Curriculum

Contents

How

Tools

- Zoom for lectures and exams
- moodle for announcements and submissions
- cocalc.com (or sage locally)

How

Tools

- Zoom for lectures and exams
- moodle for announcements and submissions
- cocalc.com (or sage locally)

What you want to know

- 1 midterm + 6 homeworks + 1 final
- Work on a semester project for +15%
- All exams are oral exams.
- Participation is +15%

Logic

Propositional Logic

Why logic?

- Logic rules give precise meaning to mathematical statements.
- Used to distinguish valid and invalid mathematical arguments.
- Many applications to computer science and engineering
- Automated theorem proving
- computer circuits, computer programming, formal verification of the correctness of programs, etc.

Proposition

Definition

A proposition is a

- declarative sentence (a sentence that declares a fact)
- that is either true or false, but not both.

Proposition

Definition

A proposition is a

- declarative sentence (a sentence that declares a fact)
- that is either true or false, but not both.

Examples

- Ankara is the capital of Turkey
- Istanbul is the capital of Turkey
- $1 + 1 = 3$
- $5 + 1 = 6$

Proposition

Definition

A proposition is a

- declarative sentence (a sentence that declares a fact)
- that is either true or false, but not both.

Examples

- Ankara is the capital of Turkey
- Istanbul is the capital of Turkey
- $1 + 1 = 3$
- $5 + 1 = 6$

Non-examples

- What time is it?
- $x + 1 = 3$
- Run slowly
- $x^2 + y^2 = z^2$

Propositional Calculus

Notation

Letters (usually p,q,r,...) to denote **propositional variables**.

Propositional Calculus

Notation
Letters (usually p,q,r,. . .) to denote **propositional variables**.

Truth value
The **truth value** of a proposition is true (T) or false (F).

Logical operators

Negation

Let p be a proposition. The negation of p, denoted by $\bar{p}$ is the proposition: "It is not the case that p"
The truth value of $\bar{p}$ is the opposite of the truth value of p.

Logical operators

Negation

Let p be a proposition. The negation of p, denoted by $\bar{p}$ is the proposition: "It is not the case that p"
The truth value of $\bar{p}$ is the opposite of the truth value of p.

Examples

What is the negation of:

- my computer runs Linux
- Teams is better than Zoom
- I am at least 190cm tall

Logical operators

Negation

Let p be a proposition. The negation of p, denoted by $\bar{p}$ is the proposition: "It is not the case that p"
The truth value of $\bar{p}$ is the opposite of the truth value of p.

Examples

What is the negation of:

- my computer runs Linux
- Teams is better than Zoom
- I am at least 190cm tall

Truth table

p	$\bar{p}$
T	F
F	T

Logical operators

Conjuction

Let p and q be propositions. The conjunction of p and q, denoted by $p \wedge q$, is the proposition: "p and q"
The truth value of $p \wedge q$ is true when both p and q are true and false otherwise.

Logical operators

Conjuction

Let p and q be propositions. The conjunction of p and q, denoted by $p \land q$, is the proposition: "p and q"
The truth value of $p \land q$ is true when both p and q are true and false otherwise.

Examples

- p Mehmet's computer runs Linux
- q Mehmet's computer has 8Gb of memory

What is the conjunction of p and q?

Logical operators

Conjuction

Let p and q be propositions. The conjunction of p and q, denoted by $p \wedge q$, is the proposition: "p and q"
The truth value of $p \wedge q$ is true when both p and q are true and false otherwise.

Examples

- p Mehmet's computer runs Linux
- q Mehmet's computer has 8Gb of memory

What is the conjunction of p and q?

Truth table

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Logical operators

Disjunction

Let p and q be propositions. The disjunction of p and q, denoted by $p \vee q$, is the proposition: "p or q"
The truth value of $p \vee q$ is false when both p and q are false and true otherwise.

Logical operators

Disjunction

Let p and q be propositions. The disjunction of p and q, denoted by $p \vee q$, is the proposition: "p or q"
The truth value of $p \vee q$ is false when both p and q are false and true otherwise.

Examples

- p Mehmet's computer runs Linux
- q Mehmet's computer has 8Gb of memory

What is the disjunction of p and q?

Logical operators

Disjunction

Let p and q be propositions. The disjunction of p and q, denoted by $p \vee q$, is the proposition: "p or q"
The truth value of $p \vee q$ is false when both p and q are false and true otherwise.

Examples

- p Mehmet's computer runs Linux
- q Mehmet's computer has 8Gb of memory

What is the disjunction of p and q?

Truth table

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Logical operators

Exclusive OR

Let p and q be propositions. The exclusive or of p and q, denoted by $p \oplus q$, is the proposition: "p or q but not both"

The truth value of $p \oplus q$ is true when exactly one of p and q is true and false otherwise.

Logical operators

Exclusive OR

Let p and q be propositions. The exclusive or of p and q, denoted by $p \oplus q$, is the proposition: "p or q but not both"
The truth value of $p \oplus q$ is true when exactly one of p and q is true and false otherwise.

Examples

- p Mehmet's computer runs Linux
- q Mehmet's computer runs MacOS

What is the exclusive or of p and q?

Logical operators

Exclusive OR

Let p and q be propositions. The exclusive or of p and q, denoted by $p \oplus q$, is the proposition: "p or q but not both"

The truth value of $p \oplus q$ is true when exactly one of p and q is true and false otherwise.

Examples

- p Mehmet's computer runs Linux
- q Mehmet's computer runs MacOS

What is the exclusive or of p and q?

Truth table

p	q	$p \oplus q$
T	T	T
T	F	T
F	T	T
F	F	F

Logical operators

Conditional statement

Let p and q be propositions. The conditional statement $p \rightarrow q$ is the proposition "q if and only if p".

In the conditional statement $p \rightarrow q$, proposition p is called the hypothesis and q is called the conclusion. The truth value of $p \rightarrow q$ is false when p is true and q is false, and true otherwise.

Logical operators

Conditional statement

Let p and q be propositions. The conditional statement $p \rightarrow q$ is the proposition "q if and only if p".

In the conditional statement $p \rightarrow q$, proposition p is called the hypothesis and q is called the conclusion. The truth value of $p \rightarrow q$ is false when p is true and q is false, and true otherwise.

Examples

- p Mehmet's computer runs Linux
- q Mehmet's computer is fast

What is the proposition $p \rightarrow q$?

Logical operators

Conditional statement

Let p and q be propositions. The conditional statement $p \rightarrow q$ is the proposition "q if and only if p".

In the conditional statement $p \rightarrow q$, proposition p is called the hypothesis and q is called the conclusion. The truth value of $p \rightarrow q$ is false when p is true and q is false, and true otherwise.

Examples

- p Mehmet's computer runs Linux
- q Mehmet's computer is fast

What is the proposition $p \rightarrow q$?

Truth table

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Logical operators

Bidirectional statement

Let p and q be propositions. The bidirectional statement $p \leftrightarrow q$ is the proposition "if p, then q".

The truth value of $p \leftrightarrow q$ is true when $p \rightarrow q$ and $q \rightarrow p$, and false otherwise.

Logical operators

Bidirectional statement

Let p and q be propositions. The bidirectional statement $p \leftrightarrow q$ is the proposition "if p, then q".
The truth value of $p \leftrightarrow q$ is true when $p \rightarrow q$ and $q \rightarrow p$, and false otherwise.

Examples

- p Mehmet's computer runs Linux
- q Mehmet's computer is fast

What is the proposition $p \leftrightarrow q$?

Logical operators

Bidirectional statement

Let p and q be propositions. The bidirectional statement $p \leftrightarrow q$ is the proposition "if p, then q".

The truth value of $p \leftrightarrow q$ is true when $p \to q$ and $q \to p$, and false otherwise.

Examples

- p Mehmet's computer runs Linux
- q Mehmet's computer is fast

What is the proposition $p \leftrightarrow q$?

Truth table

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Other propositions

Let p and q be propositions.

Converse

The converse of $p \rightarrow q$ is $q \rightarrow p$.

Inverse

The inverse of $p \rightarrow q$ is $\bar{p} \rightarrow \bar{q}$.

Contrapositive

The contrapositive of $p \rightarrow q$ is $\bar{q} \rightarrow \bar{p}$.

Equivalent

Let p and q be propositions. If p and q have always the same truth value, then they are called equivalent.

Example

A conditional statement and its contrapositive are equivalent.

