Chapter I: Logic, Sets and Relations

B. AMARI, bedrane.amari@g.enp.edu.dz

01/10/2024

Teaching content

1. Logic
   - Mathematical propositions
   - Quantifiers
   - Types of mathematical reasoning
2. Sets
   - Operations for Sets
   - Properties
   - Application
3. Relations
   - Equivalence relation
   - Order relation
   - Function
4. Practices
5. References

Logic

- Logic is the discipline – the foundations of which were laid down by Aristotle – which study the methods and principles of reasoning.
- In logic, *statement* is a declarative sentence that is either true or false, but not both. The key to constructing a good logical statement is that there must be no ambiguity. To be a statement, a sentence must be true or false.

Statement

Statement

statement is a sentence that is either true or false.
In logic, lower case letters are often used to represent statements such as p, q or r .

The following are statements :

- Zero times any real number is zero.
- All birds can fly. (This is a false statement. How can you establish that ?)

The following are not statements :

- Come here.
- Who are you ?
- I am lying right now. (This is a paradox).

Negation of statement

Negation

The negation of a statement is a statement that has the opposite truth value of the original statement.
Notation : $\overline{P}$ or $\neg P$ (read : "the negation of p " or "not p")

- If p is true, $\neg p$ is false.
- If p is false, $\neg p$ is true.

p	$\neg p$
T	**F**
F	**T**

Figure – Truth Table of the operator « not »

Examples of Negation

Negation of statement ?

- The car is red.

$\rightsquigarrow$ The car is not red.

- Homework is not due today.

$\rightsquigarrow$ Homework is due today.

- All birds can fly.

$\rightsquigarrow$ There is some birds who can't fly.

- $x + 2\pi > 3.$

$\rightsquigarrow$ $x + 2\pi \leqslant 3.$

- A logical operator (or connective) on mathematical statements is a word or combination of words that combines one or more mathematical statements to make a new mathematical statement.
- A compound statement is a statement that contains one or more operators. Because some operators are used so frequently in logic and mathematics, we give them names and use special symbols to represent them.

The universal quantification

The universal quantification of $P(x)$ is the proposition in any of the following forms :

- $P(x)$ is true for all values of x.
- For all x , $P(x)$.
- For each x , $P(x)$.
- For every x , $P(x)$.
- Given any x , $P(x)$.

All of them are symbolically denoted by $\forall x,\ P(x)$, which is pronounced as " for all x, $P(x)$".

The symbol $\forall$ is called the universal quantifier, and can be extended to several variables.

▷ the negation of $\forall$ is $\exists$.

The existential quantification

The existential quantification of $P(x)$ takes one of these forms :

- ▷ There exists an x such that $P(x)$.
- ▷ For some x, $P(x)$.
- ▷ There is some x such that $P(x)$.

We write, in symbol, $\exists x$, $P(x)$, which is pronounced as " There exists x such that $P(x)$."

The symbol $\exists$ is called the existential quantifier. It can be extended to several variables.
$\exists!$ means that there exist a unique.
▷ the negation of $\exists$ is $\forall$.

Conjunction

The conjunction of the statements P and Q is the statement "P and Q" and its denoted by $P \wedge Q$. The statement $P \wedge Q$ is true only when both P and Q are true.

$$P \wedge Q$$

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

Figure – Truth Table of « and »

Conjunction

Conjunction example

π lies between 3 and 4, $3 < \pi < 4$, $\pi > 3$ and $\pi < 4$;

$\pi > 3$	$\pi < 4$	$3 < \pi < 4$
T	T	**T**
T	F	**F**
F	T	**F**
F	F	**F**

Figure – Truth Table of « and »

Disjunction

The disjunction of the statements P and Q is the statement "P or Q" and its denoted by $P \vee Q$. The statement $P \vee Q$ is true only when at least one of P or Q is true.

$$p \vee q$$

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

Figure – Truth Table of « or »

Disjunction

Disjunction example

For integer a and b, $ab = 0$ if $a = 0$ or $b = 0$;

$ab = 0$	$a = 0$	$b = 0$
T	T	F
T	F	T
F	F	F
T	T	T

Figure – Truth Table of « or »

A compound statement

$$S = (p \wedge q) \wedge \neg r$$

p	q	r	$S_1 = (p \wedge q)$	$S_2 = \neg r$	S=$S_1 \wedge S_2$
T	T	T	T	F	**F**
T	T	F	T	T	**T**
T	F	T	F	F	**F**
T	F	F	F	T	**F**
F	T	T	F	F	**F**
F	T	F	F	T	**F**
F	F	T	F	F	**F**
F	F	F	F	T	**F**

Figure – Truth table of S

Logically Equivalent Statements)

Two statements are logically equivalent if they have the same truth table. It is denoted by $\equiv$.

Consider the two following statements :

- $S_1 = p$
- $S_2 = \neg(\neg p)$

p	$\neg p$	S_1	S_2
T	F	**T**	**T**
F	T	**F**	**F**

$$S_1 \equiv S_2$$

Associativity, commutativity and distributivity

Associativity

- $(p \vee q) \vee r$ and $q \vee (p \vee r)$ are equivalent.
- $(p \wedge q) \wedge r$ and $q \wedge (p \wedge r)$ are equivalent.

commutativity

- $p \vee q$ and $q \vee p$ are equivalent.
- $p \wedge q$ and $q \wedge p$ are equivalent.

distributivity

- $r \vee (p \wedge q)$ and $((r \vee p) \wedge (r \vee q))$ are equivalent.
- $r \wedge (p \vee q)$ and $((r \wedge p) \vee (r \wedge q))$ are equivalent.

Morgan's law

Morgan's law

- $\neg(p \wedge q)$ and $(\neg p \vee \neg q)$ are equivalent.
- $\neg(p \vee q)$ and $(\neg p \wedge \neg q)$ are equivalent.

Proof. ?

Implication

Implication

The implication or conditional is the statement “If P then Q” and is denoted by $P \Rightarrow Q$.
The statement $P \Rightarrow Q$ is often read as “P implies Q, and $P \Rightarrow Q$ is false only when P is true and Q is false.

P	Q	$P \Rightarrow Q$
T	T	**T**
T	F	**F**
F	T	**T**
F	F	**T**

P is the **hypotheses**, and Q the **conclusion**.

