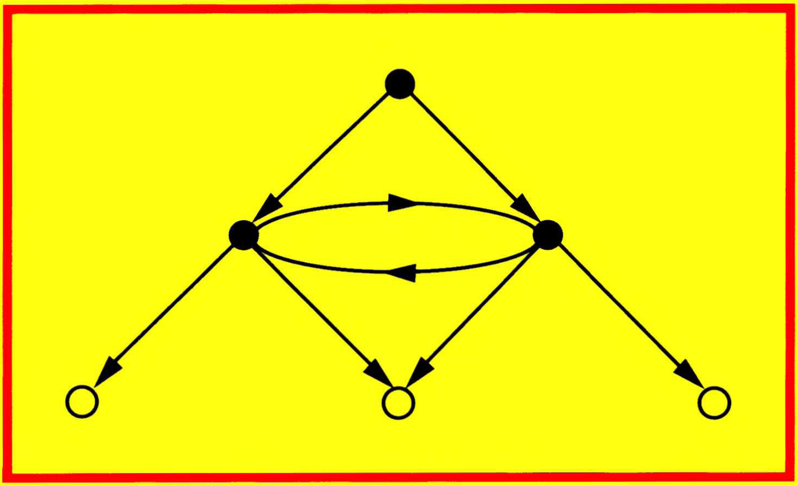
Undergraduate Texts in Mathematics

Keith Devlin

The Joy of Sets

Fundamentals of Contemporary Set Theory

Second Edition



Springer-Verlag

Keith Devlin

The Joy of Sets

Fundamentals of Contemporary Set Theory

Second Edition

With 11 illustrations

Springer-Verlag
New York Berlin Heidelberg London Paris
Tokyo Hong Kong Barcelona Budapest

1

Naive Set Theory

Zermelo–Fraenkel set theory, which forms the main topic of the book, is a rigorous theory, based on a precise set of axioms. However, it is possible to develop the theory of sets considerably without any knowledge of those axioms. Indeed, the axioms can only be fully understood after the theory *has* been investigated to some extent. This state of affairs is to be expected. The concept of a 'set of objects' is a very intuitive one, and, with care, considerable, sound progress may be made on the basis of this intuition alone. Then, by analyzing the nature of the 'set' concept on the basis of that initial progress, the axioms may be 'discovered' in a perfectly natural manner.

Following standard practice, I refer to the initial, intuitive development as 'naive set theory'. A more descriptive, though less concise, title would be 'set theory from the naive viewpoint'. Once the axioms have been introduced, this account of 'naive set theory' can be re-read, without any changes being necessary, as the elementary development of *axiomatic* set theory.

1.1 What is a Set?

In naive set theory we assume the existence of some given domain of 'objects', out of which we may build sets. Just what these objects are is of no interest to us. Our only concern is the behavior of the 'set' concept. This is, of course, a very common situation in mathematics. For example, in algebra, when we discuss a group, we are (usually) not interested in what the elements of the group are, but rather in the way the group operation acts upon those elements. When we come to develop our set theory axiomatically we shall, in fact, remove this assumption of an initial domain, since *everything* will then be a set; but that comes much later.

In set theory, there is really only one fundamental notion:

The ability to regard any collection of objects as a single entity (i.e. as a set).

It is by asking ourselves what may and what may not determine 'a collection' that we shall arrive at the axioms of set theory. For the present, we regard the two words 'set' and 'collection (of objects)' as synonymous and understood.

If a is an object and x is a set, we write

$$a \in x$$

to mean that a is an *element* of (or member of) x , and

$$a \notin x$$

to mean that a is not an element of x.

In set theory, perhaps more than in any other branch of mathematics, it is vital to set up a collection of symbolic abbreviations for various logical concepts. Because the basic assumptions of set theory are absolutely minimal, all but the most trivial assertions about sets tend to be logically complex, and a good system of abbreviations helps to make otherwise complex statements readable. For instance, the symbol $\in$ has already been introduced to abbreviate the phrase *'is an element of'*. I also make considerable use of the following (standard) logical symbols:

$\rightarrow$	abbreviates	'implies'
$\leftrightarrow$	abbreviates	'if and only if'
$\neg$	abbreviates	'not'
$\wedge$	abbreviates	'and'
$\vee$	abbreviates	'or'
$\forall$	abbreviates	'for all'
$\exists$	abbreviates	'there exists'.

Note that in the case of 'or' we adopt the usual, mathematical interpretation, whereby $\phi \vee \psi$ means that either ϕ is true or ψ is true, or else both ϕ and ψ are true, where ϕ, ψ denote any assertions in any language.

The above logical notions are not totally independent, of course. For instance, for any statements, we have

$$\begin{array}{lll}\phi \leftrightarrow \psi & \text{is the same as} & (\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi) \\ \phi \rightarrow \psi & \text{is the same as} & (\neg\phi) \vee \psi \\ \phi \vee \psi & \text{is the same as} & \neg((\neg\phi) \wedge (\neg\psi)) \\ \exists x\phi & \text{is the same as} & \neg((\forall x)(\neg\phi))\end{array}$$

where the phrase 'is the same as' means that the two expressions are logically equivalent.

Exercise 1.1.1. *Let $\phi\dot{\vee}\psi$ mean that exactly one of ϕ, ψ is true. Express $\phi\dot{\vee}\psi$ in terms of the symbols introduced above.*

Let us return now to the notion of a set. Since a set is the same as a collection of objects, a set will be uniquely determined once we know what its elements are. In symbols, this fact can be expressed as follows:

$$x = y \leftrightarrow \forall a[(a \in x) \leftrightarrow (a \in y)].$$

This principle will, in fact, form one of our axioms of set theory: the *Axiom of Extensionality.*

If x, y are sets, we say x is a subset of y if and only if every element of x is an element of y, and write

$$x \subseteq y$$

in this case. In symbols, this definition reads[1]

$$(x \subseteq y) \leftrightarrow \forall a[(a \in x) \rightarrow (a \in y)].$$

We write

$$x \subset y$$

in case x is a subset of y and x is not equal to y; thus:

$$(x \subset y) \leftrightarrow (x \subseteq y) \wedge (x \neq y)$$

where, as usual, we write $x \neq y$ instead of $\neg(x = y)$, just as we did with $\in$. Clearly we have

$$(x = y) \leftrightarrow [(x \subseteq y) \wedge (y \subseteq x)].$$

Exercise 1.1.2. *Check the above assertion by replacing the subset symbol by its definition given above, and reducing the resulting formula logically to the axiom of extensionality. Is the above statement an equivalent formulation of the axiom of extensionality?*

[1]The reader should attain the facility of 'reading' symbolic expressions such as this as soon as possible. In more complex situations the symbolic form can be by far the most intelligible one.

1.2 Operations on Sets

There are a number of simple operations that can be performed on sets, forming new sets from given sets. I consider below the most common of these.

