neq 0 \implies \exists\, x \in [0,1]\ \ f(x) \neq 0\,.$$

Non-zero integral

Example 3. Let f be integrable on $[0,1]$. Prove that

$$\text{if } \int_0^1 f(x)\,dx \neq 0\,,\ \text{then } f(x) \neq 0 \text{ for some } x \in [0,1]\,.$$

Proof. Have to prove:

$$\int_0^1 f(x)\,dx \neq 0 \implies \exists\, x \in [0,1]\ \ f(x) \neq 0\,.$$

Assume that $f(x) = 0$ for **all** $x \in [0,1]$.

Non-zero integral

Example 3. Let f be integrable on $[0,1]$. Prove that

$$\text{if } \int_0^1 f(x)\,dx \neq 0\,, \text{ then } f(x) \neq 0 \text{ for some } x \in [0,1]\,.$$

Proof. Have to prove:

$$\int_0^1 f(x)\,dx \neq 0 \implies \exists\, x \in [0,1]\;\; f(x) \neq 0\,.$$

Assume that $f(x) = 0$ for **all** $x \in [0,1]$. Then $\int_0^1 f(x)\,dx = 0$.

Non-zero integral

Example 3. Let f be integrable on $[0,1]$. Prove that

$$\text{if } \int_0^1 f(x)\,dx \neq 0\text{, then } f(x) \neq 0 \text{ for some } x \in [0,1].$$

Proof. Have to prove:

$$\int_0^1 f(x)\,dx \neq 0 \implies \exists\, x \in [0,1] \;\; f(x) \neq 0\,.$$

Assume that $f(x) = 0$ for **all** $x \in [0,1]$. Then $\int_0^1 f(x)\,dx = 0$.

Therefore, by contraposition,

Non-zero integral

Example 3. Let f be integrable on $[0,1]$. Prove that

$$\text{if } \int_0^1 f(x)\,dx \neq 0\text{, then } f(x) \neq 0 \text{ for some } x \in [0,1].$$

Proof. Have to prove:

$$\int_0^1 f(x)\,dx \neq 0 \implies \exists\, x \in [0,1]\;\; f(x) \neq 0\,.$$

Assume that $f(x) = 0$ for **all** $x \in [0,1]$. Then $\int_0^1 f(x)\,dx = 0$.

Therefore, by contraposition,

if $\int_0^1 f(x)\,dx \neq 0$, then $f(x) \neq 0$ for some $x \in [0,1]$,

Non-zero integral

Example 3. Let f be integrable on $[0,1]$. Prove that

$$\text{if } \int_0^1 f(x)\,dx \neq 0\text{, then } f(x) \neq 0 \text{ for some } x \in [0,1].$$

Proof. Have to prove:

$$\int_0^1 f(x)\,dx \neq 0 \implies \exists\, x \in [0,1] \;\; f(x) \neq 0\,.$$

Assume that $f(x) = 0$ for **all** $x \in [0,1]$. Then $\int_0^1 f(x)\,dx = 0$.

Therefore, by contraposition,

if $\int_0^1 f(x)\,dx \neq 0$, then $f(x) \neq 0$ for some $x \in [0,1]$, as required.

Proof by contradiction (indirect proof)

Idea: To prove P,

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements,

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements, Q and $\neg Q$.

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements, Q and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements, Q and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called *reductio ad absurdum*.

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements, Q and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called *reductio ad absurdum*.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements, Q and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called *reductio ad absurdum*.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$.

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements, Q and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called *reductio ad absurdum*.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... Q.

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements, Q and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called *reductio ad absurdum*.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... Q. Then ... $\neg Q$.

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements, Q and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called *reductio ad absurdum*.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... Q. Then ... $\neg Q$. Therefore, P.

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements, Q and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called *reductio ad absurdum*.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... Q. Then ... $\neg Q$. Therefore, P.

Example 1.

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements, Q and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called *reductio ad absurdum*.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... Q. Then ... $\neg Q$. Therefore, P.

Example 1. Prove that $\sqrt{2}$ is irrational.

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements, Q and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called *reductio ad absurdum*.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... Q. Then ... $\neg Q$. Therefore, P.

Example 1. Prove that $\sqrt{2}$ is irrational.

Proof. The statement to prove:

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements, Q and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called *reductio ad absurdum*.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... Q. Then ... $\neg Q$. Therefore, P.

Example 1. Prove that $\sqrt{2}$ is irrational.

Proof. The statement to prove: $\boxed{\sqrt{2} \text{ is irrational}}$.

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements, Q and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called *reductio ad absurdum*.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... Q. Then ... $\neg Q$. Therefore, P.

Example 1. Prove that $\sqrt{2}$ is irrational.

Proof. The statement to prove: $\underbrace{\boxed{\sqrt{2} \text{ is irrational}}}_{P}$.

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements, Q and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called *reductio ad absurdum*.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... Q. Then ... $\neg Q$. Therefore, P.

Example 1. Prove that $\sqrt{2}$ is irrational.

Proof. The statement to prove: $\underbrace{\boxed{\sqrt{2} \text{ is irrational}}}_{P}$.

Assume, to the contrary, that

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements, Q and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called *reductio ad absurdum*.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... Q. Then ... $\neg Q$. Therefore, P.

Example 1. Prove that $\sqrt{2}$ is irrational.

Proof. The statement to prove: $\underbrace{\boxed{\sqrt{2} \text{ is irrational}}}_{P}$.

Assume, to the contrary, that $\boxed{\sqrt{2} \text{ is rational}}$.

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements, Q and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called *reductio ad absurdum*.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... Q. Then ... $\neg Q$. Therefore, P.

Example 1. Prove that $\sqrt{2}$ is irrational.

Proof. The statement to prove: $\underbrace{\boxed{\sqrt{2} \text{ is irrational}}}_{P}$.

Assume, to the contrary, that $\underbrace{\boxed{\sqrt{2} \text{ is rational}}}_{\neg P}$.

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements, Q and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called *reductio ad absurdum*.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... Q. Then ... $\neg Q$. Therefore, P.

Example 1. Prove that $\sqrt{2}$ is irrational.

Proof. The statement to prove: $\underbrace{\boxed{\sqrt{2} \text{ is irrational}}}_{P}$.

Assume, to the contrary, that $\underbrace{\boxed{\sqrt{2} \text{ is rational}}}_{\neg P}$.

Then $\sqrt{2} = \dfrac{p}{q}$ for some $p, q \in \mathbb{Z},\ q \neq 0$.

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality,

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,
we may assume, without loss of generality, that $\gcd(p,q) = 1$.

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\boxed{\gcd(p,q) = 1}$.

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q) = 1}}_{Q}$.

$\sqrt{2}$ is irrational

Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underset{Q}{\boxed{\gcd(p,q) = 1}}$.

According to our assumption, $\sqrt{2} = \dfrac{p}{q}$.

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underset{Q}{\boxed{\gcd(p,q)=1}}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$,

$\sqrt{2}$ is irrational

Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q) = 1}}_{Q}$.

According to our assumption, $\sqrt{2} = \dfrac{p}{q}$. By squaring, we get $2 = \dfrac{p^2}{q^2}$, so $2q^2 = p^2$.

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that p^2 is even.

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q) = 1}}_{Q}$.

According to our assumption, $\sqrt{2} = \frac{p}{q}$. By squaring, we get $2 = \frac{p^2}{q^2}$, so $2q^2 = p^2$.

It means that p^2 is even. Since p has the same parity as p^2

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that p^2 is even. Since p has the same parity as p^2

(see Theorem about the same parity of an integer and its square),

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2} = \frac{p}{q}$. By squaring, we get $2 = \frac{p^2}{q^2}$, so $2q^2 = p^2$.

It means that p^2 is even. Since p has the same parity as p^2
(see Theorem about the same parity of an integer and its square),
we conclude that p should be even,

$\sqrt{2}$ is irrational

Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\dfrac{p}{q}$. By squaring, we get $2=\dfrac{p^2}{q^2}$, so $2q^2=p^2$.

It means that p^2 is even. Since p has the same parity as p^2
(see Theorem about the same parity of an integer and its square),
we conclude that p should be even, that is, $p=2k$ for some integer k.

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underset{Q}{\boxed{\gcd(p,q)=1}}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that p^2 is even. Since p has the same parity as p^2
(see Theorem about the same parity of an integer and its square),
we conclude that p should be even, that is, $p=2k$ for some integer k.

In this case, the identity $2q^2=p^2$

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that p^2 is even. Since p has the same parity as p^2 (see Theorem about the same parity of an integer and its square), we conclude that p should be even, that is, $p=2k$ for some integer k.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$,

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that p^2 is even. Since p has the same parity as p^2 (see Theorem about the same parity of an integer and its square), we conclude that p should be even, that is, $p=2k$ for some integer k.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2} = \frac{p}{q}$. By squaring, we get $2 = \frac{p^2}{q^2}$, so $2q^2 = p^2$.