Implication

Negation

$p \Rightarrow q$ is equivalent to $\neg p \vee q$.

Converse, contrapositive

The converse of $P \Rightarrow Q$is the statement $Q \Rightarrow P$. The contrapositive of $P \Rightarrow Q$ is the statement $\neg Q \Rightarrow \neg P$.

Implication

Implication

For an integer n, $P(n) : n > 3$ and $Q(n) : n > 0$. So $P(n) \Rightarrow Q(n)$.

P	Q	$P \Rightarrow Q$
T	T	**T**
T	F	**F**
F	T	**T**
F	F	**T**

Equivalence

Equivalence

The equivalence or bi-conditional is the statement " P if only if Q" and is denoted by $P \Leftrightarrow Q$.
The statement $P \Leftrightarrow Q$ is often read as "P equivalent Q, and $P \Leftrightarrow Q$ is true if and only if P and Q have the same truth value.

P	Q	$P \Leftrightarrow Q$
T	T	**T**
T	F	**F**
F	T	**F**
F	F	**T**

$P \Leftrightarrow Q$ and $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ are equivalents.

Summary of Negations

The negations of common logical expressions are summarized in the following table.

Statement	Negation
P and Q	$\neg P$ or $\neg Q$
P or Q	$\neg P$ and $\neg Q$
P $\Rightarrow$ Q	P and $\neg Q$
P $\Leftrightarrow$ Q	(P and $\neg Q$) or (Q and $\neg P$)
$\forall n, P(n)$	$\exists n$ such that not(P(n))
$\exists n$ such that P(n)	$\forall n$, not (P(n))

Direct Proofs

To prove an *if, then* statement directly, start the proof by assuming your **hypotheses** (the statements after the if) and use definitions, logic, and previously proved results to reach the desired **conclusion** (the statement after the then).

As an example, we'll prove the following theorem.

If a and b are even integers, then $a + b$ is even.

Proof. Suppose a and b are even integers. This means $a = 2k_1$ and $b = 2k_2$ for some integers k_1 and k_2. Then $a + b = 2k_1 + 2k_2 = 2(k_1 + k_2)$. Let $k = k_1 + k_2$. Then k is an integer and $a + b = 2k$. Thus, $a + b$ is even.

Proof by Cases

Consider the following theorem :

The product of two consecutive integers is even.

This can be reworded : If n is an integer, then $n(n+1)$ is even.
Proof. Suppose n is an integer. Then n is either even or odd.
Case 1 : Suppose n is even. Then $n = 2k$ for some integer k. This means that $n(n+1) = (2k)(n+1) = 2[k(n+1)]$. We know that $k(n+1)$ is an integer. Thus, $n(n+1)$ is even in the case that n is even.
Case 2 : Suppose instead that n is odd. Then $n = 2k+1$ for some integer k. This means that
$n(n+1) = n(2k+1+1) = n(2k+2) = 2[n(k+1)]$. We know that $n(k+1)$ is an integer. Thus, $n(n+1)$ is even in the case that n is odd.

Contrapositive

Recall that the statement$P \Rightarrow Q$ has the same truth value as its contrapositive $(\neg Q) \Rightarrow (\neg P)$. Therefore, if you wish to prove that $P \Rightarrow Q$ is true, you may prove instead that its contrapositive is true. This is called proof by contrapositive : you suppose not Q as your hypothesis and show that, under that assumption, not P is true.

Contrapositive

Suppose n is an integer. If n^2 is even, then n is even.

Proof. Suppose n is an integer that is not even. That is, suppose n is odd. Then $n = 2k + 1$ for some integer k, and we have $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Since $2k^2 + 2k$ is an integer, this means that n^2 is odd. Thus, if n^2 is even, it must be the case that n is even.

Contrapositive

Let n be an integer. If $n^2 + 2n < 0$, then $n < 0$.

Proof. Let n be an integer and suppose $n \geqslant 0$.
We know that $n^2 \geqslant 0$. By elementary properties of the integers, we then have

$$n^2 + 2n \geqslant 0 + 2n = 2n \geqslant 0$$

. Thus, if $n^2 + 2n < 0$, it must be the case that $n < 0$.

Contradiction

In a proof by contradiction, we use the fact that a statement and its negation have opposite truth values. To prove that P is true, suppose instead that not(P) is true and apply logic, definitions, and previous results to arrive at a conclusion you know to be false. Then you may conclude that not(P) must be FALSE and thus P must be TRUE.

Contradiction

No integer is both even and odd.

Proof. Suppose there is an integer n that is both even and odd. Since n is even, $n = 2k$ for some integer k. Since n is also odd, $n = 2k' + 1$ for some integer k'. Then by the elementary properties of integers, we have $2k = 2k' + 1; 2k - 2k' = 1; 2(k - k') = 1$. But this implies that 2 divides 1, which we know is not true since it contradicts hypothesis. Thus, no integer n is both even and odd.

Induction

The induction principle

Suppose that $P(n)$ is a statement involving a general positive integer n. Then $P(n)$ is true for all positive integers $1, 2, 3, \ldots$ if

(*i*) $P(1)$ is true, and

(*ii*) $P(k) \Rightarrow P(k+1)$ for all positive integers k.

Induction

For all positive integers n we have the inequality $n \leqslant 2^n$

Proof. $P(n)$ is the statement $n \leqslant 2^n$

(*i*) The statement $P(1)$ says that $1 \leqslant 2$ which is certainly true. This is called the **base case**.

(*ii*) The second statement that is needed is called the **inductive step**. $P(k) \Rightarrow P(k+1)$ for all positive integers k. $P(k)$ is often referred to as the **inductive hypothesis**. We write out the formal proof as follows.

Induction

We use induction on n.

Base case : For $n = 1, 2^n = 2$ and so, since $1 \leqslant 2, n \leqslant 2^n$.

Inductive step : Suppose now as inductive hypothesis that $k \leqslant 2^k$ for a positive integer k. Then $2^{k+1} = 2 \times 2^k \geqslant 2k$ (by inductive hypothesis)$= k + k \geqslant k + 1$ and so 2^{k+1} as required.

Conclusion : Hence, by induction, $n \leqslant 2^n$ for all positive integers n.

