Linear Algebra

Dr. Bui Xuan Dieu

School of Applied Mathematics and Informatics,
Hanoi University of Science and Technology

Some Information

About this course

1) 4 Credit points, 3 hours of lecture and 2 hours of exercises and discussion per week.
2) Grade:

$$\text{Progress Grades } 30\% \text{ and Final Exam Grade } 70\%, \text{ where}$$
$$\text{Progress Grades} = \text{Midterm Exam Grades} + \text{Attendance Grades}$$

Chapter 1: Sets, mapping and complex numbers

Propositions

Definition

Propositions, in logic, are statements that can be labeled as either true or false, although we may not know which. It is often denoted by $A, B, C, \ldots$ *or* p, q.

Propositions

Definition

Propositions, in logic, are statements that can be labeled as either true or false, although we may not know which. It is often denoted by $A, B, C, \ldots$ *or* p, q.

i) Any proposition has two possible truth values: $1 =$ true or $0=$ false.

ii) For notational simplicity, the symbol A may stand for the proposition A or its truth-value, depending on the situation.

Example

i) $A = 2017$ *is an odd number,* $V(A) = 1$.

ii) $B =$ *There exists life outside the earth,* $V(B) =?$

Logical operations

1) Negation $\overline{A} = 1 - A$

Logical operations

1) Negation $\overline{A} = 1 - A$

2) Conjunction

A	B	$A \wedge B$
1	1	1
1	0	0
0	1	0
0	0	0

$(A \wedge B) = \min\{A, B\}$

Logical operations

1) Negation $\overline{A} = 1 - A$

2) Conjunction

A	B	$A \wedge B$
1	1	1
1	0	0
0	1	0
0	0	0

$$(A \wedge B) = \min\{A, B\}$$

3) Disjunction

A	B	$A \vee B$
1	1	1
1	0	1
0	1	1
0	0	0

$$(A \vee B) = \max\{A, B\}$$

Logical operations

1) Negation $\overline{A} = 1 - A$

2) Conjunction

A	B	$A \wedge B$
1	1	1
1	0	0
0	1	0
0	0	0

$$(A \wedge B) = \min\{A, B\}$$

3) Disjunction

A	B	$A \vee B$
1	1	1
1	0	1
0	1	1
0	0	0

$$(A \vee B) = \max\{A, B\}$$

4) Implication

A	B	$A \rightarrow B$
1	1	1
1	0	0
0	1	1
0	0	1

$$(A \rightarrow B) = \max\{1 - A, B\}$$

Logical operations

1) Negation $\overline{A} = 1 - A$

2) Conjunction

A	B	$A \wedge B$
1	1	1
1	0	0
0	1	0
0	0	0

$(A \wedge B) = \min\{A, B\}$

3) Disjunction

A	B	$A \vee B$
1	1	1
1	0	1
0	1	1
0	0	0

$(A \vee B) = \max\{A, B\}$

4) Implication

A	B	$A \to B$
1	1	1
1	0	0
0	1	1
0	0	1

$(A \to B) = \max\{1 - A, B\}$

5) Equivalence

A	B	$A \leftrightarrow B$
1	1	1
1	0	0
0	1	0
0	0	1

Properties

1) Commutative Laws

$$A \wedge B \Leftrightarrow B \wedge A, \quad A \vee B \Leftrightarrow B \vee A$$

Properties

1) Commutative Laws

$$A \wedge B \Leftrightarrow B \wedge A, \quad A \vee B \Leftrightarrow B \vee A$$

2) Associative Laws $\begin{cases} (A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C), \\ (A \vee B) \vee C \Leftrightarrow A \vee (B \vee C) \end{cases}$

Properties

1) Commutative Laws

$$A \wedge B \Leftrightarrow B \wedge A, \quad A \vee B \Leftrightarrow B \vee A$$

2) Associative Laws $\begin{cases} (A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C), \\ (A \vee B) \vee C \Leftrightarrow A \vee (B \vee C) \end{cases}$

3) Distributive Laws $\begin{cases} A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C), \\ A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C) \end{cases}$

Properties

1) Commutative Laws

$$A \wedge B \Leftrightarrow B \wedge A, \quad A \vee B \Leftrightarrow B \vee A$$

2) Associative Laws $\begin{cases} (A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C), \\ (A \vee B) \vee C \Leftrightarrow A \vee (B \vee C) \end{cases}$

3) Distributive Laws $\begin{cases} A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C), \\ A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C) \end{cases}$

4) De Morgan's Law $\begin{cases} \overline{A \vee B} = \overline{A} \wedge \overline{B}, \\ \overline{A \wedge B} = \overline{A} \vee \overline{B} \end{cases}$

Properties

1) Commutative Laws

$$A \wedge B \Leftrightarrow B \wedge A, \quad A \vee B \Leftrightarrow B \vee A$$

2) Associative Laws $\begin{cases} (A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C), \\ (A \vee B) \vee C \Leftrightarrow A \vee (B \vee C) \end{cases}$

3) Distributive Laws $\begin{cases} A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C), \\ A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C) \end{cases}$

4) De Morgan's Law $\begin{cases} \overline{A \vee B} = \overline{A} \wedge \overline{B}, \\ \overline{A \wedge B} = \overline{A} \vee \overline{B} \end{cases}$

5) Property of the implication operator $A \rightarrow B \Leftrightarrow \overline{A} \vee B$

Properties

1) Commutative Laws

$$A \wedge B \Leftrightarrow B \wedge A, \quad A \vee B \Leftrightarrow B \vee A$$

2) Associative Laws $\begin{cases} (A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C), \\ (A \vee B) \vee C \Leftrightarrow A \vee (B \vee C) \end{cases}$

3) Distributive Laws $\begin{cases} A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C), \\ A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C) \end{cases}$

4) De Morgan's Law $\begin{cases} \overline{A \vee B} = \overline{A} \wedge \overline{B}, \\ \overline{A \wedge B} = \overline{A} \vee \overline{B} \end{cases}$

5) Property of the implication operator $A \rightarrow B \Leftrightarrow \overline{A} \vee B$

6) Property of the equivalence operator

$$A \leftrightarrow B \Leftrightarrow (A \rightarrow B) \wedge (B \rightarrow A)$$

How to prove a proposition is a tautology?

Prove that the following proposition is tautology $\left[\overline{A} \wedge (A \vee C)\right] \to C$.

1) **Truth Table**

How to prove a proposition is a tautology?

Prove that the following proposition is tautology $\left[\overline{A} \wedge (A \vee C)\right] \to C$.

1) **Truth Table**

A	C	$\overline{A}$	$A \vee C$	$\overline{A} \wedge (A \vee C)$	$[\overline{A} \wedge (A \vee C)] \to C$
1	1	0	1	0	1
1	0	0	1	0	1
0	1	1	1	1	1
0	0	1	0	0	1

2) **Logical Equivalence**

How to prove a proposition is a tautology?

Prove that the following proposition is tautology $\left[\overline{A} \wedge (A \vee C)\right] \rightarrow C$.

1) **Truth Table**

A	C	$\overline{A}$	$A \vee C$	$\overline{A} \wedge (A \vee C)$	$[\overline{A} \wedge (A \vee C)] \rightarrow C$
1	1	0	1	0	1
1	0	0	1	0	1
0	1	1	1	1	1
0	0	1	0	0	1

2) **Logical Equivalence**

$$
\begin{aligned}
&[\overline{A} \wedge (A \vee C)] \rightarrow C \\
\Leftrightarrow &[(\overline{A} \wedge A) \vee (\overline{A} \wedge C)] \rightarrow C \\
\Leftrightarrow &[0 \vee (\overline{A} \wedge C)] \rightarrow C \\
\Leftrightarrow &[(\overline{A} \wedge C)] \rightarrow C \Leftrightarrow \overline{\overline{A} \wedge C} \vee C \\
\Leftrightarrow &A \vee \overline{C} \vee C \Leftrightarrow 1.
\end{aligned}
$$

3) **by contradiction**.

How to prove a proposition is a tautology?

Prove that the following proposition is tautology $\left[\overline{A} \wedge (A \vee C)\right] \to C$.

1) **Truth Table**

A	C	$\overline{A}$	$A \vee C$	$\overline{A} \wedge (A \vee C)$	$[\overline{A} \wedge (A \vee C)] \to C$
1	1	0	1	0	1
1	0	0	1	0	1
0	1	1	1	1	1
0	0	1	0	0	1

2) **Logical Equivalence**

$$
\begin{aligned}
&[\overline{A} \wedge (A \vee C)] \to C \\
\Leftrightarrow &[(\overline{A} \wedge A) \vee (\overline{A} \wedge C)] \to C \\
\Leftrightarrow &[0 \vee (\overline{A} \wedge C)] \to C \\
\Leftrightarrow &[(\overline{A} \wedge C)] \to C \Leftrightarrow \overline{\overline{A} \wedge C} \vee C \\
\Leftrightarrow &A \vee \overline{C} \vee C \Leftrightarrow 1.
\end{aligned}
$$

3) **by contradiction**. Suppose that the propostion is false. Then,

i) $\overline{A} \wedge (A \vee C) = 1$ and $C = 0$.

ii) $\overline{A} \wedge (A \vee C) = \overline{A} \wedge (A \vee 0) = \overline{A} \wedge A = 0$.

Exercises

Exercise

Show that the following propositions are tautology

a) $[(A \to B) \wedge (B \to C)] \to (A \to C)$.

Exercise

Which of the following propositions are tautology, contradiction

a) $(p \vee q) \to (p \wedge q)$,

b) $(p \wedge q) \vee (p \to q)$,

c) $p \to (q \to p)$,

d) $(q \to (q \to p))$,

e) $(p \to q) \to q$,

f) $(p \wedge q) \leftrightarrow (q \updownarrow p)$.

Exercise

Prove that

a) $A \leftrightarrow B$ *and* $(A \wedge B) \vee (\overline{A} \wedge \overline{B})$ *are logically equivalent.*

b) $(A \to B) \to C$ *and* $A \to (B \to C)$ *are not logically equivalent.*

Binary operators

1) Binary operator XOR

A	B	$A \updownarrow B$
1	1	0
1	0	1
0	1	1
0	0	0

$$(A \updownarrow B) = \overline{A \leftrightarrow B}$$

2) Binary operator NOR

A	B	$A \uparrow B$
1	1	0
1	0	0
0	1	0
0	0	1

$$(A \uparrow B) = \overline{A \vee B}$$

3) Binary Operator NAND

A	B	$A \downarrow B$
1	1	0
1	0	1
0	1	1
0	0	1

$$(A \downarrow B) = \overline{A \wedge B}$$

Propositions with quantifiers $\forall, \exists$

1) "Every element x of the set X satisfies property $\mathcal{P}(x)$"

$$\forall x \in X, \mathcal{P}(x).$$

2) "There exists at least one element x of the set X that satisfies properties $\mathcal{P}(x)$"

$$\exists x \in X, \mathcal{P}(x).$$

Relations

$$\overline{\forall x \in X, \mathcal{P}(x)} = \exists x \in X, \overline{\mathcal{P}(x)}$$

$$\overline{\exists x \in X, \mathcal{P}(x)} = \forall x \in X, \overline{\mathcal{P}(x)}$$

Propositions with quantifiers $\forall, \exists$

Remark

To receive the negation of a proposition containing qualifiers $\forall, \exists$ *and statement* $P(x_1, \ldots, x_n)$, *we*

1) *change* $\forall$ *by* $\exists$,
2) *change* $\exists$ *by* $\forall$,
3) *change* $P(x_1, \ldots, x_n)$ *by* $\bar{P}(x_1, \ldots, x_n)$.