It means that p^2 is even. Since p has the same parity as p^2
(see Theorem about the same parity of an integer and its square),
we conclude that p should be even, that is, $p = 2k$ for some integer k.

In this case, the identity $2q^2 = p^2$ is equivalent to $2q^2 = (2k)^2$, or $q^2 = 2k^2$.

By this, q^2 is even,

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that p^2 is even. Since p has the same parity as p^2

(see Theorem about the same parity of an integer and its square),

we conclude that p should be even, that is, $p=2k$ for some integer k.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, q^2 is even, and, therefore, q is even too:

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that p^2 is even. Since p has the same parity as p^2
(see Theorem about the same parity of an integer and its square),
we conclude that p should be even, that is, $p=2k$ for some integer k.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, q^2 is even, and, therefore, q is even too: $2\,|\,q$.

$\sqrt{2}$ is irrational

Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underset{Q}{\boxed{\gcd(p,q)=1}}$.

According to our assumption, $\sqrt{2}=\dfrac{p}{q}$. By squaring, we get $2=\dfrac{p^2}{q^2}$, so $2q^2=p^2$.

It means that p^2 is even. Since p has the same parity as p^2
(see Theorem about the same parity of an integer and its square),
we conclude that p should be even, that is, $p=2k$ for some integer k .

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, q^2 is even, and, therefore, q is even too: $2\,|\,q$.

But p is also even,

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q) = 1}}_{Q}$.

According to our assumption, $\sqrt{2} = \frac{p}{q}$. By squaring, we get $2 = \frac{p^2}{q^2}$, so $2q^2 = p^2$.

It means that p^2 is even. Since p has the same parity as p^2
(see Theorem about the same parity of an integer and its square),
we conclude that p should be even, that is, $p = 2k$ for some integer k.

In this case, the identity $2q^2 = p^2$ is equivalent to $2q^2 = (2k)^2$, or $q^2 = 2k^2$.

By this, q^2 is even, and, therefore, q is even too: $2 \mid q$.

But p is also even, that is $2 \mid p$.

$\sqrt{2}$ is irrational

Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2} = \dfrac{p}{q}$. By squaring, we get $2 = \dfrac{p^2}{q^2}$, so $2q^2 = p^2$.

It means that p^2 is even. Since p has the same parity as p^2 (see Theorem about the same parity of an integer and its square), we conclude that p should be even, that is, $p = 2k$ for some integer k.

In this case, the identity $2q^2 = p^2$ is equivalent to $2q^2 = (2k)^2$, or $q^2 = 2k^2$.

By this, q^2 is even, and, therefore, q is even too: $2\,|\,q$.

But p is also even, that is $2\,|\,p$. We have got that $2\,|\,p$ and $2\,|\,q$.

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that p^2 is even. Since p has the same parity as p^2 (see Theorem about the same parity of an integer and its square), we conclude that p should be even, that is, $p=2k$ for some integer k.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, q^2 is even, and, therefore, q is even too: $2\,|\,q$.

But p is also even, that is $2\,|\,p$. We have got that $2\,|\,p$ and $2\,|\,q$.

Therefore, $\gcd(p,q)\neq 1$

$\sqrt{2}$ is irrational

Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\dfrac{p}{q}$. By squaring, we get $2=\dfrac{p^2}{q^2}$, so $2q^2=p^2$.

It means that p^2 is even. Since p has the same parity as p^2 (see Theorem about the same parity of an integer and its square), we conclude that p should be even, that is, $p=2k$ for some integer k.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, q^2 is even, and, therefore, q is even too: $2\,|\,q$.

But p is also even, that is $2\,|\,p$. We have got that $2\,|\,p$ and $2\,|\,q$.

Therefore $\boxed{\gcd(p,q)\neq 1}$,

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that p^2 is even. Since p has the same parity as p^2 (see Theorem about the same parity of an integer and its square), we conclude that p should be even, that is, $p=2k$ for some integer k .

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, q^2 is even, and, therefore, q is even too: $2\,|\,q$.

But p is also even, that is $2\,|\,p$. We have got that $2\,|\,p$ and $2\,|\,q$.

Therefore $\underbrace{\boxed{\gcd(p,q)\neq 1}}_{\neg Q}$,

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that p^2 is even. Since p has the same parity as p^2
(see Theorem about the same parity of an integer and its square),
we conclude that p should be even, that is, $p=2k$ for some integer k.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, q^2 is even, and, therefore, q is even too: $2\,|\,q$.

But p is also even, that is $2\,|\,p$. We have got that $2\,|\,p$ and $2\,|\,q$.

Therefore $\underbrace{\boxed{\gcd(p,q)\neq 1}}_{\neg Q}$, which contradicts to the fact that $\gcd(p,q)=1$.

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that p^2 is even. Since p has the same parity as p^2
(see Theorem about the same parity of an integer and its square),
we conclude that p should be even, that is, $p=2k$ for some integer k.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, q^2 is even, and, therefore, q is even too: $2\,|\,q$.

But p is also even, that is $2\,|\,p$. We have got that $2\,|\,p$ and $2\,|\,q$.

Therefore $\underbrace{\boxed{\gcd(p,q)\neq 1}}_{\neg Q}$, which contradicts to the fact that $\gcd(p,q)=1$.

This contradiction shows that the original assumption ($\sqrt{2}$ is rational)

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that p^2 is even. Since p has the same parity as p^2 (see Theorem about the same parity of an integer and its square), we conclude that p should be even, that is, $p=2k$ for some integer k.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, q^2 is even, and, therefore, q is even too: $2\,|\,q$.

But p is also even, that is $2\,|\,p$. We have got that $2\,|\,p$ and $2\,|\,q$.

Therefore $\underbrace{\boxed{\gcd(p,q)\neq 1}}_{\neg Q}$, which contradicts to the fact that $\gcd(p,q)=1$.

This contradiction shows that the original assumption ($\sqrt{2}$ is rational) was erroneous,

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that p^2 is even. Since p has the same parity as p^2 (see Theorem about the same parity of an integer and its square), we conclude that p should be even, that is, $p=2k$ for some integer k.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, q^2 is even, and, therefore, q is even too: $2\,|\,q$.

But p is also even, that is $2\,|\,p$. We have got that $2\,|\,p$ and $2\,|\,q$.

Therefore $\underbrace{\boxed{\gcd(p,q)\neq 1}}_{\neg Q}$, which contradicts to the fact that $\gcd(p,q)=1$.

This contradiction shows that the original assumption ($\sqrt{2}$ is rational) was erroneous, and $\sqrt{2}$ is actually irrational,

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that p^2 is even. Since p has the same parity as p^2
(see Theorem about the same parity of an integer and its square),
we conclude that p should be even, that is, $p=2k$ for some integer k.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, q^2 is even, and, therefore, q is even too: $2|q$.

But p is also even, that is $2|p$. We have got that $2|p$ and $2|q$.

Therefore $\underbrace{\boxed{\gcd(p,q)\neq 1}}_{\neg Q}$, which contradicts to the fact that $\gcd(p,q)=1$.

This contradiction shows that the original assumption ($\sqrt{2}$ is rational) was erroneous, and $\sqrt{2}$ is actually irrational, as required.

Euclid’s theorem

Euclid’s theorem

Theorem (Euclid).

Euclid's theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Euclid's theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Proof.

Euclid's theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Proof. Assume, to the contrary, that there are only finitely many prime numbers:

Euclid's theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Proof. Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

Euclid's theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Proof. Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n \,.$$

Construct a number N

Euclid's theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Proof. Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

Euclid's theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Proof. Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

N is not divisible by any of p_1 ,

Euclid's theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Proof. Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

N is not divisible by any of p_1 , p_2 ,

Euclid's theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Proof. Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n \, .$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

N is not divisible by any of p_1 , p_2 , $\ldots$, p_n .

Euclid's theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Proof. Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n\,.$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

N is not divisible by any of p_1, p_2, $\ldots$, p_n.

Indeed,

Euclid’s theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Proof. Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

N is not divisible by any of p_1 , p_2 , $\ldots$, p_n .

Indeed, N has a remainder of 1 when divided by any of them.

Euclid's theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Proof. Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

N is not divisible by any of p_1 , p_2 , $\ldots$, p_n .

Indeed, N has a remainder of 1 when divided by any of them.

As any natural number greater than 1 , N is divisible by some prime number.

Euclid's theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Proof. Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n\,.$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

N is not divisible by any of p_1 , p_2 , $\ldots$, p_n .

Indeed, N has a remainder of 1 when divided by any of them.

