Chapter 1

SECTION ONE

1.

Check the distributive laws for $\cup$ and $\cap$ and DeMorgan's laws.

To show that two sets M and N are equal, we need to show that for any x, $x \in M$ iff $x \in N$.

1. Distributive laws:
   a. $x \in A \cap (B \cup C)$ iff $x \in A$ and $x \in B \cup C$ iff $x \in A$ and ($x \in B$ or $x \in C$) iff ($x \in A$ and $x \in B$) or ($x \in A$ and $x \in C$) iff $x \in A \cap B$ or $x \in A \cap C$ iff $x \in (A \cap B) \cup (A \cap C)$.
   b. Similarly, for the second distributive law, $x \in A \cup (B \cap C)$ iff $x \in A$ or $x \in B \cap C$ iff $x \in A$ or ($x \in B$ and $x \in C$) iff ($x \in A$ or $x \in B$) and ($x \in A$ or $x \in C$) iff $x \in A \cup B$ and $x \in A \cup C$ iff $x \in (A \cup B) \cap (A \cup C)$.
2. DeMorgan's laws:
   a. $x \in A - (B \cup C)$ iff $x \in A$ and $x \notin B \cup C$ iff $x \in A$ and $x \notin B$ and $x \notin C$ iff $x \in A - B$ and $x \in A - C$ iff $x \in (A - B) \cap (A - C)$.
   b. Similarly, for the second DeMorgan's law, $x \in A - (B \cap C)$ iff $x \in A$ and $x \notin B \cap C$ iff $x \in A$ and ($x \notin B$ or $x \notin C$) iff $x \in A - B$ or $x \in A - C$ iff $x \in (A - B) \cup (A - C)$.

2.

Determine which of the following statements are true for all sets A, B, C, and D. If a double implication fails, determine whether one or the other of the possible implications holds. If an equality fails, determine whether the statement becomes true if the "equals" symbol is replaced by one or the other of the inclusion symbols $\subset$ or $\supset$.

(a) $A \subset B$ and $A \subset C \Leftrightarrow A \subset (B \cup C)$.

(b) $A \subset B$ or $A \subset C \Leftrightarrow A \subset (B \cup C)$.

(c) $A \subset B$ and $A \subset C \Leftrightarrow A \subset (B \cap C)$.

(d) $A \subset B$ or $A \subset C \Leftrightarrow A \subset (B \cap C)$.

(e) $A - (A - B) = B$.

(f) $A - (B - A) = A - B$.

(g) $A \cap (B - C) = (A \cap B) - (A \cap C)$,

(h) $A \cup (B - C) = (A \cup B) - (A \cup C)$,

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

(j) $A \subset C$ and $B \subset D \Rightarrow (A \times B) \subset (C \times D)$.

(k) The converse of (j).

(l) The converse of (j), assuming that A and B are nonempty.

(m) $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$.

(n) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

(o) $A \times (B - C) = (A \times B) - (A \times C)$.

(p) $(A - B) \times (C - D) = (A \times C - B \times C) - A \times D$.

(q) $(A \times B) - (C \times D) = (A - C) \times (B - D)$.

The following table summarizes the correct symbol (implication, equality or inclusion) for each statement:

$\Rightarrow$	$\Leftrightarrow$	$\Leftarrow$	$\subset$	$\supset$	=	neither
a b j	c	d l	e m	f h q	g i n o p	k

Most of these can be easily shown using diagrams similar to those on pages 10-11. However, points including cartesian product might be trickier for the case when one of the sets is empty.

(j) The right implication holds regardless of whether any set is empty (in fact, if $A \times B$ is non-empty, then all four sets A, B, C and D are non-empty).

(k), (l) Here is where the empty set can mess things up. We are asked about whether the left implication holds in (j). Assume $(A \times B) \subset (C \times D)$, and suppose we try to show that $A \subset C$. If $a \in A$ then, if we knew that there is some $b \in B$, we could argue that $(a, b) \in A \times B$, hence, $(a, b) \in C \times D$, and $a \in C$. But the problem is that B can be empty, in which case, $A \times B = \emptyset \subset C \times D$ for any C and D, regardless of whether $A \subset C$ or not.

Overall from (j)-(l) we get the following statement: for any *non-empty* sets A, B, C and D, $A \subset C$ and $B \subset D$ iff $(A \times B) \subset (C \times D)$.

3.

(a) Write the contrapositive and converse of the following statement: "If $x < 0$, then $x^2 - x > 0$," and determine which (if any) of the three statements are true,

(b) Do the same for the statement "If $x > 0$, then $x^2 - x > 0$."

Statement	Contrapositive	Converse
$x < 0 \Rightarrow x^2 - x > 0$ (true)	$x^2 - x \leq 0 \Rightarrow x \geq 0$ (true)	$x^2 - x > 0 \Rightarrow x < 0$ (false)
$x > 0 \Rightarrow x^2 - x > 0$ (false)	$x^2 - x \leq 0 \Rightarrow x \leq 0$ (false)	$x^2 - x > 0 \Rightarrow x > 0$ (false)

4.

Let A and B be sets of real numbers. Write the negation of each of the following statements:

(a) For every $a \in A$, it is true that $a^2 \in B$.

(b) For at least one $a \in A$, it is true that $a^2 \in B$.

(c) For every $a \in A$, it is true that $a^2 \notin B$.

(d) For at least one $a \notin A$, it is true that $a^2 \in B$.

Negation for (a): $\exists a \in A$ s.t. $a^2 \notin B$. (b) and (c) are negations of each other. (d): $\forall a \notin A : a^2 \notin B$.

5.

Let $\mathcal{A}$ be a nonempty collection of sets. Determine the truth of each of the following statements and of their converses:

(a) $x \in \cup_{A \in \mathcal{A}} A \Rightarrow x \in A$ for at least one $A \in \mathcal{A}$.

(b) $x \in \cup_{A \in \mathcal{A}} A \Rightarrow x \in A$ for every $A \in \mathcal{A}$.

(c) $x \in \cap_{A \in \mathcal{A}} A \Rightarrow x \in A$ for at least one $A \in \mathcal{A}$.

(d) $x \in \cap_{A \in \mathcal{A}} A \Rightarrow x \in A$ for every $A \in \mathcal{A}$.

(a) and (d): $\Leftrightarrow$ (by definition). (b): $\Leftarrow$. (c): $\Rightarrow$.

6.

Write the contrapositive of each of the statements of Exercise 5.

The three true contrapositive statements are

(a) $\forall A \in \mathcal{A} : x \notin A \Rightarrow x \notin \cup_{A \in \mathcal{A}} A$,

(c) $\forall A \in \mathcal{A} : x \notin A \Rightarrow x \notin \cap_{A \in \mathcal{A}} A$, and

(d) $\exists A \in \mathcal{A} : x \notin A \Rightarrow x \notin \cap_{A \in \mathcal{A}} A$.

The other one is false,

(b) $\exists A \in \mathcal{A} : x \notin A \Rightarrow x \notin \cup_{A \in \mathcal{A}} A$.

7.

If a set A has two elements, show that $\mathcal{P}(A)$ has four elements. How many elements does $\mathcal{P}(A)$ have if A has one element? Three elements? No elements? Why is $\mathcal{P}(A)$ called the power set of A ?

It is called the "power set" of A because for any set A with n elements $\mathcal{P}(A)$ has 2^n elements. By induction. If A has 1 element, then there are two subsets of A : the empty set and the set itself. Suppose that for any set with $n-1$ elements its power set has 2^{n-1} elements. Take a set A with n elements, and let x be an element in A . Each of its subset either contains x or it does not. We can construct all subsets of A by taking each subset of $A-\{x\}$ (which has $n-1$ elements) and by optionally adding x to it. Therefore, the number of subsets of A is twice the number of subsets of $A-\{x\}$, which, by the inductive hypothesis, is 2^{n-1} . So, we get 2^n subsets of A . (Since we based the induction on the case $n=1$, there is one more case to consider, namely, $n=0$, but obviously $\mathcal{P}(\emptyset)=1$ as there is only one subset of the empty set — the empty set itself.)

8.

Formulate and prove DeMorgan' s laws for arbitrary unions and intersections.

The first law: $A-\cup_{B\in\mathcal{B}}B=\cap_{B\in\mathcal{B}}(A-B)$. The second law: $A-\cap_{B\in\mathcal{B}}B=\cup_{B\in\mathcal{B}}(A-B)$. The proof is similar to the first problem.

9.

Let $\mathbb{R}$ denote the set of real numbers. For each of the following subsets of $\mathbb{R}\times\mathbb{R}$, determine whether it is equal to the cartesian product of two subsets of $\mathbb{R}$.

(a) $\{(x,y)|x \text{ is an integer}\}$.

(b) $\{(x,y)|0<y\leq 1\}$.

(c) $\{(x,y)|y>x\}$.

(d) $\{(x,y)|x \text{ is not an integer and } y \text{ is an integer}\}$.

(e) $\{(x,y)|x^2+y^2<1\}$.

A set C in $\mathbb{R}\times\mathbb{R}$ is the cartesian product of two sets in $\mathbb{R}$ iff $\forall x\in\mathbb{R}$ the set $Y(x)$ of y ' s such that $(x,y)\in C$ is either the empty set or does not depend on x . So, we get the positive answer in (a), (b) and (d).

SECTION TWO

1.

Let $f : A \to B$. Let $A_0 \subset A$ and $B_0 \subset B$.

(a) Show that $A_0 \subset f^{-1}(f(A_0))$ and that equality holds if f is injective.

(b) Show that $f(f^{-1}(B_0)) \subset B_0$ and that equality holds if f is surjective.

To show that for some sets X and Y, $X \subset Y$, we need to show that $\forall x \in X$, $x \in Y$, or, equivalently, show that $\forall x \notin Y$, $x \notin X$.

(a) $a \in A_0 \Rightarrow f(a) \in f(A_0) \Rightarrow a \in f^{-1}(f(A_0))$. If f is injective, then $a \notin A_0 \Rightarrow f(a) \notin f(A_0)$ (otherwise, there exists $b \in A_0$ such that $b \neq a$ and $f(a) = f(b)$) $\Rightarrow a \notin f^{-1}(f(A_0))$.

(b) $y \notin B_0 \Rightarrow f^{-1}(y) \cap f^{-1}(B_0) = \emptyset \Rightarrow y \notin f(f^{-1}(B_0))$. If f is surjective, then $f^{-1}(y) \neq \emptyset$, and $y \in B_0 \Rightarrow \exists x \in f^{-1}(y) \subset f^{-1}(B_0) \Rightarrow y \in f(f^{-1}(B_0))$.

2.

Let $f : A \to B$ and let $A_i \subset A$ and $B_i \subset B$ for $i = 0$ and $i = 1$. Show that f^{-1} preserves inclusions, unions, intersections, and differences of sets:

(a) $B_0 \subset B_1 \Rightarrow f^{-1}(B_0) \subset f^{-1}(B_1)$.

(b) $f^{-1}(B_0 \cup B_1) = f^{-1}(B_0) \cup f^{-1}(B_1)$.

(c) $f^{-1}(B_0 \cap B_1) = f^{-1}(B_0) \cap f^{-1}(B_1)$.

(d) $f^{-1}(B_0 - B_1) = f^{-1}(B_0) - f^{-1}(B_1)$.

Show that f preserves inclusions and unions only:

(e) $A_0 \subset A_1 \Rightarrow f(A_0) \subset f(A_1)$.

(f) $f(A_0 \cup A_1) = f(A_0) \cup f(A_1)$.

(g) $f(A_0 \cap A_1) \subset f(A_0) \cap f(A_1)$; show that equality holds if f is injective.

(h) $f(A_0 - A_1) \supset f(A_0) - f(A_1)$; show that equality holds if f is injective.

(a) $x \in f^{-1}(B_0) \Rightarrow f(x) \in B_0 \Rightarrow f(x) \in B_1 \Rightarrow x \in f^{-1}(B_1)$.

(b) Using (a), $f^{-1}(B_i) \subset f^{-1}(B_0 \cup B_1)$, and, therefore, $f^{-1}(B_0) \cup f^{-1}(B_1) \subset f^{-1}(B_0 \cup B_1)$. The other direction: $x \in f^{-1}(B_0 \cup B_1) \Rightarrow f(x) \in B_0$ or $f(x) \in B_1 \Rightarrow x \in f^{-1}(B_0) \cup f^{-1}(B_1)$.

(c) Using (a), $f^{-1}(B_0 \cap B_1) \subset f^{-1}(B_i)$, and, therefore, $f^{-1}(B_0 \cap B_1) \subset f^{-1}(B_0) \cap f^{-1}(B_1)$. The other direction: $x \in f^{-1}(B_0) \cap f^{-1}(B_1) \Rightarrow f(x) \in B_0$ and $f(x) \in B_1 \Rightarrow x \in f^{-1}(B_0 \cap B_1)$.

(d) $x \in f^{-1}(B_0 - B_1)$ iff $f(x) \in B_0 - B_1$ iff $f(x) \in B_0$ and $f(x) \notin B_1$ iff $x \in f^{-1}(B_0)$ and $x \notin f^{-1}(B_1)$ iff $x \in f^{-1}(B_0) - f^{-1}(B_1)$.

(e) $y \in f(A_0) \Rightarrow \exists x \in A_0 \subset A_1 : f(x) = y \Rightarrow y \in f(A_1)$.

(f) Using (e), $f(A_i) \subset f(A_0 \cup A_1) \Rightarrow f(A_0) \cup f(A_1) \subset f(A_0 \cup A_1)$. The other direction: $y \in f(A_0 \cup A_1) \Rightarrow \exists x \in A_0 \cup A_1 : f(x) = y \Rightarrow \exists x \in A_0 : f(x) = y$ or $\exists x \in A_1 : f(x) = y \Rightarrow y \in f(A_0) \cup f(A_1)$.

(g) The "$\subset$ " part follows from (e). If f is injective then $y \in f(A_0) \cap f(A_1) \Rightarrow \exists x \in A_0 : f(x) = y$ and $\exists x' \in A_1 : f(x') = y$. Since f is injective, $x = x' \in A_0 \cap A_1 \Rightarrow y \in f(A_0 \cap A_1)$.

(h) If $y \in f(A_0) - f(A_1)$, then $\exists x \in A_0 : f(x) = y$ and, hence, $x \notin A_1$. Therefore, $y \in f(A_0 - A_1)$. If f is injective then $y \in f(A_0 - A_1) \Rightarrow \exists x \in A_0 - A_1 : f(x) = y \Rightarrow y \in f(A_0)$ and $y \notin f(A_1)$ (otherwise, $y = f(x')$ for some $x' \in A_1$, and, since f is injective, $x = x' \in A_1$) $\Rightarrow y \in f(A_0) - f(A_1)$.

3.

Show that (b), (c), (f), and (g) of Exercise 2 hold for arbitrary unions and intersections.

The proofs are almost identical to those in 2 (b), (c), (f) and (g). One just needs to replace pairwise unions and intersection (as well as some wording) with arbitrary unions and intersections.

4.

Let $f : A \to B$ and $g : B \to C$.

(a) If $C_0 \subset C$, show that $(g \circ f)^{-1}(C_0) = f^{-1}(g^{-1}(C_0))$.

(b) If f and g are injective, show that $g \circ f$ is injective.

(c) If $g \circ f$ is injective, what can you say about injectivity of f and g ?

(d) If f and g are surjective, show that $g \circ f$ is surjective.

(e) If $g \circ f$ is surjective, what can you say about surjectivity of f and g ?

(f) Summarize your answers to (b)-(e) in the form of a theorem.

(a) $x \in (g \circ f)^{-1}(C_0) \Leftrightarrow g(f(x)) \in C_0 \Leftrightarrow f(x) \in g^{-1}(C_0) \Leftrightarrow x \in f^{-1}(g^{-1}(C_0))$.

(b)-(f) $g \circ f$ is injective iff f is injective and g is injective on $f(A)$. It is surjective iff g is surjective on $f(A)$ (and, therefore, is surjective on the larger set B as well). In particular, if f and g are surjective, then $f(A) = B$, and g is surjective on $f(A) = B$, i.e. $g \circ f$ is surjective.

5.

In general, let us denote the ***identity function*** for a set C by i_C. That is, define $i_C : C \to C$ to be the function given by the rule $i_C(x) = x$ for all $x \in C$. Given $f : A \to B$, we say that a function $g : B \to A$ is a ***left inverse*** for f if $g \circ f = i_A$; and we say that $h : B \to A$ is a ***right inverse*** for f if $f \circ h = i_B$.

(a) Show that if f has a left inverse, f is injective; and if f has a right inverse, f is surjective.

(b) Give an example of a function that has a left inverse but no right inverse.

(c) Give an example of a function that has a right inverse but no left inverse.

(d) Can a function have more than one left inverse? More than one right inverse?

(e) Show that if f has both a left inverse g and a right inverse h, then f is bijective and $g = h = f^{-1}$.

(a) Apply 4 (c) and (e) using the fact that the identity function is bijective.

(b) $e^x : \mathbb{R} \to \mathbb{R} - \{0\}$ has at least two left inverses $ln(|x|)$ and, for example, $ln(|max\{x, -1\}|)$ but no right inverses (it is not surjective).

(c) $x^2 : \mathbb{R} \to \overline{\mathbb{R}}_+$ has two right inverses $\sqrt{x}$ and $-\sqrt{x}$ but no left inverse (it is not injective).

(d) See (b) and (c).

(e) It follows from (a) that f is bijective, i.e. for each $y \in B$ there is unique $x \in A$ such that $f(x) = y$. Now, $g(y) = g(f(x)) = x$, and $f(x) = y = f(h(y))$, and, since f is injective, $h(y) = x$ as well.

6.

Let $f : \mathbb{R} \to \mathbb{R}$ be the function $f(x) = x^3 - x$. By restricting the domain and range of f appropriately, obtain from f a bijective function g. Draw the graphs of g and g^{-1}. (There are several possible choices for g.)

For example, $f : \{0\} \to \{0\}$. :) The graph is the point $(0,0)$. Other solutions: $f : \{1, 2\} \to \{0, 6\}$, $f : [-0.5, 0.5] \to [-\frac{3}{8}, \frac{3}{8}]$, $f : (-\infty, -1] \to (-\infty, 0]$, $f : [1, +\infty) \to [0, +\infty)$ etc.

