Analysis

Contents

1 Sets

Definition: A set is a collection of objects, called the *elements* or *members* of the set. We write $x \in X$ if x is an element of the set X and $x \notin X$ if x is not an element of X.

Two sets $X = Y$, if

$$x \in X \iff x \in Y$$

("iff" or "$\Leftrightarrow$" both mean "if and only if").

The empty set is denoted by $\varnothing$, that is, the set without any elements. X is *nonempty* if it has at least one element.

We can define sets by listing their elements:

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

We can also have infinite sets, for example:

$$\mathbb{N} = \{1, 2, 3, \dots\}, \quad \mathbb{N}_0 = \{0, 1, 2, 3, \dots\},$$

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}, \quad \mathbb{Q} = \left\{\tfrac{p}{q} : p, q \in \mathbb{Z},\ q \neq 0\right\},$$

$$\mathbb{R} = \{\text{all numbers with decimal expansions}\}.$$

1.1 Subsets

A is a subset of a set X or A is included in X, written $A \subseteq X$, if every element of A belongs to X. A is a proper subset of X, written as $A \subset X$, when $A \subseteq X$, but $A \neq X$.

Def.: The power set $\mathcal{P}(X)$ of a set X is the set of all subsets of X.

Ex.: X ={1,2,3}, then $\mathcal{P}(X)$={$\varnothing$,{1},{2},{3},{1,2},{1,3},{2,3},{1,2,3}}

The power set $\mathcal{P}(X)$ of a set X with —X—=n elements has —$\mathcal{P}(X)$—=2^n elements because, in defining a subset, we have two independent choices for each element (does it belong to the subset or not?). Thus, the notation $2^X = \mathcal{P}(X)$ is also in use.

1.2 Set operations

The intersection $A \cap B$ of two sets A, B is the set of all elements that belong to both A and B. Two sets A, B are said to be disjoint if $A \cap B = \varnothing$; that is, if A and B have no elements in common.

The union $A \cup B$ is the set of all elements that belong to A or B. Note that we always use 'or' in an inclusive sense, so that $x \in A \cup B$ if x is an element of A or B, or both A and B. (Thus, $A \cap B \subseteq A \cup B$.)

The set-difference of two sets B and A is the set of elements of B that do not belong to A, that is $B \setminus A = \{x \in B : x \notin A\}$. If we consider sets that are subsets of a fixed set X (called the universe) that is understood from the context, then we write $A^c = \overline{A} = X \setminus A$ to denote the complement of $A \subseteq X$ in X. Note that $(A^c)^c = A$.

The Cartesian product $A \times B$ of sets A, B is the set whose members all possible ordered pairs (a, b) with $a \in A$, $b \in B$, thus $A \times B = \{(a, b) : a \in A, b \in B\}$ and $|A \times B| = |A||B|$.

1.3 Algebraic properties

Intersection is a commutative operation $A \cap B = B \cap A$; and an *associative* operation, that is:

$$(A \cap B) \cap C = A \cap (B \cap C), \text{ thus} = A \cap B \cap C$$

both are also true for the union $A \cup B$. Intersection distributes over union and union distributes over intersection:

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

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

We have De Morgan's laws:

$$(a \cup B)^c = A^c \cap B^c \text{ and } (A \cap B)^c = A^c \cup B^c$$

Arbitrary many unions and intersections: Let $\mathcal{C}$ be a collection of sets. Then

$$\bigcup \mathcal{C} = \bigcup_{A \in \mathcal{C}} A = \{x : x \in A, \text{ for some } A \in \mathcal{C}\}$$

$$\bigcap \mathcal{C} = \bigcap_{A \in \mathcal{C}} A = \{x : x \in A, \text{ for all } A \in \mathcal{C}\}$$

1.4 Relations

Any subset of the Cartesian product of two sets X, Y defines a (binary) relation $R \subseteq X \times Y$ between these two sets. Given $(x, y) \in R$ we may denote this inclusion simply as xRy. Notation: $\forall$ means 'for all', $\exists$ means 'exists'. A binary relation R is *univalent* if

$$\forall x \in X, \forall y \in Y, \forall z \in Y \text{ we have } ((x, y) \in R \text{ and } (x, z) \in R) \implies y = z$$

A binary relation R is *total* if

$$\forall x \in X, \exists y \in Y \text{ we have } (x, y) \in R$$

Def.: A partially defined function is a univalent binary relation, and a function is a univalent and total binary relation. Thus a function $f : X \mapsto Y$ is defined by a univalent and total $xRy \iff y = f(x)$. The set of all functions from X to Y is commonly denoted as

$$Y^X = \prod_{x \in X} Y$$

1.5 Orders and equivalences

Def.: An order $\leq$ on a set X is a binary relation on X, s.t. for every $x, y, z \in X$:

1. $x \leq x$ (reflexivity),
2. If $x \leq y$ and $y \leq x$ then $x = y$ (antisymmetry),
3. If $x \leq y$ and $y \leq z$ then $x \leq z$ (transitivity).