As any natural number greater than 1 , N is divisible by some prime number.

By this, N should be divisible by one of the primes $p_1, p_2, \ldots, p_n$.

Euclid's theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Proof. Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

N is not divisible by any of p_1 , p_2 , $\ldots$, p_n .
Indeed, N has a remainder of 1 when divided by any of them.
As any natural number greater than 1 , N is divisible by some prime number.

By this, N should be divisible by one of the primes $p_1, p_2, \ldots, p_n$.
This contradiction shows that

Euclid's theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Proof. Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

N is not divisible by any of p_1, p_2, $\ldots$, p_n.

Indeed, N has a remainder of 1 when divided by any of them.

As any natural number greater than 1, N is divisible by some prime number.

By this, N should be divisible by one of the primes $p_1, p_2, \ldots, p_n$.
This contradiction shows that

the assumption (there are only finitely many prime numbers) was erroneous,

Euclid's theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Proof. Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

N is not divisible by any of p_1 , p_2 , $\ldots$, p_n .

Indeed, N has a remainder of 1 when divided by any of them.

As any natural number greater than 1 , N is divisible by some prime number.

By this, N should be divisible by one of the primes $p_1, p_2, \ldots, p_n$.

This contradiction shows that

the assumption (there are only finitely many prime numbers) was erroneous,

and there are infinitely many primes,

Euclid's theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Proof. Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

N is not divisible by any of p_1 , p_2 , $\ldots$, p_n .

Indeed, N has a remainder of 1 when divided by any of them.

As any natural number greater than 1 , N is divisible by some prime number.

By this, N should be divisible by one of the primes $p_1, p_2, \ldots, p_n$.

This contradiction shows that

the assumption (there are only finitely many prime numbers) was erroneous,

and there are infinitely many primes, as required.

Euclid's theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Proof. Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n\,.$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

N is not divisible by any of p_1, p_2, $\ldots$, p_n.

Indeed, N has a remainder of 1 when divided by any of them.

As any natural number greater than 1, N is divisible by some prime number.

By this, N should be divisible by one of the primes $p_1, p_2, \ldots, p_n$.

This contradiction shows that

the assumption (there are only finitely many prime numbers) was erroneous, and there are infinitely many primes, as required.

For source and comments see

Euclid's Elements, Book IX, Proposition 20.

http://aleph0.clarku.edu/ djoyce/java/elements/bookIX/propIX20.html

Proof by exhaustion (proof by cases)

Proof by exhaustion (proof by cases)

A proof by exhaustion consists of examination of every possible case.

Proof by exhaustion (proof by cases)

A proof by exhaustion consists of examination of every possible case.

Theorem about inscribed angle.

Proof by exhaustion (proof by cases)

A proof by exhaustion consists of examination of every possible case.

Theorem about inscribed angle. *An angle inscribed in a circle is half of the central angle subtending the same arc.*

Proof by exhaustion (proof by cases)

A proof by exhaustion consists of examination of every possible case.

Theorem about inscribed angle. *An angle inscribed in a circle is half of the central angle subtending the same arc.*

Proof.

Proof by exhaustion (proof by cases)

A proof by exhaustion consists of examination of every possible case.

Theorem about inscribed angle. *An angle inscribed in a circle is half of the central angle subtending the same arc.*

Proof. How an inscribed angle may be positioned with respect to the center of the circle?

Proof by exhaustion (proof by cases)

A proof by exhaustion consists of examination of every possible case.

Theorem about inscribed angle. *An angle inscribed in a circle is half of the central angle subtending the same arc.*

Proof. How an inscribed angle may be positioned with respect to the center of the circle?

Listen to the proof and try to write it down...

The triangle inequality

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a| + |b|$ *for any real numbers* a, b *.*

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a| + |b|$ *for any real numbers* a, b.

Proof

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a| + |b|$ *for any real numbers* a, b.

Proof (by cases).

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a| + |b|$ *for any real numbers* a, b *.*

Proof (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$.

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a| + |b|$ *for any real numbers* a, b *.*

Proof (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$,

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a| + |b|$ *for any real numbers* a, b *.*

Proof (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$,

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a| + |b|$ *for any real numbers* a, b*.*

Proof (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$, and, by this $|a+b| \leq |a| + |b|$.

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a| + |b|$ *for any real numbers* a, b*.*

Proof (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$, and, by this $|a+b| \leq |a| + |b|$.
- Case 2. $a \geq 0$ and $b < 0$.

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a| + |b|$ *for any real numbers* a, b*.*

Proof (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$, and, by this $|a+b| \leq |a| + |b|$.
- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$,

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a|+|b|$ *for any real numbers* a, b*.*

Proof (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a|+|b|$, and, by this $|a+b| \leq |a|+|b|$.
- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| =?$

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a|+|b|$ *for any real numbers* a, b*.*

Proof (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a|=a$, $|b|=b$, $|a+b|=a+b$, so $|a+b|=a+b=|a|+|b|$, and, by this $|a+b| \leq |a|+|b|$.
- Case 2. $a \geq 0$ and $b < 0$ .Then $|a|=a$, $|b|=-b$, $|a+b| =?$
  - Case 2a) $a+b \geq 0$.

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a|+|b|$ *for any real numbers* a, b*.*

Proof (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a|+|b|$, and, by this $|a+b| \leq |a|+|b|$.
- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| =?$
  - Case 2a) $a+b \geq 0$. Then $|a+b| = a+b < a-b = |a|+|b|$,

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a| + |b|$ *for any real numbers* a, b*.*

Proof (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$, and, by this $|a+b| \leq |a| + |b|$.
- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| =?$
  - Case 2a) $a + b \geq 0$. Then $|a+b| = a+b < a-b = |a| + |b|$, so $|a+b| \leq |a| + |b|$.

The triangle inequality

Theorem (triangle inequality). $|a+b| \le |a| + |b|$ *for any real numbers* a, b *.*

Proof (by cases).

- Case 1. $a \ge 0$ and $b \ge 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$, and, by this $|a+b| \le |a| + |b|$.
- Case 2. $a \ge 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| = ?$
  - Case 2a) $a+b \ge 0$. Then $|a+b| = a+b < a-b = |a| + |b|$, so $|a+b| \le |a| + |b|$.
  - Case 2b) $a+b < 0$.

The triangle inequality

Theorem (triangle inequality). $|a+b| \le |a| + |b|$ *for any real numbers* a, b*.*

Proof (by cases).

- Case 1. $a \ge 0$ and $b \ge 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$, and, by this $|a+b| \le |a| + |b|$.
- Case 2. $a \ge 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| = ?$
  - Case 2a) $a+b \ge 0$. Then $|a+b| = a+b < a-b = |a|+|b|$, so $|a+b| \le |a|+|b|$.
  - Case 2b) $a+b < 0$. Then $|a+b| = -a-b \le a-b = |a|+|b|$,

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a|+|b|$ *for any real numbers* a, b*.*

Proof (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a|+|b|$, and, by this $|a+b| \leq |a|+|b|$.
- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| =?$
  - Case 2a) $a+b \geq 0$. Then $|a+b| = a+b < a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.
  - Case 2b) $a+b < 0$. Then $|a+b| = -a-b \leq a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a|+|b|$ *for any real numbers* a, b *.*

Proof (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a|+|b|$, and, by this $|a+b| \leq |a|+|b|$.
- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| =?$
  - Case 2a) $a+b \geq 0$. Then $|a+b| = a+b < a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.
  - Case 2b) $a+b < 0$. Then $|a+b| = -a-b \leq a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.
- Case 3. $a < 0$ and $b \geq 0$

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a|+|b|$ *for any real numbers* a, b*.*

Proof (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a|+|b|$, and, by this $|a+b| \leq |a|+|b|$.
- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| =?$
  - Case 2a) $a+b \geq 0$. Then $|a+b| = a+b < a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.
  - Case 2b) $a+b < 0$. Then $|a+b| = -a-b \leq a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.
- Case 3. $a < 0$ and $b \geq 0$ is similar to Case 2, just swap a and b.

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a|+|b|$ *for any real numbers* a, b*.*

Proof (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a|+|b|$, and, by this $|a+b| \leq |a|+|b|$.
- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| =?$
  - Case 2a) $a+b \geq 0$. Then $|a+b| = a+b < a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.
  - Case 2b) $a+b < 0$. Then $|a+b| = -a-b \leq a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.
- Case 3. $a < 0$ and $b \geq 0$ is similar to Case 2, just swap a and b.
- Case 4. $a < 0$ and $b < 0$.