SECTION THREE

1.

Define two points (x_0, y_0) and (x_1, y_1) of the plane to be equivalent if $y_0 - x_0^2 = y_1 - x_1^2$. Check that this is an equivalence relation and describe the equivalence classes.

Reflexivity, Symmetry and Transitivity (RST) obviously hold. The equivalence classes are sets of points on parabolas $y = x^2 + c$.

2.

Let C be a relation on a set A. If $A_0 \subset A$, define the ***restriction*** of C to A_0 to be the relation $C \cap (A_0 \times A_0)$. Show that the restriction of an equivalence relation is an equivalence relation.

RST hold for the restriction of $\sim$ (follows directly from their definitions restricted to the subset; all three properties hold because the restriction includes all pairs in $\sim$ that have both elements in the subset), and the equivalence classes are those of $\sim$ intersected with the subset.

3.

Here is a "proof that every relation C that is both symmetric and transitive is also reflexive: "Since C is symmetric, aCb implies bCa. Since C is transitive, aCb and bCa together imply aCa, as desired." Find the flaw in this argument.

To prove that a relation C is reflexive, we need to prove that for *every* a, aCa. What the proof above does, it shows that for *some* a such that there happens to be b such that aCb, we can show that aCa must hold. But what if there is a such that there is no b such that either aCb or bCa holds? Then the proof cannot be applied to such a to prove that aCa.

The easiest example is the empty relation on a non-empty set. It is (vacuously) symmetric and transitive. But, of course, it is not reflexive. Given any a, there is just no b such that either aCb or bCa holds, hence, the proof does not work.

4.

Let $f : A \to B$ be a surjective function. Let us define a relation on A by setting $a_0 \sim a_1$ if

$$f(a_0) = f(a_1).$$

(a) Show that this is an equivalence relation.

(b) Let A^* be the set of equivalence classes. Show there is a bijective correspondence of A^* with B.

(a) RST clearly hold (they are inherited from the corresponding properties of the $=$ relation: $f(a) = f(a)$, $f(a) = f(b) \Rightarrow f(b) = f(a)$, and $f(a) = f(b) = f(c) \Rightarrow f(a) = f(c)$).

(b) Let $g : A^* \to B$ be a function such that $g(a^*) = f(a)$ where $a \in a^*$. g is well-defined, as the choice of $a \in a^*$ does not matter, injective, as f is different for elements in different classes (otherwise they would be in the same class), and surjective, as f is surjective.

5.

Let S and S' be the following subsets of the plane:

$$S = \{(x, y) | y = x + 1 \text{ and } 0 < x < 2\},$$

$$S' = \{(x, y) | y - x \text{ is an integer}\}.$$

(a) Show that S' is an equivalence relation on the real line and $S' \supset S$. Describe the equivalence classes of S' .

(b) Show that given any collection of equivalence relations on a set A , their intersection is an equivalence relation on A .

(c) Describe the equivalence relation T on the real line that is the intersection of all equivalence relations on the real line that contain S . Describe the equivalence classes of T .

(a) RST hold for S' ($x - x = 0$, $y - x = -(x - y)$ and $z - x = (z - y) + (y - x)$). The classes of equivalence are those points the pairwise distances between which are integer numbers. Alternatively, we can say that the class of points equivalent to x is $\{x + k | k \in \mathbb{Z}\}$. S contains *some* pairs such that the distance is 1, and, therefore, if xSy then $y - x = 1$, implying $xS'y$.

(b) If RST hold for any relation in the collection then they hold for any relation in the intersection. For example, if aRa for any $R \in \mathcal{R}$, then $(a, a) \in R$ for any $R \in \mathcal{R}$, and $(a, a) \in \cap_{R \in \mathcal{R}} R$, implying $a \cap_{R \in \mathcal{R}} Ra$. Similarly for the other properties.

(c) Every equivalence relation that contains S must have at least these pairs (x, y) : $y = x$ (reflexivity), $y = x + 1, 0 < x < 2$ (contains S), $y = x - 1, 1 < x < 3$ (symmetry), and, by transitivity and symmetry, $y = x + 2, 0 < x < 1$ and $y = x - 2, 2 < x < 3$. Let the set of these pairs be T . Then T is in the intersection. If we show that T is an equivalence relation itself, then it is the intersection (from (b) it follows that the intersection must be an equivalence relation, and, therefore, the intersection is an equivalence relation that is contained in any other equivalence relation that contains S).

But before we show that this is an equivalence relation, let us describe T less formally. T contains the following "equivalence classes" (we don't know yet that these are equivalence classes before we show that T is an equivalence relation, but within these subsets every element is related to every element, while no elements from different subsets are related): $\{x, x + 1, x + 2\}$ for $0 < x < 1$, $\{1, 2\}$, and $\{x\}$ for $x \leq 0$ and $x \geq 3$.

R and S clearly hold for T . The transitivity needs a proof. Let xTy and yTz . If $x = y$ or $y = z$ then xTz holds. If $x \neq y$ and $y \neq z$ then $x \in (0, 3)$, $y \in (0, 3)$, $y - x$ is an integer number (-2,-1,1 or 2), $z \in (0, 3)$, $z - y \in \{-2, -1, 1, 2\}$. Therefore, $z - x$ is an integer and both are in $(0, 3)$, i.e. either $x, z \in \{1, 2\}$ or $x, z \in \{a, a + 1, a + 2\}$ for some $a \in (0, 1)$. In either case, xTz .

6.

Define a relation on the plane by setting

$$(x_0, y_0) < (x_1, y_1)$$

if either $y_0 - x_0^2 < y_1 - x_1^2$, or $y_0 - x_0^2 = y_1 - x_1^2$ and $x_0 < x_1$. Show that this is an order relation on the plane, and describe it geometrically.

$(x_0, y_0) < (x_1, y_1)$ iff (x_0, y_0) lies on a lower parabola $y = x^2 + c$ or on the same parabola, but to the left of (x_1, y_1) . Comparability, Nonreflexivity and Transitivity (CnRT) hold.

7.

Show that the restriction of an order relation is an order relation.

CnRT hold for the restriction. Nonreflexivity holds because the restriction does not add any new pairs of points, and Comparability and Transitivity hold because the restriction includes all pairs of the initial relation such that both elements belong to the subset.

8.

Check that the relation defined in Example 7 is an order relation.

There are two relations defined in the example, the standard (usual) order relation on the real line, and the one such that xCy iff $x^2 < y^2$, or $x^2 = y^2$ and $x < y$. So, we are asked about this second one. In other words, we can restate the same relation as xCy iff $|x| < |y|$, or $|x| = |y|$ and $x < y$ (the closer the point is to the origin, the lower it is, and if two different points are at the same distance from the origin, then the positive one is greater than the negative one: $0 < -1 < 1 < -100 < 100$).

Comparability: for every $x \neq y$ either $x^2 > y^2$ (yCx), or $x^2 < y^2$ (xCy), or $x^2 = y^2$, in which case either $x < y$ (xCy) or $y < x$ (yCx). Nonreflexivity: for every x , $x^2 = x^2$ but $x \nless x$, so xCx does not hold. Transitivity: xCy and yCz imply $x^2 \leq y^2 \leq z^2$, and either $x^2 < z^2$ (xCz), or there are two equalities, implying $x^2 = z^2$, and $x < y < z$ (again, xCz).

9.

Check that the dictionary order is an order relation.

CnRT clearly hold. Indeed, for (a, b) , (c, d) and (e, f) , where $a, b, c, d, e, f \in A$, where A is an ordered set, the C property of A implies that either $a = c$, in which case either $b = d$ ($(a, b) = (c, d)$) or $b < d$ ($(a, b) < (c, d)$) or $b > d$ ($(a, b) > (c, d)$), or $a < c$ ($(a, b) < (c, d)$), or $a > c$ ($(a, b) > (c, d)$). Further, the nR property of A implies that $b \nless b$, hence, $(a, b) \nless (a, b)$. Finally, if $(a, b) < (c, d) < (e, f)$, then either $a < e$ (in A), implying $(a, b) < (e, f)$, or $a = c = e$ (why only these two cases?) and $b < d < f$, again implying $(a, b) < (e, f)$.

10.

(a) Show that the map $f : (-1,1) \to \mathbb{R}$ of Example 9 is order preserving.

(b) Show that the equation $g(y) = 2y/[1 + (1+4y^2)^{1/2}]$ defines a function $g : \mathbb{R} \to (-1,1)$ that is both a left and a right inverse for f.

$f(x) = x/(1-x^2)$.

(a) Using the derivative: $f'(x)(1-x^2)^2 = 1 + x^2 > 0$ implies that f is strictly increasing. Alternatively, we can argue that a) f is an odd function on $(-1,1)$ ($f(-x) = -f(x)$), so it is sufficient to show that it is increasing on $[0;1)$, b) for $0 \le x < 1$, the numerator of $f(x)$ is strictly increasing in x, while the denominator of $f(x)$ is strictly decreasing in x, where both remain non-negative. Hence, $f(x)$ is strictly increasing.

(b) We first check that $g(f(x)) = x$ for all $x \in (-1,1)$. We can parametrize $x \in (-1,1)$ as follows: $x = \tan\alpha, -\pi/4 < \alpha < \pi/4$. Note that $\cos 2\alpha > 0$, so $\cos 2\alpha = \sqrt{\cos^2 2\alpha}$. Then, $f(x) = \tan 2\alpha/2$, and $g(f(x)) = \tan 2\alpha/[1 + \sqrt{1+\tan^2 2\alpha}] = \sin 2\alpha/[\cos 2\alpha + 1] = \tan\alpha = x$. Now, we can either check directly that $f(g(y)) = y$ for all $y \in \mathbb{R}$, or use the following argument. We have shown in (a) that f is strictly increasing, and, hence, injective. It is also continuous having the negative and positive infinities as its limits when x goes to -1 and $+1$, respectively. Therefore, f is surjective, and bijective. There exists the inverse of f, f^{-1}, which is its left and right inverses. According to Exercise 5 of §2, Chapter 1, in this case every left or right inverse of f is equal to f^{-1}, implying that $g = f^{-1}$ is the left and right inverses of f.

11.

Show that an element in an ordered set has at most one immediate successor and at most one immediate predecessor. Show that a subset of an ordered set has at most one smallest element and at most one largest element.

If there are two different immediate successors of x, $a \neq b$, then $x < a$, $x < b$, and (x,a) and (x,b) are both empty, but since for the order either $a < b$ or $b < a$, one of the sets (x,a) or (x,b) is non-empty, contradiction. Similarly for immediate predecessors. "At most one smallest or largest element"-part follows from a similar argument as well (for example, if there are two different smallest elements of a set, then one has to be smaller than the other).

12.

Let $\mathbb{Z}_+$ denote the set of positive integers. Consider the following order relations on $\mathbb{Z}_+ \times \mathbb{Z}_+$:

(i) The dictionary order.

(ii) $(x_0, y_0) < (x_1, y_1)$ if either $x_0 - y_0 < x_1 - y_1$ or $x_0 - y_0 = x_1 - y_1$ and $y_0 < y_1$.

(iii) $(x_0, y_0) < (x_1, y_1)$ if either $x_0 + y_0 < x_1 + y_1$, or $x_0 + y_0 = x_1 + y_1$ and $y_0 < y_1$.

In these order relations, which elements have immediate predecessors? Does the set have a smallest element? Show that all three order types are different.

The following Figure 1↓ illustrates the orders.

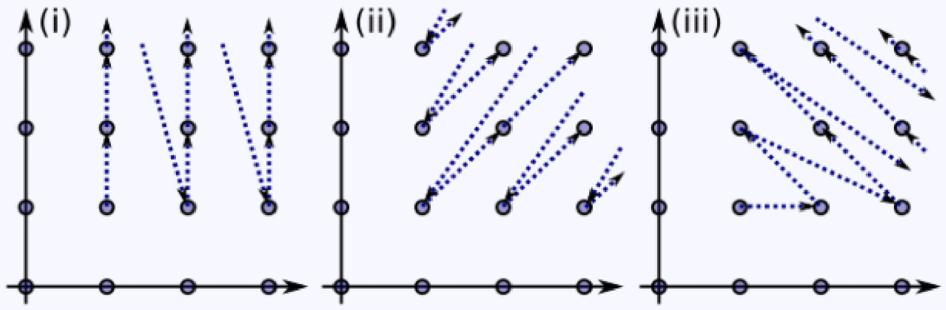

Figure 1 The three orders on $\mathbb{Z}_+ \times \mathbb{Z}_+$.

Immediate predecessors. (i) In the dictionary order every element (x, y) , $y > 1$, has an immediate predecessor $(x, y-1)$, while $(x, 1)$ does not (if $(x', y') < (x, 1)$ then $x' < x$, and $(x', y') < (x', y'+1) < (x, 1)$).

(ii) Suppose $(x', y') < (x, y)$. Consider two cases. If $x > 1$ and $y > 1$, then $(x', y') \leq (x-1, y-1) < (x, y)$ (either $x' - y' = x - y$ $= (x-1) - (y-1)$ and $y' \leq y-1$, or $x' - y' < x - y = (x-1) - (y-1)$), hence, the immediate predecessor of (x, y) in this case is $(x-1, y-1)$. If, on the other hand, $x = 1$ or $y = 1$, then $x' - y' < x - y$ (if $x' - y' = x - y$ then $y' < y$ and $x' < x$, one of which is not possible), and, hence, $(x', y') < (x'+1, y'+1) < (x, y)$, i.e. if $x = 1$ or $y = 1$, there is no immediate predecessor.

(iii) Suppose $(x', y') < (x, y)$. Consider two cases. If $y > 1$, then $(x', y') \leq (x+1, y-1) < (x, y)$ (either $x' + y' = x + y$ $= (x+1) + (y-1)$ and $y' \leq y-1$, or $x' + y' < x + y = (x+1) + (y-1)$). If $y = 1$, then $x' + y' < x + y$ (if $x' + y' = x + y$ then $y' < y = 1$), hence, $x + y > 2$ and $(x', y') \leq (1, x+y-2) < (x, y)$. Therefore, every element except $(1, 1)$ has an immediate predecessor, namely, if $y > 1$, it is $(x+1, y-1)$, and if $y = 1, x > 1$, it is $(1, x+y-2)$.

The smallest element. If there is a smallest element, then it must be the least among those without an immediate predecessor (but not vice versa, of course).

In (i) it is $(1, 1)$ and, indeed, it is the smallest.

In (ii) there is no smallest element without predecessor, as for every $(x, 1)$, we have $(1, 2) < (x, 1)$, but for every $(1, y)$, we have $(1, y+1) < (1, y)$ (another way to see that there is no smallest element in (ii): $(x, y+1) < (x, y)$).

In (iii) there is only one element without immediate predecessor, which is $(1, 1)$, and, as it is easy to see, it is the smallest element.

The order type. Given the answers for the previous questions, it is immediate that the order types are different. Indeed, if there is a bijective correspondence between two orders that preserves the order, then, as it is easy to see, it must also preserve immediate predecessors and smallest elements. However, from this point of view, the structure of each order is different.

Order	The number of elements without the immediate predecessor	Whether the order has the smallest element
(i)	Countable	+
(ii)	Countable	-
(iii)	1	+

> In fact, the order type of the order (ii) is that of the dictionary order on $\mathbb{Z} \times \mathbb{Z}_+$. And the order type of the order (iii) is that of $\mathbb{Z}_+$.
>
> Indeed, imagine, first, the dictionary order on $\mathbb{Z} \times \mathbb{Z}_+$, which is the order in (i) extended to the left for all x ' s. Now, take this dictionary order, and place it into the positive corner as in (ii). I.e. a point $(x, 1)$ goes to the point $(x+1, 1)$ if $x \geq 0$, or $(1, 1-x)$ if $x < 0$. We kind of bended the line $(x, 1)$ of the dictionary order to fit it into the corner. Now, for each point $(x, 1)$ of the original order, we take all points above it and place them to the diagonal that starts from the point where the point $(x, 1)$ was placed. For example, $(0, n)$ becomes (n, n) , $(1, n)$ becomes $(1+n, n)$, $(-1, n)$ becomes $(n, 1+n)$ etc. I hope you can see how the dictionary order on $\mathbb{Z} \times \mathbb{Z}_+$ becomes the order in (ii) (see Figure 1↑).
>
> If not, then here is a formal bijective correspondence: $f(x, y) = (\max(0, x) + y, \max(0, -x) + y)$. Let denote it as $f(x, y) = (a_{x,y}, b_{x,y})$. Note that $a_{x,y} - b_{x,y} = \max(0, x) - \max(0, -x) = x$ for all x , so that in the dictionary order $(x, y) < (x', y')$ iff $x < x'$, or $x = x'$ and $y < y'$ iff $a_{x,y} - b_{x,y} < a_{x',y'} - b_{x',y'}$ or $a_{x,y} - b_{x,y} = a_{x',y'} - b_{x',y'}$ and $x = x', y < y'$, i.e. $b_{x,y} < b_{x',y'}$, iff in the order (ii) $f(x, y) = (a_{x,y}, b_{x,y}) < (a_{x',y'}, b_{x',y'}) = f(x', y')$.
>
> Now, consider $\mathbb{Z}_+$. Place 1 to $(1, 1)$, 2 to $(2, 1)$ and 3 to $(1, 2)$, then 4 , 5 and 6 to $(3, 1)$, $(2, 2)$ and $(1, 3)$, correspondingly, and continue this way to get exactly the order (iii) illustrated in Figure 1↑. A more formal bijective correspondence between the two is also, of course, possible.

13.

Prove the following:

Theorem. If an ordered set A has the least upper bound property, then it has the greatest lower bound property.

Let S be a non-empty subset bounded from below. Let L be the set of all lower bounds of S . L is non-empty, as S is bounded from below and there is at least one lower bound, and bounded from above by any element in S . Therefore, L has the lowest upper bound x such that for any upper bound x' of $L : x \leq x'$. We show that x is the greatest lower bound of S . First, it is a lower bound of S , as any element z in S is an upper bound of L , implying $x \leq z$ for all z in S . Besides, for any other lower bound x' of S , $x' \in L$, therefore, $x' \leq x$.

