Appendix

Background Material

Historically speaking, it is of course quite untrue
that mathematics is free from contradiction;
non-contradiction appears as a goal to be achieved,
not as a God-given quality that has been granted us once for all.

Nicolas Bourbaki

1. SET THEORY

This section reviews some conventions about set theory which are used in this book, as well as some facts which will be referred to occasionally.

First, a remark about definitions: Any definition of a word or a phrase will have roughly the form

(1.1) *xxx* if @#&$% ,

where *xxx* is the word which is being defined and @#&$% is its defining property. For example, the sentence "An integer n is *positive* if $n > 0$" defines the notion of a positive integer. In a definition, the word *if* means *if and only if*. So in the definition of the positive integers, all integers which don't satisfy the requirement $n > 0$ are ruled out.

The notation

(1.2) {s ∈ S | @#&$%}

stands for the subset of S consisting of all elements s such that @#&$% is true. Thus if $\mathbb{Z}$ denotes the set of all integers, then $\mathbb{N} = \{n \in \mathbb{Z} \mid n > 0\}$ describes $\mathbb{N}$ as the set of positive integers or *natural numbers*.

Elements $a_1, \ldots, a_n$ of a set are said to be *distinct* if no two of them are equal.

A *map* φ from a set S to a set T is any function whose *domain* of definition is S and whose *range* is T. The words *function* and *map* are used synonymously. We require that a function be single-valued. This means that every element $s \in S$ must have a uniquely determined *image* $\varphi(s) \in T$. The range T of φ is not required to be the set of values of the function. By definition of a function, every image element $\varphi(s)$ is contained in T, but we allow the possibility that some elements $t \in T$ are not taken on by the function at all. We also take the domain and range of a function as part of its definition. If we restrict the domain to a subset, or if we extend the range, then the function obtained is considered to be different.

The domain and range of a map may also be described by the use of an arrow. Thus the notation $\varphi: S \to T$ tells us that φ is a map from S to T. The statement that $t = \varphi(s)$ may be described by a wiggly arrow: $s \rightsquigarrow t$ means that the element $s \in S$ is sent to $t \in T$ by the map under consideration. For example, the map $\varphi: \mathbb{Z} \to \mathbb{Z}$ such that $\varphi(n) = 2n + 1$ is described by $n \rightsquigarrow 2n + 1$.

The *image* of the map φ is the subset of T of elements which have the form $\varphi(s)$ for some $s \in S$. It will often be denoted by im φ, or by $\varphi(S)$:

(1.3) $$\operatorname{im} \varphi = \{t \in T \mid t = \varphi(s) \text{ for some } s \in S\}.$$

In case im φ is the whole range T, the map is said to be *surjective*. Thus φ is surjective if every $t \in T$ has the form $\varphi(s)$ for some $s \in S$.

The map φ is called *injective* if distinct elements s_1, s_2 of S have distinct images, that is, if $s_1 \neq s_2$ implies that $\varphi(s_1) \neq \varphi(s_2)$. A map which is both injective and surjective is called a *bijective* map. A *permutation* of a set S is a bijective map from S to itself.

Let $\varphi: S \to T$ and $\psi: T \to S$ be two maps. Then ψ is called an *inverse function* of φ if both of the composed maps $\varphi \circ \psi: T \to T$ and $\psi \circ \varphi: S \to S$ are the identity maps, that is, if $\varphi(\psi(t)) = t$ for all $t \in T$ and $\psi(\varphi(s)) = s$ for all $s \in S$. The inverse function is often denoted by φ^{-1}.

(1.4) **Proposition.** A map $\varphi: S \to T$ has an inverse function if and only if it is bijective.