An order is *linear* or *total* if $\forall x, y \in X$ either $x \leq y$ or $y \leq x$. If $\leq$ is an order, then we define a strict order by $x < y$ if $x \leq y$ and $x \neq y$.

If for a relation $\sim$ in 2. instead of antisymmetry we have *symmetry*: If $x \sim y$ then $y \sim x$ then $\sim$ is called an equivalence relation.

2 Functions

Per definition a function $f : X \mapsto Y$ is a univalent and total relation, that is for every $x \in X$ there is a unique $y = f(x) \in Y$. $Do(f) = X$ is called the *domain* of f, and $Ran(f) = \{y \in Y : \exists x \in X, y = f(x)\} \subseteq Y$ is called the range of f. Also $f(A) = \{y \in Y : \exists x \in A, y = f(x)\}$ for some $A \subseteq X$.

Ex.: The identity function $id_X : X$ on a set X is the function that maps every element of X to itself, that is $id_X(x) = x$ for all $x \in X$.

Ex.: the characteristic or indicator function $\chi_A : X \mapsto \{0, 1\}$ of $A \subseteq X$ is defined as

$$\chi_A(x) = \begin{cases} 1, & x \in A, \\ 0, & x \notin A. \end{cases}$$

The graph of a function $f : X \mapsto Y$ is defined as

$$G_f = \{(x, y) \in X \times Y : y = f(x)\}$$

2.1 Properties of functions

A function $f : X \mapsto Y$ is

1. injective (one-to-one) if it maps distinct elements to distinct elements, that is $x_1, x_2 \in X$ and $x_1 \neq x_2$ implies that $f(x_1) \neq f(x_2)$,
2. surjective (onto) if its range $Ran(f) =$ Y, that is for every y there exists an x, s.t. $y = f(x)$.
3. If a function is both injective and surjective then its bijective.

We define the composition $f \circ g(z) = f(g(z))$ of functions $f : Y \mapsto X$ and $g : Z \mapsto Y$. Note that we need the inclusion $Ran(g) \subseteq Do(f)$. $\circ$ is associative.

A bijective function $f : X \mapsto Y$ has an inverse $f^{-1} : Y \mapsto X$ defined by

$$f^{-1}(y) = x \text{ if and only if } f(x) = y$$

that is $f \circ f^{-1} = id_Y$ and $f^{-1} \circ f = id_X$.

If $f : x \mapsto Y$ is merely injective than still $f : X \mapsto Ran(f)$ is bijective, thus invertible on its range with inverse $f^{-1} : Ran(f) \mapsto X$.

2.2 Groups, monoids, fields

Def.: Given a function $f : X \times X \mapsto X$ we may denote $f(x, y) = x*y$ and consider this as a binary operation on X. For example addition of integers is such an operation. The we say that * is/has

1. Associative, if $x * (y * z) = (x * y) * z$,
2. Commutative, if $x * y = y * x$,
3. Neutral element, if there exists $e \in X$ (a neutral element), s.t. $x * e = e * x = x$,
4. Inverse elements, if for all $x \in X$ there exists $x' \in X$ called an inverse of x, s.t. $x * x' = x' * x = e$ where e is a neutral element.

Def.: $(X, *)$ is called a

1. Semigroup, if * is associative,
2. Monoid, if $(X, *)$ is a semigroup and has a neutral element,
3. Group, if $(X, *)$ is a monoid and every element $x \in X$ has an inverse.

Theorem: In a group $(X, *)$ the neutral element $e \in X$ and inverse x' for any fixed $x \in X$ are unique.

Proof.: Indeed, if there would be two neutral elements e, e', then $e' = e * e' = e$. Also assuming $x * y = e = x * z$, implies $x' * (x * y) = x' * (x * z)$, that is $y = z = x'$.

Let $(X, \cdot, +)$ be given with binary operations $\cdot$ and $+$.

Def.: $(X, \cdot, +)$ is a field if

1. $(X, \cdot, +)$ is a commutative group with neutral element 0,
2. $(X \setminus \{0\}, \cdot)$ is a commutative group,
3. $\cdot$ distributes over $+$ (distributivity), that is: $x \cdot (y + z) = x \cdot y + x \cdot z$. In this case $+$ is usually called addition and $\cdot$ multiplication.

