Mathematical Preliminaries

Mathematical Preliminaries

- Sets
- Functions
- Relations
- Graphs
- Proof Techniques

SETS

A set is a collection of elements

$$A = \{1, 2, 3\}$$

$$B = \{train, bus, bicycle, airplane\}$$

Membership

$$1 \in A$$

$$ship \notin B$$

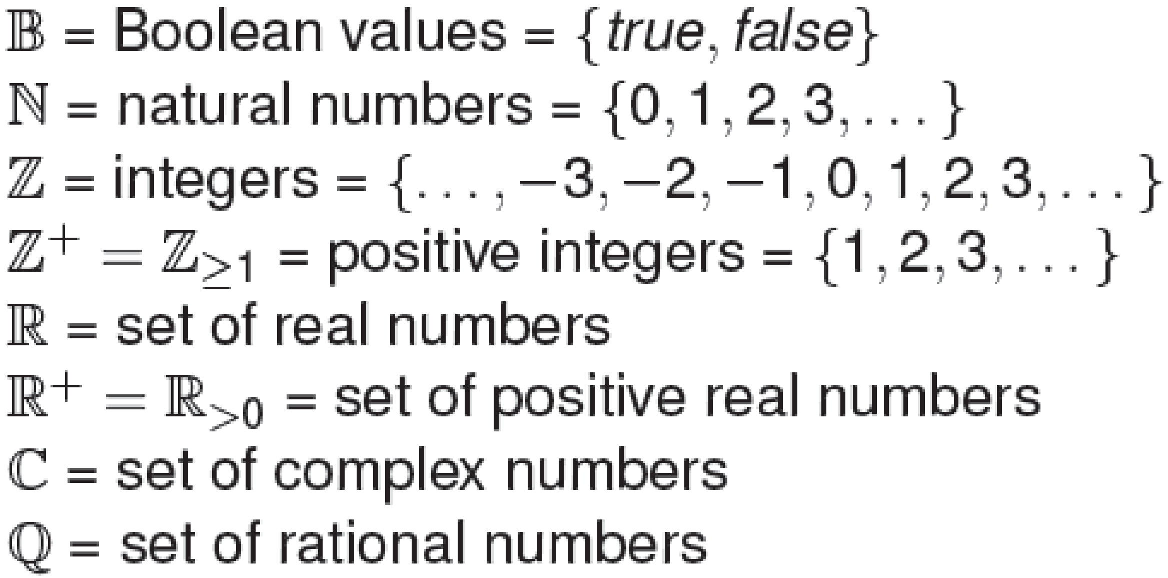
Set Representations

$C = \{ a, b, c, d, e, f, g, h, i, j, k \}$

$C = \{ a, b, \ldots, k \}$ → *finite set*

$S = \{ 2, 4, 6, \ldots \}$ → *infinite set*

Some important sets



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

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

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

$\mathbb{Z}^+ = \mathbb{Z}_{\geq 1}$ = positive integers = $\{1, 2, 3, \ldots\}$

$\mathbb{R}$ = set of real numbers

$\mathbb{R}^+ = \mathbb{R}_{>0}$ = set of positive real numbers

$\mathbb{C}$ = set of complex numbers

$\mathbb{Q}$ = set of rational numbers

Set Representations

- Specify the property (or properties) that all members of the set must satisfy.
  $S = \{x \mid x \text{ is a positive integer less than } 100\}$
  $S = \{x \mid x \in \mathbb{Z}^+ \;\wedge\; x < 100\}$
  $S = \{x \in \mathbb{Z}^+ \mid x < 100\}$
- A predicate can be used, e.g.,

  $$S = \{x \mid P(x)\}$$

  where $P(x)$ is true iff x is a prime number.
- Positive rational numbers

  $$\mathbb{Q}^+ = \{x \in \mathbb{R} \mid \exists p, q \in \mathbb{Z}^+ \; x = p/q\}$$

Set Representations

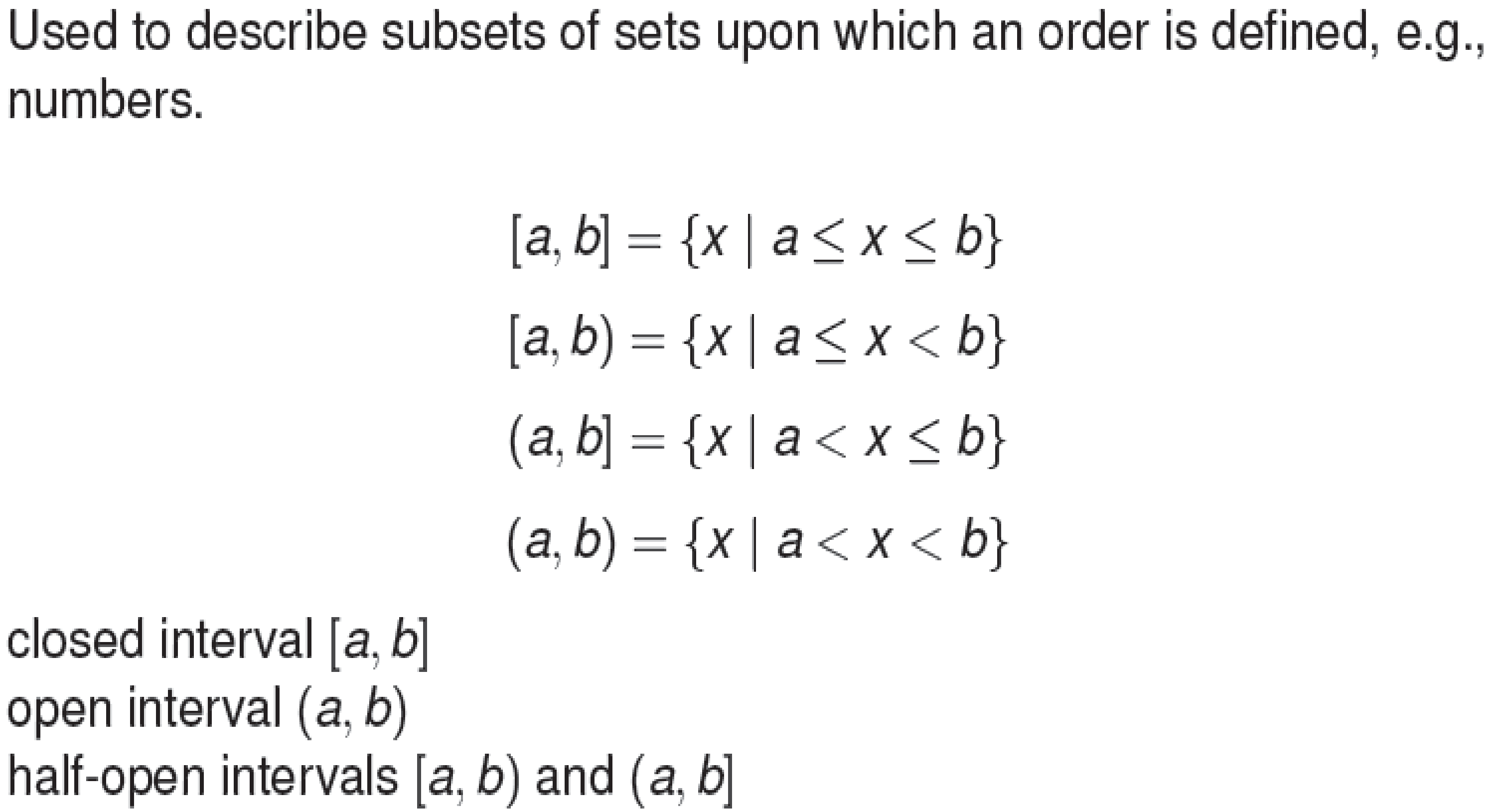
Order not important

$S = \{a, b, c, d\} = \{b, c, a, d\}.$

Listing more than once does not change the set.

$S = \{a, b, c, d\} = \{a, b, c, b, c, d\}.$

Interval Notations



Used to describe subsets of sets upon which an order is defined, e.g., numbers.

$$[a, b] = \{x \mid a \leq x \leq b\}$$

$$[a, b) = \{x \mid a \leq x < b\}$$

$$(a, b] = \{x \mid a < x \leq b\}$$

$$(a, b) = \{x \mid a < x < b\}$$

closed interval $[a, b]$
open interval (a, b)
half-open intervals $[a, b)$ and $(a, b]$

Universal Set

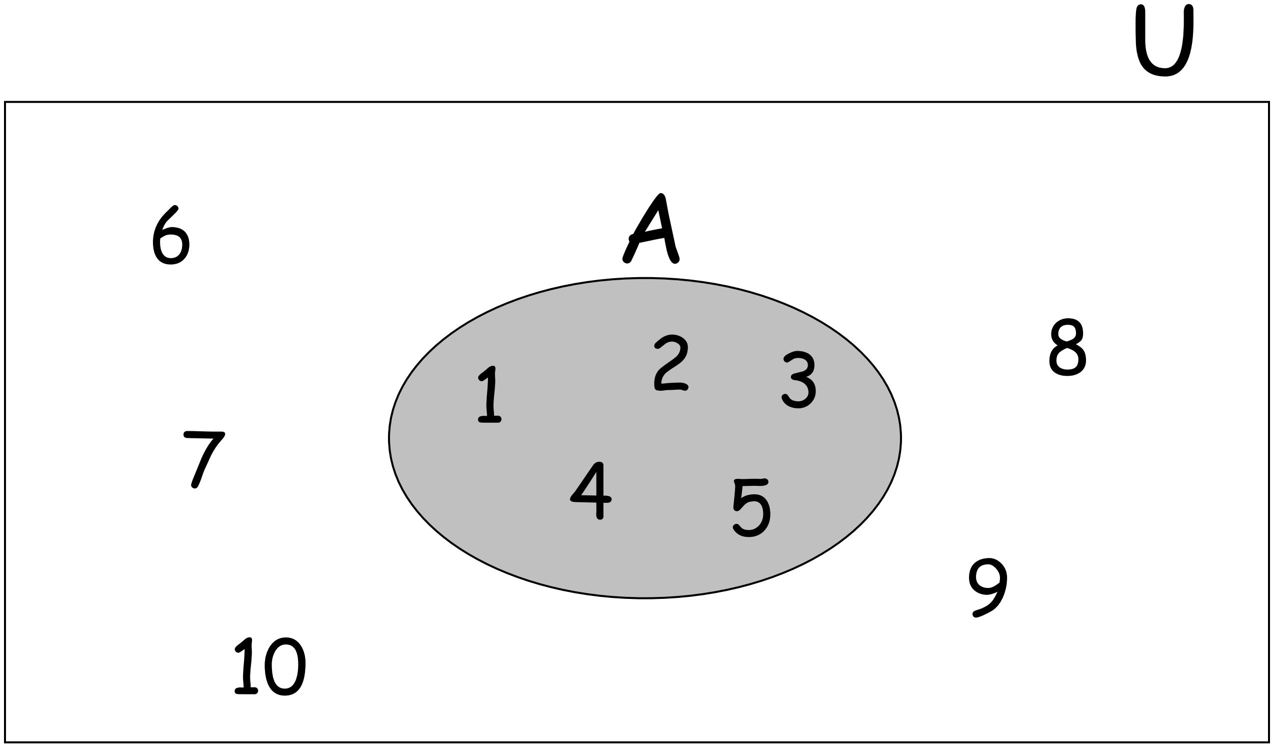
A universal set is the collection of all objects in a particular context or theory.

Depends the context or theory under consideration.

For example, we might define *U* as the set of all living things on planet earth. In that case, the set of all dogs is a subset of *U*, the set of all fish is another subset of *U*, and the set of all trees is yet another subset of *U*.

