

Student Online Teaching Advice Notice

The materials and content presented within this session are intended solely for use in a context of teaching and learning at Trinity.

Any session recorded for subsequent review is made available solely for the purpose of enhancing student learning.

Students should not edit or modify the recording in any way, nor disseminate it for use outside of a context of teaching and learning at Trinity.

Please be mindful of your physical environment and conscious of what may be captured by the device camera and microphone during videoconferencing calls.

Recorded materials will be handled in compliance with Trinity's statutory duties under the Universities Act, 1997 and in accordance with the University's [policies and procedures](#).

Further information on data protection and best practice when using videoconferencing software is available at https://www.tcd.ie/info_compliance/data-protection/.

© Trinity College Dublin 2020



Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

6 Mathematical Induction

Task: Understand how to construct a proof using mathematical induction.

$\mathbb{N} = \{0, 1, 2, \dots\}$ set of natural numbers.

Recall that \mathbb{N} is constructed using 2 axioms:

1. $0 \in \mathbb{N}$
2. If $n \in \mathbb{N}$, then $n + 1 \in \mathbb{N}$

Remarks:

1. This is exactly the process of counting.
2. If we start at 1, then we construct $\mathbb{N}^* = \{1, 2, 3, 4, \dots\} = \mathbb{N} \setminus \{0\}$

via the axioms

1. $1 \in \mathbb{N}^*$
2. if $n \in \mathbb{N}^*$, then $n + 1 \in \mathbb{N}^*$

\mathbb{N} or \mathbb{N}^* is used for mathematical induction.

6.1 Mathematical Induction Consists of Two Steps:

Step 1 Prove statement $P(1)$ called the base case.

Step 2 For any n , assume $P(n)$ and prove $P(n+1)$. This is called the inductive step.

In other words, step 2 proves the statement $\forall n P(n) \rightarrow P(n+1)$

Remark: Step 2 is not just an implication but infinitely many! In logic notation, we have:

Step 1 $P(1)$

Step 2 $\forall n (P(n) \rightarrow P(n+1))$

Therefore, $\forall n P(n)$

Let's see how the argument proceeds:

1. $P(1)$ Step 1 (base case)
2. $P(1) \rightarrow P(2)$ by Step 2 with $n = 1$
3. $P(2)$ by Modus Ponens (tautology #10) applied to 1 & 2
4. $P(2) \rightarrow P(3)$ by Step 2 with $n = 2$
5. $P(3)$ by Modus Ponens (tautology #10) applied to 3 & 4
6. $P(3) \rightarrow P(4)$ by Step 2 with $n = 3$

7. $P(4)$ by Modus Ponens (tautology #10) applied to 5 & 6

\vdots

8. $P(n)$ for any n .

This is like a row of dominos: knocking over the first one in a row makes all the others fall. Another idea is climbing a ladder.

Examples:

1. Prove $1 + 3 + 5 + \dots + (2n - 1) = n^2$ by induction.

Base Case: Verify statement for $n = 1$

When $n = 1$, $2n - 1 = 2 \times 1 - 1 = 1^2$

Inductive Step: Assume $P(n)$, i.e. $1 + 3 + 5 + \dots + (2n - 1) = n^2$ and seek to prove $P(n + 1)$, i.e. the statement $1 + 3 + 5 + \dots + (2n - 1) + [2(n + 1) - 1] = (n + 1)^2$

We start with LHS: $\underbrace{1 + 3 + 5 + \dots + (2n - 1)}_{n^2} + [2(n + 1) - 1] = n^2 + 2n + 2 - 1 = n^2 + 2n + 1 = (n + 1)^2$

2. Prove $1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$ by induction.

Base Case: Verify statement for $n = 1$

When $n = 1$, $1 = \frac{1 \times (1+1)}{2} = \frac{1 \times 2}{2} = 1$

Inductive Step: Assume $P(n)$, i.e. $1 + 2 + 3 + \dots + n = \frac{n \times (n+1)}{2}$ and seek to prove $1 + 2 + 3 + \dots + n + (n + 1) = \frac{(n+1)(n+2)}{2}$

$\underbrace{1 + 2 + 3 + \dots + n}_{\frac{n(n+1)}{2}} + n + 1 = \frac{n(n+1)}{2} + n + 1 = (n + 1)(\frac{n}{2} + 1) = (n + 1)\frac{n+2}{2} = \frac{(n+1)(n+2)}{2}$ as needed.

Remarks:

1. For some arguments by induction, it might be necessary to assume not just $P(n)$ at the inductive step but also $P(1), P(2), \dots, P(n - 1)$. This is called strong induction.

