UNIT 1

Sets, Relations, and Functions

Contents

1. Introduction to set theory

1.1. Baseline definitions and notation

Definition: *SET*

A **set** is a relation or collection of elements or objects.

Notation:

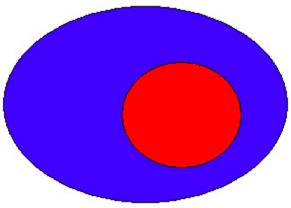
- The sets are denoted with capital letters: A, B, C, …
- Their elements are denoted with lowercase: t, u, v, …
- When t is an element of A is written as $t \in A$. In contrast, when it is not an element of A is written as $t \notin A$.
- The elements of a set are enclosed in curly brackets $A = \{t: t \in A\}$
- If a set has a finite number of elements, the set can be represented enumerating its elements $A = \{a, b, c, d\}$.
- The large finite sets or the infinite sets are described through one or more properties that fulfill all their elements $\mathbb{Z} = \{z | z = 0 \vee z = n \vee z = -n \text{ being } n \in \mathbb{N}\}$ or $B = \{x | x \in \mathbb{N} \wedge x > 3\}$

(The vertical bar | is read "*such that*", like the colon ":" or the semicolon ";". The symbol ∨ means "*or*", and ∧ represents the conjunction "*and*")

Definition: *SUBSET*

A is a ***subset*** of B, if $(\forall t)(t \in A \rightarrow t \in B)$. It is denoted by $A \subseteq B$.

You can also say that A is contained in B.



Comments:

- $A \subset B$ means that A is strictly contained in B. This will happen when, in addition to the previous condition $(\forall t)(t \in A \rightarrow t \in B)$, we have that $(\exists t)(t \in B \wedge t \notin A)$. The subsets of B that fulfill this new condition are called **proper** (or strict) **subsets**.
- If B is a set, ∅ and B are subsets of this set.
- If $\exists t \in A$ then $t \notin B \Rightarrow A \subseteq B$ is false.
- $(A \subseteq B) \wedge (B \subseteq A) \Rightarrow A = B$

Examples:

- $A = \{1,2,3\}$ is a subset of the natural numbers. $A \subseteq \mathbb{N}$, in fact $A \subset \mathbb{N}$
- $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$

Definition: *CARDINAL OF A SET*

The ***cardinal number or cardinality of a set*** is the number of elements that compose the set. It is denoted by $n(A)$ or $|A|$.

Examples:

- The ***empty set*** $\emptyset$ is the set that has no elements. $n(\emptyset) = 0$.
- The ***singleton sets***, also known as *unit sets*, are composed of exactly one element $\{x\}$. $n(\{x\}) = 1$
- For any number of objects, $x_1, x_2, \dots x_n$ there exists a set whose elements are those objects $\{x_1, x_2, \dots x_n\}$, in this case $n(\{x_1, x_2, \dots x_n\}) = n$.
- The set of the natural numbers is $\mathbb{N} = \{1,2, \dots\}$ and $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ is the set of all the integers. These sets fulfill that $n(\mathbb{N}) = n(\mathbb{Z})$.
- $P = \{x | x \text{ is even}\}$, the set of the even numbers fulfills that $n(P) = n(\mathbb{Z})$.

Property: *Axiom of extensionality*

$$t \in A \leftrightarrow t \in B \Rightarrow A = B$$

If all the elements of two sets are equal, then the sets are equal.

In this case, their cardinality will also be equal.

Example:

- $\{a, b\} = \{b, a\}$, is the same set with a different representation.

Comments:

- A different way of stating this axiom is $A \subseteq B \wedge B \subseteq A \Rightarrow A = B$. Note that $A \subseteq B$ is equivalent to say that if $t \in A \rightarrow t \in B$.
- This axiom is used to prove the equality between two sets. Nevertheless, when the sets are finite, we will be using the following axiom.

Axiom

Let $A, B \subseteq X$ be finite sets such that $A \subseteq B$ and $n(A) = n(B)$ then $A = B$.

Definition: *POWER SET*

Let A be a set, the ***power set of A*** is the set that contains all the subsets of A. It is denoted by: $\wp(A) = \{x | x \subseteq A\}$

It fulfills that $n(\wp(A)) = |\wp(A)| = 2^{n(A)} = 2^{|A|}$

Examples:

- Empty set, $\wp(\emptyset) = \{\emptyset\}$
- If $A = \{1,2,3\}$, $\wp(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\} = A\}$

Definition: *COMPLEMENT OF A SET*

The complement of the set A respect to another set X such that $A \subseteq X$, or $A \in \wp(X)$, is composed of all the elements in X which are not in A.

$$A' = A^c = \overline{A} = \{x | x \in X \wedge x \notin A\}$$

Comments:

- Some authors call the set which is used as reference to calculate the complement of a set *universal set*.
- In case of real numbers, the set that is used as reference to calculate the complement of a set is the real number line. $\mathbb{R}$

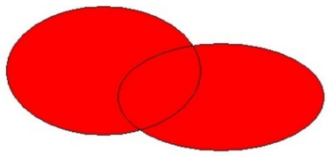
Examples:

- If $X = \mathbb{N}$ and $A = \{n|(4 < n < 26), n \in \mathbb{N}\}$, then $A^c = \{n|(n \leq 4) \vee (n \geq 26), n \in \mathbb{N}\}$
- If $X = \mathbb{R}$ and $A = [2,3] \subset \mathbb{R}$, $A^c = (-\infty, 2) \cup (3, +\infty)$
- If $X = A = \{1,2,3\}$, $\{2,3\}' = \{1\}$, $\{3\}' = \{1,2\}$, $A^c = \emptyset$

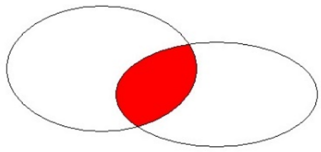
1.2. Algebra of sets

1.2.1. Operations between sets

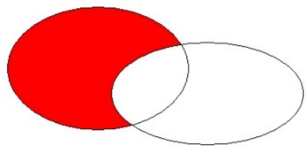
The ***Union*** of two sets results in a new set whose elements belong to some of the two initial sets: $A \cup B = \{x|(x \in A) \vee (x \in B)\}$



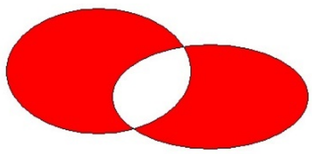
The ***Intersection*** of two sets results in a new set whose elements belong to the two initial sets: $A \cap B = \{x|(x \in A) \wedge (x \in B)\}$



The ***relative complement*** or ***set difference*** of two sets is composed of the elements that belong to one of the initial sets and are not present in the other initial set: $A - B = \{x|x \in A \wedge x \notin B\} = A \cap B'$