$U = \{ 1 , \ldots , 10 \}$

$A = \{ 1, 2, 3, 4, 5 \}$



Set Operations

$A = \{ 1, 2, 3 \}$ $B = \{ 2, 3, 4, 5 \}$

- Union

  $A \cup B = \{ 1, 2, 3, 4, 5 \}$

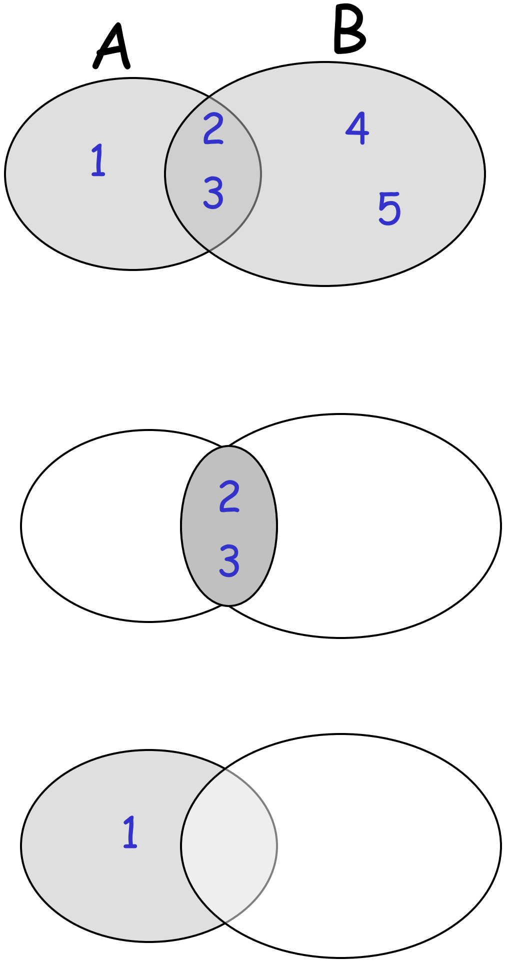
- Intersection

  $A \cap B = \{ 2, 3 \}$

- Difference

  $A - B = \{ 1 \}$

  $B - A = \{ 4, 5 \}$

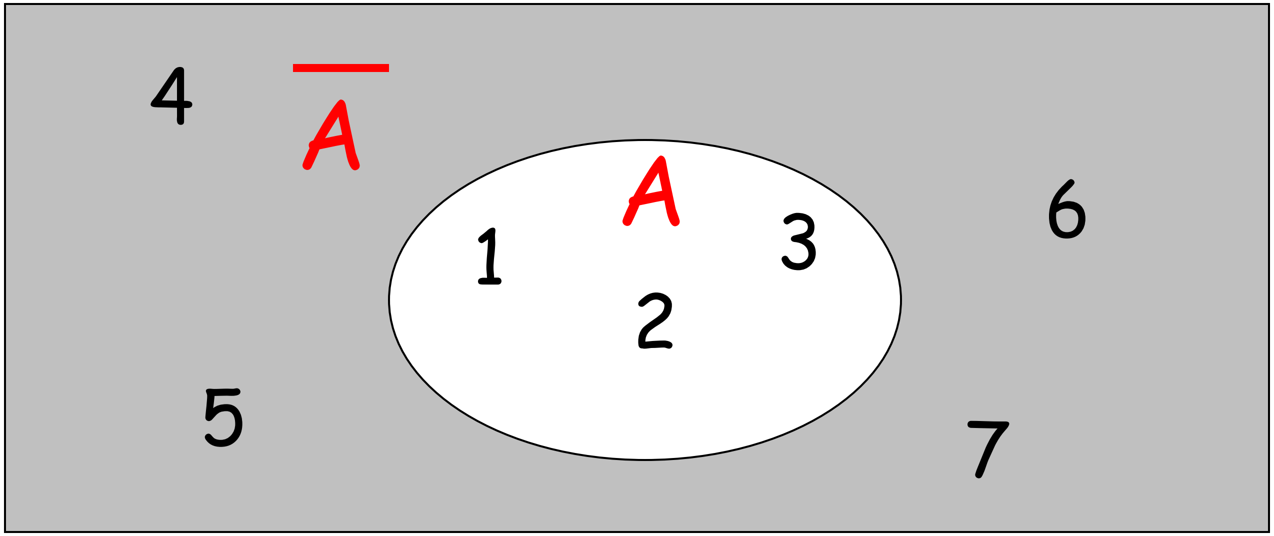


Venn diagrams

- Complement

Universal set = {1, ..., 7}

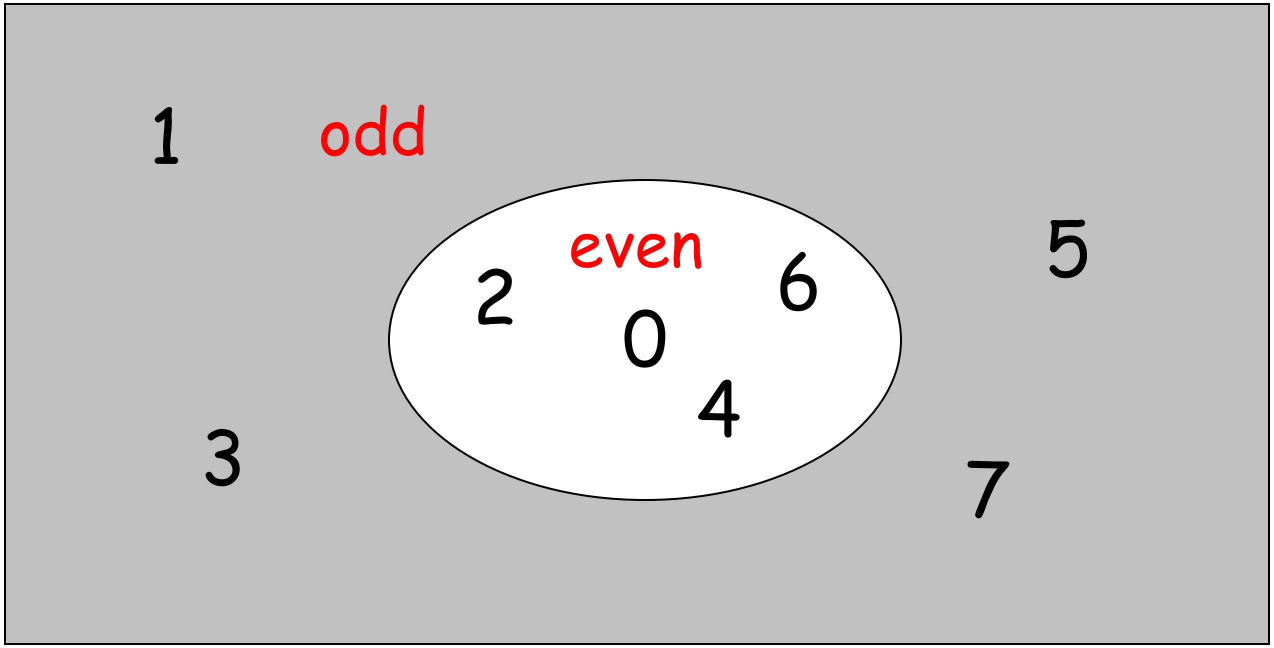
$A = \{ 1, 2, 3 \} \Rightarrow \overline{A} = \{ 4, 5, 6, 7\}$



$\overline{\overline{A}} = A$

$$\overline{\{\text{ even integers }\}} = \{\text{ odd integers }\}$$

Integers



DeMorgan's Laws

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

Empty, Null Set: $\emptyset$

$\emptyset = \{ \}$

$S \cup \emptyset = S$

$S \cap \emptyset = \emptyset$

$\overline{\emptyset}$ = Universal Set

$S - \emptyset = S$

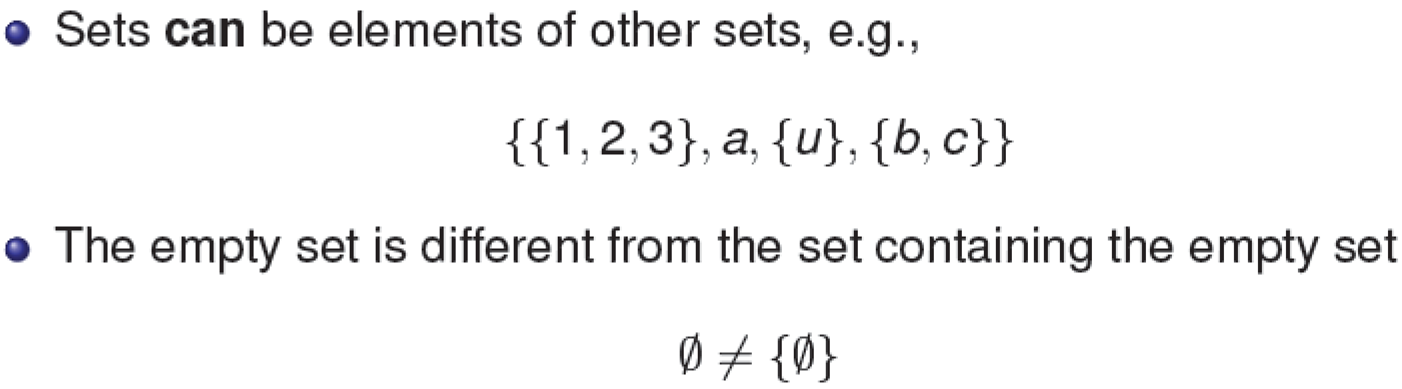
$\emptyset - S = \emptyset$

Singleton set

A **singleton**, also known as a **unit set**, is a set with exactly one element.

For example, the set {0} is a singleton.

To Remember



- Sets **can** be elements of other sets, e.g.,

$$\{\{1,2,3\}, a, \{u\}, \{b,c\}\}$$

- The empty set is different from the set containing the empty set

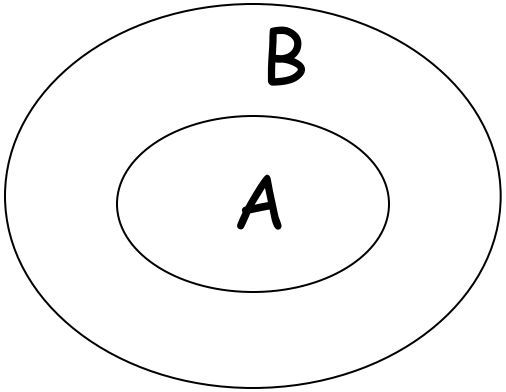
$$\emptyset \neq \{\emptyset\}$$

Subset

$A = \{1, 2, 3\}$ $B = \{1, 2, 3, 4, 5\}$

$A \subseteq B$

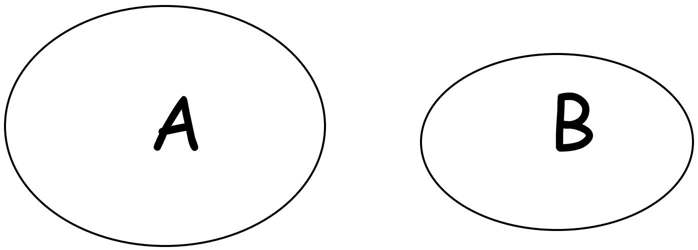
Proper Subset: $A \subset B$



Disjoint Sets

$A = \{ 1, 2, 3 \}$ $B = \{ 5, 6 \}$

$A \cap B = \emptyset$



Set Cardinality

- For finite sets

$A = \{ 2, 5, 7 \}$

$|A| = 3$

(set size)

Powersets

A powerset is a set of sets

$S = \{ a, b, c \}$

Powerset of S = the set of all the subsets of S

$2^S = \{ \emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\} \}$

Observation: $| 2^S | = 2^{|S|}$ $(8 = 2^3)$

Cartesian Product

$A = \{ 2, 4 \}$ $B = \{ 2, 3, 5 \}$

$A \times B = \{ (2, 2), (2, 3), (2, 5), (4, 2), (4, 3), (4, 5) \}$

$|A \times B| = |A| \; |B|$

Generalizes to more than two sets

$A \times B \times \ldots \times Z$

Sequences and Tuples

A *sequence* is a list of objects in some order. For example, sequences of the students' names in alphabetic order such as *(Alice,Bob)*. In contrast to sets, repetitions and order matter in sequences. The sequences $(7, 21, 57)$ and $(7, 7, 21, 57)$ are not equal.

Finite sequences are called *tuples*. In particular, a sequence with k elements is called k-tuple (as well as *pair*, *triple*, *quadriple*, etc.)

All k-tuples $(x_1, x_2, \ldots, x_k)$, where x_i is taken from the set A_i, form a set $A_1 \times A_2 \times \cdots \times A_k$, called the *Cartesian product* or *cross product* of the sets $A_1, A_2, \ldots, A_k$. For example, if $A_1 = \{p, q\}$ and $A_2 = \{1, 2, 3\}$ then

$$A_1 \times A_2 = \{(p, 1), (p, 2), (p, 3), (q, 1), (q, 2), (q, 3)\}.$$

	1	2	3
p	(p,1)	(p,2)	(p,3)
q	(q,1)	(q,2)	(q,3)

Relations

Definition

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

Example: Database R contains tuples (Street name, House number, currently inhabited flag), i.e., $R \subseteq \mathit{Strings} \times \mathbb{N} \times \mathbb{B}$. So R is a 3-ary relation.

Definition

Given sets A and B, $R \subseteq A \times B$ is a binary relation from A to B.

The property $(x, y) \in R$ is also written as xRy.
Example: $R \subseteq \mathbb{R} \times \mathbb{Z}$ where $(x, y) \in R$ iff $y = \lfloor x \rfloor$ (rounding down).

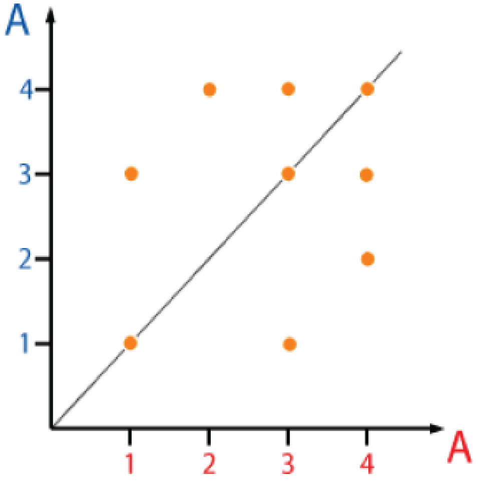
Definition

$R \subseteq A \times A$ is called a relation on A.

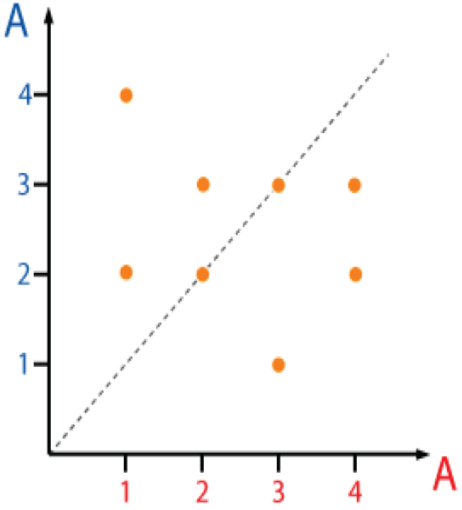
Example: $\leq \subseteq \mathbb{Z} \times \mathbb{Z}$ is the ‘less or equal’ relation on the integers.

Relations

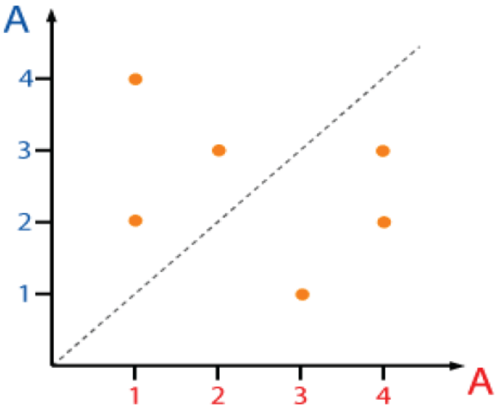
A symmetric relation on the set $A = \{1,2,3,4\}$



An antisymmetric relation on the set $A = \{1,2,3,4\}$



An asymmetric relation on the set $A = \{1,2,3,4\}$



Equivalence Relations

- Reflexive: $x \, R \, x$
- Symmetric: $x \, R \, y \Rightarrow y \, R \, x$
- Transitive: $x \, R \, y$ and $y \, R \, z \Rightarrow x \, R \, z$

Example: R = '='

