SETS AND RELATIONS

THE NATURE OF TRUTH

By a sentence we mean a statement that has a definite truth value, true (T) or false (F).
„In 1492 Columbus sailed the ocean blue." (T)
„Napoleon won the battle of Waterloo." (F)

More generally, we mean a statement, possibly involving some variables, which is either true or false whenever we assign particular values to each of the variables.
The statement „$x \leq 5$" is true for x=4 and false for x=6.
The statement „For every x hold $x \leq 5$" is definitely false.
The statement „There exists an x such that $x \leq 5$" is definitely true.

The phrase for every x (sometimes for all x, for every x, for any x,...) is called a universal quantifier and is denoted by $\forall x$.
The phrase there exists an x (sometimes there is an x, ...) is called an existential quantifier and is denoted by $\exists x$.

THE NATURE OF TRUTH

If the truth of a formula depends on the value of, say x, we will use notation like P(x) to denote the statement.

A sentence $\forall x\, P(x)$ is true if and only if P(x) is true no matter what value (from the universe of discourse) is substituted for x.
A sentence $\exists x\, P(x)$ is true if and only if there is at least one value of x (from the universe of discourse) that makes P(x) true.

An axiom is a statement that is accepted as true without proof.
Mathematical objects come into existence by definition.
A theorem is a declarative statement for which there is a proof.

IF-THEN

The vast majority of theorem can be expressed in the form

„If A, then B.“

Example

Theorem „The sum two even numbers is even“ can be rephrased „If x and y are even numbers, then $x + y$ is also even.“

The statement „If A, then B.“ means:
Every time condition A is true, condition B must be true as well.
The statement „If A, then B“ promisses that condition B is true whenewer A is true but makes no claim about B when A is false.
Condition A is called hypothesis.
Condition B is called conclusion.
A is sufficient condition for B.
B is necessary condition for A.

IF-THEN

Example

Imagine, I am a politician running for office, and I announce in public,
„If I am elected, then I will lower taxes."
Under what circumstances would you call me a liar?

- Suppose I am elected and I lower taxes. Certainly you would not call me a liar. I kept my promise.
- Suppose I am elected and I do not lower taxes. Now you have every right to call me a liar. I have broken my promise.
- Suppose I am not elected and somebody manage to get taxes lower. You certainly would not call me a liar. I have not broken my promise.
- Suppose I am not elected and taxes are not lower. You would not accuse me of lying. I promised to lower taxes only if I were elected.

IF-THEN

We might have condition A true or false, and we might have condition B true or false. Let us summarize this in a chart. If the statement „If A, then B" is true, we have the following.

Condition A	Condition B	
True	True	Possible
True	False	Impossible
False	True	Possible
False	False	Possible

Proof is an argument that establishes the truth of a theorem. The typical way to disprove an IF–THEN statement is to create a counterexample.

The statement „If A, then B."

Negation of this statement: „A and also negation of B".

Thus, a counterexample to such a statement would be an instance where A is true, but B is false.

The statement $\forall x$: If $A(x)$, then B(x).

Negation of this statement: $\exists x$: $A(x)$ and negation of $B(x)$.

Thus, a counterexample to such a statement would be an example of finding one value of x that satisfies $A(x)$, but not $B(x)$.

Sets and Operations

A set is a repetition-free, unorder collection of objects.
We introduced four special sets of numbers. These sets are

- $\mathbb{N}$ the natural numbers,
- $\mathbb{Z}$ the integers,
- $\mathbb{Q}$ the rational numbers,
- $\mathbb{R}$ the real numbers.

A given object is either a member of a set or it is not. The simplest way to specify a set is to list elements between curly braces, for example $\{1, 3, 5, 9\}$. More often, set-builder notation is used. The form of this notation is

$$\{\textit{dummy variable} \in \textit{set}; \textit{conditions}\}.$$

For example $\{x \in \mathbb{N}; x \text{ is odd and } x \leq 10\}$
An object that belongs to a set is called an element of a set. Membership in a set is denoted with the symbol $\in$. The notation $x \in A$ means that the object x is a member of the set A. The notation $x \notin A$ means x is not an element of A.