If x and y are sets, the *union* of x and y is the set consisting of the members of x together with the members of y, and is denoted by

$$x \cup y.$$

Thus, in symbols, we have

$$(z = x \cup y) \leftrightarrow \forall a[(a \in z) \leftrightarrow (a \in x \vee a \in y)].$$

In the above, in order to avoid proliferation of brackets, I have adopted the convention that the symbol $\in$ predominates over logical symbols. This convention, and a similar one for $=$, will be adhered to throughout. An alternative way of denoting the above definition is

$$(a \in x \cup y) \leftrightarrow (a \in x \vee a \in y).$$

Using this last formulation, it is easy to show that the union operation on sets is both commutative and associative; thus

$$x \cup y = y \cup x,$$

$$x \cup (y \cup z) = (x \cup y) \cup z.$$

The beginner should check these and any similar assertions made in this chapter.

The *intersection* of sets x and y is the set consisting of those objects that are members of both x and y, and is denoted by

$$x \cap y.$$

Thus

$$(a \in x \cap y) \leftrightarrow (a \in x \wedge a \in y).$$

The intersection operation is also commutative and associative.

The (*set-theoretic*) *difference* of sets x and y is the set consisting of those elements of x that are not elements of y, and is denoted by

$$x - y.$$

Thus

$$(a \in x - y) \leftrightarrow (a \in x \wedge a \notin y).$$

Care should be exercised with the difference operation at first. Notice that $x - y$ is always defined and is always a subset of x, regardless of whether y is a subset of x or not.

Exercise 1.2.1. *Prove the following assertions directly from the definitions. The drawing of 'Venn diagrams' is forbidden; this is an exercise in the manipulation of logical formalisms.*

(i) $x \cup x = x \;\; ; \quad x \cap x = x$;

(ii) $x \subseteq x \cup y \;\; ; \quad x \cap y \subseteq x$;

(iii) $[(x \subseteq z) \wedge (y \subseteq z)] \rightarrow [x \cup y \subseteq z]$;

(iv) $[(z \subseteq x) \wedge (z \subseteq y)] \rightarrow [z \subseteq x \cap y]$;

(v) $x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$;

(vi) $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$;

(vii) $(x \subseteq y) \leftrightarrow (x \cap y = x) \leftrightarrow (x \cup y = y)$.

Exercise 1.2.2. *Let x, y be subsets of a set z. Prove the following assertions:*

(i) $z - (z - x) = x$;

(ii) $(x \subseteq y) \leftrightarrow [(z - y) \subseteq (z - x)]$;

(iii) $x \cup (z - x) = z$;

(iv) $z - (x \cup y) = (z - x) \cap (z - y)$;

(v) $z - (x \cap y) = (z - x) \cup (z - y)$.

Exercise 1.2.3. *Prove that for any sets x, y,*

$$x - y = x - (x \cap y).$$

In set theory, it is convenient to regard the collection of no objects as a set, the *empty* (or *null*) *set*. This set is usually denoted by the symbol $\emptyset$, a derivation from a Scandinavian letter.

Exercise 1.2.4. *Prove, from the axiom of extensionality, that there is only one empty set. (This requires a sound mastery of the elementary logical concepts introduced earlier.)*

Two sets x and y are said to be *disjoint* if they have no members in common; in symbols,

$$x \cap y = \emptyset.$$

Exercise 1.2.5. *Prove the following*:

(i) $x - \emptyset = x$;

(ii) $x - x = \emptyset$;

(iii) $x \cap (y - x) = \emptyset$;

(iv) $\emptyset \subseteq x$.

1.3 Notation for Sets

Suppose we wish to provide an accurate description of a set x. How can we do this? Well, if the set concerned is finite, we can enumerate its members: if x consists of the objects $a_1, \ldots, a_n$, we can denote x by

$$\{a_1, \ldots, a_n\}.$$

Thus, the statement

$$x = \{a_1, \ldots, a_n\}$$

should be read as 'x is the set whose elements are $a_1, \ldots, a_n$'. For example, the *singleton* of a is the set

$$\{a\}$$

and the *doubleton* of a, b is the set

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

In the case of infinite sets, we sometimes write

$$\{a_1, a_2, a_3, \ldots\}$$

to denote the set whose elements are precisely

$$a_1, a_2, a_3, \ldots .$$

An alternative notation is possible in the case where the set concerned is defined by some *property* P: if x is the set of all those a for which $P(a)$ holds, we may write

$$x = \{a \mid P(a)\}.$$

Thus, for example, the set of all real numbers may be denoted by

$$\{a \mid a \text{ is a real number}\}.$$

Exercise 1.3.1. *Prove the following equalities*:

(i) $x \cup y = \{a \mid a \in x \vee a \in y\}$;

(ii) $x \cap y = \{a \mid a \in x \wedge a \in y\}$;

(iii) $x - y = \{a \mid a \in x \wedge a \notin y\}$.

1.4 Sets of Sets

So far, I have been tacitly distinguishing between sets and objects. Admittedly, I did not restrict in any way the choice of initial objects — they could themselves be sets; but I did distinguish these initial objects from the sets of those objects that we could form. However, as I said at the beginning, the main idea in set theory is that any collection of objects can be regarded as a single entity (i.e. a set). Thus we are entitled to build sets out of entities that are themselves sets. Commencing with some given domain of objects then, we can first build sets of those objects, then sets of sets of objects, then sets of sets of sets of objects, and so on. Indeed, we can make more complicated sets, some of whose elements are basic objects, and some of which are sets of basic objects, etc.

For example, we can *define* the ordered pair of two objects a, b by

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

According to this definition, (a, b) is a set: it is a set of sets of objects.

Exercise 1.4.1. *Show that the above definition does define an ordered-pair operation; i.e. prove that for any a, b, a', b'*

$$(a, b) = (a', b') \leftrightarrow (a = a' \wedge b = b').$$

(Don't forget the case $a = b$.)

The inverse operations $(-)_0, (-)_1$ to the ordered pair are defined thus: if $x = (a, b)$, then $(x)_0 = a$ and $(x)_1 = b$. If x is not an ordered pair, $(x)_0$ and $(x)_1$ are undefined.

The *n-tuple* $(a_1, \ldots, a_n)$ may now be defined iteratively, thus

$$(a_1, \ldots, a_n) = ((a_1, \ldots, a_{n-1}), a_n).$$

It is clear that

$$(a_1, \ldots, a_n) = (a'_1, \ldots, a'_n) \quad \text{if and only if} \quad a_1 = a'_1 \wedge \ \ldots \ \wedge a_n = a'_n.$$

The inverse operations to the n-tuple are defined in the obvious way, so that if $x = (a_0, \ldots, a_{n-1})$, then $(x)^n_0 = a_0, \ldots, (x)^n_{n-1} = a_{n-1}$.

Of course, it is not important how an ordered-pair operation is defined. What counts is its behavior. Thus, the property described in Exercise 1.4.1 is the only requirement we have of an ordered pair. In naive set theory, we could just take (a, b) as a basic, undefined operation from pairs of objects to objects. But when we come to axiomatic set theory a definition of the ordered pair operation in terms of sets, such as the one above, will be necessary. Though there are other definitions, the one given is the most common, and it is the one I shall use throughout this book.

