Chapter ZERO

Useful Facts about Sets

We assume that the reader already has some familiarity with normal everyday set-theoretic apparatus. Nonetheless, we give here a brief summary of facts from set theory we will need; this will at least serve to establish the notation. It is suggested that the reader, instead of poring over this chapter at the outset, simply refer to it if and when issues of a set-theoretic nature arise in later chapters. The author's favorite book on set theory is of course his *Elements of Set Theory* (see the list of references at the end of this book).

First a word about jargon. Throughout the book we will utilize an assortment of standard mathematical abbreviations. We use "⊣" to signify the end of a proof. A sentence "If . . . , then . . ." will sometimes be abbreviated ". . . ⇒ . . . ." We also have "⇐" for the converse implication (for the peculiar way the word "implication" is used in mathematics). For "if and only if" we use the shorter "iff" (this has become part of the mathematical language) and the symbol "⇔." For the word "therefore" we have the "∴" abbreviation.

The notational device that extracts "$x \neq y$" as the denial of "$x = y$" and "$x \notin y$" as the denial of "$x \in y$" will be extended to other cases. For example, in Section 1.2 we define "$\Sigma \models \tau$"; then "$\Sigma \not\models \tau$" is its denial.

Now then, a *set* is a collection of things, called its members or elements. As usual, we write "$t \in A$" to say that t is a member of A, and "$t \notin A$" to say that t is not a member of A. We write "$x = y$" to

mean that x and y are the same object. That is, the expression "x" on the left of the equals sign is a name for the same object as is named by the other expression "y." If $A = B$, then for any object t it is automatically true that $t \in A$ iff $t \in B$. This holds simply because A and B are the same thing. The converse is the principle of extensionality: If A and B are sets such that for every object t,

$$t \in A \quad \text{iff} \quad t \in B,$$

then $A = B$. This reflects the idea of what a set *is*; a set is determined just by its members.

A useful operation is that of adjoining one extra object to a set. For a set A, let $A; t$ be the set whose members are (i) the members of A, plus (ii) the (possibly new) member t. Here t may or may not already belong to A, and we have

$$A; t = A \cup \{t\}$$

using notation defined later, and

$$t \in A \quad \text{iff} \quad A; t = A.$$

One special set is the empty set $\varnothing$, which has no members at all. Any other set is said to be *nonempty*. For any object x there is the singleton set $\{x\}$ whose only member is x. More generally, for any finite number $x_1, \ldots, x_n$ of objects there is the set $\{x_1, \ldots, x_n\}$ whose members are exactly those objects. Observe that $\{x, y\} = \{y, x\}$, as both sets have exactly the same members. We have only used different expressions to denote the set. If order matters, we can use ordered pairs (discussed later).

This notation will be stretched to cover some simple infinite cases. For example, $\{0, 1, 2, \ldots\}$ is the set $\mathbb{N}$ of natural numbers, and $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is the set $\mathbb{Z}$ of all integers.

We write "$\{x \mid \_x\_\}$" for the set of all objects x such that $\_x\_$. We will take considerable liberty with this notation. For example, $\{\langle m, n\rangle \mid m < n \text{ in } \mathbb{N}\}$ is the set of all ordered pairs of natural numbers for which the first component is smaller than the second. And $\{x \in A \mid \_x\_\}$ is the set of all elements x in A such that $\_x\_$.

If A is a set all of whose members are also members of B, then A is a subset of B, abbreviated "$A \subseteq B$." Note that any set is a subset of itself. Also, $\varnothing$ is a subset of every set. ("$\varnothing \subseteq A$" is "vacuously true," since the task of verifying, for every member of $\varnothing$, that it also belongs to A requires doing nothing at all. Or from another point of view, "$A \subseteq B$" can be false only if some member of A fails to belong to B. If $A = \varnothing$, this is impossible.) From the set A we can form a new set, the *power set* $\mathcal{P}A$ of A, whose members are the subsets of A. Thus

$$\mathcal{P}A = \{x \mid x \subseteq A\}.$$

For example,

$$\mathcal{P}\varnothing = \{\varnothing\},$$
$$\mathcal{P}\{\varnothing\} = \{\varnothing, \{\varnothing\}\}.$$