Precedence of logical operators

Operator	Precedence
$\overline{}$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

Truth Tables

$p \vee \bar{q} \to (p \wedge q)$

p	q	$\bar{q}$	$p \vee \bar{q}$	$p \wedge q$	$p \vee \bar{q} \to (p \wedge q)$
T	T	F	T	T	T
T	F	T	T	F	F
F	T	F	F	F	T
F	F	T	T	F	F

Propositional Equivalence

Definition
A proposition that is always true is called a **tautology**.

Definition
A proposition that is always false is called a **contradiction**.

Tautology or Contradiction?

- $p \wedge \bar{p}$
- $p \vee \bar{p}$
- $p \vee (p \rightarrow q)$
- $\bar{q} \wedge (p \rightarrow q)$

Logical Equivalence

Definition

The propositions p and q are called **logically equivalent** if $p \leftrightarrow q$ is a tautology.

Notation

We denote logical equivalence by $\equiv$ or $\Leftrightarrow$, i.e., $p \equiv q$ or $p \Leftrightarrow q$. Note that this is not a compound proposition, these symbols are not logical connectives.

De Morgan's Laws

- $\overline{p \wedge p} \equiv \bar{p} \vee \bar{q}$
- $\overline{p \vee p} \equiv \bar{p} \wedge \bar{q}$

Proof of Logical Equivalences

De Morgan's Laws

- $\overline{p \wedge p} \equiv \bar{p} \vee \bar{q}$
- $\overline{p \vee p} \equiv \bar{p} \wedge \bar{q}$

p	q	$p \vee q$	$\overline{p \vee q}$	$\bar{p}$	$\bar{q}$	$\bar{p} \wedge \bar{q}$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

Proof of Logical Equivalences

Prove that $p \rightarrow q$ and $\bar{p} \vee q$ are logically equivalent.

Proof of Logical Equivalences

Prove that $p \rightarrow q$ and $\bar{p} \vee q$ are logically equivalent.

p	q	$\bar{p}$	$\bar{p} \vee q$	$p \rightarrow q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Equivalences

TABLE 6 **Logical Equivalences.**

Equivalence	*Name*
$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	Identity laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws

TABLE 7 **Logical Equivalences Involving Conditional Statements.**

$p \to q \equiv \neg p \vee q$

$p \to q \equiv \neg q \to \neg p$

$p \vee q \equiv \neg p \to q$

$p \wedge q \equiv \neg(p \to \neg q)$

$\neg(p \to q) \equiv p \wedge \neg q$

$(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$

$(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$

$(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$

$(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$

TABLE 8 **Logical Equivalences Involving Biconditional Statements.**

$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$

$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$

$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

Example

Prove that $\overline{p \vee (\bar{p} \wedge q)}$ and $\bar{p} \wedge \bar{q}$ are logically equivalent.

Example

Prove that $\overline{p \vee (\bar{p} \wedge q)}$ and $\bar{p} \wedge \bar{q}$ are logically equivalent.

$$
\begin{aligned}
\overline{p \vee (\bar{p} \wedge q)} &\equiv \bar{p} \wedge \overline{\bar{p} \wedge q} && (1)\\
&\equiv \bar{p} \wedge (\bar{\bar{p}} \vee \bar{q}) && (2)\\
&\equiv \bar{p} \wedge (p \vee \bar{q}) && (3)\\
&\equiv (\bar{p} \wedge p) \vee (\bar{p} \wedge \bar{q}) && (4)\\
&\equiv F \vee (\bar{p} \wedge \bar{q}) && (5)\\
&\equiv (\bar{p} \wedge \bar{q}) \vee F && (6)\\
&\equiv \bar{p} \wedge \bar{q} && (7)
\end{aligned}
$$

Predicates

Is "$x > 3$" a proposition?

Predicates

Is "$x > 3$" a proposition?
The statement has two parts, a variable (x) and a predicate (> 3).

Predicate

Let P denote a statement depending on some variable x. We denote it by $P(x)$ and it has a defined truth value when the variable is assigned a value.

Predicates

Is "$x > 3$" a proposition?
The statement has two parts, a variable (x) and a predicate (> 3).

Predicate

Let P denote a statement depending on some variable x. We denote it by $P(x)$ and it has a defined truth value when the variable is assigned a value.

Examples

- $x > 3$
- Computer x is functioning properly
- City x is the capital of Turkey
- P(x,y) : x+y=3

Predicates

Is "$x > 3$" a proposition?
The statement has two parts, a variable (x) and a predicate (> 3).

Predicate

Let P denote a statement depending on some variable x. We denote it by $P(x)$ and it has a defined truth value when the variable is assigned a value.

Examples

- $x > 3$
- Computer x is functioning properly
- City x is the capital of Turkey
- P(x,y) : x+y=3

We can have unary, binary or in general n-ary predicates.

Predicates

Is "$x > 3$" a proposition?
The statement has two parts, a variable (x) and a predicate (> 3).

Predicate

Let P denote a statement depending on some variable x. We denote it by $P(x)$ and it has a defined truth value when the variable is assigned a value.

Examples

- $x > 3$
- Computer x is functioning properly
- City x is the capital of Turkey
- P(x,y) : x+y=3

We can have unary, binary or in general n-ary predicates.

You used that already

if $x > 0$ then $x := x + 1$

Quantifiers: Universal

Definition

The universal quantification of $P(x)$ is the statement

$$P(x) \text{ for all values of } x \text{ in the domain.}$$

Notation

The notation $\forall x P(x)$ denotes the universal quantification of $P(x)$.
Here $\forall$ is called the universal quantifier.

Note

An element for which $P(x)$ is false is a counterexample of $\forall x P(x)$.

Quantifiers: Existential

Definition

The existential quantification of $P(x)$ is the statement

There exists x in the domain such that $P(x)$.

Notation

The notation $\exists x P(x)$ denotes the existential quantification of $P(x)$. Here $\exists$ is called the existential quantifier.

Note

An element for which $P(x)$ is false is a counterexample of $\forall x P(x)$.

Quantifiers

TABLE 1 Quantifiers.		
Statement	***When True?***	***When False?***
$\forall x P(x)$	$P(x)$ is true for every x.	There is an x for which $P(x)$ is false.
$\exists x P(x)$	There is an x for which $P(x)$ is true.	$P(x)$ is false for every x.

Induction

We want to prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a a predicate.

Induction

We want to prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a a predicate.

- Verify that $P(1)$ is true
- Show that the conditional statement $P(k) \to P(k+1)$ is true for all positive integers k.

Induction

The Gauss

Prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$

Induction

The Gauss

Prove that $1+2+\cdots+n=\frac{n(n+1)}{2}$

Proof:

Induction

The Gauss

Prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$

Proof:

basis $P(1)$ is true because $1 = \frac{1(1+1)}{2}$

step Assume $P(k)$ is true for arbitrary k, which means that $1 + 2 + \cdots + k = \frac{k(k+1)}{2}$.
Now we have to show that under this assumption $P(k+1)$ is true, namely $1 + 2 + \cdots + k + (k+1) = \frac{(k+1)(k+2)}{2}$.
Let's add $(k+1)$ in both sides of the assumption:

$$1 + 2 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1) \tag{8}$$

$$= \frac{k(k+1) + 2(k+1)}{2} \tag{9}$$

$$= \frac{(k+2)(k+1)}{2} \tag{10}$$

Sets

Sets

What is a set?

Sets

What is a set?

A set is an **unordered collection of objects**.

Notation

The objects in a set are called **elements** or **members** of the set.
If a is an element of A, we write $a \in A$.
If a is not an element of A, we write $a \notin A$.

Set description

Roster method

We write the elements in curly brackets.

Set description

Roster method

We write the elements in curly brackets.

Examples

- $O = \{1, 3, 5\}$
- $T = \{$Istanbul, Izmir, Ankara$\}$
- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$
- $A = \{0, 1, 2, 3\}$
- $B = \{0, 3, 2, 1\}$
- $C = \{0, 1, 2, 3, 2\}$

Be careful how you use ellipses...

Set description

Set builder

We characterize the elements in the set.

Set description

Set builder

We characterize the elements in the set.

Examples

- $O = \{x \in \mathbb{N} : x \text{ is odd and } x < 6\}$
- $\mathbb{Q}^+ = \{x \in \mathbb{R} : x = \frac{a}{b} \text{ for some } a, b \in \mathbb{N}\}$
- $T = \{\text{cities of Turkey}\}$

The : could also be $|$.

Set description

Intervals

A set containing all (real) numbers between two bounds.

Set description

Intervals

A set containing all (real) numbers between two bounds.

Examples

- $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$
- $(a, b] = \{x \in \mathbb{R} : a < x \leq b\}$
- $[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$
- $(a, b) = \{x \in \mathbb{R} : a < x < b\}$

Closed and open intervals

What can a set contain?