Sets and Operations

The number of elements in a set A is denoted $|A|$ and called the cardinality of A. A set is called finite if its cardinality is an integer. Otherwise, it is called infinite. The empty set is the set with no members. The symbol for the emty set is $\emptyset$.

Definition

Suppose A and B are sets. We say that A is a subset of B provided every element of A is also an element of B. The notation $A \subseteq B$ means A is a subset of B.

It is clear that $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. Morever, $\emptyset \subseteq A$ and $A \subseteq A$ for every set A.

Definition

Let A be a set. The power set of A is a set $\mathcal{P}(A)$ of all subsets.

Example

The power set of the set $A = \{a, b, c\}$ is
$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

Sets and Operations

Let U be a set of all objects under consideration and $A, B \subseteq U$.

Definition

The union of A and B is the set of all elements that are in A or B. The union of A and B is denoted $A \cup B$.

$$A \cup B = \{x \in U;\ x \in A \text{ or } x \in B\}.$$

Definition

The intersection of A and B is the set of all elements that are in A and B. The intersection of A and B is denoted $A \cap B$.

$$A \cap B = \{x \in U;\ x \in A \text{ and } x \in B\}.$$

Sets and Operations

Definition

The set difference, $A - B$, is the set of all elements of A that are not in B.

$$A - B = \{x \in U;\ x \in A \text{ and } x \notin B\}.$$

Definition

The symmetric difference of A and B, denoted $A \div B$, is the set of all elements in A but not in B or in B but not in A.

$$A \div B = \{x \in U;\ x \in (A \cup B) \text{ and } x \notin (A \cap B)\}.$$

Definition

The complement of A, denoted $\overline{A}$, is the set of all objects in U that are not in A.

$$\overline{A} = \{x \in U;\ x \notin A\}.$$

$\overline{A} = U - A$

Sets and Operations

Theorem

Let A, B and C denote sets. The following are true:

1. *Commutative properties*
   $A \cap B = B \cap A, \qquad A \cup B = B \cup A,$
2. *Associative properties*
   $A \cap (B \cap C) = (A \cap B) \cap C, \qquad A \cup (B \cup C) = (A \cup B) \cup C,$
3. *Distributive properties*
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C),$
4. *DeMorgans Laws*
   $\overline{A \cap B} = \overline{A} \cup \overline{B}, \qquad \overline{A \cup B} = \overline{A} \cap \overline{B},$
5. $A \cap \emptyset = \emptyset, \qquad A \cup U = U,$
6. $\overline{(\overline{A})} = A,$
7. $A \cap U = A, \qquad A \cup \emptyset = A,$
8. $A \cap A = A, \qquad A \cup A = A,$
9. $A \cup \overline{A} = U,$
10. $A \cap \overline{A} = \emptyset.$

Definition

We call sets A and B disjoint provided $A \cap B = \emptyset$.
Let $A_1, A_2, \dots A_n$ be a collection of sets. The sets are called pairwise disjoint provided $A_i \cap A_j = \emptyset$ whenever $i \neq j$.

Definition

Let A be a set. A partition of A is a set of nonempty, pairwise disjoint sets $A_1, A_2, \dots A_n$ whose union is A.

In other words, the collection of sets $A_1, A_2, \dots A_n$ is a partition of A if

$$A_1 \cup A_2 \cup \cdots \cup A_n = A$$

and

$$A_i \cap A_j = \emptyset \text{ for every } i, j \in \{1, 2, \dots n\}, i \neq j.$$

Integers and Division

Definition

Let a and b be integers. We say that a is divisible by b provided there is an integer q so that

$$a = b \cdot q.$$

The notation for this is $b \mid a$ (we read it „b divides a ")
We also say „b is divisor of a", „b is factor of a", „a is multiple of a".