If x is any set, the collection of *all* subsets of x is a well-defined collection of objects and, hence, may itself be regarded as an entity (i.e. set). It is called the *power set* of x, denoted by $\mathcal{P}(x)$. Thus

$$\mathcal{P}(x) = \{y \mid y \subseteq x\}.$$

Suppose now that x is a set of sets of objects. The *union* of x is the set of all elements of all elements of x, and is denoted by $\bigcup x$. Thus

$$\bigcup x = \{a \mid \exists y(y \in x \wedge a \in y)\}.$$

Extending our logical notation by writing

$$(\exists y \in x)$$

to mean 'there exists a y in x such that', this may be re-written as

$$\bigcup x = \{a \mid (\exists y \in x)(a \in y)\}.$$

The *intersection* of x is the set of all objects that are elements of all elements of x, and is denoted by $\bigcap x$. Thus

$$\bigcap x = \{a \mid \forall y(y \in x \to a \in y)\}.$$

Or, more succinctly,

$$\bigcap x = \{a \mid (\forall y \in x)(a \in y)\}$$

where $(\forall y \in x)$ means 'for all y in x'.

If $x = \{y_i \mid i \in I\}$ (so I is some indexing set for the elements of x), we often write

$$\textstyle\bigcup_{i \in I} y_i$$

for $\bigcup x$ and

$$\bigcap_{i \in I} y_i$$

for $\bigcap x$. This ties in with our earlier notation to some extent, since we clearly have, for any sets x, y,

$$x \cup y = \bigcup\{x, y\}, \quad x \cap y = \bigcap\{x, y\}.$$

Exercise 1.4.2.

(i) *What are* $\bigcup\{x\}$ *and* $\bigcap\{x\}$?

(ii) *What are* $\bigcup\emptyset$ *and* $\bigcap\emptyset$?

Verify your answers.

Exercise 1.4.3. *Prove that if* $\{x_i \mid i \in I\}$ *is a family of sets, then*

(i) $\bigcup_{i \in I} x_i = \{a \mid (\exists i \in I)(a \in x_i)\}$;

(ii) $\bigcap_{i \in I} x_i = \{a \mid (\forall i \in I)(a \in x_i)\}$.

Exercise 1.4.4. *Prove the following:*

(i) $(\forall i \in I)(x_i \subseteq y) \to (\bigcup_{i \in I} x_i \subseteq y)$;

(ii) $(\forall i \in I)(y \subseteq x_i) \to (y \subseteq \bigcap_{i \in I} x_i)$;

(iii) $\bigcup_{i \in I}(x_i \cup y_i) = (\bigcup_{i \in I} x_i) \cup (\bigcup_{i \in I} y_i)$;

(iv) $\bigcap_{i \in I}(x_i \cap y_i) = (\bigcap_{i \in I} x_i) \cap (\bigcap_{i \in I} y_i)$;

(v) $\bigcup_{i \in I}(x_i \cap y) = (\bigcup_{i \in I} x_i) \cap y$;

(vi) $\bigcap_{i \in I}(x_i \cup y) = (\bigcap_{i \in I} x_i) \cup y$.

Exercise 1.4.5. *Let* $\{x_i \mid i \in I\}$ *be a family of subsets of* z. *Prove:*

(i) $z - \bigcup_{i \in I} x_i = \bigcap_{i \in I}(z - x_i)$;

(ii) $z - \bigcap_{i \in I} x_i = \bigcup_{i \in I}(z - x_i)$.

1.5 Relations

If x, y are sets, the *cartesian product* of x and y is defined to be the set

$$x \times y = \{(a, b) \mid a \in x \wedge b \in y\}.$$

More generally, if $x_1, \ldots, x_n$ are sets, we define their cartesian product by

$$x_1 \times \ldots \times x_n = \{(a_1, \ldots, a_n) \mid a_1 \in x_1 \wedge \ \ldots \ \wedge a_n \in x_n\}.$$

A *unary relation* on a set x is defined to be a subset of x. An n-ary relation on x, for $n > 1$, is a subset of the n-fold cartesian product $x \times \ldots \times x$.

Notice that an n-ary relation on x is a unary relation on the n-fold product $x \times \ldots \times x$.

These formal definitions provide a concrete realization within set theory of the intuitive concept of a relation.

However, as is often the case in set theory, having seen how a concept may be defined set-theoretically, we revert at once to the more familiar notation. For example, if P is some property that applies to pairs of elements of a set x, we often speak of 'the binary relation P on x', though strictly speaking, the relation concerned is the *set*

$$\{(a, b) \mid a \in x \wedge b \in x \wedge P(x, y)\}.$$

Also common is the tacit identification of such a property P with the relation it defines, so that $P(a, b)$ and $(a, b) \in P$ mean the same.

Similarly, going in the opposite direction, if R is some binary relation on a set x, I often write $R(a, b)$ instead of $(a, b) \in R$. Indeed, in the specific case of binary relations, I sometimes go even further, writing aRb instead of $R(a, b)$. In the case of ordering relations, this notation is, of course, very common: we rarely write $< (a, b)$ or $(a, b) \in <$, though from a set-theoretic point of view, both could be said to be more accurate than the more common notation $a < b$.

Binary relations play a particularly important role in set theory and, indeed, in mathematics as a whole. The rest of this section is devoted to a rapid review of binary relations.

There are several properties that apply to binary relations. Let R denote any binary relation on a set x. We say:

R	is *reflexive*	if	$(\forall a \in x)(aRa)$;
R	is *symmetric*	if	$(\forall a, b \in x)(aRb \rightarrow bRa)$;
R	is *antisymmetric*	if	$(\forall a, b \in x)[(aRb \wedge a \neq b) \rightarrow \neg(bRa)]$;
R	is *connected*	if	$(\forall a, b \in x)[(a \neq b) \rightarrow (aRb \vee bRa)]$;
R	is *transitive*	if	$(\forall a, b, c \in x)[(aRb \wedge bRc) \rightarrow (aRc)]$.

Notice the obvious use of the repeated quantifier in the above, writing, for example, $(\forall a, b \in x)$ instead of the more cumbersome $(\forall a \in x)(\forall b \in x)$.

Exercise 1.5.1. *Which of the above properties are satisfied by the membership relation $\in$ on a set x ?*

A binary relation on a set is said to be an *equivalence relation* just in case it is reflexive, symmetric, and transitive. If R is an equivalence relation on a set x, the *equivalence class* of an element a of x under the equivalence relation R is defined to be the set

$$[a] = [a]_R = \{b \in x \mid aRb\}.$$

Exercise 1.5.2. *Let R be an equivalence relation on a set x. Then R partitions x into a collection of disjoint equivalence classes.*

Examples of equivalence relations pervade the whole of contemporary pure mathematics. So too do examples of our next concept, that of an ordering relation.

A *partial ordering* of a set x is a binary relation on x which is reflexive, antisymmetric, and transitive. Usually (but not always), partial orderings are denoted by the symbol $\leq$.

A *partially ordered set*, or *poset*, consists of a set x together with a partial ordering $\leq$ of x. More formally, we define the poset to be the ordered pair $(x, \leq)$.

Let $(x, \leq)$ be a poset, and let $y \subseteq x$. An element a of y is a *minimal element* of y if and only if there is no b in y such that $b < a$, where, as usual, we write $b < a$ to denote $b \leq a \wedge b \neq a$.

A poset $(x, \leq)$ is said to be *well-founded* if every nonempty subset of x has a minimal element. (Equivalently, we often say that the ordering relation $\leq$ is well-founded.)