14.

If C is a relation on a set A, define a new relation D on A by letting $(b, a) \in D$ if $(a, b) \in C$.

(a) Show that C is symmetric if and only if $C = D$.

(b) Show that if C is an order relation, D is also an order relation.

(c) Prove the converse of the theorem in Exercise 13.

(a) C is symmetric iff for all a, b, $aCb \Leftrightarrow bCa$ iff for all a, b, $bDa \Leftrightarrow aDb$ iff D is symmetric.

(b) If C satisfies comparability and nonreflexivity, so does D. If C is transitive, then for all a, b, c, aDb and bDc imply cCb and bCa, which imply cCa, which implies aDc, so D is also transitive.

(c) Denote C as $<$ and D as $>$. Then, using (b) to argue that $(A, <)$ is an ordered set iff $(A, >)$ is an ordered set, if $(A, <)$ has the greatest lower bound property, then for every $B \subset A$ such that $\exists x : x \leq b$ for all $b \in B$, there is $a \in A$ such that $a \leq b$ for all $b \in B$, and for every d such that $d \leq b$ for all $b \in B$, $d \leq a$, then for every $B \subset A$ such that $\exists x : b \geq x$ for all $b \in B$, there is $a \in A$ such that $b \geq a$ for all $b \in B$, and for every d such that $b \geq d$ for all $b \in B$, $a \geq d$, then $(A, >)$ has the least upper bound property, then (using Exercise 13) $(A, >)$ has the greatest lower bound property, then (using the same argument as above for $(A, >)$) $(A, <)$ has the least upper bound property.

I don’ t know if this looks any easier than a direct argument similar to Exercise 13 would do.

15.

Assume that the real line has the least upper bound property,

(a) Show that the sets

$$[0,1] = \{x|0 \leq x \leq 1\},$$
$$[0,1) = \{x|0 \leq x < 1\}$$

have the least upper bound property.

(b) Does $[0,1] \times [0,1]$ in the dictionary order have the least upper bound property? What about $[0,1] \times [0,1)$? What about $[0,1) \times [0,1]$?

(a) For $[0,1]$ all subsets are bounded from above (by 1 , for example), and the least upper bound of a subset of $[0,1]$ in the real line is the same as the one in $[0,1]$ (it has to be ≤ 1 , as 1 is an upper bound for any such subset).

For $[0,1)$ bounded from above are those subsets that have the least upper bound in the real line less than 1 (if the least upper bound is 1 , then there are points in the subset that are greater than $1-\epsilon$ for every $\epsilon > 0$, so there is no upper bound of the subset in $[0,1)$). Therefore, the same least upper bound is the one in $[0,1)$.

(b) $A = X \times Y = [0,1] \times [0,1]$ or $[0,1) \times [0,1]$. Let B be a bounded from above subset of A , and M be the set of all x -coordinates of all points in B . Since B is bounded from above in A , M is bounded from above in X , so let m be its least upper bound. If $m \notin M$ then there are no points in B with x -coordinate equal to m , but for any $z < m$ there is a point in B such that its x -coordinate is greater than z . Therefore, in this case $(m,0)$ is the least upper bound of B . If $m \in M$ then there are some points in B such that their x -coordinate is m , and the set of all their y -coordinates has the least upper bound n in $[0,1]$ (see (a)). Then, (m,n) is the least upper bound of B .

$A = [0,1] \times [0,1)$ does not satisfy the property, as, for example, $B = \{0\} \times [0,1)$ is bounded from above (by $(1,0)$, for example), but B has no least upper bound (for any $m > 0$, $(m,0)$ is an upper bound of B , but there is no upper bound $(0,y)$).

SECTION FOUR

1.

Prove the following "laws of algebra" for $\mathbb{R}$, using only axioms (1)-(5):

(a) If $x + y = x$, then $y = 0$.

(b) $0 \cdot x = 0$. [*Hint:* Compute $(x + 0) \cdot x$.]

(c) $-0 = 0$.

(d) $-(-x) = x$.

(e) $x(-y) = -(xy) = (-x)y$.

(f) $(-1)x = -x$.

(g) $x(y - z) = xy - xz$.

(h) $-(x + y) = -x - y$; $-(x - y) = -x + y$.

(i) If $x \neq 0$ and $x \cdot y = x$, then $y = 1$.

(j) $x/x = 1$ if $x \neq 0$.

(k) $x/1 = x$.

(l) $x \neq 0$ and $y \neq 0 \Rightarrow xy \neq 0$.

(m) $(1/y)(1/z) = 1/(yz)$ if $y, z \neq 0$.

(n) $(x/y)(w/z) = (xw)/(yz)$ if $y, z \neq 0$.

(o) $(x/y) + (w/z) = (xz + wy)/(yz)$ if $y, z \neq 0$.

(p) $x \neq 0 \Rightarrow 1/x \neq 0$.

(q) $1/(w/z) = z/w$ if $w, z \neq 0$.

(r) $(x/y)/(w/z) = (xz)/(yw)$ if $y, w, z \neq 0$.

(s) $(ax)/y = a(x/y)$ if $y \neq 0$.

(t) $(-x)/y = x/(-y) = -(x/y)$ if $y \neq 0$.

(a) $y = 0 + y = ((-x) + x) + y = (-x) + (x + y) = (-x) + x = 0$.

(b) Using (a), $x \cdot x = (x + 0) \cdot x = x \cdot x + 0 \cdot x$ implies $0 \cdot x = 0$.

(c) $-0 = (-0) + 0 = 0$.

(d) $-(-x) = -(-x) + ((-x) + x) = (-(-x) + (-x)) + x = x$.

(e) Using (b), $x(-y) = x(-y) + (xy + (-(xy)))$ $= (x(-y) + xy) + (-(xy))$ $= x((-y) + y) + -(xy) = -(xy)$. Similarly for $(-x)y$.

(f) This follows from (e).

(g) This follows from the distributive law and (e).

(h) Using the associative and commutative laws, we can omit parentheses and regroup terms in addition: $-(x + y) = -(x + y) + (x - x) + (y - y) = -(x + y) + (x + y) + (-x) + (-y)$ $= -x - y$, and similarly for $-(x - y)$.

(i) Similar to (a), $y = ((1/x) \cdot x) \cdot y = (1/x) \cdot (x \cdot y) = (1/x) \cdot x = 1$.

(j) By definition, $x/x = x \cdot (1/x) = 1$.

(k) By definition, $1/1 = 1$ as $1 \cdot 1 = 1$, hence, $x/1 = x \cdot (1/1) = x \cdot 1 = x$.

(l) From (b) it follows that there is no z such that $0 \cdot z = 1$. However, if $x \neq 0$ and $y \neq 0$, then $(xy) \cdot ((1/x) \cdot (1/y))$ $= ((yx) \cdot (1/x)) \cdot (1/y)$ $= (y \cdot (x \cdot (1/x))) \cdot (1/y)$ $= y \cdot (1/y)$ $= 1$, hence, $xy \neq 0$.

(m) See the second part of (l) that shows that $1/(xy) = (1/x) \cdot (1/y)$ for $x, y \neq 0$.

(n) Using associativity and commutativity we can regroup terms and then use (m): $(x/y) \cdot (w/z) = x \cdot w \cdot ((1/y) \cdot (1/z)) = (xw) \cdot (1/(yz)) = (xw)/(yz)$.

(o) Using (j) and (n), $x/y = (x/y) \cdot (z/z)$ $= (xz)/(yz)$ $= (xz) \cdot (1/(yz))$, and similarly $w/z = (wy) \cdot (1/(yz))$, so that we can use the distributive law.

(p) Again, from (b) it follows that if $y \cdot z = 1$ for some y and z , then neither y nor z equals 0 , but we have $x \cdot (1/x) = 1$.

(q) Using (n) and (j), $(z/w) \cdot (w/z) = (zw)/(zw) = 1$.

(r) Using (q) and (n), $(x/y)/(w/z) = (x/y) \cdot (z/w) = (xz)/(yw)$.

(s) Using (n) and (k), $(ax)/y = (ax)/(1 \cdot y) = (a/1) \cdot (x/y) = a \cdot (x/y)$.

(t) Using (f), (s) and then (f) again, we immediately get $(-x)/y = -(x/y)$. Also, using (f) and (d), $(-1) \cdot (-1) = -(-1) = 1$, hence, $1/(-1) = -1$, and, using (f), (n) and (f) again, $x/(-y) = (1/(-1)) \cdot (x/y) = (-1) \cdot (x/y) = -(x/y)$.

2.

Prove the following "laws of inequalities" for $\mathbb{R}$, using axioms (1)-(6) along with the results of Exercise 1:

(a) $x > y$ and $w > z \Rightarrow x + w > y + z$.

(b) $x > 0$ and $y > 0 \Rightarrow x + y > 0$ and $x \cdot y > 0$.

(c) $x > 0 \Leftrightarrow -x < 0$.

(d) $x > y \Leftrightarrow -x < -y$.

(e) $x > y$ and $z < 0 \Rightarrow xz < yz$.

(f) $x \neq 0 \Rightarrow x^2 > 0$, where $x^2 = x \cdot x$.

(g) $-1 < 0 < 1$.

(h) $xy > 0 \Leftrightarrow x$ and y are both positive or both negative.

(i) $x > 0 \Rightarrow 1/x > 0$.

(j) $x > y > 0 \Rightarrow 1/x < 1/y$.

(k) $x < y \Rightarrow x < (x + y)/2 < y$.

(a) $x + w > x + z > y + z$.

(b) Using (a), $x + y > 0 + 0 = 0$, and using Exercise 1(b), $x \cdot y > 0 \cdot y = 0$.

(c) If $x > 0$, then $x + (-x) = 0 > 0 + (-x) = -x$, and if $(-x) < 0$, then $(-x) + x = 0 < 0 + x = x$.

(d) Similar to (c) (from left to right add $(-x) + (-y)$ to both sides, from right to left add $x + y$ to both sides).

(e) Using (c) and Exercise 1(d), $z = -(-z) < 0$ implies $-z > 0$, so, using Exercise 1(e), $x \cdot (-z) = -(xz) > y \cdot (-z) = -(yz)$, and by (d), $xz < yz$.

(f) If $x > 0$ then (b) implies $x^2 > 0$, and if $x < 0$ then (e) and Exercise 1(b) imply $0 \cdot x = 0 < x^2$.

(g) $1 \cdot 1 = 1$ implies two things: a) from Exercise 1(b) it follows that $1 \neq 0$, and b) from (f) it follows that $1^2 = 1 > 0$. Now, using (c), $-1 < 0$.

(h) If x and y are both positive, then, by (b), $xy > 0$. If they are both negative, then, by (e) and Exercise 1(b), $0 \cdot y = 0 < yx$. If at least one of them is 0 , then Exercise 1(b) implies $xy = 0$. If $x > 0$ and $y < 0$, then, by (e) and Exercise 1(b), $xy < 0 \cdot y = 0$. Similarly, if $x < 0$ and $y > 0$, $xy < 0$.

(i) Using (g) and (h), $x \cdot (1/x) = 1 > 0$ implies that x and $1/x$ are both positive or both negative.

(j) Using transitivity, $x > 0$, using (i), $1/x > 0$ and $1/y > 0$, and now we can just multiply both sides of $x > y$ by $1/x$ and then by $1/y$.

(k) First, add x or y to both sides of $x < y$ to obtain $x + x < x + y$ and $x + y < y + y$. Now, argue that for any z , $(z + z)/2 = (z \cdot 1 + z \cdot 1) \cdot (1/2) = z \cdot (1 + 1) \cdot (1/(1 + 1)) = z$. Further, using (g) and (a), $1 + 1 = 2 > 0 + 0 = 0$, and (i) implies $1/2 > 0$. Hence, $(x + x)/2 = x < (x + y)/2 < (y + y)/2 = y$.

3.

(a) Show that if $\mathcal{A}$ is a collection of inductive sets, then the intersection of the elements of $\mathcal{A}$ is an inductive set.

(b) Prove the basic properties (1) and (2) of $\mathbb{Z}_+$.

(a) For every $x \in \cap_{A \in \mathcal{A}} A$, $x \in A$ for all $A \in \mathcal{A}$, therefore, $x + 1 \in A$ for all $A \in \mathcal{A}$, therefore, $x + 1 \in \cap_{A \in \mathcal{A}} A$. Moreover, $1 \in A$ for all $A \in \mathcal{A}$, hence, $1 \in \cap_{A \in \mathcal{A}} A$, and $\cap_{A \in \mathcal{A}} A$ is inductive.

(b) $\mathbb{Z}_+$ is inductive by (a). And if A is an inductive set of positive integers, then it is both a subset and superset of $\mathbb{Z}_+$.

4.

(a) Prove by induction that given $n \in \mathbb{Z}_+$, every nonempty subset of $\{1, \ldots, n\}$ has a largest element.

(b) Explain why you cannot conclude from (a) that every nonempty subset of $\mathbb{Z}_+$ has a largest element.

(a) Let A be the set of all positive integers n for which this statement is true. It is true for $n = 1$, as $\{1\}$ has only one nonempty subset, namely $\{1\}$ itself with the largest element 1 , so $1 \in A$. Suppose $n \in A$. Then every nonempty subset of $\{1, \ldots, n+1\}$ either contains $n+1$ or does not. In the first case, $n+1$ is the largest element of the subset, and in the second case, the subset is also a subset of $\{1, \ldots, n\}$ and, hence, has the largest element. Therefore, $n+1 \in A$, A is an inductive subset of $\mathbb{Z}_+$, and $A = \mathbb{Z}_+$.

(b) Because the statement is proved for all such subsets that are contained within some set $\{1, \ldots, n\}$, i.e. all bounded from above subsets. But, as it was shown in the text, there are some unbounded subsets as well, for example, the set $\mathbb{Z}_+$ itself. To compare to Theorem 4.1, where for every $n \in D$ the smallest element has to be not greater than n , and, hence, be an element of $\{1, \ldots, n\}$, in our case, the largest element d (if it exists at all) has to be not smaller than any $n \in D$, which by itself does not imply that there is any set S_m such that $d \in S_m$.

5.

Prove the following properties of $\mathbb{Z}$ and $\mathbb{Z}_+$:

(a) $a, b \in \mathbb{Z}_+ \quad \Rightarrow \quad a+b \in \mathbb{Z}_+$. [*Hint:* Show that given $a \in \mathbb{Z}_+$, the set $X = \{x | x \in \mathbb{R} \text{ and } a+x \in \mathbb{Z}_+\}$ is inductive.]

(b) $a, b \in \mathbb{Z}_+ \Rightarrow a \cdot b \in \mathbb{Z}_+$.

(c) Show that $a \in \mathbb{Z}_+ \quad \Rightarrow \quad a-1 \in \mathbb{Z}_+ \cup \{0\}$. [*Hint:* Let $X = \{x | x \in \mathbb{R} \text{ and } x-1 \in \mathbb{Z}_+ \cup \{0\}\}$; show that X is inductive.]

(d) $c, d \in \mathbb{Z} \Rightarrow c+d \in \mathbb{Z}$ and $c-d \in \mathbb{Z}$. [*Hint:* Prove it first for $d=1$.]

(e) $c, d \in \mathbb{Z} \Rightarrow c \cdot d \in \mathbb{Z}$.

(a) Using hint: given $a \in \mathbb{Z}_+$, it easy to see that $1 \in X$, as $a+1 \in \mathbb{Z}_+$, and X is inductive, as if $a+x \in \mathbb{Z}_+$, then $a+(x+1) = (a+x)+1 \in \mathbb{Z}_+$. Hence, $\mathbb{Z}_+ \subset X$. (Note, that, in general, $X \neq \mathbb{Z}_+$ but showing that $\mathbb{Z}_+ \subset X$ is enough for our purposes.)

(b) Similarly here, but using (a): define X similarly to (a) but for multiplication, argue that $1 \in X$, which is kind of obvious, and then argue, using (a), that if $x \in X$, i.e. if $a \cdot x \in \mathbb{Z}_+$, then $x+1 \in X$, i.e. $a \cdot (x+1) = a \cdot x + a \in \mathbb{Z}_+$.

(c) Using hint: $1 \in X$ as $1-1=0 \in \mathbb{Z}_+ \cup \{0\}$, and if $x \in X$, then $x-1 \in \mathbb{Z}_+ \cup \{0\}$, and $(x+1)-1 = x = (x-1)+1 \in \mathbb{Z}_+ \subset \mathbb{Z}_+ \cup \{0\}$, implying $x+1 \in X$. Therefore, X is inductive, and $\mathbb{Z}_+ \subset X$.

For (d) and (e) we first prove the following statement.

Theorem If $A \subset \mathbb{Z}$ is such that $0 \in A$, and $x \in A$ implies $x-1, x+1 \in A$, then .

> Indeed, is inductive, so that , , and , implies that is inductive as well, i.e. , and for all , . Overall, , i.e. .

We can now prove (d) and (e) similar to (a) and (b). But first, using the hint, we prove (d) for . Let . Then, as , , and if , then , and . Further, if then (using (c)), if then , and if then for some , so that . Similar, if then , if then , and if then for some , so that where, by (c), either or , but in either case . Overall, , so that , and, by the theorem, .

Now, having (d) for the case , we prove that if , then for every , . We define , argue that as , and if , then as (note that, in (d), we use the proved case , and for multiplication in (e), we use (d)). Hence, we show that satisfies the conditions of the theorem above, and .

6.

Let $a \in \mathbb{R}$. Define inductively

$$a^1 = a,$$
$$a^{n+1} = a^n \cdot a$$

for $n \in \mathbb{Z}_+$. (See §7 for a discussion of the process of inductive definition.) Show that for $n, m \in \mathbb{Z}_+$ and $a, b \in \mathbb{R}$,

$$a^n a^m = a^{n+m},$$
$$(a^n)^m = a^{nm},$$
$$a^m b^m = (ab)^m.$$

These are called the ***laws of exponents***. [*Hint:* For fixed n, prove the formulas by induction on m.]