Example

$11 \mid 44 \qquad -5 \mid 105 \qquad -9 \mid -99 \qquad 10 \nmid 129$

Theorem

Let $a, b \in \mathbb{Z}$ with $b > 0$. There exist integers q and r so that

$$a = b \cdot q + r \qquad 0 \leq r < b$$

Morever, there is only one such pair of integers q and r that satisfies these conditions.
The integer q is called quotient and r is called remainder.

Integers and Division

Definition

Let m be a positive integer. We say that integers a and b are congruent modulo m and we write

$$a \equiv b \pmod{m}$$

provided $m \mid (a-b)$.

Example

$23 \equiv 8 \pmod 5$ $\quad 101 \equiv 36 \pmod 5$ $\quad 11 \equiv 23 \pmod 2$ $\quad 11 \not\equiv 99 \pmod{10}$

It is easy to see that for $a, b, c, d, x \in \mathbb{Z},\ m, k \in \mathbb{N}$:

- $a \equiv b \pmod m$ if and only if $a = m \cdot q_1 + r$ and $b = m \cdot q_2 + r$ for $0 \leq r < m,\ q_1,\ q_2 \in \mathbb{Z}$.
- If $a \equiv b \pmod m$ then $a \cdot x \equiv b \cdot x \pmod m$.
- If $a \equiv b \pmod m$ then $a^k \equiv b^k \pmod m$.
- If $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then $a \cdot c \equiv b \cdot d \pmod m$.

Integers and Division

Definition

Let $a, b \in \mathbb{Z}$. We call an integer d a common divisor of a and b provided $d \mid a$ and $d \mid b$.

Definition

Let $a, b \in \mathbb{Z}$. We call an integer d the greatest common divisor of a and b provided

- $d \mid a$ *and* $d \mid b$,
- *if* $c \mid a$ *and* $c \mid b$, *then* $c \leq d$.

Denote $gcd(a, b)$

Example

The common divisors of $a = -30$ and -24 are numbers $-6, -3, -2, -1, 1, 2, 3, 6$.
$gcd(-30, -24) = 6$.

Note $gcd(-30, -24) = gcd(-30, 24) = gcd(30, -24) = gcd(30, 24)$.

EUCLIDs Algorithm

INPUT: Positive integers $a, b,\ a > b$
OUTPUT: $gcd(a, b)$

1. step $a = b \cdot q + r \qquad 0 \leq r < b$
2. step If $r \neq 0$, then $a := b$ and $b := r$ and go back to step one.
   If $r = 0$, then stop and $gcd(a, b)$ is the last non-zero remainder.

Relations

Definition

The Cartesian product of sets A and B, denoted $A \times B$, is the set of all ordered pairs formed by taking an element from A together with an element from B in all possible ways.

$$A \times B = \{(x, y);\ x \in A \text{ and } y \in B\}.$$

Example

The Cartesian product $A \times B$ of the sets $A = \{1, 2, 3\}$ and $B = \{4, 5\}$ is $A \times B = \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5)\}$.

Definition

(a, b)=(c, d) *if and only if* $a = c$ *and* $b = d$.

Relations

Let A and B be sets.

Definition

A relation from A to B is any subset $\mathcal{R}$ of the Cartesian product $A \times B$. That is $\mathcal{R} \subseteq A \times B$.

Tha fact $(a, b) \in \mathcal{R}$ we usually write $a\mathcal{R}b$ and we say that a is related to b.

Definition

A relation on A is any subset of $A \times A$. That is $\mathcal{R} \subseteq A \times A$.

Definition

Let $\mathcal{R}$ be a relation on a set A.

