Computational Mathematics

Contents

1 Elementary Set Theory **2**
1.1 Relations Among Sets 2
1.2 Basic Operations of Sets 3
1.3 Index Sets 4
1.4 Some More Set Operations 4
1.5 Relations 5
1.5.1 Equivalence Relations and Partitions 6
1.5.2 Partial Order Relations 7
1.6 Functions 7

1 Elementary Set Theory

A set is (informally) an unordered collection of elements. More formally, any set is defined by the membership relation $\in$ (read "belongs to", "is an element of", "is a member of", or "is in"), where $s \in S$ if and only if s is an element of the set S. If x is not a member of S, then we write $x \notin S$. We may define a set either as a list of all its members enclosed by curly braces – $\{$ and $\}$ – or in the form $Y = \{\, x \in X \mid P(x) \,\}$, where X is a previously defined set, and $P(x)$ is a predicate (a function with a true/false value depending on the value of x) – then Y is the set consisting of all members of X that satisfy the predicate $P(x)$ (i.e., those $x \in X$ for which $P(x)$ is true). The latter form of defining a set is called the set-builder notation. For example

$$S = \{1, \text{‘a’}, 2.5, +, 9, -3\}$$

defines S to be the set consisting of the six elements 1, ‘a’, 2.5, $+$, 9, and -3, and

$$T = \{\, s \in S \mid s \text{ is a number} \,\}$$

defines T to be the set consisting of the four elements 1, 2.5, 9, and -3. The symbol $\mid$ is read as "such that" (and can be replaced by a $:$ as well).

The universal set (usually denoted by U) is the set consisting of all elements currently under consideration. We may write $\{\, x \mid P(x) \,\}$ to mean $\{\, x \in U \mid P(x) \,\}$.

The empty set (or null set) is the set $\varnothing$ that has no elements. That is, for every element a of the universal set, $a \notin \varnothing$.

Note. A variant of the set-builder notation replaces the element on the left side of $\mid$ by an expression involving one or more elements, with the specifications of memberships of these elements appearing on the right side of $\mid$, along with other predicates, if any. For example

$$S = \{\, 2n \mid n \in \mathbb{Z} \,\}$$

defines S to be the set of all elements obtained by doubling an integer – in other words, S is the set of even integers.

1.1 Relations Among Sets

A set A is a subset of a set B, denoted by $A \subseteq B$, if every element of A is an element of B. That is, for any element a (of the universal set), $a \in A \implies a \in B$. Then B is a superset of A, denoted by $B \supseteq A$. We may also say that B contains A, or that A is contained in B.

Two sets A and B are equal, written $A = B$, if each contains the other – i.e., $A \subseteq B$ and $B \subseteq A$. This is equivalent to the statement that A and B have exactly the same elements. Otherwise, A is not equal to B (written $A \neq B$). A is a proper subset of A (or is properly contained in B) if $A \subseteq B$ and $A \neq B$. Then we write $A \subsetneq B$. Similarly, B is a proper superset of A, denoted by $B \supsetneq A$, if $B \supseteq A$ and $B \neq A$.

Note. It is also common to use $\subset$ and $\supset$ instead of $\subseteq$ and $\supseteq$, respectively. They are usually *not* alternatives to $\subsetneq$ and $\supsetneq$, except when explicitly stated to be so.

The set of all subsets of a set A is called the power set of A, is denoted by 2^A or $\mathcal{P}(A)$. That is,

$$2^A = \{\, S \mid S \subseteq A \,\}.$$

Exercise 1.1. Let A, B, and C be arbitrary sets.

1. Show that $A \subseteq A$.
2. Show that if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.
3. Show that the $\supseteq$ also satisfies these properties.
4. Show that $\varnothing \subseteq A$.
5. Show that if A is a set consisting of n elements, for some non-negative integer n, then 2^A contains 2^n elements.

1.2 Basic Operations of Sets

The union of two sets A and B is the set $A \cup B$ consisting of all elements that belong to A or B:

$$A \cup B = \{\, x \mid x \in A \text{ or } x \in B \,\}.$$

The intersection of two sets A and B is the set $A \cap B$ consisting of all elements that belong to A and B:

$$A \cap B = \{\, x \mid x \in A \text{ and } x \in B \,\}.$$

The complement of a set A is the set $\overline{A}$ of all elements (of the universal set) that do not belong to A:

$$\overline{A} = \{\, x \mid x \notin A \,\}.$$

We may also denote the complement of A by A', A^c, or $U \setminus A$.

