Discrete Mathematics & Mathematical Reasoning
Basic Structures: Sets, Functions and Relations

Colin Stirling

Informatics

Some slides based on ones by Myrto Arapinis

Some important sets

$\mathbb{B} = \{\text{true}, \text{false}\}$ Boolean values

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ Natural numbers

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ Integers

$\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ Positive integers

$\mathbb{R}$ Real numbers

$\mathbb{R}^+$ Positive real numbers

$\mathbb{Q}$ Rational numbers

$\mathbb{C}$ Complex numbers

$\emptyset$ Empty set

Sets defined using comprehension

- $S = \{x \mid P(x)\}$ where $P(x)$ is a predicate

Sets defined using comprehension

- $S = \{x \mid P(x)\}$ where $P(x)$ is a predicate
- Example Subsets of sets upon which an order is defined

$$
\begin{array}{lcll}
[a,b] & = & \{x \mid a \leq x \leq b\} & \text{closed interval} \\
[a,b) & = & \{x \mid a \leq x < b\} & \\
(a,b] & = & \{x \mid a < x \leq b\} & \\
(a,b) & = & \{x \mid a < x < b\} & \text{open interval}
\end{array}
$$

Notation

- $x \in S$ membership

Notation

- $x \in S$ membership
- $A \cup B$ union; $A \cap B$ intersection; $A - B$ difference

Notation

- $x \in S$ membership
- $A \cup B$ union; $A \cap B$ intersection; $A - B$ difference
- $A \subseteq B$ subset; $A \supseteq B$ superset

Notation

- $x \in S$ membership
- $A \cup B$ union; $A \cap B$ intersection; $A - B$ difference
- $A \subseteq B$ subset; $A \supseteq B$ superset
- $A = B$ set equality

Notation

- $x \in S$ membership
- $A \cup B$ union; $A \cap B$ intersection; $A - B$ difference
- $A \subseteq B$ subset; $A \supseteq B$ superset
- $A = B$ set equality
- $\mathcal{P}(A)$ powerset (set of all subsets of A); also 2^A

Notation

- $x \in S$ membership
- $A \cup B$ union; $A \cap B$ intersection; $A - B$ difference
- $A \subseteq B$ subset; $A \supseteq B$ superset
- $A = B$ set equality
- $\mathcal{P}(A)$ powerset (set of all subsets of A); also 2^A
- $|A|$ cardinality

Notation

- $x \in S$ membership
- $A \cup B$ union; $A \cap B$ intersection; $A - B$ difference
- $A \subseteq B$ subset; $A \supseteq B$ superset
- $A = B$ set equality
- $\mathcal{P}(A)$ powerset (set of all subsets of A); also 2^A
- $|A|$ cardinality
- $A \times B$ cartesian product (tuple sets)

A proper mathematical definition of set is complicated (Russell's paradox)

A proper mathematical definition of set is complicated (Russell's paradox)

- The set of cats is not a member of itself

A proper mathematical definition of set is complicated (Russell's paradox)

- The set of cats is not a member of itself
- The set of non-cats (all things that are not cats) is a member of itself

A proper mathematical definition of set is complicated (Russell's paradox)

- The set of cats is not a member of itself
- The set of non-cats (all things that are not cats) is a member of itself
- Let S be the set of all sets which are not members of themselves

A proper mathematical definition of set is complicated (Russell's paradox)

- The set of cats is not a member of itself
- The set of non-cats (all things that are not cats) is a member of itself
- Let S be the set of all sets which are not members of themselves
- $S = \{x \mid x \notin x\}$ (using naive comprehension)

A proper mathematical definition of set is complicated (Russell's paradox)

- The set of cats is not a member of itself
- The set of non-cats (all things that are not cats) is a member of itself
- Let S be the set of all sets which are not members of themselves
- $S = \{x \mid x \notin x\}$ (using naive comprehension)
- Question: is S a member of itself ($S \in S$) ?

A proper mathematical definition of set is complicated (Russell's paradox)

- The set of cats is not a member of itself
- The set of non-cats (all things that are not cats) is a member of itself
- Let S be the set of all sets which are not members of themselves
- $S = \{x \mid x \notin x\}$ (using naive comprehension)
- Question: is S a member of itself ($S \in S$) ?
- $S \in S$ provided that $S \notin S$; $S \notin S$ provided that $S \in S$

A proper mathematical definition of set is complicated (Russell's paradox)

- The set of cats is not a member of itself
- The set of non-cats (all things that are not cats) is a member of itself
- Let S be the set of all sets which are not members of themselves
- $S = \{x \mid x \notin x\}$ (using naive comprehension)
- Question: is S a member of itself ($S \in S$) ?
- $S \in S$ provided that $S \notin S$; $S \notin S$ provided that $S \in S$
- Modern formulations (such as Zermelo-Fraenkel set theory) restrict comprehension. (However, it is impossible to prove in ZF that ZF is consistent unless ZF is inconsistent.)