Propositions with quantifiers $\forall, \exists$

Remark

To receive the negation of a proposition containing qualifiers $\forall, \exists$ and statement $P(x_1, \ldots, x_n)$, we

1) *change $\forall$ by $\exists$,*
2) *change $\exists$ by $\forall$,*
3) *change $P(x_1, \ldots, x_n)$ by $\bar{P}(x_1, \ldots, x_n)$.*

Exercise

Find the negation p if

a) $p =$ "$\forall \epsilon > 0, \exists \delta > 0 : \forall x, |x - x_0| < \delta, |f(x) - f(x_0)| < \epsilon.$"

Propositions with quantifiers $\forall, \exists$

Remark

To receive the negation of a proposition containing qualifiers $\forall, \exists$ and statement $P(x_1, \ldots, x_n)$, we

1) *change* $\forall$ *by* $\exists$,
2) *change* $\exists$ *by* $\forall$,
3) *change* $P(x_1, \ldots, x_n)$ *by* $\bar{P}(x_1, \ldots, x_n)$.

Exercise

Find the negation p if

a) $p =$ "$\forall \epsilon > 0, \exists \delta > 0 : \forall x, |x - x_0| < \delta, |f(x) - f(x_0)| < \epsilon.$"
b) $p = \lim\limits_{n \to +\infty} x_n = \infty \Leftrightarrow \forall M > 0, \exists N \in \mathbb{N} : \forall n \geq N, |x_n| > M.$
c) $p = \lim\limits_{n \to +\infty} x_n = L \Leftrightarrow \forall \epsilon > 0, \exists N \in \mathbb{N} : \forall n \geq N, |x_n - L| < \epsilon.$

Chapter 1: Sets, mapping and complex numbers

Definitions and notations

1) A set is a collection of objects or things.

Definitions and notations

1) A set is a collection of objects or things.
2) Let A be a set. If a is an element of A, then we denote by $a \in A$. Otherwise, $a \notin A$.

Definitions and notations

1) A set is a collection of objects or things.
2) Let A be a set. If a is an element of A, then we denote by $a \in A$. Otherwise, $a \notin A$.
3) The set containing no any element is called the empty set and denoted by $\emptyset$.

Definitions and notations

1) A set is a collection of objects or things.
2) Let A be a set. If a is an element of A, then we denote by $a \in A$. Otherwise, $a \notin A$.
3) The set containing no any element is called the empty set and denoted by $\emptyset$.
4) Description of a set:
   i) Roster notation (or listing notation).
   ii) Set-builder notation.
   iii) Venn diagram.

Algebra of sets

1) Inclusion $A \subset B \Leftrightarrow \forall x \in A \Rightarrow x \in B$

Algebra of sets

1) Inclusion $A \subset B \Leftrightarrow \forall x \in A \Rightarrow x \in B$
2) Set equality $A = B \Leftrightarrow A \subset B$ and $B \subset A$

Algebra of sets

1) Inclusion $A \subset B \Leftrightarrow \forall x \in A \Rightarrow x \in B$
2) Set equality $A = B \Leftrightarrow A \subset B$ and $B \subset A$
3) Union

Algebra of sets

1) Inclusion $A \subset B \Leftrightarrow \forall x \in A \Rightarrow x \in B$
2) Set equality $A = B \Leftrightarrow A \subset B$ and $B \subset A$
3) Union

$$\begin{cases} x \in A \cup B \Leftrightarrow x \in A \text{ or } x \in B \\ \end{cases}$$

Algebra of sets

1) Inclusion $A \subset B \Leftrightarrow \forall x \in A \Rightarrow x \in B$
2) Set equality $A = B \Leftrightarrow A \subset B$ and $B \subset A$
3) Union

$$\begin{cases} x \in A \cup B \Leftrightarrow x \in A \text{ or } x \in B \\ x \notin A \cup B \Leftrightarrow x \notin A \text{ and } x \notin B \end{cases}$$

Algebra of sets

1) Inclusion $A \subset B \Leftrightarrow \forall x \in A \Rightarrow x \in B$
2) Set equality $A = B \Leftrightarrow A \subset B$ and $B \subset A$
3) Union

$$\begin{cases} x \in A \cup B \Leftrightarrow x \in A \text{ or } x \in B \\ x \notin A \cup B \Leftrightarrow x \notin A \text{ and } x \notin B \end{cases}$$

4) Intersection

Algebra of sets

1) Inclusion $A \subset B \Leftrightarrow \forall x \in A \Rightarrow x \in B$
2) Set equality $A = B \Leftrightarrow A \subset B$ and $B \subset A$
3) Union

$$\begin{cases} x \in A \cup B \Leftrightarrow x \in A \text{ or } x \in B \\ x \notin A \cup B \Leftrightarrow x \notin A \text{ and } x \notin B \end{cases}$$

4) Intersection

$$\begin{cases} x \in A \cap B \Leftrightarrow x \in A \text{ and } x \in B \\ \end{cases}$$

Algebra of sets

1) Inclusion $A \subset B \Leftrightarrow \forall x \in A \Rightarrow x \in B$
2) Set equality $A = B \Leftrightarrow A \subset B$ and $B \subset A$
3) Union

$$\begin{cases} x \in A \cup B \Leftrightarrow x \in A \text{ or } x \in B \\ x \notin A \cup B \Leftrightarrow x \notin A \text{ and } x \notin B \end{cases}$$

4) Intersection

$$\begin{cases} x \in A \cap B \Leftrightarrow x \in A \text{ and } x \in B \\ x \notin A \cap B \Leftrightarrow x \notin A \text{ or } x \notin B \end{cases}$$

Algebra of sets

1) Inclusion $A \subset B \Leftrightarrow \forall x \in A \Rightarrow x \in B$
2) Set equality $A = B \Leftrightarrow A \subset B$ and $B \subset A$
3) Union

$$\begin{cases} x \in A \cup B \Leftrightarrow x \in A \text{ or } x \in B \\ x \notin A \cup B \Leftrightarrow x \notin A \text{ and } x \notin B \end{cases}$$

4) Intersection

$$\begin{cases} x \in A \cap B \Leftrightarrow x \in A \text{ and } x \in B \\ x \notin A \cap B \Leftrightarrow x \notin A \text{ or } x \notin B \end{cases}$$

5) Subtraction

Algebra of sets

1) Inclusion $A \subset B \Leftrightarrow \forall x \in A \Rightarrow x \in B$
2) Set equality $A = B \Leftrightarrow A \subset B$ and $B \subset A$
3) Union

$$\begin{cases} x \in A \cup B \Leftrightarrow x \in A \text{ or } x \in B \\ x \notin A \cup B \Leftrightarrow x \notin A \text{ and } x \notin B \end{cases}$$

4) Intersection

$$\begin{cases} x \in A \cap B \Leftrightarrow x \in A \text{ and } x \in B \\ x \notin A \cap B \Leftrightarrow x \notin A \text{ or } x \notin B \end{cases}$$

5) Subtraction

$$\begin{cases} x \in A \setminus B \Leftrightarrow x \in A \text{ and } x \notin B \\ \end{cases}$$

Algebra of sets

1) Inclusion $A \subset B \Leftrightarrow \forall x \in A \Rightarrow x \in B$
2) Set equality $A = B \Leftrightarrow A \subset B$ and $B \subset A$
3) Union

$$\begin{cases} x \in A \cup B \Leftrightarrow x \in A \text{ or } x \in B \\ x \notin A \cup B \Leftrightarrow x \notin A \text{ and } x \notin B \end{cases}$$

4) Intersection

$$\begin{cases} x \in A \cap B \Leftrightarrow x \in A \text{ and } x \in B \\ x \notin A \cap B \Leftrightarrow x \notin A \text{ or } x \notin B \end{cases}$$

5) Subtraction

$$\begin{cases} x \in A \setminus B \Leftrightarrow x \in A \text{ and } x \notin B \\ x \notin A \setminus B \Leftrightarrow x \notin A \text{ or } x \in B \end{cases}$$

Algebra of sets

1) Inclusion $A \subset B \Leftrightarrow \forall x \in A \Rightarrow x \in B$
2) Set equality $A = B \Leftrightarrow A \subset B$ and $B \subset A$
3) Union

$$\begin{cases} x \in A \cup B \Leftrightarrow x \in A \text{ or } x \in B \\ x \notin A \cup B \Leftrightarrow x \notin A \text{ and } x \notin B \end{cases}$$

4) Intersection

$$\begin{cases} x \in A \cap B \Leftrightarrow x \in A \text{ and } x \in B \\ x \notin A \cap B \Leftrightarrow x \notin A \text{ or } x \notin B \end{cases}$$

5) Subtraction

$$\begin{cases} x \in A \setminus B \Leftrightarrow x \in A \text{ and } x \notin B \\ x \notin A \setminus B \Leftrightarrow x \notin A \text{ or } x \in B \end{cases}$$

6) Complement
   If $A \subset X$, then $\overline{A} = X \setminus A$ is called the complement of A in X.

Algebra Sets

Example

Let

$$A = \{x \in \mathbb{R} | x^2 - 4x + 3 \leq 0\}, \quad B = \{x \in \mathbb{R} || x - 1| \leq 1\},$$

and

$$C = \{x \in \mathbb{R} | x^2 - 5x + 6 \leq 0\}.$$

Find $(A \cup B) \cap C$ and $(A \cap B) \cup C$.

Set Identities

1) Commutative laws:
   $A \cup B = B \cup A, \quad A \cap B = B \cap A$

Set Identities

1) Commutative laws:
$A \cup B = B \cup A, \quad A \cap B = B \cap A$
2) Associative laws:

$$(A \cup B) \cup C = A \cup (B \cup C), \quad (A \cap B) \cap C = A \cap (B \cap C)$$

Set Identities

1) Commutative laws:
$A \cup B = B \cup A, \quad A \cap B = B \cap A$
2) Associative laws:
$$(A \cup B) \cup C = A \cup (B \cup C), \quad (A \cap B) \cap C = A \cap (B \cap C)$$
3) Distributive laws:
$$\begin{cases} A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \\ A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \end{cases}$$

Set Identities

1) Commutative laws:
$A \cup B = B \cup A, \quad A \cap B = B \cap A$
2) Associative laws:
$$(A \cup B) \cup C = A \cup (B \cup C), \quad (A \cap B) \cap C = A \cap (B \cap C)$$
3) Distributive laws:
$$\begin{cases} A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \\ A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \end{cases}$$
4) Property of the complement
If $A, B \subset X$, then $A \setminus B = A \cap \overline{B}$

Set Identities

1) Commutative laws:
   $A \cup B = B \cup A, \quad A \cap B = B \cap A$
2) Associative laws:
$$(A \cup B) \cup C = A \cup (B \cup C), \quad (A \cap B) \cap C = A \cap (B \cap C)$$
3) Distributive laws:
$$\begin{cases} A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \\ A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \end{cases}$$
4) Property of the complement
   If $A, B \subset X$, then $A \setminus B = A \cap \overline{B}$
5) De Moorgan's Law
$$\overline{A \cap B} = \overline{A} \cup \overline{B}, \quad \overline{\cap A_i} = \cup \overline{A_i}$$
$$\overline{A \cup B} = \overline{A} \cap \overline{B}, \quad \overline{\cup A_i} = \cap \overline{A_i}$$

Mathematical Logic and Sets

1) Negation $\overline{A}$
2) Conjunction $A \wedge B$
3) Disjunction $A \vee B$
4) Implication $A \Rightarrow B$
5) Equivalence $A \Leftrightarrow B$

1) Complement $\overline{A} = X \setminus A$
2) Intersection $A \cap B$
3) Union $A \cup B$
4) Inclusion $A \subset B$
5) Set equality $A = B$

Three possible methods to prove set equality

1) Double inclusion
2) Set identities
3) Membership tables.