The ***symmetric difference*** between A and B results in a new set which is defined by the following relation: $\boldsymbol{A \Delta B} = (\boldsymbol{A} - \boldsymbol{B}) \cup (\boldsymbol{B} - \boldsymbol{A}) = \{\boldsymbol{x}|\boldsymbol{x} \in (\boldsymbol{A} \cup \boldsymbol{B}) - (\boldsymbol{A} \cap \boldsymbol{B})\}$



Comments:

- If S is a set whose elements are sets (Family of sets), then
  - ✓ $\cup S = \{x|x \text{ belongs to SOME element of } S\}$
  - ✓ $\cap S = \{x|x \text{ belongs to ALL the elements of } S\}$
- For each set $A \subseteq X$, it is verified that $\cup \wp(A) = A$ and $\cap \wp(A) = \emptyset$
- If for each $n \in \mathbb{N}$, we have A_n, and $i, j \in \mathbb{N}$, then $S = \{A_n : n \in \mathbb{N}\}$ is an indexed family, a family (set of sets) such that its elements (sets) are indexed (e.g., by natural numbers) and it is possible to use different notations:
  - ✓ $\cup \{A_n|n \in \mathbb{N}\} = \bigcup_{n\in\mathbb{N}} A_n = \bigcup_n A_n$
  - ✓ $\cap \{A_n|n \in \mathbb{N}\} = \bigcap_{n\in\mathbb{N}} A_n = \bigcap_n A_n$
  - ✓ $\cup \{A_n|i \leq n \leq j, n \in \mathbb{N}\} = \bigcup_{n=i}^{j} A_n$
  - ✓ $\cap \{A_n|i \leq n \leq j, n \in \mathbb{N}\} = \bigcap_{n=i}^{j} A_n$
- If $A \cap B = \emptyset$, then A and B are ***disjoint sets***.

- $A \cup A' = X$
- $Card(A \cup B) = Card(A) + Card(B) - Card(A \cap B)$
- $Card(A - B) = Card(A) - Card(A \cap B)$
- $Card(A \Delta B) = Card(A) + Card(B) - 2Card(A \cap B)$

Examples:

- Given $\mathbb{N}_n = \{1,2,\dots n\}$, then
  - ✓ $\cup\{\mathbb{N}_n : n \in \mathbb{N}\} = \bigcup_{n\in\mathbb{N}} \mathbb{N}_n = \bigcup_n \mathbb{N}_n = \mathbb{N}$
  - ✓ $\cap\{\mathbb{N}_n : n \in \mathbb{N}\} = \bigcap_{n\in\mathbb{N}} \mathbb{N}_n = \bigcap_n \mathbb{N}_n = \{1\}$
- $\mathbb{N}^* = \mathbb{N} \cup \{0\}$ are called cardinal numbers (used to count).

1.2.2. Properties of set algebra

Remember that quadruple $(P(X), (\ \ )^c, \cup, \cap)$ belongs to Boolean algebra, where:

- $(\ )^c: P(X) \to P(X) | A \to A$, the unary operation that returns the complement of a set.
- $\cup: P(X) \times P(X) \to P(X) | (A, B) \to A \cup B$, the binary operation that returns the union of two sets.
- $\cap: P(X) \times P(X) \to P(X) | (A, B) \to A \cap B$, the binary operation that returns the intersection of two sets.

Therefore, the properties of these operations are the ones derived from the structure of the Boolean algebra.

Properties of set algebra	
Idempotent Laws	$A \cup A = A$ $A \cap A = A$
Involution and Complement Laws	$(A')' = A$ $X' = \emptyset \quad \emptyset' = X$ $A \cup A' = X \quad A \cap A' = \emptyset$
Commutative Laws	$A \cup B = B \cup A$ $A \cap B = B \cap A$
Associative Laws	$(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$
Distributive Laws	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
DeMorgan's Laws	$(A \cup B)' = A' \cap B'$ $(A \cap B)' = A' \cup B'$
Identity Laws	$A \cup \emptyset = A$ $A \cap X = A$ $A \cup X = X$ $A \cap \emptyset = \emptyset$

Idempotent Laws.

1. $A \cup A = A$

   Proof: Using the axiom of extensionality.

$$\left.\begin{array}{l}(A\cup A)\subseteq A:\\ t\in A\cup A\Rightarrow t\in A\vee t\in A\Rightarrow t\in A\\ A\subseteq \big((A\cup A)\big):\\ t\in A\Rightarrow t\in A\vee t\in A\Rightarrow t\in A\cup A\end{array}\right\}\Rightarrow A\cup A=A$$

2. $A \cap A = A$

   Proof: Using the axiom of extensionality.

$$\left.\begin{array}{l}(A\cap A)\subseteq A:\\ t\in A\cap A\Rightarrow t\in A\wedge t\in A\Rightarrow t\in A\\ A\subseteq (A\cap A):\\ t\in A\Rightarrow t\in A\wedge t\in A\Rightarrow t\in A\cap A\end{array}\right\}\Rightarrow A= A\cap A$$

Involution and Complement Laws.

1. $A \cup A' = X$

   Proof: Using the axiom of extensionality.

$$A\cup A'\subseteq X:$$

$$t\in A\cup A'\Rightarrow t\in A\vee t\in A'\Rightarrow t\in X\ \ (A,A'\subset X)$$

$$X\subseteq A\cup A':$$

$$t\in X\Rightarrow\begin{cases} t\in A\Rightarrow t\in A\cup A'\\ t\notin A\Rightarrow t\in A'\Rightarrow t\in A\cup A'\end{cases}$$

2. $A \cap A' = \emptyset$

   Proof: By reductio ad absurdum.

   $A\cap A'\neq\emptyset\Rightarrow\exists t\in A\cap A'\Rightarrow t\in A\wedge t\in A'\Rightarrow t\notin A'\wedge t\notin A$ Contradiction!!

3. $(A')' = A$

   Proof: Using the axiom of extensionality.

$$(A')'\subseteq A$$

$$t\in (A')'\Rightarrow t\in X=A\cup A'\wedge t\notin A'\Rightarrow t\in A$$

$$A\subseteq (A')'$$

$$t\in A\Rightarrow t\notin A'\Rightarrow t\in (A')'$$

4. $X' = \emptyset$

   Proof: By reductio ad absurdum.

   $X'\neq\emptyset\Rightarrow\exists t\in X'\Rightarrow t\notin X$ Contradiction!!

5. $\emptyset' = X$

   Proof: By reductio ad absurdum.

   $\emptyset'\neq X\Rightarrow\exists t\in X\wedge t\notin\emptyset'\Rightarrow t\in\emptyset$ Contradiction!!