Sets of sets

A set can contain other sets as elements.

What can a set contain?

Sets of sets

A set can contain other sets as elements.

Examples

- $A = \{\mathbb{N}, \mathbb{R}, \mathbb{Q}\}$
- $B = \{\{\mathbb{N}, \mathbb{R}, \mathbb{Q}\}, \mathbb{N}\}$

Sets

Equality

Two sets A and B are equal if and only if they contain the same elements. In that case we write $A = B$.

$$A = B \leftrightarrow (\forall x(x \in A \leftrightarrow x \in B))$$

Examples

- $A = \{0, 1, 2, 3\}$
- $B = \{0, 3, 2, 1\}$
- $C = \{0, 1, 2, 3, 2\}$

Sets

Equality

Two sets A and B are equal if and only if they contain the same elements. In that case we write $A = B$.

$$A = B \leftrightarrow (\forall x(x \in A \leftrightarrow x \in B))$$

Examples

- $A = \{0, 1, 2, 3\}$
- $B = \{0, 3, 2, 1\}$
- $C = \{0, 1, 2, 3, 2\}$

Empty set

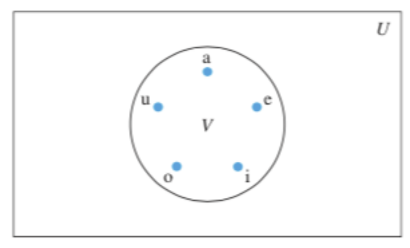
The empty set (or null set) is a set containing no elements and we denote it by $\emptyset$.

Singleton set

A set containing a single element is called a singleton set.

Venn diagrams

The vowels in English



Subset

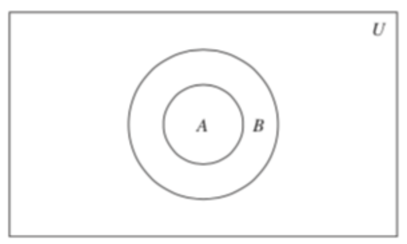
Definition

Set A is a subset of set B if and only if every element of A is also an element of B.

$$\forall x(x \in A \to B)$$

If A is a subset of B we write $A \subseteq B$.

Venn diagram



Subset

Proofs

- To prove $A \subseteq B$, we show that if $x \in A$ then $x \in B$.
- To prove $A \not\subseteq B$, we find an $x \in A$ such that $x \notin B$.

Theorem

For every set A

- $\emptyset \subseteq A$
- $A \subseteq A$

Proper subset

$$\forall x\,(x \in A \to x \in B) \land \exists x\,(x \in B \land x \notin A)$$

Showing equality

- $A \subseteq B$
- $B \subseteq A$

Size of a set

Cardinality

Let A be a set. If there are exactly n distinct elements in A, where n is a non-negative integer, we say that A is a finite set and its cardinality is n.
We denote it by $|A| = n$.

Infinite set

A set is infinite if it is not finite.

More sets

Powerset

Given a set A, the powerset of A is the set of all subsets of A.
We denote it by $\mathcal{P}(A)$.

More sets

Powerset

Given a set A, the powerset of A is the set of all subsets of A. We denote it by $\mathcal{P}(A)$.

What is the cardinality of $\mathcal{P}(A)$ if the cardinality of A is n?

More sets

Powerset

Given a set A, the powerset of A is the set of all subsets of A. We denote it by $\mathcal{P}(A)$.

What is the cardinality of $\mathcal{P}(A)$ if the cardinality of A is n?

Cartesian Product

Let A and B be sets. The Cartesian product of A and B, denoted by $A \times B$ is the set of all pairs (a, b) where $a \in A$ and $b \in B$.

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}$$

More sets

Powerset

Given a set A, the powerset of A is the set of all subsets of A. We denote it by $\mathcal{P}(A)$.

What is the cardinality of $\mathcal{P}(A)$ if the cardinality of A is n?

Cartesian Product

Let A and B be sets. The Cartesian product of A and B, denoted by $A \times B$ is the set of all pairs (a, b) where $a \in A$ and $b \in B$.

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}$$

What is the cardinality of $A \times B$ if the cardinality of A is n and the cardinality of B is m?

More sets

Powerset

Given a set A, the powerset of A is the set of all subsets of A. We denote it by $\mathcal{P}(A)$.

What is the cardinality of $\mathcal{P}(A)$ if the cardinality of A is n?

Cartesian Product

Let A and B be sets. The Cartesian product of A and B, denoted by $A \times B$ is the set of all pairs (a, b) where $a \in A$ and $b \in B$.

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}$$

What is the cardinality of $A \times B$ if the cardinality of A is n and the cardinality of B is m?

Cartesian Product of many sets

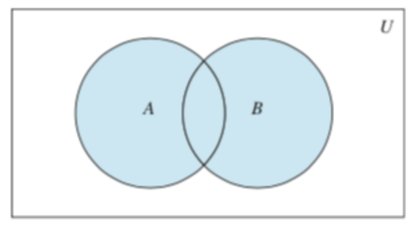
$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_i \in A_i \text{ for } i = 1, 2, 3 \ldots, n\}$$

Set operations

Union

Let A and B be sets. The **union** of A and B, denoted by $A \cup B$, is the set containing those elements that belong in A or in B.

$$A \cup B = \{x : x \in A \vee x \in B\}$$



Examples

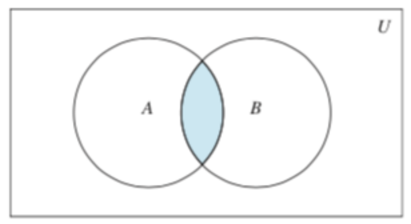
Let $A = \{1, 3, 5\}$ and $B\{1, 2, 4\}$, then $A \cup B = \{1, 2, 3, 4, 5\}$.

Set operations

Intersection

Let A and B be sets. The **intersection** of A and B, denoted by $A \cap B$, is the set containing those elements that belong both in A and in B.

$$A \cap B = \{x : x \in A \wedge x \in B\}$$



Examples

Let $A = \{1, 3, 5\}$ and $B\{1, 2, 4\}$, then $A \cap B = \{1\}$.

Inclusion-Exclusion

Question

Let A and B be finite sets. What is the cardinality of $A \cup B$?

Inclusion-Exclusion

Question

Let A and B be finite sets. What is the cardinality of $A \cup B$?

$$|A \cup B| = |A| + |B| - |A \cap B|$$

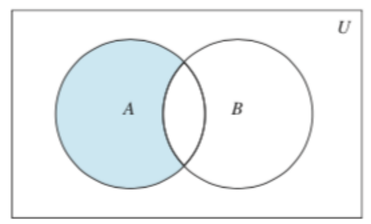
This follows a general principle that appears in many places and is called **inclusion-exclusion**.

Set operations

Difference

Let A and B be sets. The **difference** of A and B, denoted by $A - B$, is the set containing those elements that belong in A but not in B.

$$A - B = \{x : x \in A \land x \notin B\}$$



Examples

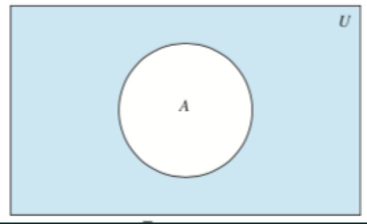
Let $A = \{1, 3, 5\}$ and $B\{1, 2, 4\}$, then $A - B = \{3, 5\}$.

Set operations

Complement

Let A and B be sets. The **complement** of A with respect to B is the difference of A and B.
When we say the "complement of A", we mean the complement with respect to the universal set U. We denote it by $\bar{A}$.

$$\bar{A} = \{x \in U : x \notin A\}$$



Identinties

TABLE 1 Set Identities.

Identity	*Name*
$A \cap U = A$ $A \cup \emptyset = A$	Identity laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws

Example

Use set builder notation and logical equivalences to establish the first De Morgan law $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Solution: We can prove this identity with the following steps.

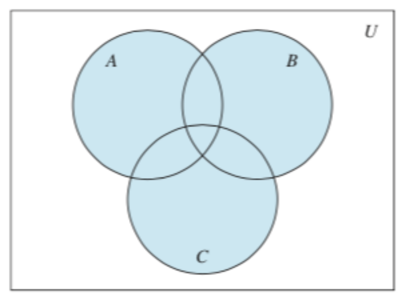
$$
\begin{aligned}
\overline{A \cap B} &= \{x \mid x \notin A \cap B\} && \text{by definition of complement} \\
&= \{x \mid \neg(x \in (A \cap B))\} && \text{by definition of does not belong symbol} \\
&= \{x \mid \neg(x \in A \wedge x \in B)\} && \text{by definition of intersection} \\
&= \{x \mid \neg(x \in A) \vee \neg(x \in B)\} && \text{by the first De Morgan law for logical equivalences} \\
&= \{x \mid x \notin A \vee x \notin B\} && \text{by definition of does not belong symbol}
\end{aligned}
$$

Set operations

Generalized Union

The **union** of a collection of sets is the set containing those elements that belong to at least one of the sets in the collection.