Sets (definitions)

Cantor's Concept of a Set

A *set* S is any collection of definite, distinguishable objects of our intuition or of our intellect to be conceived as a whole. The objects are called the *elements* or *members* of S.

Membership relation

$x \in A$ means that the object x is a member of the set A. If x is not a member of A then $x \notin A$. $x_1, x_2, \ldots, x_n \in A$ is shorthand for $x_1 \in A \wedge x_2 \in A \wedge \cdots \wedge x_n \in A$.

Empty set : $\{x \in A \mid x \neq x\}$ for any set A is the set with no elements, symbolized by $\emptyset$.

Subset

Subset

If every element of a set A is also an element of B, then we say that A is a *subset* of B, and write $A \subseteq B$. If A is not a subset of B we write $A \nsubseteq B$. If $A \subseteq B$ but $A \neq B$, we write $A \subsetneq B$ and say that A is a *proper subset* of B.

Every set is a subset of itself, and $\emptyset$ is a subset of every set. The set of even numbers is a subset of the set of natural numbers. Also, $\{a, b\} \subseteq \{a, b, c\}$. But $\{a, b, e\}$ is not a subset of $\{a, b, c\}$.

Proposition

$A = B$ iff both $A \subseteq B$ and $B \subseteq A$.

Power Set

Subset

The set consisting of all subsets of a set A is called the *power set of* A, written $\mathcal{P}(\mathcal{A})$.

$$\mathcal{P}(\mathcal{A}) = \{B : B \subseteq A\}$$

What are all the possible subsets of $\{a, b, c\}$? They are : $\emptyset$, $\{a\}$, $\{b\}$, $\{c\}$, $\{a, b\}$, $\{a, c\}$, $\{b, c\}$, $\{a, b, c\}$. The set of all these subsets is $\mathcal{P}(\{a, b, c\})$:

$$\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$$

Some Important Sets

We will mostly be dealing with sets whose elements are mathematical objects. Four such sets are important enough to have specific names :

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

the set of natural numbers

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

the set of integers

$$\mathbb{Q} = \{\frac{m}{n}, m, n \in \mathbb{Q} \text{ and } n \neq 0\}$$

the set of rationals

$$\mathbb{R} = (-\infty, \infty)$$

the set of real numbers (the continuum)

Operations for Sets

Inclusion

If A and B are sets, then A is *included in* B iff each member of A is a member of B. Symbolized : $A \subseteq B$. We also say that A is a *subset* of B. Equivalently, B *includes* A, symbolized by $B \supseteq A$.

The set A is *properly included in* B (A is a *proper subset* of B / B *properly includes* A) iff $A \subseteq B$ and $A \neq B$.

Among the basic properties of the inclusion relation are

$$X \subseteq X;$$
$$X \subseteq Y \wedge Y \subseteq Z \Rightarrow X \subseteq Z;$$
$$X \subseteq Y \wedge Y \subseteq X \Rightarrow X = Y.$$

Operations for Sets

Union, intersection

Union

For sets A and B, the set of all objects which are members of either A or B. $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$.

intersection

For sets A and B, the set of all objects which are members of both A and B. $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.

Considering A_i for each $i \in I$, we may also use these abbreviations :

$$\bigcup_{i \in I} A_i = \bigcup \{A_i\} i \in I$$

$$\bigcap_{i \in I} A_i = \bigcap \{A_i\} i \in I$$

Operations for Sets

Union, intersection

Lemma

For every pair of sets A and B the following inclusions hold :

$$\emptyset \subseteq A \cap B \subseteq A \subseteq A \cup B.$$

Proof

Take $x \in \emptyset$. Since this is false, we can conclude $x \in A \cap B$ and so $\emptyset \subseteq A \cap B$. Now take $x \in A \cap B$. Then $x \in \{y \mid y \in A \text{ and } y \in B\}$ and so $x \in \{y \mid y \in A\} = A$ and thus $A \cap B \subseteq A$. Now take $x \in A$. Then we must have $x \in \{y \mid y \in A \text{ or } y \in B\} = A \cup B$. Then $A \subseteq A \cup B$.

Other notions

Disjoint $A \cap B = \emptyset$ for sets A and B.

Partition For a set X, a disjoint collection $\mathcal{A}$ of nonempty and distinct subsets of X such that each member of X is a member of some (exactly one) member of $\mathcal{A}$.

absolute complement of A : $A^c = \{x \mid x \notin A\}$, the set of all members which are not in A.

Difference of A and B :The *set difference* $A \setminus B$ is the set of all elements of A which are not also elements of B, i.e., $A \setminus B = \{x \in A \text{ and } x \notin B\}$.

Symmetric difference of A and B : $A \triangle B = (A \setminus B) \cup (B \setminus A)$, i.e., $\{x \in A \text{ and } x \notin B \text{ or } x \notin A \text{ and } x \in B\}$

Some important results

Theorem

For any subsets A, B, C of a set U the following equations are identities. Here A^c is an abbreviation for $U \setminus A$.

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

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

2. $A \cup B = B \cup A$.

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

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

3'. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

4. $A \cup \emptyset = A$.

4'. $A \cap U = A$.

5. $A \cup A^c = U$

5'. $A \cap A^c = \emptyset$.

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

Proof. Assume $x \in A \cup (B \cap C)$. Then $x \in A$ or $x \in B \cap C$. If $x \in A$ then $x \in A \cup B$ and $x \in A \cup C$ and so $x \in (A \cup B) \cap (A \cup C)$. Otherwise if $x \in B \cap C$ then $x \in B$ and $x \in C$. Since $x \in B$ we have $x \in A \cup B$. Since $x \in C$ we have $x \in A \cup C$. Then $x \in (A \cup B) \cap (A \cup C)$ and therefore $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.
Now assume $x \in (A \cup B) \cap (A \cup C)$. Then $x \in A \cup B$ and $x \in A \cup C$. Since $x \in A \cup B$ we have $x \in A$ or $x \in B$. If $x \in A$ then $x \in A \cup (B \cap C)$. Otherwise if $x \in B$ then $x \in A \cup B$. Since $x \in A \cup C$ we also have that $x \in A$ or $x \in C$. If $x \in A$ then $x \in A \cup (B \cap C)$. Otherwise if $x \in C$ then since $x \in B$ we have $x \in B \cap C$ and so $x \in A \cup (B \cap C)$. Therefore $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. Hence $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Some important results

Theorem

For all subsets A and B of a set U, the following statements are valid. Here A^c is an abbreviation for $U \setminus A$.