Communicative Laws

1. $A \cup B = B \cup A$

   Proof: Using the axiom of extensionality.

$$t \in A \cup B \Leftrightarrow t \in A \vee t \in B \Leftrightarrow t \in B \vee t \in A \Leftrightarrow t \in B \cup A$$

2. $A \cap B = B \cap A$

   Proof: Using the axiom of extensionality.

$$t \in A \cap B \Leftrightarrow t \in A \wedge t \in B \Leftrightarrow t \in B \wedge t \in A \Leftrightarrow t \in B \cap A$$

Associative Laws.

1. $(A \cup B) \cup C = A \cup (B \cup C)$

   Proof: Using the axiom of extensionality.

$$t \in (A \cup B) \cup C \Leftrightarrow \big(t \in (A \cup B)\big) \vee (t \in C) \Leftrightarrow (t \in A) \vee (t \in B) \vee (t \in C) \Leftrightarrow$$
$$\Leftrightarrow (t \in A) \vee \big((t \in B) \vee (t \in C)\big) \Leftrightarrow (t \in A) \vee (t \in B \cup C) \Leftrightarrow t \in A \cup (B \cup C)$$

2. $(A \cap B) \cap C = A \cap (B \cap C)$

   Proof: Using the axiom of extensionality.

$$t \in (A \cap B) \cap C \Leftrightarrow \big(t \in (A \cap B)\big) \wedge (t \in C) \Leftrightarrow (t \in A) \wedge (t \in B) \wedge (t \in C) \Leftrightarrow$$
$$\Leftrightarrow (t \in A) \wedge \big((t \in B) \wedge (t \in C)\big) \Leftrightarrow (t \in A) \wedge (t \in B \cup C) \Leftrightarrow t \in A \cap (B \cap C)$$

Distributive Laws.

1. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

   Proof: Using the axiom of extensionality.

$$t \in A \cup (B \cap C) \Leftrightarrow (t \in A) \vee (t \in B \cap C) \Leftrightarrow (t \in A) \vee \big((t \in B) \wedge (t \in C)\big) \Leftrightarrow$$
$$\Leftrightarrow \big((t \in A) \vee (t \in B)\big) \wedge \big((t \in A) \vee (t \in C)\big) \Leftrightarrow (t \in A \cup B) \wedge (t \in A \cup C) \Leftrightarrow t \in (A \cup B) \cap (A \cup C)$$

2. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

   Proof: Using the axiom of extensionality.

$$t \in A \cap (B \cup C) \Leftrightarrow (t \in A) \wedge (t \in B \cup C) \Leftrightarrow (t \in A) \wedge \big((t \in B) \vee (t \in C)\big) \Leftrightarrow$$
$$\Leftrightarrow \big((t \in A) \wedge (t \in B)\big) \vee \big((t \in A) \wedge (t \in C)\big) \Leftrightarrow (t \in A \cap B) \vee (t \in A \cap C) \Leftrightarrow t \in (A \cap B) \cup (A \cap C)$$

DeMorgan's Laws.

1. $(A \cup B)' = A' \cap B'$

   Proof: Using the axiom of extensionality.

$$(A \cup B)' \subseteq A' \cap B'$$
$$t \in (A \cup B)' \Rightarrow t \notin (A \cup B) \Rightarrow (t \notin A) \wedge (t \notin B) \Rightarrow t \in A' \wedge t \in B' \Rightarrow t \in A' \cap B'$$
$$A' \cap B' \subseteq (A \cup B)'$$
$$t \in A' \cap B' \Rightarrow t \in A' \wedge t \in B' \Rightarrow (t \notin A) \wedge (t \notin B) \Rightarrow t \notin (A \cup B) \Rightarrow t \in (A \cup B)'$$

2. $(A \cap B)' = A' \cup B'$

   Proof: Using the axiom of extensionality.

$$(A \cap B)' \subseteq A' \cup B'$$

$$t \in (A \cap B)' \Rightarrow t \notin A \cap B \Rightarrow (t \notin A) \vee (t \notin B) \Rightarrow (t \in A') \vee (t \in B') \Rightarrow t \in A' \cup B'$$

$$(A \cap B)' \supseteq A' \cup B'$$

$$t \in A' \cup B' \Rightarrow t \in A' \vee t \in B' \Rightarrow \begin{cases} t \notin A \Rightarrow t \notin A \cap B \\ t \notin B \Rightarrow t \notin A \cap B \end{cases} \Rightarrow t \in (A \cap B)'$$

Identity Laws

1. $A \cup \emptyset = A$

   Proof: Using the axiom of extensionality.

$$(\emptyset \subseteq A) \wedge (A \subseteq A) \Rightarrow \emptyset \cup A \subseteq A$$

$$A \subseteq A \Rightarrow A \subseteq \emptyset \cup A$$

2. $A \cap X = A$

   Proof: Using the axiom of extensionality.

$$t \in A \cap X \Leftrightarrow (t \in A) \wedge (t \in X) \Rightarrow t \in A$$

$$t \in A \wedge A \subseteq X \Rightarrow t \in A \wedge t \in X \Rightarrow t \in A \cap X$$

3. $A \cup X = X$

   Proof: Using the axiom of extensionality.

$$t \in A \cup X \Leftrightarrow \begin{cases} t \in A, A \subseteq X \Rightarrow t \in X \\ t \in X \end{cases} \Rightarrow t \in X$$

$$t \in X \Rightarrow (t \in X) \vee (t \in A) \Leftrightarrow t \in A \cup X$$

4. $A \cap \emptyset = \emptyset$

   Proof: By reductio ad absurdum.

$\exists t \in A \cap \emptyset \Leftrightarrow (t \in A) \wedge (t \in \emptyset) \Rightarrow t \in \emptyset$ Contradiction!!

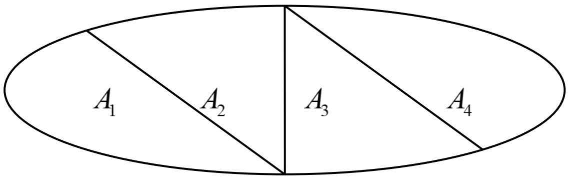
1.3. Partitions

Definition:

Given a set $A \subseteq X$, a **partition of A** is a family of sets $S = \{A_i, i \in I\}$, where $I \subseteq \mathbb{N}$ is a finite or infinite set called ***index set***, verifying that:

1. $A_i \subseteq A \wedge A_i \neq \emptyset$ (A_i *is not an empty subset of* A)
2. $A = \bigcup_{i \in I} A_i = \cup P(A)$ (A *results from the union of the sets* $A_i, i \in I$)
3. $A_i \cap A_j = \emptyset \forall i, j \in I$ (*The elements of* S *are disjointed in groups of two*)

Examples:

- 

- For the set $\mathbb{N}_7 = \{1,2,3,4,5,6,7\}$, $S = \{\{i\}, i \in \mathbb{N}_7\}$ is a partition. However, $S' = \{\mathbb{N}_j, j \in \mathbb{N}_7\}$ is not a partition because the elements of S' are not disjointed although the rest of the properties are fulfilled.
- Considering $A_1 = \{1,2,3,5,7,11,13\}, A_2 = \{9\}, A_3 = \{4,6,8,10,12\}$, $S = \{A_i, i \in \mathbb{N}_3\}$ is a partition in three parts of the set $\mathbb{N}_{13}$.