Lemma 1.5.1 Let $(x, \leq)$ be a poset. $(x, \leq)$ is well-founded if and only if there is no sequence $\{a_n\}_{n=0}^{\infty}$ of elements of x such that $a_{n+1} < a_n$ for all n, i.e. no sequence $\{a_n\}_{n=0}^{\infty}$ such that $a_0 > a_1 > a_2 > \ldots$.

Proof: Suppose $(x, \leq)$ is not well-founded. Let $y \subseteq x$ have no minimal element. Let $a_0 \in y$. Since a_0 is not minimal in y, we can find $a_1 \in y$, $a_1 < a_0$. Again, a_1 is not minimal in y, so we can find $a_2 \in y$, $a_2 < a_1$. Proceeding inductively, we obtain a sequence $a_0 > a_1 > a_2 > \ldots$.

Now suppose there is a sequence $a_0 > a_1 > a_2 > \ldots$. Let y be the set $\{a_0, a_1, a_2, \ldots\}$. Clearly, y has no minimal member. □

The subset relation $\subseteq$ on the power set, $\mathcal{P}(x)$, of a set x clearly constitutes a partial ordering of $\mathcal{P}(x)$. Indeed, the subset relation on *any* collection of sets is a partial ordering of that collection. In fact, up to isomorphism, the subset relation is the *only* partial ordering there is, as I prove next.

Theorem 1.5.2 Let $(x, \leq)$ be a poset. Then there is a set y of subsets of x such that $(x, \leq) \cong (y, \subseteq)$.

Proof: For each $a \in x$, let $z_a = \{b \in x \mid b \leq a\}$, and let $y = \{z_a \mid a \in x\}$. Define a map π from x to y by $\pi(a) = z_a$. Clearly π is a bijection. Moreover, $a_1 \leq a_2 \leftrightarrow z_{a_1} \subseteq z_{a_2}$, so π is an isomorphism between $(x, \leq)$ and $(y, \subseteq)$. □

A *total ordering* (or *linear ordering*) of a set x is a connected, partial ordering of x. A *totally ordered set* (or *toset*) is a pair $(x, \leq)$ such that $\leq$ is a total ordering of the set x.

A *well-ordering* of a set x is a well-founded, total ordering of x. A *well-ordered set* (or *woset*) is a pair $(x, \leq)$ such that $\leq$ is a well-ordering of x. The concept of a well-ordering is central in set theory, as we see presently.

1.6 Functions

We all know, more or less, what a function is. Indeed, in Section 1.5 we have already made use of functions in stating and proving Theorem 1.5.2. But there we followed the usual mathematical practice of using the function concept without worrying too much about what a function really is. In this section we give a formal, set-theoretic definition of the function concept.

Let R be an $(n+1)$-ary relation on a set x. The *domain* of R is defined to be the set

$$\mathrm{dom}(R) = \{a \mid \exists b[(a, b) \in R]\}.$$

The *range* of R is defined to be the set

$$\mathrm{ran}(R) = \{b \mid \exists a[(a, b) \in R]\}.$$

If $n = 1$, so that R is a binary relation, then it is clear what is meant by these definitions: elements of R are ordered pairs, $\mathrm{dom}(R)$ is the set of first components of members of R, and $\mathrm{ran}(R)$ the set of second components. But what if $n > 1$? In this case, any member of R will be an $(n + 1)$-tuple. But what is an $(n + 1)$-tuple? Well, by definition, an $(n + 1)$-tuple, c, has the form (a, b) where a is an n-tuple and b is an object in x. Thus, even if $n > 1$, the elements of R will still be *ordered pairs*, only now the domain of R will consist not of elements of x but elements of the n-fold product $x \times \ldots \times x$. So in all cases, $\mathrm{dom}(R)$ is the set of first components of members of R and $\mathrm{ran}(R)$ is the set of second components.

Although the notions of domain and range for an arbitrary relation are quite common in more advanced parts of set theory, chances are that the reader is not used to these concepts. But when we define the notion of a function as a special sort of relation, as we do below, you will see at once that the above definitions coincide with what one usually means by the 'domain' and 'range' of a function.

An n-ary *function* on a set x is an $(n+1)$-ary relation, R, on x such that for every $a \in \mathrm{dom}(R)$ there is exactly one $b \in \mathrm{ran}(R)$ such that $(a, b) \in R$.

As usual, if R is an n-ary function on x and $a_1, \ldots, a_n, b \in x$, we write

$$R(a_1, \ldots, a_n) = b$$

instead of

$$(a_1, \ldots, a_n, b) \in R.$$

Exercise 1.6.1. *Comment on the assertion that a set-theorist is a person for whom all functions are unary. (This is a serious exercise, and concerns a subtle point which often causes problems for the beginner.)*

I write

$$f : x \to y$$

to denote that f is a function such that $\mathrm{dom}(f) = x$ and $\mathrm{ran}(f) \subseteq y$.

Notice that if $f : x \to y$, then $f \subseteq x \times y$.

A *constant function* from a set x to a set y is a function of the form

$$f = \{(a, k) \mid a \in \mathrm{dom}(f)\}$$

where k is a fixed member of y.

The *identity function* on x is the unary function defined by

$$\mathrm{id}_x = \{(a, a) \mid a \in x\}.$$

If $f : x \to y$ and $g : y \to z$, we define $g \circ f : x \to z$ by

$$g \circ f(a) = g(f(a))$$

for all $a \in x$.

Exercise 1.6.2. *Express $g \circ f$ as a set of ordered pairs.*

Let $f : x \to y$. If $u \subseteq x$, we define the *image* of u under f to be the set

$$f[u] = \{f(a) \mid a \in u\};$$

and if $v \subseteq y$, we define the *preimage* of v under f to be the set

$$f^{-1}[v] = \{a \in x \mid f(a) \in v\}.$$

Exercise 1.6.3. *Let $f : x \to y$, and let $v_i \in y$, for $i \in I$. Prove that:*

(i) $f^{-1}\bigcup_{i\in I}[v_i] = \bigcup_{i\in I} f^{-1}[v_i]$;

(ii) $f^{-1}\bigcap_{i\in I}[v_i] = \bigcap_{i\in I} f^{-1}[v_i]$;

(iii) $f^{-1}[v_i - v_j] = f^{-1}[v_i] - f^{-1}[v_j]$.

If $f : x \to y$ and $u \subseteq x$, we define the *restriction* of f to u by

$$f \quad u = \{(a, f(a)) \mid a \in u\}.$$

Notice that $f \quad u$ is a function, with domain u.

Exercise 1.6.4. *Prove that if $f : x \to y$ and $u \subseteq x$, then*

(i) $f[u] = \mathrm{ran}(f \quad u)$;

(ii) $f \quad u = f \cap (u \times ran(f))$.

Let $f : x \to y$. We say f is *injective* (or *one-one*) if and only if

$$a \neq b \to f(a) \neq f(b).$$

We say f is *surjective* (or *onto*) (relative to the given set y) if and only if

$$f[x] = y.$$

We say f is *bijective* if and only if it is both injective and surjective. In this last case we often write $f : x \leftrightarrow y$.

If $f : x \to y$ is bijective, then f has a unique inverse function, f^{-1}, defined by

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

Thus, $f^{-1} : y \to x$, $f^{-1} \circ f = \mathrm{id}_x$, and $f \circ f^{-1} = \mathrm{id}_y$.