6. If, for all A, $A \cup B = A$, then $B = \emptyset$.
6'. If, for all A, $A \cap B = A$ then $B = U$.
7,7'. If $A \cup B = U$ and $A \cap B = \emptyset$, then $B = A^c$.
8,8'. $(A^c)^c = A$.
9. $\emptyset^c = U$. 9'. $U^c = \emptyset$.
10. $A \cup A = A$ 10'. $A \cap A = A$.
11. $A \cup U = U$ 11'. $A \cap \emptyset = \emptyset$.
12. $A \cup (A \cap B) = A$. 12'. $A \cap (A \cup B) = A$.
13. $(A \cup B)^c = A^c \cap B^c$ 13'. $(A \cap B)^c = A^c \cup B^c$.

Example : Showing item

$(A \cap B)^c = A^c \cup B^c$.

Proof. Take $x \in (A \cap B)^c$. Then $x \notin A \cap B$. Then $x \notin A$ or $x \notin B$. Then $x \in A^c$ or $x \in B^c$ and so $x \in A^c \cup B^c$. Therefore $(A \cap B)^c \subseteq A^c \cup B^c$.
Now take $x \in A^c \cup B^c$. Then $x \in A^c$ or $x \in B^c$ and so $x \notin A$ or $x \notin B$. Then $x \notin A \cap B$ and so $x \in (A \cap B)^c$. Therefore $A^c \cup B^c \subseteq (A \cap B)^c$ and so $(A \cap B)^c = A^c \cup B^c$.

Theorem

The following statements about sets A and B are equivalent to one another.

I) $A \subseteq B$

II) $A \cap B = A$

III) $A \cup B = B$

Proof :

(I) implies (II). Assume $A \subseteq B$. Since, for all A and B, $A \cap B \subseteq A$, it is sufficient to prove that $A \subseteq A \cap B$. But if $x \in A$, then $x \in B$ and, hence, $x \in A \cap B$. Hence $A \subseteq A \cap B$.
(II) implies (III). Assume $A \cap B = A$. Then
$A \cup B = (A \cap B) \cup B = (A \cup B) \cap (B \cup B) = (A \cup B) \cap B = B$.
(III) implies (I). Assume $A \cup B = B$. Then this and the identity $A \subseteq A \cup B$ imply $A \subseteq B$.

Cartesian product

Cartesian product

Given sets A and B, their *Cartesian product* $A \times B$ is defined by

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

If $A = \{0, 1\}$, and $B = \{1, a, b\}$, then their product is

$$A \times B = \{(0, 1), (0, a), (0, b), (1, 1), (1, a), (1, b)\}.$$

Proposition

If A has n elements and B has m elements, then $A \times B$ has $n \cdot m$ elements.

Theory of equations for the algebra of sets

Equation formed : $\cup$, $\cap$, and $\overline{}$ on symbols $A_1, A_2, \ldots, A_n \in \mathcal{P}(U)$. $X \subset U$ constrained only by the equation.

Step I. Two sets are equal iff their symmetric difference is equal to $\emptyset$. Hence, an equation in X is equivalent to one whose righthand side is $\emptyset$.

Step II. An equation in X with righthand side $\emptyset$ is equivalent to one of the form

$$(A \cap X) \cup (B \cap \overline{X}) = \emptyset,$$

where A and B are free of X.

Theory of equations for the algebra of sets

Equation formed : $\cup$, $\cap$, and $\overline{}$ on symbols $A_1, A_2, \ldots, A_n \in \mathcal{P}(U)$.
$X \subset U$ constrained only by the equation.

Step III. The union of two sets is equal to $\emptyset$ iff each set is equal to $\emptyset$. Hence the equation in Step II is equivalent to the pair of simultaneous equations

$$A \cap X = \emptyset, B \cap \overline{X} = \emptyset.$$

Step IV. The above pair of equations, and hence the original equation, has a solution iff $B \subseteq \overline{A}$. In this event, any X, such that $B \subseteq X \subseteq \overline{A}$, is a solution.

Introduction

In mathematics the word "relation" is used in the sense of relationship. The following partial sentences (or predicates) are examples of relations : is less than, is included in, divides, is a member of, is congruent to, is the mother of. In this section the concept of a relation will be developed within the framework of set theory. The motivation for the forthcoming definition is this : A (binary) relation is used in connection with pairs of objects considered in a definite order.

Binary relation

A *binary relation* on a set A is a subset of A^2. If $\mathcal{R} \subseteq A^2$ is a binary relation on A and $x, y \in A$, we write $x\mathcal{R}y$ for $(x, y) \in \mathcal{R}$.

Special Properties of Relations

Reflexivity

A relation $\mathcal{R} \subseteq A^2$ is *reflexive* iff, for every $x \in A$, $x\mathcal{R}x$.

Transitivity

A relation $\mathcal{R} \subseteq A^2$ is *transitive* iff, whenever $x\mathcal{R}y$ and $y\mathcal{R}z$, then also $x\mathcal{R}z$.

Symmetry

A relation $\mathcal{R} \subseteq A^2$ is *symmetric* iff, whenever $x\mathcal{R}y$, then also $y\mathcal{R}x$.

Anti-symmetry

A relation $\mathcal{R} \subseteq A^2$ is *anti-symmetric* iff, whenever both $x\mathcal{R}y$ and $y\mathcal{R}x$, then $x = y$ (or, in other words : if $x \neq y$ then either $\neg x\mathcal{R}y$ or $\neg y\mathcal{R}x$.

Equivalence relation

Equivalence relation

A relation $\mathcal{R} \subseteq A^2$ that is reflexive, symmetric, and transitive is called an *equivalence relation*. Elements x and y of A are said to be *Equivalencerelation-equivalent* if $x\mathcal{R}y$.