- *If for all $x \in A$ we have $x\mathcal{R}x$, we call $\mathcal{R}$ reflexive.*
- *If for all $x, y \in A$ we have $x\mathcal{R}y \Rightarrow y\mathcal{R}x$, we call $\mathcal{R}$ symmetric.*
- *If for all $x, y \in A$ we have $(x\mathcal{R}y \wedge y\mathcal{R}x) \Rightarrow x = y$, we call $\mathcal{R}$ antisymmetric.*
- *If for all $x, y, z \in A$ we have $(x\mathcal{R}y \wedge y\mathcal{R}z) \Rightarrow x\mathcal{R}z$, we call $\mathcal{R}$ transitive.*

Relations

Definition

Let $\mathcal{R}$ be a relation on a set A. We say $\mathcal{R}$ is an equivalence relation provided it is reflexive, symmetric and transitive.

Definition

Let $\mathcal{R}$ be an equivalence relation on a set A and let $a \in A$.The equivalence class of a, denoted $[a]$, is the set of all elements of A related to a. That is

$$[a] = \{x \in A; x\mathcal{R}a\}$$

Theorem

Let $\mathcal{R}$ be an equivalence relation on a set A. The equivalence classes of $\mathcal{R}$ form a partition of the set A.

Relations

Example

Consider the relation $\leq$ (less than or equal to) on the integers.

- Note that $\leq$ is reflexive because for any integer x, it is true that $x \leq x$.
- The relation $\leq$ is not symmetric because that would mean that $x \leq y \Rightarrow y \leq x$. This is false, for example $3 \leq 8$, but $8 \not\leq 3$.
- However, $\leq$ is antisymmetric. If we know $x \leq y$ and $y \leq x$, it must be case that $x = y$.
- It is transitive, since $x \leq y$ and $y \leq z$ imply that $x \leq z$.

Example

Consider the relation $<$ (strict less than) on the integers.

- Note that $<$ is not reflexive because $x < x$ is never true.
- The relation $<$ is not symmetric because that would mean that $x < y \Rightarrow y < x$. This is false, for example $3 < 8$, but $8 \not< 3$.
- The relation $<$ is antisymmetric, but it fulfills the condition vacuously. The condition states $(x < y \text{ and } y < x) \Rightarrow x = y$. However, it is impossible to have both $x < y$ and $y < x$, so the hypothesis of this if-then statement can never satisfied. Therefore it is true.
- Finally, it is transitive, since $x < y$ and $y < z$ imply that $x < z$ for all integers x, y, z.

Example

Consider the relation $\mid$ (divides) on the integers.

- $\forall x \in \mathbb{Z}$: $x \mid x$. Since $\exists q = 1 \in \mathbb{Z} : x = x \cdot 1$, the relation $\mid$ is reflexive.
- $\forall x, y \in \mathbb{Z}$: $x \mid y \Rightarrow y \mid x$. As $3 \mid 9$ and $9 \nmid 3$, the relation $\mid$ is not symmetric.
- $\forall x, y \in \mathbb{Z}$: $(x \mid y \land y \mid x) \Rightarrow x = y$. As $-4 \mid 4$ and $4 \mid -4$, but $-4 \neq 4$ the relation $\mid$ is not antisymmetric.
- $\forall x, y, z \in \mathbb{Z}$: $(x \mid y \land y \mid z) \Rightarrow x \mid z$. Since $\exists q_1, q_2 \in \mathbb{Z} : y = x \cdot q_1$ and $z = y \cdot q_2$, we have $z = x \cdot q_1 \cdot q_2 = x \cdot q_3$. It implies $x \mid z$. The relation $\mid$ is transitive.

Example

Consider the relation $\mid$ (divides) on the naturals numbers.

- The relation $\mid$ on the naturals numbers is reflexive and transitive because $\mid$ on the integers is reflexive and transitive.
- The relation $\mid$ is not symmetric because we have counterexample $3 \mid 9$ and $9 \nmid 3$.
- However, $\mid$ is antisymmetric. If we know $x \mid y$ and $y \mid x$, it means $\exists q_1, q_2 \in \mathbb{Z} : y = x \cdot q_1$ and $x = y \cdot q_2$. We have $y = y \cdot q_1 \cdot q_2$. Thus $q_1 \cdot q_2 = 1$. It must be the case that $q_1 = q_2 = 1$, so $x = y$.