Following the hint, we prove the equalities by induction on m, but we prove them for all $n \in \mathbb{Z}_+$ at the same time, why not? Let A, B and C be the sets of all positive integers m such that the first, second and third equality above, respectively, holds for every $n \in \mathbb{Z}_+$ and $a, b \in \mathbb{R}$. Then, $1 \in A \cap B \cap C$, as, by definition, $x^1 = x$ for all $x \in \mathbb{R}$, and for all $n \in \mathbb{Z}_+$ and $a, b \in \mathbb{R}$, $a^n \cdot a^1 = a^n \cdot a = a^{n+1}$, $(a^n)^1 = a^n = a^{n \cdot 1}$, and $a^1 \cdot b^1 = ab = (ab)^1$. Now, we show that if $m \in A$, then $m + 1 \in A$. Again, by definition, for every $n \in \mathbb{Z}_+$ and $a \in \mathbb{R}$, $a^n a^{m+1} = a^n \cdot (a^m \cdot a) = (a^n \cdot a^m) \cdot a = a^{n+m} a = a^{(n+m)+1} = a^{n+(m+1)}$. Hence, A is inductive, and $A = \mathbb{Z}_+$. We are going to use this fact to prove that B is inductive as well. By definition, for every $n \in \mathbb{Z}_+$ and $a \in \mathbb{R}$, $(a^n)^{m+1} = (a^n)^m a^n = a^{nm} a^n$ [here we use the fact that $A = \mathbb{Z}_+$] $= a^{nm+n} = a^{n(m+1)}$, hence, $B = \mathbb{Z}_+$. Finally, again by definition, for every $n \in \mathbb{Z}_+$ and $a, b \in \mathbb{R}$, $a^{m+1} b^{m+1} = (a^m a)(b^m b) = (a^m b^m)(ab) = (ab)^m (ab) = (ab)^{m+1}$, hence, C is inductive, and $C = \mathbb{Z}_+$.

7.

Let $a \in \mathbb{R}$ and $a \neq 0$. Define $a^0 = 1$, and for $n \in \mathbb{Z}_+$, $a^{-n} = 1/a^n$. Show that the laws of exponents hold for $a, b \neq 0$ and $n, m \in \mathbb{Z}$.

Using the theorem stated in the solution to Exercise 5, we can again, similar to Exercise 6, define A , B and C to be the sets of all integers m such that the first, second and third law of exponents, respectively, holds for all $n \in \mathbb{Z}$ and $a, b \in \mathbb{R} - \{0\}$. Then, $0 \in A \cap B \cap C$, as, by definition, for every $n \in \mathbb{Z}$ and $a, b \in \mathbb{R} - \{0\}$, $a^n a^0 = a^n \cdot 1 = a^{n+0}$, $(a^n)^0 = 1 = a^{n \cdot 0}$, and $a^0 b^0 = 1 \cdot 1 = 1 = (ab)^0$.

To prove the "induction" step stated in the theorem of Exercise 5, we may find it useful to note that $a^n a = a^{n+1}$ for all $n \in \mathbb{Z}$, regardless of whether n is positive, zero or negative. Indeed, if n is positive, then this is just by definition, if $n = 0$ then we have $a = a$, if $n = -1$ then we have $(1/a) \cdot a = 1 = a^0$, and if $n < -1 < 0$ then $n + 1 < 0$ and, by denoting $m = -n$, $m > 1 > 0$, we have $(1/a^m) \cdot a = 1/a^{m-1}$, which follows from $(1/a^m) \cdot a \cdot a^{m-1} = 1$. Similarly, for every $n \in \mathbb{Z}$, $a^n a^{-1} = a^n (1/a) = a^{n-1}$. This follows from the fact that $n - 1 \in \mathbb{Z}$ and $a^{n-1} a = a^n$.

Now, if $m \in A$, then for every $n \in \mathbb{Z}$ and $a \in \mathbb{R} - \{0\}$, $a^n a^{m+1} = a^n a^m a$ $= a^{n+m} a = a^{n+m+1}$, and $a^n a^{m-1} = a^n a^{m-1} a a^{-1} = a^n a^m a^{-1} = a^{n+m} a^{-1} = a^{n+m-1}$, hence, $m - 1, m + 1 \in A$, A satisfies the conditions of the theorem, and $A = \mathbb{Z}$. If $m \in B$, then for every $n \in \mathbb{Z}$ and $a \in \mathbb{R} - \{0\}$, $(a^n)^{m+1} = (a^n)^m a^n = a^{nm} a^n$ [using the fact that $A = \mathbb{Z}$] $= a^{nm+n} = a^{n(m+1)}$, and $(a^n)^{m-1} = (a^n)^m (a^n)^{-1} = a^{nm} (a^n)^{-1}$ $= a^{n(m-1)+n} (a^n)^{-1}$ [using $A = \mathbb{Z}$ again] $= a^{n(m-1)} a^n (a^n)^{-1} = a^{n(m-1)}$. Hence, $B = \mathbb{Z}$. If $m \in C$, then for every $n \in \mathbb{Z}$ and $a, b \in \mathbb{R} - \{0\}$, $a^{m+1} b^{m+1} = a^m a b^m b = a^m b^m ab$ $= (ab)^m (ab)$ $(ab)^{m+1}$, and $a^{m-1} b^{m-1} = a^m a^{-1} b^m b^{-1} = a^m b^m a^{-1} b^{-1} = (ab)^m a^{-1} b^{-1}$ $= (ab)^{m-1} (ab) a^{-1} b^{-1} = (ab)^{m-1}$. Therefore, $C = \mathbb{Z}$.

8.

(a) Show that $\mathbb{R}$ has the greatest lower bound property.

(b) Show that $\inf\{1/n | n \in \mathbb{Z}_+\} = 0$.

(c) Show that given a with $0 < a < 1$, $\inf\{a^n | n \in \mathbb{Z}_+\} = 0$. [*Hint:* Let $h = (1 - a)/a$, and show that $(1 + h)^n \geq 1 + nh$.]

(a) See Exercise 13 of §3.

(b) 0 is a lower bound, as $n > 0$ implies $1/n > 0$ (Exercise 2(i)), but for every $x > 0$ there is $n > 1/x > 0$ ($\mathbb{Z}_+$ is unbounded), therefore, $1/n < x$ (Exercise 2(j)). That is, every positive number is not a lower bound for the set, and 0 is the greatest lower bound.

(c) Using hint, if $0 < a < 1$, then $1/a > 1$ (Exercise 2(j)), and $h = (1 - a)/a$ $= 1/a - 1 > 0$, hence, if we show that for a positive h , $(1 + h)^n \geq 1 + nh$, we can use this fact to argue that for every $x > 0$ there exists n such that $(1 + h)^n = (1/a)^n = 1/a^n > 1/x$ (all we need is to find n such that $1 + nh > 1/x$, or $n > (1/x - 1)/h$, which always exists as $\mathbb{Z}_+$ is unbounded), and, therefore, $a^n < x$, implying there is no positive lower bound. To show that $(1 + h)^n \geq 1 + nh$ for all positive integer n we can use the induction principle again: $(1 + h)^1 = 1 + 1 \cdot h$, and $(1 + h)^n \geq 1 + nh$ implies $(1 + h)^{n+1} \geq (1 + nh)(1 + h)$ $= 1 + (n + 1)h + nh^2 \geq 1 + (n + 1)h$. Now, since $a > 0$, by induction, $a^n > 0$ for all $n \in \mathbb{Z}_+$, and 0 is the greatest lower bound for the set.

9.

(a) Show that every nonempty subset of $\mathbb{Z}$ that is bounded above has a largest element.

(b) If $x \notin \mathbb{Z}$, show there is exactly one $n \in \mathbb{Z}$ such that $n < x < n+1$.

(c) If $x - y > 1$, show there is at least one $n \in \mathbb{Z}$ such that $y < n < x$.

(d) If $y < x$, show there is a rational number z such that $y < z < x$.

(a) Suppose $A \subset \mathbb{Z}$ and $A \neq \emptyset$. If all elements of A are negative, then the set $-A = \{n| -n \in A\} \subset \mathbb{Z}_+$ has the smallest element, which is the largest element of A. If $0 \in A$ and there are no positive numbers in A, then 0 is the largest element of A. Finally, if A has positive integers, then, using Exercise 4(a) and the fact that A is bounded above by some real number, and, hence, by a positive integer number m, i.e. $A \cap \mathbb{Z}_+ \subset \{1, \dots, m\}$, we conclude that A has a largest element.

(b) Consider the set $A \subset \mathbb{Z}$ of integers less than x. It is nonempty ($-n \in A$ where $n > -x$), bounded from above by x, has a largest element (by (a)), which is n such that $n < x$ and $n + 1 \geq x$. But $x \notin \mathbb{Z}$, so that $x < n+1$.

(c) Use (b) to find n such that $n < x \leq n+1$ (i.e., unlike (b), x can be an integer number, in which case we let $n = x - 1$), and use other proved properties to verify that this $y < x - 1 \leq n$.

(d) Consider $x - y > 0$, then find $n \in \mathbb{Z}_+$ such that $n > 1/(x-y) > 0$. We have $nx - ny > 1$, so we can use (c) to find $m \in \mathbb{Z}$ such that $ny < m < nx$. It follows that m/n is a rational number between x and y.

10.

Show that every positive number a has exactly one positive square root, as follows:

(a) Show that if $x > 0$ and $0 \leq h < 1$, then

$$(x+h)^2 \leq x^2 + h(2x+1),$$
$$(x-h)^2 \geq x^2 - h(2x).$$

(b) Let $x > 0$. Show that if $x^2 < a$, then $(x+h)^2 < a$ for some $h > 0$; and if $x^2 > a$, then $(x-h)^2 > a$ for some $h > 0$.

(c) Given $a > 0$, let B be the set of all real numbers x such that $x^2 < a$. Show that B is bounded above and contains at least one positive number. Let $b = \sup B$; show that $b^2 = a$.

(d) Show that if b and c are positive and $b^2 = c^2$, then $b = c$.

(a) The inequalities follow from $0 \leq h^2 \leq h$.

(b) One needs to take $h > 0$ sufficiently small to ensure $h(2x) < h(2x+1) < |a - x^2|$, and use (a) here.

(c) If $a < 1$ then $a \in B$, as $a < 1$ implies $a^2 < a$, and B is bounded by 1, as $x^2 < a < 1$ implies $x < 1$. If $a \geq 1$ then $(0,1) \subset B$, as $0 < x < 1$ implies $x^2 < 1 \leq a$, and B is bounded by a, as $x \geq a \geq 1$ implies $x^2 \geq xa \geq a$. Now, suppose that $b^2 < a$, then, using (b), for some $h > 0$, $(b+h)^2 < a$, and $b + h > b$ is in B, hence, b is not an upper bound of B. Now, suppose that $b^2 > a$, then, using (b), for some $h > 0$, $(b-h)^2 > a$, and for every $x \in B$, $x < b - h$ (otherwise, $x \geq b - h > 0$, and $x^2 \geq (b-h)x \geq (b-h)^2 > a$), hence, b is not the least upper bound of B. Therefore, $b^2 = a$.

(d) If both are positive and one is less than the other, say $0 < b < c$, then $b^2 < bc < c^2$. We can only add that even if b and c are known to be nonnegative, $b^2 = c^2$ still implies $b = c$, as $x^2 = 0$ iff $x = 0$.

11.

Given $m \in \mathbb{Z}$, we say that m is ***even*** if $m/2 \in \mathbb{Z}$, and m is odd otherwise.

(a) Show that if m is odd, $m = 2n+1$ for some $n \in \mathbb{Z}$. [*Hint:* Choose n so that $n < m/2 < n+1$.]

(b) Show that if p and q are odd, so are $p \cdot q$ and p^n, for any $n \in \mathbb{Z}_+$.

(c) Show that if $a > 0$ is rational, then $a = m/n$ for some $m, n \in \mathbb{Z}_+$ where not both m and n are even. [*Hint:* Let n be the smallest element of the set $\{x | x \in \mathbb{Z}_+ \text{ and } x \cdot a \in \mathbb{Z}_+\}$.]

(d) *Theorem.* $\sqrt{2}$ *is irrational.*

(a) According to Exercise 9(b), $m/2 \notin \mathbb{Z}$ implies there is $n \in \mathbb{Z}$ such that $n < m/2 < n+1$. Then, $2n < m < 2n+2$, so that $m = 2n+1$ (this last point requires some clarification, namely, $2n+2 = (2n+1)+1$, and there is no $z \in \mathbb{Z}$ such that $2n < z < 2n+1$ or $2n+1 < z < (2n+1)+1$, see page 32, so the only possibility for $m \in \mathbb{Z}$ is $m = 2n+1$).

(b) In addition to (a), we need its converse, that is if $m = 2n+1$ for some $n \in \mathbb{Z}$, then m is odd. Indeed, in this case, $n < m/2 < n+1$, and, according to page 32, there are no integer number between n and $n+1$. Now, if p and q are odd, then for some $m, n \in \mathbb{Z}$, $p = 2m+1$ and $q = 2n+1$, hence, $p \cdot q = 2(2mn + m + n) + 1$ is odd. From this, by induction, if p and p^n is odd, then $p^{n+1} = p^n p$ is odd.

(c) Using the hint, n is the smallest positive integer such that $na \in \mathbb{Z}_+$. Let $m = na$, then $a = m/n$. If both m and n are even, then $n/2 \in \mathbb{Z}_+$, $(n/2)a = m/2 \in \mathbb{Z}_+$ and $n/2 < n$, contradiction.

(d) By definition, $\sqrt{2} \geq 0$, and $\sqrt{2} \neq 0$ as $0^2 = 0$. Assuming $\sqrt{2}$ is rational, by using (c), $\sqrt{2} = m/n$, where at least one of m and n is odd. Then $m^2/n^2 = 2$, $2n^2 = m^2$, and m^2 is even, as $m^2/2 = n^2$. Now, from (b) it follows that m is even, as otherwise m^2 would be odd, hence, $m = 2k$ for some $k \in \mathbb{Z}_+$. Therefore, $2n^2 = 4k^2$, and $n^2 = 2k^2$. Using the same argument, n^2 is even, and, hence, n must be even as well. Contradiction.

SECTION FIVE

1.

Show there is a bijective correspondence of $A \times B$ with $B \times A$.

$f(a, b) = (b, a)$. It is clearly injective and surjective.

2.

(a) Show that if $n > 1$ there is bijective correspondence of

$$A_1 \times \cdots \times A_n \text{ with } (A_1 \times \cdots \times A_{n-1}) \times A_n.$$

(b) Given the indexed family $\{A_1, A_2, \ldots\}$, let $B_i = A_{2i-1} \times A_{2i}$ for each positive integer i. Show there is bijective correspondence of $A_1 \times A_2 \times \cdots$ with $B_1 \times B_2 \times \cdots$.

(a) $f(a_1, a_2, \ldots, a_n) = ((a_1, \ldots, a_{n-1}), a_n)$. It is clearly injective and surjective.

> Note: by $(a_1, \ldots, a_k)$ we, of course, mean the function from the index set $\{1, \ldots, k\}$ to $\cup_{i=1}^{k} A_i$ such that $x(i) = a_i$ where $a_i \in A_i$, i.e. it is the specific element of the product $\prod_{i=1}^{k} A_i$. So, the range of f consists of the pair where the first element is a function itself, and the second one is an element of A_n.

(b) $f(a_1, a_2, \ldots) = ((a_1, a_2), (a_3, a_4), \ldots)$. It is clearly injective and surjective. See the note above.

3.

Let $A = A_1 \times A_2 \times \cdots$ and $B = B_1 \times B_2 \times \cdots$.

(a) Show that if $B_i \subset A_i$, for all i, then $B \subset A$. (Strictly speaking, if we are given a function mapping the index set $\mathbb{Z}_+$ into the union of the sets B_i, we must change its range before it can be considered as a function mapping $\mathbb{Z}_+$ into the union of the sets A_i. We shall ignore this technicality when dealing with cartesian products).

(b) Show the converse of (a) holds if B is nonempty.

(c) Show that if A is nonempty, each A_i is nonempty. Does the converse hold? (We will return to this question in the exercises of §19.)

(d) What is the relation between the set $A \cup B$ and the cartesian product of the sets $A_i \cup B_i$? What is the relation between the set $A \cap B$ and the cartesian product of the sets $A_i \cap B_i$?

(a) If f mapping $\mathbb{Z}_+$ into $\cup_{i \in \mathbb{Z}_+} B_i$ is such that $\forall i : f(i) \in B_i$, then it maps $\mathbb{Z}_+$ into $\cup_{i \in \mathbb{Z}_+} A_i \supset \cup_{i \in \mathbb{Z}_+} B_i$, and $\forall i: f(i) \in B_i \subset A_i$.

(b) If B is non-empty then all B_i are non-empty. If there is i such that $B_i \subset A_i$ does not hold, then there is some x in $B_i - A_i$, and there is an element f in B such that $f(i) = x \notin A_i$. Hence, $f \in B - A$. Contradiction.

> Compare (a) and (b) to Exercise 2 (j)-(l) of §1.

(c) If A is non-empty, then there is $f \in A$ such that $\forall i \in \mathbb{Z}_+$, $f(i) \in A_i$, i.e. for $i \in \mathbb{Z}_+$, A_i is non-empty. The converse. The comment in parentheses means that one needs to be careful in making an argument for the converse statement. In this case we will need to implicitly rely on the axiom of choice to argue that we can select one element x_i from each set A_i so that $f(i) = x_i \in A$. If we had an uncountable number of sets, the use of the axiom of choice would be crucial. In fact, the axiom of choice is equivalent to a more general version of the converse statement.

(d) Both imply the same set of functions $f : \mathbb{Z}_+ \to \cup_{i \in \mathbb{Z}_+} A_i \cup \cup_{i \in \mathbb{Z}_+} B_i$ such that $f(i) \in A_i \cup B_i$, but $A \cup B$ also requires that either for all $i \in \mathbb{Z}_+$, $f(i) \in \cup_{i \in \mathbb{Z}_+} A_i$, or for all $i \in \mathbb{Z}_+$, $f(i) \in \cup_{i \in \mathbb{Z}_+} B_i$. So $A \cup B \subset \prod_{i \in \mathbb{Z}_+} (A_i \cup B_i)$. But for the intersection we have the same set of functions $f : \mathbb{Z}_+ \to \cup_{i \in \mathbb{Z}_+} A_i \cap \cup_{i \in \mathbb{Z}_+} B_i$ such that each $f(i)$ must be in $A_i \cap B_i$.