The *union* of A and B, $A \cup B$, is the set of all things that are members of A or B (or both). For example, $A; t = A \cup \{t\}$. Similarly, the *intersection* of A and B, $A \cap B$, is the set of all things that are members of both A and B. Sets A and B are *disjoint* iff their intersection is empty (i.e., if they have no members in common). A collection of sets is *pairwise disjoint* iff any two members of the collection are disjoint.

More generally, consider a set A whose members are themselves sets. The union, $\bigcup A$, of A is the set obtained by dumping all the members of A into a single set:

$$\bigcup A = \{x \mid x \quad \text{belongs to some member of } A\}.$$

Similarly for nonempty A,

$$\bigcap A = \{x \mid x \quad \text{belongs to all members of } A\}.$$

For example, if

$$A = \{\{0, 1, 5\}, \{1, 6\}, \{1, 5\}\},$$

then

$$\bigcup A = \{0, 1, 5, 6\},$$

$$\bigcap A = \{1\}.$$

Two other examples are

$$A \cup B = \bigcup\{A, B\},$$

$$\bigcup \mathcal{P}A = A.$$

In cases where we have a set A_n for each natural number n, the union of all these sets, $\bigcup\{A_n \mid n \in \mathbb{N}\}$, is usually denoted "$\bigcup_{n\in\mathbb{N}} A_n$" or just "$\bigcup_n A_n$."

The ordered pair $\langle x, y\rangle$ of objects x and y must be defined in such a way that

$$\langle x, y\rangle = \langle u, v\rangle \qquad \text{iff} \qquad x = u \quad \text{and} \quad y = v.$$

Any definition that has this property will do; the standard one is

$$\langle x, y\rangle = \{\{x\}, \{x, y\}\}.$$

For ordered triples we define

$$\langle x, y, z\rangle = \langle\langle x, y\rangle, z\rangle.$$

More generally we define n-tuples recursively by

$$\langle x_1, \ldots, x_{n+1} \rangle = \langle \langle x_1, \ldots, x_n \rangle, x_{n+1} \rangle$$

for $n > 1$. It is convenient to define also $\langle x \rangle = x$; the preceding equation then holds also for $n = 1$. S is a *finite sequence* (or *string*) of members of A iff for some positive integer n, we have $S = \langle x_1, \ldots, x_n \rangle$, where each $x_i \in A$. (Finite sequences are often defined to be certain finite functions, but the above definition is slightly more convenient for us.)

A *segment* of the finite sequence $S = \langle x_1, \ldots, x_n \rangle$ is a finite sequence

$$\langle x_k, x_{k+1}, \ldots, x_{m-1}, x_m \rangle, \qquad \text{where} \quad 1 \leq k \leq m \leq n.$$

This segment is an *initial segment* iff $k = 1$ and it is *proper* iff it is different from S.

If $\langle x_1, \ldots, x_n \rangle = \langle y_1, \ldots, y_n \rangle$, then it is easy to see that $x_i = y_i$ for $1 \leq i \leq n$. (The proof uses induction on n and the basic property of ordered pairs.) But if $\langle x_1, \ldots, x_m \rangle = \langle y_1, \ldots, y_n \rangle$, then it does not in general follow that $m = n$. After all, every ordered triple is also an ordered pair. But we claim that m and n can be unequal only if some x_i is itself a finite sequence of y_j's, or the other way around:

Lemma 0A Assume that $\langle x_1, \ldots, x_m \rangle = \langle y_1, \ldots, y_m, \ldots, y_{m+k} \rangle$. Then $x_1 = \langle y_1, \ldots, y_{k+1} \rangle$.