Notice that whenever $f : x \to y$ and $v \subseteq y$, then the *set* $f^{-1}[v]$ is defined, regardless of whether f is bijective (and hence has an inverse function) or not. If, in fact, f is bijective, so that f^{-1} exists, then the two possible interpretations of $f^{-1}[v]$ clearly coincide. Thus, our choice of notation should cause no problems.

Having defined the notion of a function now, we may give a very general definition of a 'cartesian product' of an arbitrary (possibly infinite) family of sets.

Let $x_i, i \in I$, be a family of sets. The *cartesian product* of the family $\{x_i \mid i \in I\}$ is defined to be the set

$$\textstyle\prod_{i \in I} x_i = \{f \mid (f : I \to \bigcup_{i \in I} x_i) \wedge (\forall i \in I)(f(i) \in x_i)\}.$$

If $x_i = x$ for all $i \in I$, we write x^I instead of $\prod_{i \in I} x_i$.

Now, in case I is finite, the above identity provides us with a second definition of 'cartesian product', quite different from the first. However, though formally different, the two notions of finite cartesian product are clearly closely related, and either definition of product may be used. In general, we use the original definition for finite products, using the notation $x_1 \times \ldots \times x_n$, and the above definition for infinite (or arbitrary) products, writing $\prod_{i \in I} x_i$.

Exercise 1.6.5. *What set is the cartesian product $x^{\{1\}}$?*

Exercise 1.6.6. *The ordered-pair operation (a, b) defines a binary function on sets. The inverse functions to the function are defined as follows: if $w = (a, b)$, then $(w)_0 = a$ and $(w)_1 = b$.*

Prove that if w is an ordered pair, then

(i) $(w)_0 = \bigcup \bigcap w$;

(ii) $(w)_1 = \begin{cases} \bigcup [\bigcup w - \bigcap w] & , \text{ if } \bigcup w \neq \bigcap w \\ \bigcup \bigcup w & , \text{ if } \bigcup w = \bigcap w \end{cases}$

To avoid unnecessary complication, I have not bothered to specify the set on which the above functions are defined. This is, of course, common mathematical practice when one is only interested in the behavior of the functions concerned.

1.7 Well-Orderings and Ordinals

I promised earlier that well-orderings would return, and here they come. I start out by explaining why well-orderings play an important role in set theory.

You are doubtless familiar with the principle of mathematical induction in proving results about the positive integers. Indeed, this method is not restricted to proving results about the positive integers but will work for any set that may be enumerated as a sequence $\{a_n\}_{n=0}^{\infty}$ indexed by the positive integers. Now what makes the induction method work is the fact that the positive integers are well-ordered. There is, after all, no real possibility of ever proving, case by case, that some property $P(n)$ holds for *every* positive integer n. But since the positive integers are well-ordered, if $P(n)$ were ever to fail, it would fail at a *least* n, and then we would have $P(n-1)$ true but $P(n)$ false, and it is precisely this situation that we exclude in our 'induction proof'.

Is it possible to extend this powerful method of proof to cover transfinite sets that are not enumerable as an integer-indexed sequence? Well, a natural place to start looking for an answer is to see if we can extend the positive integers into the transfinite, to obtain a system of numbers suitable for enumerating any set, however large. To do this we adopt more or less the same method that a small child uses when learning the number concept. The child first learns to count collections, by enumerating them in a linear way, and then, after repeating this process many times, abstracts from it the concept of 'natural number'. This is just what we will do, only in a more formal manner. Of course, since we are going to allow infinite collections, we shall not be doing any actual 'counting', but the concept of a well-ordering will provide the mathematical counterpart to this.

Recall that a well-ordering of a set x is a total ordering of x that is well-founded. Now, according to our previous definition, a partial ordering of a set x is well-founded if and only if every nonempty subset y of x has a minimal element (i.e. an element of y having no predecessor in y). But in the case of total orderings, an element of a subset y of x will be minimal if and only if it is the unique smallest member of y. Thus an alternative definition of a well-ordering of a set x is a total ordering of x such that every nonempty subset of x has a (unique) smallest member. This formulation enables us to prove:

Theorem 1.7.1 [Induction on a Well-Ordering] Let $(X, \leq)$ be a woset. Let E be a subset of X such that:

(i) the smallest element of X is a member of E;

(ii) for any $x \in X$, if $\forall y[y < x \to y \in E]$, then $x \in E$.

Then $E = X$.

Proof: Suppose $E \neq X$. Let x be the smallest member of the nonempty set $X - E$. Then, by (i), x is not the smallest member of X. But by choice of x, we have $y < x \to y \in E$. Hence, by (ii), $x \in E$, a contradiction. □

Notice the notation adopted above. I used capital letters to denote sets and lower-case letters to denote their elements. This is a very common notational convention, which I shall often adopt. Of course, it is really only helpful in simple situations; once there are sets of sets floating about it becomes rather confusing.

Theorem 1.7.1 allows us to prove results by induction on a well-founded set, but it does not provide us with a system of transfinite numbers for 'counting'. For that we need to isolate just what it is that all wosets have in common. So we commence by comparing wosets.

Let $(X, \leq)$, $(X', \leq')$ be wosets. A function $f : X \to X'$ is an *order isomorphism* if and only if f is bijective and

$$x < y \to f(x) <' f(y).$$

I write $f : X \cong X'$ in this case. (As usual, I adopt the convention of writing X in place of $(X, \leq)$, etc., it being clear from the context that X is a set with a well-ordering here.)

Theorem 1.7.2 Let $(X, \leq)$ be a woset, $Y \subseteq X$, $f : X \cong Y$. Then for all $x \in X$, $x \leq f(x)$.

Proof: Let $E = \{x \in X \mid f(x) < x\}$. We must prove that $E = \emptyset$. Suppose otherwise. Then E has a smallest member, x_0. Since $x_0 \in E$, it follows that $f(x_0) < x_0$. Let $x_1 = f(x_0)$. Since $x_1 < x_0$, applying f gives $f(x_1) < f(x_0)$. Thus $f(x_1) < x_1$. Thus $x_1 \in E$.

But $x_1 < x_0$, so this contradicts the choice of x_0 as the least member of E, and the proof is complete. □

Theorem 1.7.3 Let $(X, \leq)$, $(X', \leq')$ be wosets. If $(X, \leq) \cong (X', \leq')$, there is exactly one order-isomorphism $f : X \cong X'$.

Proof: Let $f : X \to X'$, $g : X \to X'$. Set $h = f^{-1} \circ g$. It is easily seen that $h : X \cong X$. So, by Theorem 1.7.2, $x \le h(x)$ for all $x \in X$. So, applying f, we see that for any $x \in X, f(x) \le f(h(x)) = g(x)$. Similarly, $g(x) \le f(x)$ for any $x \in X$. Thus $f = g$, and the proof is complete. □

It should be noticed that the above result does not hold for any tosets; well-ordering is essential. For example, let $\mathcal{Z}$ be the set of all integers, $\le$ the usual ordering on $\mathcal{Z}$. For any integer m, the mapping $f_m : \mathcal{Z} \to \mathcal{Z}$ defined by $f_m(n) = n+m$ is an order-isomorphism, and $m \ne m'$ implies $f_m \ne f_{m'}$.