Consider the following example. Let all A_i be the set of even numbers, and all B_i be the set of number divisible by 5. Then A is the set of all sequences of even numbers, and B is the set of all sequences of numbers divisible by 5. $A_i \cup B_i$ is the set of all numbers that are either even or divisible by 5, so $\prod_{i \in \mathbb{Z}_+} (A_i \cup B_i)$ contains all sequences of numbers that are either even or divisible by 5, while $A \cup B$ is the set of all sequences such that either all numbers in the sequence are even, or all numbers in the sequence are divisible by 5. Clearly, the latter is a subset of the former, and, for example, $(5, 2, 2, \ldots) \in \prod_{i \in \mathbb{Z}_+} (A_i \cup B_i) - (A \cup B)$. On the other hand, $A_i \cap B_i$ consists of the numbers divisible by 10, and both $\prod_{i \in \mathbb{Z}_+} (A_i \cap B_i)$ and $A \cap B$ contain the sequences of such numbers only.

4.

Let $m, n \in \mathbb{Z}_+$. Let $X \neq \emptyset$.

(a) If $m \leq n$, find an injective map $f : X^m \to X^n$.

(b) Find a bijective map $g : X^m \times X^n \to X^{m+n}$.

(c) Find an injective map $h : X^n \to X^\omega$.

(d) Find a bijective map $k : X^n \times X^\omega \to X^\omega$.

(e) Find a bijective map $l : X^\omega \times X^\omega \to X^\omega$.

(f) If $A \subset B$, find an injective map $m : (A^\omega)^n \to B^\omega$.

Let $x \in X$. Please also see the note to Exercise 2.

(a) $f(x_1, \ldots, x_m) = (x_1, \ldots, x_m, x, \ldots, x)$. It is clearly injective.

(b) $g((x_1, \ldots, x_m), (y_1, \ldots, y_n)) = (x_1, \ldots, x_m, y_1, \ldots, y_n)$. It is clearly injective and surjective.

(c) $h(x_1, \ldots, x_n) = (x_1, \ldots, x_n, x, x, \ldots)$. It is clearly injective.

(d) $k((x_1, \ldots, x_n), (y_1, y_2, \ldots)) = (x_1, \ldots, x_n, y_1, y_2, \ldots)$. It is clearly injective (if x ' s or y ' s are different, so is the image) and surjective.

(e) $l((x_1, x_2, \ldots), (y_1, y_2, \ldots)) = (x_1, y_1, x_2, y_2, \ldots)$. It is clearly injective and surjective.

(f) $m((a_{11}, a_{12}, \ldots), \ldots, (a_{n1}, a_{n2}, \ldots)) = (a_{11}, a_{21}, \ldots, a_{n1}, a_{12}, a_{22}, \ldots, a_{n2}, \ldots)$. It maps to B^ω as $a_{ij} \in A \subset B$, and is clearly injective. It may be not be surjective (unlike (e)) if A is a proper subset of B.

5.

Which of the following subsets of $\mathbb{R}^\omega$ can be expressed as the cartesian product of subsets of $\mathbb{R}$?

(a) $\{\mathbf{x}|x_j \text{ is an integer for all } i\}$.

(b) $\{\mathbf{x}|x_i \geq i \text{ for all } i\}$.

(c) $\{\mathbf{x}|x_i \text{ is an integer for all } i \geq 100\}$.

(d) $\{\mathbf{x}|x_2 = x_3\}$.

It is possible iff the set of the possible values of x_i does not depend on the specific values of other x_j in the sense that, given all values of x_j for $j \neq i$, the set of possible values of x_i should be either the empty set or a fixed set X_i (compare to Exercise 10 of §1). If this is true, then the set $X = \prod_{i \in \mathbb{Z}_+} X_i$. So, we get the positive answer in (a), (b) and (c). Namely, we have $\mathbb{Z}^\omega$, $(\overline{\mathbb{R}}_+ + 1) \times (\overline{\mathbb{R}}_+ + 2) \times \cdots$ where $\overline{\mathbb{R}}_+ + k = \{x \in \mathbb{R}|x \geq k\}$, and $\underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{99} \times \mathbb{Z} \times \mathbb{Z} \times \cdots$, respectively. In (d), when $x_2 = c$, x_3 can take values from $\{c\}$ only, so the set in (d) is not a cartesian product.

SECTION SIX

1.

Make a list of all the injective maps

$$f : \{1,2,3\} \to \{1,2,3,4\}.$$

Show that none is bijective. (This constitutes a *direct* proof that a set A of cardinality three does not have cardinality four.)

(b) How many injective maps

$$f : \{1,\ldots,8\} \to \{1,\ldots,10\}$$

are there? (You can see why one would not wish to try to prove directly that there is no bijective correspondence between these sets.)

(a) An injective correspondence will have its image set consisting of three elements of $\{1,2,3,4\}$. We can exclude one of the four elements from the set $\{1,2,3,4\}$, and for each case there are 6 ways to define a bijective correspondence of $\{1,2,3\}$ with the remaining set of 3 elements. You can explicitly write down these $4 \times 6 = 24$ injective correspondences.

(b) Similarly, we can exclude 2 elements from $\{1,\ldots,10\}$ (45 combinations), and define a bijection between $\{1,\ldots,8\}$ and the remaining subset of $\{1,\ldots,10\}$ consisting of 8 elements ($8! = 40320$ combinations). The total number of injective functions is $45 \times 40320 = 1,814,400$ combinations. If you spend 5 seconds on average to write down each bijective correspondence, it will take you 105 days to complete the list.

2.

Show that if B is not finite and $B \subset A$, then A is not finite.

Using Corollary 6.6, if A were finite, B would be finite too. Or, alternatively, using Corollary 6.7, if A is finite, then there is an injective function from A into a section of the positive integers, and the restriction of the function on B is an injective function from B into a section of the positive integers. Contradiction.

3.

Let X be the two-element set $\{0,1\}$. Find a bijective correspondence between X^ω and a proper subset of itself.

$f(x_1, x_2, \dots) = (0, x_1, x_2, \dots)$ is a bijective correspondence between the set of all $\{0,1\}$ -sequences and those starting with 0 .

4.

Let A be a nonempty finite simply ordered set.

(a) Show that A has a largest element. [*Hint:* Proceed by induction on the cardinality of A .]

(b) Show that A has the order type of a section of the positive integers.

(a) By induction. If there is only one element in A then it is the largest. Suppose there is a largest element for any finite set of cardinality $n-1$. If A has n elements, and $x \in A$, then $A - \{x\}$ has the largest element y (by induction), and y is the largest element of A if $x < y$, otherwise x is the largest element of A .

(b) The bijection is constructed by induction: if A has n elements and for all ordered finite sets of cardinality $n-1$ the fact is proved, we simply take b , the largest element of A , and extend the order preserving bijection f of $A - \{b\}$ with $\{1, \dots, n-1\}$ (the existence of which is assumed by the induction hypothesis) by letting $f(b) = n$.

A more interesting approach is to define f without induction: $f(a) =$ the cardinality of $S_a = \{x \in A | x \le a\}$. S_a is a non-empty subset of A ($a \le a$), so, it has cardinality form 1 to n (Corollary 6.6). Further, if $a < b$, then $x \le a$ implies $x \le b$, and $b \nleq a$, i.e. $S_a \subsetneq S_b$, and $f(a) < f(b)$ (Corollary 6.6). Overall, we have an injective function f from A to S_{n+1} , but we also have a bijective function g from A to S_{n+1} (A has cardinality n), so that f must be bijective ($f \circ g^{-1}$ is a bijective correspondence of S_{n+1} with the image set of f).

> See Theorem 10.1 (page 64), which has a solution for both 4 (a) and (b).

5.

If $A \times B$ is finite, does it follow that A and B are finite?

If it was given that both sets A and B are nonempty, then the answer would be yes. Indeed, if we assume that $A \times B$ is finite, then there is an injective function f from $A \times B$ to S_n for some $n \in \mathbb{Z}_+$ (Corollary 6.7). And if B is nonempty, then for a fixed $b \in B$, the restriction of f on $A \times \{b\}$ is an injective function from $A \times \{b\}$ to S_n , but then there is an obvious bijective correspondence of A and $A \times \{b\}$, the composite of which with f proves A to be finite (Corollary 6.7). Similarly, if A is nonempty, then B is finite. But if sets can be empty, then, as it was noted by Fran in the comments below, their product may be empty (finite) while one set is empty and the other is infinite: $\mathbb{R} \times \emptyset = \emptyset$.

6.

(a) Let $A = \{1, \ldots, n\}$. Show there is a bijection of $\mathcal{P}(A)$ with the cartesian product X^n , where X is the two-element set $X = \{0, 1\}$.

(b) Show that if A is finite, then $\mathcal{P}(A)$ is finite.

(a) Let $f(S) = (i_1, \ldots, i_n)$ where $i_j = 1$ iff $j \in S$. In other words, the sequence of 0 and 1 tells which numbers are in the subset and which are not. f is clearly injective and surjective.

(b) Let $g : A \to \{1, \ldots, n\}$ be bijective. For $S \subset A$, let $h(S) = (i_1, \ldots, i_n)$ where $i_j = 1$ iff $g^{-1}(j) \in S$ (similar to (a)). Then, h is a bijective correspondence between $\mathcal{P}(A)$ and X^n , which, according to Corollary 6.8, is finite. Hence, there is a bijective correspondence l of X^n with a finite section of the positive numbers, and $l \circ h$ is a bijective correspondence of $\mathcal{P}(A)$ with the same section of the positive numbers.

7.

If A and B are finite, show that the set of all functions $f : A \to B$ is finite.

Since A is finite, there is a bijective function $g : A \to \{1, \ldots, n\}$. There is also a bijective correspondence h between the set of all functions $\{f\}$ and B^n , namely, $h(f) = (f(g^{-1}(1)), \ldots, f(g^{-1}(n)))$ (basically, we use g to order the elements of A , $a_i = g^{-1}(i)$, and then h lists the images of $a_1, \ldots, a_n$). We can now use Corollary 6.8, to argue that, since B is finite, B^n is finite, and so is the set of all functions $\{f\}$ (using the composite of h and a bijective correspondence of B^n with a section of the positive integer numbers).

SECTION SEVEN

1.

Show that $\mathbb{Q}$ is countably infinite.

To show that $\mathbb{Q}$ is countably infinite, we can follow Example 3 on page 48 with the only difference that for $n, m \in \mathbb{Z}_+$, $g(n, 2m) = \frac{m-1}{n}$, $g(n, 2m-1) = -\frac{m}{n}$.

Alternatively, $\mathbb{Q} = \mathbb{Q}_+ \cup \{0\} \cup \mathbb{Q}_-$, where the latter is in an obvious bijective correspondence with the former (so, we can use Theorem 7.5 and Example 3, page 48).

2.

Show that the maps f and g of Examples 1 and 2 are bijections.

Example 1. f is surjective as for every $m \in \mathbb{Z}_+$, either $m = 2k$, $k \geq 1$, and $f(k) = 2k$, or $m = 2k-1$, $k \geq 1$, and $f(-k+1) = 2k-1$, and f is injective, as for every $m, n \in \mathbb{Z}$, $2m \neq -2n+1$, $2m = 2n \Rightarrow m = n$, and $-2m+1 = -2n+1 \Rightarrow m = n$.

Example 2. f is surjective as if $a, b \in \mathbb{Z}_+$ and $a \geq b$ then $f(a-b+1, b) = (a, b)$ where $a-b+1 \in \mathbb{Z}_+$, and f is injective as for every $x, y \in \mathbb{Z}_+$, if $x+y-1 = x'+y'-1$ and $y = y'$ then $x = x'$.

g is injective, as for every $x, y \in \mathbb{Z}_+$ such that $1 \leq y \leq x$, $g(x,1) \leq g(x,y)$ $< g(x,x)+1 = g(x+1,1)$, so that for $x, y, x', y' \in \mathbb{Z}_+$ such that $1 \leq y \leq x$ and $1 \leq y' \leq x'$, $g(x,y) = g(x',y') \Rightarrow (x,y) = (x',y')$, and g is surjective as for every $n \in \mathbb{Z}_+$, we can let $x = \sup\{k \in \mathbb{Z}_+ | g(k,1) \leq n\}$ (note that $g(1,1) = 1 \leq n < g(n+1,1)$, hence, the supremum exists and $x \geq 1$) and $y = n - \frac{(x-1)x}{2}$ (note that $y \in \mathbb{Z}$, and, by definition, $y = n - g(x,1) + 1 \geq 1$ and $y = n - g(x+1,1) + x + 1 < x + 1$), so that $g(x,y) = n$.

3.

Let X be the two-element set $\{0,1\}$. Show there is a bijective correspondence between the set $\mathcal{P}(\mathbb{Z}_+)$ and the cartesian product X^ω.

Similar to Exercise 6(a) of §6, i.e., given a subset of positive integers, we construct the sequence of 0' s and 1' s indicating for each positive integer number whether it is in the subset or not. The function is clearly injective and surjective.

4.

(a) A real number x is said to be ***algebraic*** (over the rationals) if it satisfies some polynomial equation of positive degree

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

with rational coefficients a_i . Assuming that each polynomial equation has only finitely many roots, show that the set of algebraic numbers is countable.

(b) A real number is said to be ***transcendental*** if it is not algebraic. Assuming the reals are uncountable, show that the transcendental numbers are uncountable. (It is a somewhat surprising fact that only two transcendental numbers are familiar to us: e and π . Even proving these two numbers transcendental is highly nontrivial.)

(a) Let x be an algebraic number of degree n if it is a root of a polynomial of degree n with rational coefficients. Then, the set of all algebraic numbers is the countable union of the sets of algebraic numbers of a finite degree, and if we show that the latter sets are all countable, we are done. Now let us map the set of all algebraic numbers of degree n to the set $\mathbb{Z}_+ \times \mathbb{Q}^n$ by $f(x) = (k, a_0, \ldots, a_{n-1})$, where x is the k th root of the polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ (we pick any such polynomial for x , and we know that for each such polynomial there are only finite number of roots, so we order different roots of the polynomial, and determine k for x). f is clearly injective, and since $\mathbb{Z}_+ \times \mathbb{Q}^n$ is countable, we have a composite of two injections being an injective correspondence from the set of all algebraic numbers of degree n to $\mathbb{Z}_+$. Note, that, in fact, the set of all algebraic numbers is countably infinite, as it contains $\mathbb{Q}$, being algebraic numbers of degree 1 .

> Of course, we could have avoided considering each set of algebraic numbers of a particular degree by constructing f the same way for the whole set of algebraic numbers, but then, as the range of f we would have the set of all infinite sequences of rational numbers that are eventually zero (such sequences have all zeros starting from some coordinate), which is also countable, but this fact has not been proved yet, so we would have to prove it anyway (see also Exercise 5).

(b) If it were countable, then the set of the real numbers would be countable as the union of the countable sets of algebraic and transcendental numbers.

5.

Determine, for each of the following sets, whether or not it is countable. Justify your answers.

(a) The set A of all functions $f : \{0, 1\} \to \mathbb{Z}_+$.

(b) The set B_n of all functions $f : \{1, \ldots, n\} \to \mathbb{Z}_+$.

(c) The set $C = \cup_{n \in \mathbb{Z}_+} B_n$.

(d) The set D of all functions $f : \mathbb{Z}_+ \to \mathbb{Z}_+$.

(e) The set E of all functions $f : \mathbb{Z}_+ \to \{0, 1\}$.

(f) The set F of all functions $f : \mathbb{Z}_+ \to \{0, 1\}$ that are "eventually zero." [We say that f is ***eventually zero*** if there is a positive integer N such that $f(n) = 0$ for all $n > N$.]

(g) The set G of all functions $f : \mathbb{Z}_+ \to \mathbb{Z}_+$ that are eventually 1 .

(h) The set H of all functions $f : \mathbb{Z}_+ \to \mathbb{Z}_+$ that are eventually constant.

(i) The set I of all two-element subsets of $\mathbb{Z}_+$.

(j) The set J of all finite subsets of $\mathbb{Z}_+$.

(a) (b) (c) (d) (e) As a general result, the set of all functions from a set A of cardinality α (α is either a positive integer if A is finite or ω if A is countably infinite) to a set B is in a bijective correspondence with B^α (there is a bijection between them, see Exercise 7 of §6). Hence, we get countably infinite sets in (a), (b) and (c) (using Corollary 7.4, Theorem 7.5 and Theorem 7.6), and uncountable sets in (d) and (e) (using Theorem 7.7).

(f) (g) To continue the general result stated above, the set F of all functions from $\mathbb{Z}_+$ to a set B that are eventually a given fixed element $b \in B$ is in a bijective correspondence with the countable union over $n \in \mathbb{Z}_+$ of the sets F_n all functions from S_n to B s.t. $f(n) \neq b$ (where $F_1 = \{\emptyset\}$). Indeed, having a sequence $(b_1, \ldots, b_m, b, b, \ldots)$ where $b_m \neq b$, we map it to the function $f : S_{m+1} \to B$ such that $f(i) = b_i$, and, hence, $f(m) \neq b$. It is clear that the mapping is injective and surjective. Now, F_1 is a singleton, $F_2 : \{1\} \to B - \{b\}$ is in a bijective correspondence with $B - \{b\}$, and for $n \geq 3$, each F_n is clearly in a bijective correspondence with $B^{n-2} \times (B - \{b\})$. So, if B is countable, so is each F_n for $n \geq 2$, and their countable union together with F_1 is countably infinite. And this is what we get in both (f) and (g).

(h) We further continue our result, the set of all functions from $\mathbb{Z}_+$ to a set B that are eventually constant is simply the union over $b \in B$ of the sets of all functions from $\mathbb{Z}_+$ to B that are eventually b . Hence, if B is countable, we have the countable union of countably infinite sets (according to (f) and (g)), which is countably infinite.