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$$

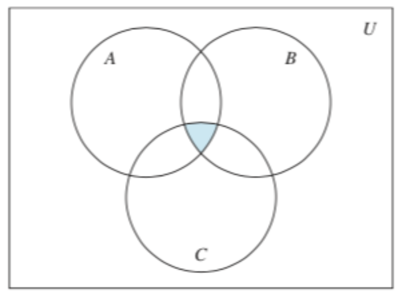


Set operations

Generalized Intersection

The **intersection** of a collection of sets is the set containing those elements that belong to all of the sets in the collection.

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$$



Relations

Relations

Definition

Let A and B be sets.
A binary relation from A to B is a subset of $A \times B$.

Relations

Definition
Let A and B be sets.
A binary relation from A to B is a subset of $A \times B$.

Intuition
A binary relation from A to B is a set R of ordered pairs,

Relations

Definition

Let A and B be sets.
A binary relation from A to B is a subset of $A \times B$.

Intuition

A binary relation from A to B is a set R of ordered pairs, where the first element of each ordered pair comes from A and the second element comes from B.

Relations

Definition

Let A and B be sets.
A binary relation from A to B is a subset of $A \times B$.

Intuition

A binary relation from A to B is a set R of ordered pairs, where the first element of each ordered pair comes from A and the second element comes from B.

Notation

We use the notation aRb to denote that $(a, b) \in R$.
If (a, b) belongs to R, then a is related to b by R.

Relations

Definition

Let A be the set of students in GTU bilmuh,
and let B be the set of courses.

Relations

Definition

Let A be the set of students in GTU bilmuh,
and let B be the set of courses.
Let R be the relation expressing if a is a student enrolled in course b.

Relations

Definition

Let A be the set of students in GTU bilmuh,
and let B be the set of courses.
Let R be the relation expressing if a is a student enrolled in course b.
For example, if Ali and Hatice are enrolled in BIL211, the pairs (Ali, BIL211) and (Hatice, BIL211) belong to R.

Relations

Definition

Let A be the set of students in GTU bilmuh,
and let B be the set of courses.
Let R be the relation expressing if a is a student enrolled in course b.
For example, if Ali and Hatice are enrolled in BIL211, the pairs (Ali, BIL211) and (Hatice, BIL211) belong to R.
If Hatice is also enrolled in BIL426, then the pair (Hatice, BIL426) is also in R.

Relations on a set

Definition

Let A be a set. A relation on a set A is a relation from A to A.

Relations on a set

Definition

Let A be a set. A relation on a set A is a relation from A to A.

Intuition

A subset of $A \times A$.

Relations on a set

Definition

Let A be a set. A relation on a set A is a relation from A to A.

Intuition

A subset of $A \times A$.

Example

Let A be the set $\{1, 2, 3, 4\}$. Which ordered pairs are in the relation $R = \{(a, b) : \ a \text{ divides } b\}$?

Relations on a set

Definition

Let A be a set. A relation on a set A is a relation from A to A.

Intuition

A subset of $A \times A$.

Example

Let A be the set $\{1, 2, 3, 4\}$. Which ordered pairs are in the relation $R = \{(a, b) : \text{ a divides } b\}$?
$R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)\}$.

Relations on a set

Definition
Let A be a set. A relation on a set A is a relation from A to A.

Intuition
A subset of $A \times A$.

Example
Let A be the set $\{1, 2, 3, 4\}$. Which ordered pairs are in the relation $R = \{(a, b) : \text{ } a \textit{ divides } b\}$?
$R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)\}$.

Question
How many relations are there on a set with n elements?

Properties of Relations

Reflexive

A relation R on a set A is called reflexive if $(a, a) \in R$ for every element $a \in A$.

Properties of Relations

Reflexive

A relation R on a set A is called reflexive if $(a, a) \in R$ for every element $a \in A$.

$\forall a \in A\,((a, a) \in R)$

Properties of Relations

Reflexive

A relation R on a set A is called reflexive if $(a, a) \in R$ for every element $a \in A$.
$\forall a \in A\,((a, a) \in R)$

Example

Which of the following relations on $\{1, 2, 3, 4\}$ are reflexive:

- $R_1 = \{(1, 1), (1, 2), (2, 1)\}$
- $R_2 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}$
- $R_3 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}$
- $R_4 = \{(3, 4)\}$
- $R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$
- $R_6 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\}$

Properties of Relations

Reflexive

A relation R on a set A is called reflexive if $(a, a) \in R$ for every element $a \in A$.
$\forall a \in A\,((a, a) \in R)$

Example

Which of the following relations on $\{1, 2, 3, 4\}$ are reflexive:

- $R_1 = \{(1, 1), (1, 2), (2, 1)\}$
- $R_2 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}$
- $R_3 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}$
- $R_4 = \{(3, 4)\}$
- $R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$
- $R_6 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\}$

Question

Is the "divides" relation reflexive?

Properties of Relations

Symmetric

A relation R on a set A is called symmetric if $(b, a) \in R$ whenever $(a, b) \in R$,for all $a, b \in A$.

Properties of Relations

Symmetric

A relation R on a set A is called symmetric if $(b, a) \in R$ whenever $(a, b) \in R$,for all $a, b \in A$.
$\forall a \forall b \, ((a, b) \in R \rightarrow (b, a) \in R)$

Properties of Relations

Symmetric

A relation R on a set A is called symmetric if $(b, a) \in R$ whenever $(a, b) \in R$,for all $a, b \in A$.
$\forall a \forall b ((a, b) \in R \rightarrow (b, a) \in R)$

Example

Which of the following relations on $\{1, 2, 3, 4\}$ are symmetric:

- $R_1 = \{(1, 1), (1, 2), (2, 1)\}$
- $R_2 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}$
- $R_3 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}$
- $R_4 = \{(3, 4)\}$
- $R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$
- $R_6 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\}$

Properties of Relations

Symmetric

A relation R on a set A is called symmetric if $(b, a) \in R$ whenever $(a, b) \in R$,for all $a, b \in A$.
$\forall a \forall b\,((a, b) \in R \to (b, a) \in R)$

Example

Which of the following relations on $\{1, 2, 3, 4\}$ are symmetric:

- $R_1 = \{(1,1),(1,2),(2,1)\}$
- $R_2 = \{(1,1),(1,2),(2,1),(2,2),(3,4),(4,1),(4,4)\}$
- $R_3 = \{(2,1),(3,1),(3,2),(4,1),(4,2),(4,3)\}$
- $R_4 = \{(3,4)\}$
- $R_5 = \{(1,1),(1,2),(1,3),(1,4),(2,2),(2,3),(2,4),(3,3),(3,4),(4,4)\}$
- $R_6 = \{(1,1),(1,2),(1,4),(2,1),(2,2),(3,3),(4,1),(4,4)\}$

Question

Is the "divides" relation symmetric?

Properties of Relations

Antisymmetric

A relation R on a set A is called antisymmetric if for all $a, b \in A$, $(a, b) \in R$ and $(b, a) \in R$ implies that $a = b$.

Properties of Relations

Antisymmetric

A relation R on a set A is called antisymmetric if for all $a, b \in A$, $(a, b) \in R$ and $(b, a) \in R$ implies that $a = b$.
$\forall a \forall b \, (((a, b) \in R) \land ((b, a) \in R) \rightarrow (a = b))$

Properties of Relations

Antisymmetric

A relation R on a set A is called antisymmetric if for all $a, b \in A$, $(a, b) \in R$ and $(b, a) \in R$ implies that $a = b$.
$\forall a \forall b (((a, b) \in R) \land ((b, a) \in R) \to (a = b))$

Example

Which of the following relations on $\{1, 2, 3, 4\}$ are antisymmetric:

- $R_1 = \{(1, 1), (1, 2), (2, 1)\}$
- $R_2 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}$
- $R_3 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}$
- $R_4 = \{(3, 4)\}$
- $R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$
- $R_6 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\}$

Properties of Relations

Antisymmetric

A relation R on a set A is called antisymmetric if for all $a, b \in A$, $(a, b) \in R$ and $(b, a) \in R$ implies that $a = b$.
$\forall a \forall b \, (((a, b) \in R) \wedge ((b, a) \in R) \rightarrow (a = b))$

Example

Which of the following relations on $\{1, 2, 3, 4\}$ are antisymmetric:

- $R_1 = \{(1, 1), (1, 2), (2, 1)\}$
- $R_2 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}$
- $R_3 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}$
- $R_4 = \{(3, 4)\}$
- $R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$
- $R_6 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\}$

Question

Is the "divides" relation antisymmetric?