1.4. Sequences and strings

In general, a sequence is a sorted collection or list of elements. The natural numbers are the set of numbers that we usually use to define an order. To sort a set of elements, we have to assign a natural value to each element. This natural value indicates the order of the element in the set. If we assign the value 1, it will be the first element of the set. In contrast, if we assign the value 4, it will be the fourth element of the set.

If a is a sequence, its elements are denoted by $a_1,\ a_2,\ \dots\ a_n,\ \dots.$ and they are called ***terms of the sequence***.

The n[th] term denoted by a_n is called ***general term***. You can calculate any term in the sequence if you know the formula for a_n in terms of n.

Comments:

- Other notations are allowed for the sequences:
  - ✓ $\{a_n\} = \{a_n\}_{n=1}^{\infty}$ if the sequence is infinite, that is, sequences have infinite terms.
  - ✓ $\{a_n\} = \{a_n\}_{n=1}^{k}$ with $k \in \mathbb{N}$ for sequences with only k terms.
- Sometimes, instead of considering a_1 as the first term, a_0 is considered as the first term so $\{a_n\} = \{a_n\}_{n=0}^{\infty}$
- If we have a sequence that is composed of numbers $\{a_n\}, a_n \in \mathbb{R}$, we can denote the sum and the product of its elements as follows:

$$\sum_{n=1}^{\infty} a_n = a_1 + a_2 + \dots + a_n + \dots$$

$$\textstyle\sum_{k=1}^{n} a_k = a_1 + a_2 + \dots + a_n \qquad \prod_{n=1}^{\infty} a_n = a_1 \cdot a_2 \cdot \dots \cdot a_n \cdot \dots$$

$$\prod_{k=1}^{n} a_k = a_1 \cdot a_2 \cdot \dots \cdot a_n$$

Definitions:

A sequence $a = \{a_n\}$ is ***monotone***, if its terms are increasing $a_1 \le a_2 \le a_3 \le \dots \le a_n \le \dots$, or if its terms are decreasing $a_1 \ge a_2 \ge a_3 \ge \dots \ge a_n \ge \dots$

A sequence is $a = \{a_n\}$ is ***bounded*** if there is a finite positive real number M, $\exists M \in \mathbb{R}^+,\ M < \infty$, such that $|a_n| < M\ \forall n \in \mathbb{N}$

Examples:

- For the sequence $\{a_n\} = \{3 + (-1)^n\}$, the general term $a_n = 3 + (-1)^n$ allows us to calculate the rest, for example $a_1 = 3 - 1 = 2,\ a_2 = 3 + (-1)^2 = 4,\ a_3 = 3 + (-1)^3 = 2 \dots$

This sequence is not monotone, but it is bounded because we can select $M = 3$ fulfilling the definition.

- The sequence $1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ \dots$ is called Fibonacci sequence and its general term is $a_n = a_{n-1} + a_{n-2}$. This general term requires two values to be calculated, so we must start from the two given values, which are $a_1 = a_2 = 1$.

This sequence is monotone, but it is not bounded.

Definition:

Given the sequence $\{a_n\}$ defined by $n = m, m+1, m+2 \ldots$ and $n_1, n_2, n_3 \ldots$ is a strictly increasing sequence $(n_k < n_{k+1} \forall k)$, then the sequence formed from the elements $\{a_{n_k}\}$ is called ***subsequence*** of $\{a_n\}$.

Example:

- The sequence of the even numbers defined as $\{a_n = 2 \cdot n\}$ is clearly a subsequence of the natural numbers.
- Given the sequence $1,3,5,7$, the sequence $7,3$ is not a subsequence of the previous sequence because the order of the elements is not preserved. The subsequences must preserve the order with respect to the sequence from which is obtained.

Definition: *STRINGS*

Given a set X, a ***string over*** X is a finite sequence of elements of X.

Comments:

- Since a string is a sequence, the order is important: $aabbcc$ is a different string from $abcabc$.
- Repetitions can be specified with superscripts, for example: $aaabbbcc = a^3b^3c^2$
- A string with no elements is called *null string* and is denoted by λ.
- The set of all the strings over X is denoted by X^*.
- The length (cardinality) of a string is its number of elements. If α is a string, we can denote its cardinality by $|\alpha|$. For example,

$$\alpha = aabbc^3 \rightarrow |\alpha| = 7$$

- If α and β are strings over X, $\alpha\beta$ is other string over X called ***concatenation*** of α and β . This new string is composed of the string α followed by the elements of β. For example,

$$\alpha = a^2bcdd, \beta = e^3fg \rightarrow \alpha\beta = a^2bcd^2e^3fg$$

- The strings are also called words.

1.5. Cartesian product

Definitions:

Given two sets $A, B \subseteq X$, where X is considered as the universal set.

The ***cartesian product of A and B,*** denoted by $A \times B$, is the set formed by pairs (a, b) where $a \in A \wedge b \in B$, that is:

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

Notation*:*

The elements $(a, b) \in A \times B$ are called ***ordered pairs*** and they fulfill that $(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d$.

Comments:

- If A and B are finite, the cardinality of the cartesian product is equal to the product of the cardinalities of A and B: $|A \times B| = |A| \cdot |B|$
- The definition of cartesian product can be extended to more than two sets: If $n \in \mathbb{N}, n \geq 3$ and $A_1, A_2, \ldots, A_n \subseteq X$, the ***cartesian product of $A_1, A_2, \ldots, A_n$,*** denotated by $A_1 \times A_2 \times \ldots \times A_n$, is the set defined as follows:

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n): a_1 \in A_1 \wedge a_2 \in A_2 \wedge \ldots \wedge a_n \in A_n\}$$

Its elements are called ***n-tuples***, and similarly, they fulfill that $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \Leftrightarrow a_1 = b_1 \wedge a_2 = b_2 \wedge \ldots \wedge a_n = b_n$

Theorem:

Given three sets $A, B, C \subseteq X$ where X is considered the universal set, it is verified that:

1. $A \times \emptyset = \emptyset$
2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
3. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
4. $(A \cup B) \times C = (A \times C) \cup (B \times C)$
5. $(A \cap B) \times C = (A \times C) \cap (B \times C)$

Proof: Exercise

Examples:

1. Given $X = \{1,2,3,4,5,6,7\}, A = \{2,3,4\}$ and $B = \{4,5\}$, then:
    a. $A \times B = \{(2,4),(2,5),(3,4),(3,5),(4,4),(4,5)\}$
    b. $B \times A = \{(4,2),(4,3),(4,4),(5,2),(5,3),(5,4)\}$
    c. $B^2 = B \times B = \{(4,4),(4,5),(5,4),(5,5)\}$
    d. $B^3 = B \times B \times B = \{(a,b,c): a,b,c \in B\}, (4,5,5) \in B$
2. The cartesian product $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ is known as *real plane* in geometry.