(i) Let $f : I \to A$ be such that $f(\{a, b\}) = g \in A$ where $g(0) = \min\{a, b\}$ and $g(1) = \max\{a, b\}$. f is clearly injective, and A , according to (a), is countably infinite. So is I (it is infinite as it contains, for example, all two-element sets of the form $\{n, n+1\}$ for $n \in \mathbb{Z}_+$).

(j) Similar to (i), if J_n is the set of all n -element subsets of $\mathbb{Z}_+$, then J_0 contains one subset only, and for $n \geq 1$, there is an injective correspondence $f_n : J_n \to B_n$ such that $f_n(\{a_1, \ldots a_n\}) = g \in B_n$ where $g(1) < g(2) < \ldots < g(n)$ and $g(\{1, \ldots, n\}) = \{a_1, \ldots, a_n\}$. Since, according to (b), for all $n \in \mathbb{Z}_+$, B_n is countably infinite, so is J (including J_0).

6.

We say that two sets A and B ***have the same cardinality*** if there is a bijection of A with B. ™

(a) Show that if $B \subset A$ and if there is an injection

$$f : A \to B,$$

then A and B have the same cardinality. [*Hint:* Define $A_1 = A$, $B_1 = B$, and for $n > 1$, $A_n = f(A_{n-1})$ and $B_n = f(B_{n-1})$. (Recursive definition again!) Note that $A_1 \supset B_1 \supset A_2 \supset B_2 \supset A_3 \supset \cdots$. Define a bijection $h : A \to B$ by the rule

$$h(x) = \begin{cases} f(x) & \text{if } x \in A_n - B_n \text{ for some } n, \\ x & \text{otherwise.} \end{cases}]$$

(b) *Theorem (Schroeder-Bernstein theorem). If there are injections $f : A \to C$ and $g : C \to A$, then A and C have the same cardinality.*

(a) The hint is actually almost the proof.

1. $B_1 = B \subset A = A_1$. Hence, $A_2 = f(A_1) \subset B = B_1$ and $B_2 = f(B_1) \subset f(A_1) = A_2$. Further, for $n \geq 2$, if $B_n = f(B_{n-1}) \subset A_n = f(A_{n-1}) \subset B_{n-1}$, then $B_{n+1} = f(B_n) \subset f(A_n) = A_{n+1}$ and $A_{n+1} = f(A_n) \subset f(B_{n-1}) = B_n$. So, by induction, we get the sequence of subsets.
2. We show that h is well-defined. For all $x \in A$, $h(x) \in B$, as if $x \in A - B = A_1 - B_1$ then $h(x) = f(x) \in B$, otherwise $x \in B$, and $h(x) = x$ or $h(x) = f(x)$, in either case $h(x) \in B$.
3. We show that h is bijective. Let $C_n = A_n - B_n$ and $X = A - \cup_{n \in \mathbb{Z}_+} C_n$. Then all C_n ' s and X are pairwise disjoint (for $m > n$, $C_m \subset A_m \subset B_n$ and $B_n \cap C_n = \emptyset$). The restriction of h on C_n is a bijection $h_n : C_n \to C_{n+1}$ because $f|A_n : A_n \to A_{n+1}$ and $f|B_n : B_n \to B_{n+1}$ are bijections. The restriction of h on X is the identity function. Since the image sets of all functions h_n and $h|_X$ are pairwise disjoint, and $h(A) = X \cup \cup_{n \in \mathbb{Z}_+} C_{n+1} = A - C_1 = B$, we conclude that h is injective and surjective, i.e. bijective.

(b) $h : C \to f(A) \subset C$ defined by $h(c) = (f \circ g)(c) \in f(A)$ is an injection, therefore, by (a), C has the same cardinality as $f(A)$, and there is a bijection $m : f(A) \to C$. Also, $l : A \to f(A)$ defined by $l(a) = f(a)$ is a bijection. Overall, the composite of l and m is a bijection of A with C, so that C and A have the same cardinality.

7.

Show that the sets D and E of Exercise 5 have the same cardinality.

The two uncountable sets. What is the purpose of this exercise? In Exercise 5 we concluded that all sets except D and E are countably infinite, hence, they all have the same cardinality. However, we also showed that D and E are uncountable, which, by itself, does not imply they have the same cardinality. So, here we show that, in fact, they do.

There is an obvious injection from E to D (each function into $\{0, 1\}$ can be considered as a function into $\mathbb{Z}_+$). To construct the opposite injection note that each function in D can be considered as an infinite countable sequence of positive integers, while a function in E can be considered as an infinite countable sequence on 0 ' s and 1 ' s. For each sequence $(n_1, n_2, \ldots)$ of positive integers in D we assign the sequence of 0 ' s and 1 ' s such that first there are $f(1)$ 0' s then 1 then $f(2)$ 0' s then 1 etc.: $(\underbrace{0, \ldots, 0}_{n_1}, 1, \underbrace{0, \ldots, 0}_{n_2}, 1, \ldots)$. Having the two injections, according to Exercise 6(b), we conclude that the sets D and E have the same cardinality.

8.

> Let X denote the two-element set $\{0,1\}$; let $\mathcal{B}$ be the set of *countable* subsets of X^ω . Show that X^ω and $\mathcal{B}$ have the same cardinality.

Every countable subset $B \subset X^\omega$ (i.e., every $B \in \mathcal{B}$) can be represented (not uniquely, but injectively) as a countable sequence $B = (b_1, b_2, \dots)$ of its elements, i.e. as a countable sequence of countably infinite sequences of $0'$ s and $1'$ s: $b_i = (0,0,1,0,1,\dots)$. Hence, B can be represented (not uniquely, but injectively) as a countable table (with a countable number of columns equal to the number of elements in B , and countably infinite number of rows) by putting each b_i as column i of the table. If there are finite number of columns in the resulting table (a finite number of elements in B) then we add countably infinite number of columns having the same sequence b that does not belong to B . This way, as it is easy to see, we have constructed a unique countably infinite table for each countable set $B \subset X^\omega$ (unique, because we can easily reconstruct set B given its table).

More formally, given a countable $B \subset X^\omega$, we would represent it as a sequence of its elements $(b_1, b_2, \dots)$, and map it to $x \in (X^\omega)^\omega$ such that, if i is no greater than the number of elements in B , then $(x_i)_j = (b_i)_j$, otherwise, when there are n elements in B and $i > n$, for $j \le n$, $(x_i)_j = 1 - (b_j)_j$, and for $j > n$, $(x_i)_j = 0$. Note that for $i > n \ge j$, $x_i \ne x_j$. It is easy to see that the mapping is injective.

In its turn, every countably infinite table can be injectively associated with a countable sequence of $0'$ s and $1'$ s. We can use a bijection $h : \mathbb{Z}_+ \to \mathbb{Z}_+ \times \mathbb{Z}_+$ to define the i th element of the sequence as the element of the table having coordinates $h(i)$. Then, different tables will map to different sequences.

Note again, that different countable sets B cannot be mapped to the same table, and different tables cannot correspond to the same final sequence of $0'$ s and $1'$ s. So, we have an injection one way.

Here is an example. Let B be the set of all sequences $b_i = (\underbrace{1,\dots,1}_{i},0,0,\dots)$. Since B is countable, it can be represented as a sequence of its elements (for example, $(b_1, b_2, \dots)$). This representation is not unique, but different B' s cannot have the same representation. Then, the infinite table (matrix) and the injection from the table to a sequence of $0'$ s and $1'$ s can be constructed, for example, as shown in Figure 1↓.

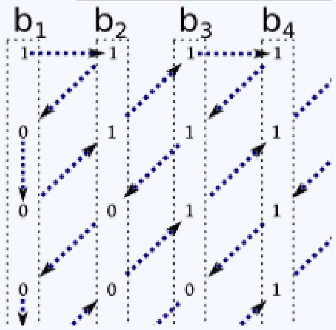

Figure 1 Mapping of B to a sequence of 0 ' s and 1 ' s.

Vice versa, every sequence in X^ω corresponds to a subset containing this one sequence only (singleton).

Having the two injections, we conclude, according to Exercise 6(b), that the two uncountable sets have the same cardinality.

9.

This exercise shows that one has to be careful in defining recursive functions, as an arbitrary recursive relation may "define" several functions or a function that does not exist.

(a) The formula

$$(*) \qquad \begin{aligned} h(1) &= 1, \\ h(2) &= 2, \\ h(n) &= [h(n+1)]^2 - [h(n-1)]^2 \qquad \text{for } n \geq 2 \end{aligned}$$

is not one to which the principle of recursive definition applies. Show that nevertheless there does exist a function $h : \mathbb{Z}_+ \to \mathbb{R}$ satisfying this formula. [*Hint:* Reformulate $(*)$ so that the principle will apply and require h to be positive.]

(b) Show that the formula $(*)$ of part (a) does not determine h uniquely. [*Hint:* If h is a positive function satisfying $(*)$, let $f(i) = h(i)$ for $i \neq 3$, and let $f(3) = -h(3)$.]

(c) Show that there is no function $h : \mathbb{Z}_+ \to \mathbb{R}$ satisfying the formula

$$\begin{aligned} h(1) &= 1, \\ h(2) &= 2, \\ h(n) &= [h(n+1)]^2 + [h(n-1)]^2 \qquad \text{for } n \geq 2. \end{aligned}$$

(a) The last expression can be rewritten as $[h(n+1)]^2 = h(n) + [h(n-1)]^2$. By taking the positive root we ensure that h takes positive values only, and, hence, always exists (as the sum of the two terms on the right will be always positive). In other words, we rewrite the last expression as $h(n) = \sqrt{h(n-1) + [h(n-2)]^2}$ for $n \geq 3$. Now, the recursive formula is well-defined, and the principle of recursive definition applies to it.

(b) Let h and f be two functions both satisfying the recursive relation described by $(*)$ such that $h(1) = f(1) = 1$, $h(2) = f(2) = 2$, $h(3) = \sqrt{3}$, $f(3) = -\sqrt{3}$, and for $n \geq 4$, $\frac{h}{f}(n) = \sqrt{\frac{h}{f}(n-1) + \left[\frac{h}{f}(n-2)\right]^2}$ (I am not sure why Munkres says $f(i) = h(i)$ for $i \neq 3$).

(c) $h^2(3) = h(2) - [h(1)]^2 = 1$, $h^2(4) = h(3) - [h(2)]^2 \leq 1 - 4 < 0$.

SECTIONG EIGHT

1.

Let $(b_1, b_2, \ldots)$ be an infinite sequence of real numbers. The sum $\sum_{k=1}^{n} b_k$ is defined by induction as follows:

$$\sum_{k=1}^{n} b_k = b_1 \qquad \text{for } n = 1,$$
$$\sum_{k=1}^{n} b_k = (\sum_{k=1}^{n-1} b_k) + b_n \qquad \text{for } n > 1.$$

Let A be the set of real numbers; choose ρ so that Theorem 8.4 applies to define this sum rigorously. We sometimes denote the sum $\sum_{k=1}^{n} b_k$ by the symbol $b_1 + b_2 + \cdots + b_n$.

Let $a_0 = b_1$ and $\rho(f : \{1, \ldots, n\} \to \mathbb{R}) = f(n) + b_{n+1}$, then $\sum_{k=1}^{1} b_k \stackrel{def}{=} h(1) = b_1$, and $\sum_{k=1}^{n} b_k \stackrel{def}{=} h(n) = \rho(h|\{1, \ldots, n-1\}) = h(n-1) + b_n \stackrel{def}{=} (\sum_{k=1}^{n-1} b_k) + b_n$.

2.

Let $(b_1, b_2, \ldots)$ be an infinite sequence of real numbers. We define the product $\prod_{k=1}^{n} b_k$ by the equations

$$\prod_{k=1}^{1} b_k = b_1,$$
$$\prod_{k=1}^{n} b_k = (\prod_{k=1}^{n-1} b_k) \cdot b_n \qquad \text{for } n > 1.$$

Use Theorem 8.4 to define this product rigorously. We sometimes denote the product $\prod_{k=1}^{n} b_k$ by the symbol $b_1 b_2 \cdots b_n$.

Let $a_0 = b_1$ and $\rho(f : \{1, \ldots, n\} \to \mathbb{R}) = f(n) \cdot b_{n+1}$, then $\prod_{k=1}^{1} b_k \stackrel{def}{=} h(1) = b_1$, and $\prod_{k=1}^{n} b_k \stackrel{def}{=} h(n) = \rho(h|\{1, \ldots, n-1\}) = h(n-1) \cdot b_n \stackrel{def}{=} (\prod_{k=1}^{n-1} b_k) \cdot b_n$.

3.

Obtain the definitions of a^n and $n!$ for $n \in \mathbb{Z}_+$ as special cases of Exercise 2.

Those are the cases of Exercise 2, when for $n \in \mathbb{Z}_+$, $b_n = a$ and $b_n = n$, respectively.

4.

The *Fibonacci numbers* of number theory are defined recursively by the formula

$$\lambda_1 = \lambda_2 = 1,$$
$$\lambda_n = \lambda_{n-1} + \lambda_{n-2} \qquad \text{for } n > 2.$$

Define them rigorously by use of Theorem 8.4.

Let $a_0 = 1$, $\rho(f : \{1\} \to \mathbb{Z}_+) = 1$ and for $n > 1$, $\rho(f : \{1, \ldots, n\} \to \mathbb{Z}_+) = f(n-1) + f(n)$, then $\lambda_1 \stackrel{def}{=} h(1) = 1$, $\lambda_2 \stackrel{def}{=} h(2) = \rho(h|\{1\}) = 1$, and for $n > 2$, $\lambda_n \stackrel{def}{=} h(n) = \rho(h|\{1, \ldots, n-1\}) = h(n-2) + h(n-1) \stackrel{def}{=} \lambda_{n-2} + \lambda_{n-1}$.

5.

Show that there is a unique function $h : \mathbb{Z}_+ \to \mathbb{R}_+$ satisfying the formula

$$h(1) = 3,$$
$$h(i) = [h(i-1) + 1]^{1/2} \qquad \text{for } i > 1.$$

Let $a_0 = 3$, and $\rho(f : \{1, \ldots, n\} \to \mathbb{R}_+) = \sqrt{f(n) + 1}$. ρ is well-defined, as $f(n) + 1 > 0$. Then, according to Theorem 8.4, there is a unique h satisfying the equations above.

6.

(a) Show that there is no function $h : \mathbb{Z}_+ \to \mathbb{R}_+$ satisfying the formula

$$h(1) = 3,$$
$$h(i) = [h(i-1) - 1]^{1/2} \qquad \text{for } i > 1.$$

Explain why this example does not violate the principle of recursive definition.

(b) Consider the recursion formula

$$h(1) = 3,$$
$$h(i) = \begin{Bmatrix} [h(i-1) - 1]^{1/2} & \text{if } h(i-1) > 1 \\ 5 & \text{if } h(i-1) \le 1 \end{Bmatrix} \qquad \text{for } i > 1.$$

Show that there exists a unique function $h : \mathbb{Z}_+ \to \mathbb{R}_+$ satisfying this formula.

(a) $h(2) = \sqrt{2} < 2$, $h(3) < \sqrt{2 - 1} = 1$, so that $h(3) - 1 < 0$, and $h(4)$ is not well defined. It does not violate the principle, because there is no well defined ρ function. If we try to define ρ similar to Exercise 5, i.e. $\rho(f : \{1, \ldots, n\} \to \mathbb{R}_+) = \sqrt{f(n) - 1}$, then the definition does not work for f such that $f(n) < 1$.

(b) Here there is a well-defined ρ , namely, $\rho(f : \{1, \ldots, n\} \to \mathbb{R}_+) = \begin{cases} \sqrt{f(n) - 1} & \text{if } f(n) > 1 \\ 5 & \text{if } f(n) \le 1 \end{cases}$, which together with $a_0 = 3$ allows us to apply Theorem 8.4.

7.

Prove Theorem 8.4.

First, similar to Lemma 8.1, by induction, we prove that for $n \in \mathbb{Z}_+$ there exists a function $h_n : \{1, \ldots, n\} \to A$ satisfying the equations $(*)$ of Theorem 8.4 for all i in its domain. Namely, this is true for $n = 1$, $h_1(1) = a_0$, and, given this is true for n , i.e. there is h_n , we define $h_{n+1}(i) = h_n(i)$ for $i \le n$, and $h_{n+1}(n+1) = \rho(h_n)$. Note, that $h_{n+1}(1) = h_n(1) = \cdots = h_1(1) = a_0$, and $h_n = h_{n+1}|\{1, \ldots, n\}$, hence, the equations $(*)$ hold for h_{n+1} .

Then, similar to Lemma 8.2, we prove that for every $m \le n$, and g_m and h_n satisfying $(*)$ on their domains, respectively, $h_n|\{1, \ldots, m\} = g_m$. Again, we argue that $g_m(1) = h_n(1)$, and for every $1 \le k < m$, $h_n|\{1, \ldots, k\} = g_m|\{1, \ldots, k\}$ implies $h_n|\{1, \ldots, k+1\} = g_m|\{1, \ldots, k+1\}$ as both satisfy $(*)$.

Finally, as in Theorem 8.3, we construct h for all positive integers by taking the union of the rules of all h_n ' s. The argument is, in fact, almost identical to the proof of Theorem 8.3, as the latter mostly operates in general terms without even using the particular definition of ρ it is proved for.

8.

Verify the following version of the principle of recursive definition: Let A be a set. Let ρ be a function assigning, to every function f mapping a section S_n of $\mathbb{Z}_+$ into A, an element $\rho(f)$ of A. Then there is a unique function $h : \mathbb{Z}_+ \to A$ such that $h(n) = \rho(h|S_n)$ for each $n \in \mathbb{Z}_+$.

The difference between the two definitions is that the former (in the text) requires $\rho(f)$ to be defined for any function f that maps a *nonempty* section of the positive integers to A and also requires $h(1) = a_0$, while the latter (in the exercise) requires $\rho(f)$ to be additionally specified for the (unique) function f_0 that maps the empty section $S_1 = \emptyset$ to A and also requires the initial value $h(1)$ to be equal to $\rho(h|S_1) = \rho(f_0)$. As it is easy to see, if, given either a_0 or $\rho(f_0)$, we define the other one by $\rho(f_0) = a_0$, then both definitions become equivalent.