Properties of Relations

Transitive

A relation R on a set A is called transitive if for all $a, b, c \in A$, $(a, b) \in R$ and $(b, c) \in R$ implies that $(a, c) \in R$.

Properties of Relations

Transitive

A relation R on a set A is called transitive if for all $a, b, c \in A$, $(a, b) \in R$ and $(b, c) \in R$ implies that $(a, c) \in R$.

$\forall a \forall b \forall c \left(((a, b) \in R) \wedge ((b, c) \in R) \rightarrow ((a, c) \in R)\right)$

Properties of Relations

Transitive

A relation R on a set A is called transitive if for all $a, b, c \in A$, $(a, b) \in R$ and $(b, c) \in R$ implies that $(a, c) \in R$.
$\forall a \forall b \forall c\, (((a, b) \in R) \wedge ((b, c) \in R) \to ((a, c) \in R))$

Example

Which of the following relations on $\{1, 2, 3, 4\}$ are transitive:

- $R_1 = \{(1,1), (1,2), (2,1)\}$
- $R_2 = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$
- $R_3 = \{(2,1), (3,1), (3,2), (4,1), (4,2), (4,3)\}$
- $R_4 = \{(3,4)\}$
- $R_5 = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}$
- $R_6 = \{(1,1), (1,2), (1,4), (2,1), (2,2), (3,3), (4,1), (4,4)\}$

Properties of Relations

Transitive

A relation R on a set A is called transitive if for all $a, b, c \in A$, $(a, b) \in R$ and $(b, c) \in R$ implies that $(a, c) \in R$.
$\forall a \forall b \forall c \, (((a, b) \in R) \wedge ((b, c) \in R) \rightarrow ((a, c) \in R))$

Example

Which of the following relations on $\{1, 2, 3, 4\}$ are transitive:

- $R_1 = \{(1, 1), (1, 2), (2, 1)\}$
- $R_2 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}$
- $R_3 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}$
- $R_4 = \{(3, 4)\}$
- $R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$
- $R_6 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\}$

Question

Is the "divides" relation transitive?

Combining Relations

Observation

Relations are sets, so we can treat them as sets

Combining Relations

Observation

Relations are sets, so we can treat them as sets

Example

Consider the following relations on $\mathbb{Z}$:

- $R_1 = \{(a, b) : a \geq b\}$
- $R_2 = \{(a, b) : a \leq b\}$

Combining Relations

Observation

Relations are sets, so we can treat them as sets

Example

Consider the following relations on $\mathbb{Z}$:

- $R_1 = \{(a, b) : a \geq b\}$
- $R_2 = \{(a, b) : a \leq b\}$

What are the following relations?

- $R_1 \cap R_2$
- $R_1 \cup R_2$
- $R_1 - R_2$

n-ary Relations

Definition

Let $A_1, A_2, \ldots, A_n$ be sets. An n-ary relation on these sets is a subset of $A_1 \times A_2 \times \cdots \times A_n$.

The sets $A_1, A_2, \ldots, A_n$ are called the domains of the relation, and n is called its degree.

n-ary Relations

Definition

Let $A_1, A_2, \ldots, A_n$ be sets. An n-ary relation on these sets is a subset of $A_1 \times A_2 \times \cdots \times A_n$.
The sets $A_1, A_2, \ldots, A_n$ are called the domains of the relation, and n is called its degree.

Example

Let R be the degree 3 relation on $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ consisting of triples (a, b, c), where $a < b < c$.

n-ary Relations

Definition

Let $A_1, A_2, \ldots, A_n$ be sets. An n-ary relation on these sets is a subset of $A_1 \times A_2 \times \cdots \times A_n$.
The sets $A_1, A_2, \ldots, A_n$ are called the domains of the relation, and n is called its degree.

Example

Let R be the degree 3 relation on $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ consisting of triples (a, b, c), where $a < b < c$.
Then $(1, 2, 3) \in R$, but $(2, 4, 3) \notin R$.

n-ary Relations

Definition

Let $A_1, A_2, \ldots, A_n$ be sets. An n-ary relation on these sets is a subset of $A_1 \times A_2 \times \cdots \times A_n$.
The sets $A_1, A_2, \ldots, A_n$ are called the domains of the relation, and n is called its degree.

Example

Let R be the degree 3 relation on $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ consisting of triples (a, b, c), where $a < b < c$.
Then $(1, 2, 3) \in R$, but $(2, 4, 3) \notin R$.

Example

Let R be the relation on $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}^+$ consisting of triples (a, b, m), where $a \equiv b (mod\ m)$.

n-ary Relations

Definition

Let $A_1, A_2, \ldots, A_n$ be sets. An n-ary relation on these sets is a subset of $A_1 \times A_2 \times \cdots \times A_n$.
The sets $A_1, A_2, \ldots, A_n$ are called the domains of the relation, and n is called its degree.

Example

Let R be the degree 3 relation on $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ consisting of triples (a, b, c), where $a < b < c$.
Then $(1, 2, 3) \in R$, but $(2, 4, 3) \notin R$.

Example

Let R be the relation on $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}^+$ consisting of triples (a, b, m), where $a \equiv b(mod\ m)$.
$(8, 2, 3), (-1, 9, 5), (14, 0, 7) \in R$.
$(7, 2, 3), (-2, -8, 5), (11, 0, 6) \notin R$.

Types of Relations

Equivalence

A relation R on a set A is called an equivalence relation if it is

- reflexive
- symmetric
- transitive

Notation

Two elements a and b that are related by an equivalence relation are called equivalent, and we denote that by $a \equiv b$.

Types of Relations

Equivalence

A relation R on a set A is called an equivalence relation if it is

- reflexive
- symmetric
- transitive

Notation

Two elements a and b that are related by an equivalence relation are called equivalent, and we denote that by $a \equiv b$.

Example

Let R be the relation on the set of real numbers such that $(a, b) \in R$ if and only if $a - b$ is an integer.
This is an equivalence relation:

- $a - a$ is an integer
- if $a - b$ is integer then $b - a$ is integer
- if $a - b$ and $b - c$ are integer then $a - c$ is integer

Types of Relations

Equivalence

A relation R on a set A is called an equivalence relation if it is

- reflexive
- symmetric
- transitive

Notation

Two elements a and b that are related by an equivalence relation are called equivalent, and we denote that by $a \equiv b$.

Question

Let R be the relation on the set of integers such that $(a, b) \in R$ if and only if $a = b$ or $a = -b$.
Is this an equivalence relation?

Equivalence Classes

Definition

Let R be an equivalence relation on a set A. The set of all elements that are related to an element a of A is called the equivalence class of a.
The equivalence class of a with respect to R is denoted by $[a]_R$.

Equivalence Classes

Definition

Let R be an equivalence relation on a set A. The set of all elements that are related to an element a of A is called the equivalence class of a.

The equivalence class of a with respect to R is denoted by $[a]_R$.

Theorem

Let R be an equivalence relation on a set A.

The following are equivalent:

- $(a, b) \in R$
- $[a] = [b]$
- $[a] \cap [b] \neq \emptyset$

Equivalence Classes

Definition

Let R be an equivalence relation on a set A. The set of all elements that are related to an element a of A is called the equivalence class of a.
The equivalence class of a with respect to R is denoted by $[a]_R$.

Theorem

Let R be an equivalence relation on a set S. Then the equivalence classes of R form a partition of S.
Conversely, given a partition $\{A_i : i \in I\}$ of the set S, there is an equivalence relation R that has the sets A_i, for $i \in I$, as its equivalence classes.

POSET

Order Relations

Definition

Let A be a set.
A relation R on A is called a partial ordering or partial order if it is reflexive, antisymmetric, and transitive.
A set A together with a partial ordering R is called a partially ordered set, or poset, and is denoted by (A, R).
Members of A are called elements of the poset.

Order Relations

Definition

Let A be a set.
A relation R on A is called a partial ordering or partial order if it is reflexive, antisymmetric, and transitive.
A set A together with a partial ordering R is called a partially ordered set, or poset, and is denoted by (A, R).
Members of A are called elements of the poset.