2. Binary relations.

A relation is a condition that allows to compare pairs of elements on a set and check if these pairs of elements are or not related depending on some criteria.

Examples:

On the set $\mathbb{Z}$, we could define a relation that uses the following criteria:

Two integers are related if their difference returns an even number.

This condition would be represented as follows:

$$\forall (a,b) \in \mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2, aRb \Leftrightarrow b - a = 2 \cdot n, n \in \mathbb{Z}$$

Note that, in this case, the two integers will be **related** if both are even or odd numbers:

$$aRb \Leftrightarrow \begin{cases} a \wedge b \text{ even numbers} \\ a \wedge b \text{ odd numbers} \end{cases} \Leftrightarrow (a \wedge b \text{ even numbers}) \vee (a \wedge b \textit{ odd numbers})$$

$$R = \{(2n, 2m); n, m \in \mathbb{Z}\} \cup \{(2n+1, 2m+1); n, m \in \mathbb{Z}\} \subset \mathbb{Z} \times \mathbb{Z}$$

Two integers are **not related** when they have opposite parities (i.e., when one of them is even and the other is odd).

$$a \not{R} b \Leftrightarrow \begin{cases} a \text{ even number} \wedge b \text{ odd number} \\ a \text{ odd number} \wedge b \text{ even number} \end{cases} \Leftrightarrow (a \text{ even number} \wedge b \text{ odd number}) \vee (a \text{ odd number} \wedge b \text{ even number})$$

A relation R can also be shown as a table, which represents the relation of some elements to others. For example:

Student	*Year*
Alfredo	1º
Alicia	2º
Antonio	3º
Belén	2º
Carlos	1º
Esteban	4º
Rosa	3º

The table shows the relation between the students and the year in which they are enrolled.

Note that this table is just a set of ordered pairs where the first element of the ordered pair is related to the second one.

In this case a student will be **related** to the year in which he is enrolled, and this student will **not** be **related** to the rest of the years.

If $A = \{\text{Alfredo, Alicia, Antonio, Belén,Carlos, Estenban, Rosa}\}$ and $B = \{1º, 2º, 3º, 4º\}$, the set of ordered pairs, denoted as the relation R, is just a subset of $A \times B$: $R =$ $\{(\text{Alfredo,1º}), (\text{Alicia,2º}), (\text{Antonio,3º}), (\text{Belén,2º}), (\text{Carlos,1º}), (\text{Esteban,4º}), (\text{Rosa,3º})\} \subseteq A \times B$

2.1. Definitions

Definition:

For the subsets $A, B \subseteq X$, any subset of $A \times B$ is a *(binary)* ***relation*** of A on B.

Any subset of $A \times A = A^2$ is called *(binary)* ***relation on A.***

If $R \subseteq A \times B$ is a relation of A on B, it can be denoted by: $(a, b) \in R \Leftrightarrow aRb$

If $R \subseteq A \times B$ is a relation of A on B, the set $\{a|(a, b) \in R, \text{for some } b \in B\}$ can be called ***domain*** of the relation and the set $\{b|(a, b) \in R, \text{for some } a \in A\}$ can be called ***range*** of the relation.

Comment:

When the relation is represented by a table, the first column of the table is the domain and the second one is the range.

Example:

Based on the definition of a relation, we could define the relation of the first example through the following subset $\mathbb{Z}^2$:

$$R = \{(a, b): b - a = 2n, n \in \mathbb{Z}\} \subseteq \mathbb{Z}^2.$$

Therefore, we would write that $aRb \Leftrightarrow (a, b) \in R \subseteq \mathbb{Z}^2$

Suppose that we consider the set $A = \{a, b, c\}$ and we want to define a relation on A from the following subset $R = \{(a, b), (a, c), (b, a), (a, a)\} \subseteq A \times A = A^2$, given $A^2 = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}$.

We could say that $aRb, aRc, aRa, \text{and } bRa$ but $b\not{R}b, b\not{R}c, c\not{R}a, c\not{R}b, \text{and } c\not{R}c$.

2.2. Composition of relations and Inverse relation

Definition:

If S and R are two relations, $S \subset A \times B, R \subset B \times C$, the ***composition of relations*** is a relation denoted by $R \circ S$ and defined as follows:

$$R \circ S = \{(a, c); (\exists b)\big((a, b) \in S\big) \wedge \big((b, c) \in R\big)\} \subset A \times C$$

$$(a, c) \in R \circ S \Leftrightarrow (\exists b)(aSb \wedge bRc)$$

Comments:

Note that the path of the first relation S has to be contained in the domain of the second relation R, so that the two relations R and S can be defined through the form $R \circ S$.

Definition:

For each relation R of A on B, we can obtain other relation R^{-1}, of B on A. We have just to invert the order of the two terms as follows:

$(b, a) \in R^{-1} \subseteq B \times A \Leftrightarrow (a, b) \in R \subseteq A \times B.$

The new relation, R^{-1}, is called ***inverse relation*** of R and fulfills that $R^{-1} \circ R = A \times A$

2.3. Properties of relations

Definitions:

Given a relation R on A:

1. R is ***reflexive*** if all element $a \in A$ is related to itself $(a,a) \in R$, or in other words: $a \in A \rightarrow aRa$.
2. R is ***symmetric*** if it verifies that $(a,b) \in R \rightarrow (b,a) \in R$, or in other words: $aRb \rightarrow bRa$.
3. R is ***transitive*** if it verifies that $(a,b),(b,c) \in R \rightarrow (a,c) \in R$, or in other words: $aRb \wedge bRc \rightarrow aRc$.
4. R is ***antisymmetric*** if it verifies that $(a,b) \in R \wedge (b,a) \in R \rightarrow a = b$, or in other words: $aRb \wedge a \neq b \rightarrow bRa$.

Comments:

- Note that a relation cannot be simultaneously symmetric and antisymmetric.
- Other possible definition for the antisymmetric relation is:

$$R \text{ antisymmetric} \Leftrightarrow \forall (a,b) \in R, a \neq b \rightarrow (b,a) \notin R$$

- From these properties, we can define two types of relations on a set: equivalence relations and partial orders.