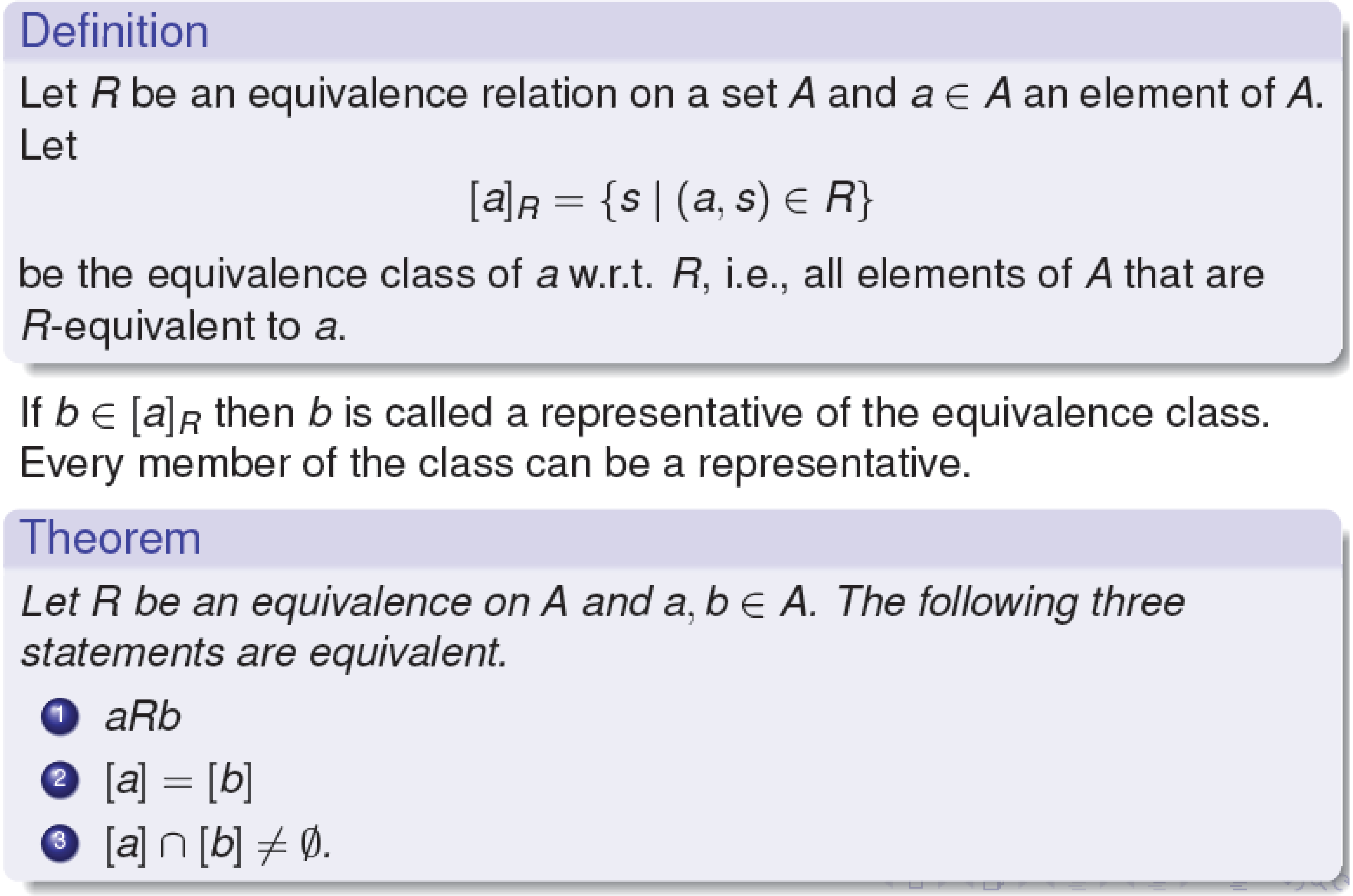
- $x = x$
- $x = y \Rightarrow y = x$
- $x = y$ and $y = z \Rightarrow x = z$

Equivalence Relation

Q: What other equivalence relations you know?

Q: Is the *less or equal* relation ($\leq$) an equivalence relation?

Equivalence Classes



Definition

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

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

be the equivalence class of a w.r.t. R, i.e., all elements of A that are R-equivalent to a.

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

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

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

Equivalence Classes

For equivalence relation R

equivalence class of $x = \{y : x \mathrel{R} y\}$

Example:

$$R = \{ (1, 1), (2, 2), (1, 2), (2, 1), (3, 3), (4, 4), (3, 4), (4, 3) \}$$

Equivalence class of $1 = \{1, 2\}$

Equivalence class of $3 = \{3, 4\}$

Partial Order

Definition

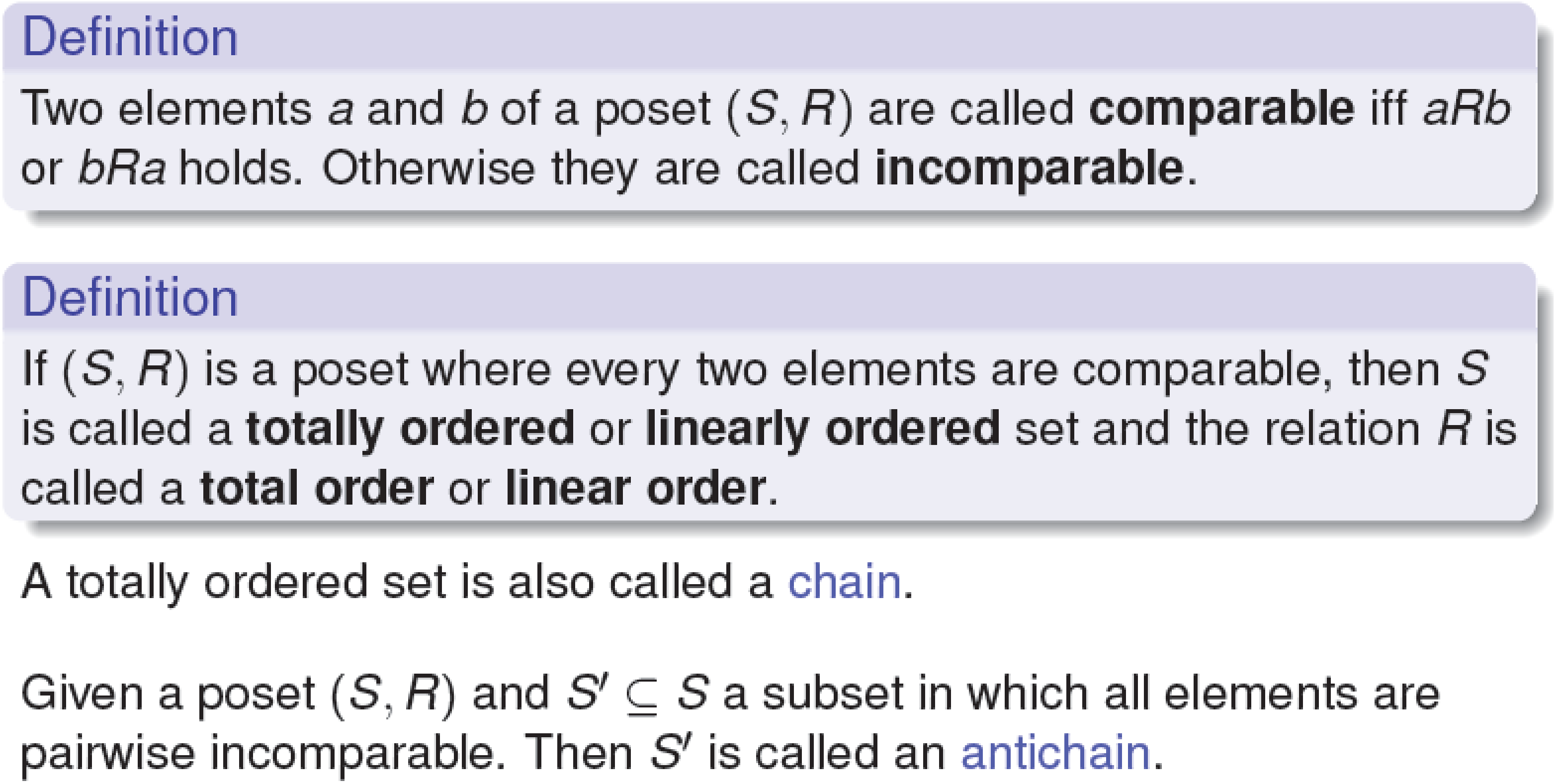
A relation R on a set A is called a **partial order** iff it is reflexive, antisymmetric and transitive.
If R is a partial order, we call (A, R) a partially ordered set, or poset.

Example: $\leq$ is a partial order, but $<$ is not (since it is not reflexive).

Example: Let $a|b$ denote the fact that a divides b. Formally: $\exists k \in \mathbb{Z}\ ak = b$. Show that the relation $|$ is a partial order, i.e., $(\mathbb{Z}^{+}, |)$ is a poset.

Example: Set inclusion $\subseteq$ is partial order, i.e., $(2^{A}, \subseteq)$ is a poset.

Comparable and Total Order



Definition

Two elements a and b of a poset (S, R) are called **comparable** iff aRb or bRa holds. Otherwise they are called **incomparable**.

Definition

If (S, R) is a poset where every two elements are comparable, then S is called a **totally ordered** or **linearly ordered** set and the relation R is called a **total order** or **linear order**.

A totally ordered set is also called a chain.

Given a poset (S, R) and $S' \subseteq S$ a subset in which all elements are pairwise incomparable. Then S' is called an antichain.

Functions as Relations

Definition

Let A, B be nonempty sets. A relation $f \subseteq A \times B$ is called a **partial function** from A to B iff it satisfies the function condition

$$(a, b) \in f \wedge (a, c) \in f \;\rightarrow\; b = c$$

I.e., f assigns every element $a \in A$ at most one element in B.
Partial functions from A to B are denoted as $f : A \rightarrow B$, and we write $f(a) = b$ instead of $(a, b) \in f$.
Functions are also called mappings or transformations.

Definition

A partial function $f : A \rightarrow B$ is called a **total function** iff every element in A is assigned an element in B, i.e., $\forall a \in A \exists b \in B \, (a, b) \in f$.

Terminology about Functions

Let $f : A \to B$ be a function from A to B.

- We say that f maps A to B.
- A is called the domain of f.
- B is called the codomain of f.
- If $f(a) = b$ then b is the image of a under f and a is the preimage of b.
- $f(A) := \{b \in B \mid \exists a \in A\, f(a) = b\}$ is called the range of f. (Note the difference between the range and the codomain.)
- Two functions $f : A \to B$ and $g : A' \to B'$ are equal iff $A = A'$, $B = B'$ and $\forall a \in A\, f(a) = g(a)$.

Types of Functions

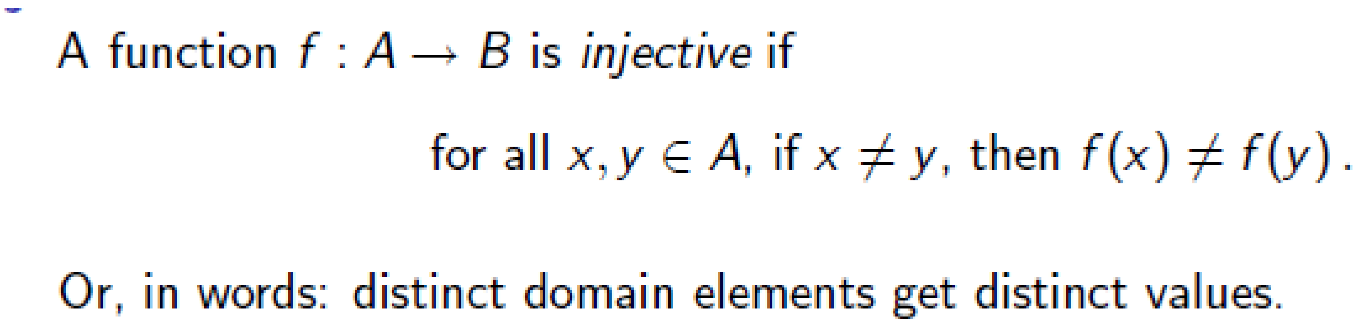
A function $f : A_1 \times A_2 \times \cdots \times A_k \longrightarrow B$ is called a k-ary function. *Unary functions* correspond to the case $k = 1$, while *binary functions* correspond to the case $k = 2$.

A function $f : A \longrightarrow \{\text{TRUE}, \text{FALSE}\}$ is called a *predicate* or *property*. For example, the property *even* defines evenness of a given integer: even(4) $= \text{TRUE}$ and even(5) $= \text{FALSE}$.

A property $f : A \times A \times \cdots \times A \longrightarrow \{\text{TRUE}, \text{FALSE}\}$, whose domain is the set of k-tuples, is called k*-ary relation* (on A). An example of a binary relation is the *beats* relation between scissors, paper, and stone (see p.9 in Sipser).

For binary relation R, we often use *infix notation* writing xRy instead of $R(x, y) = \text{TRUE}$.

Injective Functions

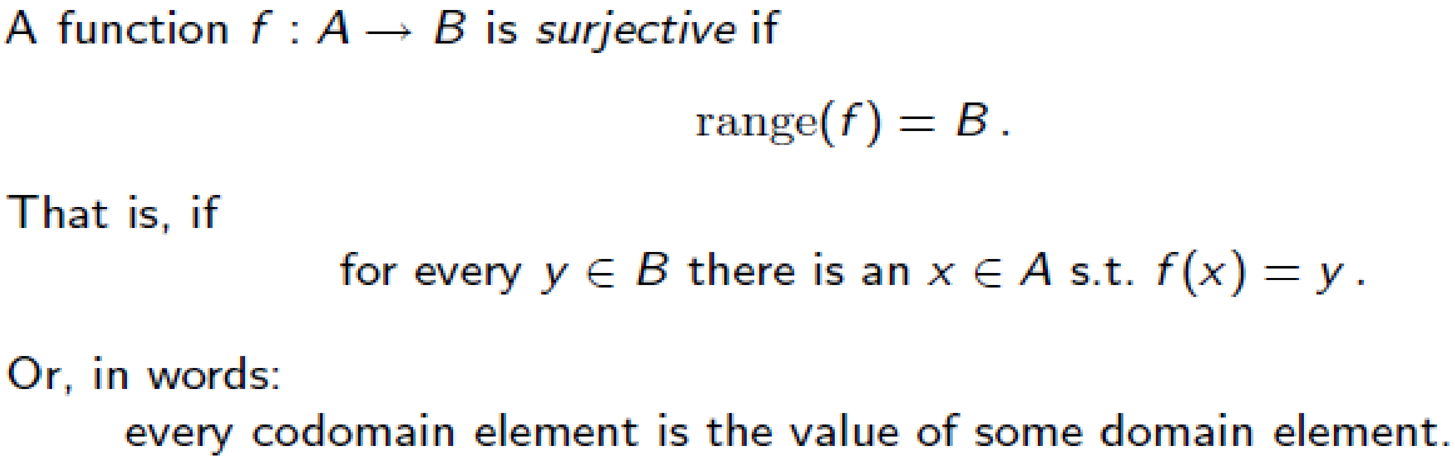


A function $f : A \to B$ is *injective* if

$$\text{for all } x, y \in A, \text{ if } x \neq y, \text{ then } f(x) \neq f(y) .$$

Or, in words: distinct domain elements get distinct values.