Question

- Show that $\mathbb{Z}$ together with $\leq$ is a POSET
- Show that $\mathbb{Z}^+$ together with $|$ is a POSET
- Show that $\mathcal{P}(S)$ together with $\subseteq$ is a POSET

Order Relations

Definition

Two elements a and b of a POSET $(A, \oplus)$ are called comparable if either $a \oplus b$ or $b \oplus a$.

Otherwise they are called incomparable.

Order Relations

Definition

Two elements a and b of a POSET $(A, \oplus)$ are called comparable if either $a \oplus b$ or $b \oplus a$.

Otherwise they are called incomparable.

Question

- In the POSET $(\mathbb{Z}, \leq)$ are 3 and 9 comparable?
- In the POSET $(\mathbb{Z}, \leq)$ are 3 and 5 comparable?
- In the POSET $(\mathbb{Z}^+, |)$ are 3 and 9 comparable?
- In the POSET $(\mathbb{Z}^+, |)$ are 3 and 5 comparable?

Total Order

Definition

If $(A, \leq)$ is a POSET and every two elements of A are comparable, then A is called a totally ordered or linearly ordered set, and $\leq$ is called a total order or a linear order.

A totally ordered set is also called a chain.

Total Order

Definition

If $(A, \leq)$ is a POSET and every two elements of A are comparable, then A is called a totally ordered or linearly ordered set, and $\leq$ is called a total order or a linear order.

A totally ordered set is also called a chain.

Example

The POSET $(\mathbb{Z}, \leq)$

Non-example

The POSET $(\mathbb{Z}^+, |)$

Well-ordered sets

Definition

$(A, \leq)$ is a well-ordered set if it is a POSET such that $\leq$ is a total ordering and every nonempty subset of A has a least element.

Well-ordered sets

Definition

$(A, \leq)$ is a well-ordered set if it is a POSET such that $\leq$ is a total ordering and every nonempty subset of A has a least element.

Example

The POSET $(\mathbb{Z}\times, \leq_{lex})$

Non-example

The POSET $(\mathbb{Z}, \leq)$

Hasse diagram

Definition

The directed graph of the relation, after we remove the arrows for

- reflexivity (loops)
- transitivity

We draw it by arrows going upwards.

Hasse diagram

Definition

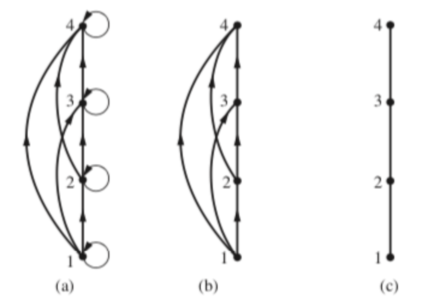
The directed graph of the relation, after we remove the arrows for

- reflexivity (loops)
- transitivity

We draw it by arrows going upwards.

Example

The POSET $(\{1,2,3,4\}, \leq)$



Hasse diagram

Definition

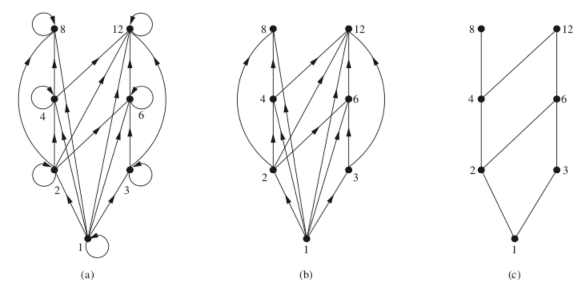
The directed graph of the relation, after we remove the arrows for

- reflexivity (loops)
- transitivity

We draw it by arrows going upwards.

Example

The POSET $(\{1, 2, 3, 4, 6, 8, 12\}, |)$



Maximal and Minimal elements

Definition

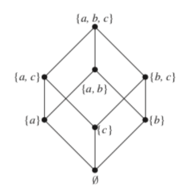
- **maximal** $a \in A$ is maximal if $\nexists b \in A : a \leq b$
- **minimal** $a \in A$ is minimal if $\nexists b \in A : b \leq a$
- **greatest** $a \in A$ the greatest element if $\forall b \in A : b \leq a$
- **least** $a \in A$ the least element if $\forall b \in A : a \leq b$

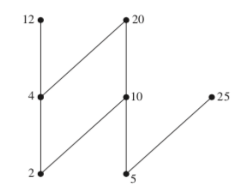
Maximal and Minimal elements

Definition

- **maximal** $a \in A$ is maximal if $\nexists b \in A : a \leq b$
- **minimal** $a \in A$ is minimal if $\nexists b \in A : b \leq a$
- **greatest** $a \in A$ the greatest element if $\forall b \in A : b \leq a$
- **least** $a \in A$ the least element if $\forall b \in A : a \leq b$

Examples





Upper and Lower Bounds

Let B be a subset of A, where $(A, \leq)$ is a POSET

Definition

upper $u \in A$ such that $\forall b \in B : b \leq u$

lower $\ell \in A$ such that $\forall b \in B : \ell \leq b$

Then we call it an upper bound of B or a lower bound of B respectively.

Upper and Lower Bounds

Let B be a subset of A, where $(A, \leq)$ is a POSET

Definition

upper $u \in A$ such that $\forall b \in B : b \leq u$

lower $\ell \in A$ such that $\forall b \in B : \ell \leq b$

Then we call it an upper bound of B or a lower bound of B respectively.

Least Upper Bound and Greatest Lower Bound

lub of B x is an upper bound of B and is the least among upper bounds of B.

glb of B x is a lower bound of B and is the greatest among lower bounds of B.

Upper and Lower Bounds

Let B be a subset of A, where $(A, \leq)$ is a POSET

Definition

upper $u \in A$ such that $\forall b \in B : b \leq u$

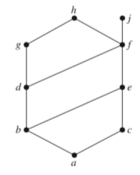
lower $\ell \in A$ such that $\forall b \in B : \ell \leq b$

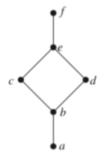
Then we call it an upper bound of B or a lower bound of B respectively.

Least Upper Bound and Greatest Lower Bound

lub of B x is an upper bound of B and is the least among upper bounds of B.

glb of B x is a lower bound of B and is the greatest among lower bounds of B.





Lattice

Definition

A partially ordered set in which every pair of elements has both a least upper bound and a greatest lower bound is a lattice.

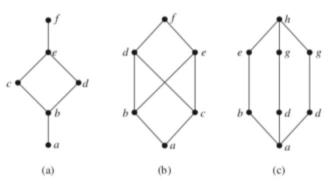
Lattice

Definition

A partially ordered set in which every pair of elements has both a least upper bound and a greatest lower bound is a lattice.

Question

Which of these POSETs are lattices?



- $(\mathbb{Z}^+, |)$
- $(1, 2, 3, 4, 5, |)$
- $(1, 2, 4, 8, 16, |)$
- $(\mathcal{P}(S), \subseteq)$

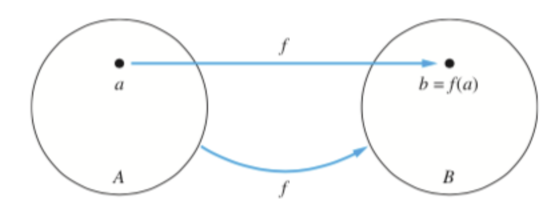
Functions

Functions

Definition

Let A and B be non-empty sets.

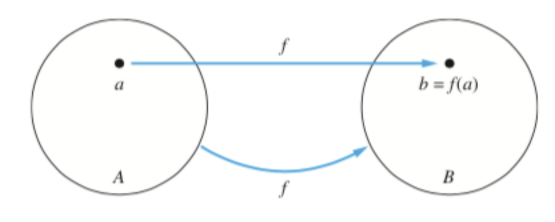
- A function f from A to B is an assignment of exactly one element of B to each element of A.
- We write $f(a) = b$ if b is the unique element of B assigned by the function f to the element a of A.



Notation

If f is a function from A to B, we write $f : A \to B$.

Functions



Terminology

- A is the domain of f
- B is the codomain of f
- b is the image of a
- a is the preimage of b
- The range (or image) of f is the set of all images of elements of the domain.

Functions

Examples

Which ones are functions?