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a| + |b|$ *for any real numbers* a, b*.*

Proof (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$, and, by this $|a+b| \leq |a| + |b|$.
- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| = ?$
  - Case 2a) $a+b \geq 0$. Then $|a+b| = a+b < a-b = |a| + |b|$, so $|a+b| \leq |a| + |b|$.
  - Case 2b) $a+b < 0$. Then $|a+b| = -a-b \leq a-b = |a| + |b|$, so $|a+b| \leq |a| + |b|$.
- Case 3. $a < 0$ and $b \geq 0$ is similar to Case 2, just swap a and b.
- Case 4. $a < 0$ and $b < 0$ .Then $|a| = -a$, $|b| = -b$, $|a+b| = -a-b$,

The triangle inequality

Theorem (triangle inequality). $|a+b| \le |a| + |b|$ *for any real numbers* a, b*.*

Proof (by cases).

- Case 1. $a \ge 0$ and $b \ge 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$, and, by this $|a+b| \le |a| + |b|$.
- Case 2. $a \ge 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| =?$
  - Case 2a) $a+b \ge 0$. Then $|a+b| = a+b < a-b = |a| + |b|$, so $|a+b| \le |a| + |b|$.
  - Case 2b) $a+b < 0$. Then $|a+b| = -a-b \le a-b = |a| + |b|$, so $|a+b| \le |a| + |b|$.
- Case 3. $a < 0$ and $b \ge 0$ is similar to Case 2, just swap a and b.
- Case 4. $a < 0$ and $b < 0$ .Then $|a| = -a$, $|b| = -b$, $|a+b| = -a-b$, so $|a+b| = -a-b = |a| + |b|$,

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a| + |b|$ *for any real numbers* a, b *.*

Proof (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$, and, by this $|a+b| \leq |a| + |b|$.
- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| = ?$
  - Case 2a) $a+b \geq 0$. Then $|a+b| = a+b < a-b = |a| + |b|$, so $|a+b| \leq |a| + |b|$.
  - Case 2b) $a+b < 0$. Then $|a+b| = -a-b \leq a-b = |a| + |b|$, so $|a+b| \leq |a| + |b|$.
- Case 3. $a < 0$ and $b \geq 0$ is similar to Case 2, just swap a and b .
- Case 4. $a < 0$ and $b < 0$ .Then $|a| = -a$, $|b| = -b$, $|a+b| = -a-b$, so $|a+b| = -a-b = |a| + |b|$, and, by this $|a+b| \leq |a| + |b|$.

The triangle inequality

Theorem (triangle inequality). $|a+b| \le |a| + |b|$ *for any real numbers* a, b *.*

Proof (by cases).

- Case 1. $a \ge 0$ and $b \ge 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$, and, by this $|a+b| \le |a| + |b|$.
- Case 2. $a \ge 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| =?$
  - Case 2a) $a+b \ge 0$. Then $|a+b| = a+b < a-b = |a| + |b|$, so $|a+b| \le |a| + |b|$.
  - Case 2b) $a+b < 0$. Then $|a+b| = -a-b \le a-b = |a| + |b|$, so $|a+b| \le |a| + |b|$.
- Case 3. $a < 0$ and $b \ge 0$ is similar to Case 2, just swap a and b .
- Case 4. $a < 0$ and $b < 0$ .Then $|a| = -a$, $|b| = -b$, $|a+b| = -a-b$, so $|a+b| = -a-b = |a| + |b|$, and, by this $|a+b| \le |a| + |b|$.

Therefore, $|a+b| \le |a| + |b|$ for all real numbers a and b ,

The triangle inequality

Theorem (triangle inequality). $|a+b| \leq |a| + |b|$ *for any real numbers* a, b.

Proof (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$, and, by this $|a+b| \leq |a| + |b|$.
- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| =?$
  - Case 2a) $a+b \geq 0$. Then $|a+b| = a+b < a-b = |a| + |b|$, so $|a+b| \leq |a| + |b|$.
  - Case 2b) $a+b < 0$. Then $|a+b| = -a-b \leq a-b = |a| + |b|$, so $|a+b| \leq |a| + |b|$.
- Case 3. $a < 0$ and $b \geq 0$ is similar to Case 2, just swap a and b.
- Case 4. $a < 0$ and $b < 0$ .Then $|a| = -a$, $|b| = -b$, $|a+b| = -a-b$, so $|a+b| = -a-b = |a| + |b|$, and, by this $|a+b| \leq |a| + |b|$.

Therefore, $|a+b| \leq |a| + |b|$ for all real numbers a and b, as required.

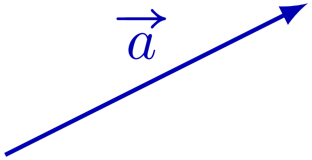
The triangle inequality

The triangle inequality

Why the inequality $|a+b| \leq |a| + |b|$ is called the triangle inequality?

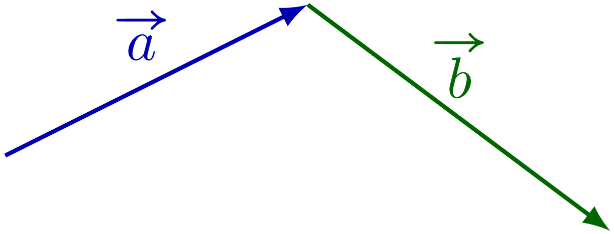
The triangle inequality

Why the inequality $|a+b| \leq |a| + |b|$ is called the triangle inequality?



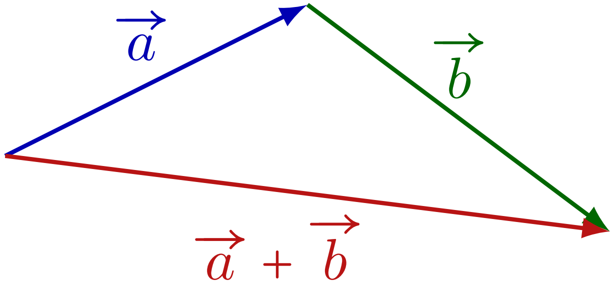
The triangle inequality

Why the inequality $|a+b| \leq |a| + |b|$ is called the triangle inequality?



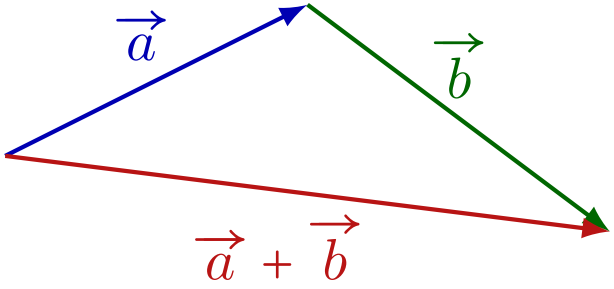
The triangle inequality

Why the inequality $|a+b| \leq |a| + |b|$ is called the triangle inequality?



The triangle inequality

Why the inequality $|a+b| \leq |a| + |b|$ is called the triangle inequality?



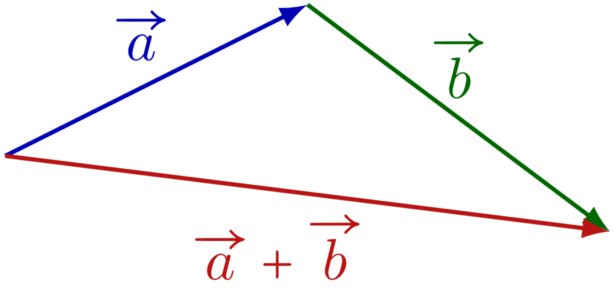
$$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$$

.

.

The triangle inequality

Why the inequality $|a+b| \leq |a| + |b|$ is called the triangle inequality?



$$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$$

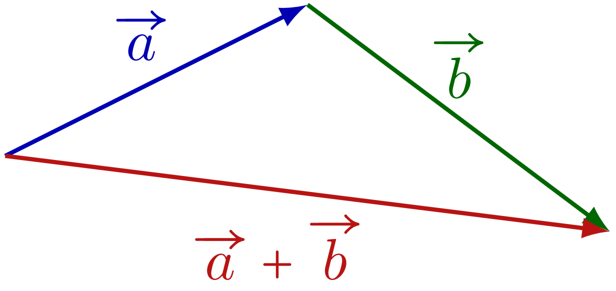
Corollary 1. $|a-b| \leq |a| + |b|$ for all $a, b \in \mathbb{R}$.

.

.

The triangle inequality

Why the inequality $|a+b| \le |a| + |b|$ is called the triangle inequality?



$$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$$

Corollary 1. $|a-b| \le |a| + |b|$ for all $a, b \in \mathbb{R}$.

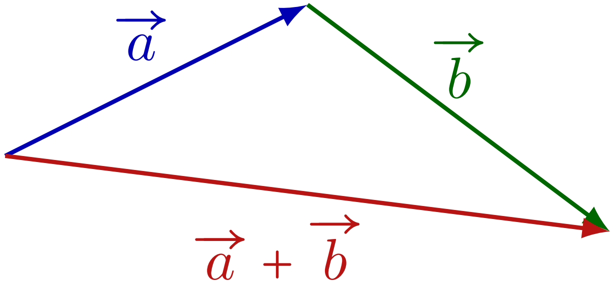
Proof. Apply the triangle inequality to a and $-b$:

.