Equivalence relation

Example

A nice example of equivalence relations comes from modular arithmetic. For any a, b, and $n \in \mathbb{Z}^+$, say that $a \equiv_n b$ iff dividing a by n gives the same remainder as dividing b by n. (Somewhat more symbolically : $a \equiv_n b$ iff, for some $k \in \mathbb{N}$, $a - b = kn$.) Now, $\equiv_n$ is an equivalence relation, for any n. And there are exactly n distinct equivalence classes generated by $\equiv_n$; that is, $\mathbb{N}/_{\equiv_n}$ has n elements. These are : the set of numbers divisible by n without remainder, i.e., $\mathcal{C}(0)_{\equiv_n}$; the set of numbers divisible by n with remainder 1, i.e., $\mathcal{C}(1)_{\equiv_n}$; ... ; and the set of numbers divisible by n with remainder $n-1$, i.e., $\mathcal{C}(n-1)_{\equiv_n}$.

Equivalence class, quotient set

Equivalence class, quotient set

Let $\mathcal{R} \subseteq A^2$ be an equivalence relation. For each $x \in A$, the *equivalence class* of x in A is the set, noted $\mathcal{C}(x)$ or $\overline{x}$, $\mathcal{C}(x)_{\mathcal{R}} = \{y \in A : x\mathcal{R}y\}$. The *quotient* set of A under $\mathcal{R}$ is $\mathcal{A}/R = \{\mathcal{C}(x)_R : x \in A\}$, i.e., the set of these equivalence classes.

Example

In the previous example, for $n = 3$ we have $a\mathcal{R}b \Leftrightarrow \exists k \in \mathbb{N} : a - b = 3k$; $\mathcal{C}(2)_{\mathcal{R}} = \{y \in \mathbb{N} : y\mathcal{R}2\} = \{y \in \mathbb{N} : y = 3k + 2, k \in \mathbb{N}\} = \{2, 5, 8, \cdots\}$. And $\mathbb{N}/\mathcal{R} = \{\mathcal{C}(x)_{\mathcal{R}} : x \in \mathbb{N}\} = \{\mathcal{C}(0), \mathcal{C}(1), \mathcal{C}(2)\}$.

Proposition

If $\mathcal{R} \subseteq A^2$ is an equivalence relation, then $x\mathcal{R}y$ iff $\mathcal{C}(x)_{\mathcal{R}} = \mathcal{C}(y)_{\mathcal{R}}$.

Let $\mathcal{R}$, on $\mathbb{R}$: $x\mathcal{R}y \Leftrightarrow x^2 - y^2 = x - y$

- $\mathcal{R}$ is an equivalence relation ;

  Reflexive : For $x \in \mathbb{R}, x^2 - x^2 = x - x$, thus $x\mathcal{R}x$,

  Transitive : For $x, y, z \in \mathbb{R}$, if $x\mathcal{R}y$ and $y\mathcal{R}z$ then $(x^2 - y^2 = x - y$ and $y^2 - z^2 = y - z) \Rightarrow x^2 - z^2 = x - z$, thus $x\mathcal{R}z$,

  Symmetric : For $x, y \in \mathbb{R}$, if $x\mathcal{R}y$ then $x^2 - y^2 = x - y \Rightarrow y^2 - x^2 = y - x$, thus $y\mathcal{R}x$,

- Let $x \in \bar{a}$ if $x\mathcal{R}a \Rightarrow x^2 - a^2 = x - a$, $\mathcal{R}$ is reflexive, so $x = a$ is a solution,
  $x^2 - a^2 = x - a \Rightarrow (x + a)(x - a) = x - a \Rightarrow x + a = 1, x = 1 - a$ is the other solution, $\bar{a} = \{a, 1 - a\}$.
- The quotient set $\mathbb{R}/\mathcal{R} = \{a \in \mathbb{R} : \{a, 1 - a\}\}$

Order introduction

- Many of our comparisons involve describing some objects as being "less than", "equal to", or "greater than" other objects, in a certain respect. These involve *order* relations.
- But there are different kinds of order relations. For instance, some require that any two objects be comparable, others don't. Some include identity (like $\leqslant$) and some exclude it (like $<$).

Kinds of order

Preorder

A relation which is both reflexive and transitive is called a *preorder.*

Partial order

A preorder which is also anti-symmetric is called a *partial order*.

Linear order

A partial order which is also connected is called a *total order* or *linear order.*

Connectivity

A relation $\mathcal{R} \subseteq A^2$ is *connected* if for all $x, y \in A$, if $x \neq y$, then either $x\mathcal{R}y$ or $y\mathcal{R}x$.

Orders examples

An important partial order is the relation $\subseteq$ on a set of sets. This is not in general a linear order, since if $a \neq b$ and we consider $\mathcal{P}(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$, we see that $\{a\} \nsubseteq \{b\}$ and $\{a\} \neq \{b\}$ and $\{b\} \nsubseteq \{a\}$.

Proposition

Every linear order is also a partial order, and every partial order is also a preorder, but the converses don't hold.

Orders examples

The relation of *divisibility without remainder* gives us a partial order which isn't a linear order. For integers n, m, we write $n \mid m$ to mean n (evenly) divides m, i.e., iff there is some integer k so that $m = kn$. On $\mathbb{N}$, this is a partial order, but not a linear order : for instance, $2 \nmid 3$ and also $3 \nmid 2$. Considered as a relation on $\mathbb{Z}$, divisibility is only a preorder since it is not anti-symmetric : $1 \mid -1$ and $-1 \mid 1$ but $1 \neq -1$.

Particular order

Irreflexivity

A relation $R \subseteq A^2$ is called *irreflexive* if, for all $x \in A$, not $x\mathcal{R}x$.

Asymmetry

A relation $R \subseteq A^2$ is called *asymmetric* if for no pair $x, y \in A$ we have both $x\mathcal{R}y$ and $y\mathcal{R}x$.

Strict order

A *strict order* is a relation which is irreflexive, asymmetric, and transitive.

Strict linear order

A strict order which is also connected is called a *strict total order* or *strict linear order*.

minimal/maximal element

minimal/maximal element

Let $(A, \preceq)$ be a poset, where $\preceq$ represents an arbitrary partial order. Then an element $b \in A$ is a minimal element of A if there is no element $a \in A$ that satisfies $a \preceq b$. Similarly an element $b \preceq A$ is a maximal element of A if there is no element $a \in A$ that satisfies $b \preceq a$.