Proving set equality

Example

Prove that $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

Proving set equality

Example

Prove that $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

Double inclusion

$\boxed{\Rightarrow}$ Suppose that $x \in A \cap (B \setminus C)$

Need to prove $x \in (A \cap B) \setminus (A \cap C)$.

Proving set equality

Example

Prove that $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

Double inclusion

$\boxed{\Rightarrow}$ Suppose that $x \in A \cap (B \setminus C)$
Need to prove $x \in (A \cap B) \setminus (A \cap C)$.

$\boxed{\Leftarrow}$ Suppose $x \in (A \cap B) \setminus (A \cap C)$
Need to prove $x \in A \cap (B \setminus C)$.

Proving set equality

Example

Prove that $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

Proving set equality

Example

Prove that $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

Set identities

$$
\begin{aligned}
&(A \cap B) \setminus (A \cap C) \\
=&(A \cap B) \cap (\overline{A} \cup \overline{C}) \\
=&[(A \cap B) \cap \overline{A}] \cup [A \cap B \cap \overline{C}] \\
=&A \cap (B \setminus C).
\end{aligned} \tag{1}
$$

Proving set equality

Example

Prove that $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

Proving set equality

Example

Prove that $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

Membership tables

A	B	C	$B \setminus C$	$A \cap (B \setminus C)$	$A \cap B$	$A \cap C$	$(A \cap B) \setminus (A \cap C)$
1	1	1	0	0	1	1	0
1	1	0	1	1	1	0	1
1	0	1	0	0	0	1	0
1	0	0	0	0	0	0	0
0	1	1	0	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0

1) "1" =membership, "0" =non-membership.
2) Two sets are equal, iff they have identical columns.

Proving set equality

Example

Let A, B, C be arbitrary sets. Prove that

a) $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

b) $A \cup (B \setminus A) = A \cup B$.

c) If $(A \cap C) \subset (A \cap B)$ and $(A \cup C) \subset (A \cup B)$, then $C \subset B$.

d) $A \setminus (A \setminus B) = A \cap B$.

e) $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

f) $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

g) $(A \cap B) \times C = (A \times C) \cap (B \times C)$.

h) Is it true that $(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times D)$. If not, give a counterexample.

The cartesian product: Let A, B be sets.

$$A \times B = \{(a, b) | a \in A \text{ and } b \in B\}, \quad (a, b) = (c, d) \Leftrightarrow a = c, b = d.$$

Chapter 1: Sets, mapping and complex numbers

Maps

Definition

$$f : X \to Y,$$
$$x \mapsto y \in Y(unique)$$

Maps

Definition

$$f : X \to Y,$$
$$x \mapsto y \in Y(unique)$$

Image, Preimage

Let $f : X \to Y$ and $A \subset X, C \subset Y$.

i) **The Image**
$f(A) = \{y \in Y | \exists x \in A, f(x) = y\}$.

Maps

Definition

$$f : X \to Y,$$
$$x \mapsto y \in Y(unique)$$

Image, Preimage

Let $f : X \to Y$ and $A \subset X, C \subset Y$.

i) **The Image**
$f(A) = \{y \in Y | \exists x \in A, f(x) = y\}$.

ii) **The preimage**
$f^{-1}(C) = \{x \in X | f(x) \in C\}$.

Maps

Definition

$$\begin{aligned} f : X &\to Y, \\ x &\mapsto y \in Y(unique) \end{aligned}$$

Image, Preimage

Let $f : X \to Y$ and $A \subset X, C \subset Y$.

i) **The Image**
$f(A) = \{y \in Y | \exists x \in A, f(x) = y\}$.

ii) **The preimage**
$f^{-1}(C) = \{x \in X | f(x) \in C\}$.

$\boxed{y \in f(A) \Leftrightarrow \exists x \in A : y = f(x)}$ $\boxed{x \in f^{-1}(C) \Leftrightarrow f(x) \in C}$

Image, preimage

Properties

Let $f : X \to Y$ and $A, B \subset X, \quad C, D \subset Y$.

a) $f(A \cup B) = f(A) \cup f(B)$,

b) $f(A \cap B) \subset f(A) \cap f(B)$,

c) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$,

d) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.

i) $y \in f(A) \Leftrightarrow \exists x \in A : y = f(x)$,

ii) $x \in f^{-1}(C) \Leftrightarrow f(x) \in C$

Image, preimage

Example

Let $f: X \to Y$ and $A, B \subset X, \quad C, D \subset Y$. Prove that

e) $f^{-1}(C \setminus D) = f^{-1}(C) \setminus f^{-1}(D)$,

f) $A \subset f^{-1}(f(A))$,

g) $C \supset f(f^{-1}(C))$.

Image, preimage

Example

Let $f : X \to Y$ and $A, B \subset X, \quad C, D \subset Y$. Prove that

e) $f^{-1}(C \setminus D) = f^{-1}(C) \setminus f^{-1}(D)$,

f) $A \subset f^{-1}(f(A))$,

g) $C \supset f(f^{-1}(C))$.

Example

Let $f : \mathbb{R}^2 \to \mathbb{R}^2, f(x, y) = (2x, 2y)$ and

$$A = \{(x, y) \in \mathbb{R}^2 | (x - 4)^2 + y^2 = 4\}.$$

Find $f(A), f^{-1}(A)$.

Maps

Injective,surjective, bijective mappings

Let $f : X \to Y$ be a map.

a) **Injective**

i) $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, or

Maps

Injective,surjective, bijective mappings

Let $f : X \to Y$ be a map.

a) **Injective**

i) $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, or

ii) $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$, or

Maps

Injective,surjective, bijective mappings

Let $f : X \to Y$ be a map.

a) **Injective**

i) $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, or

ii) $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$, or

iii) $\forall y \in Y$, the eq. $f(x) = y$ has **at most** one solution.

Maps

Injective,surjective, bijective mappings

Let $f : X \to Y$ be a map.

a) **Injective**

i) $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, or

ii) $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$, or

iii) $\forall y \in Y$, the eq. $f(x) = y$ has **at most** one solution.

b) **Surjective**

i) $\forall y \in Y, \exists x \in X$ such that $f(x) = y$, or

Maps

Injective,surjective, bijective mappings

Let $f : X \to Y$ be a map.

a) **Injective**

i) $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, or

ii) $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$, or

iii) $\forall y \in Y$, the eq. $f(x) = y$ has **at most** one solution.

b) **Surjective**

i) $\forall y \in Y$, $\exists x \in X$ such that $f(x) = y$, or

ii) $\forall y \in Y$, the eq. $f(x) = y$ has **at least** one solution.

c) **Bijective** $=$ injective $+$ surjective.

$\forall y \in Y$, the eq. $f(x) = y$ has **a unique solution**.

Injective,surjective, bijective mappings

Example

Which of the following maps are injective, surjective, bijective?

a) $f:\mathbb{R}\to\mathbb{R}, f(x)=3-2x$,

b) $f:(-\infty,0]\to[4,+\infty), f(x)=x^2+4$,

c) $f:(1,+\infty)\to(-1,+\infty), f(x)=x^2-2x$,

d) $f:\mathbb{R}\setminus\{1\}\to\mathbb{R}\setminus\{3\}, f(x)=\frac{3x+1}{x-1}$,

e) $f:[4,9]\to[21,96], f(x)=x^2+2x-3$,

f) $f:\mathbb{R}\to\mathbb{R}, f(x)=3x-2|x|$,

g) $f:(-1,1)\to\mathbb{R}, f(x)=\ln\frac{1+x}{1-x}$,

h) $f:\mathbb{R}\setminus\{0\}\to\mathbb{R}, f(x)=\frac{1}{x}$,

i) $f:\mathbb{R}\to\mathbb{R}, g(x)=\frac{2x}{1+x^2}$.

Composition of maps, inverse maps

Composition of maps, inverse maps

Let $f: X \to Y, \quad g: Y \to Z$.

i) Composition $(g \circ f)(x) = g(f(x))$.

Composition of maps, inverse maps

Composition of maps, inverse maps

Let $f : X \to Y, \quad g : Y \to Z$.

i) Composition $(g \circ f)(x) = g(f(x))$.

ii) If f is bijective, then $f^{-1} : Y \to X$ is called the inverse map of f.

Composition of maps, inverse maps

Composition of maps, inverse maps

Let $f : X \to Y, \quad g : Y \to Z$.

i) Composition $(g \circ f)(x) = g(f(x))$.

ii) If f is bijective, then $f^{-1} : Y \to X$ is called the inverse map of f.

Properties

i) $h \circ (g \circ f) = (h \circ g) \circ f$,

Composition of maps, inverse maps

Composition of maps, inverse maps

Let $f : X \to Y, \quad g : Y \to Z$.

i) Composition $(g \circ f)(x) = g(f(x))$.

ii) If f is bijective, then $f^{-1} : Y \to X$ is called the inverse map of f.

Properties

i) $h \circ (g \circ f) = (h \circ g) \circ f$,

ii) $f \circ \mathrm{Id} = \mathrm{Id} \circ f =$

Composition of maps, inverse maps

Composition of maps, inverse maps

Let $f : X \to Y, \quad g : Y \to Z$.

i) Composition $(g \circ f)(x) = g(f(x))$.

ii) If f is bijective, then $f^{-1} : Y \to X$ is called the inverse map of f.

Properties

i) $h \circ (g \circ f) = (h \circ g) \circ f$,

ii) $f \circ \mathrm{Id} = \mathrm{Id} \circ f = f$,

iii) $(f^{-1})^{-1} =$

Composition of maps, inverse maps

Composition of maps, inverse maps

Let $f: X \to Y, \quad g: Y \to Z.$

i) Composition $(g \circ f)(x) = g(f(x))$.

ii) If f is bijective, then $f^{-1}: Y \to X$ is called the inverse map of f.