Surjective Functions



A function $f : A \to B$ is *surjective* if

$$\mathrm{range}(f) = B\,.$$

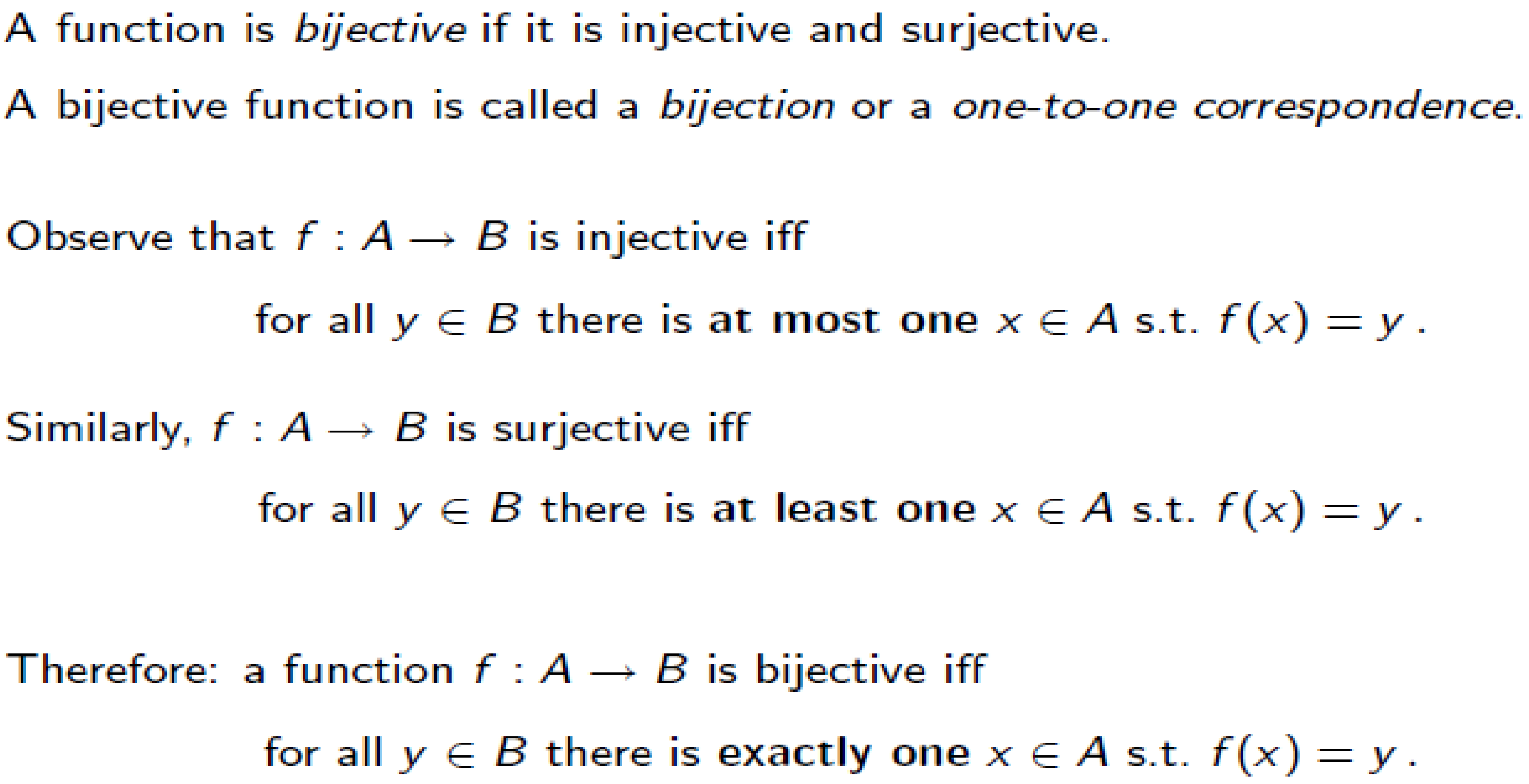
That is, if

for every $y \in B$ there is an $x \in A$ s.t. $f(x) = y$.

Or, in words:

every codomain element is the value of some domain element.

Bijective Function



A function is *bijective* if it is injective and surjective.

A bijective function is called a *bijection* or a *one-to-one correspondence*.

Observe that $f : A \longrightarrow B$ is injective iff

for all $y \in B$ there is **at most one** $x \in A$ s.t. $f(x) = y$.

Similarly, $f : A \longrightarrow B$ is surjective iff

for all $y \in B$ there is **at least one** $x \in A$ s.t. $f(x) = y$.

Therefore: a function $f : A \longrightarrow B$ is bijective iff

for all $y \in B$ there is **exactly one** $x \in A$ s.t. $f(x) = y$.

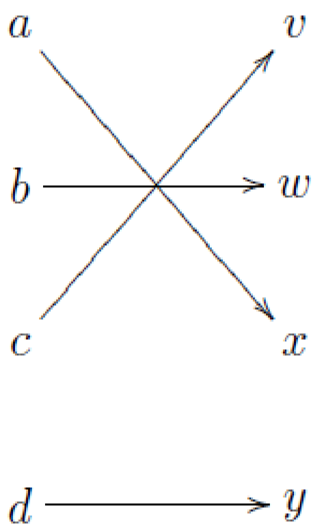
Example 2.2.3. *$f\colon A \to B$ where $A = \{a, b, c, d\}$ and $B = \{v, w, x, y, z\}$ defined by the relation below is an injection, but not a surjection.*

$$\begin{tikzcd}
a \arrow[r] & v \\
b \arrow[r] & w \\
c \arrow[dr] & x \\
d \arrow[dr] & y \\
 & z
\end{tikzcd}$$

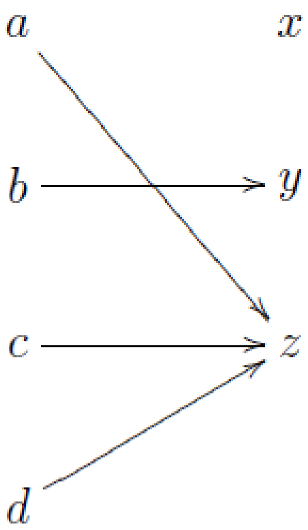
Example 2.2.2. *$f\colon A \to B$ where $A = \{a, b, c, d\}$ and $B = \{x, y, z\}$ defined by the relation below is a surjection, but not an injection.*

$$\begin{tikzcd}
a \arrow[r] & x \\
b \arrow[r] & y \\
c \arrow[r] & z \\
d \arrow[ur] &
\end{tikzcd}$$

Example 2.2.4. *$f\colon A \to B$ where $A = \{a, b, c, d\}$ and $B = \{v, w, x, y\}$ defined by the relation below both a surjection and an injection, and therefore a bijection. Notice that for a function to be a bijection, the domain and codomain must have the same cardinality.*



Example 2.2.1. *Let* $A = \{a, b, c, d\}$ *and* $B = \{x, y, z\}$. *The function* f *is defined by the relation pictured below. This function is neither injective nor surjective.*



Definition

A function $f : A \to B$ is **injective** (“one-to-one”) iff $f(a) = f(b) \to a = b$. Then f is called an **injection**.

Definition

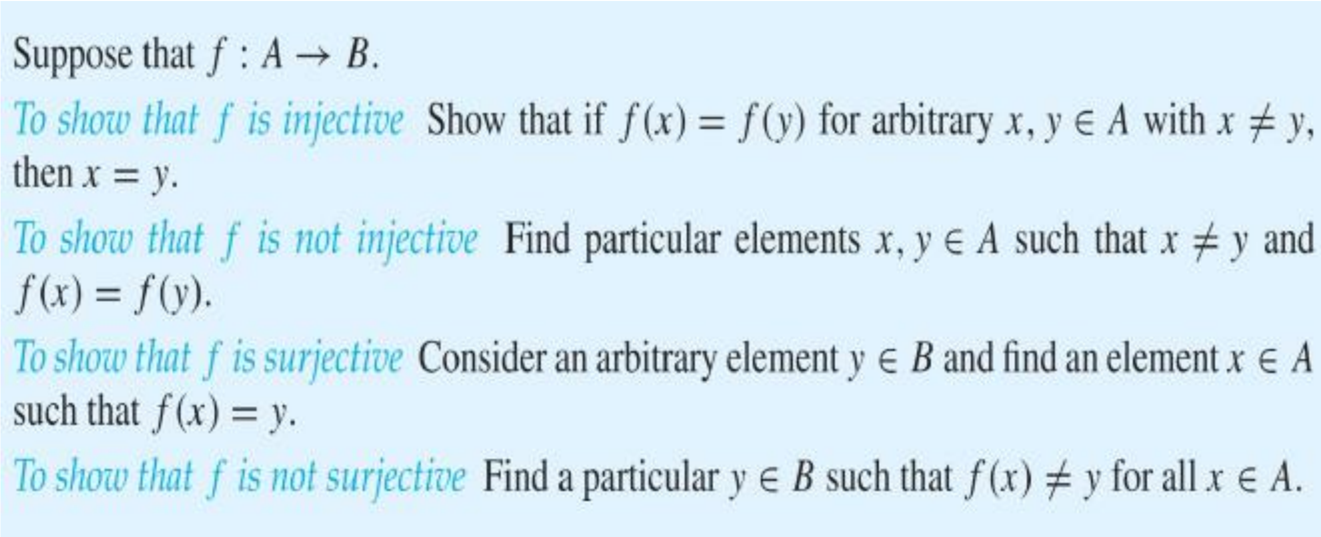
A function $f : A \to B$ is **surjective** (“onto”) iff $\forall b \in B \, \exists a \in A \; f(a) = b$. Then f is called a **surjection**.

A function $f : A \to B$ is surjective iff $f(A) = B$, i.e., the range is equal to the codomain.

Definition

A function $f : A \to B$ is **bijective** iff it is injective and surjective. Then f is called a **bijection** or **one-to-one correspondence**.

Reasoning about injection/surjection



Suppose that $f : A \to B$.

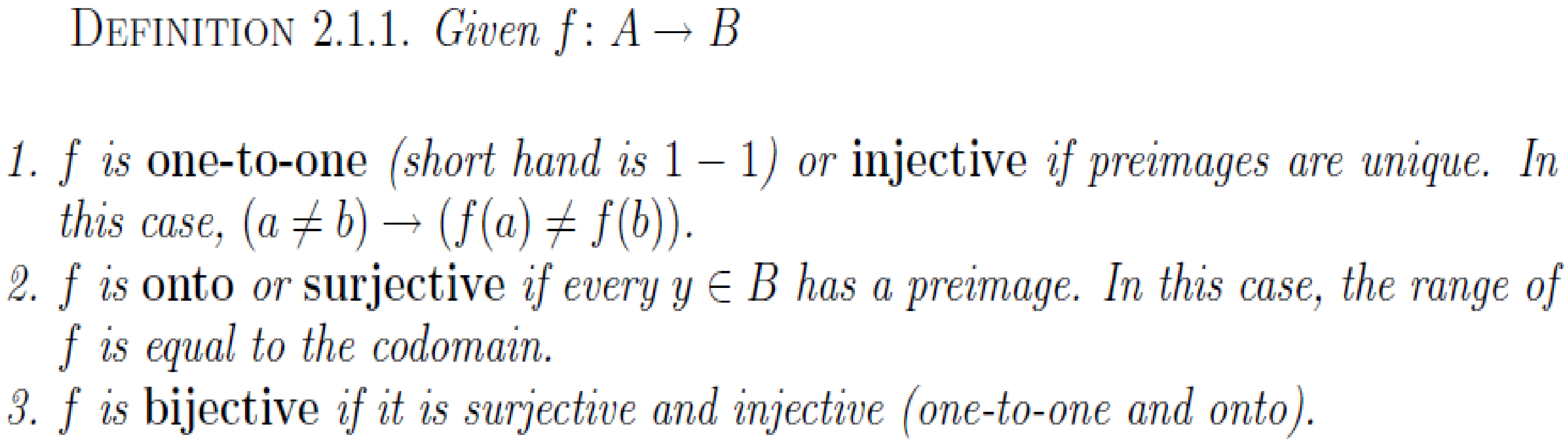
To show that f is injective Show that if $f(x) = f(y)$ for arbitrary $x, y \in A$ with $x \neq y$, then $x = y$.

To show that f is not injective Find particular elements $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$.

To show that f is surjective Consider an arbitrary element $y \in B$ and find an element $x \in A$ such that $f(x) = y$.

To show that f is not surjective Find a particular $y \in B$ such that $f(x) \neq y$ for all $x \in A$.

Properties of Functions



Definition 2.1.1. *Given $f\colon A \to B$*

1. *f is* **one-to-one** *(short hand is $1-1$) or* **injective** *if preimages are unique. In this case, $(a \neq b) \to (f(a) \neq f(b))$.*
2. *f is* **onto** *or* **surjective** *if every $y \in B$ has a preimage. In this case, the range of f is equal to the codomain.*
3. *f is* **bijective** *if it is surjective and injective (one-to-one and onto).*

Function Composition

For $g : A \longrightarrow B$ and $f : C \longrightarrow D$, with $B \subset C$, we define the *composition* of f and g, denoted $f \circ g$, as the function from $A \longrightarrow D$ s.t.

$$(f \circ g)(x) = f(g(x)) \, .$$

For example, if f and g are functions of type $\mathcal{N} \longrightarrow \mathcal{N}$ s.t.

$$f(x) = x + 1 \quad \text{and} \quad g(x) = 2^x$$

then $f \circ g$ is the function of type $\mathcal{N} \longrightarrow \mathcal{N}$ s.t.

$$(f \circ g)(x) = 2^x + 1$$

and $g \circ f$ is the function of type $\mathcal{N} \longrightarrow \mathcal{N}$ s.t.

$$(g \circ f)(x) = 2^{x+1} \, .$$

Notice that for all bijections $f : A \longrightarrow B$,

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

for all $x \in A$, and

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

for all $y \in B$.

That is to say,

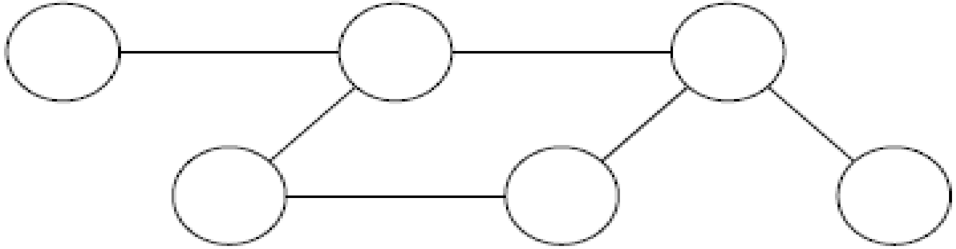
$$f^{-1} \circ f = \{ (x, x) \mid x \in A \}$$

and

$$f \circ f^{-1} = \{ (y, y) \mid y \in B \} .$$

Undirected Graphs

An (undirected) *graph* is a pair (V, E) where V is a set of objects called *nodes* or *vertices*, and E is a set of 2-element subsets of V, called *edges*.
Graphs have convenient graphical representation: vertices are drawn as dots on a plane, while edges are drawn as lines connecting corresponding pairs of vertices, e.g.:

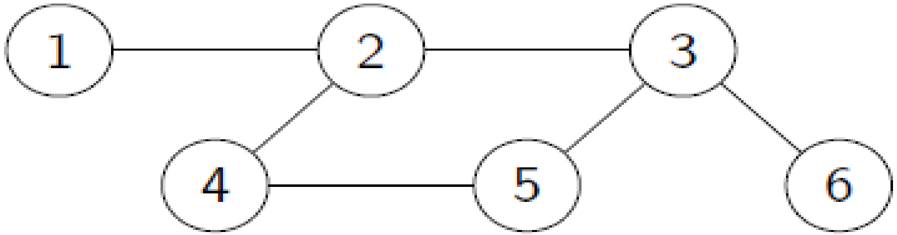


In *unlabeled graph*, the vertices have no labels and can be distinguished only from the perspective of edges.

Q: Which vertices in this graph are indistinguishable?