The set of $\{\{1\}, \{2\}, \{1, 2\}\}$ with $\subseteq$ has two minimal elements $\{1\}$ and $\{2\}$. Note that $\{1\}$, and $\{2\}$ are not related to each other in $\subseteq$. Hence we can not say which is "smaller than" which, that is, they are not comparable

The ordered pair $(A, \mathcal{R})$ is called a poset (partially ordered set) when $\mathcal{R}$ is a partial order.

Least/greatest element

least/greatest element

Let $(A, \preceq)$ be a poset. Then an element $b \in A$ is the least element of A if for every element $a \in A$, $b \preceq a$.

- Note that the least element of a poset is unique if one exists because of the antisymmetry of $\preceq$.
- The poset of the set of natural numbers with the less-than-or-equal-to relation has the least element 0.
- The poset of the powerset of $\{1, 2\}$ with $\subseteq$ has the least element $\emptyset$.

Introduction

A particular binary relation is :

$$f \subseteq A \times B : \forall x \in A, \forall y \in B;\ xfy \text{ iff } y = f(x)$$

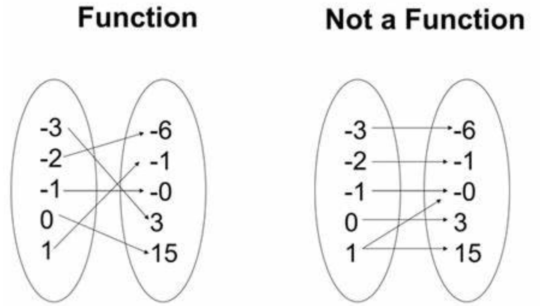
A *function* is a map which sends each element of a given set to a specific element in some (other) given set.

Function, definition

Function

A *function* is a relation such that no two distinct members have the same first coordinate.

$$f \subseteq A \times B \wedge (x, y), (x, z) \in f \Rightarrow y = z$$



Function, definition

- Synonyms for function : transformation, map, mapping, correspondence, operator.
- We call A the *domain* of f and B the *codomain* of f.
- The elements of A are called inputs or *arguments* of f, and the element of B that is paired with an argument x by f is called the *value of f* for argument x, written $f(x)$.
- The *range* $ran(f)$ of f is the subset of the codomain consisting of the values of f for some argument ; $ran(f) = \{f(x) : x \in A\}$.

Functions examples

Multiplication takes pairs of natural numbers as inputs and maps them to natural numbers as outputs, so goes from $\mathbb{N} \times \mathbb{N}$ (the domain) to $\mathbb{N}$ (the codomain). As it turns out, the range is also $\mathbb{N}$, since every $n \in \mathbb{N}$ is $n \times 1$.

We can also define functions by cases. For instance, we could define $h\colon \mathbb{N} \to \mathbb{N}$ by

$$h(x) = \begin{cases} \frac{x}{2} & \text{if } x \text{ is even} \\ \frac{x+1}{2} & \text{if } x \text{ is odd.} \end{cases}$$

Since every natural number is either even or odd, the output of this function will always be a natural number. Just remember that if you define a function by cases, every possible input must fall into exactly one case. In some cases, this will require a proof that the cases are exhaustive and exclusive.

Function, definition

Y^X : The set of all functions on X into Y.
$Y^X \subseteq \mathcal{P}(X \times Y)$.

Restriction of f to A : $f \cap (A \times Y)$ where $f : X \to Y$ and $A \subseteq X$.
Denoted $f|A$.
$f|A : A \to Y$ such that $(f|A)(a) = f(a)$ for $a \in A$.
We have $(f|A) \subseteq f$.

Extension of g to f : $g \subseteq f$.

Identity map on X : $I_X(x) = x$ for all $x \in X$.

Characteristic function of A : $\chi_A(x) = 1$ if $x \in A$ else $\chi_A(x) = 0$ for $A \subseteq X$.

Direct images of A : $\{f(A) : x \in A\}$ where $f : X \to Y$ and $A \subseteq X$.

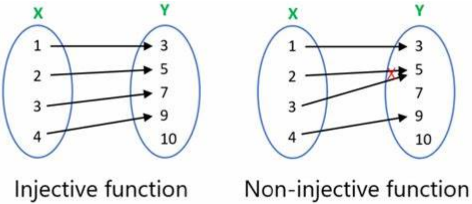
Reciprocal images B : $A = \{x \in X : f(x) \in B\}$ where $f : X \to Y$ and $B \subseteq Y, A \subseteq X$.

Kinds of Functions

injective function

Injection

A function $f : A \to B$ is *injective* iff for each $y \in B$ there is at most one $x \in A$ such that $f(x) = y$. We call such a function a injection from A to B.



Kinds of Functions

injective function

- If you want to show that f is a injection, you need to show that for any elements x and y of f's domain, if $f(x) = f(y)$, then $x = y$.
- The function f is an "injection" means that
  - $\forall x_1, x_2 \in A, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ or,
  - $\forall x_1, x_2 \in A, f(x_1) = f(x_2) \Rightarrow x_1 = x_2$
- The function f is not an "injection" means that $\exists \forall x_1, x_2 \in A, x_1 \neq x_2 \wedge f(x_1) = f(x_2)$

Kinds of Functions

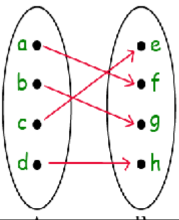
Surjective function

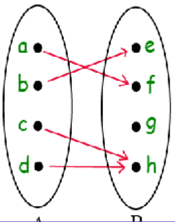
Surjection

A function $f : A \to B$ is *surjective* iff B is also the range of f, i.e., for every $y \in B$ there is at least one $x \in A$ such that $f(x) = y$, or in symbols :

$$(\forall y \in B)(\exists x \in A) : f(x) = y.$$

We call such a function a surjection from A to B.