Ex.: the rational numbers $\mathbb{Q}$ is a field, moreover an ordered field $(\mathbb{Q}, \cdot, +, \leq)$ equipped with the total order $x \leq y \iff 0 \leq y - x$, where 0 is the neutral element of $+$.

Ex.: the set of real numbers $\mathbb{R}$ is also a totally ordered field $(\mathbb{R}, \cdot, +, \leq)$

Axiom: the $\leq$ order of $\mathbb{R}$ satisfies

I. $x \leq y$ implies $x + z \leq y + z$,

II. $x < y$ and $z > 0$ implies $xz < yz$.

2.3 Supremum and infimum

Def.: A set $A \subseteq \mathbb{R}$ is *bounded from above*, if $\exists M \in \mathbb{R}$ s.t. $x \leq M$ for all $x \in A$; and it is *bounded from below*, if $\exists m \in \mathbb{R}$ s.t. $x \geq m$ for all $x \in A$. If both holds for A, then it is bounded. ('s.t.' is short hand for 'such that')

Def.: If $M \in \mathbb{R}$ is an upper bound of $A \subseteq \mathbb{R}$ s.t. for any other upper bound $M' \in \mathbb{R}$ of A we have $M \leq M'$, then M is called the least upper bound of A, denoted as

$$M = \sup A$$

Similarly, the greatest lower bound of $A \subseteq \mathbb{R}$, if exists, is denoted by

$$m = \inf A$$

meaning $m \geq m'$ for any lower bound m of A. If $A = \{x_i : i \in I\} \subseteq \mathbb{R}$ for an index set I, we also write:

$$\sup A = \sup_{i \in I} x_i \text{ and } \inf A = \inf_{i \in I} x_i$$

Fact: by the definition supremum and infimum of a set, if they exist, are both unique and $\sup A \geq \inf A$ for nonempty $A \subseteq \mathbb{R}$.

Def.: if $\sup A \in A$, then we call it the maximum of A denoted by $\max A$, similarly if $\inf A \in A$, then we call it the minimum of A denoted by $\min A$.

Ex.: Let $\mathbb{R} \supseteq A = \{\frac{1}{n} : n \in \mathbb{N}\}$. Then $\sup A = 1$ belongs to A, while $\inf A = 0$ does not belong to A.

Def.: let us introduce the elements ∞,$-\infty$, so that $\infty > x > -\infty$ for any $x \in \mathbb{R}$ and define the extended real numbers as $\overline{\mathbb{R}} = \{\infty, -\infty\} \cup \mathbb{R}$. If a set $A \subseteq \mathbb{R}$ is not bounded from above then define $\sup A = \infty$, and if $A \subseteq \mathbb{R}$ is not bounded from below then define $\inf A = -\infty$. Also define $\sup \emptyset = -\infty$ and $\inf \emptyset = \infty$.

2.4 (Order) Completeness

Consider $A = \{x \in \mathbb{Q} : x^2 \leq 2\}$. This set is bounded from above but has no least upper bound in $\mathbb{Q}$.

Def(Completeness).: a totally ordered field Z is complete, if all nonempty upper bounded subsets of Z have a least upper bound in Z. We call this the least upper bound property.

Theorem(Dedekind): There exists a unique (up to $(\cdot, +, \leq)$-preserving transformation) ordered complete field satisfying the order axioms I., II. that contains $\mathbb{Q}$ and it is the field $\mathbb{R}$. Such a transformation $\phi : \mathbb{R} \mapsto \mathcal{M}$ satisfies $\phi(x + y) = \phi(x) + \phi(y), \phi(xy) = \phi(x)\phi(y), x \leq y \implies \phi(x) \leq \phi(y)$.

2.5 Archimedean property

Theorem(Archimedean property): If $x \in \mathbb{R}$, then there exists $n \in \mathbb{Z}$ such that $x < n$.

Proof: Suppose, for contradiction, that there exists $x \in \mathbb{R}$ s.t. $x > n$ for all $n \in \mathbb{Z}$. Then x is an upper bound of $\mathbb{Z} \subseteq \mathbb{R}$, so $M = \sup \mathbb{Z} \in \mathbb{R}$ exists. Since $n \leq M$ for all $n \in \mathbb{Z}$, we have $n - 1 \leq M - 1$ for all $n \in \mathbb{Z}$, which implies $n \leq M - 1$ for all $n \in \mathbb{Z}$. But then $M - 1$ is an upper bound of $\mathbb{Z}$ that is strictly less than $M = \sup \mathbb{Z}$, a contradiction to $M = \sup \mathbb{Z}$ being the least upper bound.

Corollary: For every $0 < \epsilon \in \mathbb{R}$, there exists an $n \in \mathbb{N}$, s.t. $0 < \frac{1}{n} < \epsilon$.