Notice also that if $m < 0$, then $f_m(n) < n$ for all n, so this example also shows that Theorem 1.7.2 requires well-ordering as well.

Let $(X, \le)$ be a woset, $a \in X$. By the *segment* X_a of X determined by a we mean the set

$$X_a = \{x \in X \mid x < a\}.$$

Theorem 1.7.4 Let $(X, \le)$ be a woset. There is no isomorphism of X onto a segment of X.

Proof: Suppose $f : X \cong X_a$. By Theorem 1.7.2, $x \le f(x)$ for all x in X. In particular, therefore, $a \le f(a)$. But $\mathrm{ran}(f) = X_a$, so $f(a) \in X_a$, giving $f(a) < a$, a contradiction. □

Notice that well-ordering is required for Theorem 1.7.4. For example, let $\mathcal{Z}^-$ denote the nonpositive integers, and define $f : \mathcal{Z}^- \cong \mathcal{Z}_0^-$ by $f(n) = n - 1$.

Theorem 1.7.5 Let $(X, \le)$ be a woset, $A = \{X_a \mid a \in x\}$. Then

$$(X, \le) \cong (A, \subseteq).$$

Proof: Define $f : X \cong A$ by $f(a) = X_a$. □

An *ordinal* is defined to be a woset $(X, \le)$ such that $X_a = a$ for all a in X. (I am not making any claims about the existence of such sets at the moment.)

Exercise 1.7.1. *Suppose $(X, \le)$ is an ordinal. What is the first member of X? Well, if x_0 is the first member of X, then $X_{x_0} = \emptyset$, so as $(X, \le)$ is an ordinal, $x_0 = X_{x_0} = \emptyset$. Now what is the second member, x_1, of X? In general, what is the n'th member of X ? What can you guess about both the existence and uniqueness of ordinals?*

Let $(X, \leq)$ be an ordinal. Then, for x, y in X, we have

$$x < y \text{ if and only if } X_x \subset X_y \text{ if and only if } x \subset y.$$

The first equivalence here holds for any woset, the second holds because, if X is an ordinal, $X_x = x$ and $X_y = y$.

Thus the ordering of an ordinal X is the subset relation. In other words, when we specify an ordinal, we do not have to say what the ordering is; it must be the subset relation.

Theorem 1.7.6 Let X be an ordinal. If $a \in X$, then X_a is an ordinal.

Proof: Let $b \in X_a$. Then

$$\begin{aligned}(X_a)_b &= \{x \in X_a \mid x < b\} = \{x \in X \mid x < a \wedge x < b\} \\ &= \{x \in X \mid x < b\} = X_b = b\end{aligned}$$

and the theorem follows. □

Theorem 1.7.7 Let X be an ordinal. Let $Y \subset X$. If Y is an ordinal, then $Y = X_a$ for some $a \in X$.

Proof: Let a be the smallest element of $X - Y$. Thus $X_a \subseteq Y$. Now let $b \in Y$. Then $Y_b = b = X_b$, so if $a < b$, then $a \in X_b$; so $a \in Y_b$, and hence $a \in Y$, which is not the case. Thus $b \leq a$. But $b \neq a$, since $b \in Y$. Hence $b < a$. Thus $b \in X_a$. This proves that $Y \subseteq X_a$. Hence $Y = X_a$. □

Theorem 1.7.8 If X, Y are ordinals, then $X \cap Y$ is an ordinal.

Proof: Let $a \in X \cap Y$. Then $X_a = a = Y_a$, i.e.

$$\{x \in X \mid x < a\} = a = \{y \in Y \mid y < a\}.$$

Hence

$$a = \{z \in X \cap Y \mid z < a\} = (X \cap Y)_a$$

and the proof is complete. □

Theorem 1.7.9 Let X, Y be ordinals. If $X \neq Y$, then one is a segment of the other.

Proof: If $X \subset Y$ or $Y \subset X$, we are done by Theorem 1.7.7. So suppose otherwise. Thus $X \cap Y \subset X$ and $X \cap Y \subset Y$. Now, by Theorem 1.7.8, $X \cap Y$ is an ordinal, so by Theorem 1.7.7, $X \cap Y = X_a$ for some $a \in X$ and $X \cap Y = Y_b$ for some $b \in Y$. Then

$$a = X_a = X \cap Y = Y_b = b.$$

But $a \in X, b \in Y$. Thus $a = b \in X \cap Y$. But $X \cap Y = X_a$, so

$$x \in X \cap Y \rightarrow x < a.$$

In particular, $a < a$, and we have a contradiction. □

Theorem 1.7.10 If X, Y are isomorphic ordinals, then $X = Y$.

Proof: Let $f : X \cong Y$. We prove that $f = \mathrm{id}_X$. Set

$$E = \{x \in X \mid f(x) \neq x\}.$$

We must prove that $E = \emptyset$. Suppose otherwise, and let a be the smallest member of E. Then $x < a \rightarrow f(x) = x$, so $X_a = Y_{f(a)}$. But then $a = X_a = Y_{f(a)} = f(a)$, contrary to $a \in E$. □

Theorem 1.7.11 Let $(X, \leq)$ be a woset such that for each $a \in X$, X_a is isomorphic to an ordinal. Then X is isomorphic to an ordinal.

Proof: For each $a \in X$, let $g_a : X_a \cong Z(a)$ be an isomorphism of X_a onto an ordinal $Z(a)$. By Theorems 1.7.10 and 1.7.3, both $Z(a)$ and g_a are unique. Hence this defines a function Z on X. Let W be its range.[2] That is,

$$W = \{Z(a) \mid a \in X\}.$$

Define $f : X \rightarrow W$ by

$$f(a) = Z(a).$$

Claim: If $x, y \in X$, then $x < y \rightarrow Z(x) \subset Z(y)$.

Proof of claim: Let $x, y \in X$, $x < y$. Then

$$g_x : X_x \cong Z(x). \tag{1}$$

[2]When we come to describe the axioms of set theory, the reader will be able to see that what we are actually doing here is applying the Axiom of Replacement. So this step is, in fact, one of the deeper steps in our present development. If the reader finds this footnote confusing, it just demonstrates what a natural principle the Axiom of Replacement is.

Also, since

$$\begin{aligned} X_x &= \{z \in X \mid z < x\} \\ &= \{z \in X \mid z < y \wedge z < x\} \\ &= \{z \in X_y \mid z < x\} \\ &= (X_y)_x, \end{aligned}$$

we have

(2) $$(g_y \quad X_x) : X_x \cong (Z(y))_{g_y(x)}.$$

Now, $Z(y)$ is an ordinal, so by Theorem 1.7.6, $(Z(y))_{g_y(x)}$ is an ordinal. But by (1) and (2), $Z(x) \cong (Z(y))_{g_y(x)}$. Hence by Theorem 1.7.10,

(3) $$Z(x) = (Z(y))_{g_y(x)}.$$

Thus, in particular, $Z(x) \subset Z(y)$. The claim is proved.

By the claim, f is a bijection of X onto W. Also by the claim, f is an order isomorphism of X onto the poset $(W, \subseteq)$. Thus, in particular, W is well-ordered by $\subseteq$. We finish the proof by showing that W is an ordinal.