Kinds of Functions

Surjective function

- If you want to show that f is a surjection, then you need to show that every object in f's codomain is the value of $f(x)$ for some input x.
- Note that any function *induces* a surjection. After all, given a function $f : A \to B$, let $f' : A \to ran(f)$ be defined by $f'(x) = f(x)$. Since $ran(f)$ is *defined* as $\{f(x) \in B : x \in A\}$, this function f' is guaranteed to be a surjection

Examples

The constant function $f : \mathbb{N} \to \mathbb{N}$ given by $f(x) = 1$ is neither injective, nor surjective.
The identity function $f : \mathbb{N} \to \mathbb{N}$ given by $f(x) = x$ is both injective and surjective.
The successor function $f : \mathbb{N} \to \mathbb{N}$ given by $f(x) = x + 1$ is injective but not surjective.
The function $f : \mathbb{N} \to \mathbb{N}$ defined by :

$$f(x) = \begin{cases} \frac{x}{2} & \text{if } x \text{ is even} \\ \frac{x+1}{2} & \text{if } x \text{ is odd.} \end{cases}$$

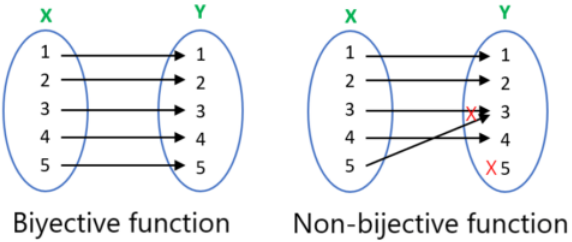
is surjective, but not injective.

Kinds of Functions

Bijective function

bijection

A function $f : A \to B$ is *bijective* iff it is both surjective and injective. We call such a function a bijection from A to B (or between A and B).



Kinds of Functions

Bijective function

- Bijections are also sometimes called *one-to-one correspondences*, since they uniquely pair elements of the codomain with elements of the domain.
- If you want to show that f is a bijection, then you need to show that :

$$(\forall y \in B)(\exists! x \in A) : y = f(x).$$

Kinds of Functions

Bijective function

Bijection examples

- ▷ $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$ is not bijective, but $f_{|[0,+\infty[}$,or $f_{|]-\infty,0]}$ is bijective.
- ⇝ Let $y \in \mathbb{R}, y = f(x) \Rightarrow y = x^2 \Rightarrow x = \{-y, +y\}$. If $y \in \mathbb{R}^+$, or $y \in \mathbb{R}^-$ then $x = y$ or $x = -y$ respectively. Thus, there is a unique solution.
- ▷ $f : \mathbb{R}^+ \to \mathbb{R}^+ . x \mapsto \sqrt{x}$ is bijective.
- ⇝ The unique solution of $y = \sqrt{x}$ is $x = y^2$.

Operations on functions

Inverses of Functions

Inverses of Functions

A function $g\colon B \to A$ is an *inverse* of a function $f\colon A \to B$ if $f(g(y)) = y$ and $g(f(x)) = x$ for all $x \in A$ and $y \in B$.

- If f has an inverse g, we often write f^{-1} instead of g.
- A good candidate for an inverse of $f\colon A \to B$ is $g\colon B \to A$ "defined by"

$$g(y) = \text{"the" } x \text{ such that } f(x) = y.$$

Operations on functions

Inverses of Functions

Proposition

P_1 : If $f : A \to B$ is injective, then there is a *left inverse* $g : B \to A$ of f so that $g(f(x)) = x$ for all $x \in A$.

P_2 : If $f : A \to B$ is surjective, then there is a *right inverse* $h : B \to A$ of f so that $f(h(y)) = y$ for all $y \in B$.

P_3 : If $f : A \to B$ is bijective, there is a function $f^{-1} : B \to A$ so that for all $x \in A$, $f^{-1}(f(x)) = x$ and for all $y \in B$, $f(f^{-1}(y)) = y$.

P_4 : If $f : A \to B$ has a left inverse g and a right inverse h, then $h = g$.

P_5 : Every function f has at most one inverse.

Operations on functions

Inverses of Functions

Inversion examples

- ▷ $f : \mathbb{R} \to [0, +\infty[: x \mapsto exp(x)$ is injective, then there is a *left inverse* $g : [0, +\infty[\to \mathbb{R}$ of f so that $g(f(x)) = x$ for all $x \in \mathbb{R}$.

$\rightsquigarrow$ $ln(exp(x)) = x$

- ▷ $f : \mathbb{R} \to [0, +\infty[: x \mapsto exp(x)$ is surjective, then there is a *right inverse* $h : [0, +\infty[\to \mathbb{R}$ of f so that $f(h(y)) = y$ for all $y \in [0, +\infty[$.

$\rightsquigarrow$ $exp(ln(x)) = x$

$\rightsquigarrow$ $f(x) = exp(x)$ and $f^{-1}(x) = ln(x)$, $g(x) = h(x) = ln(x)$.

Operations on functions

Composition of Functions

Composition

Let $f: A \to B$ and $g: B \to C$ be functions. The *composition* of f with g is $(f^\circ g): A \to C$, where $(f^\circ g)(x) = f(g(x))$.

Proposition

P_1 : If $f: A \to B$ and $g: B \to C$ are both injective, then $(f^\circ g): A \to C$ is injective.

P_2 : If $f: A \to B$ and $g: B \to C$ are both surjective, then $(f^\circ g): A \to C$ is surjective.

Isomorphism

An *isomorphism* is a bijection that preserves the structure of the sets it relates, where structure is a matter of the relationships that obtain between the elements of the sets.

Isomorphism

Let U be the pair $\langle X, R\rangle$ and V be the pair $\langle Y, S\rangle$ such that X and Y are sets and R and S are relations on X and Y respectively. A bijection f from X to Y is an *isomorphism* from U to V iff it preserves the relational structure, that is, for any x_1 and x_2 in X, $(x_1, x_2) \in R$ iff $(f(x_1), f(x_2)) \in S$.

Consider the following two sets $X = \{1, 2, 3\}$ and $Y = \{4, 5, 6\}$, and the relations less than and greater than. The function $f : X \to Y$ where $f(x) = 7 - x$ is an isomorphism between $(X, <)$ and $(Y, >)$.