.

The triangle inequality

Why the inequality $|a+b| \le |a| + |b|$ is called the triangle inequality?



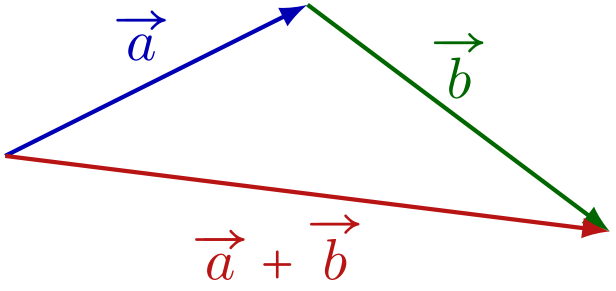
$$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$$

Corollary 1. $|a-b| \le |a| + |b|$ for all $a, b \in \mathbb{R}$.

Proof. Apply the triangle inequality to a and $-b$:
$|a + (-b)| \le |a| + |-b|$.

The triangle inequality

Why the inequality $|a+b| \le |a| + |b|$ is called the triangle inequality?



$$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$$

Corollary 1. $|a-b| \le |a| + |b|$ for all $a, b \in \mathbb{R}$.

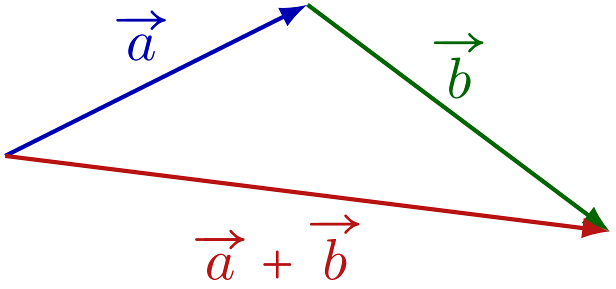
Proof. Apply the triangle inequality to a and $-b$:
$|a + (-b)| \le |a| + |-b|$.
Since $a + (-b) = a - b$ and $|-b| = |b|$,

.

.

The triangle inequality

Why the inequality $|a+b| \leq |a|+|b|$ is called the triangle inequality?



$$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$$

Corollary 1. $|a-b| \leq |a|+|b|$ for all $a, b \in \mathbb{R}$.

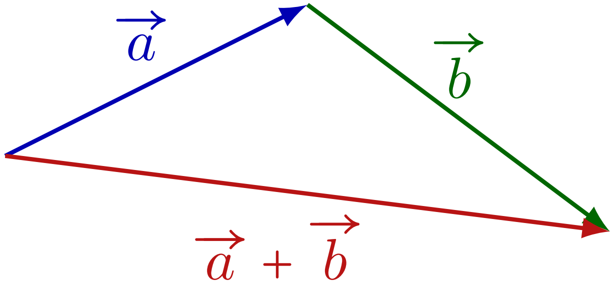
Proof. Apply the triangle inequality to a and $-b$:
$|a+(-b)| \leq |a| + |-b|$.
Since $a+(-b) = a-b$ and $|-b| = |b|$,
we have got $|a-b| \leq |a|+|b|$, as required.

.

.

The triangle inequality

Why the inequality $|a+b| \le |a| + |b|$ is called the triangle inequality?



$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$

Corollary 1. $|a-b| \le |a| + |b|$ for all $a, b \in \mathbb{R}$.

Proof. Apply the triangle inequality to a and $-b$:
$|a+(-b)| \le |a| + |-b|$.
Since $a + (-b) = a - b$ and $|-b| = |b|$,
we have got $|a-b| \le |a| + |b|$, as required.

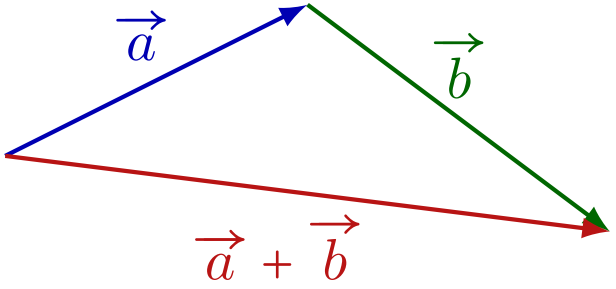
Corollary 2. $||a| - |b|| \le |a-b|$ for all $a, b \in \mathbb{R}$.

.

.

The triangle inequality

Why the inequality $|a+b| \le |a| + |b|$ is called the triangle inequality?



$$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$$

Corollary 1. $|a-b| \le |a| + |b|$ for all $a, b \in \mathbb{R}$.

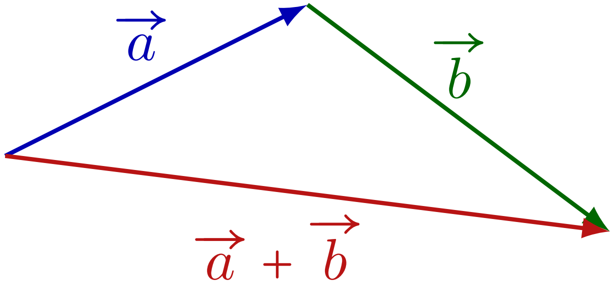
Proof. Apply the triangle inequality to a and $-b$:
$|a + (-b)| \le |a| + |-b|$.
Since $a + (-b) = a - b$ and $|-b| = |b|$,
we have got $|a-b| \le |a| + |b|$, as required.

Corollary 2. $||a| - |b|| \le |a-b|$ for all $a, b \in \mathbb{R}$.

Proof. $|a| = |(a-b) + b|$

The triangle inequality

Why the inequality $|a+b| \le |a| + |b|$ is called the triangle inequality?



$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$

Corollary 1. $|a-b| \le |a| + |b|$ for all $a, b \in \mathbb{R}$.

Proof. Apply the triangle inequality to a and $-b$:
$|a+(-b)| \le |a| + |-b|$.
Since $a + (-b) = a - b$ and $|-b| = |b|$,
we have got $|a-b| \le |a| + |b|$, as required.

Corollary 2. $||a| - |b|| \le |a-b|$ for all $a, b \in \mathbb{R}$.

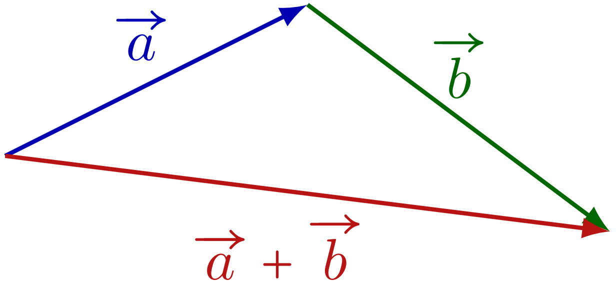
Proof. $|a| = |(a-b)+b| \le |a-b| + |b|$

.

.

The triangle inequality

Why the inequality $|a+b| \le |a| + |b|$ is called the triangle inequality?



$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$

Corollary 1. $|a-b| \le |a| + |b|$ for all $a, b \in \mathbb{R}$.

Proof. Apply the triangle inequality to a and $-b$:
$|a + (-b)| \le |a| + |-b|$.
Since $a + (-b) = a - b$ and $|-b| = |b|$,
we have got $|a-b| \le |a| + |b|$, as required.

Corollary 2. $||a| - |b|| \le |a-b|$ for all $a, b \in \mathbb{R}$.

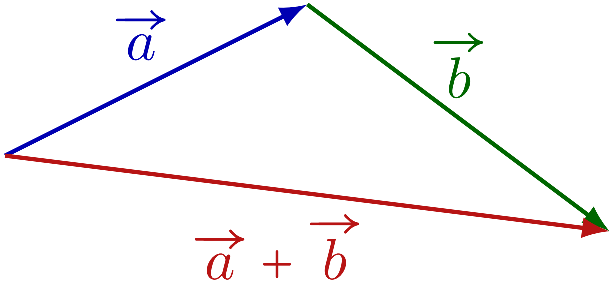
Proof. $|a| = |(a-b) + b| \le |a-b| + |b| \implies |a| - |b| \le |a-b|$.

.

.

The triangle inequality

Why the inequality $|a+b| \le |a| + |b|$ is called the triangle inequality?



$$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$$

Corollary 1. $|a-b| \le |a| + |b|$ for all $a, b \in \mathbb{R}$.

Proof. Apply the triangle inequality to a and $-b$:
$|a+(-b)| \le |a| + |-b|$.
Since $a+(-b) = a-b$ and $|-b| = |b|$,
we have got $|a-b| \le |a| + |b|$, as required.