Functions

- Assume A and B are non-empty sets

Functions

- Assume A and B are non-empty sets
- A function f from A to B is an assignment of exactly one element of B to each element of A

Functions

- Assume A and B are non-empty sets
- A function f from A to B is an assignment of exactly one element of B to each element of A
- $f(a) = b$ if f assigns b to a

Functions

- Assume A and B are non-empty sets
- A function f from A to B is an assignment of exactly one element of B to each element of A
- $f(a) = b$ if f assigns b to a
- $f : A \rightarrow B$ if f is a function from A to B

One-to-one or injective functions

Definition

$f : A \to B$ is injective iff $\forall a, c \in A$ (if $f(a) = f(c)$ then $a = c$)

One-to-one or injective functions

Definition

$f : A \to B$ is injective iff $\forall a, c \in A$ (if $f(a) = f(c)$ then $a = c$)

- Is the identity function $\iota_A : A \to A$ injective?

One-to-one or injective functions

Definition

$f : A \to B$ is injective iff $\forall a, c \in A$ (if $f(a) = f(c)$ then $a = c$)

- Is the identity function $\iota_A : A \to A$ injective? YES

One-to-one or injective functions

Definition

$f : A \to B$ is injective iff $\forall a, c \in A$ (if $f(a) = f(c)$ then $a = c$)

- Is the identity function $\iota_A : A \to A$ injective? YES
- Is the function $\sqrt{\cdot} : \mathbb{Z}^+ \to \mathbb{R}^+$ injective?

One-to-one or injective functions

Definition

$f : A \to B$ is injective iff $\forall a, c \in A$ (if $f(a) = f(c)$ then $a = c$)

- Is the identity function $\iota_A : A \to A$ injective? YES
- Is the function $\sqrt{\cdot} : \mathbb{Z}^+ \to \mathbb{R}^+$ injective? YES

One-to-one or injective functions

Definition

$f : A \to B$ is injective iff $\forall a, c \in A$ (if $f(a) = f(c)$ then $a = c$)

- Is the identity function $\iota_A : A \to A$ injective? YES
- Is the function $\sqrt{\cdot} : \mathbb{Z}^+ \to \mathbb{R}^+$ injective? YES
- Is the squaring function $\cdot^2 : \mathbb{Z} \to \mathbb{Z}$ injective?

One-to-one or injective functions

Definition

$f : A \to B$ is injective iff $\forall a, c \in A$ (if $f(a) = f(c)$ then $a = c$)

- Is the identity function $\iota_A : A \to A$ injective? YES
- Is the function $\sqrt{\cdot} : \mathbb{Z}^+ \to \mathbb{R}^+$ injective? YES
- Is the squaring function $\cdot^2 : \mathbb{Z} \to \mathbb{Z}$ injective? NO

One-to-one or injective functions

Definition

$f : A \to B$ is injective iff $\forall a, c \in A$ (if $f(a) = f(c)$ then $a = c$)

- Is the identity function $\iota_A : A \to A$ injective? YES
- Is the function $\sqrt{\cdot} : \mathbb{Z}^+ \to \mathbb{R}^+$ injective? YES
- Is the squaring function $\cdot^2 : \mathbb{Z} \to \mathbb{Z}$ injective? NO
- Is the function $|\cdot| : \mathbb{R} \to \mathbb{R}$ injective?

One-to-one or injective functions

Definition

$f : A \to B$ is injective iff $\forall a, c \in A$ (if $f(a) = f(c)$ then $a = c$)

- Is the identity function $\iota_A : A \to A$ injective? YES
- Is the function $\sqrt{\cdot} : \mathbb{Z}^+ \to \mathbb{R}^+$ injective? YES
- Is the squaring function $\cdot^2 : \mathbb{Z} \to \mathbb{Z}$ injective? NO
- Is the function $|\cdot| : \mathbb{R} \to \mathbb{R}$ injective? NO

One-to-one or injective functions

Definition

$f : A \to B$ is injective iff $\forall a, c \in A$ (if $f(a) = f(c)$ then $a = c$)

- Is the identity function $\iota_A : A \to A$ injective? YES
- Is the function $\sqrt{\cdot} : \mathbb{Z}^+ \to \mathbb{R}^+$ injective? YES
- Is the squaring function $\cdot^2 : \mathbb{Z} \to \mathbb{Z}$ injective? NO
- Is the function $|\cdot| : \mathbb{R} \to \mathbb{R}$ injective? NO
- Assume $m > 1$. Is $\text{mod}\, m : Z \to \{0, \ldots, m-1\}$ injective?

