Appendix A

Set theory and functions

A.1 Sets

We assume you have a working knowledge of (informal) set theory. Here, we only give a brief review.

Notation and definitions

A *set* S is a collection of *elements*. If x is an element of the set S, we write $x \in S$. Otherwise, we write $x \notin S$. An element of S may also be called a *member* or a *point* of S (or in S), and we may write that S *contains* x.

The set with no elements is called the *empty set* and is denoted $\emptyset$. A set with at least one element is *nonempty*. Other sets with standard names are:

$\mathbb{R}$	the set of all real numbers
$\mathbb{Z}$	the set of all integers
$\mathbb{N}$	the set of all positive integers
$\mathbb{Q}$	the set of all rational numbers
$\not{\mathbb{Q}}$	the set of all irrational numbers

A set can be described by listing its elements, as in $A := \{1, 3, 5, 7, 9\}$. (We use the symbol := when we define a mathematical object as equal to an already known or defined object, as in "$A := \{1, 3, 5, 7, 9\}$" above. Occasionally we also use it as a reminder that an equality is by definition, and that no computations or deep thinking are needed to justify it.)

More often, a set is described by a rule, for example,

$$B := \{ \, k \in \mathbb{N} \mid k \text{ leaves a remainder of 3 when divided by 5} \, \}, \tag{A.1.1}$$

where the vertical line means "such that" (some authors use a colon rather than vertical line).

If a, b are real numbers and $a \leq b$, we define $[a, b] := \{ \, x \in \mathbb{R} \mid a \leq x \leq b \, \}$ and $[a, b) := \{ \, x \in \mathbb{R} \mid a \leq x < b \, \}$. Similar definitions apply to $(a, b]$ and (a, b).

Let A, B be sets. The notation $A \subset B$ means that whenever $x \in A$, then $x \in B$. In this case, A is said to be a *subset* of B. Thus, $\emptyset \subset A$ for all A. If $A \subset B$ and $B \subset A$, we write $A = B$ and say that A and B are *equal* (or "the same"). Of course, $A = B$ if and only if $B = A$. If A and B are not equal, we write $A \neq B$. If $A \subset B$ but $A \neq B$, then A is a *proper subset* of B, denoted by $A \subsetneq B$. The *complement of B in A*, denoted $A \setminus B$, is the set of all elements in A that are not in B. Thus $\mathbb{R} \setminus \mathbb{Q} = \not{\mathbb{Q}}$. Some authors denote the complement of B in A by $A - B$.

Operations on sets

If A and B are sets, then their *union* $A \cup B$ and their *intersection* $A \cap B$ are defined by

$$\begin{aligned} A \cup B &:= \{\, x \mid x \text{ is in } A \text{ or } B \text{ or both} \,\} \\ A \cap B &:= \{\, x \mid x \text{ is in both } A \text{ and } B \,\} \end{aligned} \tag{A.1.2}$$

(In the definition of $\cup$, we could omit "or both", since in mathematics, "or" is always inclusive; in mathematical usage, "would you like tea or coffee?" could be answered, "I'd like both tea and coffee".)

The sets A and B are *disjoint* if $A \cap B = \emptyset$. Let $\mathcal{F}$ be a collection of sets. Then the elements in $\mathcal{F}$ are *pairwise disjoint* if any two distinct elements in $\mathcal{F}$ are disjoint.

If $\mathcal{F}$ is a collection of sets, then $\bigcup_{F \in \mathcal{F}} F$ denotes the union of all sets in $\mathcal{F}$ and $\bigcap_{F \in \mathcal{F}} F$ denotes the intersection of all sets in $\mathcal{F}$:

$$\bigcup_{F \in \mathcal{F}} F \quad := \quad \{\, x \mid x \in G \text{ for some } G \in \mathcal{F} \,\}, \tag{A.1.3}$$

$$\bigcap_{F \in \mathcal{F}} F \quad := \quad \{\, x \mid x \in G \text{ for each } G \in \mathcal{F} \,\}. \tag{A.1.4}$$

When $\mathcal{F}$ has only finitely many sets $F_1, \ldots, F_n$, then $\bigcup_{F \in \mathcal{F}} F$ is often written as $F_1 \cup \cdots \cup F_n$ or $\bigcup_{k=1}^{n} F_k$; similarly, $\bigcap_{F \in \mathcal{F}} F$ is often written as $F_1 \cap \cdots \cap F_n$ or $\bigcap_{k=1}^{n} F_k$.