Proof. We use induction on m. If $m = 1$, the conclusion is immediate. For the inductive step, assume that $\langle x_1, \ldots, x_m, x_{m+1} \rangle = \langle y_1, \ldots, y_{m+k}, y_{m+1+k} \rangle$. Then the first components of this ordered pair must be equal: $\langle x_1, \ldots, x_m \rangle = \langle y_1, \ldots, y_{m+k} \rangle$. Now apply the inductive hypothesis. ⊣

For example, suppose that A is a set such that no member of A is a finite sequence of other members. Then if $\langle x_1, \ldots, x_m \rangle = \langle y_1, \ldots, y_n \rangle$ and each x_i and y_j is in A, then by the above lemma $m = n$. Whereupon we have $x_i = y_i$ as well.

From sets A and B we can form their *Cartesian product*, the set $A \times B$ of all pairs $\langle x, y \rangle$ for which $x \in A$ and $y \in B$. A^n is the set of all n-tuples of members of A. For example, $A^3 = (A \times A) \times A$.

A *relation* R is a set of ordered pairs. For example, the ordering relation on the numbers 0–3 is captured by — and in fact *is* — the set of ordered pairs

$$\{\langle 0, 1 \rangle, \langle 0, 2 \rangle, \langle 0, 3 \rangle, \langle 1, 2 \rangle, \langle 1, 3 \rangle, \langle 2, 3 \rangle\}.$$

The *domain* of R (written dom R) is the set of all objects x such that $\langle x, y \rangle \in R$ for some y. The *range* of R (written ran R) is the set of all objects y such that $\langle x, y \rangle \in R$ for some x. The union of dom R and ran R is the *field* of R, fld R.

An *n-ary relation* on A is a subset of A^n. If $n > 1$, it is a relation. But a 1-ary (unary) relation on A is simply a subset of A. A particularly simple binary relation on A is the equality relation $\{\langle x, x\rangle \mid x \in A\}$ on A. For an n-ary relation R on A and subset B of A, the *restriction* of R to B is the intersection $R \cap B^n$. For example, the relation displayed above is the restriction to the set $B = \{0, 1, 2, 3\}$ of the ordering relation on $\mathbb{N}$.

A *function* is a relation F with the property of being *single-valued*: For each x in dom F there is only one y such that $\langle x, y\rangle \in F$. As usual, this unique y is said to be the value $F(x)$ that F assumes at x. (This notation goes back to Euler. It is a pity he did not choose $(x)F$ instead; that would have been helpful for the *composition* of functions: $f \circ g$ is the function whose value at x is $f(g(x))$, obtained by applying first g and then f.)

We say that F *maps* A into B and write

$$F : A \to B$$

to mean that F is a function, dom $F = A$, and ran $F \subseteq B$. If in addition ran $F = B$, then F maps A *onto* B. F is *one-to-one* iff for each y in ran F there is only one x such that $\langle x, y\rangle \in F$. If the pair $\langle x, y\rangle$ is in dom F, then we let $F(x, y) = F(\langle x, y\rangle)$. This notation is extended to n-tuples; $F(x_1, \ldots, x_n) = F(\langle x_1, \ldots, x_n\rangle)$.

An *n-ary operation* on A is a function mapping A^n into A. For example, addition is a binary operation on $\mathbb{N}$, whereas the successor operation S (where $S(n) = n + 1$) is a unary operation on $\mathbb{N}$. If f is an n-ary operation on A, then the *restriction* of f to a subset B of A is the function g with domain B^n which agrees with f at each point of B^n. Thus,

$$g = f \cap (B^n \times A).$$

This g will be an n-ary operation on B iff B is *closed* under f, in the sense that $f(b_1, \ldots, b_n) \in B$ whenever each b_i is in B. In this case, $g = f \cap B^{n+1}$, in agreement with our definition of the restriction of a relation. For example, the addition operation on $\mathbb{N}$, which contains such triples as $\langle\langle 3, 2\rangle, 5\rangle$, is the restriction to $\mathbb{N}$ of the addition operation on $\mathbb{R}$, which contains many more triples.