One-to-one or injective functions

Definition

$f : A \to B$ is injective iff $\forall a, c \in A$ (if $f(a) = f(c)$ then $a = c$)

- Is the identity function $\iota_A : A \to A$ injective? YES
- Is the function $\sqrt{\cdot} : \mathbb{Z}^+ \to \mathbb{R}^+$ injective? YES
- Is the squaring function $\cdot^2 : \mathbb{Z} \to \mathbb{Z}$ injective? NO
- Is the function $|\cdot| : \mathbb{R} \to \mathbb{R}$ injective? NO
- Assume $m > 1$. Is $\text{mod}\, m : Z \to \{0, \ldots, m-1\}$ injective? NO

Onto or surjective functions

Definition

$f : A \to B$ is surjective iff $\forall b \in B\ \exists a \in A\ (f(a) = b)$

Onto or surjective functions

Definition

$f : A \to B$ is surjective iff $\forall b \in B\ \exists a \in A\ (f(a) = b)$

- Is the identity function $\iota_A : A \to A$ surjective?

Onto or surjective functions

Definition

$f : A \to B$ is surjective iff $\forall b \in B\ \exists a \in A\ (f(a) = b)$

- Is the identity function $\iota_A : A \to A$ surjective? YES

Onto or surjective functions

Definition

$f : A \to B$ is surjective iff $\forall b \in B\ \exists a \in A\ (f(a) = b)$

- Is the identity function $\iota_A : A \to A$ surjective? YES
- Is the function $\sqrt{\cdot} : \mathbb{Z}^+ \to \mathbb{R}^+$ surjective?

Onto or surjective functions

Definition

$f : A \to B$ is surjective iff $\forall b \in B\ \exists a \in A\ (f(a) = b)$

- Is the identity function $\iota_A : A \to A$ surjective? YES
- Is the function $\sqrt{\cdot} : \mathbb{Z}^+ \to \mathbb{R}^+$ surjective? NO

Onto or surjective functions

Definition

$f : A \to B$ is surjective iff $\forall b \in B\ \exists a \in A\ (f(a) = b)$

- Is the identity function $\iota_A : A \to A$ surjective? YES
- Is the function $\sqrt{\cdot} : \mathbb{Z}^+ \to \mathbb{R}^+$ surjective? NO
- Is the function $\cdot^2 : \mathbb{Z} \to \mathbb{Z}$ surjective?

Onto or surjective functions

Definition

$f : A \to B$ is surjective iff $\forall b \in B\ \exists a \in A\ (f(a) = b)$

- Is the identity function $\iota_A : A \to A$ surjective? YES
- Is the function $\sqrt{\cdot} : \mathbb{Z}^+ \to \mathbb{R}^+$ surjective? NO
- Is the function $\cdot^2 : \mathbb{Z} \to \mathbb{Z}$ surjective? NO

Onto or surjective functions

Definition

$f : A \to B$ is surjective iff $\forall b \in B\ \exists a \in A\ (f(a) = b)$

- Is the identity function $\iota_A : A \to A$ surjective? YES
- Is the function $\sqrt{\cdot} : \mathbb{Z}^+ \to \mathbb{R}^+$ surjective? NO
- Is the function $\cdot^2 : \mathbb{Z} \to \mathbb{Z}$ surjective? NO
- Is the function $|\cdot| : \mathbb{R} \to \mathbb{R}$ surjective?