Exercise 1.2. Let A, B, and C be arbitrary sets.

1. Show that $A \cap B \subseteq A \subseteq A \cup B$.
2. Show that $\cup$ is
   (i) associative: $(A \cup B) \cup C = A \cup (B \cup C)$,
   (ii) commutative: $A \cup B = B \cup A$, and
   (iii) idempotent: $A \cup A = A$.
3. Prove that $\cap$ is also associative, commutative, and idempotent.
4. Prove that $\cup$ distributes over $\cap$ and vice-versa:

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

5. Prove that $\cup$ and $\cap$ satisfy the law of absorption:

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

6. Show that the following are equivalent:
   (a) $A \subseteq B$.
   (b) $A \cup B = B$.
   (c) $A \cap B = A$.
7. Prove that $\cup$, $\cap$ and $\bar{}$ satisfy De Morgan's laws. That is:

$$\overline{(A \cup B)} = \overline{A} \cap \overline{B}$$
$$\overline{(A \cap B)} = \overline{A} \cup \overline{B}.$$

8. Show that $A \cap \overline{A} = \varnothing$.

Two sets A and B are disjoint if their intersection is empty – i.e., $A \cap B = \varnothing$. Note that A and $\overline{A}$ are always disjoint. Also note that $\varnothing$ is disjoint with all sets, and is the unique set that is disjoint with itself.

Since $\cup$ and $\cap$ are associative, expressions of the form $A_1 \cup A_2 \cup \cdots \cup A_n$ and $A_1 \cap A_2 \cap \cdots \cap A_n$ are well-defined and unambiguous. These are called the n-ary (or finite) union and intersection, and denote them as $\bigcup_{i=1}^n A_i$ and $\bigcap_{i=1}^n A_i$, respectively. But it is possible to define unions and intersections of collections of sets even more generally. For this, we will discuss the concept of an indexing set.

1.3 Index Sets

A set I is an index set (or indexing set) of a set S if we can write S as

$$S = \{s_i \mid i \in I\}.$$

That is, each element of $s_i \in S$ corresponds to a unique element $i \in I$. Then S is indexed by I, and it is common to write $S = \{s_i\}_{i \in I}$.

Let $\mathcal{A} = \{A_i\}_{i \in I}$ be a collection of sets (for some index set I). Thus, for each $i \in I$, A_i itself is a set in the collection $\mathcal{A}$. Then we can define the union and intersection of the sets in $\mathcal{A}$, as given below.

$$\bigcup_{i \in I} A_i = \{\, a \mid a \in A_i,\ \exists i \in I \,\}$$
$$\bigcap_{i \in I} A_i = \{\, a \mid a \in A_i,\ \forall i \in I \,\}$$

We refer to these operations as arbitrary unions and intersections. In the particular case where I is a set containing finitely many elements, these reduce to the finite union and intersection defined earlier.

1.4 Some More Set Operations

We say that (a,b) (or $\langle a,b \rangle$) is an ordered pair where the first element is a and the second element is b. Formally, we may define the ordered pair in terms of sets as $(a,b) = \{a, \{a,b\}\}$. Note that this is only one possible "encoding" of the concept of an ordered pair, and in practice, we do not think of (a,b) as the (unordered) set $\{a, \{a,b\}\}$.

The Cartesian product of two sets A and B, denoted by $A \times B$, is the set of all ordered pairs of elements with the first element from A and the second from B. That is,

$$A \times B = \{\, (a,b) \mid a \in A,\ b \in B \,\}.$$

The disjoint union (or coproduct) of two sets A and B, denoted by $A \sqcup B$, consists of all the ordered pairs of the form (x,i) where $i = 1$ when $x \in A$ and $i = 2$ when $x \in B$. That is,

$$A \sqcup B = \{\, (a,1) \mid a \in A \,\} \cup \{\, (b,2) \mid b \in B \,\}.$$

The disjoint union is also denoted by $A \coprod B$, $A \mathbin{\dot\cup} B$, or $A \uplus B$.