Properties

i) $h \circ (g \circ f) = (h \circ g) \circ f,$

ii) $f \circ \mathrm{Id} = \mathrm{Id} \circ f = f,$

iii) $(f^{-1})^{-1} = f,$

iv) $f \circ f^{-1} = f^{-1} \circ f =$

Composition of maps, inverse maps

Composition of maps, inverse maps

Let $f : X \to Y, \quad g : Y \to Z$.

i) Composition $(g \circ f)(x) = g(f(x))$.

ii) If f is bijective, then $f^{-1} : Y \to X$ is called the inverse map of f.

Properties

i) $h \circ (g \circ f) = (h \circ g) \circ f$,

ii) $f \circ \mathrm{Id} = \mathrm{Id} \circ f = f$,

iii) $(f^{-1})^{-1} = f$,

iv) $f \circ f^{-1} = f^{-1} \circ f = \mathrm{Id}$,

v) $(g \circ f)^{-1} =$

Composition of maps, inverse maps

Composition of maps, inverse maps

Let $f : X \to Y, \quad g : Y \to Z$.

i) Composition $(g \circ f)(x) = g(f(x))$.

ii) If f is bijective, then $f^{-1} : Y \to X$ is called the inverse map of f.

Properties

i) $h \circ (g \circ f) = (h \circ g) \circ f$,

ii) $f \circ \mathrm{Id} = \mathrm{Id} \circ f = f$,

iii) $(f^{-1})^{-1} = f$,

iv) $f \circ f^{-1} = f^{-1} \circ f = \mathrm{Id}$,

v) $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$,

Composition of maps, inverse maps

Composition of maps, inverse maps

Let $f : X \to Y, \quad g : Y \to Z$.

i) Composition $(g \circ f)(x) = g(f(x))$.

ii) If f is bijective, then $f^{-1} : Y \to X$ is called the inverse map of f.

Properties

i) $h \circ (g \circ f) = (h \circ g) \circ f$,

ii) $f \circ \mathrm{Id} = \mathrm{Id} \circ f = f$,

iii) $(f^{-1})^{-1} = f$,

iv) $f \circ f^{-1} = f^{-1} \circ f = \mathrm{Id}$,

v) $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$,

Injectivity, Surjectivity, Bijectivity of the composition

i) f and g injective $\Rightarrow g \circ f$ injective.

Composition of maps, inverse maps

Composition of maps, inverse maps

Let $f : X \to Y, \quad g : Y \to Z$.

i) Composition $(g \circ f)(x) = g(f(x))$.

ii) If f is bijective, then $f^{-1} : Y \to X$ is called the inverse map of f.

Properties

i) $h \circ (g \circ f) = (h \circ g) \circ f$,

ii) $f \circ \mathrm{Id} = \mathrm{Id} \circ f = f$,

iii) $(f^{-1})^{-1} = f$,

iv) $f \circ f^{-1} = f^{-1} \circ f = \mathrm{Id}$,

v) $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$,

Injectivity, Surjectivity, Bijectivity of the composition

i) f and g injective $\Rightarrow g \circ f$ injective.

ii) f and g surjective $\Rightarrow g \circ f$ surjective,

Composition of maps, inverse maps

Composition of maps, inverse maps

Let $f : X \to Y, \quad g : Y \to Z$.

i) Composition $(g \circ f)(x) = g(f(x))$.

ii) If f is bijective, then $f^{-1} : Y \to X$ is called the inverse map of f.

Properties

i) $h \circ (g \circ f) = (h \circ g) \circ f$,

ii) $f \circ \mathrm{Id} = \mathrm{Id} \circ f = f$,

iii) $(f^{-1})^{-1} = f$,

iv) $f \circ f^{-1} = f^{-1} \circ f = \mathrm{Id}$,

v) $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$,

Injectivity, Surjectivity, Bijectivity of the composition

i) f and g injective $\Rightarrow g \circ f$ injective.

ii) f and g surjective $\Rightarrow g \circ f$ surjective,

iii) f and g bijective $\Rightarrow g \circ f$ bijective.

Composition of maps, inverse maps

Example

Let $f : X \to Y, \quad g : Y \to Z$. Prove that

a) f surjective and $g \circ f$ injective $\Rightarrow g$ injective,

b) give an example to show that $g \circ f$ is injective, but g is not,

c) g injective and $g \circ f$ surjective $\Rightarrow f$ surjective,

d) give an example to show that $g \circ f$ is surjective but f is not.

Restriction, characteristic functions

Restriction

i) Let $f : X \to Y$ and $A \subset X$. The restriction $f_A : A \to Y$ given by $f_A(x) = f(x)\ \forall x \in A$.

ii) g is the restriction of $f \Rightarrow f$ is an extension of g.

Restriction, characteristic functions

Restriction

i) Let $f : X \to Y$ and $A \subset X$. The restriction $f_A : A \to Y$ given by $f_A(x) = f(x)\ \forall x \in A$.

ii) g is the restriction of $f \Rightarrow f$ is an extension of g.

Characteristic functions

Let $A \subset X$, the map $f : A \to \{0, 1\}$ given by $f(x) = \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } x \notin A \end{cases}$

is called the characteristic function.

Restriction, characteristic functions

Restriction

i) Let $f : X \to Y$ and $A \subset X$. The restriction $f_A : A \to Y$ given by $f_A(x) = f(x)\ \forall x \in A$.

ii) g is the restriction of $f \Rightarrow f$ is an extension of g.

Characteristic functions

Let $A \subset X$, the map $f : A \to \{0, 1\}$ given by $f(x) = \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } x \notin A \end{cases}$

is called the characteristic function.

The canonical projection

Let $X = X_1 \times X_2$. The map $p_1 : X \to X_1$ given by $p(x_1, x_2) = x_1$ is called the canonical projection on X_1.

Substitutions

Substitutions

A bijection $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$ is called a substitution (or permutation).

Substitutions

Substitutions

A bijection $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$ is called a substitution (or permutation).

Properties

i) Composition of substitutions is a substitution.

Substitutions

Substitutions

A bijection $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$ is called a substitution (or permutation).

Properties

i) Composition of substitutions is a substitution.

ii) The inverse map of a substitution is a substitution.

Substitutions

Substitutions

A bijection $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$ is called a substitution (or permutation).

Properties

i) Composition of substitutions is a substitution.

ii) The inverse map of a substitution is a substitution.

iii) There are $n!$ substitutions.

Substitutions

Substitutions

A bijection $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$ is called a substitution (or permutation).

Properties

i) Composition of substitutions is a substitution.
ii) The inverse map of a substitution is a substitution.
iii) There are $n!$ substitutions.

Example

a) Let $|X| = m, |Y| = n$. Find the number of maps from X to Y.
b) Let $|X| = m, |Y| = n$, where $m < n$. Find the number of injection from X to Y.

Substitutions

Cycle

i) cycle of length k

$$(i_1, i_2, \ldots, i_k) \Leftrightarrow \begin{cases} f(i_1) &= i_2, \\ f(i_2) &= i_3, \\ &\vdots \\ f(i_k) &= i_1 \end{cases} \text{ and } f(j) = j \text{ otherwise.}$$

ii) A cycle of length 2 is called a transposition.

Substitutions

Cycle

i) cycle of length k

$$(i_1, i_2, \ldots, i_k) \Leftrightarrow \begin{cases} f(i_1) &= i_2, \\ f(i_2) &= i_3, \\ &\vdots \\ f(i_k) &= i_1 \end{cases} \text{ and } f(j) = j \text{ otherwise.}$$

ii) A cycle of length 2 is called a transposition.

Theorem

i) Any substitution is a product of cycles.

ii) Any substitution is a product of transpositons.

Substitutions

Example

Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 2 & 1 & 5 & 7 & 6 & 9 & 10 & 8 \end{pmatrix},$$

and

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 1 & 2 & 5 & 7 & 6 & 9 & 8 & 10 \end{pmatrix}$$

i) Compute σ^{-1} and $\tau \circ \sigma$.

ii) Write σ, τ as a product of disjoint cycles.

Substitutions

Example

Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 2 & 1 & 5 & 7 & 6 & 9 & 10 & 8 \end{pmatrix},$$

and

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 1 & 2 & 5 & 7 & 6 & 9 & 8 & 10 \end{pmatrix}$$

i) Compute σ^{-1} and $\tau \circ \sigma$.

ii) Write σ, τ as a product of disjoint cycles.

Example

Let $|X| = n$ and f be a bijection from X to X. Prove that there exists $k \in \mathbb{N}$ such that $f^k = \mathrm{Id}_X$, where $f^k = f \circ f \cdots \circ f$ (k-times).

Substitutions

Parity of a permutation

Let $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$ be a permutatiton.

i) (i, j) is called an inversion if $i < j$ and $f(i) > f(j)$.

Substitutions

Parity of a permutation

Let $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$ be a permutatiton.

i) (i, j) is called an inversion if $i < j$ and $f(i) > f(j)$.

ii) f is called even if the number of inversions is even,

iii) f is called odd if the number of inversions is odd.

Substitutions

Parity of a permutation

Let $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$ be a permutatiton.

i) (i, j) is called an inversion if $i < j$ and $f(i) > f(j)$.

ii) f is called even if the number of inversions is even,

iii) f is called odd if the number of inversions is odd.

iv) If $N(f)$ is the number of inversions. Then $\operatorname{sign}(f) = (-1)^{N(f)}$.

Substitutions

Parity of a permutation

Let $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$ be a permutatiton.

i) (i,j) is called an inversion if $i < j$ and $f(i) > f(j)$.

ii) f is called even if the number of inversions is even,

iii) f is called odd if the number of inversions is odd.

iv) If $N(f)$ is the number of inversions. Then $\text{sign}(f) = (-1)^{N(f)}$.

Theorem

Let $f, g \in S_n$. Then,

i) $\text{sign}(f \circ g) = \text{sign}(f).\text{sign}(g)$,

Substitutions

Parity of a permutation

Let $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$ be a permutatiton.

i) (i, j) is called an inversion if $i < j$ and $f(i) > f(j)$.

ii) f is called even if the number of inversions is even,

iii) f is called odd if the number of inversions is odd.

iv) If $N(f)$ is the number of inversions. Then $\operatorname{sign}(f) = (-1)^{N(f)}$.

Theorem

Let $f, g \in S_n$. Then,

i) $\operatorname{sign}(f \circ g) = \operatorname{sign}(f).\operatorname{sign}(g)$,

ii) $\operatorname{sign}(f) = \operatorname{sign}(f^{-1})$,

Substitutions

Parity of a permutation

Let $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$ be a permutatiton.

i) (i, j) is called an inversion if $i < j$ and $f(i) > f(j)$.

ii) f is called even if the number of inversions is even,

iii) f is called odd if the number of inversions is odd.

iv) If $N(f)$ is the number of inversions. Then $\operatorname{sign}(f) = (-1)^{N(f)}$.

Theorem

Let $f, g \in S_n$. Then,

i) $\operatorname{sign}(f \circ g) = \operatorname{sign}(f).\operatorname{sign}(g)$,

ii) $\operatorname{sign}(f) = \operatorname{sign}(f^{-1})$,

iii) If f is a cycle of length k, then $\operatorname{sign}(f) = (-1)^{k-1}$.