Onto or surjective functions

Definition

$f : A \to B$ is surjective iff $\forall b \in B\ \exists a \in A\ (f(a) = b)$

- Is the identity function $\iota_A : A \to A$ surjective? YES
- Is the function $\sqrt{\cdot} : \mathbb{Z}^+ \to \mathbb{R}^+$ surjective? NO
- Is the function $\cdot^2 : \mathbb{Z} \to \mathbb{Z}$ surjective? NO
- Is the function $|\cdot| : \mathbb{R} \to \mathbb{R}$ surjective? NO

Onto or surjective functions

Definition

$f : A \to B$ is surjective iff $\forall b \in B\ \exists a \in A\ (f(a) = b)$

- Is the identity function $\iota_A : A \to A$ surjective? YES
- Is the function $\sqrt{\cdot} : \mathbb{Z}^+ \to \mathbb{R}^+$ surjective? NO
- Is the function $\cdot^2 : \mathbb{Z} \to \mathbb{Z}$ surjective? NO
- Is the function $|\cdot| : \mathbb{R} \to \mathbb{R}$ surjective? NO
- Assume $m > 1$. Is $\mathrm{mod}\, m : Z \to \{0, \ldots, m-1\}$ surjective?

Onto or surjective functions

Definition

$f : A \to B$ is surjective iff $\forall b \in B\ \exists a \in A\ (f(a) = b)$

- Is the identity function $\iota_A : A \to A$ surjective? YES
- Is the function $\sqrt{\cdot} : \mathbb{Z}^+ \to \mathbb{R}^+$ surjective? NO
- Is the function $\cdot^2 : \mathbb{Z} \to \mathbb{Z}$ surjective? NO
- Is the function $|\cdot| : \mathbb{R} \to \mathbb{R}$ surjective? NO
- Assume $m > 1$. Is $\mathrm{mod}\, m : Z \to \{0, \ldots, m-1\}$ surjective? YES

One-to-one correspondence or bijection

Definition

$f : A \rightarrow B$ is a bijection iff it is both injective and surjective

One-to-one correspondence or bijection

Definition

$f : A \to B$ is a bijection iff it is both injective and surjective

- Is the identity function $\iota_A : A \to A$ a bijection?

One-to-one correspondence or bijection

Definition

$f : A \to B$ is a bijection iff it is both injective and surjective

- Is the identity function $\iota_A : A \to A$ a bijection? YES

One-to-one correspondence or bijection

Definition

$f : A \to B$ is a bijection iff it is both injective and surjective

- Is the identity function $\iota_A : A \to A$ a bijection? YES
- Is the function $\sqrt{\cdot} : \mathbb{R}^+ \to \mathbb{R}^+$ a bijection?

One-to-one correspondence or bijection

Definition

$f : A \to B$ is a bijection iff it is both injective and surjective

- Is the identity function $\iota_A : A \to A$ a bijection? YES
- Is the function $\sqrt{\cdot} : \mathbb{R}^+ \to \mathbb{R}^+$ a bijection? YES

One-to-one correspondence or bijection

Definition

$f : A \to B$ is a bijection iff it is both injective and surjective

- Is the identity function $\iota_A : A \to A$ a bijection? YES
- Is the function $\sqrt{\cdot} : \mathbb{R}^+ \to \mathbb{R}^+$ a bijection? YES
- Is the function $\cdot^2 : \mathbb{R} \to \mathbb{R}$ a bijection?

One-to-one correspondence or bijection

Definition

$f : A \to B$ is a bijection iff it is both injective and surjective

- Is the identity function $\iota_A : A \to A$ a bijection? YES
- Is the function $\sqrt{\cdot} : \mathbb{R}^+ \to \mathbb{R}^+$ a bijection? YES
- Is the function $\cdot^2 : \mathbb{R} \to \mathbb{R}$ a bijection? NO

One-to-one correspondence or bijection

Definition

$f : A \to B$ is a bijection iff it is both injective and surjective

- Is the identity function $\iota_A : A \to A$ a bijection? YES
- Is the function $\sqrt{\cdot} : \mathbb{R}^+ \to \mathbb{R}^+$ a bijection? YES
- Is the function $\cdot^2 : \mathbb{R} \to \mathbb{R}$ a bijection? NO
- Is the function $|\cdot| : \mathbb{R} \to \mathbb{R}$ a bijection?