Note. The second element in each ordered pair (i.e., 1 or 2) only serves to distinguish the elements that are originally from A, from those that are originally from B. Thus, for example, if x is an element common to both A and B, then $A \sqcup B$ contains two "copies" of x, namely $(x,1)$ and $(x,2)$. When A and B are disjoint, $A \sqcup B$ is equivalent to $A \cup B$ (where the meaning of "equivalent" will be formalised later).

We can also define Cartesian products and disjoint unions of a collection of sets. Let $\mathcal{A} = \{A_i\}_{i\in I}$ be a collection of sets indexed by I. Then the Cartesian product of the collection $\mathcal{A}$ is

$$\prod_{i\in I} = \{\,(a_i)_{i\in I} \mid a_i \in A_i,\ i \in I\,\}$$

where $(a_i)_{i\in I}$ is a sequence of elements indexed by I, with $a_i \in A_i$ for each $i \in I$. The disjoint union of the collection $\mathcal{A}$ is

$$\bigsqcup_{i\in I} = \bigcup_{i\in I}\{\,(a_i, i) \mid a_i \in A_i,\ i \in I\,\} = \bigcup_{i\in I} A_i \times \{i\}.$$

Note. We will formally define sequences later, in Section 1.6.

The difference of two sets A and B is the set $A \setminus B$ consisting all elements of A that are not elements of B. That is,

$$A \setminus B = \{a \in A \mid a \notin B\}.$$

The difference of A and B is also denoted by $A - B$. Note that $A \setminus B = A \setminus (A \cap B)$.

The symmetric difference of two sets A and B is the set $A \mathbin{\triangle} B$ consisting of all the elements that are present in exactly one of A and B. That is,

$$A \mathbin{\triangle} B = (A \setminus B) \cup (B \setminus A).$$

The symmetric difference of A and B is also denoted as $A \ominus B$.

Exercise 1.3. Let A and B be arbitrary sets.

1. Show that $(A \cup B) \setminus B = A \setminus B$.
2. Show that $A \mathbin{\triangle} B = (A \cup B) \setminus (A \cap B)$.
3. Show that $(2^A, \triangle)$ is an Abelian group. That is:
   (i) $\triangle$ is associative.
   (ii) $\triangle$ is commutative.
   (iii) $\exists E \in 2^A, \forall S \in 2^A, S \mathbin{\triangle} E = S$.
   (iv) $\forall S \in 2^A, \exists T \in 2^A, S \mathbin{\triangle} T = E$.

   What is the order of any non-identity element of this group?

1.5 Relations

A relation R from a set A to a set B, denoted $R\colon A \longrightarrow B$, is a subset of $A \times B$, i.e, $R \subseteq A \times B$. If $(a, b) \in R$, then we write aRb, and if $(a, b) \notin R$, then we write $a\not{R}b$. The set A is the domain and B the codomain of R. Note that $\varnothing$ is also a relation, called the empty or void relation, from A to B.

Note. A relation from a set A to a set B is a binary relation. More generally, if $A_1, \ldots, A_n$ are n sets, then a subset of $A_1 \times \cdots \times A_n$ is an n-ary relation.

A relation $R\colon A \longrightarrow B$ is said to be

1. left-total if for each $a \in A$, aRb for some $b \in B$.
2. right-total if for each $b \in B$, aRb for some $a \in A$.
3. left-unique if for each $b \in B$, if $a, a' \in A$ are such that aRb and $a'Rb$, then $a = a'$.
4. right-unique if for each $a \in A$, if $b, b' \in B$ are such that aRb and aRb', then $b = b'$.

A relation from A to itself is said to be a relation on (or over) A (also called a homogeneous relation on A). Such relations can have a number of properties. In the following, let $\sim$ be a relation on a set A.

1. Reflexivity: For all $a \in A$, $a \sim a$.
2. Symmetry: For all $a, b \in A$, if $a \sim b$, then $b \sim a$.
3. Anti-symmetry: For all $a, b \in A$, if $a \sim b$ and $b \sim a$, then $a = b$.
4. Transitivity: For all $a, b, c \in A$, if $a \sim b$ and $b \sim c$, then $a \sim c$.
5. Irreflexivity: For all $a \in A$, $a \nsim a$.
6. Asymmetry: For all $a \in A$, if $a \sim b$, then $b \nsim a$.