A particularly simple unary operation on A is the *identity* function Id on A, given by the equation

$$Id(x) = x \qquad \text{for} \quad x \in A.$$

Thus $Id = \{\langle x, x\rangle \mid x \in A\}$.

For a relation R, we define the following:

R is *reflexive* on A iff $\langle x, x\rangle \in R$ for every x in A.

R is *symmetric* iff whenever $\langle x, y\rangle \in R$, then also $\langle y, x\rangle \in R$.

R is *transitive* iff whenever both $\langle x, y\rangle \in R$ and $\langle y, z\rangle \in R$ (if this ever happens), then also $\langle x, z\rangle \in R$.

R satisfies *trichotomy* on A iff for every x and y in A, exactly one of the three possibilities, $\langle x, y\rangle \in R$, $x = y$, or $\langle y, x\rangle \in R$, holds.

R is an *equivalence relation* on A iff R is a binary relation on A that is reflexive on A, symmetric, and transitive.

R is an *ordering relation* on A iff R is transitive and satisfies trichotomy on A.

For an equivalence relation R on A we define, for $x \in A$, the *equivalence class* $[x]$ of x to be $\{y \mid \langle x, y\rangle \in R\}$. The equivalence classes then *partition* A. That is, the equivalence classes are subsets of A such that each member of A belongs to exactly one equivalence class. For x and y in A,

$$[x] = [y] \quad \text{iff} \quad \langle x, y\rangle \in R.$$

The set $\mathbb{N}$ of natural numbers is the set $\{0, 1, 2, \ldots\}$. (Natural numbers can also be defined set-theoretically, a point that arises briefly in Section 3.7.) A set A is *finite* iff there is some one-to-one function f mapping (for some natural number n) the set A onto $\{0, 1, \ldots, n-1\}$. (We can think of f as "counting" the members of A.)

A set A is *countable* iff there is some function mapping A one-to-one into $\mathbb{N}$. For example, any finite set is obviously countable. Now consider an infinite countable set A. Then from the given function f mapping A one-to-one into $\mathbb{N}$, we can extract a function f' mapping A one-to-one *onto* $\mathbb{N}$. For some $a_0 \in A$, $f(a_0)$ is the least member of ran f, let $f'(a_0) = 0$. In general there is a unique $a_n \in A$ such that $f(a_n)$ is the $(n+1)$st member of ran f; let $f'(a_n) = n$. Note that $A = \{a_0, a_1, \ldots\}$. (We can also think of f' as "counting" the members of A, only now the counting process is infinite.)

THEOREM 0B Let A be a countable set. Then the set of all finite sequences of members of A is also countable.

PROOF. The set S of all such finite sequences can be characterized by the equation

$$S = \bigcup_{n \in \mathbb{N}} A^{n+1}.$$

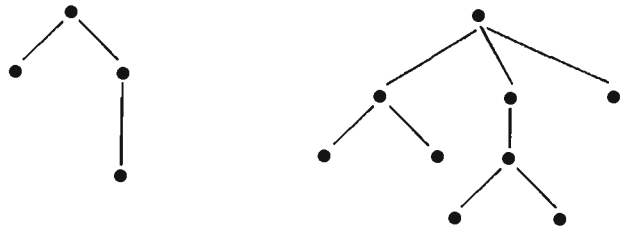
Since A is countable, we have a function f mapping A one-to-one into $\mathbb{N}$.

The basic idea is to map S one-to-one into $\mathbb{N}$ by assigning to $\langle a_0, a_1, \ldots, a_m\rangle$ the number $2^{f(a_0)+1}3^{f(a_1)+1} \cdot \ldots \cdot p_m^{f(a_m)+1}$, where p_m is the $(m+1)$st prime. This suffers from the defect that this assignment might not be well-defined. For conceivably there could be $\langle a_0, a_1, \ldots, a_m\rangle = \langle b_0, b_1, \ldots, b_n\rangle$, with a_i and b_j in A but with $m \neq n$. But this is not serious; just assign to each member of S the *smallest* number obtainable in the above

fashion. This gives us a well-defined map; it is easy to see that it is one-to-one. ⊣