Base Case: Prove $P(1)$

Inductive Step: Assume $P(1), P(2), \dots, P(n)$ and prove $P(n + 1)$.

An example of result requiring the use of strong induction is the Fundamental Theorem of Arithmetic: $\forall n \in \mathbb{N}, n \geq 2, n$ can be expressed as a product of one or more prime numbers.

2. One has to be careful with arguments involving induction. Here is an illustration why:

Polya's argument that all horses are the same colour:

Base Case: $P(1)$ There is only one horse, so that has a colour.

Inductive Step Assume any n horses are the same colour.

Consider a group of $n + 1$ horses. Exclude the first horse and look at the other n . All of these are the same colour by our assumption. Now exclude the last horse. The remaining n horses are the same colour by our assumption. Therefore, the first horse, the horses in the middle, and the last horse are all of the same colour. We have established the inductive step.

Q: Where does the argument fail?

A: For $n = 2$, $P(2)$ is false because there are no middle horses to compare to.

3. The Grand Hotel Cigar Mystery

Recall Hilbert's hotel - the grand Hotel. Suppose that the Grand Hotel does not allow smoking and no cigars may be taken into the hotel. In spite of the rules, the guest in Room 1 goes to Room 2 to get a cigar. The guest in Room 2 goes to Room 3 to get 2 cigars (one for him and one for the person in room 1), etc. In other words, guest in Room N goes to Room $N+1$ to get N cigars. They will each get back to their rooms, smoke one cigar, and give the rest to the person in Room $N-1$.

Q: Where is the fallacy?

A: This is an induction argument without a base case. No cigars are allowed in the hotel, so no guests have cigars. An induction cannot get off the ground without a base case.

7 Abstract Algebra

Task: Understand binary operations, semigroups, monoids, and groups as well as their properties.

7.1 Binary Operations

Definition: Let A be a set. A binary operation $*$ on A is an operation applied to any two elements $x, y \in A$ that yields an element $x * y$ in A . In other words, $*$ is a binary operation on A if $\forall x, y \in A, x * y \in A$.

Examples:

1. $\mathbb{R}, +$ addition on $\mathbb{R} : \forall x, y \in \mathbb{R}, x + y \in \mathbb{R}$
2. $\mathbb{R}, -$ subtraction on $\mathbb{R} : \forall x, y \in \mathbb{R}, x - y \in \mathbb{R}$
3. \mathbb{R}, \times multiplication on $\mathbb{R} : \forall x, y \in \mathbb{R}, x \times y \in \mathbb{R}$
4. $\mathbb{R}, /$, division on \mathbb{R} is NOT a binary operation because $\forall x \in \mathbb{R} \exists 0 \in \mathbb{R}$ s.t. $\frac{x}{0}$ is undefined (not an element of \mathbb{R})
5. Let A be the set of all lists or strings. Concatenation is a binary operation.

Definition: A binary operation $*$ on a set A is called commutative if $\forall x, y \in A, x * y = y * x$

Examples:

1. $\mathbb{R}, +$ is commutative since $\forall x, y \in \mathbb{R}, x + y = y + x$
2. \mathbb{R}, \times is commutative since $\forall x, y \in \mathbb{R}, x \times y = y \times x$
3. $\mathbb{R}, -$ is not commutative since $\forall x, y \in \mathbb{R}, x - y \neq y - x$ in general. $x - y = y - x$ only if $x = y$
4. Let M_n be the set of n by n matrices with entries in \mathbb{R} , and let $*$ be matrix multiplication. $\forall A, B \in M_n, A * B \in M_n$, so $*$ is a binary operation, but $A * B \neq B * A$ in general. Therefore $*$ is not commutative.

Definition: A binary operation $*$ on a set A is called associative if $\forall x, y, z \in A$
 $(x * y) * z = x * (y * z)$

Examples:

1. $\mathbb{R}, +$ is associative since $\forall x, y, z \in \mathbb{R}, (x + y) + z = x + (y + z)$
2. \mathbb{R}, \times is associative since $\forall x, y, z \in \mathbb{R}, (x \times y) \times z = x \times (y \times z)$
3. Intersection \cap on sets is associative since $\forall A, B, C$ sets $(A \cap B) \cap C = A \cap (B \cap C)$.
4. Union \cup on sets is associative since $\forall A, B, C$ sets $(A \cup B) \cup C = A \cup (B \cup C)$
5. $\mathbb{R}, -$ is not associative since $(1 - 3) - 5 = -2 - 5 = -7$ but $1 - (3 - 5) = 1 - (-2) = 1 + 2 = 3$

Remark: When we are dealing with associative binary operations we can drop the parentheses, **i.e.** $(x * y) * z$ can be written $x * y * z$.