One-to-one correspondence or bijection

Definition

$f : A \to B$ is a bijection iff it is both injective and surjective

- Is the identity function $\iota_A : A \to A$ a bijection? YES
- Is the function $\sqrt{\cdot} : \mathbb{R}^+ \to \mathbb{R}^+$ a bijection? YES
- Is the function $\cdot^2 : \mathbb{R} \to \mathbb{R}$ a bijection? NO
- Is the function $|\cdot| : \mathbb{R} \to \mathbb{R}$ a bijection? NO

Function composition

Definition

Let $f : B \to C$ and $g : A \to B$. The composition function $f \circ g : A \to C$ is $(f \circ g)(a) = f(g(a))$

Results about function composition

Theorem

The composition of two functions is a function

Results about function composition

Theorem

The composition of two functions is a function

Theorem

The composition of two injective functions is an injective function

Results about function composition

Theorem

The composition of two functions is a function

Theorem

The composition of two injective functions is an injective function

Theorem

The composition of two surjective functions is a surjective function

Results about function composition

Theorem

The composition of two functions is a function

Theorem

The composition of two injective functions is an injective function

Theorem

The composition of two surjective functions is a surjective function

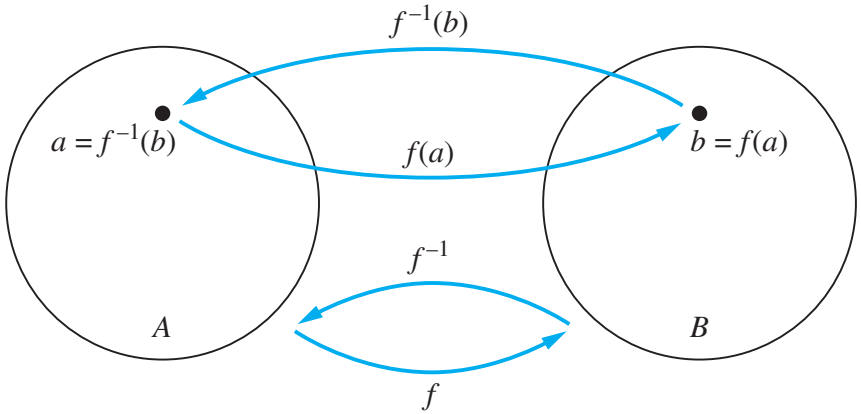
Corollary

The composition of two bijections is a bijection

Inverse function

Definition

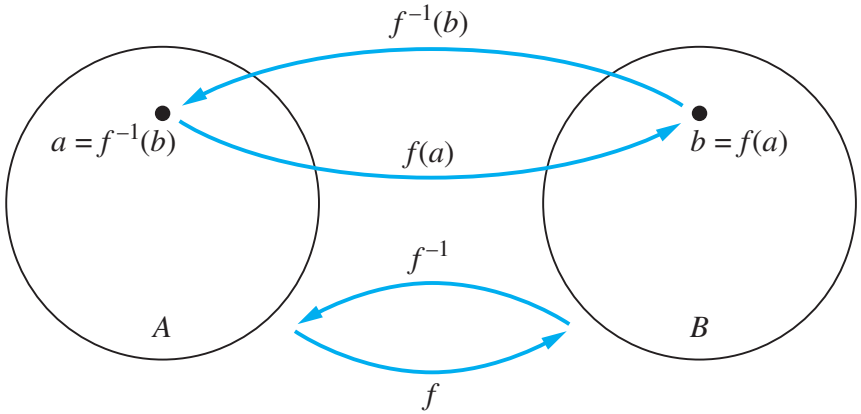
If $f : A \to B$ is a bijection, then the inverse of f, written $f^{-1} : B \to A$ is $f^{-1}(b) = a$ iff $f(a) = b$



Inverse function

Definition

If $f : A \to B$ is a bijection, then the inverse of f, written $f^{-1} : B \to A$ is $f^{-1}(b) = a$ iff $f(a) = b$

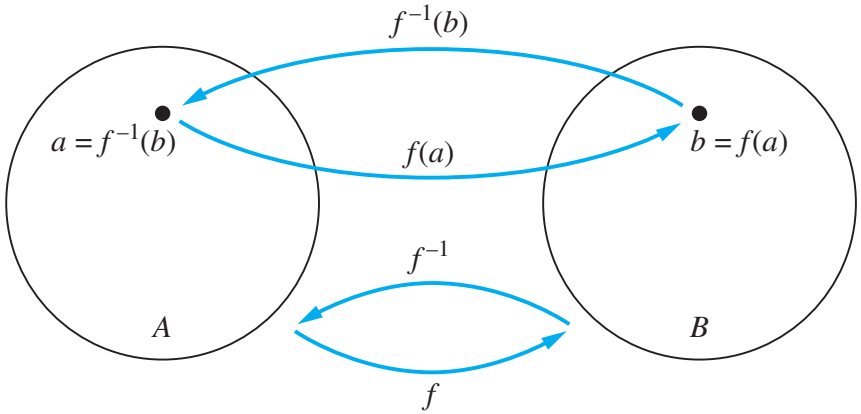


What is the inverse of $\iota_A : A \to A$?