Example 1.1. The following list gives examples of familiar relations satisfying one or more of the above properties:

1. The relations $=$ (on any set of elements where equality is defined), $\leq$ and $\geq$ (on any set of real numbers), $\mid$ (*divides*, see Exercise 1.7), $\subseteq$ and $\supseteq$ (on any collection of sets), $\cong$ and $\sim$ (on any set of triangles), and $\parallel$ (on any set of lines) are reflexive.
2. The relations $=$, $\neq$, $\cong$, $\sim$, $\parallel$, $\perp$ are symmetric.
3. The relations $\mid$ (on any set of non-negative integers), $\leq$, $\geq$, $\subseteq$, $\supseteq$ are anti-symmetric.
4. The relations $=$, $\leq$, $\geq$, $<$, $>$, $\mid$, $\subseteq$, $\supseteq$, $\subsetneq$, $\supsetneq$, $\cong$, $\sim$, $\parallel$ are transitive.
5. The relations $\neq$ and $\perp$ are irreflexive.
6. The relations $<$, $>$, $\subsetneq$, $\supsetneq$ are asymmetric.

Exercise 1.4.

1. Let $\sim$ be the relation of the set $A = \{a, b\}$ defined by $a \sim a$, $a \sim b$. Is $\sim$ transitive?
2. Show that every asymmetric relation is irreflexive.
3. Prove or disprove: Any transitive, irreflexive relation is asymmetric.
4. Prove or disprove: Any symmetric, transitive relation is reflexive.

1.5.1 Equivalence Relations and Partitions

A reflexive, symmetric, and transitive relation is called an equivalence relation. For example, $=$, $\cong$, $\sim$, and $\parallel$ are equivalence relations. If $\sim$ is an equivalence relation on a set A, and $a \in A$, then the equivalence class of a, denoted as $[a]$ or $\overline{a}$ is the set of all elements of A that a is related to by $\sim$. That is,

$$[a] = \{\, b \in A \mid a \sim b \,\}.$$

Example 1.2. Let $A = \{1, 2, 3, 4, 5\}$, and define a relation $\sim$ on A as follows: For any $a, b \in A$, $a \sim b$ if and only if $a - b$ is even. Then, for example, the equivalence class of 1 is $[1] = \{1, 3, 5\}$, and the equivalence class of 2 is $[2] = \{2, 4, 6\}$. Note that $[1] = [3] = [5]$ and $[2] = [4] = [6]$. Also observe that $[1]$ and $[2]$ are disjoint, and $[1] \cup [2] = A$.

An equivalence relation on a set is essentially the same as a partition of the set, as you will show in Exercises 1.5 and 1.6. A partition of a set S is a collection of non-empty and pairwise disjoint subsets of S whose union is equal to S. That is, a partition of S is a collection $\{P_i\}_{i \in I}$ of sets $P_i \subseteq S$, $i \in I$, such that

1. $P_i \neq \varnothing$, for each $i \in I$,
2. $P_i \cap P_j = \varnothing$, for all $i, j \in I$, $i \neq j$, and
3. $\bigcup_{i \in I} P_i = S$.

The subsets P_i, $i \in I$, are called the parts of the partition P.

Example 1.3. Let $S = \{1,2,3,4,5\}$. Then $P = \{\{1,3,5\},\{2,4,6\}\}$ and $Q = \{\{1,4\},\{2\},\{3,5\}\}\}$ are two different partitions of S.

Exercise 1.5. Let $\sim$ be an equivalence relation on a set A. Show that the following hold:

1. For all $a \in A$, $a \in [a]$, and hence, each equivalence class is non-empty and $A = \bigcup_{a\in A}[a]$.
2. For all $a, b \in A$, if $a \neq b$, then $[a] \cap [b] = \varnothing$ (i.e., any two equivalence classes are either disjoint or identical).
3. The set of all equivalence classes of $\sim$ is a partition of A.