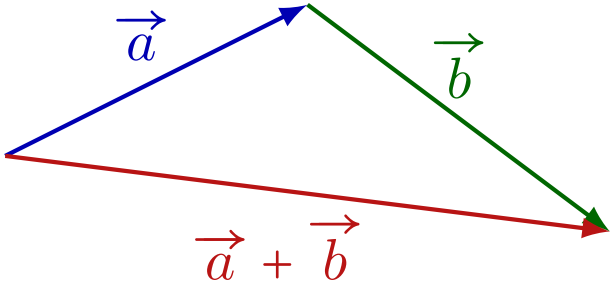
Corollary 2. $||a| - |b|| \le |a-b|$ for all $a, b \in \mathbb{R}$.

Proof. $|a| = |(a-b)+b| \le |a-b| + |b| \implies |a| - |b| \le |a-b|$.
$|b| = |(b-a)+a| \le |b-a| + |a| \implies |a| - |b| \ge -|a-b|$.

.

The triangle inequality

Why the inequality $|a+b| \leq |a| + |b|$ is called the triangle inequality?



$$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$$

Corollary 1. $|a-b| \leq |a| + |b|$ for all $a, b \in \mathbb{R}$.

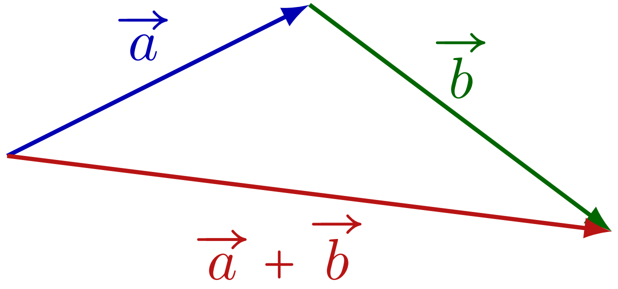
Proof. Apply the triangle inequality to a and $-b$:
$|a+(-b)| \leq |a| + |-b|$.
Since $a+(-b) = a-b$ and $|-b| = |b|$,
we have got $|a-b| \leq |a| + |b|$, as required.

Corollary 2. $||a| - |b|| \leq |a-b|$ for all $a, b \in \mathbb{R}$.

Proof. $|a| = |(a-b)+b| \leq |a-b| + |b| \implies |a| - |b| \leq |a-b|$.
$|b| = |(b-a)+a| \leq |b-a| + |a| \implies |a| - |b| \geq -|a-b|$.
Therefore, $-|a-b| \leq |a| - |b| \leq |a-b|$.

The triangle inequality

Why the inequality $|a+b| \leq |a| + |b|$ is called the triangle inequality?



$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$

Corollary 1. $|a-b| \leq |a| + |b|$ for all $a, b \in \mathbb{R}$.

Proof. Apply the triangle inequality to a and $-b$:
$|a+(-b)| \leq |a| + |-b|$.
Since $a+(-b) = a-b$ and $|-b| = |b|$,
we have got $|a-b| \leq |a| + |b|$, as required.

Corollary 2. $||a|-|b|| \leq |a-b|$ for all $a, b \in \mathbb{R}$.

Proof. $|a| = |(a-b)+b| \leq |a-b| + |b| \implies |a| - |b| \leq |a-b|$.
$|b| = |(b-a)+a| \leq |b-a| + |a| \implies |a| - |b| \geq -|a-b|$.
Therefore, $-|a-b| \leq |a| - |b| \leq |a-b|$. Hence $||a|-|b|| \leq |a-b|$, as required.

The triangle inequality, another proof

Let us give another proof of the triangle inequality.

The triangle inequality, another proof

Let us give another proof of the triangle inequality.

For any real numbers a and b, we have

The triangle inequality, another proof

Let us give another proof of the triangle inequality.

For any real numbers a and b, we have

$(a+b)^2 = a^2 + b^2 + 2ab$

The triangle inequality, another proof

Let us give another proof of the triangle inequality.

For any real numbers a and b, we have

$$(a+b)^2 = a^2 + b^2 + 2ab \underbrace{\leq}_{ab \leq |ab|} a^2 + b^2 + 2|ab|$$

The triangle inequality, another proof

Let us give another proof of the triangle inequality.

For any real numbers a and b, we have

$$(a+b)^2 = a^2 + b^2 + 2ab \underbrace{\leq}_{ab \leq |ab|} a^2 + b^2 + 2|ab| = |a|^2 + |b|^2 + 2|a||b|$$

The triangle inequality, another proof

Let us give another proof of the triangle inequality.

For any real numbers a and b, we have

$$(a+b)^2 = a^2 + b^2 + 2ab \underbrace{\leq}_{ab \leq |ab|} a^2 + b^2 + 2|ab| = |a|^2 + |b|^2 + 2|a||b| = (|a| + |b|)^2 \, .$$

The triangle inequality, another proof

Let us give another proof of the triangle inequality.

For any real numbers a and b, we have

$$(a+b)^2 = a^2 + b^2 + 2ab \underbrace{\leq}_{ab \leq |ab|} a^2 + b^2 + 2|ab| = |a|^2 + |b|^2 + 2|a||b| = (|a| + |b|)^2 .$$

Therefore, $(a+b)^2 \leq (|a| + |b|)^2$.

The triangle inequality, another proof

Let us give another proof of the triangle inequality.

For any real numbers a and b, we have

$$(a+b)^2 = a^2 + b^2 + 2ab \underbrace{\leq}_{ab \leq |ab|} a^2 + b^2 + 2|ab| = |a|^2 + |b|^2 + 2|a||b| = (|a| + |b|)^2 .$$

Therefore, $(a+b)^2 \leq (|a| + |b|)^2$. From this we get

The triangle inequality, another proof

Let us give another proof of the triangle inequality.

For any real numbers a and b, we have

$$(a+b)^2 = a^2 + b^2 + 2ab \underbrace{\leq}_{ab \leq |ab|} a^2 + b^2 + 2|ab| = |a|^2 + |b|^2 + 2|a||b| = (|a| + |b|)^2 .$$

Therefore, $(a+b)^2 \leq (|a| + |b|)^2$. From this we get

$$\sqrt{(a+b)^2} \leq \sqrt{(|a| + |b|)^2} ,$$

The triangle inequality, another proof

Let us give another proof of the triangle inequality.

For any real numbers a and b, we have

$$(a+b)^2 = a^2+b^2+2ab \underbrace{\leq}_{ab\leq|ab|} a^2+b^2+2|ab| = |a|^2+|b|^2+2|a||b| = (|a|+|b|)^2 .$$

Therefore, $(a+b)^2 \leq (|a|+|b|)^2$. From this we get

$\sqrt{(a+b)^2} \leq \sqrt{(|a|+|b|)^2}$, which implies

$|a+b| \leq ||a|+|b||$.

The triangle inequality, another proof

Let us give another proof of the triangle inequality.

For any real numbers a and b, we have

$$(a+b)^2 = a^2+b^2+2ab \underbrace{\leq}_{ab\leq|ab|} a^2+b^2+2|ab| = |a|^2+|b|^2+2|a||b| = (|a|+|b|)^2 .$$

Therefore, $(a+b)^2 \leq (|a|+|b|)^2$. From this we get

$\sqrt{(a+b)^2} \leq \sqrt{(|a|+|b|)^2}$, which implies

$|a+b| \leq ||a|+|b||$.

Since $||a|+|b|| = |a|+|b|$,

The triangle inequality, another proof

Let us give another proof of the triangle inequality.

For any real numbers a and b, we have

$$(a+b)^2 = a^2 + b^2 + 2ab \underbrace{\leq}_{ab \leq |ab|} a^2 + b^2 + 2|ab| = |a|^2 + |b|^2 + 2|a||b| = (|a| + |b|)^2 .$$

Therefore, $(a+b)^2 \leq (|a| + |b|)^2$. From this we get

$\sqrt{(a+b)^2} \leq \sqrt{(|a| + |b|)^2}$, which implies

$|a+b| \leq ||a| + |b||$.

Since $||a| + |b|| = |a| + |b|$, we get $|a+b| \leq |a| + |b|$.

How to prove an equivalence

How to prove an equivalence

To prove a statement of type $P \iff Q$,

How to prove an equivalence

To prove a statement of type $P \iff Q$, we may use one of two alternatives:

How to prove an equivalence

To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: P

How to prove an equivalence

To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R$

How to prove an equivalence

To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S$

How to prove an equivalence

To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

How to prove an equivalence

To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$

How to prove an equivalence

To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

How to prove an equivalence

To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

Example 1.