The sign of a permutation

Example

Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 2 & 1 & 5 & 7 & 6 & 9 & 10 & 8 \end{pmatrix},$$

and

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 1 & 2 & 5 & 7 & 6 & 9 & 8 & 10 \end{pmatrix}$$

i) Compute σ^{-1} and $\tau \circ \sigma$.

ii) Write σ, τ as a product of disjoint cycles.

iii) Compute $\text{sign}(\sigma), \text{sign}(\tau)$.

Chapter 1: Sets, mapping and complex numbers

Binary operators

Binary operators

Let G be a set. A binary operator on G is a map

$$\begin{aligned} * : G \times G &\to G, \\ (x, y) &\mapsto x * y. \end{aligned}$$

Binary operators

Binary operators

Let G be a set. A binary operator on G is a map

$$\begin{aligned} * : G \times G &\to G, \\ (x, y) &\mapsto x * y. \end{aligned}$$

Properties of binary operators

We say that

i) $*$ is commutative if $\forall a, b \in X, a * b = b * a$.

Binary operators

Binary operators

Let G be a set. A binary operator on G is a map

$$\begin{aligned} * : G \times G &\to G, \\ (x, y) &\mapsto x * y. \end{aligned}$$

Properties of binary operators

We say that

i) $*$ is commutative if $\forall a, b \in X, a * b = b * a$.

ii) $*$ is associative if $\forall a, b, c \in X, (a * b) * c = a * (b * c)$.

Binary operators

Binary operators

Let G be a set. A binary operator on G is a map

$$\begin{aligned} * : G \times G &\to G, \\ (x, y) &\mapsto x * y. \end{aligned}$$

Properties of binary operators

We say that

i) $*$ is commutative if $\forall a, b \in X, a * b = b * a$.

ii) $*$ is associative if $\forall a, b, c \in X, (a * b) * c = a * (b * c)$.

iii) e is the identity for $*$ if $\forall a \in X, a * e = e * a = a$.

Binary operators

Binary operators

Let G be a set. A binary operator on G is a map

$$\begin{aligned} * : G \times G &\to G, \\ (x, y) &\mapsto x * y. \end{aligned}$$

Properties of binary operators

We say that

i) $*$ is commutative if $\forall a, b \in X, a * b = b * a$.

ii) $*$ is associative if $\forall a, b, c \in X, (a * b) * c = a * (b * c)$.

iii) e is the identity for $*$ if $\forall a \in X, a * e = e * a = a$.

iv) $x' \in X$ is called the inverse element of x if $x * x' = x' * x = e$.

Binary operators

i) commutative $a * b = b * a$.

ii) associative $(a * b) * c = a * (b * c)$.

iii) identity $a * e = e * a = a$.

iv) the inverse $x * x' = x' * x = e$.

Example

Consider the commutativity, associativity and find the identity element, the inverse element.

a) $x * y := xy + 1$,

b) $x * y := \frac{1}{2}xy$,

c) $(x_1, x_2) \circ (y_1, y_2) := \left(\frac{x_1+y_1}{2}, \frac{x_2+y_2}{2}\right)$.

Groups

Definition

A group is a pair $(G, *)$ *satisfies*

G1) *Associativity:*

$$(x * y) * z = x * (y * z), \quad \forall x, y, z \in G,$$

G2) $\exists$ *the identity element* e

$$x * e = e * x = x, \quad \forall x \in G,$$

G3) $\exists$ *the inverse for any* $x \in G$

$$x * x' = x' * x = e.$$

Groups

Definition

A group is a pair $(G, *)$ *satisfies*

G1) *Associativity:*

$$(x * y) * z = x * (y * z), \quad \forall x, y, z \in G,$$

G2) $\exists$ *the identity element* e

$$x * e = e * x = x, \quad \forall x \in G,$$

G3) $\exists$ *the inverse for any* $x \in G$

$$x * x' = x' * x = e.$$

G is called *commutative* or abelian if $x * y = y * x, \ \forall x, y \in G$.

Groups

	Logics		Sets		Maps	$\mathbb{N}$		$\mathbb{Z}$		$\mathbb{Q}$		$\mathbb{R}$	
	$\vee$	$\wedge$	$\cup$	$\cap$	$\circ$	$+$	$\times$	$+$	$\times$	$+$	$\times$	$+$	$\times$
Asso.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Identity	F	T	$\emptyset$	X	Id	0	1	0	1	0	1	0	1
Inverse	x	x	x	x	f^{-1}	✓	x	✓	x	✓	x	✓	x
Commu.	✓	✓	✓	✓	x	✓	✓	✓	✓	✓	✓	✓	✓

i) Logics $=$ the set of propositions,

ii) Sets $= P(X)$ the collection of subsets of X,

iii) Maps $= B(X)$ the set of bijection from X to X.

Open your mind

$$1+1=1$$

$$1+2=2 \qquad 2+1=2$$

$$2+2 = 1$$

Open your mind

$$1+1=1$$

$$1+2=2 \qquad 2+1=2$$

$$2+2=1$$

wtf? No, I'm not kidding!

Open your mind

$$1+1=1$$

$$1+2=2 \qquad 2+1=2$$

$$2+2=1$$

wtf? No, I'm not kidding!

Prove that $(\{1,2\},+)$ is a group.

Groups

Properties

1) the identity element e is unique.
2) the inverse element x' of x is unique.

Groups

Properties

1) the identity element e is unique.
2) the inverse element x' of x is unique.
3) Division $\begin{cases} x * y = x * z \Rightarrow y = z, \\ x * z = y * z \Rightarrow x = y. \end{cases}$

Groups

Properties

1) the identity element e is unique.
2) the inverse element x' of x is unique.
3) Division $\begin{cases} x * y = x * z \Rightarrow y = z, \\ x * z = y * z \Rightarrow x = y. \end{cases}$

Notationally,

i) $"+"$ the identity $e := 0$ and the inverse element of x is $-x$.

ii) $"\times"$ the identity $e =: 1$ and the inverse element of x is x^{-1}.

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Example

1) $(\mathbb{N}, +)$,

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Example

1) $(\mathbb{N}, +), (\mathbb{N}, \times),$

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Example

1) $(\mathbb{N}, +), (\mathbb{N}, \times), (\mathbb{Z}, +),$

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Example

1) $(\mathbb{N}, +), (\mathbb{N}, \times), (\mathbb{Z}, +), (\mathbb{Z}, \times),$

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Example

1) $(\mathbb{N}, +), (\mathbb{N}, \times), (\mathbb{Z}, +), (\mathbb{Z}, \times), (\mathbb{Q}, +),$

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Example

1) $(\mathbb{N}, +), (\mathbb{N}, \times), (\mathbb{Z}, +), (\mathbb{Z}, \times), (\mathbb{Q}, +), (\mathbb{Q}, \times),$

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Example

1) $(\mathbb{N}, +), (\mathbb{N}, \times), (\mathbb{Z}, +), (\mathbb{Z}, \times), (\mathbb{Q}, +), (\mathbb{Q}, \times), (\mathbb{R}, +),$

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Example

1) $(\mathbb{N}, +), (\mathbb{N}, \times), (\mathbb{Z}, +), (\mathbb{Z}, \times), (\mathbb{Q}, +), (\mathbb{Q}, \times), (\mathbb{R}, +), (\mathbb{R}, \times),$

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Example

1) $(\mathbb{N}, +), (\mathbb{N}, \times), (\mathbb{Z}, +), (\mathbb{Z}, \times), (\mathbb{Q}, +), (\mathbb{Q}, \times), (\mathbb{R}, +), (\mathbb{R}, \times)$,
2) $(\mathbb{Z}/5, +)$,

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Example

1) $(\mathbb{N}, +), (\mathbb{N}, \times), (\mathbb{Z}, +), (\mathbb{Z}, \times), (\mathbb{Q}, +), (\mathbb{Q}, \times), (\mathbb{R}, +), (\mathbb{R}, \times)$,
2) $(\mathbb{Z}/5, +), (\mathbb{Z}/5, \times)$,

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Example

1) $(\mathbb{N}, +), (\mathbb{N}, \times), (\mathbb{Z}, +), (\mathbb{Z}, \times), (\mathbb{Q}, +), (\mathbb{Q}, \times), (\mathbb{R}, +), (\mathbb{R}, \times)$,
2) $(\mathbb{Z}/5, +), (\mathbb{Z}/5, \times)$,
3) $(2\mathbb{Z}, +)$,

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Example

1) $(\mathbb{N}, +), (\mathbb{N}, \times), (\mathbb{Z}, +), (\mathbb{Z}, \times), (\mathbb{Q}, +), (\mathbb{Q}, \times), (\mathbb{R}, +), (\mathbb{R}, \times)$,
2) $(\mathbb{Z}/5, +), (\mathbb{Z}/5, \times)$,
3) $(2\mathbb{Z}, +), (2\mathbb{Z}, \times)$,

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Example

1) $(\mathbb{N}, +), (\mathbb{N}, \times), (\mathbb{Z}, +), (\mathbb{Z}, \times), (\mathbb{Q}, +), (\mathbb{Q}, \times), (\mathbb{R}, +), (\mathbb{R}, \times)$,
2) $(\mathbb{Z}/5, +), (\mathbb{Z}/5, \times)$,
3) $(2\mathbb{Z}, +), (2\mathbb{Z}, \times), (2\mathbb{Z} + 1, +)$,

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Example

1) $(\mathbb{N}, +), (\mathbb{N}, \times), (\mathbb{Z}, +), (\mathbb{Z}, \times), (\mathbb{Q}, +), (\mathbb{Q}, \times), (\mathbb{R}, +), (\mathbb{R}, \times)$,
2) $(\mathbb{Z}/5, +), (\mathbb{Z}/5, \times)$,
3) $(2\mathbb{Z}, +), (2\mathbb{Z}, \times), (2\mathbb{Z} + 1, +), (2\mathbb{Z} + 1, \times)$,

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Example

1) $(\mathbb{N}, +), (\mathbb{N}, \times), (\mathbb{Z}, +), (\mathbb{Z}, \times), (\mathbb{Q}, +), (\mathbb{Q}, \times), (\mathbb{R}, +), (\mathbb{R}, \times)$,
2) $(\mathbb{Z}/5, +), (\mathbb{Z}/5, \times)$,
3) $(2\mathbb{Z}, +), (2\mathbb{Z}, \times), (2\mathbb{Z}+1, +), (2\mathbb{Z}+1, \times)$,
4) $(X = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}, +)$,

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Example

1) $(\mathbb{N}, +), (\mathbb{N}, \times), (\mathbb{Z}, +), (\mathbb{Z}, \times), (\mathbb{Q}, +), (\mathbb{Q}, \times), (\mathbb{R}, +), (\mathbb{R}, \times)$,
2) $(\mathbb{Z}/5, +), (\mathbb{Z}/5, \times)$,
3) $(2\mathbb{Z}, +), (2\mathbb{Z}, \times), (2\mathbb{Z}+1, +), (2\mathbb{Z}+1, \times)$,
4) $(X = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}, +)$,
5) $(X = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}, \times)$,

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Example

1) $(\mathbb{N}, +), (\mathbb{N}, \times), (\mathbb{Z}, +), (\mathbb{Z}, \times), (\mathbb{Q}, +), (\mathbb{Q}, \times), (\mathbb{R}, +), (\mathbb{R}, \times)$,
2) $(\mathbb{Z}/5, +), (\mathbb{Z}/5, \times)$,
3) $(2\mathbb{Z}, +), (2\mathbb{Z}, \times), (2\mathbb{Z}+1, +), (2\mathbb{Z}+1, \times)$,
4) $(X = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}, +)$,
5) $(X = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}, \times)$,
6) $(X = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}, +)$,

Groups

Example

Let X be arbitrary set and $x * y = x, \forall x, y \in X$. Prove that $(X, *)$ is a semigroup.