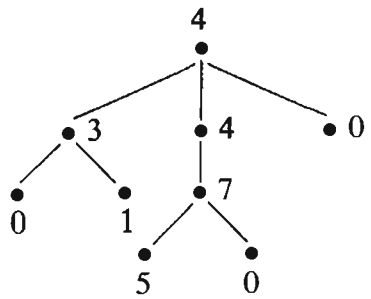
At times we will speak of *trees*, which can be useful in providing intuitive pictures of some situations. But our comments on trees will always be informal; the theorems and proofs will not rely on trees. Accordingly, our discussion here of trees will be informal.

For each tree there is an underlying finite partial ordering. We can draw a picture of this partial ordering R; if $\langle a, b\rangle \in R$, then we put a lower than b and connect the points by a line. Pictures of two typical tree orderings are shown.



(In mathematics, trees grow downward, not upward.) There is always a highest point in the picture (the *root*). Furthermore, while branching is permitted below some vertex, the points *above* any given vertex must lie along a line.

In addition to this underlying finite partial ordering, a tree also has a labeling function whose domain is the set of vertices. For example, one tree, in which the labels are natural numbers, is shown.



At a few points in the book we will use the axiom of choice. But usually these uses can be eliminated if the theorems in question are restricted to countable languages. Of the many equivalent statements of the axiom of choice, Zorn's lemma is especially useful.

Say that a collection C of sets is a *chain* iff for any elements x and y of C, either $x \subseteq y$ or $y \subseteq x$.

Zorn's Lemma Let A be a set such that for any chain $C \subseteq A$, the set $\bigcup C$ is in A. Then there is some element $m \in A$ which is maximal in the sense that it is not a subset of any other element of A.

Cardinal Numbers

All infinite sets are big, but some are bigger than others. (For example, the set of real numbers is bigger than the set of integers.) Cardinal numbers provide a convenient, although not indispensable, way of talking about the size of sets.

It is natural to say that two sets A and B have the same size iff there is a function that maps A one-to-one onto B. If A and B are finite, then this concept is equivalent to the usual one: If you count the members of A and the members of B, then you get the same number both times. But it is applicable even to infinite sets A and B, where counting is difficult.

Formally, then, say that A and B are *equinumerous* (written $A \sim B$) iff there is a one-to-one function mapping A onto B. For example, the set $\mathbb{N}$ of natural numbers and the set $\mathbb{Z}$ of integers are equinumerous. It is easy to see that equinumerosity is reflexive, symmetric, and transitive.

For finite sets we can use natural numbers as measures of size. The same natural number would be assigned to two finite sets (as measures of their size) iff the sets were equinumerous. Cardinal numbers are introduced to enable us to generalize this situation to infinite sets.

To each set A we can assign a certain object, the *cardinal number* (or *cardinality*) of A (written card A), in such a way that two sets are assigned the same cardinality iff they are equinumerous:

$$\text{card } A = \text{card } B \quad \text{iff} \quad A \sim B. \tag{K}$$

There are several ways of accomplishing this; the standard one these days takes card A to be the least ordinal equinumerous with A. (The success of this definition relies on the axiom of choice.) We will not discuss ordinals here, since for our purposes it matters very little what card A actually is, any more than it matters what the number 2 actually is. What matters most is that (K) holds. It is helpful, however, if for a finite set A, card A is the natural number telling how many elements A has. Something is a *cardinal number*, or simply a *cardinal*, iff it is card A for some set A.

(Georg Cantor, who first introduced the concept of cardinal number, characterized in 1895 the cardinal number of a set M as "the general concept which, with the help of our active intelligence, comes from the set M upon abstraction from the nature of its various elements and from the order of their being given.")