How to prove an equivalence

To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

Example 1. Let a, b, c be the lengths of the sides of a triangle

How to prove an equivalence

To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

Example 1. Let a, b, c be the lengths of the sides of a triangle and $a \leq b \leq c$.

How to prove an equivalence

To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

Example 1. Let a, b, c be the lengths of the sides of a triangle and $a \leq b \leq c$. Using the law of cosines, prove that the triangle is right if and only if $a^2 + b^2 = c^2$.

How to prove an equivalence

To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

Example 1. Let a, b, c be the lengths of the sides of a triangle and $a \leq b \leq c$. Using the law of cosines, prove that the triangle is right if and only if $a^2 + b^2 = c^2$.

Proof. What is the law of cosines?

How to prove an equivalence

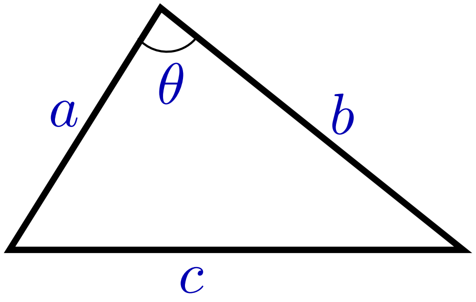
To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

Example 1. Let a, b, c be the lengths of the sides of a triangle and $a \leq b \leq c$. Using the law of cosines, prove that the triangle is right if and only if $a^2 + b^2 = c^2$.

Proof. What is the law of cosines?



How to prove an equivalence

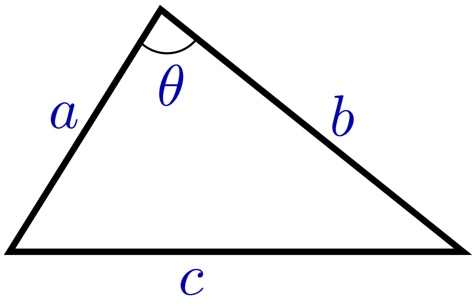
To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

Example 1. Let a, b, c be the lengths of the sides of a triangle and $a \leq b \leq c$. Using the law of cosines, prove that the triangle is right if and only if $a^2 + b^2 = c^2$.

Proof. What is the law of cosines?



$$c^2 = a^2 + b^2 - 2ab\cos\theta$$

How to prove an equivalence

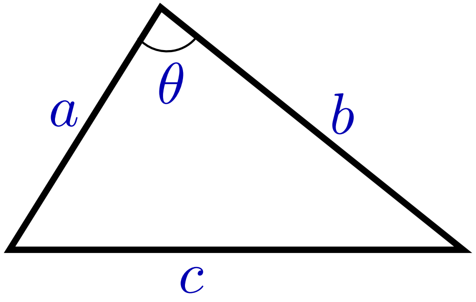
To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

Example 1. Let a, b, c be the lengths of the sides of a triangle and $a \le b \le c$. Using the law of cosines, prove that the triangle is right if and only if $a^2 + b^2 = c^2$.

Proof. What is the law of cosines?



$$c^2 = a^2 + b^2 - 2ab\cos\theta$$

A triangle with the sides a, b, c is right

How to prove an equivalence

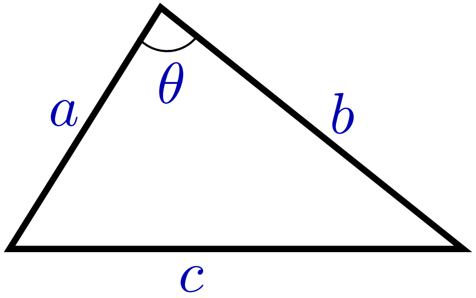
To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

Example 1. Let a, b, c be the lengths of the sides of a triangle and $a \leq b \leq c$. Using the law of cosines, prove that the triangle is right if and only if $a^2 + b^2 = c^2$.

Proof. What is the law of cosines?



$$c^2 = a^2 + b^2 - 2ab\cos\theta$$

A triangle with the sides a, b, c is right $\underset{?}{\iff}$ $\theta = 90^\circ$

How to prove an equivalence

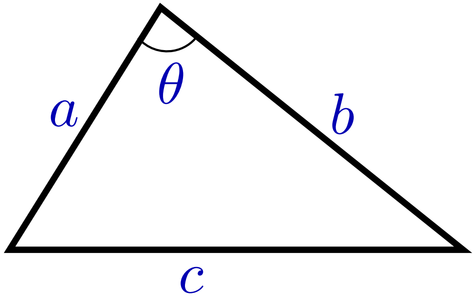
To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

Example 1. Let a, b, c be the lengths of the sides of a triangle and $a \le b \le c$. Using the law of cosines, prove that the triangle is right if and only if $a^2 + b^2 = c^2$.

Proof. What is the law of cosines?



$$c^2 = a^2 + b^2 - 2ab\cos\theta$$

A triangle with the sides a, b, c is right $\underset{?}{\iff}$ $\theta = 90^\circ$ $\underset{?}{\iff}$ $\cos\theta = 0$

How to prove an equivalence

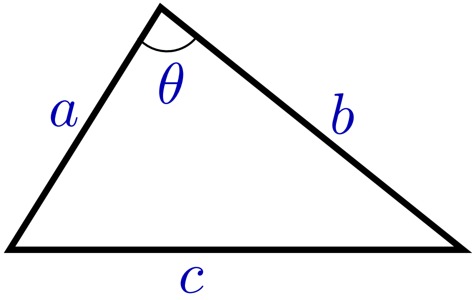
To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

Example 1. Let a, b, c be the lengths of the sides of a triangle and $a \leq b \leq c$. Using the law of cosines, prove that the triangle is right if and only if $a^2 + b^2 = c^2$.

Proof. What is the law of cosines?



$$c^2 = a^2 + b^2 - 2ab\cos\theta$$

A triangle with the sides a, b, c is right $\underset{?}{\iff}$ $\theta = 90^\circ$ $\underset{?}{\iff}$ $\cos\theta = 0$

$$\underset{?}{\iff} c^2 = a^2 + b^2 .$$

An integer and its cube have the same parity

An integer and its cube have the same parity

Example 2. Let n be an integer.

An integer and its cube have the same parity

Example 2. Let n be an integer. Prove that n is even iff n^3 is even.

An integer and its cube have the same parity

Example 2. Let n be an integer. Prove that n is even iff n^3 is even.

Proof. Let us prove first that

$$n \text{ is even } \implies n^3 \text{ is even.}$$

An integer and its cube have the same parity

Example 2. Let n be an integer. Prove that n is even iff n^3 is even.

Proof. Let us prove first that

$$n \text{ is even } \implies n^3 \text{ is even.}$$

Let n be even,

An integer and its cube have the same parity

Example 2. Let n be an integer. Prove that n is even iff n^3 is even.

Proof. Let us prove first that

$$n \text{ is even} \implies n^3 \text{ is even.}$$

Let n be even, so $n = 2k$ for some $k \in \mathbb{Z}$.

An integer and its cube have the same parity

Example 2. Let n be an integer. Prove that n is even iff n^3 is even.

Proof. Let us prove first that

$$n \text{ is even } \implies n^3 \text{ is even.}$$

Let n be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$,

An integer and its cube have the same parity

Example 2. Let n be an integer. Prove that n is even iff n^3 is even.

Proof. Let us prove first that

$$n \text{ is even } \implies n^3 \text{ is even.}$$

Let n be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

An integer and its cube have the same parity

Example 2. Let n be an integer. Prove that n is even iff n^3 is even.

Proof. Let us prove first that

$$n \text{ is even} \implies n^3 \text{ is even.}$$

Let n be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even} \implies n \text{ is even.}$$

An integer and its cube have the same parity

Example 2. Let n be an integer. Prove that n is even iff n^3 is even.

Proof. Let us prove first that

$$n \text{ is even } \implies n^3 \text{ is even.}$$

Let n be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even } \implies n \text{ is even.}$$

Assume that n is odd.

An integer and its cube have the same parity

Example 2. Let n be an integer. Prove that n is even iff n^3 is even.

Proof. Let us prove first that

$$n \text{ is even} \implies n^3 \text{ is even.}$$

Let n be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even} \implies n \text{ is even.}$$

Assume that n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$.

An integer and its cube have the same parity

Example 2. Let n be an integer. Prove that n is even iff n^3 is even.

Proof. Let us prove first that

$$n \text{ is even} \implies n^3 \text{ is even.}$$

Let n be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even} \implies n \text{ is even.}$$

Assume that n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. In this case,
$n^3 = (2k + 1)^3 =$

An integer and its cube have the same parity

Example 2. Let n be an integer. Prove that n is even iff n^3 is even.