Examples:

Given $A = \{1,2,3,4\}$.

The relation $R_1 = \{(1,2),(2,1),(1,1)\}$ on A is symmetric, but it is neither reflexive, nor transitive.

The relation $R_2 = \{(1,2),(2,1),(1,3),(3,1)\}$ on A is symmetric, but it is neither reflexive, nor transitive.

The relation $R_3 = \{(1,1),(2,2),(3,3),(4,4)\}$ on A is reflexive, symmetric and transitive. The transitive property could not be obvious, but you can realize that there is no element in conflict the definition. In fact, this corresponds to the identity relation in A.

The relation $R_4 = \{(1,1),(1,2),(1,3),(1,4),(2,2),(2,3),(2,4),(3,3),(3,4),(4,4)\}$ on A is reflexive, transitive, and antisymmetric.

Note that R_4 can be also defined by $aRb \Leftrightarrow a \leq b, \forall (a,b) \in A^2$

2.4. Equivalence relations

Definitions:

Given an arbitrary set A, R is an ***equivalence relation*** on A , if it fulfills the following properties:

1. Reflexive $\forall a \in A aRa$
2. Symmetric $\forall a,b \in A aRb \leftrightarrow bRa$
3. Transitive $\forall a,b,c \in A, aRb \wedge bRc \rightarrow aRc$

Given an equivalence relation on a set A and an element $a \in A$, the ***equivalence class*** is composed of the set of elements belonging to A which are related to the element $a \in A$.

$$[a] = \{b \in A, aRb\}$$

The ***quotient set*** $A/R = \{[a], a \in A\}$ is the set composed of all the equivalence classes that are defined by a relation R on a set A.

Theorem:

If R is an equivalence relation on A $(R \subseteq A \times A)$.

The quotient set $A/R = \{[a], a \in A\}$ of the equivalence classes defines a partition of the set A. In other words, $A/R = \{[a], a \in A\}$ verifies that:

1) $\bigcup_{[a]\in A/R} [a] = A$

2) $\forall a, b \in A, [a] \neq [b] (a \not R b) \Rightarrow [a] \cap [b] = \emptyset$

Proof: *(Exercise)*

Comments:

Note that if R is an equivalence relation on A, whenever we take two arbitrary elements, we will obtain one of the following alternative solutions:

$$\begin{cases} aRb \leftrightarrow [a] = [b] \\ a\not R b \leftrightarrow [a] \cap [b] = \emptyset \end{cases}$$

Example:

Given the relation R on $\mathbb{Z}$ defined by $\forall (a, b) \in \mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2, aRb \Leftrightarrow b - a \text{ even number}$.

We will check if R is an equivalence relation verifying if it fulfills the reflexive, symmetric, and transitive properties:

1. Reflexive: $\forall a \in \mathbb{Z},\ a - a = 0 = 2 \cdot 0 \rightarrow aRa$

(We can consider the zero as an even number)

2. Symmetric:$\forall\ a, b \in \mathbb{Z},\ aRb \rightarrow a - b \text{ even number } (a - b = 2 \cdot n) \rightarrow$

$$\rightarrow b - a \text{ even number } \big(b - a = 2 \cdot (-n)\big) \leftrightarrow bRa$$

3. Transitive:

$$\forall a, b, c \in \mathbb{Z}, \quad aRb \wedge bRc \leftrightarrow (a - b), (b - c) \text{ even numbers} \rightarrow$$
$$\rightarrow (a - b) + (b - c) \text{ even number} \rightarrow$$
$$\rightarrow (a - c) \text{ even number} \leftrightarrow aRb$$

Since the previous relation R is reflexive, symmetric, and transitive, we can say that R is an equivalence relation.

Now, let us see what its equivalence classes are and whether these equivalence classes form a partition of $\mathbb{Z}$.

Given $0,1 \in \mathbb{Z}$, the equivalence classes of these two elements belong to R by:

$$[0] = \{a \in \mathbb{Z} |\ 0Ra\}$$
$$= \{a \in \mathbb{Z} |\ a - 0 \textit{ is an even number}\}$$
$$= \{a \in \mathbb{Z} |\ a = 2n, n \in \mathbb{Z}\}$$
$$= \{\dots, -4, -2, 0, 2, 4, 6, \dots\}$$

$$[1] = \{a \in \mathbb{Z} |\ 1Ra\}$$
$$= \{a \in \mathbb{Z} |\ a - 1 \textit{ is an even number}\}$$
$$= \{a \in \mathbb{Z} |\ a - 1 = 2n, n \in \mathbb{Z}\}$$
$$= \{a \in \mathbb{Z} |\ a = 2n + 1, n \in \mathbb{Z}\}$$
$$= \{\dots, -1, 0, 1, 3, \dots\}$$

Each element of $\mathbb{Z}$ is in one of these equivalence classes, so it is even or odd.

The union of the two equivalence classes is $\mathbb{Z}$:

$$\mathbb{Z} = [0] \cup [1] = \{a | a = 2n, n \in \mathbb{Z}\} \cup \{a | a = 2n+1, n \in \mathbb{Z}\} = \{a | (a = 2n) \vee (a = 2n+1), n \in \mathbb{Z}\}$$

Moreover, if an integer is even, it cannot be odd*. Therefore, the intersection of the equivalence classes is the empty set $[0] \cap [1] = \emptyset$.

**Suppose that there is an element* a *of* $\mathbb{Z}$ *that was simultaneously even and odd.*

$$\left.\begin{array}{l} a \text{ even number} \rightarrow a = 2n \\ a \text{ odd number} \rightarrow a = 2n+1 \end{array}\right\} \rightarrow 2n = 2n+1 \rightarrow 0 = 1 ¡!$$

There would be a contradiction since 0 and 1 are different numbers.

This proves that a number cannot be simultaneously even and odd. If there was such a number, we would have to accept that 0=1 and this is false.

Therefore, we can also verify that $[0] \cap [1] = \emptyset$.

Finally, we can conclude that $\mathbb{Z}|_R = \{[0], [1]\}$ is a partition of $\mathbb{Z}$:

1. $[0] \cup [1] = \mathbb{Z}$
2. $[0] \cap [1] = \emptyset$

Theorem:

Given $P = \{A_i, i \in I\}$, which is partition of the set A .

The relation $R \subseteq A \times A$ defined by:

$$aRb \leftrightarrow \exists i \in I, a, b \in A_i$$

is an equivalence relation on A, its quotient set is P, and its equivalence classes are in the form $[a] = A_i$ if $a \in A_i$.