Inverse function

Definition

If $f : A \to B$ is a bijection, then the inverse of f, written $f^{-1} : B \to A$ is $f^{-1}(b) = a$ iff $f(a) = b$



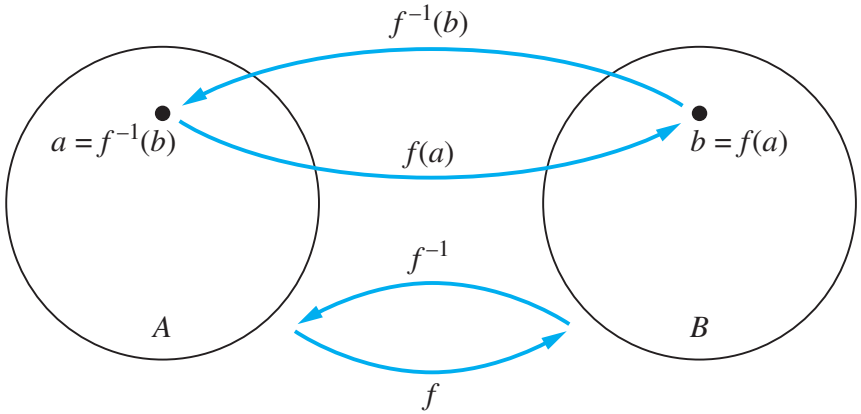
What is the inverse of $\iota_A : A \to A$?

What is the inverse of $\sqrt{}:\mathbb{R}^+ \to \mathbb{R}^+$?

Inverse function

Definition

If $f : A \to B$ is a bijection, then the inverse of f, written $f^{-1} : B \to A$ is $f^{-1}(b) = a$ iff $f(a) = b$



What is the inverse of $\iota_A : A \to A$?

What is the inverse of $\sqrt{}:\mathbb{R}^+ \to \mathbb{R}^+$?

What is $f^{-1} \circ f$? and $f \circ f^{-1}$?

The floor and ceiling functions

Definition

The floor function $\lfloor\ \rfloor : \mathbb{R} \to \mathbb{Z}$ is $\lfloor x \rfloor$ equals the largest integer less than or equal to x

Definition

The ceiling function $\lceil\ \rceil : \mathbb{R} \to \mathbb{Z}$ is $\lceil x \rceil$ equals the smallest integer greater than or equal to x

The floor and ceiling functions

Definition

The floor function $\lfloor\ \rfloor : \mathbb{R} \to \mathbb{Z}$ is $\lfloor x \rfloor$ equals the largest integer less than or equal to x

Definition

The ceiling function $\lceil\ \rceil : \mathbb{R} \to \mathbb{Z}$ is $\lceil x \rceil$ equals the smallest integer greater than or equal to x

$$\left\lfloor \frac{1}{2} \right\rfloor = \left\lceil -\frac{1}{2} \right\rceil = \lfloor 0 \rfloor = \lceil 0 \rceil = 0$$

The floor and ceiling functions

Definition

The floor function $\lfloor\ \rfloor : \mathbb{R} \to \mathbb{Z}$ is $\lfloor x \rfloor$ equals the largest integer less than or equal to x

Definition

The ceiling function $\lceil\ \rceil : \mathbb{R} \to \mathbb{Z}$ is $\lceil x \rceil$ equals the smallest integer greater than or equal to x

$$\left\lfloor \frac{1}{2} \right\rfloor = \left\lceil -\frac{1}{2} \right\rceil = \lfloor 0 \rfloor = \lceil 0 \rceil = 0$$

$$\lfloor -6.1 \rfloor = -7 \qquad \lceil 6.1 \rceil = 7$$

Useful tips about floors and ceilings

- When showing properties of floors is to let $x = n + \epsilon$ if $\lfloor x \rfloor = n$ where $0 \leq \epsilon < 1$
- Similarly, for ceilings let $x = n - \epsilon$ if $\lceil x \rceil = n$ where $0 \leq \epsilon < 1$

Useful tips about floors and ceilings

- When showing properties of floors is to let $x = n + \epsilon$ if $\lfloor x \rfloor = n$ where $0 \leq \epsilon < 1$
- Similarly, for ceilings let $x = n - \epsilon$ if $\lceil x \rceil = n$ where $0 \leq \epsilon < 1$
- Prove

$$\forall x \in \mathbb{R}\, (\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + 1/2 \rfloor)$$