Example

1) $(\mathbb{N}, +), (\mathbb{N}, \times), (\mathbb{Z}, +), (\mathbb{Z}, \times), (\mathbb{Q}, +), (\mathbb{Q}, \times), (\mathbb{R}, +), (\mathbb{R}, \times)$,
2) $(\mathbb{Z}/5, +), (\mathbb{Z}/5, \times)$,
3) $(2\mathbb{Z}, +), (2\mathbb{Z}, \times), (2\mathbb{Z}+1, +), (2\mathbb{Z}+1, \times)$,
4) $(X = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}, +)$,
5) $(X = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}, \times)$,
6) $(X = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}, +)$,
7) $(X = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}, \times)$.

Group homomorphism

Group homomorphism

Let G and G' be groups. The map $\varphi : G \to G'$ is called a group homomorphism if

$$\varphi(xy) = \varphi(x)\varphi(y),\ \forall x, y \in G.$$

Remark: $\varphi(e) = e', \quad \varphi(x^{-1}) = [\varphi(x)]^{-1}.$

Group homomorphism

Group homomorphism

Let G and G' be groups. The map $\varphi : G \to G'$ is called a group homomorphism if

$$\varphi(xy) = \varphi(x)\varphi(y), \ \forall x, y \in G.$$

Remark: $\varphi(e) = e'$, $\quad \varphi(x^{-1}) = [\varphi(x)]^{-1}$.

Definition

1) *Group homomorphism + injective = Monomorphism,*
2) *Group homomorphism + surjective = Epimorphism,*
3) *Group homomorphism + bijective = Isomorphism, write* $G \cong G'$.

Group homomorphism

Definition

1) Group homomorphism + injective = Monomorphism,

2) Group homomorphism + surjective = Epimorphism,

3) Group homomorphism + bijective = Isomorphism, write $G \cong G'$.

Example

i) $i : \mathbb{Z} \to \mathbb{Q}, n \mapsto n$ is a Monomorphism.

ii) The projection $p : \mathbb{Z} \to \mathbb{Z}/n$ is an Epimorphism.

iii) $\exp : \mathbb{R} \to \mathbb{R}^+, x \mapsto e^x$ is an Isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$.

Rings

Definition

A ring is a tripple $(R, +, \times)$ *satisfies*

R1) $(R, +)$ *is a commutative group.*

R2) $\times$ *is associative:*

$$(xy)z = x(yz), \quad \forall x, y, z \in R$$

R3) *distributive*

$$\begin{aligned}(x+y)z &= xz + yz \\ z(x+y) &= zx + zy, \quad \forall x, y, z \in R\end{aligned}$$

Rings

Definition

A ring is a tripple $(R, +, \times)$ *satisfies*

R1) $(R, +)$ *is a commutative group.*

R2) $\times$ *is associative:*

$$(xy)z = x(yz), \quad \forall x, y, z \in R$$

R3) *distributive*

$$\begin{aligned}(x+y)z &= xz + yz \\ z(x+y) &= zx + zy, \quad \forall x, y, z \in R\end{aligned}$$

i) *commutative* or *abelian* $xy = yx, \quad \forall x, y \in R.$

ii) *Ring with identity* $\exists e$ such that $ex = xe = x, \quad \forall x \in R.$

Rings

	$\mathbb{N}$		$\mathbb{Z}$		$\mathbb{Q}$		$\mathbb{R}$	
	$+$	$\times$	$+$	$\times$	$+$	$\times$	$+$	$\times$
R1	x		✓		✓		✓	
R2	✓		✓		✓		✓	
R3	✓		✓		✓		✓	
commutative		✓		✓		✓		✓
with identity		✓		✓		✓		✓

Rings

	$\mathbb{N}$		$\mathbb{Z}$		$\mathbb{Q}$		$\mathbb{R}$	
	$+$	$\times$	$+$	$\times$	$+$	$\times$	$+$	$\times$
R1	x		✓		✓		✓	
R2	✓		✓		✓		✓	
R3	✓		✓		✓		✓	
commutative		✓		✓		✓		✓
with identity		✓		✓		✓		✓

Example

Let $X = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$ and $Y = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$.

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2},$$

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2},$$

Fields

Definition

F is a field if

i) F is a commutative ring with identity $1 \neq 0$.

ii) $\exists$ *the inverse element* x^{-1} *for every* $x \neq 0$.

Fields

Definition

F is a field if

i) F is a commutative ring with identity $1 \neq 0$.

ii) $\exists$ the inverse element x^{-1} for every $x \neq 0$.

Example

a) $(\mathbb{Z}, +, \times)$ is not a field.

Fields

Definition

F is a field if

i) F is a commutative ring with identity $1 \neq 0$.

ii) $\exists$ *the inverse element* x^{-1} *for every* $x \neq 0$.

Example

a) $(\mathbb{Z}, +, \times)$ is not a field.

b) $(\mathbb{Q}, +, \times), (\mathbb{R}, +, \times)$ are fields.

Fields

Definition

F is a field if

i) F is a commutative ring with identity $1 \neq 0$.

ii) $\exists$ the inverse element x^{-1} for every $x \neq 0$.

Example

a) $(\mathbb{Z}, +, \times)$ is not a field.

b) $(\mathbb{Q}, +, \times), (\mathbb{R}, +, \times)$ are fields.

Example

Let $X = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$ and $Y = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$.

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2},$$

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2},$$

The characteristic of a field

Definition

Let R be a ring with identity 1. The smallest natural number n such that $0 = 1 + 1 + \cdots + 1$ (n terms) is called the characteristic of the ring R and is denoted by $\mathrm{Char}(R)$. If there is no such natural number, then the characteristic is zero.

Example

a) $\mathrm{Char}(\mathbb{Z}) = \mathrm{Char}(\mathbb{Q}) = 0$,

b) $\mathrm{Char}(\mathbb{Z}/n) = n$.

The characteristic of a field

Definition

Let R be a ring with identity 1. The smallest natural number n such that $0 = 1 + 1 + \cdots + 1$ (n terms) is called the characteristic of the ring R and is denoted by $\mathrm{Char}(R)$. If there is no such natural number, then the characteristic is zero.

Example

a) $\mathrm{Char}(\mathbb{Z}) = \mathrm{Char}(\mathbb{Q}) = 0$,

b) $\mathrm{Char}(\mathbb{Z}/n) = n$.

Proposition

If R is a field, then $\mathrm{Char}(R)$ is either 0 or a prime number.

Ring of integers

Definition

Let $m, n \in \mathbb{Z}$. We say that m divides n and write $m|n$ if

$$n = km, \text{ for some } k \in \mathbb{Z}.$$

Ring of integers

Definition

Let $m, n \in \mathbb{Z}$. We say that m divides n and write $m|n$ if

$$n = km, \text{ for some } k \in \mathbb{Z}.$$

Then m is a divisor of n and n is a multiple of m.

Ring of integers

Definition

Let $m, n \in \mathbb{Z}$. *We say that* m *divides* n *and write* $m|n$ *if*

$$n = km, \text{ for some } k \in \mathbb{Z}.$$

Then m *is a divisor of* n *and* n *is a multiple of* m.

Definition

If $a, d \in \mathbb{Z}$ *and* $d > 0$ *then there exist unique integers* q *and* r *such that*

$$a = qd + r, 0 \leq r < d.$$

Ring of integers

Definition

Let $m, n \in \mathbb{Z}$. We say that m divides n and write $m|n$ if

$$n = km, \text{ for some } k \in \mathbb{Z}.$$

Then m is a divisor of n and n is a multiple of m.

Definition

If $a, d \in \mathbb{Z}$ and $d > 0$ then there exist unique integers q and r such that

$$a = qd + r, 0 \leq r < d.$$

The number q is called the quotient and r is called the remainder.

Ring of integers

Definition

Let $m, n \in \mathbb{Z}$. *We say that* m *divides* n *and write* $m|n$ *if*

$$n = km, \text{ for some } k \in \mathbb{Z}.$$

Then m *is a divisor of* n *and* n *is a multiple of* m.

Definition

If $a, d \in \mathbb{Z}$ *and* $d > 0$ *then there exist unique integers* q *and* r *such that*

$$a = qd + r, 0 \leq r < d.$$

The number q *is called the quotient and* r *is called the remainder.*

Ring of integers

Definition

Two integers a, b are said to be congruent modulo n if $n|(a-b)$.

Proposition

The congruence modulo m relation is an equivalence relation.

The set of congruence class modulo m is denoted by

$$\mathbb{Z}_m := \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}.$$

Ring of integers

Definition

Two integers a, b are said to be congruent modulo n if $n|(a-b)$.

Proposition

The congruence modulo m relation is an equivalence relation.

The set of congruence class modulo m is denoted by

$$\mathbb{Z}_m := \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}.$$

Proposition

$\mathbb{Z}_m$ together with the addition and multiplication defined as follow

$$\bar{a} + \bar{b} = \overline{a+b}, \quad \bar{a}.\bar{b} = \overline{ab}$$

is a ring.

Euclidean Algorithm

Definition

Given two natural integers a, b.

i) $\mathrm{GCD}(a, b) = \max\{d \text{ such that } d|a, d|b\}$.

ii) $\mathrm{LCD}(a, b) = \min\{d \text{ such that } a|d, b|d\}$.

If $\mathrm{GCD}(a, b) = 1$ then a, b are said to be coprime.

Euclidean Algorithm

Definition

Given two natural integers a, b.

i) $\text{GCD}(a, b) = \max\{d \textit{ such that } d|a, d|b\}$.

ii) $\text{LCD}(a, b) = \min\{d \textit{ such that } a|d, b|d\}$.

If $\text{GCD}(a, b) = 1$ then a, b are said to be coprime.

Proposition

For natural numbers a, b we have $ab = \text{GCD}(a, b).\text{LCD}(a, b)$.

Euclidean Algorithm

Definition

Given two natural integers a, b.

i) $\mathrm{GCD}(a, b) = \max\{d \textit{ such that } d|a, d|b\}$.

ii) $\mathrm{LCD}(a, b) = \min\{d \textit{ such that } a|d, b|d\}$.

If $\mathrm{GCD}(a, b) = 1$ then a, b are said to be coprime.

Proposition

For natural numbers a, b *we have* $ab = \mathrm{GCD}(a, b).\mathrm{LCD}(a, b)$.

Proposition

Suppose that natural numbers a, b, q, r *satisfy*

$$a = bq + r,$$

then $\mathrm{GCD}(a, b) = \mathrm{GCD}(b, r)$.