Proof

Let us prove that the relation $R \subseteq A \times A$ defined by $aRb \leftrightarrow \exists i \in I, a, b \in A_i$ is an equivalence relation:

1. Reflexive:

$$\forall a \in A \xrightarrow[P=\{A_i\}_{i\in I} \text{ partition}]{} a \in \bigcup_{i \in I} A_i \longrightarrow \exists i, a \in A_i \longrightarrow aRa$$

2. Symmetric:

$$\forall a, b \in A aRb \rightarrow \exists i \in I a, b \in A_i \rightarrow \exists i \in I b, a \in A_i \rightarrow bRa$$

3. Transitive:

$$\forall a, b, c \in A, aRb \wedge bRc \leftrightarrow \exists i \in I, a, b \in A_i \wedge \exists j \in I, b, c \in A_j$$

$$\rightarrow b \in A_i \cap A_j \underset{P=\{A_i\}_{i\in I} \text{ is a partition}}{=} \begin{cases} \emptyset & i \neq j \\ A_i = A_j & i = j \end{cases}$$

$$\xrightarrow{A_i \cap A_j \neq \emptyset \rightarrow i = j} i \in I, a, b, c \in A_i = A_j$$

$$\rightarrow \exists i \in I, a, c \in A_i \leftrightarrow aRc$$

Therefore, the previous relation is an equivalence relation.

Now, let us check the classes of the correspondent quotient set:

Suppose $a \in A$ and $i \in I$ is the index such that $a \in A_i$.

By definition $bRa \leftrightarrow b \in A_i$, so $[a] = \{b \in A, aRb\} = \{b \in A, b \in A_i\} = A_i$ q.e.d.

Comments

The last two theorems allow us to state that the partitions of a set and the equivalence relations of a set are the same. We can define as many partitions in a set as equivalence relations there are in that set.

2.5. Partial orders

Definitions:

Given an arbitrary set A, a relation R is a ***partial order*** on A, if it verifies the following properties:

1. Reflexive $\forall a \in A aRa$
2. Antisymmetric $\forall a, b \in A aRb \wedge bRa \rightarrow a = b$
3. Transitive $\forall a, b, c \in A, aRb \wedge bRc \rightarrow aRc$

A partial order R on A is also a **total** or **linear order** if it verifies that any two elements of the set are related by R:

$$\forall a, b \in A \rightarrow aRb \vee bRa$$

In a total order, all the elements can be compared. In contrast, in a partial order, there may be pairs of elements that cannot be compared.

Example:

Let us define on $\mathbb{N}$ the '**divides**' relation denoted by $a|b$, a 'divides' b, $a|b \leftrightarrow \exists n \in \mathbb{N}: b = a \cdot n$. In other words, a 'divides b if the remainder of dividing b by a is zero:

$$\forall (a, b) \in \mathbb{N} \times \mathbb{N} = \mathbb{N}^2, aRb \leftrightarrow a|b \leftrightarrow \exists n \in \mathbb{N}: b = a \cdot n$$

Let us check that it is a partial order:

1. Reflexive $\forall a \in \mathbb{N},\ a = a \cdot 1 \rightarrow a|a \rightarrow aRa$
2. Antisymmetric

$$\forall a, b \in \mathbb{N} aRb \wedge bRa \rightarrow \begin{cases} a|b \\ b|a \end{cases}$$

$$\rightarrow \exists n, m \in \mathbb{N}: \begin{cases} a = b \cdot n \\ b = a \cdot m \end{cases}$$

$$\rightarrow a = a \cdot m \cdot n \wedge n, m \in \mathbb{N} \rightarrow m = n = 1 \rightarrow a = b$$

3. Transitive

$$\forall a, b, c \in \mathbb{N}, aRb \wedge bRc \rightarrow \begin{cases} a|b \\ b|c \end{cases} \rightarrow \exists n, m \in \mathbb{N}: \begin{cases} a = b \cdot n \\ b = c \cdot m \end{cases} \rightarrow a = c \cdot m \cdot n \wedge n \cdot m \in \mathbb{N} \rightarrow aRc$$

Note that this relation is a partial order, but it is not a total order. For example, 7 does not divide 3 and 3 does not divide 7. These two elements cannot be compared.

3. Functions

A function is a rule that associates the elements of a set to the element of another set. Each element of the first set is associated to only one element of the second set.

3.1. Definitions

Given two non-empty sets A and B, a ***function f from A to B,*** denoted by $f: A \to B$, is a relation of A on B verifying that each element of the set A is present exactly once as the first component of an ordered pair:

$$\forall a \in A, (a, b), (a, b') \in f \to b = b'$$

A is the ***domain*** of the function f and B is the ***codomain.***

Sometimes, it is denoted by $A = Dom(f)$.

We usually write $f(a) = b$ when (a, b) is an ordered pair of the function f. Therefore, the previous condition is denoted by:

$$\forall a \in A, f(a) = b \wedge f(a) = b' \to b = b'.$$

If $f(a) = b$, b is known as the ***image of a by f*** and a is the ***preimage of b.***

The set of images by f, denoted by $f(A)$, is called ***range of f.***

$$f(A) = \{f(a): a \in A\} = Im(f)$$

$$b \in f(A) = Im(f) \subseteq B \Leftrightarrow (\exists a \in A)(f(a) = b)$$

Comments:

- ✓ Other way of denoting the condition that a relation has to fulfill to be a function would be:

$$f: A \to B \text{ Function} \Leftrightarrow (\forall a \in A)\left((\exists! b \in f(A))(f(a) = b)\right)$$

- ✓ Remember that a function is a subset of $A \times B$, denoted by:

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

Examples:

- (The identity function) Given a set A, Id_A is a function, because if $(a, b), (a, b') \in Id_A$ then $a = b$ y $a = b'$, then b=b'. Therefore, the identity relation is also a function.
- The divides relation $| \in \mathbb{Z}^2$ is not a function because an integer can divide more than one number. For example, $(2,4) \in |$ and $(2,10) \in |$, but $4 \neq 10$.
- The relation 'mother' that relates each person to their mother is a function because every human has only one mother.