SECTION NINE

1.

Define an injective map $f : \mathbb{Z}_+ \to X^\omega$ without using the choice axiom.

For $n \in \mathbb{Z}_+$, $f(n) = (\underbrace{1, \dots, 1}_{n}, 0, 0, \dots)$.

2.

Find if possible a choice function for each of the following collections, without using the choice axiom:

(a) The collection $\mathcal{A}$ of nonempty subsets of $\mathbb{Z}_+$.

(b) The collection $\mathcal{B}$ of nonempty subsets of $\mathbb{Z}$.

(c) The collection $\mathcal{C}$ of nonempty subsets of the rational numbers $\mathbb{Q}$.

(d) The collection $\mathcal{D}$ of nonempty subsets of X^ω , where $X = \{0, 1\}$.

(a) Take the lowest element of each subset.

(b) For a subset, take its lowest positive element if there is at least one, otherwise take its largest element (in this latter case the set is bounded from above by 0).

(c) First, for every $q \in \mathbb{Q}$, we consider its *unique* representation as a pair of integer numbers (m_q, n_q) such that $\frac{m_q}{n_q} = q$ is irreducible and n_q is positive. The fact that it is possible and the pair is uniquely determined should not depend on the axiom of choice. Then, for every nonempty set A of rational numbers, we consider the set of denominators $N = \{n_q | q \in A\} \subset \mathbb{Z}_+$, use the choice function defined in (a) to pick one of its elements, i.e. we find the lowest denominator $n = \inf N$, then, we construct the set $B = \{q \in A | n_q = n\} \subset A$ corresponding to the lowest denominator n , consider the set of numerators $M = \{m_q | q \in B\} \subset \mathbb{Z}$, and use the choice function defined in (b) to choose one of its elements, which we call m . Then, $m \in M$ implies $m = m_q$ for some $q \in B \subset A$, for which $n_q = n$, and $\frac{m}{n} = \frac{m_q}{n_q} = q \in A$. q is the chosen element.

(d) A nonempty subset of X^ω is a (possibly, *uncountable*) set of infinite sequences of 0 and 1 . We need to provide a general rule that would work for any such subset and pick one of its sequences. Think about it. ;) As a hint, each sequence of 0 ′ s and 1 ′ s corresponds to a real number from $[0, 1]$, and each real number from $[0, 1]$ corresponds to one or two (if it is a rational number from $(0, 1)$) sequences of 0 ′ s and 1 ′ s. If we can explicitly construct a choice function in (d), then, based on it, we can explicitly construct a choice function for the collection of all subsets of $[0, 1]$. But then, one can use this choice function to explicitly well-order $[0, 1]$ (see §10), something that is not possible (Feferman?).

3.

Suppose that A is a set and $\{f_n\}_{n \in \mathbb{Z}_+}$ is a given indexed family of injective functions

$$f_n : \{1, \ldots, n\} \to A.$$

Show that A is infinite. Can you define an injective function $f : \mathbb{Z}_+ \to A$ without using the choice axiom?

If it were finite, there would be a bijective function $g : A \to \{1, \ldots, m\}$ for some $m \in \mathbb{Z}_+$, but then $g \circ f_{m+1} : \{1, \ldots, m+1\} \to \{1, \ldots, m\}$ would be injective.

We can define f recursively. Let $a_0 = f_1(1)$, and

$$\begin{aligned}\rho(h : S_{n+1} \to A) = f_{n+1}(\inf\{k \in \mathbb{Z}_+ | k \leq n+1 \\ \& \ f_{n+1}(k) \notin h(\{1, \ldots, n\})\}).\end{aligned}$$

ρ is well-defined as f_{n+1} is injective, so for at least one $1 \leq k \leq n+1$, $f_{n+1}(k) \notin h(\{1, \ldots, n\})$. Further, the function f defined by this recursive relation is such that $f(1) = a_0 = f_1(1)$, and $f(n+1) = \rho(f | \{1, \ldots, n\}) \notin f(\{1, \ldots, n\})$.

4.

There was a theorem in §7 whose proof involved an infinite number of arbitrary choices. Which one was it? Rewrite the proof so as to make explicit the use of the choice axiom. (Several of the earlier exercises have used the choice axiom also.)

Theorem 7.5. We must consider the collection of the sets F_n of all surjective functions from $\mathbb{Z}_+$ onto A_n , and the set F of all surjective functions from $\mathbb{Z}_+$ onto J , and choose one function from each set of the collection.

5.

(a) Use the choice axiom to show that if $f: A \to B$ is surjective, then f has a right inverse $h: B \to A$.

(b) Show that if $f: A \to B$ is injective and A is not empty, then f has a left inverse. Is the axiom of choice needed?

(a) If B is empty, then the statement is vacuously true, otherwise A is not empty (f is surjective). Consider the collection $\mathcal{A}$ of nonempty sets $\{f^{-1}(y)\}_{y \in B}$ (f is surjective), and let c be a choice function for $\mathcal{A}$. For every $y \in B$, let $h(y) = c(f^{-1}(y))$. Then $(f \circ h)(y) = y$ for every $y \in B$.

(b) The axiom of choice is not needed. Let $a_0 \in A$. For $b \in f(A)$, there is unique $a \in A$ such that $b = f(a)$, so let $g(b) = a$. For $b \notin f(A)$, let $g(b) = a_0$. We have $(g \circ f)(a) = a$ for all $a \in A$.

6.

Most of the famous paradoxes of naive set theory are associated in some way or other with the concept of the "set of all sets." None of the rules we have given for forming sets allows us to consider such a set. And for good reason--the concept itself is self-contradictory. For suppose that $\mathcal{A}$ denotes the "set of all sets."

(a) Show that $\mathcal{P}(\mathcal{A}) \subset \mathcal{A}$; derive a contradiction.

(b) (*Russell' s paradox.*) Let $\mathcal{B}$ be the subset of $\mathcal{A}$ consisting of all sets that are not elements of themselves;

$$\mathcal{B} = \{A | A \in \mathcal{A} \text{ and } A \notin A\}.$$

(Of course, there may be *no* set A such that $A \in A$; if such is the case, then $\mathcal{B} = \mathcal{A}$.) Is $\mathcal{B}$ an element of itself or not?

(a) $\mathcal{P}(\mathcal{A})$ is the set of all subsets of $\mathcal{A}$, and every subset is a set itself and is in the "set of all sets", hence, $\mathcal{P}(\mathcal{A}) \subset \mathcal{A}$. Therefore, there is a surjection f from $\mathcal{A}$ onto $\mathcal{P}(\mathcal{A})$, contradicting Theorem 7.8. Namely, let $\mathcal{B} = \{B \in \mathcal{A} | B \notin f(B)\}$. We have $\mathcal{B} \in \mathcal{P}(\mathcal{A})$, but for every $B \in \mathcal{A}$: $B \in f(B)$ iff $B \notin \mathcal{B}$, implying $f(B) \neq \mathcal{B}$. Therefore, f is not surjective. The second part of the proof is based on the Cantor's theorem.

(b) Neither. In other words, for every $B \in \mathcal{A}$, $B \in \mathcal{B}$ iff $B \notin B$, implying $B \neq \mathcal{B}$. In particular, $\mathcal{B} \neq \mathcal{B}$.

7.

Let A and B be two nonempty sets. If there is an injection of B into A, but no injection of A into B, we say that A has ***greater cardinality*** than B.

(a) Conclude from Theorem 9.1 that every uncountable set has greater cardinality than $\mathbb{Z}_+$.

(b) Show that if A has greater cardinality than B, and B has greater cardinality than C, then A has greater cardinality than C.

(c) Find a sequence $A_1, A_2, \dots$ of infinite sets, such that for each $n \in \mathbb{Z}_+$, the set A_{n+1} has greater cardinality than A_n.

(d) Find a set that for every n has cardinality greater than A_n.

(a) An uncountable set is infinite (injection one way by Theorem 9.1; remember how the injection was constructed "by induction" in the proof of the theorem and then the role of the Axiom of Choice was discussed after the proof?), but not countably infinite (no injection the other way by Theorem 7.1).

(b) There are injections $C \to B \to A$, therefore, there is an injection $C \to A$. If there were an injection $A \to C$ then there would be an injection $B \to A \to C$.

(c) $A_{n+1} = \mathcal{P}(A_n)$, A_1 is arbitrary.

(d) $\mathcal{P}(\cup_i A_i)$.

8.

* Show that $\mathcal{P}(\mathbb{Z}_+)$ and $\mathbb{R}$ have the same cardinality. [*Hint:* You may use the fact that every real number has a decimal expansion, which is unique if expansions that end in an infinite string of 9 ' s are forbidden.]

A famous conjecture of set theory, called the *continuum hypothesis*, asserts that there exists no set having greater cardinality than $\mathbb{Z}_+$ and lesser cardinality than $\mathbb{R}$. The *generalized continuum hypothesis* asserts that, given the infinite set A, there is no set having greater cardinality than A and lesser cardinality than $\mathcal{P}(A)$. Surprisingly enough, both of these assertions have been shown to be independent of the usual axioms for set theory. For a readable expository account, see [Sm].

Two sets have the same cardinality if there is a bijection between them (Exercise 6 of §7). Further, the same exercise shows that if for two sets there are injections from each one into the other, then the sets have the same cardinality. We are going to use this fact. We show that there are injections $\mathbb{R} \leftrightarrow [0,1) \leftrightarrow \mathcal{P}(\mathbb{Z}_+)$.

There is a bijective function h from $\mathcal{P}(\mathbb{Z}_+)$ onto $\{0,1\}^\omega$ given by $f(S)_i = 1$ iff $i \in S$ for every $S \subset \mathbb{Z}_+$. Now we use the following fact (which is slightly different from the one in the exercise as it uses a binary not decimal expansion): every real number $x \in [0,1)$ has a unique binary expansion such that it does not end in an infinite sequence of 1 ' s, moreover, different x ' s correspond to different expansions. We call this injective expansion as $f : [0,1) \to \{0,1\}^\omega$. Now, using this fact, it is immediate that $h^{-1} \circ f$ is an injection from $[0,1)$ into $\mathcal{P}(\mathbb{Z}_+)$. Further, if we take any sequence $s = (s_1, s_2, \dots)$ of 0 ' s and 1 ' s, and construct a new sequence $s' = (0, s_1, 0, s_2, \dots)$, then there is a unique real number $x \in [0,1)$ corresponding to the constructed sequence, and different sequences correspond to different numbers. Hence, there is an injection g from $\{0,1\}^\omega$ into $[0,1)$, and $g \circ h$ is an injection from $\mathcal{P}(\mathbb{Z}_+)$ into $[0,1)$.

It remains to show that there are injections from $\mathbb{R}$ into $[0,1)$ and vice versa. One way, take $f(x) = 1/(1+e^x)$, and the other way $[0,1) \subset \mathbb{R}$.

SECTION TEN

1.

Show that every well-ordered set has the least upper bound property.

If for a nonempty subset of a well-ordered set the set of its upper bounds is nonempty, then it has the smallest element, which must be the least upper bound of the subset.

2.

(a) Show that in a well-ordered set, every element except the largest (if one exists) has an immediate successor.

(b) Find a set in which every element has an immediate successor that is not well-ordered.

(a) If an element α of the set is not the largest, then $\{x|\alpha < x\}$ is not empty and has the least element m , which is the successor of α as $\alpha < m$ and there is no x such that $\alpha < x < m$.

(b) $\mathbb{Z}$.

3.

Both $\{1,2\} \times \mathbb{Z}_+$ and $\mathbb{Z}_+ \times \{1,2\}$ are well-ordered in the dictionary order. Do they have the same order type?

No, the first set has an element $(2,1)$ which is not the smallest element of the set but has no immediate predecessor, while the second set does not have such an element (therefore, there is no order preserving bijection, as if there is, say f , then $f(2,1)$ cannot be the smallest element, hence, it must have a predecessor p , but then $f^{-1}(p) < (2,1)$, that is $f^{-1}(p) = (1,x)$, and $p < f(1,x+1) < f(2,1)$).

4.

(a) Let $\mathbb{Z}_-$ denote the set of negative integers in the usual order. Show that a simply ordered set A fails to be well-ordered if and only if it contains a subset having the same order type as $\mathbb{Z}_-$.

(b) Show that if A is simply ordered and every countable subset of A is well-ordered, then A is well-ordered.

(a) If $B \subset A$ has the order type of $\mathbb{Z}_-$, then B has no smallest element (as there is a bijection into $\mathbb{Z}_-$ preserving the order). If A is not-well ordered then there exists a nonempty $B \subset A$ that has no smallest element. Let $b_1 \in B$. For $n \in \mathbb{Z}_+$, there is $b_{n+1} \in B$ less than b_n . By induction, there is a sequence $(b_1, b_2, \dots) \in B^\omega$ such that $b_1 > b_2 > \cdots$, and the subset $\{b_1, b_2, \dots\} \subset B \subset A$ has the same order type as $\mathbb{Z}_-$ ($f(b_n) = -n$).

(b) It follows from (a). If A is not well-ordered, then there is a countable subset having the same order type as $\mathbb{Z}_-$, which is not well-ordered.

5.

Show the well-ordering theorem implies the choice axiom.

Given a collection of disjoint sets take their well-ordered union and for each set take its smallest element in the union.

6.

Let S_Ω be the minimal uncountable well-ordered set.

(a) Show that S_Ω has no largest element.

(b) Show that for every $\alpha \in S_\Omega$, the subset $\{x|\alpha < x\}$ is uncountable.

(c) Let X_0 be the subset of S_Ω consisting of all elements x such that x has no immediate predecessor. Show that X_0 is uncountable.

(a) A section by any element must be countable, however, if there were the largest element α, the section $S_\alpha = S_\Omega - \{\alpha\}$ would be uncountable.

(b) $S_\Omega = S_\alpha \cup \{\alpha\} \cup \{x|\alpha < x\}$ is uncountable, therefore, at least one of the sets on the right must be uncountable.

(c) Every countable subset of S_Ω has an upper bound (Theorem 10.3). Suppose X_0 is countable, and α is its upper bound. Using (a) and Exercise 2(a), every $\beta \in S_\Omega$ has an immediate successor, which we call $s(\beta)$. Then, the set $A = \{\alpha, s(\alpha), s^2(\alpha), \ldots\}$ is a countable, hence, bounded from above subset of S_Ω. According to Exercise 1, A has the least upper bound, call it γ. Then, γ has no immediate predecessor. Indeed, suppose δ is an immediate predecessor of γ, but then, $\delta < s^n(\alpha) \le \gamma$ for some $n \in \mathbb{Z}_+ \cup \{0\}$, and $\gamma = s(\delta) < s^{n+1}(\alpha)$. We conclude that $\gamma \in X_0$, and $\gamma \ge s(\alpha) > \alpha \ge \gamma \in X_0$. Contradiction.

In few words, the two facts that (a) every countable subset of S_Ω is bounded from above, and (b) for every element of S_Ω there is a greater element that has no immediate predecessor, imply that X_0 cannot be bounded from above, and, hence, cannot be countable.

7.

Let J be a well-ordered set. A subset J_0 of J is said to be ***inductive*** if for every $\alpha \in J$,

$$(S_\alpha \subset J_0) \Rightarrow \alpha \in J_0.$$

Theorem (The principle of transfinite induction). If J is a well-ordered set and J_0 is an inductive subset of J, then $J_0 = J$.

Let A be a set of all elements not in J_0, and suppose it is not empty. Then it has the smallest element α, and $S_\alpha \subset J_0$ (the section can be empty, it does not matter). Therefore, $\alpha \in J_0$. Contradiction. We conclude that A is empty, and $J_0 = J$.

8.

(a) Let A_1 and A_2 be disjoint sets, well-ordered by $<_1$ and $<_2$, respectively. Define an order relation on $A_1 \cup A_2$ by letting $a < b$ either if $a, b \in A_1$ and $a <_1 b$, or if $a, b \in A_2$ and $a <_2 b$, or if $a \in A_1$ and $b \in A_2$. Show that this is a well-ordering.

(b) Generalize (a) to an arbitrary family of disjoint well-ordered sets, indexed by a well-ordered set.

(a) For a nonempty subset B, if there is $a \in B \cap A_1$ then the smallest element of B is the $<_1$-smallest element of $B \cap A_1$, otherwise $B \subset A_2$, and the smallest element of B is the $<_2$-smallest element of $B \subset A_2$.

(b) Let $\{A_\alpha\}_{\alpha \in J}$ be a family of disjoint well-ordered (by $<_\alpha$, respectively) sets where the index set J is well-ordered by $<_J$. Define an order relation on $A = \cup_{\alpha \in J} A_\alpha$ such that $a < b$ iff either $a \in A_\alpha$, $b \in A_\beta$ and $\alpha <_J \beta$, or $a, b \in A_\alpha$ and $a <_\alpha b$. Then, $<$ is a well-ordering on A. Indeed, for a nonempty set $B \subset A$, the set of indexes $I = \{\alpha | B \cap A_\alpha \neq \emptyset\}$ is not empty, hence, there is the $<_J$-smallest element γ of I. Further, the set $C = B \cap A_\gamma$ is not empty, and, hence, there is the $<_\gamma$-smallest element c of C. For every $b \in B$, $b \in A_\alpha$ for some α, and either $\gamma <_J \alpha$, or $\gamma = \alpha$ and $c \leq_\gamma b$. In either case, we conclude that $c \leq b$, and c is the smallest element of B.

9.

Consider the subset A of $(\mathbb{Z}_+)^\omega$ consisting of all infinite sequences of positive integers $\mathbf{x} = (x_1, x_2, \ldots)$ that end in an infinite string of 1's. Give A the following order: $\mathbf{x} < \mathbf{y}$ if $x_n < y_n$ and $x_i = y_i$ for $i > n$. We call this the "antidictionary order" on A.

(a) Show that for every n, there is a section of A that has the same order type as $(\mathbb{Z}_+)^n$ in the dictionary order.

(b) Show A is well-ordered.

(a) Consider $\mathbf{x}^{(n)} = (\underbrace{1, \ldots, 1}_{n}, 2, 1, 1, \ldots)$, $n \geq 0$. Then, $\mathbf{x} < \mathbf{x}^{(n)}$ iff $1 = x_{n+1} = x_{n+2} = \ldots$.