Undirected Graphs

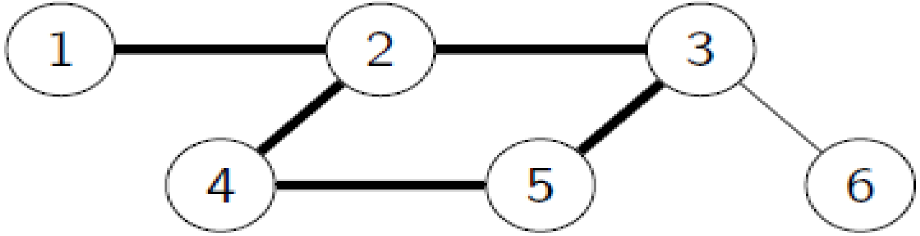
An (undirected) *graph* is a pair (V, E) where V is a set of objects, called *nodes* or *vertices*, and E is a set of 2-element subsets of V, called *edges*.



In *labeled graph* $G = (V, E)$ the vertices are labeled (usually with elements of V). In particular, for this the shown graph, we have:
$V = \{1, 2, 3, 4, 5, 6\}$
$E = \{(1, 2), (2, 4), (2, 3), (3, 5), (4, 5), (3, 6)\}$
(by convention, we write $(1, 2)$ instead of $\{1, 2\}$ and assume that $(1, 2) = (2, 1)$ is the same edge)
Two vertices are *adjacent* if they are connected by an edge (e.g., vertices 3 and 5). A vertex and an edge are *incident* if the vertex represents an endpoint of the edge.

Undirected Graphs

An (undirected) *graph* is a pair (V, E) where V is a set of objects, called *nodes* or *vertices*, and E is a set of 2-element subsets of V, called *edges*.

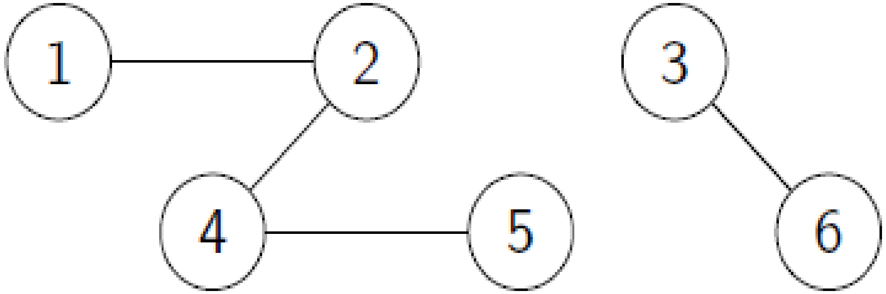


A *path* in a graph is a sequence of vertices, where every two consecutive vertices are adjacent (e.g., vertices $(1, 2, 4, 5, 3, 2)$ form a path). A graph is *connected* if there is a path between any two vertices; and *disconnected* otherwise.

A *cycle* is a path where starting and ending vertices coincide and viewed as a single vertex (so that a cycle has neither starting nor ending vertex). A path/cycle is called *simple* if it does not repeat any vertices.

Undirected Graphs

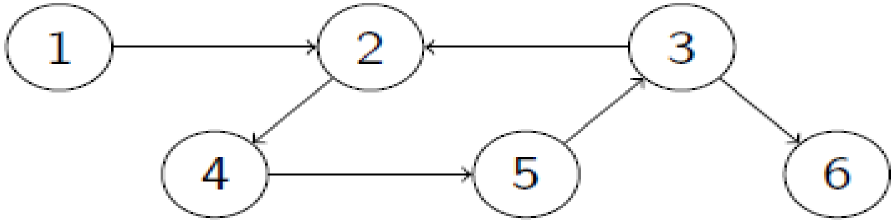
An (undirected) *graph* is a pair (V, E) where V is a set of objects, called *nodes* or *vertices*, and E is a set of 2-element subsets of V, called *edges*.



A graph having no cycles is called *acyclic graph* (or *forest*). An acyclic graph consists of one or more connected components, called *trees*. In other words, a tree is a connected graph without cycles.

Directed Graphs

A *directed graph* (*digraph*) is a pair (V, E) where V is a set of objects, called *nodes* or *vertices*, and E is a set of pairs of elements of V, called *directed edges* or *arcs*.



Differences from undirected graph:

- Vertices have incoming degree (*indegree*) as well as outgoing degree (*outdegree*).
- Paths are directed; a directed path comes into a vertex through an incoming edge and leaves it through outgoing edge.
- In a *strongly connected* (component of) graph, there is a directed path connecting any vertex with any other vertex.

Q: Find strongly connected component in the shown graph.

Boolean Operation

Boolean values are TRUE $= 1$ and FALSE $= 0$.

Boolean operations: *conjunction* (AND, $\wedge$), *disjunction* (OR, $\vee$), *exclusive or* (XOR, addition modulo 2, $\oplus$), *equality* (equivalence, iff, "if and only if", $\leftrightarrow$)

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

$\oplus$	0	1
0	0	1
1	1	0

$\leftrightarrow$	0	1
0	1	0
1	0	1

Other Boolean operations: *negation* (NOT, $\neg$), *implication* $\rightarrow$
Q: In what respect negation and implication differ from the operations mentioned above?

$\neg 0 = 1$, $\neg 1 = 0$;
$0 \rightarrow 0 = 1$, $0 \rightarrow 1 = 1$, (FALSEimplies whatever!)
$1 \rightarrow 0 = 0$, $1 \rightarrow 1 = 1$, (TRUEcan imply only TRUE).

Arguments of boolean operations are called *operands*.

Boolean Operations

Both $\{\wedge, \neg\}$ and $\{\vee, \neg\}$ are complete set of Boolean operations, i.e., *any* binary Boolean operations can be expressed in terms of the elements of either of these sets.

Boolean operations $\wedge$ and $\vee$ satisfy the *distributive law* similarly for arithmetic operations $\times$ and $+$:

- For any three numbers a, b, c, we have

$$a \times (b + c) = (a \times b) + (a \times c)$$

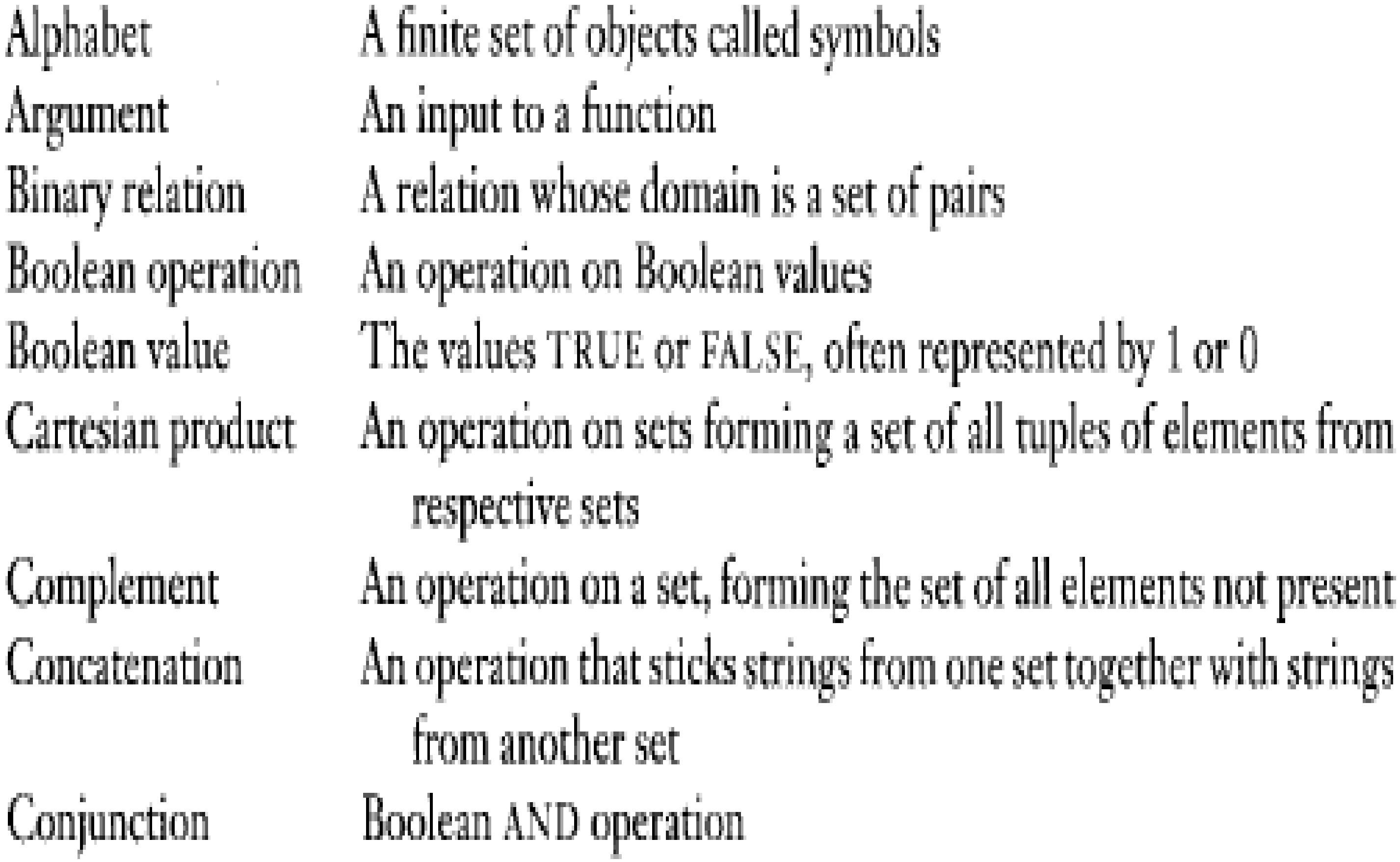
- Similarly, for any three Boolean values P, Q, R, we have

$$P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$$

as well as

$$P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R).$$

Various operations on sets

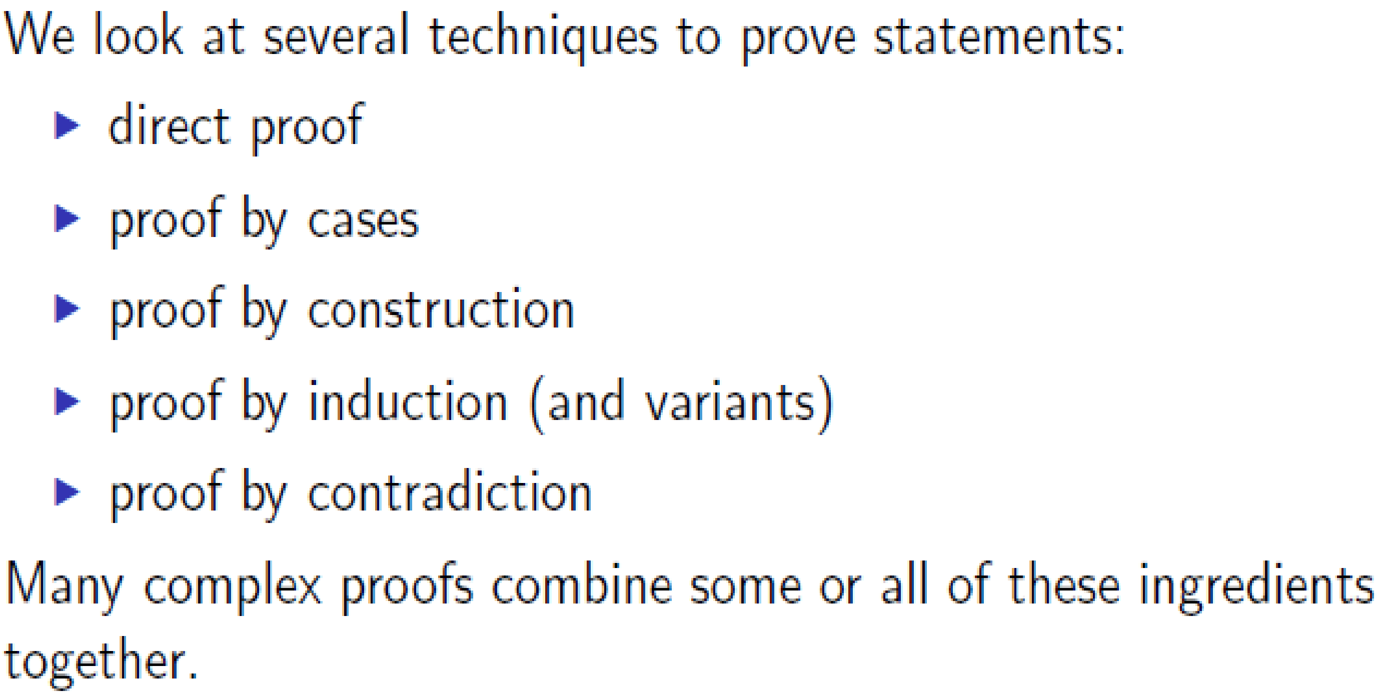


Alphabet	A finite set of objects called symbols
Argument	An input to a function
Binary relation	A relation whose domain is a set of pairs
Boolean operation	An operation on Boolean values
Boolean value	The values TRUE or FALSE, often represented by 1 or 0
Cartesian product	An operation on sets forming a set of all tuples of elements from respective sets
Complement	An operation on a set, forming the set of all elements not present
Concatenation	An operation that sticks strings from one set together with strings from another set
Conjunction	Boolean AND operation

Connected graph	A graph with paths connecting every two nodes
Cycle	A path that starts and ends in the same node
Directed graph	A collection of points and arrows connecting some pairs of points
Disjunction	Boolean OR operation
Domain	The set of possible inputs to a function
Edge	A line in a graph
Element	An object in a set
Empty set	The set with no members
Empty string	The string of length zero
Equivalence relation	A binary relation that is reflexive, symmetric, and transitive
Function	An operation that translates inputs into outputs
Graph	A collection of points and lines connecting some pairs of points
Intersection	An operation on sets forming the set of common elements
k-tuple	A list of *k* objects

Language	A set of strings
Member	An object in a set
Node	A point in a graph
Pair	A list of two elements, also called a 2-tuple
Path	A sequence of nodes in a graph connected by edges
Predicate	A function whose range is {TRUE, FALSE}
Property	A predicate
Range	The set from which outputs of a function are drawn
Relation	A predicate, most typically when the domain is a set of k-tuples
Sequence	A list of objects
Set	A group of objects
Simple path	A path without repetition
String	A finite list of symbols from an alphabet
Symbol	A member of an alphabet
Tree	A connected graph without simple cycles
Union	An operation on sets combining all elements into a single set
Vertex	A point in a graph

Methods of proof



We look at several techniques to prove statements:

- direct proof
- proof by cases
- proof by construction
- proof by induction (and variants)
- proof by contradiction

Many complex proofs combine some or all of these ingredients together.