3.2. Types of functions: Injective functions, surjective functions, and bijective functions

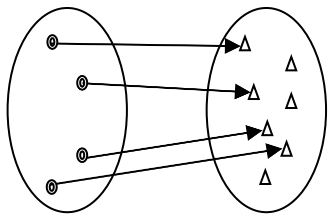
Definition:

A function $f: A \to B$ is called ***injective*** if two different elements of the domain have different images.

$$f: A \to B \text{ ***Injective function*** } \Leftrightarrow \forall a, a' \in A, a \neq a' \Rightarrow f(a) \neq f(a')$$

Or equivalently, two equal elements of the image set have the same preimages in the domain.

$$f: A \to B \text{ ***Injective function*** } \Leftrightarrow \forall b, b' \in f(A) \subseteq B, b = f(a) = f(a') = b' \Rightarrow a = a'$$



Comments:

- Other way to denote the condition to verify that a function is injective would be:

$$f: A \to B \text{ ***Injective function*** } \Leftrightarrow (\forall b \in f(A)), ((\exists!\, a \in A), (f(a) = b))$$

Every element of $Im(f) = f(A)$ has only one preimage by f in A

- If $f: A \to B$ is an injective function and $A, B \subseteq X$ are two finite sets, then it must be fulfilled that:

$$|A| \leq |B|$$

Theorem:

Given $f: A \to B$ with $A_1, A_2 \subseteq A$, then:

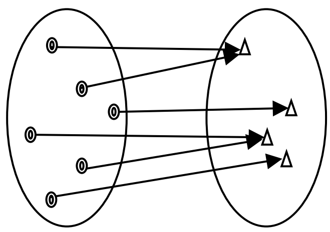
1. $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$

2. $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$ and if $f: A \to B$ is injective $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$

Definition:

A function $f: A \to B$ is ***onto or surjective*** if $f(A) = B$. That means that every element of the codomain has at least one preimage by f. Therefore:

$$f: A \to B \text{ ***Surjective function*** } \Leftrightarrow (\forall b \in B)((\exists a \in A)(f(a) = b))$$



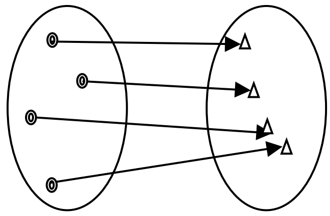
Comments:

- If $A, B \subseteq X$ are two finite sets, $f: A \to B$ must fulfill the following condition to be a surjective function: $|A| \geq |B|$

Definition:

A function $f: A \to B$ is ***bijective*** if it is injective and surjective. That means that every element of the codomain has only one preimage by f. Therefore:

$$f: A \to B \text{ ***Bijective function*** } \Leftrightarrow (\forall b \in B)((\exists!\, a \in A)(f(a) = b))$$



Comments:

- If $A, B \subseteq X$ are two finite sets, $f: A \to B$ must fulfill the following condition to be a bijective function: $|A| \leq |B| \wedge |A| \geq |B| \Rightarrow |A| = |B|$.

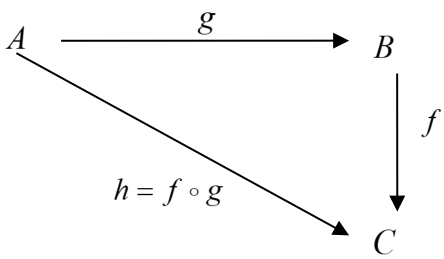
3.3. Composition of functions

Definition:

Given two functions $g: A \to B$ and $f: B \to C$, we defined the ***composite function of*** g ***and*** f, denoted by $f \circ g$, as the function $f \circ g: A \to C$, which based on the composition of relations is expressed as follows:

$$\begin{aligned} f \circ g &= \{(a,c): (\exists b \in B)\big((a,b) \in g \wedge (b,c) \in f\big)\} \\ &= \{(a,c): (\exists b \in B)(g(a) = b \wedge f(b) = c)\} \\ &= \{(a,c): (f\big(g(a)\big) = c\} \end{aligned}$$

We usually denoted it by $f \circ g(a) = f(g(a))$.



Comments:

- In fact, $f \circ g$ is a function that satisfy the definition:
  If $f \circ g(a) = b \wedge f \circ g(a) = b'$ then we obtain that $b = f\big(g(a)\big) = b'$
- To the definition be meaningful, $g(A) \subseteq B$. In other words, the image of g must be in the domain of f.
- The composition of functions is not commutative in general.
- If $f: A \to B$, then:
  a. $f \circ Id_A = f$.
  b. $Id_B \circ f = f$.
- Finally, we can note that the composition of functions is associative. If $g: A \to B$, $f: B \to C$ and $h: C \to D$, then $(h \circ f) \circ g = h \circ (f \circ g)$

3.4. Invertible function and Inverse function

Definition:

A function $f: A \to B$ is ***invertible***, whether an inverse relation $f^{-1}: B \to A$ is also a function. In this case, f^{-1} is called ***inverse function*** of f.

Comments:

- The inverse relation of a function can follows the form of: $f^{-1} = \{(f(a), a): a \in A\}$.
- If f is invertible, it fulfills that $A = Dom(f) = Im(f^{-1})$ and that $Dom(f^{-1}) = Im(f)$.

Proposal:

For the function $f: A \to B$, the following statements are equal:

1. f is injective.
2. For all $a, b \in A, a \neq b \Rightarrow f(a) \neq f(b)$.
3. f is invertible.

Proof *(Exercise)*

Comments

Note that if f is invertible, then $f = (f^{-1})^{-1}$, then f^{-1} is invertible (and injective for the previous proposal).

Many functions can be expressed as a composition of several basic functions.

In many cases, to determine if a function is injective, it shall be sufficient to analyze the basic functions that compose it. The same applies for determining if a function is surjective.

Theorem:

Given $g: A \to B$ and $f: B \to C$:

1. If g and f are injective, then $f \circ g$ is injective.
2. If g and f are surjective, then $f \circ g$ is surjective.
3. If g and f are bijective, then $f \circ g$ is bijective.

The opposite case is not true.

Proof *(Exercise)*

Theorem:

Given $g: A \to B$ and $f: B \to C$:

1. If $f \circ g$ is injective, then g is injective.
2. If $f \circ g$ is surjective, then f is surjective.

Proof *(Exercise)*

3.5. Some special functions

- If $A_1 \subseteq A$ and $f: A \to B$, $f|_{A_1}: A_1 \to B$ is the ***restriction of f to A,*** defined as:

$$f|_{A_1}(a) = f(a) \forall a \in A_1.$$

- If $A_1 \subseteq A f: A_1 \to B$ and $g: A \to B$ is other function fulfilling that $g(a) = f(a) \forall a \in A_1$, then g is an ***extension of f to A.***

- If $A_1 \subseteq A$, the function $Id_A|_{A_1}$ is called ***inclusion of A_1 in*** A. The inclusion is an injective function, but it is not a surjective function if $A_1 \subset A$.

- For any non-empty set $A, B \subseteq X$, any function defined as $f: A \times A \to B$ is a ***binary operation*** on A. Furthermore, if $B \subseteq A$, then A is ***closed*** under the operation f.

References

R. Johnsonbaugh, "Discrete mathematics". Prentice Hall, 1997.

W. K. Grassmann and J.P. Tremblay, "Logic and discrete mathematics : a computer science perspective". Prentice Hall, 1996.