The greatest common divisor

Euclidean Algorithm

1) Express $a = bq_1 + r_1$,
2) $b = r_1 q_2 + r_2$,
3) $r_1 = r_2 q_3 + r_3$,
4) $\cdots$
5) $r_{k-2} = r_{k-1} q_k + r_k$,
6) The last step $r_{n-1} = r_n q_{n+1}$.

Then $r_n = \text{GCD}(a, b)$.

The greatest common divisor

Euclidean Algorithm

1) Express $a = bq_1 + r_1$,
2) $b = r_1 q_2 + r_2$,
3) $r_1 = r_2 q_3 + r_3$,
4) $\cdots$
5) $r_{k-2} = r_{k-1} q_k + r_k$,
6) The last step $r_{n-1} = r_n q_{n+1}$.

Then $r_n = \mathrm{GCD}(a, b)$.

Example

Find $\mathrm{GCD}(3195, 630), \mathrm{GCD}(1243, 3124), \mathrm{GCD}(123456789, 987654321)$

The greatest common divisor

Euclidean Algorithm

1) Express $a = bq_1 + r_1$,
2) $b = r_1 q_2 + r_2$,
3) $r_1 = r_2 q_3 + r_3$,
4) $\cdots$
5) $r_{k-2} = r_{k-1} q_k + r_k$,
6) The last step $r_{n-1} = r_n q_{n+1}$.

Then $r_n = \mathrm{GCD}(a, b)$.

Example

Find $\mathrm{GCD}(3195, 630), \mathrm{GCD}(1243, 3124), \mathrm{GCD}(123456789, 987654321)$

Example

Find integers a, b such that $1243a + 3124b = 11$.

Presentation of integers

Definition

Given a positive integer b. If

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0, \quad 0 \leq a_j < b, a_k \neq 0,$$

then the above presentation is said to be the expansion of n by base b and we denote $n = (a_k a_{k-1} \cdots a_1 a_0)_b$.

If $b = 2$ then we have the binary expansion of n.

Presentation of integers

Definition

Given a positive integer b. If

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0, \quad 0 \leq a_j < b, a_k \neq 0,$$

then the above presentation is said to be the expansion of n by base b and we denote $n = (a_k a_{k-1} \cdots a_1 a_0)_b$.

If $b = 2$ then we have the binary expansion of n.

Algorithm for expantion of n by base b.

1) Write $n = bq_0 + a_0$,
2) $q_0 = bq_1 + a_1$,
3) $\cdots$
4) The last step $q_{m-1} = bq_m + a_m$ if $q_m = 0$.

Then $n = (a_m a_{m-1} \ldots a_1 a_0)_b$.

Presentation ofintegers

Example

Presentation the following numbers by the base 6:

a) 2011, b) 3125.

Presentation ofintegers

Example

Presentation the following numbers by the base 6:

a) 2011,

b) 3125.

Example

a) $3145_{(7)} + 5436_{(7)}$,

b) $6145_{(7)} - 5451_{(7)}$,

c) $3142_{(7)} : 6_{(7)}$,

d) $3142_{(7)} \times 54_{(7)}$.

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	11	13	15
3	3	6	12	15	21	24
4	4	11	15	22	26	33
5	5	13	21	26	34	42
6	6	15	24	33	42	51

Field of Complex Numbers

Introduction

i) The eq. $X^2 - 2 = 0$ has no rational solution $\Rightarrow$ construct the field of real numbers,

Field of Complex Numbers

Introduction

i) The eq. $X^2 - 2 = 0$ has no rational solution $\Rightarrow$ construct the field of real numbers,

ii) The eq. $X^2 + 1 = 0$ has no real solution $\Rightarrow$ construct new numbers.

Field of Complex Numbers

Introduction

i) The eq. $X^2 - 2 = 0$ has no rational solution $\Rightarrow$ construct the field of real numbers,

ii) The eq. $X^2 + 1 = 0$ has no real solution $\Rightarrow$ construct new numbers.

iii) Let i be a "formal notation" that satisfies $i^2 = -1$. Then, we have numbers of the form $a + bi, a, b \in \mathbb{R}$.

Field of Complex Numbers

Introduction

i) The eq. $X^2 - 2 = 0$ has no rational solution $\Rightarrow$ construct the field of real numbers,

ii) The eq. $X^2 + 1 = 0$ has no real solution $\Rightarrow$ construct new numbers.

iii) Let i be a "formal notation" that satisfies $i^2 = -1$. Then, we have numbers of the form $a + bi, a, b \in \mathbb{R}$.

Let $\mathbb{C} = \mathbb{R} \times \mathbb{R}$. No structure is provided.

The field of complex numbers

We define

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, c)(c, d) = (ac - bd, ad + bc).$$

Proposition

$(\mathbb{C}, +, \times)$ *is a field, called the field of complex numbers.*

The field of complex numbers

We define

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, c)(c, d) = (ac - bd, ad + bc).$$

Proposition

$(\mathbb{C}, +, \times)$ *is a field, called the field of complex numbers.*

Remark

i) The additive identity is

The field of complex numbers

We define

$$(a,b)+(c,d)=(a+c,b+d),\quad (a,c)(c,d)=(ac-bd,ad+bc).$$

Proposition

$(\mathbb{C},+,\times)$ *is a field, called the field of complex numbers.*

Remark

i) The additive identity is $(0,0)$.

ii) The multiplicative identity is

The field of complex numbers

We define

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, c)(c, d) = (ac - bd, ad + bc).$$

Proposition

$(\mathbb{C}, +, \times)$ *is a field, called the field of complex numbers.*

Remark

i) The additive identity is $(0, 0)$.

ii) The multiplicative identity is $(1, 0)$.

iii) The inverse element of $(a, b) \neq (0, 0)$ is $(a, b)^{-1} =$

The field of complex numbers

We define

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, c)(c, d) = (ac - bd, ad + bc).$$

Proposition

$(\mathbb{C}, +, \times)$ *is a field, called the field of complex numbers.*

Remark

i) The additive identity is $(0, 0)$.

ii) The multiplicative identity is $(1, 0)$.

iii) The inverse element of $(a, b) \neq (0, 0)$ is $(a, b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$.

The field of complex numbers

We define

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, c)(c, d) = (ac - bd, ad + bc).$$

Proposition

$(\mathbb{C}, +, \times)$ *is a field, called the field of complex numbers.*

Remark

i) The additive identity is $(0, 0)$.

ii) The multiplicative identity is $(1, 0)$.

iii) The inverse element of $(a, b) \neq (0, 0)$ is $(a, b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$.

iv) what is i?

The field of complex numbers

Real numbers

$$(a,0)+(b,0)=(a+b,0), \quad (a,0)(b,0)=(ab,0).$$

Each $(a,0)\in\mathbb{C}$ behaves like $a\in\mathbb{R}$.

The field of complex numbers

Real numbers

$$(a,0)+(b,0)=(a+b,0), \quad (a,0)(b,0)=(ab,0).$$

Each $(a,0)\in\mathbb{C}$ behaves like $a\in\mathbb{R}$.

Canonical form

Let $i=(0,1)$, then $i^2=(0,1)(0,1)=(-1,0)\equiv -1$.

$$z=(a,b)=a(1,0)+b(0,1)=a+bi$$

What is i

i is nothing but $(0,1)$

The canonical form of complex numbers

Definition

$z = a + bi$, *where* $a, b \in \mathbb{R}$ *and* $i^2 = -1$, *is called the canonical form of* z.

i) $a = \mathrm{Re}(z)$ *the real part,*

ii) $b = \mathrm{Im}(z)$ *the imaginary part.*

The canonical form of complex numbers

Definition

$z = a + bi$, where $a, b \in \mathbb{R}$ and $i^2 = -1$, is called the canonical form of z.

i) $a = \mathrm{Re}(z)$ the real part,

ii) $b = \mathrm{Im}(z)$ the imaginary part.

Operations in canonical form

i) Addition $(a + bi) + (c + di) =$

The canonical form of complex numbers

Definition

$z = a + bi$, *where* $a, b \in \mathbb{R}$ *and* $i^2 = -1$, *is called the canonical form of* z.

i) $a = \mathrm{Re}(z)$ *the real part,*

ii) $b = \mathrm{Im}(z)$ *the imaginary part.*

Operations in canonical form

i) Addition $(a + bi) + (c + di) = (a + c) + (b + d)i$,

The canonical form of complex numbers

Definition

$z = a + bi$, where $a, b \in \mathbb{R}$ and $i^2 = -1$, is called the canonical form of z.

i) $a = \operatorname{Re}(z)$ the real part,

ii) $b = \operatorname{Im}(z)$ the imaginary part.

Operations in canonical form

i) Addition $(a + bi) + (c + di) = (a + c) + (b + d)i$,

ii) Subtraction $(a + bi) - (c + di) =$

The canonical form of complex numbers

Definition

$z = a + bi$, where $a, b \in \mathbb{R}$ and $i^2 = -1$, is called the canonical form of z.

i) $a = \mathrm{Re}(z)$ the real part,

ii) $b = \mathrm{Im}(z)$ the imaginary part.

Operations in canonical form

i) Addition $(a + bi) + (c + di) = (a + c) + (b + d)i$,

ii) Subtraction $(a + bi) - (c + di) = (a - c) + (b - d)i$,

The canonical form of complex numbers

Definition

$z = a + bi$, *where* $a, b \in \mathbb{R}$ *and* $i^2 = -1$, *is called the canonical form of* z.

i) $a = \mathrm{Re}(z)$ *the real part,*

ii) $b = \mathrm{Im}(z)$ *the imaginary part.*

Operations in canonical form

i) Addition $(a + bi) + (c + di) = (a + c) + (b + d)i$,

ii) Subtraction $(a + bi) - (c + di) = (a - c) + (b - d)i$,

iii) Multiplication $(a + bi)(c + di) =$

The canonical form of complex numbers

Definition

$z = a + bi$, *where* $a, b \in \mathbb{R}$ *and* $i^2 = -1$, *is called the canonical form of* z.

i) $a = \text{Re}(z)$ *the real part,*

ii) $b = \text{Im}(z)$ *the imaginary part.*

Operations in canonical form

i) Addition $(a + bi) + (c + di) = (a + c) + (b + d)i$,

ii) Subtraction $(a + bi) - (c + di) = (a - c) + (b - d)i$,

iii) Multiplication $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$,

The canonical form of complex numbers

Definition

$z = a + bi$, *where* $a, b \in \mathbb{R}$ *and* $i^2 = -1$, *is called the canonical form of* z.

i) $a = \mathrm{Re}(z)$ *the real part,*

ii) $b = \mathrm{Im}(z)$ *the imaginary part.*

Operations in canonical form

i) Addition $(a + bi) + (c + di) = (a + c) + (b + d)i$,

ii) Subtraction $(a + bi) - (c + di) = (a - c) + (b - d)i$,

iii) Multiplication $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$,

iv) Division $\frac{a+bi}{c+di} =$

The canonical form of complex numbers

Definition

$z = a + bi$, *where* $a, b \in \mathbb{R}$ *and* $i^2 = -1$, *is called the canonical form of* z.

i) $a = \mathrm{Re}(z)$ *the real part,*

ii) $b = \mathrm{Im}(z)$ *the imaginary part.*

Operations in canonical form

i) Addition $(a + bi) + (c + di) = (a + c) + (b + d)i$,

ii) Subtraction $(a + bi) - (c + di) = (a - c) + (b - d)i$,

iii) Multiplication $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$,

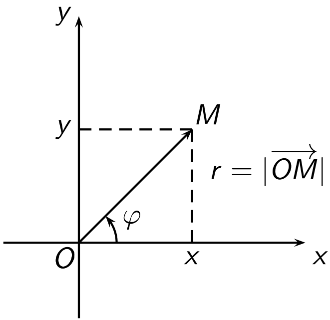
iv) Division $\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{c^2+d^2}$

Polar form of complex numbers

Let $\begin{cases} r = |\overrightarrow{OM}| \\ \varphi = (Ox, \overrightarrow{OM}) \end{cases}$ then $z = r(\cos\varphi + i\sin\varphi)$ (the polar form).

i) Modulus $|z| = \sqrt{a^2 + b^2}$,

ii) Argument $\operatorname{Arg} z = \varphi$.