Example

Let $m \in \mathbb{N}$. For the relation $\mathcal{R} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z};\ x \equiv y \pmod{m}\}$ determine whether the relation is an equivalence relation. If it is equivalence relation, find the equivalence classes for $m = 2$.

Solution: We need to show that relation $\mathcal{R}$ is reflexive, symmetric and transitive.

- To show that relation $\mathcal{R}$ is reflexive, we have to show

  $$\forall x \in \mathbb{Z} : x \equiv x \pmod{m}.$$

  It means $m \,|\, (x - x)$, that is $m \,|\, 0$. Clearly 0 is multiple of m. Thus the relation $\mathcal{R}$ is reflexive.

- To show symmetry, we must prove

  $$\forall x, y \in \mathbb{Z} : x \equiv y \pmod{m} \Rightarrow y \equiv x \pmod{m}.$$

  This is an IF-THEN statement, so we suppose $m \,|\, (x - y)$. So, there is an integer q such that $(x - y) = q \cdot m$. But then $(y - x) = (-q) \cdot m$. And so $m \,|\, (y - x)$. Therefore $y \equiv x \pmod{m}$. Thus the relation $\mathcal{R}$ is symmetric.

Relatins

- To show that relation $\mathcal{R}$ is transitive, we must prove

$$\forall x, y, z \in \mathbb{Z} : (x \equiv y \pmod{m} \wedge y \equiv z \pmod{m}) \Rightarrow x \equiv z \pmod{m}.$$

We suppose $m \mid (x - y)$ and also $m \mid (y - z)$. So, $\exists q_1, q_2 \in \mathbb{Z} : (x - y) = q_1 \cdot m$ and $(y - z) = q_2 \cdot m$. By adding both equations, we have $(x - z) = (q_1 + q_2) \cdot m = q_3 \cdot m$. It implies $m \mid (x - z)$. Therefore $x \equiv z \pmod{m}$. So, the relation $\mathcal{R}$ is transitive.

Therefore the relation $\mathcal{R}$ is equivalence relation.
Consider the equivalence relation congruence (mod 2).
What is equivalence class [1]? By definition, $[1] = \{x \in \mathbb{Z};\ x \equiv 1 \pmod{2}\}$. This is the set of all integers x such that $2 \mid (x - 1)$, i.e. x is odd. The set [1] is the set of odd numbers.
It is not hard to see that equivalence class [0] is the set of even numbers.
The equivalence relation congruence (mod 2) has only two equivalence classes: the set of odd integers and the set of even integers.

Functions

A function is a special kind of a relation. A relation $\mathcal{R}$ from A to B is a subset of the Cartesian product $A \times B$.

Definition

A relation f is called a function provided $(a, b) \in f$ and $(a, c) \in f$ imply $b = c$.

Definition

Let f be a function and let a be an object. The notation $f(a)$ is defined provided there exists an object b so that $(a, b) \in f$. In this case $f(a) = b$.

Definition

Let f be a function. The set of all possible first elements of the ordered pairs in f is called the domain of f and is denoted $\operatorname{dom} f$. The set of all possible second elements of the ordered pairs in f is called the image of f and is denoted $\operatorname{im} f$.

Functions

Definition

Let f be a function and let A and B be sets. We say that f is a function from A to B provided $\operatorname{dom} f = A$ and $\operatorname{im} f \subseteq B$. In this case, we write $f : A \to B$.

Definition

We say that f is one-to-one provided, whenewer for all $x_1, x_2 \in \operatorname{dom} f$: if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$.
We say that f is onto provided, for all $y \in \operatorname{im} f$ there is an $x \in \operatorname{dom} f$ so that $f(x) = y$.
We call f a bijection provided it is both one-to-one and onto.