Lecture 16 : Definitions, theorems, proofs

Meanings

- **Definition** : an explanation of the mathematical meaning of a word.
- **Theorem** : A statement that has been proven to be true.
- **Proposition** : A less important but nonetheless interesting true statement.
- **Lemma**: A true statement used in proving other true statements (that is, a less important theorem that is helpful in the proof of other results).
- **Corollary**: A true statment that is a simple deduction from a theorem or proposition.
- **Proof**: The explanation of why a statement is true.
- **Conjecture**: A statement believed to be true, but for which we have no proof. (a statement that is being proposed to be a true statement).
- **Axiom**: A basic assumption about a mathematical situation. (a statement we assume to be true).

Group Axioms

Definition

A Group is a set G together with an operation $\#$, for which the following axioms are satisfied.

A_1. **Closure:** $\forall a, b \in G$, $a\#b \in G$

A_2. **Associativity:** $\forall a, b, c \in G$, $(a\#b)\#c = a\#(b\#c)$

A_3. **Identity element:** $\exists e \in G$ such that $\forall a \in G$, $a\#e = e\#a = a$

A_4. **Inverse element:** $\forall a \in G$, $\exists b \in G$ such that $a\#b = b\#a = e$

1. Is $\mathbb{N}$ with $+$ a group?

Group Axioms

Definition

A Group is a set G together with an operation $\#$, for which the following axioms are satisfied.

A_1. **Closure:** $\forall a, b \in G$, $a\#b \in G$

A_2. **Associativity:** $\forall a, b, c \in G$, $(a\#b)\#c = a\#(b\#c)$

A_3. **Identity element:** $\exists e \in G$ such that $\forall a \in G$, $a\#e = e\#a = a$

A_4. **Inverse element:** $\forall a \in G$, $\exists b \in G$ such that $a\#b = b\#a = e$

1. Is $\mathbb{N}$ with $+$ a group?
2. Is $\mathbb{Z}$ with $+$ a group?

Group Axioms

Definition

A Group is a set G together with an operation $\#$, for which the following axioms are satisfied.

A_1. **Closure:** $\forall a, b \in G$, $a\#b \in G$

A_2. **Associativity:** $\forall a, b, c \in G$, $(a\#b)\#c = a\#(b\#c)$

A_3. **Identity element:** $\exists e \in G$ such that $\forall a \in G$, $a\#e = e\#a = a$

A_4. **Inverse element:** $\forall a \in G$, $\exists b \in G$ such that $a\#b = b\#a = e$

1. Is $\mathbb{N}$ with $+$ a group?
2. Is $\mathbb{Z}$ with $+$ a group?
3. Do the axioms imply that if G is a group and $a, b \in G$ then $a\#b = b\#a$?

Group Axioms

Definition

A Group is a set G together with an operation $\#$, for which the following axioms are satisfied.

A_1. **Closure:** $\forall a, b \in G$, $a\#b \in G$

A_2. **Associativity:** $\forall a, b, c \in G$, $(a\#b)\#c = a\#(b\#c)$

A_3. **Identity element:** $\exists e \in G$ such that $\forall a \in G$, $a\#e = e\#a = a$

A_4. **Inverse element:** $\forall a \in G$, $\exists b \in G$ such that $a\#b = b\#a = e$

1. Is $\mathbb{N}$ with $+$ a group?
2. Is $\mathbb{Z}$ with $+$ a group?
3. Do the axioms imply that if G is a group and $a, b \in G$ then $a\#b = b\#a$?
4. Can you give an example of a group (all axioms $A_1 - A_4$ are satisfied) whose elements do not commute with each other?

Group Theorems

Definition

A Group is a set G together with an operation $\#$, for which the following axioms are satisfied.

A_1. **Closure:** $\forall a, b \in G$, $a\#b \in G$

A_2. **Associativity:** $\forall a, b, c \in G$, $(a\#b)\#c = a\#(b\#c)$

A_3. **Identity element:** $\exists e \in G$ such that $\forall a \in G$, $a\#e = e\#a = a$

A_4. **Inverse element:** $\forall a \in G$, $\exists b \in G$ such that $a\#b = b\#a = e$

Theorem

The identity element is unique.

proof:

Theorem

For every element $a \in G$ there exists a unique inverse.

proof:

Axiomatic system 1:

Definition

Undefined terms: *member, committee*

A_1. Every committee is a collection of at least two members.

A_2. Every member is on at least one committee.

1. Find two different models for this set of axioms.

Axiomatic system 1:

Definition

Undefined terms: *member, committee*

A_1. Every committee is a collection of at least two members.

A_2. Every member is on at least one committee.

1. Find two different models for this set of axioms.
2. Discuss how it can be made categorical (there is a one-to-one correspondence between the elements in the model that preserves their relationship).

Axiomatic system 2:

Definition

Undefined terms: *point, line*

A_1. Every line is a set of at least two points.

A_2. Each two lines intersect in a unique point.

A_3. There are precisely three lines.

Find two different models for this set of axioms.

Definitions

Provide a definition of a circle.

Definitions

Provide a definition of a circle.
Provide a definition of a sphere.

Definitions

Provide a definition of a circle.
Provide a definition of a sphere.
Provide a definition of a ball.

Definitions

Is the subset of a group also a group? Provide examples to support your claim.

Definitions

Is the subset of a group also a group? Provide examples to support your claim.

Provide a formal definition of a subroup.

Definitions

Is the subset of a group also a group? Provide examples to support your claim.
Provide a formal definition of a subroup.
Provide a definition of a triangle.

Definitions

Is the subset of a group also a group? Provide examples to support your claim.
Provide a formal definition of a subroup.
Provide a definition of a triangle.
Provide a definition of a quadrilateral.

Definitions

Is the subset of a group also a group? Provide examples to support your claim.
Provide a formal definition of a subroup.
Provide a definition of a triangle.
Provide a definition of a quadrilateral.
Provide a definition of a trapezoid.

Definitions

Is the subset of a group also a group? Provide examples to support your claim.

Provide a formal definition of a subroup.

Provide a definition of a triangle.

Provide a definition of a quadrilateral.

Provide a definition of a trapezoid.

Provide a definition of a parallelogram.

Definitions

Is the subset of a group also a group? Provide examples to support your claim.
Provide a formal definition of a subroup.
Provide a definition of a triangle.
Provide a definition of a quadrilateral.
Provide a definition of a trapezoid.
Provide a definition of a parallelogram.
Provide a definition of a rectangle.

Definitions

Is the subset of a group also a group? Provide examples to support your claim.

Provide a formal definition of a subroup.
Provide a definition of a triangle.
Provide a definition of a quadrilateral.
Provide a definition of a trapezoid.
Provide a definition of a parallelogram.
Provide a definition of a rectangle.
Provide a definition of a square.

Definitions

Is the subset of a group also a group? Provide examples to support your claim.
Provide a formal definition of a subroup.
Provide a definition of a triangle.
Provide a definition of a quadrilateral.
Provide a definition of a trapezoid.
Provide a definition of a parallelogram.
Provide a definition of a rectangle.
Provide a definition of a square.

Formulate conjectures involving the above figures, and their diagonals.
Example: A parallelogram is a rectangle if and only if its diagonals have equal lengths.