Let $y \in X$. Since $Z(y)$ is an ordinal, we have

$$x < y \rightarrow (Z(y))_{g_y(x)} = g_y(x).$$

So by (3),

(4) $$x < y \rightarrow Z(x) = g_y(x).$$

Hence,

$$\begin{aligned} W_{z(y)} &= \{Z(x) \mid Z(x) \subset Z(y)\} \\ &= \{Z(x) \mid x < y\} \\ &= \{g_y(x) \mid x < y\} \\ &= g_y[X_y] \\ &= Z(y). \end{aligned}$$

Thus, as $Z(y)$ was an arbitrary member of W (since y was an arbitrary member of X), W is an ordinal. □

Exercise 1.7.2. *During the course of the above proof, I emphasized one point by a footnote. From the point of view of naive set theory, there is no problem: the proof is a sound mathematical argument. But when we* *come to axiomatize set theory we shall want to state explicitly all procedures which may be used to construct sets. Try to formulate, in a precise manner, the construction principle we used at the crucial part of the proof of Theorem 1.7.11. (The footnote may be of some assistance here.)*

Theorem 1.7.12 Every woset is isomorphic to a unique ordinal.

Proof: The uniqueness assertion follows from Theorem 1.7.10. We prove existence.

Let $(X, \leq)$ be a woset. By Theorem 1.7.11, it suffices to prove that for every $a \in X$, X_a is isomorphic to an ordinal. Let

$$E = \{a \in X \mid X_a \text{ is not isomorphic to an ordinal}\}.$$

We show that $E = \emptyset$. Suppose otherwise. Let a be the smallest element of E. Thus, if $x < a, X_x$ is isomorphic to an ordinal. But for $x < a, X_x = (X_a)_x$. Hence every segment of X_a is isomorphic to an ordinal. Hence by Theorem 1.7.11, X_a is isomorphic to an ordinal, contrary to $a \in E$. $\square$

If $(X, \leq)$ is a woset, I shall denote by $\mathrm{Ord}(X)$ the unique ordinal isomorphic to X. Clearly, if X, Y are wosets, we shall have $X \cong Y$ if and only if $\mathrm{Ord}(X) = \mathrm{Ord}(Y)$. Since the ordinals have a certain uniqueness property (in the sense of Theorem 1.7.10), this means that we may use the ordinals as a yardstick for 'measuring' the 'length' of any woset: $\mathrm{Ord}(X)$ being the 'length' of the woset X.

But just how reasonable is it to take the ordinals, as defined above, as a system of 'numbers', which is what I am now proposing? Well, by Theorem 1.7.9, the ordinals are totally ordered by $\subset$. In fact, Theorem 1.7.9 tells us more: if X, Y are ordinals, then

$$\begin{aligned} X \subset Y \quad & \text{if and only if} \quad X = Y_a \quad (\text{for some } a \in Y) \\ & \text{if and only if} \quad X = a \qquad (\text{since } Y_a = a) \\ & \text{if and only if} \quad X \in Y. \end{aligned}$$

Thus the ordering $\subset$ on ordinals and the ordering $\in$ on ordinals are identical. This implies also that the ordinals are well-ordered by $\subset$, or, equivalently, by $\in$. To see this, we make use of Lemma 1.5.1. Suppose the ordinals were not well-ordered by $\subset$. Then we could find a sequence $\{X(n)\}_{n=0}^{\infty}$ of ordinals such that

$$X(0) \supset X(1) \supset X(2) \supset \dots .$$

Now, for all $n > 0, X(n) \subset X(0)$, so $X(n) \in X(0)$. Thus $\{X(n+1)\}_{n=0}^{\infty}$ is a decreasing (under $\subset$) sequence of members of $X(0)$. But since $X(0)$ is an ordinal, it is well-ordered by $\subset$, so we have a contradiction.

From the above, it would seem, therefore, that the ordinals constitute an eminently reasonable number system, suitable for 'measuring' the 'length' of any woset.

It is common in contemporary set theory to reserve lower-case Greek letters $\alpha, \beta, \gamma, \ldots$ to denote ordinals. (Since the ordering of an ordinal is always $\subset$, there is, of course, no need to specify the ordering each time. But it should be remembered that an ordinal is, strictly speaking, a *well-ordered* set.) It is also customary to denote the order relation between ordinals by

$$\alpha < \beta$$

instead of the two equivalent forms

$$\alpha \subset \beta \ , \ \alpha \in \beta,$$

though the latter is also quite common.

Since the ordinals will 'measure' any woset, they will certainly measure any finite woset. But so too will the positive integers. So do we have some duplication here? Well no, because in mathematics one (almost) never bothers to *define* the integers as specific objects. As a result of our development of ordinals, we obtain, *gratis*, a neat definition of the natural numbers as specific sets; namely, the finite ordinals.

What do the ordinals look like as sets? Well, if α is an ordinal, then by definition we will have

$$\alpha = \{\beta \mid \beta < \alpha\}.$$

That is, an ordinal is the set of all smaller ordinals.

In the case of the first ordinal, there is no smaller ordinal, of course. Hence the first ordinal must be the empty set, $\emptyset$ (regarded as a well-ordered set). Let us denote this ordinal by the symbol 0. Thus, by definition, ignoring the well-ordering as usual,

$$0 = \emptyset.$$

What is the second ordinal? Well, it has to be the set of all smaller ordinals, so if we denote the second ordinal by 1, we must have

$$1 = \{0\}.$$

The third ordinal, which we denote by 2, is

$$2 = \{0, 1\}.$$

The pattern is now clear. We have

$$3 = \{0, 1, 2\},$$
$$4 = \{0, 1, 2, 3\},$$

and in general,

$$n = \{0, 1, 2, \ldots, n-1\}.$$

Notice that the ordinal n is a set with exactly n elements, making the finite ordinals ideal for 'measuring' finite sets. Notice also that if α, β are distinct finite ordinals, then one must be a segment of the other and, hence, an element of the other.

What will be the first infinite ordinal? Clearly, it must be the set (ordered by inclusion)

$$\{0, 1, 2, \ldots, n, n+1, \ldots\}.$$

We denote this ordinal by ω. And the next? Clearly

$$\{0, 1, 2, \ldots, n, n+1, \ldots, \omega\}.$$

In general, if α is an ordinal, the next ordinal will be

$$\alpha \cup \{\alpha\}.$$

It is customary to denote the first ordinal after α by $\alpha + 1$, the (*ordinal*) *successor* of α. Thus

$$\alpha + 1 = \alpha \cup \{\alpha\}.$$

If, as in the case of ω above,

$$0, 1, 2, \ldots, \omega, \omega + 1, \ldots, \alpha, \alpha + 1, \ldots$$

is a listing of some initial segment of the well-ordered collection of ordinals having no greatest member, then the next ordinal will be the set

$$\{0, 1, 2, \ldots, \omega, \omega + 1, \ldots, \alpha, \alpha + 1, \ldots\}.$$

Since such an ordinal will have no greatest member, it cannot be the successor of any ordinal. Such an ordinal is called a *limit ordinal.* For example, ω is a limit ordinal. An ordinal that is the successor of some ordinal is called a *successor ordinal.*

A *sequence* is a function whose domain is an ordinal. If f is a sequence and $\mathrm{dom}(f) = \alpha$, we say f is an α-*sequence*. If $f(\xi) = x_\xi$ for all $\xi < \alpha$, we often write

$$\langle x_\xi \mid \xi < \alpha \rangle$$

in place of f. Then, for $\beta < \alpha$,

$$\langle x_\xi \mid \xi < \beta \rangle$$

denotes $f \quad \beta$. This clearly gives a precise meaning to what we generally think of as a (transfinite, perhaps) sequence. The 'sequences' of elementary analysis are just the special case of ω-sequences, of course; so

$$\{a_n\}_{n=0}^{\infty} = \langle a_n \mid n < \omega \rangle.$$

Exercise 1.7.3. *I have already introduced the notation $\alpha + 1$ for the next ordinal after α. Let us denote by $\alpha + n$ the n-th ordinal after α, where n is any natural number. Show that if α is any ordinal, either α is a limit ordinal or else there is a limit ordinal β and a natural number n such that $\alpha = \beta + n$. (Hint. Use Theorem 1.7.1.)*

The ordinals thus provide us with a continuation of the natural numbers into the transfinite. Further discussion of ordinals will have to be postponed until we have developed the axiomatic foundation of our set theory.