Proof. Assume that φ has an inverse function ψ, and let us show that φ is both surjective and injective. Let t be any element of T, and let $s = \psi(t)$. Then $\varphi(s) = \varphi(\psi(t)) = t$. So t is in the image of φ. This shows that φ is surjective. Next, let s_1, s_2 be distinct elements of S, and let $t_i = \varphi(s_i)$. Then $\psi(t_i) = s_i$. So t_1, t_2 have distinct images in S, which shows that they are distinct. Therefore φ is injective. Conversely, assume that φ is bijective. Then since φ is surjective, every element $t \in T$ has the form $t = \varphi(s)$ for some $s \in S$. Since φ is injective, there can be only one such element s. So we define ψ by the following rule: $\psi(t)$ is the unique element $s \in S$ such that $\psi(s) = t$. This map is the required inverse function. □

Let $\varphi: S \to T$ be a map, and let U be a subset of T. The *inverse image* of U is defined to be the set

(1.5) $$\varphi^{-1}(U) = \{s \in S \mid \varphi(s) \in U\}.$$

This set is defined whether or not φ has an inverse function. The notation φ^{-1}, as used here, is symbolic.

A set is called *finite* if it contains finitely many elements. If so, the number of its elements, sometimes called its *cardinality*, will be denoted by $|S|$. We will also call this number the *order* of S. If S is infinite, we write $|S| = \infty$. The following theorem is quite elementary, but it is a very important principle.

(1.6) **Theorem.** Let $\varphi: S \to T$ be a map between finite sets.

(a) If φ is injective, then $|S| \leq |T|$.
(b) If φ is surjective, then $|S| \geq |T|$.
(c) If $|S| = |T|$, then φ is bijective if and only if it is either injective or surjective. □

The contrapositive of part (a) is often called the *pigeonhole principle*: *If* $|S| > |T|$, *then* φ *is not injective*. For example, if there are 87 socks in 79 drawers, then some drawer contains at least two socks.

An infinite set S is called *countable* if there is a bijective map $\varphi: \mathbb{N} \to S$ from the set of natural numbers to S. If there is no such map, then S is said to be *uncountable*.

(1.7) **Proposition.** The set $\mathbb{R}$ of real numbers is uncountable.

Proof. This proof is often referred to as Cantor's diagonal argument. Let $\varphi: \mathbb{N} \to \mathbb{R}$ be any map. We list the elements of the image of φ in the order $\varphi(1), \varphi(2), \varphi(3), \ldots$, and we write each of these real numbers in decimal notation. For example, the list might begin as follows:

$$\begin{array}{l}
\varphi(1) = 8\ 2\ .\underline{3}\ 5\ 4\ 7\ 0\ 9\ 8\ 4\ 5\ 3\ 4 \ldots \\
\varphi(2) = \quad\ \ .1\ \underline{2}\ 3\ 9\ 0\ 3\ 4\ 5\ 7\ 0\ 0 \ldots \\
\varphi(3) = \quad 5\ .9\ 0\ \underline{8}\ 4\ 0\ 5\ 9\ 8\ 6\ 7\ 5 \ldots \\
\varphi(4) = 1\ 2\ .8\ 7\ 4\ \underline{3}\ 5\ 2\ 6\ 4\ 4\ 4\ 4 \ldots \\
\varphi(5) = \quad\ \ .0\ 0\ 1\ 4\ \underline{4}\ 1\ 0\ 0\ 3\ 4\ 9 \ldots \\
\quad \vdots \qquad\qquad\qquad \vdots
\end{array}$$

We will now determine a real number which is not on the list. Consider the real number u whose decimal expansion consists of the underlined digits: $u = .3\ 2\ 8\ 3\ 4 \ldots$. We form a new real number by changing each of these digits, say

$$v = .4\ 5\ 1\ 4\ 2 \ldots .$$

Notice that $v \neq \varphi(1)$, because the first digit, 4, of v is not equal to the corresponding digit, 3, of $\varphi(1)$. Also, $v \neq \varphi(2)$, because the second digit, 5, of v is not equal to the corresponding digit of $\varphi(2)$. Similarly, $v \neq \varphi(n)$ for all n. This shows that φ is not surjective, which completes the proof, except for one point.

Some real numbers have two decimal expansions: .99999... is equal to 1.00000..., for example. This creates a problem with our argument. We have to choose v so that infinitely many of its digits are different from 9 and 0. The easiest way is to avoid these digits altogether. □