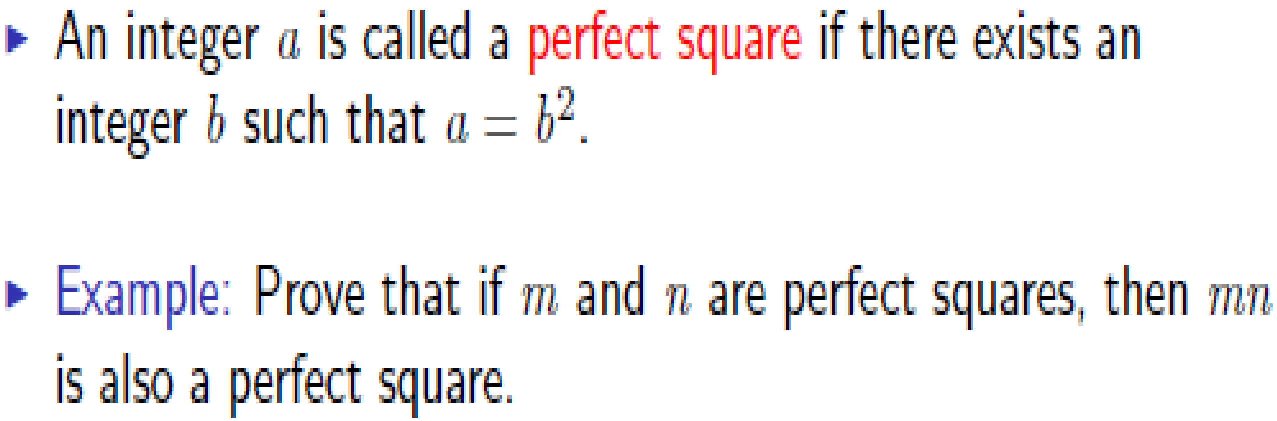
Direct Proof

- Direct proof: $p \to q$ proved by directly showing that if p is true, then q must follow

---

- To prove $p \to q$ in a direct proof, first assume p is true.
- Then use rules of inference, axioms, previously shown theorems/lemmas to show that q is also true
- Example: If n is an odd integer, than n^2 is also odd.
- Proof: Assume n is odd. By definition of oddness, there must exist some integer k such that $n = 2k + 1$. Then, $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd. Thus, if n is odd, n^2 is also odd. □
- Observe: This proof implicitly uses universal generalization and existential instantiation (where?)

Direct Proof: another example



- An integer a is called a perfect square if there exists an integer b such that $a = b^2$.
- Example: Prove that if m and n are perfect squares, then mn is also a perfect square.

Direct Proofs: example

Theorem

For any integer x, if $x \geq 4$, then $2^x \geq x^2$.

Proof.

Notice that $2^4 = 16 = 4^2$, so the statement is true for $x = 4$.
Now consider the sequences of values on the left-hand side and on the right-hand side:

$$2^4, 2^5, 2^6, \ldots \qquad \text{and} \qquad 4^2, 5^2, 6^2, \ldots$$

Taking the ratio of adjacent terms in each sequence, we see that

$$\frac{2^{x+1}}{2^x} = \frac{2^1}{2^0} = 2,$$

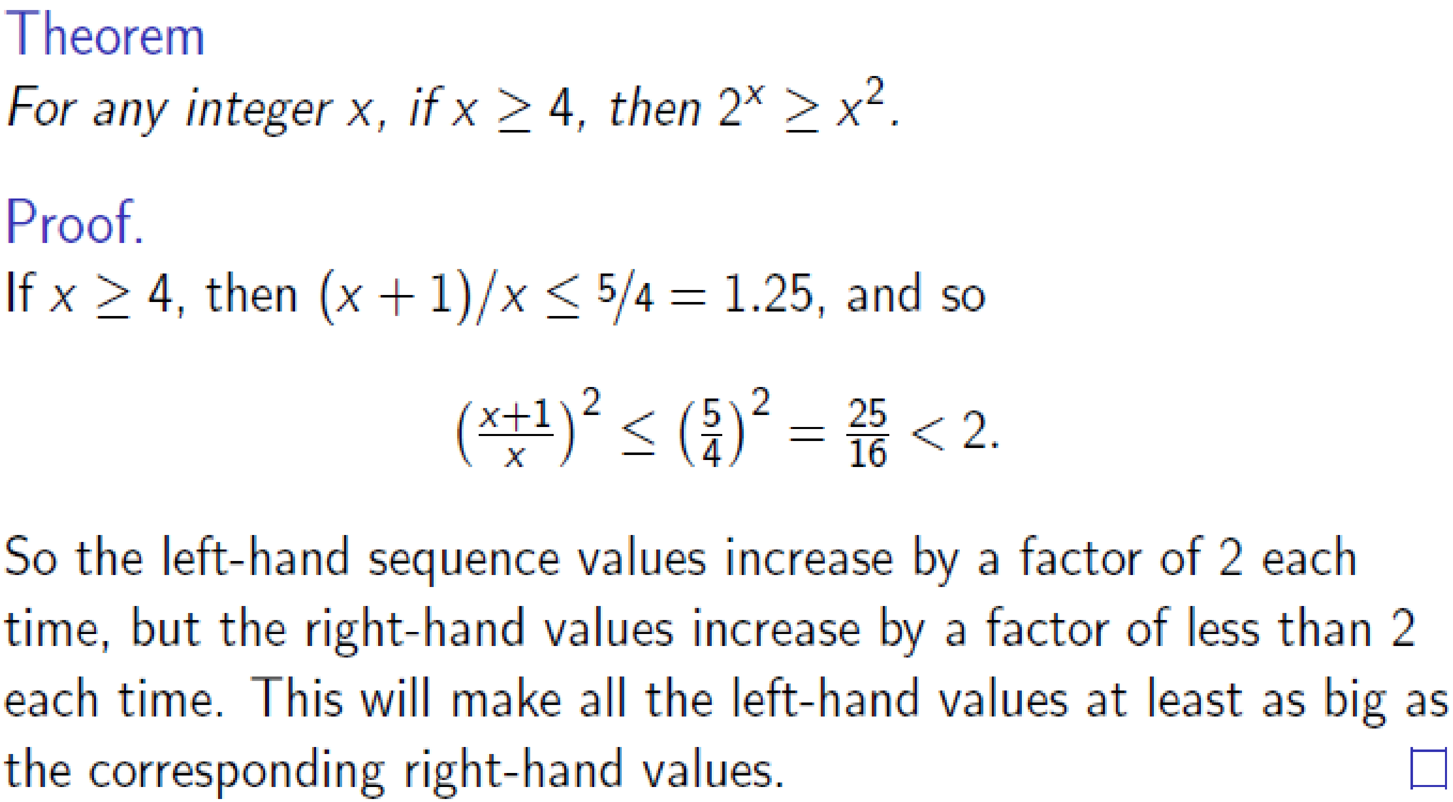
and

$$\frac{(x+1)^2}{x^2} = \left(\frac{x+1}{x}\right)^2.$$

...

$\sqcap$

Direct Proofs: example



Theorem

For any integer x, if $x \geq 4$, then $2^x \geq x^2$.

Proof.

If $x \geq 4$, then $(x+1)/x \leq {}^5/_4 = 1.25$, and so

$$\left(\frac{x+1}{x}\right)^2 \leq \left(\frac{5}{4}\right)^2 = \frac{25}{16} < 2.$$

So the left-hand sequence values increase by a factor of 2 each time, but the right-hand values increase by a factor of less than 2 each time. This will make all the left-hand values at least as big as the corresponding right-hand values. □

Direct Proofs: features

- We start by assuming the hypothesis, infer some new statements based on the hypothesis and using easy and familiar facts about numbers ("high school math"), and eventually reach the conclusion.
- The proof above is not completely formal, because we don't bother proving these facts from high school math (e.g., the fact that $(^a/_b)^2 = ^{a^2}/_{b^2}$ for all real a and b), but that is fine; these facts are so easy and intuitively obvious that proving them would be a tedious waste of time and obscure the key points of the whole proof itself.

Proof by Contraposition

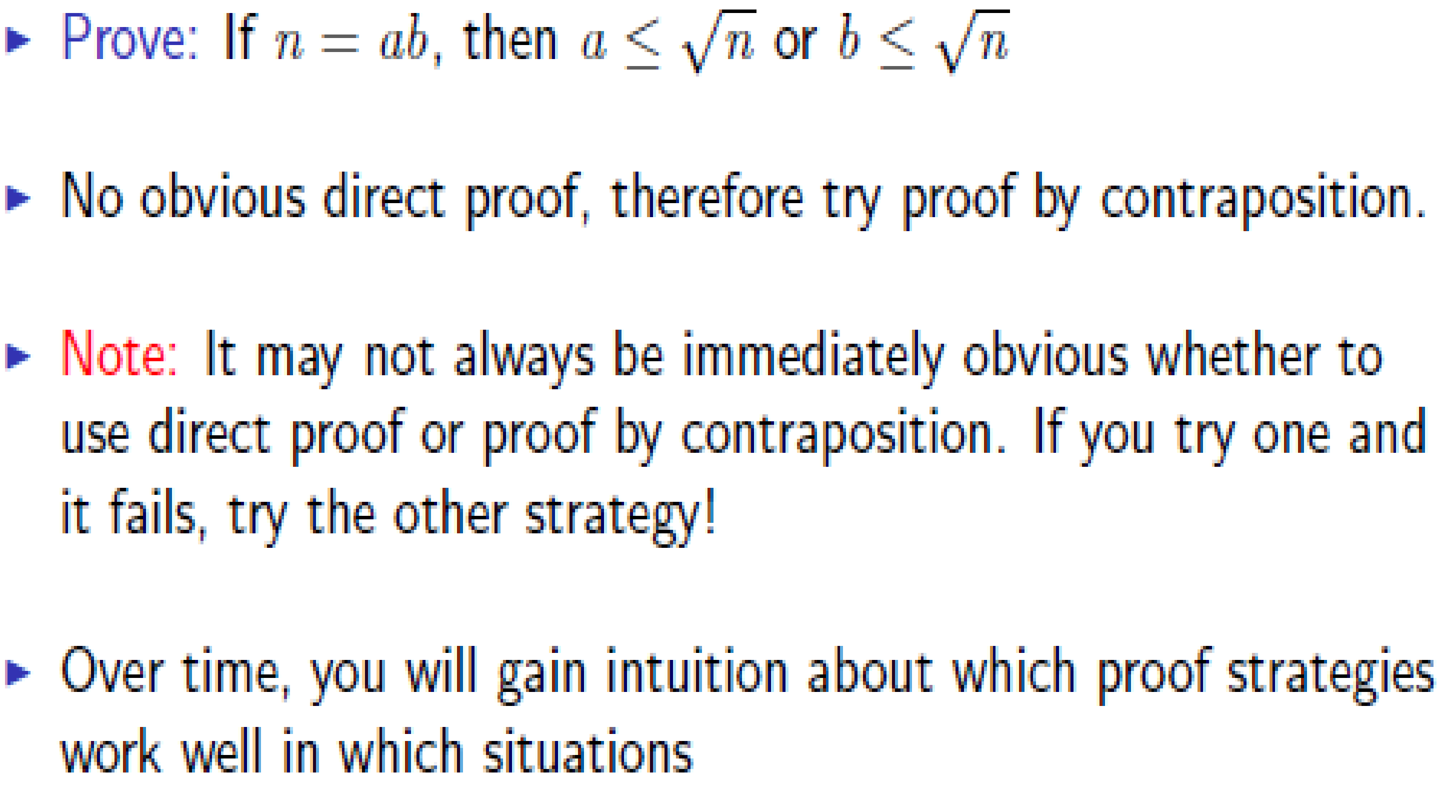
- Proof by contraposition: Prove $p \to q$ by proving $\neg q \to \neg p$

- Recall: The contrapositive of $p \to q$ is $\neg q \to \neg p$
- Recall: A formula and its contrapositive are logically equivalent
- Hence, if you can prove $\neg q \to \neg p$, have shown $p \to q$
- This makes no difference from a logical point of view, but sometimes the contrapositive is easier to show by direct proof than the original
- Thus, in proof by contraposition, assume $\neg q$ and then use axioms, inference rules etc. to show that $\neg p$ must follow

Proof by Contraposition: example

- Prove: If n^2 is odd, then n is odd.
- What is the contrapositive of this statement?
- Proof: Suppose n is even. Then, there exists integer k such that $n = 2k$.
- Then, $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$
- Thus, n^2 is also even. □

Proof by Contraposition: another example



- Prove: If $n = ab$, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$
- No obvious direct proof, therefore try proof by contraposition.
- Note: It may not always be immediately obvious whether to use direct proof or proof by contraposition. If you try one and it fails, try the other strategy!
- Over time, you will gain intuition about which proof strategies work well in which situations

Proof by Cases

- In some cases, it is very difficult to prove a theorem by applying the same argument in all cases
- For example, we might need to consider different arguments for negative and non-negative integers
- Proof by cases allows us to apply different arguments in different cases and combine the results
- Specifically, suppose we want to prove statement p, and we know that we have either q or r
- If we can show $q \to p$ and $r \to p$, then we can conclude p