1.8 Problems

1. (Boolean Algebras)

A boolean algebra, $\mathcal{B}$, is a structure consisting of a set B with a unary operation (*complement*) and two binary operations $\wedge$ (*meet*) and $\vee$ (*join*). The axioms to be satisfied by this structure are:

(B1) $b \vee c = c \vee b\ ,\quad b \wedge c = c \wedge b$;

(B2) $b \vee (c \vee d) = (b \vee c) \vee d\ ,\quad b \wedge (c \wedge d) = (b \wedge c) \wedge d$;

(B3) $(b \wedge c) \vee c = c\ ,\quad (b \vee c) \wedge c = c$;

(B4) $b \wedge (c \vee d) = (b \wedge c) \vee (b \wedge d)\ ,\quad b \vee (c \wedge d) = (b \vee c) \wedge (b \vee d)$;

(B5) $(b \wedge -b) \vee b = b\ ,\quad (b \vee -b) \wedge b = b$.

Prove the following:

A. The elements $b \wedge -b$ are all equal and denoted by 0 (zero).

B. The elements $b \vee -b$ are all equal and denoted by 1 (unity).

C. Any nonempty set $\mathcal{F}$ of subsets of a set X that is closed under union, intersection, and complement with respect to X is a boolean algebra under the operations meet = intersection, join = union, complement = complement in X.

Such a set $\mathcal{F}$ is called a *field of subsets* of X. For example, $\mathcal{P}(x)$ is a boolean algebra under the above boolean operations. It can be shown that every boolean algebra is isomorphic to a field of sets. (This is Stone's Theorem. See [6] for details.)

D. Let X be a topological space. Let $\mathcal{C}$ denote the set of all clopen (i.e. closed and open) subsets of X. $\mathcal{C}$ is a field of sets and, hence, is a boolean algebra.

E. Let X be a topological space. Let $\mathcal{R}$ be the set of all closed sets A such that $A =$ closure interior A. Define $A \vee B = A \cup B$, $A \wedge B =$ closure interior $A \cap B$, $-A =$ closure $(X - A)$. Then $\mathcal{R}$ is a boolean algebra. $\mathcal{R}$ is not usually a field of sets, since, in general, $\wedge$ is not the same as $\cap$.

We may define a binary relation on the boolean algebra $\mathcal{B}$ by

$$b \leq c \quad \text{if and only if} \quad b = b \wedge c.$$

Prove the following:

F. For any b, c, $\ b \leq c$ if and only if $b \vee c = c$.

G. $\leq$ is a partial ordering of B; 0 is the unique minimum element under $\leq$, and 1 is the unique maximum.

H. For any b, c, $\ b \wedge c \leq b \leq b \vee c$.

It is possible to define a boolean algebra as a poset satisfying certain conditions. In this case, $b \vee c$ turns out to be the unique least upper bound of b and c, and $b \wedge c$ is the unique greatest lower bound.

2. (Ideals and Filters)

Let B be a boolean algebra. A nonempty subset I of B is called an *ideal* if and only if:

(a) $b, c \in I \to b \vee c \in I$;

(b) $[b \in I \text{ and } c \in B] \to b \wedge c \in I$.

Prove the following:

A. $I \subseteq B$ is an ideal if and only if (a) and (b)$'$ hold, where

(b)$'$ $[b \in I \text{ and } c \in B] \rightarrow c \in I$.

B. $0 \in I$ for every ideal I; if $1 \in I$, then $I = B$.

C. If $b \in B$, then $\{c \in B \mid c \leq b\}$ is an ideal; it is called the *principal ideal* generated by b. Any ideal not of this form is said to be *nonprincipal*.

D. Let X be an infinite set. Let I be the set of all finite subsets of X. I is a nonprincipal ideal in the field of sets $\mathcal{P}(X)$.

A *measure* on a boolean algebra B is a function $\mu: B \rightarrow [0,1]$ such that:

(i) $\mu(0) = 0$, $\mu(1) = 1$;

(ii) if $b \wedge c = 0$, then $\mu(b \vee c) = \mu(b) + \mu(c)$.

E. Prove that, if μ is a measure on B, then $\{b \in B \mid \mu(b) = 0\}$ is an ideal in B.

F. Let B be a boolean algebra. Show that, if $I_t, t \in T$, are ideals in B, so too is

$$\bigcap\nolimits_{t \in T} I_t.$$

Deduce that if $X \subseteq B$, there is a unique smallest ideal containing X; it is called the ideal *generated* by X.

A nonempty set $F \subseteq B$ is called a *filter* if and only if:

(a) $b, c \in F \rightarrow b \wedge c \in F$;

(b) $[b \in F \text{ and } c \in B] \rightarrow b \vee c \in F$.

G. Show that in the above definition, (b) can be replaced by

(b)$'$ $[b \in F \text{ and } b \leq c] \rightarrow c \in F$.

H. Prove that a subset $F \subseteq B$ is a filter if and only if the set $\{-b \mid b \in F\}$ is an ideal. The filter $\{-b \mid b \in I\}$ is called the *dual* of the ideal I; the ideal $\{-b \mid b \in F\}$ is the *dual* of the filter F.

An ideal in the field of sets $\mathcal{P}(X)$ is sometimes said to be an ideal *on* the set X; similarly a filter *on* the set X.

3. (The Order Topology)

Let $(X, <)$ be a toset. The *order topology* on X is the topology determined by taking as open subbase all sets of the form $\{x \in X \mid x < a\}$ or $\{x \in X \mid x > a\}$ for $a \in X$.

A. Prove that the order topology on X is the smallest topology with the property that whenever $a, b \in X$ and $a < b$, there are neighborhoods U of a and V of b such that $U < V$ (i.e. such that $x < y$ whenever $x \in U$ and $y \in V$).

B. Prove that, if X is connected (under the order topology), then X is complete as a toset; i.e. every nonempty subset with an upper bound has a least upper bound.

If there are points a, b in X such that $a < b$ and for no c in X is $a < c < b$, we say X has a *gap*.

C. Prove that X is connected (with the order topology) if and only if X is complete (as a toset) and has no gaps.

D. Prove that X is complete (as a toset) if and only if every closed (in the order topology), bounded subset of X is compact.