# Lesson 2

## Proofs and induction
## Irrationality of $\sqrt{2}$

MATH 311, Section 4, FALL 2022

September 9th, 2022

# Three principles

## Well ordering principle (A)

If $A$ is a non-empty subset of non-negative integers $\mathbb{N}_0$, then $A$ contains the smallest number.

## The principle of induction (B)

If $A$ is a subset of non-negative integers $\mathbb{N}_0$ such that

- A. (Base step): $0 \in A$.
- B. (Induction step): Whenever $A$ contains a number $n$, it also contains the number $n + 1$.

Then $A = \mathbb{N}_0$.

## The maximum principle (C)

A non-empty subset of $\mathbb{N}_0$, which is bounded from above contains the greatest number.

# Our goal

Our goal is to prove that the statements (A), (B), and (C) are equivalent. In order to prove that, we will show:

1. (A) $\Rightarrow$ (B)
2. (B) $\Rightarrow$ (A)
3. (A) $\Rightarrow$ (C)
4. (C) $\Rightarrow$ (A)

# (A) $\Rightarrow$ (B)

If $A$ is a set of non-negative integers such that

1. $0 \in A$.
2. Whenever $A$ contains a number $n$, it also contains $n+1$.

We want to establish $A = \mathbb{N}_0$. Suppose for contradiction that $A \neq \mathbb{N}_0$. Then $\mathbb{N}_0 \setminus A \neq \emptyset$. By well ordering principle (B) there is the smallest element $m$ of $\mathbb{N}_0 \setminus A$.

1. Since $0 \in A$, we have $m \neq 0$,
2. Observe that $m-1 \in A$, because otherwise $m-1 \in \mathbb{N}_0 \setminus A$, which contradicts the fact that $m$ is the smallest element of $\mathbb{N}_0 \setminus A$. **But if** $m-1 \in A$**, then by (2) we have** $m \in A$, which is impossible.

The implication (A) $\Rightarrow$ (B) follows.

# (B) $\Rightarrow$ (A)

Let $A \subseteq \mathbb{N}_0 = \{0, 1, 2, \ldots\}$ such that $A \neq \emptyset$. Suppose for contradiction that $A$ does not have a least element.

- It is easy to see that $0 \notin A$, because otherwise it would be a minimal element of $A$ (as 0 is the minimal element of $\mathbb{N}_0$).
- We also see $1 \notin A$, otherwise it is a minimal element of $A$.
- We continue and assume that $1, 2, \ldots, n \notin A$. Then $n + 1 \notin A$, otherwise $n + 1$ is the smallest element of $A$.

Now use the principle of induction and conclude that $A = \emptyset$.

# (A) $\Rightarrow$ (C)

Suppose that $A \neq \emptyset$ and bounded.

$$\underbrace{\exists}_{\text{there exists}} \quad M \in \mathbb{N}_0 \quad \underbrace{\forall}_{\text{for all}} a \in A \;\; a \leq M$$

This means that $M - a \geq 0$ for all $a \in A$. Let us consider the set

$$B = \{M - a \;:\; a \in A\} \neq \emptyset.$$

By the well ordering principle (A) there is $b \in A$ such that $M - b$ is the smallest element of $B$.
Thus

$$M - b \leq M - a$$

for all $a \in A$, equivalently $a \leq b$ for all $a \in A$.

# (C) $\Rightarrow$ (A)

Let $A \subseteq \mathbb{N}_0$, $A \neq \emptyset$. We show that $A$ has a minimal element. Let

$$B = \{n \in \mathbb{N}_0 \ : \ n \leq a \text{ for every } a \in A\} = \{n \in \mathbb{N}_0 \ : \ \forall a \in A \ n \leq a\}$$

The set $B$ is bounded and $0 \in B$ since $0 \leq n$ for any $n \in \mathbb{N}_0$. Thus, by the maximum principle (C) we are able to find $b_0 \in B$ such that $b_0$ is maximal in $B$. We see

$$\forall a \in A \ \ \forall b \in B \ \ b \leq b_0 \leq a.$$

The proof will be complete if we show $b_0 \in A$. Assume for contradiction $b_0 \neq a$ and $b_0 \leq a$ for all $a \in A$. Thus $b_0 < a$ for all $a \in A$. Hence

$$b_0 + 1 \leq a$$

for any $a \in A$. Then $b_0 + 1 \in B$, but $b_0$ is the maximal element of $B$, which gives contradiction.

# Induction - example 1/2

Example

Prove that 6 divides the number $7^n - 1$ for all $n \in \mathbb{N}_0$.

**Solution.** Let $A$ be the set of $n$ for which 6 divides $7^n - 1$.

$$A = \{n \in \mathbb{N}_0 \ : \ 6 \text{ divides } 7^n - 1\}$$

Our goal is to show $A = \mathbb{N}_0$. We will use **the induction principle**. We have to check the base step and the induction step.
**Base step.** Let us check if $0 \in A$. We have $7^0 - 1 = 0$ hence 6 divides 0.