- $f : \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x^3$
- $f : \mathbb{R} \to \mathbb{Z}$ where $f(x) = x^3$
- $f : \mathbb{Z} \to \mathbb{R}$ where $f(x) = x^3$
- $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = \sqrt{x}$
- $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = e^{2\ x^{10}}$

Operations on Functions

Let $f : A \to C$ and $g : B \to C$.
If C (the codomain) has an addition and a multiplication, then

Addition

$$(f + g)(x) = f(x) + g(x)$$

Multiplication

$$(f\ g)(x) = f(x)\ g(x)$$

Examples

Find the sum and product of the following pairs of functions

- $f : \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x^3$ and $g : \mathbb{Z} \to \mathbb{Z}$ where $g(x) = x^5$
- $f : \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x^3$ and $g : \mathbb{R} \to \mathbb{Z}$ where $g(x) = \text{floor}(x)$
- $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = x^3$ and $g : \mathbb{R} \to \mathbb{R}$ where $g(x) = 3\ x$

Properties of Functions

One-to-one

A function $f : A \rightarrow B$ is called one-to-one or injective if and only if

$$f(a) = f(b) \rightarrow a = b$$

for all a and b in the domain of f.

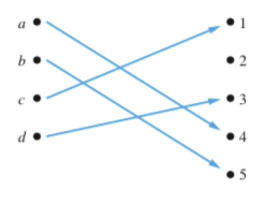
Properties of Functions

One-to-one

A function $f : A \to B$ is called one-to-one or injective if and only if

$$f(a) = f(b) \to a = b$$

for all a and b in the domain of f.



Examples

Which ones are 1-1?

- $f : \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x^3 + 5$
- $f : \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x^2 + 5$
- $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = e^x$

Properties of Functions

Onto

A function $f : A \to B$ is called onto or surjective if and only if

$$\forall b \in B \exists a \in A : f(a) = b$$

for all a and b in the domain of f.

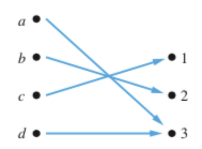
Properties of Functions

Onto

A function $f : A \to B$ is called onto or surjective if and only if

$$\forall b \in B \exists a \in A : f(a) = b$$

for all a and b in the domain of f.



Examples

Which ones are onto?

- $f : \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x^3 + 5$
- $f : \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x^2 + 5$
- $f : \mathbb{Z} \to \mathbb{Z}_+$ where $f(x) = x^3$
- $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = e^x$

Properties of Functions

Correspondence

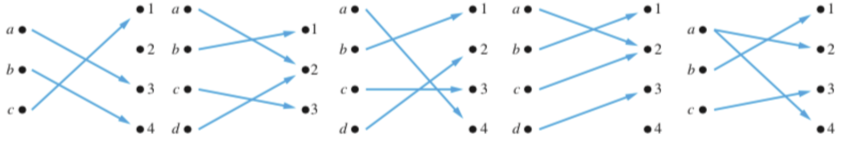
A function $f : A \rightarrow B$ is called an one-to-one correspondence if it is one-to-one and onto.

Such a function is also called **bijection**.

Properties of Functions

Correspondence

A function $f : A \to B$ is called an one-to-one correspondence if it is one-to-one and onto.
Such a function is also called **bijection**.



Examples

Which ones are bijections?

- $f : \mathbb{Z} \to \mathbb{Z}_+$ where $f(x) = x^3$
- $f : \mathbb{Z}_+ \to \mathbb{Z}_+$ where $f(x) = x^2$
- $f : \mathbb{Z} \to \mathbb{Z}_+$ where $f(x) = x + 3$
- $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = e^x$

Operations on Functions

Let $f : A \to B$ be a bijection.

Inverse

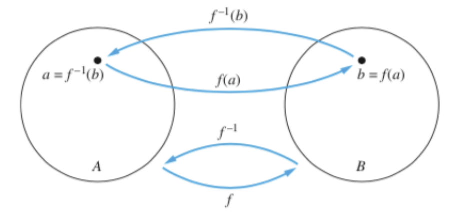
The inverse function of f is a function that assigns an element $b \in B$ to the unique element $a \in A$ such that $f(a) = b$. We denote it by f^{-1}. Thus $f^{-1}(b) = a$ when $f(a) = b$.

Operations on Functions

Let $f : A \to B$ be a bijection.

Inverse

The inverse function of f is a function that assigns an element $b \in B$ to the unique element $a \in A$ such that $f(a) = b$.
We denote it by f^{-1}. Thus $f^{-1}(b) = a$ when $f(a) = b$.

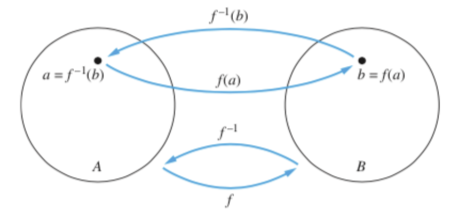


Operations on Functions

Let $f : A \to B$ be a bijection.

Inverse

The inverse function of f is a function that assigns an element $b \in B$ to the unique element $a \in A$ such that $f(a) = b$.
We denote it by f^{-1}. Thus $f^{-1}(b) = a$ when $f(a) = b$.



Examples

What are their inverses?

- $f : \mathbb{Z} \to \mathbb{Z}_+$ where $f(x) = x^3$
- $f : \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x + 1$
- $f : \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x^2 + 1$

Algebra

Introduction to Algebra

Notation

- $\mathbb{N}$ The set of natural numbers $0, 1, 2, \ldots$
- $\mathbb{Z}$ The set of integer numbers $\ldots, -2, -1, 0, 1, 2, \ldots$
- $\mathbb{Q}$ The set of rational numbers $\left\{\frac{a}{b} : a, b \in \mathbb{Z}\right\}$
- $\mathbb{R}$ The set of real numbers

Operations

Definition

Given a set A, a binary operation on A is a function $\oplus : A \times A \to A$

Examples

- Addition on integers
- Multiplication on integers
- Division on reals

Non-examples

- Division on integers
- Subtraction on natural numbers

Properties of operations

Properties

- associative
- commutative
- distributive

Special elements

- neutral : $e \oplus a = a \oplus e = a \ \forall a \in A$
- inverse : $a \oplus b = e$ for $a, b \in A$ where e is the neutral element

Group like structures

Semigroup

A set S together with an associative operation closed on S is called a semigroup.

Examples

- Addition on integers
- Multiplication on reals

Group like structures

Semigroup

A set S together with an associative operation closed on S is called a semigroup.

Examples

- Addition on integers
- Multiplication on reals

Monoid

A semigroup $(S, \oplus)$ with a neutral element is called a semigroup.

Examples

- Addition on integers
- Multiplication on reals

Group like structures

Group

A monoid $(S, \oplus)$ where every element is invertible is called a group

Examples

- Addition on integers
- Symmetries of a square
- Set of all permutations

What is the operation for the last two?

Group like structures

Group

A monoid $(S, \oplus)$ where every element is invertible is called a group

Examples

- Addition on integers
- Symmetries of a square
- Set of all permutations

What is the operation for the last two?

Non-examples

- Multiplication on reals

Ring like structures

Group

A ring $(R, \oplus, \otimes)$ is a set with two operations that is:

- Abelian group with respect to $\oplus$
  - $(a \oplus b) \oplus c = a \oplus (b \oplus c)\ \forall a, b, c \in R$
  - $a \oplus b = b \oplus a \forall a, b \in R$
  - $\exists 0 \in R : a \oplus 0 = 0 \oplus a = a\ \forall a \in R$
  - $\forall a \in R, \exists -a \in R : a \oplus -a = 0$
- Monoid under $\otimes$
  - $(a \otimes b) \otimes c = a \otimes (b \otimes c) \forall a, b, c \in R$
  - $\exists 1 \in R : a \otimes 1 = 1 \otimes a = a\ \forall a \in R$
- $\otimes$ is distributive wrt $\oplus$
  - $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)\ \forall a, b, c \in R$
  - $(b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a)\ \forall a, b, c \in R$

Examples

- Integers

Ring like structures

Field

A ring $(R, \oplus, \otimes)$ is a set with two operations that is:

- Abelian group with respect to $\oplus$
  - $(a \oplus b) \oplus c = a \oplus (b \oplus c) \forall a, b, c \in R$
  - $a \oplus b = b \oplus a \forall a, b \in R$
  - $\exists 0 \in R : a \oplus 0 = 0 \oplus a = a \ \forall a \in R$
  - $\forall a \in R, \exists -a \in R : a \oplus -a = 0$
- R^* is a monoid under $\otimes$
  - $(a \otimes b) \otimes c = a \otimes (b \otimes c) \forall a, b, c \in R$
  - $\exists 1 \in R : a \otimes 1 = 1 \otimes a = a \ \forall a \in R$
  - $\forall a \in R^*, \exists a^{-1} \in R : a \otimes a^{-1} = 1$
- $\otimes$ is distributive wrt $\oplus$
  - $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c) \ \forall a, b, c \in R$
  - $(b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a) \ \forall a, b, c \in R$

Examples

- Rationals

Sequences

Set of sequences

Consider the set S_R of all sequences with elements from a ring R.
Then this set is a ring.