Corollary(integer part): If $x \in \mathbb{R}$, then there exists $[x] = n \in \mathbb{Z}$ called the integer part of x, such that $n \leq x < n + 1$.

2.6 Further properties

Def(dense set).: $A \subseteq \mathbb{R}$ is dense in $\mathbb{R}$, if for any $0 < \epsilon, x \in \mathbb{R}$ there exists $a \in A$, s.t. $x - \epsilon < a < x + \epsilon$.

Theorem(density of rationals): $\mathbb{Q} \subseteq \mathbb{R}$ is dense in $\mathbb{R}$.

Proof: Let $0 < \epsilon, x \in \mathbb{R}$. Then for any $n \in \mathbb{N}$ we have

$$[nx] \leq nx < [nx] + 1$$

which gives

$$\frac{[nx]}{n} \leq x < \frac{[nx]}{n} + \frac{1}{n}$$

Pick $n \in \mathbb{N}$, s.t. $0 < \frac{1}{n} < \epsilon$. Then we have

$$\frac{[nx]}{n} \leq x < \frac{[nx]}{n} + \frac{1}{n} < \frac{[nx]}{n} + \epsilon$$

which implies $x - \epsilon < \frac{[nx]}{n} < x + \epsilon$ as wanted.

2.7 Properties of sup and inf

Theorem:

1. Given $A \in \mathbb{R}$, then $M = \sup A$ if and only if
   (a) M is an upper bound of A,
   (b) for every $M' < M$ there exists $x \in A$ s.t. $M' < x$.
2. If $A \subseteq B \subseteq \mathbb{R}$, then $\sup A \leq \sup B$ and $\inf B \leq \inf A$.
3. If $A \subseteq \mathbb{R}$, then $\inf A \leq \sup A$.
4. If $A \subseteq \mathbb{R}$, then $-\inf A = \sup(-A)$.
5. If $A \subseteq \mathbb{R} \ni \alpha \geq 0$, then $\sup(\alpha A) = \alpha \sup(A)$.
6. If $A, B \subseteq \mathbb{R}$, we have $\sup(A+B) \leq \sup A + \sup B$, $\inf(A+B) \geq \inf A + \inf B$ where $A + B = \{x \in \mathbb{R} : x = a + b, a \in A, b \in B\}$.
7. Let $\mathcal{C}$ be a family of sets in $\mathbb{R}$, then $\sup(\cup\mathcal{C}) = \sup\{\sup A : A \in \mathcal{C}\}$.

2.8 Intervals and topology of $\mathbb{R}$

Def.: Let $a, b \in \mathbb{R}$.

1. Closed interval $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$,
2. Open interval $(a, b) = \{x \in \mathbb{R} : a < x < b\}$,
3. Half-open intervals $(a, b] = \{x \in \mathbb{R} : a < x \leq b\}, [a, b) = \{x \in \mathbb{R} : a \leq x < b\}$
4. $[a, \infty) = \{x \in \mathbb{R} : a \leq x\}, (a, \infty) = \{x \in \mathbb{R} : a < x\}, (-\infty, b] = \{x \inf \mathbb{R} : b \geq x\}, (-\infty, b) = \{x \in \mathbb{R} : b > x\}$

Def.: $A \subseteq \mathbb{R}$ is open if for every $x \in A$ there exists $0 < \epsilon \in \mathbb{R}$ s.t. $(x - \epsilon, x + \epsilon) \subseteq A$.
Def.: $B \subseteq \mathbb{R}$ is closed if $B^C = \{x \in \mathbb{R} : x \notin B\}$ is open.
Def.: $U \subseteq \mathbb{R}$ is a neighborhood of $z \in \mathbb{R}$, if there exists $0 < \epsilon \in \mathbb{R}$ s.t. $(z - \epsilon, z + \epsilon) \subseteq U$.
Theorem: Arbitrary union of open sets is open, and an intersection of finite number of open sets is open.
Def.: Let $A \subseteq \mathbb{R}$, then $x \in \mathbb{R}$ is

1. an interior point of a, if there exists $0 < \epsilon \in \mathbb{R}$ s.t. $(x - \epsilon, x + \epsilon) \subseteq A$;
2. an isolated point of A, if $x \in A$ and there exists $0 < \epsilon \in \mathbb{R}$ s.t. x is the only point of A that belongs to $(x - \epsilon, x + \epsilon)$;
3. a boundary point of A, if for every $0 < \epsilon \in \mathbb{R}$ the interval $(x - \epsilon, x + \epsilon)$ contains at least a point in A and at least a point not in A;
4. an accumulation point of A, if for every $0 < \epsilon \in \mathbb{R}$ the interval $(x - \epsilon, x + \epsilon)$ contains a point in A distinct from x.