Example 1

$$f : \mathbb{R}^2 \to \mathbb{R}, (x, y) \mapsto xy$$

and

$$g : \mathbb{R} \to \mathbb{R}^2, x \mapsto (x, x^2)$$

- ▷ $f^\circ g : \mathbb{R} \to \mathbb{R}, x \mapsto x^3$ and $g^\circ f : \mathbb{R}^2 \to \mathbb{R}^2, (x, y) \mapsto (xy, x^2y^2)$
- ⇝ $A = \{(1, 2), (\sqrt{2}, \frac{2}{\sqrt{2}})\}$, $B = \{(2, -7)\}$
- ▷ $f(A) = \{2\}$ and $g^{-1}(B) = \emptyset$
- ⇝ f is not injective. g is not surjective. (Proof)
- ⇝ f is surjective. g is injective. (Proof)

Example 2

On $\mathbb{R}^2$, we consider the relation defined by :

$$(a, b)\nabla(c, d) \text{ if and only if } a^2 + b^2 = c^2 + d^2.$$

1. Prove that ∇ is an equivalence relation.

$\rightsquigarrow$ ∇ is a reflexive, transitive and symmetric relation.

2. Describe the equivalence class (a, b) of the pair (a, b).

$\rightsquigarrow$ $C(a, b) = \{(x, y) \in \mathbb{R}^2 : a^2 + b^2 = x^2 + y^2\}$.

3. Let $\mathbb{R}^2_{/\$}$ be the quotient set for this relation. Prove that the application

$$\begin{aligned} \mathbb{R}^2_{/\nabla} &\to [0, +\infty[\\ (a, b) &\mapsto a^2 + b^2 \end{aligned}$$

is well-defined and that it is a bijection.

Example 2

1. Let $\mathbb{R}^2_{/\$}$ be the quotient set for this relation. Prove that the application

$$\mathbb{R}^2_{/\nabla} \to [0, +\infty[$$
$$(a, b) \mapsto a^2 + b^2$$

is well-defined and that it is a bijection.

$\rightsquigarrow$ Well-defined because if
$\forall (a, b), (c, d) \in \mathbb{R}^2_{/\nabla} \Rightarrow f(a, b) = f(c, d)$

$\rightsquigarrow$ f is a bijection because $\forall r = a^2 + b^2 \in [0, +\infty[$ there is a unique classes $C(a, b) \in \mathbb{R}^2_{/\nabla}$ such that $f(a, b) = a^2 + b^2 = r^2$

Example 3

Lets A and $B \in P(E)$. Consider the function
$f : P(E) \longrightarrow P(A) \times P(B)$ defined by :

$$f(X) = (X \cap A; X \cap B)$$

Example 3

f injective $\Leftrightarrow A \cup B = E$

$\Rightarrow$ Since A and $B \in P(E)(A \cup B) \subset E$. Let $(A \cup B) \supset E$. Assume that $E \not\subset A \cup B : \exists x \in E, x \notin A \cup B \Longrightarrow \exists x \in E$ and $x \notin A$ and $x \notin B \Longrightarrow \{x\} \cap A = \{x\} \cap B = \emptyset \Longrightarrow f(\{x\}) = (\{x\} \cap A, \{x\} \cap B) = (\emptyset, \emptyset) = f(\emptyset)$ with $\{x\} \neq \emptyset$. Thus, f is not injective. Contradiction.

$\Leftarrow$ Lets $X_1, X_2 \in P(E) : f(X_1) = f(X_2) \Longrightarrow (X_1 \cap A, X_1 \cap B) = (X_2 \cap A, X_2 \cap B) \Longrightarrow (X_1 \cap A = X_2 \cap A)$ and $(X_1 \cap B = X_2 \cap B) \Longrightarrow (X_1 \cap A) \cup (X_1 \cap B) = (X_2 \cap A) \cup (X_2 \cap B) \Longrightarrow X_1 \cap (A \cup B) = X_2 \cap (A \cup B) \Longrightarrow X_1 \cap (E) = X_2 \cap (E) \Longrightarrow X_1 = X_2$, so f injective.

Example 3

f surjective $\Leftrightarrow A \cap B = \emptyset$

$\Rightarrow$ $(A \cap B) \supset \emptyset$. To show that $(A \cap B) \subset \emptyset$, assume $\exists x \in A \cap B \Longrightarrow \{x\} \cap A = \{x\} = \{x\} \cap B$. But $(\{x\}, \emptyset) \in P(A) \times P(B)$ and there is no $Y \in P(E) : (\{x\}, \emptyset) = (Y \cap A; Y \cap B)$ because $x \in B$ so f is not surjective. Contradiction.

$\Leftarrow$ Assume that $\exists (Y_1, Y_2) \in P(A) \times P(B)$ and $(Y_1, Y_2) \neq f(X), \forall X \in P(E)$, thus $(Y_1, Y_2) \neq (X \cap A, X \cap B), \forall X \in P(E)$. $X = Y_1 \cup Y_2$, $(Y_1, Y_2) \neq ((Y_1 \cup Y_2) \cap A, (Y_1 \cup Y_2) \cap B)) =$ $((Y_1 \cap A) \cup (Y_2 \cap B)), ((Y_1 \cap B) \cup (Y_2 \cap B))$ but $Y_1 \in P(A)$, $Y_2 \in P(B)$ and $A \cap B = \emptyset$, so $(Y_1, Y_2) \neq (Y_1 \cap A, Y_2 \cap B) = (Y_1, Y_2)$, contradiction. f is surjective.

Example 4

1. A.KUROSH, Cours d'algèbre supérieure. Edition MIR MOSCOU.
2. D.FADEEV et I.SOMINSKY Recueil d'exercices d'algèbre supérieure. Edition MIR MOSCOU.
3. J.RIVAUD Exercices avec solutions tome 1, 2 VUIBERT.
4. LEBSIR HABIB, Travaux dirigés d'algèbre générale. Dar el-Houda Ain M'LILA.
5. Jean-Pierre ESCOFIER, Toute l'algèbre de la licence. Cours et exercices corrigés. DUNOD.

References

1. J. Lelong-Ferrand, J.M.Arnaudiès Cours de mathématiques. Tome 1 Algèbre troisiéme édition. Classes préparatoires premier cycle universitaire,DUNOD.
2. Richard Zach. Sets, Logic, Computation : An Open Introduction to Metalogic. University of Calgary.
3. S. BALAC, F. STURM.ALGEBRE et ANALYSE : Cours de Mathematique de premiere annee avec exercices corriges. PRESSES POLYTECHNIQUES ET UNIVERSITAIRES ROMANDES.