Say that A is *dominated* by B (written $A \preceq B$) iff A is equinumerous with a subset of B. In other words, $A \preceq B$ iff there is a one-to-one function mapping A into B. The companion concept for cardinals is

$$\text{card } A \leq \text{card } B \quad \text{iff} \quad A \preceq B.$$

(It is easy to see that $\leq$ is well defined; that is, whether or not $\kappa \leq \lambda$ depends only on the cardinals κ and λ themselves, and not the choice of

sets having these cardinalities.) Dominance is reflexive and transitive. A set A is dominated by $\mathbb{N}$ iff A is countable. The following is a standard result in this subject.

Schröder–Bernstein Theorem (a) For any sets A and B, if $A \preceq B$ and $B \preceq A$, then $A \sim B$.
(b) For any cardinal numbers κ and λ, if $\kappa \leq \lambda$ and $\lambda \leq \kappa$, then $\kappa = \lambda$.

Part (b) is a simple restatement of part (a) in terms of cardinal numbers. The following theorem, which happens to be equivalent to the axiom of choice, is stated in the same dual manner.

Theorem 0C (a) For any sets A and B, either $A \preceq B$ or $B \preceq A$.
(b) For any cardinal numbers κ and λ, either $\kappa \leq \lambda$ or $\lambda \leq \kappa$.

Thus of any two cardinals, one is smaller than the other. (In fact, any nonempty set of cardinal numbers contains a smallest member.) The smallest cardinals are those of finite sets: $0, 1, 2, \ldots$. There is next the smallest infinite cardinal, card $\mathbb{N}$, which is given the name $\aleph_0$. Thus we have

$$0, 1, 2, \ldots, \aleph_0, \aleph_1, \ldots,$$

where $\aleph_1$ is the smallest cardinal larger than $\aleph_0$. The cardinality of the real numbers, card $\mathbb{R}$, is called "$2^{\aleph_0}$." Since $\mathbb{R}$ is uncountable, we have $\aleph_0 < 2^{\aleph_0}$.

The operations of addition and multiplication, long familiar for finite cardinals, can be extended to all cardinals. To compute $\kappa + \lambda$ we choose disjoint sets A and B of cardinality κ and λ, respectively. Then

$$\kappa + \lambda = \text{card}(A \cup B).$$

This is well defined; i.e., $\kappa + \lambda$ depends only on κ and λ, and not on the choice of the disjoint sets A and B. For multiplication we use

$$\kappa \cdot \lambda = \text{card}(A \times B).$$

Clearly these definitions are correct for finite cardinals. The arithmetic of infinite cardinals is surprisingly simple (with the axiom of choice). The sum or product of two infinite cardinals is simply the larger of them:

Cardinal Arithmetic Theorem For cardinal numbers κ and λ, if $\kappa \leq \lambda$ and λ is infinite, then $\kappa + \lambda = \lambda$. Furthermore, if $\kappa \neq 0$, then $\kappa \cdot \lambda = \lambda$.

In particular, for infinite cardinals κ,

$$\aleph_0 \cdot \kappa = \kappa.$$

THEOREM 0D For an infinite set A, the set $\bigcup_n A^{n+1}$ of all finite sequences of elements of A has cardinality equal to card A.

We already proved this for the case of a countable A (see Theorem 0B).

PROOF. Each A^{n+1} has cardinality equal to card A, by the cardinal arithmetic theorem (applied n times). So we have the union of $\aleph_0$ sets of this size, yielding $\aleph_0 \cdot \text{card } A = \text{card } A$ points altogether. ⊣

EXAMPLE. It follows that the set of algebraic numbers has cardinality $\aleph_0$. First, we can identify each polynomial (in one variable) over the integers with the sequence of its coefficients. Then by the theorem there are $\aleph_0$ polynomials. Each polynomial has a finite number of roots. To give an extravagant upper bound, note that even if each polynomial had $\aleph_0$ roots, we would then have $\aleph_0 \cdot \aleph_0 = \aleph_0$ algebraic numbers altogether. Since there are at least this many, we are done.

Since there are uncountably many (in fact, $2^{\aleph_0}$) real numbers, it follows that there are uncountably many (in fact, $2^{\aleph_0}$) transcendental numbers.