Useful tips about floors and ceilings

- When showing properties of floors is to let $x = n + \epsilon$ if $\lfloor x \rfloor = n$ where $0 \leq \epsilon < 1$
- Similarly, for ceilings let $x = n - \epsilon$ if $\lceil x \rceil = n$ where $0 \leq \epsilon < 1$
- Prove

$$\forall x \in \mathbb{R}\, (\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + 1/2 \rfloor)$$

- Proof in book

Prove $\lceil x \rceil + \lceil y \rceil = \lceil x + y \rceil$

Prove $\lceil x \rceil + \lceil y \rceil = \lceil x + y \rceil$

False; counterexample $x = 1/2$ and $y = 1/2$

The factorial function

Definition

The factorial function $f : \mathbb{N} \to \mathbb{N}$, denoted as $f(n) = n!$ assigns to n the product of the first n positive integers

$$f(0) = 0! = 1$$

and

$$f(n) = n! = 1 \cdot 2 \cdot \cdots \cdot (n-1) \cdot n$$

Relations

Definition

A binary relation R on sets A and B is a subset $R \subseteq A \times B$

Relations

Definition

A binary relation R on sets A and B is a subset $R \subseteq A \times B$

- R is a set of tuples (a, b) with $a \in A$ and $b \in B$

Relations

Definition

A binary relation R on sets A and B is a subset $R \subseteq A \times B$

- R is a set of tuples (a, b) with $a \in A$ and $b \in B$
- Often we write $a\,R\,b$ for $(a, b) \in R$

Relations

Definition

A binary relation R on sets A and B is a subset $R \subseteq A \times B$

- R is a set of tuples (a, b) with $a \in A$ and $b \in B$
- Often we write $a\,R\,b$ for $(a, b) \in R$
- R is a relation on A if $B = A$

Relations

Definition

A binary relation R on sets A and B is a subset $R \subseteq A \times B$

- R is a set of tuples (a, b) with $a \in A$ and $b \in B$
- Often we write $a\,R\,b$ for $(a, b) \in R$
- R is a relation on A if $B = A$

Relations

Definition

A binary relation R on sets A and B is a subset $R \subseteq A \times B$

- R is a set of tuples (a, b) with $a \in A$ and $b \in B$
- Often we write $a\,R\,b$ for $(a, b) \in R$
- R is a relation on A if $B = A$

Definition

Given sets $A_1, \ldots, A_n$, a subset $R \subseteq A_1 \times \cdots \times A_n$ is an n-ary relation

Examples

- Divides $|$: $\mathbb{Z}^+ \times \mathbb{Z}^+$ is $\{(n, m) \mid \exists k \in \mathbb{Z}^+ \ (m = kn)\}$

Examples

- Divides $|$: $\mathbb{Z}^+ \times \mathbb{Z}^+$ is $\{(n, m) \mid \exists k \in \mathbb{Z}^+ \ (m = kn)\}$
- Let $m > 1$ be an integer. $R = \{(a, b) \mid a \bmod m = b \bmod m\}$

Examples

- Divides $| : \mathbb{Z}^+ \times \mathbb{Z}^+$ is $\{(n, m) \mid \exists k \in \mathbb{Z}^+ \ (m = kn)\}$
- Let $m > 1$ be an integer. $R = \{(a, b) \mid a \bmod m = b \bmod m\}$
- Written as $a \equiv b \pmod{m}$

Properties of binary relations

A binary relation R on A is called

- reflexive iff $\forall x \in A\, (x, x) \in R$

Properties of binary relations

A binary relation R on A is called

- reflexive iff $\forall x \in A\, (x, x) \in R$
- $\leq$, $=$, and $|$ are reflexive, but $<$ is not

Properties of binary relations

A binary relation R on A is called

- reflexive iff $\forall x \in A\ (x, x) \in R$
- $\leq$, $=$, and $|$ are reflexive, but $<$ is not
- symmetric iff $\forall x, y \in A\ ((x, y) \in R \rightarrow (y, x) \in R)$
- $=$ is symmetric, but $\leq$, $<$, and $|$ are not

Properties of binary relations

A binary relation R on A is called

- reflexive iff $\forall x \in A\ (x, x) \in R$
- $\leq$, $=$, and $|$ are reflexive, but $<$ is not
- symmetric iff $\forall x, y \in A\ ((x, y) \in R \rightarrow (y, x) \in R)$
- $=$ is symmetric, but $\leq$, $<$, and $|$ are not
- antisymmetric iff $\forall x, y \in A\ (((x, y) \in R \wedge (y, x) \in R) \rightarrow x = y)$