Exercise 1.6. Let $P = \{P_i\}_{i\in I}$ be a partition of a set A. Define a relation $\sim$ on A as follows: For any $a, b \in A$, $a \sim b$ if and only if a and b belong to the same part of the partition P (i.e., $a, b \in P_i$, $\exists i \in I$). Show that the following hold:

1. The relation $\sim$ is an equivalence relation on A.
2. The equivalence classes of $\sim$ are exactly the parts of the partition of P.

1.5.2 Partial Order Relations

A reflexive, anti-symmetric, and transitive relation is called a partial order relation (or simply a partial order). For example, $\leq$ and $\geq$ on any set of real numbers, $|$ on any set of non-negative integers, and $\subseteq$ and $\supseteq$ on any set of sets are partial order relations. A set A together with a partial order $\preccurlyeq$ on it forms a partially ordered set or poset $(A, \preccurlyeq)$.

Note. The term *partial* refers to the fact that two particular elements in a partially ordered set may be incomparable – i.e., neither may be related to the other in the partial order. For instance, consider the subsets of $S = \{x, y, z\}$, which are partially ordered by the subset relation $\subseteq$ – i.e., consider the poset $(2^S, \subseteq)$. Then $A = \{x, y\}$ and $B = \{y, z\}$ are incomparable, as neither is A a subset of B, nor is B a subset of A. On the other hand, A and $C = \{x\}$ are comparable (as $C \subseteq A$), and A and S itself are also comparable (as $A \subseteq S$). A poset in which every pair of elements is comparable (i.e., in which there are no incomparable pairs of elements) is called a total order.

Exercise 1.7. Let $|$ denote the divides relation on any set of integers. That is, for any two integers m and n, define $m \mid n$ if and only if $n = km$ for some integer k.

1. Prove that $(\mathbb{N}, |)$ is a poset. Is $(\mathbb{N}_0, |)$ also a poset?
2. Is $(\mathbb{Z}, |)$ a poset?
3. Let $n \in \mathbb{N}$, and let P be the set of all positive divisors of n. Then show that $(P, |)$ is a poset. What are all the natural numbers n such that $(P, |)$ is a total order?

1.6 Functions

A function is a left-total, right-unique binary relation. In other words, a function $f : A \longrightarrow B$ is a relation from A to B such that each element of A is related to exactly one element of B under f. If $a \in A$ is related to $b \in B$ in f, then we say that f maps a to b, and write $b = f(a)$, or $a \longmapsto b$. A function is also called a mapping. Recall that A is the domain of f and B the codomain. We may also write $\operatorname{dom} f$ and $\operatorname{cod} f$ to denote the domain and codomain of

f, respectively. The image of f, denoted as $\operatorname{im} f$ or $f(A)$, is the set of all elements b of the codomain such that $b = f(a)$ for some $a \in A$. We can write this in the following two ways:

$$\operatorname{im} f = \{\, b \in B \mid b = f(a),\ \exists a \in A \,\}$$
$$\operatorname{im} f = \{\, f(a) \mid a \in A \,\}.$$

The preimage of any element of the codomain is the set of all elements of the domain that map to it. That is, for $b \in B$, the preimage of b, denoted $f^{-1}(b)$, is defined as

$$f^{-1}(b) = \{\, a \in A \mid f(a) = b \,\}.$$

Note that the image of the function is a subset of the codomain, while the preimage of an element is the subset of the domain.

Note. Intuitively, we think of a function as a rule that assigns, to each element of the domain, a unique element of the codomain. For instance, it is common in calculus to define a function using a formula – e.g., $f\colon \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = x^2 - 1$. However, the formula or the expression itself is not the function. The function $g\colon \mathbb{Z} \longrightarrow \mathbb{Q}$, defined by the formula $g(x) = x^2 - 1$, is different from the previously defined function f, although they are both defined using the same formula. Moreover, it may not be possible to define a function using any closed-form formula.

A function is injective (or 1-1) if it is left-unique. That is, $f\colon A \longrightarrow B$ is injective if, for any $a_1, a_2 \in A$, $f(a_1) = f(a_2)$ implies that $a_1 = a_2$. A surjective (or onto) function is one in which every element of the codomain has a non-empty preimage. That is, $f\colon A \longrightarrow B$ is surjective if, for each $b \in B$, $b = f(a)$ for some $a \in A$. Note that f is surjective if and only if $\operatorname{im} f = \operatorname{cod} f$.