Let $n \in \mathbb{N}$. An *ordered n-tuple* is an expression of the form $(a_1, \ldots, a_n)$. Two ordered n-tuples $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ are *equal* if and only if $a_k = b_k$ for all $1 \leq k \leq n$. When $n = 2$, an ordered n-tuple is called an *ordered pair.* If $A_1, \ldots, A_n$ are nonempty sets, the *Cartesian product*

$A_1 \times \cdots \times A_n$ is

$$A_1 \times \cdots \times A_n := \{(a_1, \ldots, a_n) \,|\, a_k \in A_k \text{ for all } 1 \leq k \leq n\}.$$

When $A_1, \ldots A_n$ are all equal to the same set A, then $A_1 \times \cdots \times A_n$ is often written A^n. Thus, $A^2 := A \times A$, $A^3 := A \times A \times A$, and so on.

A.2 Relations

Definition A.2.1 (Binary relation). Let A be a nonempty set. A *binary relation* $\mathcal{R}$ on A is any subset of $A^2 := A \times A$. If $(a, b) \in \mathcal{R}$, we write

$$a \, \mathcal{R} \, b.$$

We need to impose some properties on $\mathcal{R}$ for it to be of interest. One possibility is that $\mathcal{R}$ encodes some kind of order. In this case, it is usually denoted by $\preccurlyeq$.

Definition A.2.2 (Partial order). A *partial order* $\preccurlyeq$ on A is a binary relation on A satisfying the following properties:

1. $a \preccurlyeq b$ and $b \preccurlyeq c$ imply $a \preccurlyeq c$.
2. $a \preccurlyeq a$ for all $a \in A$.
3. If $a \preccurlyeq b$ and $b \preccurlyeq a$, then $a = b$.

Examples A.2.3. (Partial order).

1. Let $\preccurlyeq := \left\{ (x, y) \in \mathbb{R}^2 \mid x \leq y \right\}$. Then $\preccurlyeq$ is a partial order on $\mathbb{R}$.
2. Let S be any set and let $\mathcal{P}(S)$ be the collection of all subsets of S. Then

$$\preccurlyeq := \{ (E, F) \mid E \text{ and } F \text{ are subsets of } S,\ E \subset F \}$$

is a partial order on $\mathcal{P}(S)$. △

If $\preccurlyeq$ is a partial order on A, then A is *partially ordered* by $\preccurlyeq$. Thus part 2 above says that the collection of all subsets of a given set is partially ordered by *set inclusion*.

Definition A.2.4 (Total order). Let A be partially ordered by $\preccurlyeq$. A subset B of A is *totally ordered* (by $\preccurlyeq$) if for every x and y in B, either $x \preccurlyeq y$ or $y \preccurlyeq x$.

Examples A.2.5. (Total order).

1. If $\preccurlyeq := \left\{ (x, y) \in \mathbb{R}^2 \mid x \leq y \right\}$, any subset of $\mathbb{R}$ is totally ordered by $\preccurlyeq$.
2. Let $S := \{a, b\}$ and let $\mathcal{P}(S)$ and $\preccurlyeq$ be as in part 2 of Examples A.2.3. Then $\{\{a\}, \{b\}\}$ is not totally ordered by $\preccurlyeq$. △

Definition A.2.6 (Upper bound). Let A be partially ordered by $\preccurlyeq$ and let $B \subset A$. An *upper bound* for B is an element $a \in A$ such that $b \preccurlyeq a$ for all $b \in B$.