# Induction - example 2/2

**Induction step.** Let us check that whenever $n \in A$, then $n+1 \in A$. We have

$$7^{n+1} - 1 = 7^{n+1} - 7^n + 7^n - 1$$
$$= (7-1)7^n + 7^n - 1$$
$$= \underbrace{6 \cdot 7^n}_{\text{divisible by 6}} + \underbrace{7^n - 1}_{\text{divisible by 6 since } n \in A}$$

□

# Well ordering principle - example

## Example 1/2

A sequence $(a_n)_{n\in\mathbb{N}_0}$ is given by $a_0 = -1$, $a_1 = 0$, and $a_{n+1} = 5a_n - 6a_{n-1}$ for $n \geq 1$. Prove that

$$a_n = 2 \cdot 3^n - 3 \cdot 2^n.$$

**Solution.** In the proof, we will use **well ordering principle**. Let $A$ be the set of integers $n \in \mathbb{N}_0$ such that $a_n \neq 2 \cdot 3^n - 3 \cdot 2^n$. We will show that $A = \emptyset$. Suppose for a contradiction that $A \neq \emptyset$ and let $n_0$ be the smallest element of this set. Since

$$a_0 = 2 \cdot 1 - 3 \cdot 1 = -1,$$

$$a_1 = 2 \cdot 3^1 - 3 \cdot 2^1 = 0$$

we have $n_0 \neq 0, 1$. By the minimality of $n_0$ we have

$$a_n = 2 \cdot 3^n - 3 \cdot 2^n$$

for all $0 \leq n < n_0$.

# Well ordering principle - example 2/2

Using the reccurence definition

$$a_{n_0} = 5a_{n_0-1} - 6a_{n_0-2}$$

we obtain

$$\begin{aligned} 2 \cdot 3^{n_0} - 3 \cdot 2^{n_0} \neq a_{n_0} &= 5a_{n_0-1} - 6a_{n_0-2} \\ &= 5 \cdot (2 \cdot 3^{n_0-1} - 3 \cdot 2^{n_0-1}) - 6 \cdot (2 \cdot 3^{n_0-2} - 3 \cdot 2^{n_0-2}) \\ &= 2 \cdot 3^{n_0} - 3 \cdot 2^{n_0}, \end{aligned}$$

which contradicts the minimality of $n_0$. This shows that $A = \emptyset$. $\square$

# $p^2 = 2$ - exercise

**Exercise**

Prove that the equation $p^2 = 2$ has no solution in rational numbers.

The rational numbers are

$$\mathbb{Q} = \left\{ \frac{n}{m} \ : \ n \in \mathbb{Z}, \ m \in \mathbb{Z} \setminus \{0\} \right\}.$$

# Relatively prime numbers

**Relatively prime numbers**

We say that $m, n \in \mathbb{N}$ are **relatively prime** if there is no a number $a \in \mathbb{N}$, $a \neq 1$ such that $a$ divides $m$ and $n$.

**Example 1**

The numbers 6 and 42 are not relatively prime because 3 divides both 6 and 42.

**Example 2**

The numbers 21 and 10 are relatively prime, because the set of dividors of 21 is $\{1, 3, 7, 21\}$ and the set of dividors of 10 is $\{1, 2, 5, 10\}$ and

$$\{1, 3, 7, 21\} \cap \{1, 2, 5, 10\} = \{1\}.$$

# Even and odd numbers

Recall that $n \in \mathbb{N}_0$ is **even** if it is divisable by 2. The even numbers are

$$0, 2, 4, 6, 8, 10, \ldots.$$

The number $n \in \mathbb{N}$ is **odd** if it is not divisable by 2. The odd numbers are

$$1, 3, 5, 7, 9, \ldots.$$

# Solution

## Exercise

Prove that the equation $p^2 = 2$ has no solution in rational numbers.

Assume for a contradiction that there is $\frac{m}{n} \in \mathbb{Q}$ such that $m, n$ are relatively prime and

$$p^2 = \left(\frac{m}{n}\right)^2 = 2.$$

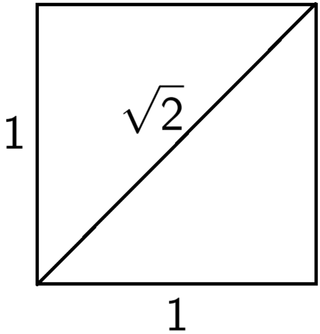
Equivalently

$$m^2 = 2n^2.$$

This implies that $m$ is even.
Since $m$ is even, then $2n^2$ must be divisable by 4.
Consequently, $n$ is also even.
Thus, $m, n$ are both even, so they are divisable by 2.
This means that $m, n$ are not relatively prime. Contradiction.

# The solution of $p^2 = 2$

The solution of $p^2 = 2$ exists as a geometric length of the diagonal of the square of side-length 1.



# Sets without minimal and maximal elements

Let

$$A = \{p \in \mathbb{Q} \ : \ p > 0, \ p^2 < 2\},$$

$$B = \{p \in \mathbb{Q} \ : \ p > 0, \ p^2 > 2\},$$

We will show that $A$ contains no largest number and $B$ contains no smallest number.

# Set $A$

$A$ **contains no largest number** means that for every $p \in A$ we can find $q \in A$ such that $p < q$.

For $p \in A$ we define

$$q = p - \frac{p^2 - 2}{p + 2} = \frac{2p + 2}{p + 2}. \tag{1}$$

Then we have

$$q^2 - 2 = \frac{2(p^2 - 2)}{(p + 2)^2}. \tag{2}$$

Since $p^2 - 2 < 0$, it follows by (1) that $p < q$.
Then, (2) shows that $q^2 < 2$, so $q \in A$.

# Set $B$

$B$ **contains no smallest number** means that for every $p \in B$ we can find $q \in B$ such that $q < p$.

Again, for $p \in A$ we define

$$q = p - \frac{p^2 - 2}{p + 2} = \frac{2p + 2}{p + 2}. \tag{3}$$

Then we have

$$q^2 - 2 = \frac{2(p^2 - 2)}{(p + 2)^2} \tag{4}$$

This time $p^2 - 2 > 0$, it follows by (3) that $q < p$.
Then, (4) shows that $q^2 > 2$, so $q \in B$.