Proof by Cases

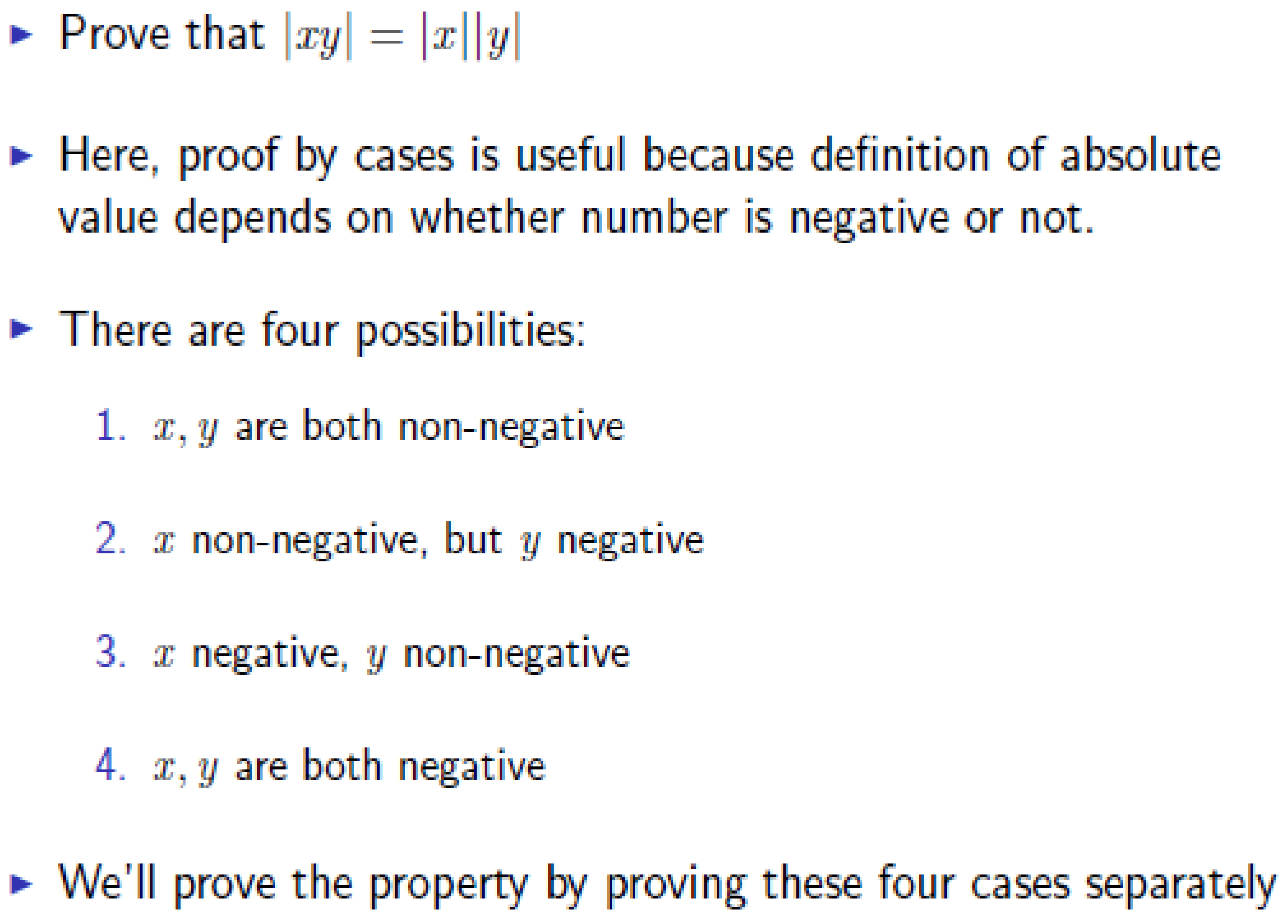
- In general, there may be more than two cases to consider
- Proof by cases says that to show

$$(p_1 \vee p_2 \ldots \vee p_k) \rightarrow q$$

it suffices to show:

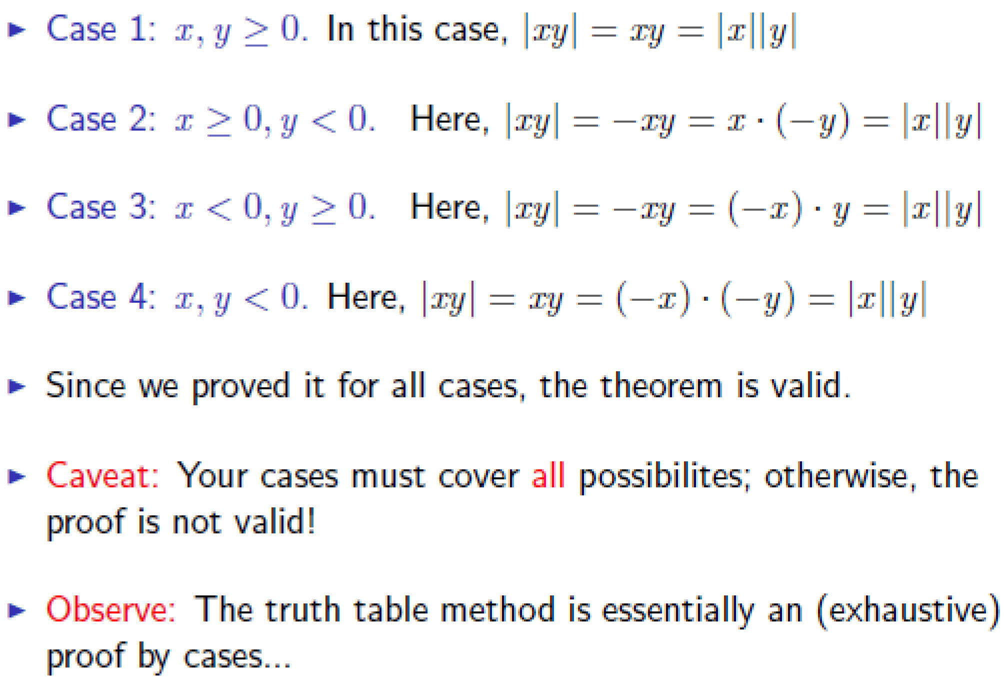
$$\begin{gathered} p_1 \rightarrow q \\ p_2 \rightarrow q \\ \ldots \\ p_k \rightarrow q \end{gathered}$$

Proof by Cases: example 1



- Prove that $|xy| = |x||y|$
- Here, proof by cases is useful because definition of absolute value depends on whether number is negative or not.
- There are four possibilities:
  1. x, y are both non-negative
  2. x non-negative, but y negative
  3. x negative, y non-negative
  4. x, y are both negative
- We'll prove the property by proving these four cases separately

Proof by Cases: example 1



- Case 1: $x, y \geq 0.$ In this case, $|xy| = xy = |x||y|$
- Case 2: $x \geq 0, y < 0.$ Here, $|xy| = -xy = x \cdot (-y) = |x||y|$
- Case 3: $x < 0, y \geq 0.$ Here, $|xy| = -xy = (-x) \cdot y = |x||y|$
- Case 4: $x, y < 0.$ Here, $|xy| = xy = (-x) \cdot (-y) = |x||y|$
- Since we proved it for all cases, the theorem is valid.
- Caveat: Your cases must cover all possibilites; otherwise, the proof is not valid!
- Observe: The truth table method is essentially an (exhaustive) proof by cases...

Proof by Cases: example 2

Theorem

There are (real) irrational numbers $a, b > 0$ such that a^b is rational.

Proof.

Consider $\sqrt{2}$, which is known to be irrational (we shall actually prove this later).

Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational. Then we set $a = b = \sqrt{2}$ and we are done.

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational. Set $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$. Then

$$a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2$$

is rational. So we are done.

In either case, we have found irrational numbers a, b such that a^b is rational. Since one of the two cases must hold, the Theorem must be true. □

Proof by Cases: features

- This proof is *non-constructive*: it does not actually give us two numbers a and b, but merely shows us that they exist. Namely, it gives us two possibilities for the pair of values and asserts that at least one of them is correct, but does not tell us which one.
- Constructive proofs are usually preferable, but there are some theorems in math that have no known constructive proof.

In general, proof by cases works as follows:

- Split the hypothesis into two (or more cases) and prove the conclusion in each case.
- The cases must be *exhaustive*, i.e., it must always be that at least one of the cases holds.

Proof by Construction

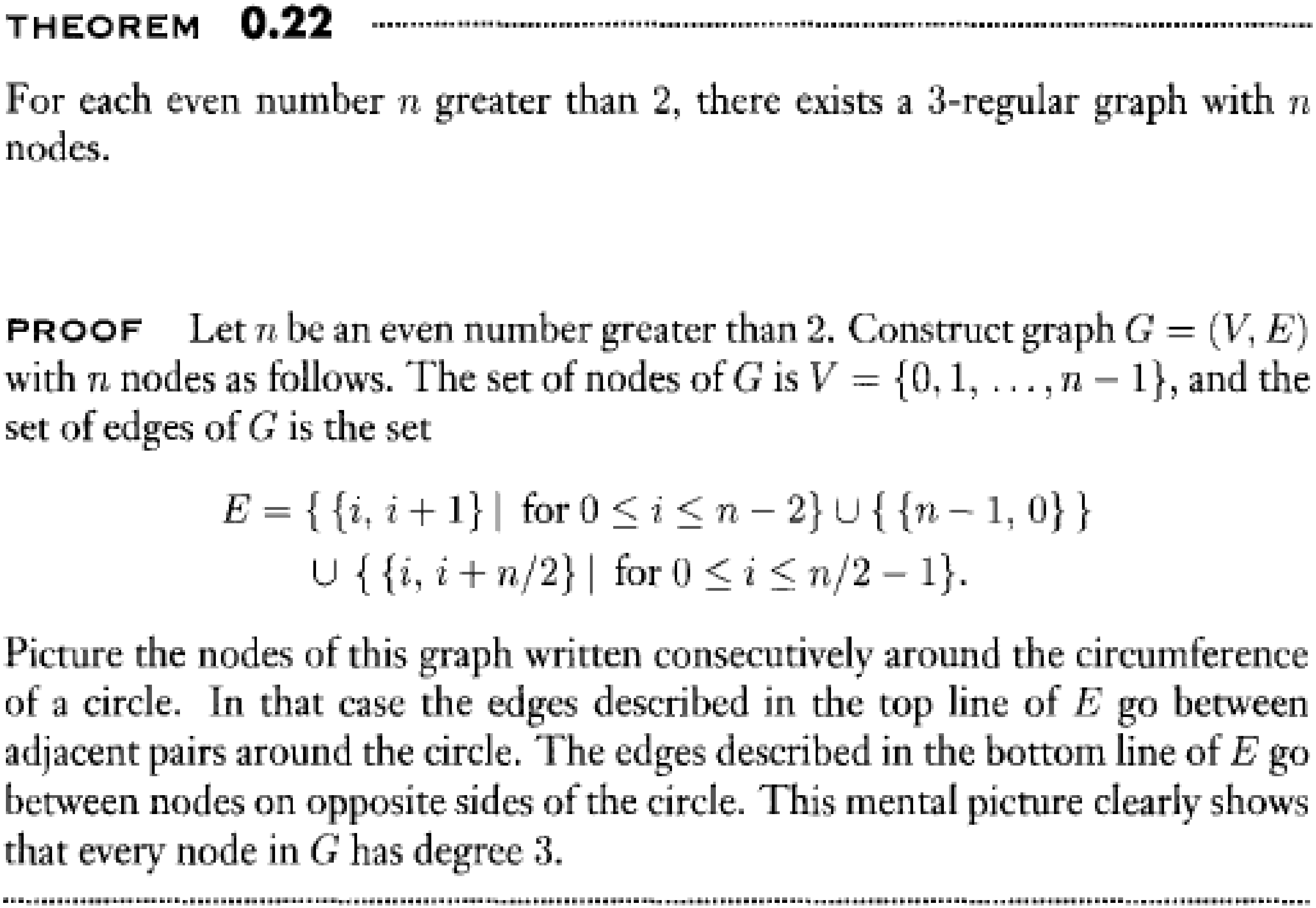
Many theorems state that a particular type of object exists. In proof by construction, we construct an object with the required properties (and prove that it indeed possesses these properties).

Let us prove the following theorem by construction. We define a graph to be k-regular if every node in the graph has degree k.

Theorem

For each even number $n > 2$, there exists a 3-regular graph with n nodes.

Proof by Construction: example



THEOREM 0.22

For each even number n greater than 2, there exists a 3-regular graph with n nodes.

PROOF Let n be an even number greater than 2. Construct graph $G = (V, E)$ with n nodes as follows. The set of nodes of G is $V = \{0, 1, \ldots, n-1\}$, and the set of edges of G is the set

$$\begin{aligned} E = \{\, \{i, i+1\} \mid \text{for } 0 \le i \le n-2\} &\cup \{\, \{n-1, 0\}\,\} \\ \cup \{\, \{i, i+n/2\} \mid \text{for } 0 \le i \le n/2-1\}. \end{aligned}$$

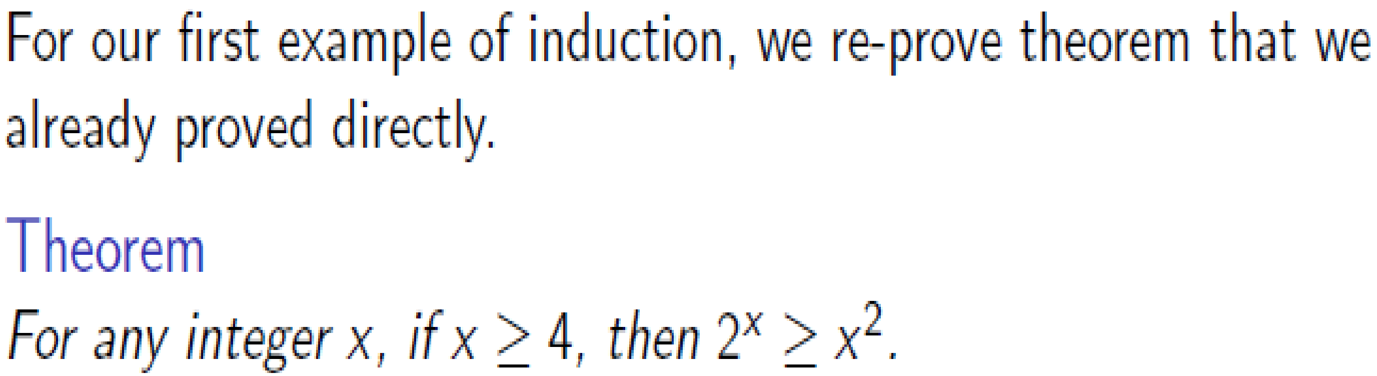
Picture the nodes of this graph written consecutively around the circumference of a circle. In that case the edges described in the top line of E go between adjacent pairs around the circle. The edges described in the bottom line of E go between nodes on opposite sides of the circle. This mental picture clearly shows that every node in G has degree 3.

Proof by Induction

Proof by induction is a method to show that all elemente of an infinite ordered set have a specified property. A proof by induction includes three major steps (illustrated with the set $\mathcal{N}$ and property $\mathbf{P}(x)$ below):

1. **Induction basis:** Direct proof that $\mathbf{P}(1)$ (more generally, $\mathbf{P}(k)$ for all $k \leq m$, i.e., all small elements in the set have the property)
2. **Induction hypothesis:** Assumption that for $i > m$, we have $\mathbf{P}(j)$ for every $j < i$.
3. **Induction step:** Proof that $\mathbf{P}(i)$ using the induction hypothesis.

Proof by Induction: example 1



For our first example of induction, we re-prove theorem that we already proved directly.

Theorem

For any integer x, if $x \geq 4$, then $2^x \geq x^2$.

Proof by Induction: example 1

Theorem

For any integer x, if $x \geq 4$, then $2^x \geq x^2$.

Proof by induction.

Let $P(n)$ be the statement that $2^n \geq n^2$. Our goal is to prove $P(n)$ for all integers $n \geq 4$... Thus we start the induction at $n = 4$ as basis for induction.

Basis: Clearly, $2^4 = 16 = 4^2$, so $P(4)$ is true.

Induction hypothesis: For an integer $n > 4$, assume that $P(n)$ is true, i.e., $2^n \geq n^2$.

Induction step: Here we must show that $P(n)$ implies $P(n+1)$. That is, we want to infer that $2^{n+1} \geq (n+1)^2$.

...continued on the next slide... □

Proof by Induction: example 1

Theorem

For any integer x, if $x \geq 4$, then $2^x \geq x^2$.

Proof by induction.