Proof. Let us prove first that

$$n \text{ is even} \implies n^3 \text{ is even.}$$

Let n be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even} \implies n \text{ is even.}$$

Assume that n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. In this case,
$n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1$

An integer and its cube have the same parity

Example 2. Let n be an integer. Prove that n is even iff n^3 is even.

Proof. Let us prove first that

$$n \text{ is even } \implies n^3 \text{ is even.}$$

Let n be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even } \implies n \text{ is even.}$$

Assume that n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. In this case, $n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$,

An integer and its cube have the same parity

Example 2. Let n be an integer. Prove that n is even iff n^3 is even.

Proof. Let us prove first that

$$n \text{ is even } \implies n^3 \text{ is even.}$$

Let n be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even } \implies n \text{ is even.}$$

Assume that n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. In this case, $n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$, which is odd.

An integer and its cube have the same parity

Example 2. Let n be an integer. Prove that n is even iff n^3 is even.

Proof. Let us prove first that

$$n \text{ is even} \implies n^3 \text{ is even.}$$

Let n be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even} \implies n \text{ is even.}$$

Assume that n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. In this case, $n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$, which is odd.
We have got that n is odd $\implies$ n^3 is odd.

An integer and its cube have the same parity

Example 2. Let n be an integer. Prove that n is even iff n^3 is even.

Proof. Let us prove first that

$$n \text{ is even } \implies n^3 \text{ is even.}$$

Let n be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even } \implies n \text{ is even.}$$

Assume that n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. In this case, $n^3 = (2k + 1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$, which is odd. We have got that n is odd $\implies$ n^3 is odd. Therefore, by contraposition,

An integer and its cube have the same parity

Example 2. Let n be an integer. Prove that n is even iff n^3 is even.

Proof. Let us prove first that

$$n \text{ is even } \implies n^3 \text{ is even.}$$

Let n be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even } \implies n \text{ is even.}$$

Assume that n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. In this case, $n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$, which is odd. We have got that n is odd $\implies n^3$ is odd. Therefore, by contraposition,

$$n^3 \text{ is even } \implies n \text{ is even.}$$

An integer and its cube have the same parity

Example 2. Let n be an integer. Prove that n is even iff n^3 is even.

Proof. Let us prove first that

$$n \text{ is even } \implies n^3 \text{ is even.}$$

Let n be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even } \implies n \text{ is even.}$$

Assume that n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. In this case, $n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$, which is odd. We have got that n is odd $\implies$ n^3 is odd. Therefore, by contraposition,

$$n^3 \text{ is even } \implies n \text{ is even.}$$

qed

How to prove uniqueness

How to prove uniqueness

In order to prove that an object is unique,

How to prove uniqueness

In order to prove that an object is unique,

one assumes that there are two such objects

How to prove uniqueness

In order to prove that an object is unique,
one assumes that there are two such objects
and come to a conclusion that they have to be equal.

How to prove uniqueness

In order to prove that an object is unique,
one assumes that there are two such objects
and come to a conclusion that they have to be equal.

Example.

How to prove uniqueness

In order to prove that an object is unique, one assumes that there are two such objects and come to a conclusion that they have to be equal.

Example. Prove that in any ring, the additive identity is unique.

How to prove uniqueness

In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

Example. Prove that in any ring, the additive identity is unique.

Proof.

How to prove uniqueness

In order to prove that an object is unique, one assumes that there are two such objects and come to a conclusion that they have to be equal.

Example. Prove that in any ring, the additive identity is unique.

Proof. Assume that there are two additive identities,

How to prove uniqueness

In order to prove that an object is unique, one assumes that there are two such objects and come to a conclusion that they have to be equal.

Example. Prove that in any ring, the additive identity is unique.

Proof. Assume that there are two additive identities, 0 and $0'$.

How to prove uniqueness

In order to prove that an object is unique, one assumes that there are two such objects and come to a conclusion that they have to be equal.

Example. Prove that in any ring, the additive identity is unique.

Proof. Assume that there are two additive identities, 0 and $0'$. Then

How to prove uniqueness

In order to prove that an object is unique, one assumes that there are two such objects and come to a conclusion that they have to be equal.

Example. Prove that in any ring, the additive identity is unique.

Proof. Assume that there are two additive identities, 0 and $0'$. Then

$0' = 0' + 0$

How to prove uniqueness

In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

Example. Prove that in any ring, the additive identity is unique.

Proof. Assume that there are two additive identities, 0 and $0'$. Then

$0' = 0' + 0$ since $a = a + 0$ for any element a in the ring

How to prove uniqueness

In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

Example. Prove that in any ring, the additive identity is unique.

Proof. Assume that there are two additive identities, 0 and $0'$. Then

$0' = 0' + 0$ since $a = a + 0$ for any element a in the ring

$= 0 + 0'$

How to prove uniqueness

In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

Example. Prove that in any ring, the additive identity is unique.

Proof. Assume that there are two additive identities, 0 and $0'$. Then

$0' = 0' + 0$ since $a = a + 0$ for any element a in the ring

$= 0 + 0'$ by commutativity of addition in the ring

How to prove uniqueness

In order to prove that an object is unique,
one assumes that there are two such objects
and come to a conclusion that they have to be equal.

Example. Prove that in any ring, the additive identity is unique.

Proof. Assume that there are two additive identities, 0 and $0'$. Then

$0' = 0' + 0$ since $a = a + 0$ for any element a in the ring

$= 0 + 0'$ by commutativity of addition in the ring

$= 0$

How to prove uniqueness

In order to prove that an object is unique, one assumes that there are two such objects and come to a conclusion that they have to be equal.

Example. Prove that in any ring, the additive identity is unique.

Proof. Assume that there are two additive identities, 0 and $0'$. Then

$0' = 0' + 0$ since $a = a + 0$ for any element a in the ring

$= 0 + 0'$ by commutativity of addition in the ring

$= 0$ since $0'$ is an additive identity:

How to prove uniqueness

In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

Example. Prove that in any ring, the additive identity is unique.

Proof. Assume that there are two additive identities, 0 and $0'$. Then

$0' = 0' + 0$ since $a = a + 0$ for any element a in the ring

$= 0 + 0'$ by commutativity of addition in the ring

$= 0$ since $0'$ is an additive identity: $a + 0' = a$ for any a in the ring.

How to prove uniqueness

In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

Example. Prove that in any ring, the additive identity is unique.

Proof. Assume that there are two additive identities, 0 and $0'$. Then

$0' = 0' + 0$ since $a = a + 0$ for any element a in the ring

$= 0 + 0'$ by commutativity of addition in the ring

$= 0$ since $0'$ is an additive identity: $a + 0' = a$ for any a in the ring.

Therefore, $0' = 0$.

How to prove uniqueness

In order to prove that an object is unique, one assumes that there are two such objects and come to a conclusion that they have to be equal.

Example. Prove that in any ring, the additive identity is unique.

Proof. Assume that there are two additive identities, 0 and $0'$. Then

$0' = 0' + 0$ since $a = a + 0$ for any element a in the ring

$= 0 + 0'$ by commutativity of addition in the ring

$= 0$ since $0'$ is an additive identity: $a + 0' = a$ for any a in the ring.

Therefore, $0' = 0$.

qed

Strategies for constructing proofs

Strategies for constructing proofs

- Understand what is given and what is to be proven.

Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication,

Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)

Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given) and conclusion (what should be proven).

Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.

Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math.

Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.

Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.

Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:

Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given) and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:
  1. *Affirming the consequent*

Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:
  1. *Affirming the consequent*
     Prove $P \implies Q$.

Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given) and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:
  1. *Affirming the consequent*
     Prove $P \implies Q$.
     "Proof." Let $Q \ldots$

Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given) and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:
  1. *Affirming the consequent*
     Prove $P \implies Q$.
     "Proof." Let $Q \ldots$
  2. *Denying the antecedent*

Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:
  1. *Affirming the consequent*
     Prove $P \implies Q$.
     "Proof." Let $Q \dots$
  2. *Denying the antecedent*
     Prove $P \implies Q$.

Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:
  1. *Affirming the consequent*
     Prove $P \implies Q$.
     "Proof." Let $Q \dots$
  2. *Denying the antecedent*
     Prove $P \implies Q$.
     "Proof." Let $\neg P \dots$

Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:
  1. *Affirming the consequent*
  Prove $P \implies Q$.
  "Proof." Let $Q \ldots$

  2. *Denying the antecedent*
  Prove $P \implies Q$.
  "Proof." Let $\neg P \ldots$

  3. *Guilt by assumption* (proof by example)

Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given) and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:
  1. *Affirming the consequent*
     Prove $P \implies Q$.
     "Proof." Let $Q \ldots$
  2. *Denying the antecedent*
     Prove $P \implies Q$.
     "Proof." Let $\neg P \ldots$
  3. *Guilt by assumption* (proof by example)
     $\exists x\, P(x) \implies \forall x\, P(x)$