Sequences

Set of sequences

Consider the set S_R of all sequences with elements from a ring R. Then this set is a ring.

What are the operations?

Sequences

Set of sequences

Consider the set S_R of all sequences with elements from a ring R. Then this set is a ring.

What are the operations? Let $a = (a_0, a_1, a_2 \ldots)$ and $b = (b_0, b_1, b_2 \ldots)$ be two elements of S_R.

Pointwise Addition

We define $c = a \oplus b$ to be $c = (a_0 + b_0, a_1 + b_1, a_2 + b_2 \ldots)$. I.e., $c_n = a_n + b_n$.

Sequences

Set of sequences

Consider the set S_R of all sequences with elements from a ring R. Then this set is a ring.

What are the operations? Let $a = (a_0, a_1, a_2 \ldots)$ and $b = (b_0, b_1, b_2 \ldots)$ be two elements of S_R.

Pointwise Addition

We define $c = a \oplus b$ to be $c = (a_0 + b_0, a_1 + b_1, a_2 + b_2 \ldots)$.
I.e., $c_n = a_n + b_n$.

Confirm the properties!

Sequences

Set of sequences

Consider the set S_R of all sequences with elements from a ring R. Then this set is a ring.

What are the operations? Let $a = (a_0, a_1, a_2 \ldots)$ and $b = (b_0, b_1, b_2 \ldots)$ be two elements of S_R.

Pointwise Addition

We define $c = a \oplus b$ to be $c = (a_0 + b_0, a_1 + b_1, a_2 + b_2 \ldots)$.
I.e., $c_n = a_n + b_n$.

Confirm the properties!

Cauchy multiplication or convolution

We define $c = a \otimes b$ to be
$c = (a_0 + b_0, a_1 b_0 + a_0 b_1, a_2 b_0 + a_1 b_1 + a_0 b_2 \ldots)$.

Sequences

Set of sequences

Consider the set S_R of all sequences with elements from a ring R. Then this set is a ring.

What are the operations? Let $a = (a_0, a_1, a_2 \ldots)$ and $b = (b_0, b_1, b_2 \ldots)$ be two elements of S_R.

Pointwise Addition

We define $c = a \oplus b$ to be $c = (a_0 + b_0, a_1 + b_1, a_2 + b_2 \ldots)$.
I.e., $c_n = a_n + b_n$.

Confirm the properties!

Cauchy multiplication or convolution

We define $c = a \otimes b$ to be
$c = (a_0 + b_0, a_1 b_0 + a_0 b_1, a_2 b_0 + a_1 b_1 + a_0 b_2 \ldots)$.
I.e., $c_n = \sum_{i+j=n} a_i + b_j$.

Sequences

Set of sequences

Consider the set S_R of all sequences with elements from a ring R. Then this set is a ring.

What are the operations? Let $a = (a_0, a_1, a_2 \ldots)$ and $b = (b_0, b_1, b_2 \ldots)$ be two elements of S_R.

Pointwise Addition

We define $c = a \oplus b$ to be $c = (a_0 + b_0, a_1 + b_1, a_2 + b_2 \ldots)$.
I.e., $c_n = a_n + b_n$.

Confirm the properties!

Cauchy multiplication or convolution

We define $c = a \otimes b$ to be
$c = (a_0 + b_0, a_1 b_0 + a_0 b_1, a_2 b_0 + a_1 b_1 + a_0 b_2 \ldots)$.
I.e., $c_n = \sum_{i+j=n} a_i + b_j$.

Is this an operation??? Does it terminate?

Sequences

Set of sequences

Consider the set S_R of all sequences with elements from a ring R. Then this set is a ring.

What are the operations? Let $a = (a_0, a_1, a_2 \dots)$ and $b = (b_0, b_1, b_2 \dots)$ be two elements of S_R.

Pointwise Addition

We define $c = a \oplus b$ to be $c = (a_0 + b_0, a_1 + b_1, a_2 + b_2 \dots)$.
I.e., $c_n = a_n + b_n$.

Confirm the properties!

Cauchy multiplication or convolution

We define $c = a \otimes b$ to be
$c = (a_0 + b_0, a_1 b_0 + a_0 b_1, a_2 b_0 + a_1 b_1 + a_0 b_2 \dots)$.
I.e., $c_n = \sum_{i+j=n} a_i + b_j$.

Is this an operation??? Does it terminate? Confirm the properties!

Formal Powerseries

The ring of formal powerseries

The set S_R of all sequences with elements from a ring R, together with pointwise addition and convolution is called the ring of formal Powerseries

Formal Powerseries

The ring of formal powerseries

The set S_R of all sequences with elements from a ring R, together with pointwise addition and convolution is called the ring of formal Powerseries

But... where is x?

Formal Powerseries

The ring of formal powerseries

The set S_R of all sequences with elements from a ring R, together with pointwise addition and convolution is called the ring of formal Powerseries

But... where is x?
That's just syntactic sugar!
What is $x^2 + 3$? It is the sequence $(3, 0, 1, 0, \dots)$
What is $2x^3 + x^3 - 3$? It is the sequence $(-3, 0, 0, 1, 2, 0, \dots)$
What is $\sum_{i=0}^{\infty} x^i$? It is the sequence $(1, 1, 1, 1, \dots)$
We have the correspondence between sequences and formal powerseries.

Formal Powerseries

The ring of formal powerseries

The set S_R of all sequences with elements from a ring R, together with pointwise addition and convolution is called the ring of formal Powerseries

But... where is x?
That's just syntactic sugar!
What is $x^2 + 3$? It is the sequence $(3, 0, 1, 0, \ldots)$
What is $2x^3 + x^3 - 3$? It is the sequence $(-3, 0, 0, 1, 2, 0, \ldots)$
What is $\sum_{i=0}^{\infty} x^i$? It is the sequence $(1, 1, 1, 1, \ldots)$
We have the correspondence between sequences and formal powerseries.

Question

Does $\sum_{i=0}^{\infty} x^i$ have a multiplicative inverse?

Polynomials

Question

What is a polynomial?

Polynomials

Question

What is a polynomial?

Polynomials

The set of sequences that are finally zero is also a ring, under the same operations. This is the ring of polynomials in one variable.

Polynomials

Question

What is a polynomial?

Polynomials

The set of sequences that are finally zero is also a ring, under the same operations. This is the ring of polynomials in one variable. We denote it by $R[x]$.

Note

That's what we call a subring!

Rational Functions

Question

The set of univariate polynomials is a ring. Can we do division?

Rational Functions

Question

The set of univariate polynomials is a ring. Can we do division?

Field of Fractions

The general construction is to take the set of all fractions of elements from a ring R. The resulting set is a field, called the field of fractions of R.

Rational Functions

Question

The set of univariate polynomials is a ring. Can we do division?

Field of Fractions

The general construction is to take the set of all fractions of elements from a ring R. The resulting set is a field, called the field of fractions of R.

Rational Functions

The field of fractions of a polynomial ring over a base ring R is called the set of rational functions over R.
We denote it by $R(x)$.

Examples

- $\frac{x+1}{x^2-x+3}$

Multivariate Polynomials

Observation

We defined the univariate polynomial ring over a ring.

Multivariate Polynomials

Observation

We defined the univariate polynomial ring over a ring.
Do it again. Define the polynomial ring over a polynomial ring!

This is the recursive construction of multivariate polynomials.

Multivariate Polynomials

Observation

We defined the univariate polynomial ring over a ring.
Do it again. Define the polynomial ring over a polynomial ring!

This is the recursive construction of multivariate polynomials.

Advantages

- It provides a natural order in the variables
- Conceptually very simple
- We can easily check it is a ring, recursively

Multivariate Polynomials

Observation

We defined the univariate polynomial ring over a ring.
Do it again. Define the polynomial ring over a polynomial ring!

This is the recursive construction of multivariate polynomials.

Advantages

- It provides a natural order in the variables
- Conceptually very simple
- We can easily check it is a ring, recursively

Disadvantages

- Usually terrible for implementation

Multivariate Polynomials

Observation

We defined the univariate polynomial ring over a ring.
Do it again. Define the polynomial ring over a polynomial ring!

This is the recursive construction of multivariate polynomials.

Advantages

- It provides a natural order in the variables
- Conceptually very simple
- We can easily check it is a ring, recursively

Disadvantages

- Usually terrible for implementation

Sparsity

How shall we represent the polynomial $x^{1000} - 2$?
How shall we represent the polynomial $x^{1000} - y^{1000}$?