Properties of binary relations

A binary relation R on A is called

- reflexive iff $\forall x \in A\ (x, x) \in R$
- $\leq$, $=$, and $|$ are reflexive, but $<$ is not
- symmetric iff $\forall x, y \in A\ ((x, y) \in R \rightarrow (y, x) \in R)$
- $=$ is symmetric, but $\leq$, $<$, and $|$ are not
- antisymmetric iff $\forall x, y \in A\ (((x, y) \in R \wedge (y, x) \in R) \rightarrow x = y)$
- $\leq$, $=$, $<$, and $|$ are antisymmetric

Properties of binary relations

A binary relation R on A is called

- reflexive iff $\forall x \in A\ (x, x) \in R$
- $\leq$, $=$, and $|$ are reflexive, but $<$ is not
- symmetric iff $\forall x, y \in A\ ((x, y) \in R \rightarrow (y, x) \in R)$
- $=$ is symmetric, but $\leq$, $<$, and $|$ are not
- antisymmetric iff $\forall x, y \in A\ (((x, y) \in R \wedge (y, x) \in R) \rightarrow x = y)$
- $\leq$, $=$, $<$, and $|$ are antisymmetric
- transitive iff $\forall x, y, z \in A\ (((x, y) \in R \wedge (y, z) \in R) \rightarrow (x, z) \in R)$
- $\leq$, $=$, $<$, and $|$ are transitive

Equivalence relations

Definition

A relation R on a set A is an equivalence relation iff it is reflexive, symmetric and transitive

Equivalence relations

Definition

A relation R on a set A is an equivalence relation iff it is reflexive, symmetric and transitive

- Let Σ^* be the set of strings over alphabet Σ. The relation $\{(s,t) \in \Sigma^* \times \Sigma^* \mid |s| = |t|\}$ is an equivalence relation

Equivalence relations

Definition

A relation R on a set A is an equivalence relation iff it is reflexive, symmetric and transitive

- Let Σ^* be the set of strings over alphabet Σ. The relation $\{(s,t) \in \Sigma^* \times \Sigma^* \mid |s| = |t|\}$ is an equivalence relation
- $|$ on integers is not an equivalence relation.

Equivalence relations

Definition

A relation R on a set A is an equivalence relation iff it is reflexive, symmetric and transitive

- Let Σ^* be the set of strings over alphabet Σ. The relation $\{(s,t) \in \Sigma^* \times \Sigma^* \mid |s| = |t|\}$ is an equivalence relation
- $|$ on integers is not an equivalence relation.
- For $m > 1$ be an integer the relation $\equiv \pmod m$ is an equivalence relation on integers

Equivalence classes

Definition

Let R be an equivalence relation on a set A and $a \in A$. Let

$$[a]_R = \{s \mid (a, s) \in R\}$$

be the equivalence class of a w.r.t. R

If $b \in [a]_R$ then b is called a representative of the equivalence class. Every member of the class can be a representative

Theorem

Result

Let R be an equivalence on A and $a, b \in A$. The following three statements are equivalent

1. aRb
2. $[a]_R = [b]_R$
3. $[a]_R \cap [b]_R \neq \emptyset$

Theorem

Result

Let R be an equivalence on A and $a, b \in A$. The following three statements are equivalent

1. aRb
2. $[a]_R = [b]_R$
3. $[a]_R \cap [b]_R \neq \emptyset$

Proof in book

Partitions of a set

Definition

A partition of a set A is a collection of disjoint, nonempty subsets that have A as their union. In other words, the collection of subsets $A_i \subseteq A$ with $i \in I$ (where I is an index set) forms a partition of A iff

1. $A_i \neq \emptyset$ for all $i \in I$
2. $A_i \cap A_j = \emptyset$ for all $i \neq j \in I$
3. $\bigcup_{i \in I} A_i = A$

Result

Theorem

1. If R is an equivalence on A, then the equivalence classes of R form a partition of A
2. Conversely, given a partition $\{A_i \mid i \in I\}$ of A there exists an equivalence relation R that has exactly the sets A_i, $i \in I$, as its equivalence classes

Result

Theorem

1. If R is an equivalence on A, then the equivalence classes of R form a partition of A
2. Conversely, given a partition $\{A_i \mid i \in I\}$ of A there exists an equivalence relation R that has exactly the sets A_i, $i \in I$, as its equivalence classes

Proof in book