Example A.2.7. Let $\mathcal{P}(S)$ and $\preccurlyeq$ be as in part 2 of Examples A.2.3. Then $\{a, b\}$ is an upper bound for $\{\{a\}, \emptyset\}$ and $\{\{a\}, \{b\}\}$. △

Definition A.2.8 (Maximal element). Let A be partially ordered by $\preccurlyeq$ and let $B \subset A$. A *maximal element* of B is an element x_0 in B such that whenever $b \in B$ and $x_0 \preccurlyeq b$, then $b = x_0$.

Example A.2.9. Let $\preccurlyeq := \{(a,b) \in \mathbb{N}^2 \mid a \text{ is a factor of } b\}$. Then $\mathbb{N}$ is partially ordered by $\preccurlyeq$. Let $A := \{3,5,7,11,14,42\}$. Then 5, 11, and 42 are maximal elements of A. But 3, 7, and 14 are not maximal elements of A since $3 \preccurlyeq 42$, $7 \preccurlyeq 14$, and $14 \preccurlyeq 42$. If each member of a set B is a prime number, then every member of B is a maximal element of B. The set $C := \{2,4,6,8,\dots\}$ has no maximal elements and no element of $\mathbb{N}$ is an upper bound for C. △

Equivalence relations

A binary relation may also encode a notion of "sameness". It is often simpler to recognize the main features of a set X by grouping together similar elements of X. For example, the set $\mathbb{Z}$ of integers can be partitioned into three groups:

$$\begin{aligned} A &:= \{\, n \in \mathbb{Z} \mid n \text{ is divisible by } 3 \,\}, \\ B &:= \{\, n \in \mathbb{Z} \mid n \text{ leaves a remainder of 1 when divided by } 3 \,\}, \\ C &:= \{\, n \in \mathbb{Z} \mid n \text{ leaves a remainder of 2 when divided by } 3 \,\}. \end{aligned} \tag{A.2.1}$$

This idea of partitioning a set into groups consisting of similar objects is useful because then we are no longer distracted by the individual differences between elements of X but can focus on the main features of X as a whole. This is the idea behind "equivalence relations".

Definition A.2.10 (Equivalence relation). An *equivalence relation* on X is a binary relation $\sim$ on X such that the following properties are satisfied:

1. Reflexivity: $x \sim x$ for all $x \in X$.
2. Symmetry: $x \sim y$ if and only if $y \sim x$.
3. Transitivity: If $x \sim y$ and $y \sim z$, then $x \sim z$.

Examples A.2.11.

1. Define a binary relation $\mathcal{R}$ on $\mathbb{Z}$ by $a \,\mathcal{R}\, b$ if and only if $a - b$ is divisible by 3. Then it is easy to see that $\mathcal{R}$ satisfies properties 1 and 2 in Definition A.2.10. If $x \,\mathcal{R}\, y$ and $y \,\mathcal{R}\, z$, then $x - y = 3k$ and $y - z = 3\ell$ for some integers k, ℓ. Thus, $x - z = 3(k + \ell)$, so that $x - z$ is divisible by 3 also. Hence, $x \,\mathcal{R}\, z$. So $\mathcal{R}$ is an equivalence relation on $\mathbb{Z}$. Thus we could write $a \sim b$, but in number theory this relation is usually denoted $a \equiv b \mod 3$
2. Let L be the line in $\mathbb{R}^2$ given by the equation $y = x$. Define $\mathbf{a} \,\mathcal{R}\, \mathbf{b}$ to mean that $\mathbf{a} := \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \mathbf{b} := \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \in \mathbb{R}^2$ are points such that $\begin{pmatrix} a_1 - b_1 \\ a_2 - b_2 \end{pmatrix}$ lies on L. Then $\mathcal{R}$ satisfies property 1 because $\mathbf{0}$ lies on L. Of course,

$$\mathbf{a} \,\mathcal{R}\, \mathbf{b} \iff a_2 - b_2 = a_1 - b_1 \iff b_2 - a_2 = b_1 - a_1 \iff \mathbf{b} \,\mathcal{R}\, \mathbf{a}.$$