We can prove that $P(n+1)$ follows from $P(n)$ with the following chain of inequalities:

$$\begin{aligned}
2^{n+1} &= 2(2^n) && \text{(sum of exponents rule)} \\
&\geq 2n^2 && \text{(inductive hypothesis: } P(n) \text{ is true)} \\
&= n^2 + n^2 \\
&\geq n^2 + 4n && \text{(since } n \geq 4 \text{, we have } n^2 \geq 4n) \\
&\geq n^2 + 2n + 1 && \text{(because } 2n \geq 8 \geq 1) \\
&= (n+1)^2.
\end{aligned}$$

Proof by Induction: example 2

Theorem

For a mortgage amount P, a monthly payment Y, and monthly multiplier M ($M = (1 + I)^{1/12} \approx 1 + I/12$ where I is the yearly interest rate), the outstanding amount P_t after t months is given by the formula:

$$P_t = PM^t - Y\frac{M^t - 1}{M - 1}.$$

Proof.

Induction basis: Prove the formula for $t = 0$. For $t = 0$, we evaluate the r.h.s. as follows:

$$PM^t - Y\frac{M^t - 1}{M - 1} = PM^0 - Y\frac{M^0 - 1}{M - 1} = P$$

which the initial mortgage amount. So the formula works for $t = 0$.

Induction hypothesis: Assume that the formula work for some $t = k$.

Proof by Induction: example 2

Theorem

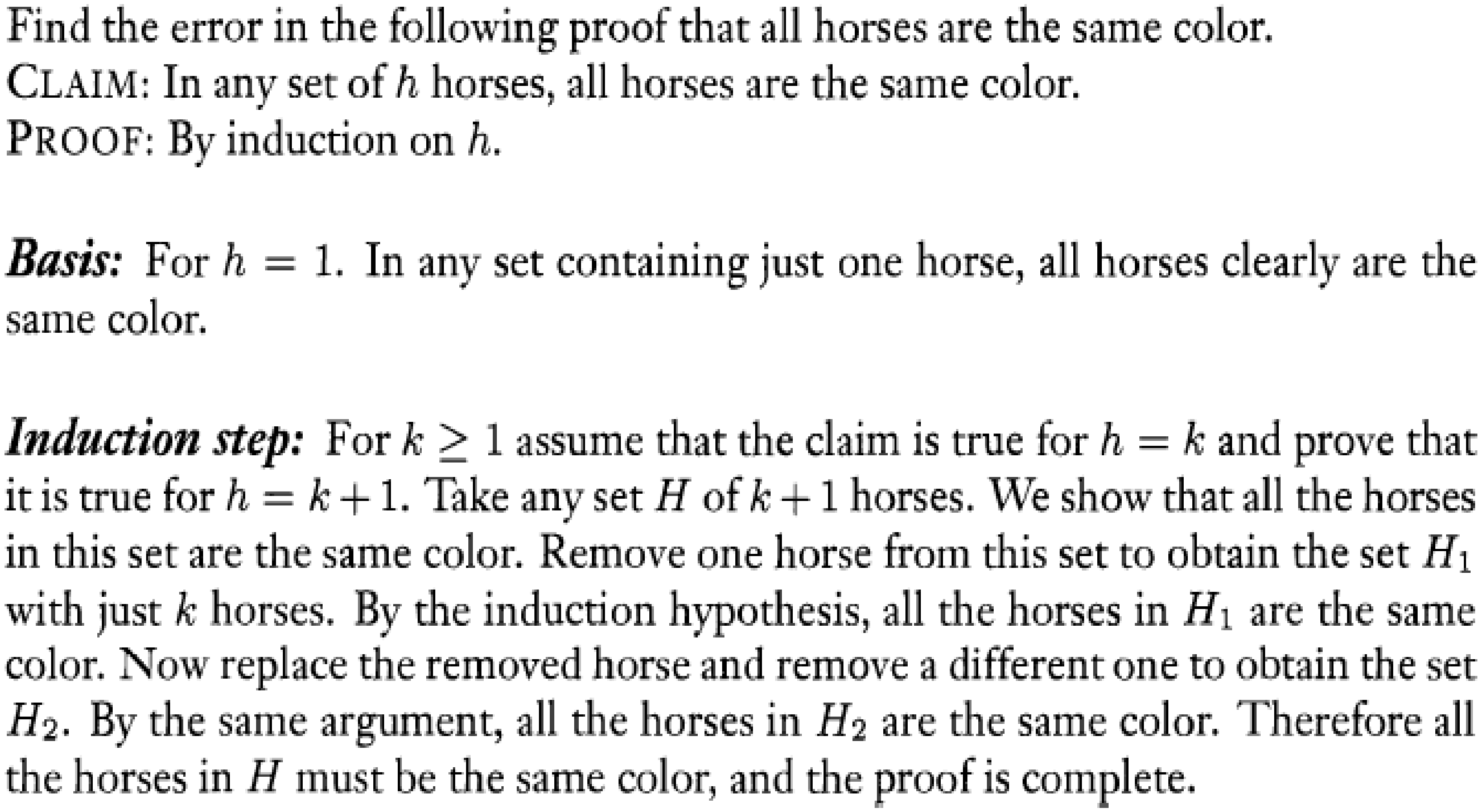
$$P_t = PM^t - Y\frac{M^t - 1}{M - 1}.$$

Proof.

Induction step: We prove that the formula works for $t = k + 1$. From definition of P_t, we know that $P_{k+1} = P_k M - Y$. By the induction hypothesis, we have formula for P_k. Plugging it in the in the previous formula gives:

$$\begin{aligned} P_{k+1} &= \left[PM^k - Y\frac{M^k - 1}{M - 1}\right] M - Y \\ &= PM^{k+1} - Y\frac{M^{k+1} - M}{M - 1} - Y\frac{M - 1}{M - 1} \\ &= PM^{k+1} - Y\frac{M^{k+1} - 1}{M - 1}. \end{aligned}$$

Proof by Induction:
The **horse paradox** is a falsidical paradox



Find the error in the following proof that all horses are the same color.
CLAIM: In any set of h horses, all horses are the same color.
PROOF: By induction on h.

Basis: For $h = 1$. In any set containing just one horse, all horses clearly are the same color.

Induction step: For $k \geq 1$ assume that the claim is true for $h = k$ and prove that it is true for $h = k+1$. Take any set H of $k+1$ horses. We show that all the horses in this set are the same color. Remove one horse from this set to obtain the set H_1 with just k horses. By the induction hypothesis, all the horses in H_1 are the same color. Now replace the removed horse and remove a different one to obtain the set H_2. By the same argument, all the horses in H_2 are the same color. Therefore all the horses in H must be the same color, and the proof is complete.

Proof by Contradiction

In one common form of argument for proving a theorem, we assume that the theorem is false and then show that this assumption leads to an obviously false consequence, called a contradiction.

We use this type of reasoning frequently in everyday life, as in the following example.

THEOREM 0.24

$\sqrt{2}$ is irrational.

PROOF First, we assume for the purposes of later obtaining a contradiction that $\sqrt{2}$ is rational. Thus

$$\sqrt{2} = \frac{m}{n},$$

where both m and n are integers. If both m and n are divisible by the same integer greater than 1, divide both by that integer. Doing so doesn't change the value of the fraction. Now, at least one of m and n must be an odd number.

We multiply both sides of the equation by n and obtain

$$n\sqrt{2} = m.$$

We square both sides and obtain

$$2n^2 = m^2.$$

Because m^2 is 2 times the integer n^2, we know that m^2 is even. Therefore m, too, is even, as the square of an odd number always is odd. So we can write $m = 2k$ for some integer k. Then, substituting $2k$ for m, we get

$$\begin{aligned} 2n^2 &= (2k)^2 \\ &= 4k^2. \end{aligned}$$

Dividing both sides by 2 we obtain

$$n^2 = 2k^2.$$

But this result shows that n^2 is even and hence that n is even. Thus we have established that both m and n are even. But we had earlier reduced m and n so that they were *not* both even, a contradiction.

Proof by Contradiction: example 1

Lemma

Every acyclic graph with $n > 0$ vertices contains a vertex of degree 0 or 1.

Proof.

(By contradiction and the pigeonhole principle.) *Suppose there is a nonempty acyclic graph G, every vertex of which has degree at least 2.*

Choose any vertex v_1 of G. v_1 has at least two neighbors, so choose a neighbor v_2 of v_1 arbitrarily. Now v_2 has at least one neighbor besides v_1, so choose such a neighbor v_3 arbitrarily. Continue in this way to pick $v_4, v_5, \ldots$ such that v_i is adjacent to v_{i+1} and $v_i \neq v_{i+2}$ for every $i \geq 1$. Since G has only finitely many vertices, by the pigeonhole principle there must be some $i < j$ such that $v_i = v_j$ and $v_i, v_{i+1}, \ldots, v_{j-1}$ are all distinct. Then $(v_i, v_{i+1}, \ldots, v_j)$ forms a simple cycle in G, which contradicts the fact that G is acyclic. Thus G must have at least one vertex of degree at most 1. □

Proof by Contradiction: example 2

Theorem

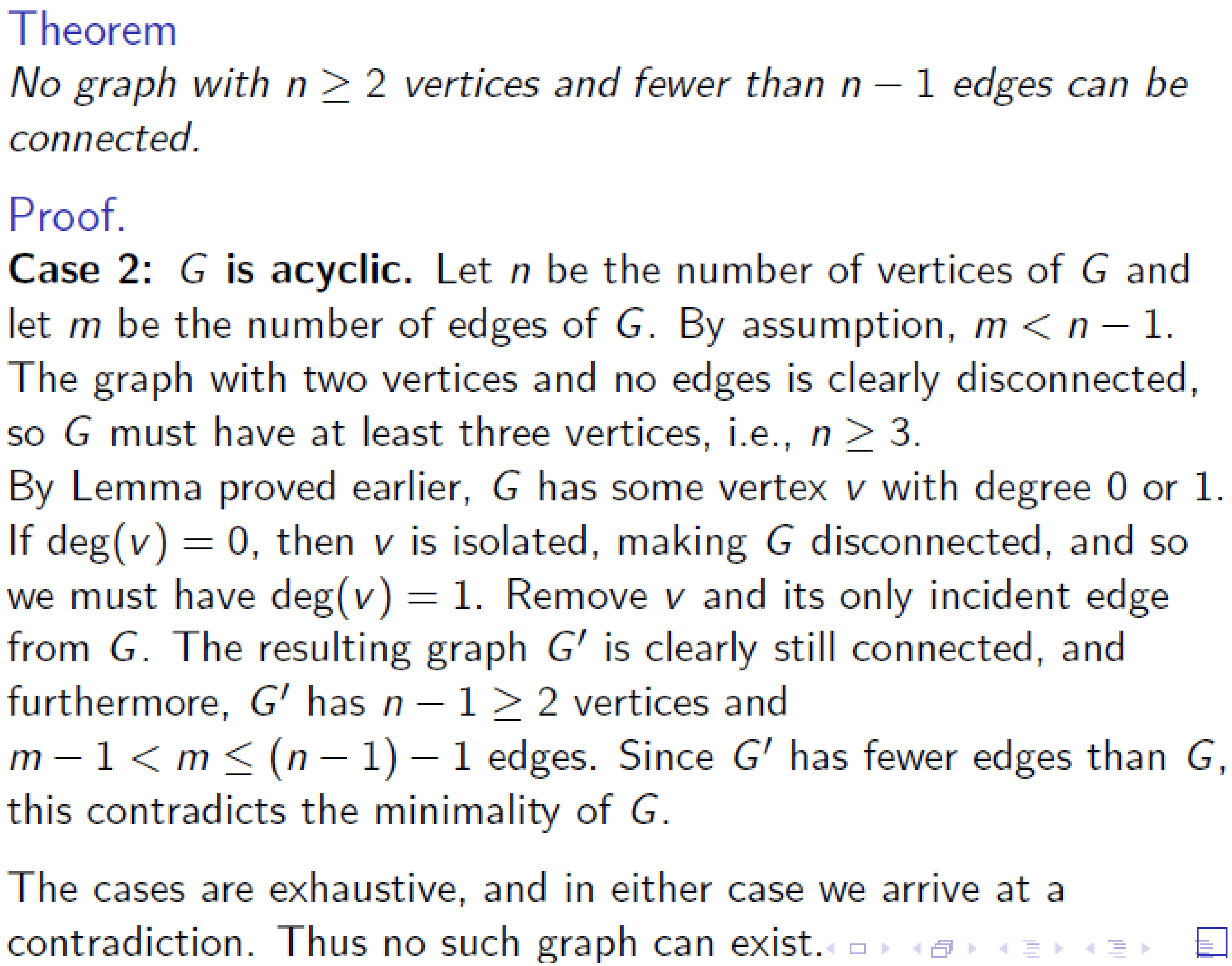
No graph with $n \geq 2$ vertices and fewer than $n-1$ edges can be connected.

Proof.

(Uses the "minimum counterexample" idea, which combines induction with contradiction.) Suppose there is a connected graph with $n \geq 2$ vertices and $m < n-1$ edges. Let G be such a graph with the least number of edges of all such graphs. There are two cases:

Case 1: G contains a cycle. Let c be a cycle in G and e be an edge in c. We remove e from G. The resulting graph G' is still connected (any path joining two vertices of G that used to go through e can be rerouted around the rest of the cycle c, giving a path in G'). But G' has fewer edges than G, which contradicts the minimality of G. □

Proof by Contradiction: example 2



Theorem

No graph with $n \geq 2$ vertices and fewer than $n-1$ edges can be connected.

Proof.

Case 2: G is acyclic. Let n be the number of vertices of G and let m be the number of edges of G. By assumption, $m < n - 1$. The graph with two vertices and no edges is clearly disconnected, so G must have at least three vertices, i.e., $n \geq 3$.
By Lemma proved earlier, G has some vertex v with degree 0 or 1. If $\deg(v) = 0$, then v is isolated, making G disconnected, and so we must have $\deg(v) = 1$. Remove v and its only incident edge from G. The resulting graph G' is clearly still connected, and furthermore, G' has $n - 1 \geq 2$ vertices and $m - 1 < m \leq (n-1) - 1$ edges. Since G' has fewer edges than G, this contradicts the minimality of G.

The cases are exhaustive, and in either case we arrive at a contradiction. Thus no such graph can exist.

Proof by Contradiction: example 3

Theorem

Any graph with $n \geq 3$ vertices and $m \geq n$ edges must contain a cycle.

Proof.

(Same "minimal counterexample" technique.) Suppose there is some acyclic graph with $n \geq 3$ vertices and at least n edges. Let G be such a graph whose n value (the number of vertices) is least among all such graphs. The graph only graph with three vertices and at least three edges is the triangle, which is clearly cyclic, so we must have $n \geq 4$.

By Lemma we proved earlier, G has a vertex v with $\deg(v) \leq 1$. Remove v and its incident edge (if there is one) from G to obtain a new graph G'. G' is clearly acyclic because G is acyclic. Furthermore, G' has $n - 1 \geq 3$ vertices and at least $n - 1$ edges, which contradicts the minimality of G. Thus no such graph can exist. □