Polar form of complex numbers

Let $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1), \quad z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2).$

Operations in polar form

1) Multiplication

$$z_1 z_2 =$$

Polar form of complex numbers

Let $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1), \quad z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2).$

Operations in polar form

1) Multiplication

$$z_1 z_2 = r_1 r_2.[\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)]$$

Hence, $|z_1 z_2| = |z_1||z_2|, \quad \operatorname{Arg}(z_1 z_2) = \operatorname{Arg} z_1 + \operatorname{Arg} z_2.$

Polar form of complex numbers

Let $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1), \quad z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$.

Operations in polar form

1) Multiplication

$$z_1 z_2 = r_1 r_2.[\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)]$$

$$\text{Hence, } |z_1 z_2| = |z_1||z_2|, \quad \operatorname{Arg}(z_1 z_2) = \operatorname{Arg} z_1 + \operatorname{Arg} z_2.$$

2) Division

$$\frac{z_1}{z_2} =$$

Polar form of complex numbers

Let $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1), \quad z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$.

Operations in polar form

1) Multiplication

$$z_1 z_2 = r_1 r_2.[\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)]$$

$$\text{Hence, } |z_1 z_2| = |z_1||z_2|, \quad \operatorname{Arg}(z_1 z_2) = \operatorname{Arg} z_1 + \operatorname{Arg} z_2.$$

2) Division

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}.\left(\cos(\varphi_1-\varphi_2) + i\sin(\varphi_1-\varphi_2)\right)$$

$$\text{Hence } \left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|}, \quad \operatorname{Arg}\left(\frac{z_1}{z_2}\right) = \operatorname{Arg} z_1 - \operatorname{Arg} z_2.$$

Polar form of complex numbers

Let $z = r(\cos\varphi + i\sin\varphi) \neq 0$.

Operations in polar form

3) Power (Moirve's formula)

$$z^n =$$

Polar form of complex numbers

Let $z = r(\cos\varphi + i\sin\varphi) \neq 0$.

Operations in polar form

3) Power (Moirve's formula)

$$z^n = r^n(\cos n\varphi + i\sin n\varphi)$$

Hence $|z^n| = |z|^n$

Polar form of complex numbers

Let $z = r(\cos\varphi + i\sin\varphi) \neq 0.$

Operations in polar form

3) Power (Moirve's formula)

$$z^n = r^n(\cos n\varphi + i\sin n\varphi)$$

$$\text{Hence } |z^n| = |z|^n$$

4) *n*-roots

$$\sqrt[n]{z} =$$

Polar form of complex numbers

Let $z = r(\cos\varphi + i\sin\varphi) \neq 0$.

Operations in polar form

3) Power (Moirve's formula)

$$z^n = r^n(\cos n\varphi + i\sin n\varphi)$$

$$\text{Hence } |z^n| = |z|^n$$

4) n-roots

$$\sqrt[n]{z} = \sqrt[n]{r}\left[\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}\right], k = \overline{0, n-1}.$$

Each nonzero complex number has exactly n different n-roots.

The field of complex numbers

Example

Find the canonical form of

a) $(1+i\sqrt{3})^9$,

b) $\frac{(1+i)^{21}}{(1-i)^{13}}$,

c) $(2+i\sqrt{12})^5(\sqrt{3}-i)^{11}$.

The field of complex numbers

Example

Find the canonical form of

a) $(1 + i\sqrt{3})^9$,

b) $\frac{(1+i)^{21}}{(1-i)^{13}}$,

c) $(2 + i\sqrt{12})^5(\sqrt{3} - i)^{11}$.

Example

Solve the following equations

a) $z^2 + z + 1 = 0$,

b) $z^2 + 2iz - 5 = 0$,

c) $z^4 - 3iz^2 + 4 = 0$,

d) $z^6 - 7z^3 - 8 = 0$,

e) $\frac{(z+i)^4}{(z-i)^4} = 1$,

f) $z^8(\sqrt{3} + i) = 1 - i$.

The field of complex numbers

Example

Find the canonical form of

a) $(1+i\sqrt{3})^9$,

b) $\frac{(1+i)^{21}}{(1-i)^{13}}$,

c) $(2+i\sqrt{12})^5(\sqrt{3}-i)^{11}$.

Example

Solve the following equations

a) $z^2+z+1=0$,

b) $z^2+2iz-5=0$,

c) $z^4-3iz^2+4=0$,

d) $z^6-7z^3-8=0$,

e) $\frac{(z+i)^4}{(z-i)^4}=1$,

f) $z^8(\sqrt{3}+i)=1-i$.

Example

Prove that if $z+\frac{1}{z}=2\cos\varphi$, then $z^n+\frac{1}{z^n}=2\cos n\varphi, \forall n\in\mathbb{N}$.

The field of complex numbers

Example

a) Find the sum of n-roots of the complex number 1.

b) Find the sum of n-roots of an arbitrary complex number $z \neq 0$.

c) Let $\epsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}, k = 0, 1, \ldots, n-1$. Compute $S = \sum_{k=0}^{n-1} \epsilon_k^m, \ (m \in \mathbb{N})$.

Example

Consider the equation $\frac{(z+1)^9 - 1}{z} = 0$.

a) Solve the above equation.

b) Compute the moduli of the solutions.

c) Compute the product of its solutions and $\prod_{k=1}^{8} \sin \frac{k\pi}{9}$.

Conjugation of complex numbers

Let $z = a + bi$.

i) $\overline{z} = a - bi$ is called the conjugate of z.

ii) In polar form, $z = r(\cos\varphi + i\sin\varphi) \Rightarrow \overline{z} = r(\cos\varphi - i\sin\varphi)$.

Properties

1) $\overline{\overline{z}} = z$

Conjugation of complex numbers

Let $z = a + bi$.

i) $\overline{z} = a - bi$ is called the conjugate of z.

ii) In polar form, $z = r(\cos\varphi + i\sin\varphi) \Rightarrow \overline{z} = r(\cos\varphi - i\sin\varphi)$.

Properties

1) $\overline{\overline{z}} = z$

2) $z + \overline{z} = 2a = 2\operatorname{Re} z$

Conjugation of complex numbers

Let $z = a + bi$.

i) $\overline{z} = a - bi$ is called the conjugate of z.

ii) In polar form, $z = r(\cos\varphi + i\sin\varphi) \Rightarrow \overline{z} = r(\cos\varphi - i\sin\varphi)$.

Properties

1) $\overline{\overline{z}} = z$
2) $z + \overline{z} = 2a = 2\,\mathrm{Re}\,z$
3) $z\overline{z} = a^2 + b^2 = |z|^2$

Conjugation of complex numbers

Let $z = a + bi$.

i) $\overline{z} = a - bi$ is called the conjugate of z.

ii) In polar form, $z = r(\cos\varphi + i\sin\varphi) \Rightarrow \overline{z} = r(\cos\varphi - i\sin\varphi)$.

Properties

1) $\overline{\overline{z}} = z$
2) $z + \overline{z} = 2a = 2\operatorname{Re} z$
3) $z\overline{z} = a^2 + b^2 = |z|^2$
4) $\frac{1}{z} = \frac{\overline{z}}{|z|^2}$

Conjugation of complex numbers

Let $z = a + bi$.

i) $\overline{z} = a - bi$ is called the conjugate of z.

ii) In polar form, $z = r(\cos\varphi + i\sin\varphi) \Rightarrow \overline{z} = r(\cos\varphi - i\sin\varphi)$.

Properties

1) $\overline{\overline{z}} = z$
2) $z + \overline{z} = 2a = 2\,\mathrm{Re}\,z$
3) $z\overline{z} = a^2 + b^2 = |z|^2$
4) $\frac{1}{z} = \frac{\overline{z}}{|z|^2}$
5) $|\overline{z}| = |z|$

Conjugation of complex numbers

Let $z = a + bi$.

i) $\overline{z} = a - bi$ is called the conjugate of z.

ii) In polar form, $z = r(\cos\varphi + i\sin\varphi) \Rightarrow \overline{z} = r(\cos\varphi - i\sin\varphi)$.

Properties

1) $\overline{\overline{z}} = z$
2) $z + \overline{z} = 2a = 2\,\mathrm{Re}\,z$
3) $z\overline{z} = a^2 + b^2 = |z|^2$
4) $\frac{1}{z} = \frac{\overline{z}}{|z|^2}$
5) $|\overline{z}| = |z|$
6) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$

Conjugation of complex numbers

Let $z = a + bi$.

i) $\overline{z} = a - bi$ is called the conjugate of z.

ii) In polar form, $z = r(\cos\varphi + i\sin\varphi) \Rightarrow \overline{z} = r(\cos\varphi - i\sin\varphi)$.

Properties

1) $\overline{\overline{z}} = z$
2) $z + \overline{z} = 2a = 2\operatorname{Re} z$
3) $z\overline{z} = a^2 + b^2 = |z|^2$
4) $\frac{1}{z} = \frac{\overline{z}}{|z|^2}$
5) $|\overline{z}| = |z|$
6) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
7) $\overline{z_1 z_2} = \overline{z_1}\ \overline{z_2}$

Conjugation of complex numbers

Let $z = a + bi$.

i) $\overline{z} = a - bi$ is called the conjugate of z.

ii) In polar form, $z = r(\cos\varphi + i\sin\varphi) \Rightarrow \overline{z} = r(\cos\varphi - i\sin\varphi)$.

Properties

1) $\overline{\overline{z}} = z$
2) $z + \overline{z} = 2a = 2\,\mathrm{Re}\, z$
3) $z\overline{z} = a^2 + b^2 = |z|^2$
4) $\frac{1}{z} = \frac{\overline{z}}{|z|^2}$
5) $|\overline{z}| = |z|$
6) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
7) $\overline{z_1 z_2} = \overline{z_1}\;\overline{z_2}$
8) $\overline{\left(\frac{z_1}{z_2}\right)} = \frac{\overline{z_1}}{\overline{z_2}}$

The field of complex numbers

Example

Solve the following equation

a) $\overline{z^7} = \frac{1}{z^3}$,

b) $z^4 = z + \overline{z}$.

Example

Let x, y, z be complex numbers that satisfy $|x| = |y| = |z| = 1$. Compare the modulus of $x + y + z$ and $xy + yz + zx$.