Therefore, the section $A_n = S_{\mathbf{x}(n)}$ contains exactly those sequences that have arbitrary values of the first n coordinates, and all 1's after that. The order of the elements of the section A_n is the "reverse dictionary". Indeed, the case $n = 0$ is trivial, and for $n \geq 1$, let $f : A_n \to (\mathbb{Z}_+)^n$ be defined by $f(x_1, \ldots, x_n) = (x_n, \ldots, x_1)$. Then, as it is easy to see, f is a bijection preserving the order (in A_n we compare all coordinates one-by-one from right to left, and in the dictionary order we compare from left to right).

(b) For every sequence $\mathbf{x} \neq (1, 1, \ldots)$ define $f(\mathbf{x}) = j \in \mathbb{Z}_+$ such that $1 = x_{j+1} = x_{j+2} = \ldots$ and $x_j \neq 1$. Additionally, define $f((1, 1, \ldots)) = 0$. Note, that $f(\mathbf{x}) < f(\mathbf{y})$ implies $\mathbf{x} < \mathbf{y}$ (but not vice versa). For every nonempty subset B of sequences, consider the set of all $J = \{f(\mathbf{x}) | \mathbf{x} \in B\}$. $J \subset \mathbb{Z}_+$ is nonempty, and, hence, has the smallest element n. Consider the set M of all sequences $\mathbf{x} \in B$ such that $f(\mathbf{x}) = n$. M is a subset of the section A_n defined in (a), which has the same type as the well-ordered set $\mathbb{Z}_+^n$. Hence, there is the smallest element $\mathbf{m} \in M \subset B$. For $\mathbf{x} \in B$, either $f(\mathbf{x}) > n = f(\mathbf{m})$, and, hence, $\mathbf{m} < \mathbf{x}$, or $f(\mathbf{x}) = f(\mathbf{m})$ and $\mathbf{m} \leq \mathbf{x}$.

10.

Theorem. Let J and C be well-ordered sets; assume that there is no surjective function mapping a section of J onto C. Then there exists a unique function $h : J \to C$ satisfying the equation

$$(*) \qquad h(x) = smallest[C - h(S_x)]$$

for each $x \in J$, where S_x is the section of J by x.

Proof.

(a) If h and k map sections of J, or all of J, into C and satisfy $(*)$ for all x in their respective domains, show that $h(x) = k(x)$ for all x in both domains.

(b) If there exists a function $h : S_\alpha \to C$ satisfying $(*)$, show that there exists a function $k : S_\alpha \cup \{\alpha\} \to C$ satisfying $(*)$.

(c) If K $\subset J$ and for all $\alpha \in K$ there exists a function $h_\alpha : S_\alpha \to C$ satisfying $(*)$, show that there exists a function

$$k : \bigcup_{\alpha \in K} S_\alpha \to C$$

satisfying $(*)$.

(d) Show by transfinite induction that for every $\beta \in J$, there exists a function $h_\beta : S_\beta \to C$ satisfying $(*)$. [*Hint:* If β has an immediate predecessor α, then $S_\beta = S_\alpha \cup \{a\}$. If not, S_β is the union of all S_α with $\alpha < \beta$.]

(e) Prove the theorem.

In fact, a more general result is true (Exercise 1 of Supplementary Exercises). Let C be any set (not necessary well-ordered), let $\mathcal{F}$ be the set of all functions mapping a section of J into C, and let $\rho : \mathcal{F} \to C$ be a function that assign to each function from $\mathcal{F}$ an element in C. Then, there exists a unique function $h : J \to C$ such that

$$(*) \qquad h(x) = \rho(h|S_x)$$

for all $x \in J$.

This is a more general result, as in this particular exercise we are asked to prove it for the particular case when $\rho(f : S_x \to C) = smallest[C - f(S_x)]$. This function is well-defined, because (i) we are given that there is no surjection from J onto C, so $C - f(S_x)$ is nonempty, and (ii) in our case C is assumed to be well-ordered, so that for every nonempty subset of C there exists its smallest element.

(a) (*This is an analogue to Lemma 8.2.*) If h and k are defined and equal on a section S_α, and α is in both domains, then $h(\alpha) = k(\alpha)$, because they both satisfy $(*)$. Hence, if h and k are defined on A, which is a section S_β or all of J, then they must be equal on A: consider the set of x ' s for which $h(x) = k(x)$, note that it is inductive (use the fact that every section of A is a section of J) and apply transfinite induction on A. The result follows from the fact that the common domain of h and k must be a section or all of J.

(b) (*This is an analogue to Lemma 8.1.*) Extend h by the formula $(*)$ (in the specific case of ρ given in the exercise, the extension is well-defined because, basically, (i) and (ii) hold; in the more general case, it is well-defined because ρ is assumed to be well-defined).

(c) (*This is an analogue to the second part of the proof of Theorem 8.3.*) This follows from (a). Take any element β in the union of sections, there is a section S_α (may be not unique) that contains the element and the corresponding function h_α. Define $k(\beta) = h_\alpha(\beta)$ (the choice of the section does not matter by (a)), and show that k satisfies $(*)$ (which is almost identical to the last paragraph of the proof of Theorem 8.3).

(d) (*This is again an analogue to Lemma 8.1, but including transfinite induction.*) Consider the set of all those β ' s for which there does not exists the function, then take its smallest element, and use the hint to show that there does exist such function. Or, use the transfinite induction: let J_0 be the set of all those β ' s for which the function exists, then if a section S_α is in the J_0 then $\alpha \in J_0$ (consider the two cases again using the hint). When using the hint, the two cases correspond to (b) and (c) proved earlier.

(e) (*This is an analogue to Theorem 8.3.*) Existence. (d) proves that for every section there is a function satisfying $(*)$. (c) proves that, therefore, there is a function satisfying $(*)$ on the union of all sections of J . The union contains all elements of J except for the largest element m in J , if the one exists (every other element has a larger element in the set; thanks to Fran for the comment). But if there is a largest element m in J , we can extend the function from the union of all sections, which is equal to S_m , to the whole $J = S_m \cup \{m\}$ using (b). The uniqueness follows from (a).

11.

Let A and B be two sets. Using the well-ordering theorem, prove that either they have the same cardinality, or one has cardinality greater than the other. [*Hint:* If there is no surjection $f : A \to B$, apply the preceding exercise.]

If there are injections both ways, then there is a bijection of A with B and the sets have the same cardinality (Schroeder-Bernstein theorem, proved in exercises of Section 7). Otherwise, there can be an injection one way only, and we need to show that there is one. If there is a surjection from A onto B , then there is an injection $B \to A$ (which is a right inverse for the surjection, which exists due to the axiom of choice, which is equivalent to the well-ordering theorem, see Exercise 5(a) of §9). If there is no surjection $A \to B$, then we can well-order both sets and use Exercise 10 to show that there is an injective function from A into B (the fact that it is injective follows immediately from the definition $(*)$).

SECTION ELEVEN

1.

If a and b are real numbers, define $a < b$ if $b - a$ is positive and rational. Show this is a strict partial order on $\mathbb{R}$. What are the maximal simply ordered subsets?

It is nonreflexive ($a - a \not> 0$) and transitive ($b - a, c - b \in \mathbb{Q}_+$ implies $c - a \in \mathbb{Q}_+$). The maximal subsets are $a + \mathbb{Q}$ for $a \in \mathbb{R}$.

2.

(a) Let $\prec$ be a strict partial order on the set A. Define a relation on A by letting $a \preceq b$ if either $a \prec b$ or $a = b$. Show that this relation has the following properties, which are called the ***partial order axioms***:

(i) $a \preceq a$ for all $a \in A$.

(ii) $a \preceq b$ and $b \preceq a \Rightarrow a = b$.

(iii) $a \preceq b$ and $b \preceq c \Rightarrow a \preceq c$.

(b) Let P be a relation on A that satisfies properties (i)-(iii). Define a relation S on A by letting aSb if aPb and $a \neq b$. Show that S is a strict partial order on A.

The purpose of the exercise is to show that the two definitions of the *partial order*, i.e. the one given by the axioms (i)-(iii) and the other one given in the text based on a strict partial order, are equivalent in the sense that a relation satisfies the axioms (i)-(iii) of a partial order if and only if there is a strict partial order inducing the relation.

(a) A strict partial order must satisfy nRT, so that (a) if $a \prec b$ then neither $a = b$ nor $b \prec a$ holds, and (b) if ($a \prec b$ or $a = b$) and ($b \prec c$ or $b = c$) then ($a \prec c$ or $a = c$). Hence, the induced relation $\preceq$ must satisfy (ii) and (iii). It also satisfies (i) by definition.

(b) S satisfies nR by definition. Now, if aSb and bSc, then aPb and bPc, and, by (iii), aPc. If at the same time $c = a$, then, by (ii), we would have $b = c$ contradicting bSc. Therefore, $a \neq c$, and aSc. Hence, S satisfies T.

3.

Let A be a set with a strict partial order $\prec$; let $x \in A$. Suppose that we wish to find a maximal simply ordered subset B of A that contains x. One plausible way of attempting to define B is to let B equal the set of all those elements of A that are comparable with x;

$$B = \{y | y \in A \text{ and either } x \prec y \text{ or } y \prec x\}.$$

But this will not always work. In which of Examples 1 and 2 will this procedure succeed and in which will it not?

On the one hand, this will definitely work if the set can be partitioned into a collection of disjoint ordered subsets such that no two elements from two different subsets are comparable. On the other hand, this will fail if, for example, x is comparable with two elements that are not comparable. So, for the set in Example 1 this will fail (every circle is comparable with two larger circles that are not comparable), and for the sets in Example 2 and Exercise 1 it will succeed.

4.

Given two points (x_0, y_0) and (x_1, y_1) of $\mathbb{R}^2$, define

$$(x_0, y_0) \prec (x_1, y_1)$$

if $x_0 < x_1$ and $y_0 \leq y_1$. Show that the curves $y = x^3$ and $y = 2$ are maximal simply ordered subsets of $\mathbb{R}^2$, and the curve $y = x^2$ is not. Find all maximal simply ordered subsets.

For a point (x, y) the points that are comparable with it are the points to the east, north-east, west and south-west of it. Therefore, a subset is ordered iff for every two points (x, y) and (x', y') in it such that $x \leq x'$, either $(x, y) = (x', y')$, or $x < x'$ and $y \leq y'$. This implies two things, first, that the ordered subset has to define a function on $\mathbb{R}$ or its subset, and, second, that the function has to be weakly increasing. In fact, these two conditions are also sufficient to define an ordered subset.

Now, suppose that for a weakly increasing function f, there is a "hole" in its domain A, i.e. there are $x' < x < x''$ such that $x', x'' \in A$, but $x \notin A$. Then, the set $f(A \cap (-\infty, x))$ is bounded from above by $f(x'')$, and it has the least upper bound m. Similarly, the set $f(A \cap (x, +\infty))$ is bounded from below by m, and it has the greatest lower bound m'. Note that, $m \leq m'$, so we can add the point (x, y) where $m \leq y \leq m'$ to f, and f will remain weakly increasing. This means that if f has "holes" in its domain, then it does not define a maximal ordered subset. There should not be any holes.

What we have so far. A maximal ordered subset has to be a weakly increasing function defined on an interval (closed [], open (), or half-open [) (], finite or infinite). Now suppose that the domain of f is bounded from below, and its image set is bounded from below as well. Then, there is a point that is to the left of the domain of f and below its image set, and we can add the point to f so that it will remain weakly increasing. Hence, at least one of the domain of f and its image set should not be bounded from below. Similarly, we conclude that at least one the domain of f and its image set should not be bounded from above.

This also implies that the domain of the function is an open interval, for if, for example, f is defined on $[a, b)$ where $b \in \mathbb{R}$ or $b = +\infty$, or on $[a, b]$ where $b \in \mathbb{R}$, then the domain is bounded from below, and f is bounded from below by $f(a)$. Similarly for the domain $(a, b]$ where $a \in \mathbb{R}$ or $a = -\infty$.

Now, suppose that $f : (a, b) \to \mathbb{R}$ is a weakly increasing function such that either $a = -\infty$ or $\lim_{x \to a+0} f(x) = -\infty$ (f is not bounded from below), and either $b = +\infty$ or $\lim_{x \to b-0} f(x) = +\infty$ (f is not bounded from above). Let us take a point (x, y) such that either $x \notin (a, b)$, or $x \in (a, b)$ and $f(x) \neq y$. If $x \notin (a, b)$, then either $x \leq a$ or $x \geq b$. In the first case when $x \leq a$, f is not bounded from below, and there is some $x' \in (a, b)$ such that $x' > x$ and $f(x') < y$. Hence, (x, y) and $(x', f(x'))$ are not comparable. Similarly, the second case when $x \geq b$. If $x \in (a, b)$, then (x, y) and $(x, f(x))$ are not comparable. We conclude that f defines a maximal subset.

Summary: a subset of $\mathbb{R}^2$ is a maximal ordered subset iff it defines a weakly increasing function $f:(a,b)\to\mathbb{R}$ such that $a=-\infty$ or f is not bounded from below, and $b=+\infty$ or f is not bounded from above. Note that f does not have to be continuous.

So, both $y=x^3$ and $y=2$ are maximal (both are weakly increasing and defined on $(-\infty,+\infty)$). But $y=x^2$ is not a maximal ordered set (it is not a weakly increasing function, so not even an ordered set), and, for example, $(0,0)$ and $(-1,1)$ are not comparable.

Other examples of maximal ordered sets defined by weakly increasing functions:

	the domain of f is unbounded from above	the domain of f is bounded from above
the domain of f is unbounded from below	$y=\operatorname{sign}x=\begin{cases}1 & x>0\\ 0 & x=0\\ -1 & x<0\end{cases}$	$y=-\frac{1}{x}$, $x<0$
the domain of f is bounded from below	$y=-\frac{1}{x}$, $x>0$	$y=\tan x$, $-\frac{\pi}{2}<x<\frac{\pi}{2}$

Note that I specifically found examples such that the function if bounded from below/above iff its domain is not bounded from below/above, and also one of these functions is not continuous, though one could have found a non-continuous function in all cases.

5.

Show that Zorn’ s lemma implies the following:

Lemma (Kuratowski). Let $\mathcal{A}$ be a collection of sets. Suppose that for every subcollection $\mathcal{B}$ of $\mathcal{A}$ that is simply ordered by proper inclusion, the union of the elements of $\mathcal{B}$ belongs to $\mathcal{A}$. Then $\mathcal{A}$ has an element that is properly contained in no other element of $\mathcal{A}$.

$\mathcal{A}$ is strictly partially ordered by proper inclusion. Given a subcollection $\mathcal{B}$ of $\mathcal{A}$, the union of the elements of $\mathcal{B}$ is an upper bound for $\mathcal{B}$, which, by assumption, is also in $\mathcal{A}$. Hence, Zorn’ s lemma implies that there is a set in $\mathcal{A}$ such that no other set in $\mathcal{A}$ contains it.

6.

A collection $\mathcal{A}$ of subsets of a set X is said to be of *finite type* provided that a subset B of X belongs to $\mathcal{A}$ if and only if every finite subset of B belongs to $\mathcal{A}$. Show that the Kuratowski lemma implies the following:

Lemma (Tukey, 1940). Let $\mathcal{A}$ be a collection of sets. If $\mathcal{A}$ is of finite type, then $\mathcal{A}$ has an element that is properly contained in no other element of $\mathcal{A}$.

Take any ordered subcollection $C\subset\mathcal{A}$, and the union of its sets U . We want to show that $U\in\mathcal{A}$. Take any finite subset B of U . For each point in B , there is a set in C containing it, and since the number of points is finite and C is ordered, there is a set in C that contains all these points, i.e. it contains B (if one set contains b_1 and another contains b_2 , then one of them has to contain both b_1 and b_2 , etc.). Since the set containing B is in $C\subset\mathcal{A}$, all its finite subsets, including B , are in $\mathcal{A}$, i.e. $B\in\mathcal{A}$. So, any finite subset of U is in $\mathcal{A}$, and therefore, $U\in\mathcal{A}$. Now apply Kuratowski lemma.

7.

Show that the Tukey lemma implies the Hausdorff maximum principle. [*Hint:* If $\prec$ is a strict partial order on A, let $\mathcal{A}$ be the collection of all subsets of A that are simply ordered by $\prec$. Show that $\mathcal{A}$ is of finite type.]

Following the hint, let $\mathcal{A}$ be the collection of ordered subsets of A. If a set A is in $\mathcal{A}$, it is ordered, and all its finite subsets are ordered as well, so all finite subsets of A are in $\mathcal{A}$. Now, suppose that for a set B all its finite subsets are in $\mathcal{A}$. Then for any two different elements of B, the set consisting of these two elements is finite, hence, is in $\mathcal{A}$ and ordered. Therefore, the set B is ordered as well. It follows that $\mathcal{A}$ is of finite type. Therefore, Tukey' s lemma implies that there is a maximal ordered set in the collection, as no other ordered set (no other set in $\mathcal{A}$) contains it.

8.

A typical use of Zorn' s lemma in algebra is the proof that every vector space has a basis. Recall that if A is a subset of the vector space V, we say a vector belongs to the *span* of A if it equals a finite linear combination of elements of A. The set A is *independent* if the only finite linear combination of elements of A that equals the zero vector is the trivial one having all coefficients zero. If A is independent and if every vector in V belongs to the span of A, then A is a *basis* for V.

(a) If A is independent and $v \in V$ does not belong to the span of A, show $A \cup \{v\}$ is independent.

(b) Show the collection of all independent sets in V has a maximal element.

(c) Show that V has a basis.

(a) If it were not independent, there would be a non-trivial linear combination equal to the zero vector. This combination must include v with a non-zero coefficient, as A is independent. But this leads to the contradiction as it implies that $v \in span(A)$.

(b) Let $\mathcal{A}$ be the collection of all independent sets in V partially ordered by the proper inclusion. Then $B \in \mathcal{A}$ iff any non-trivial linear combination of any finite number of vectors in B is not the zero vector iff any finite subset of B is in $\mathcal{A}$. Therefore, $\mathcal{A}$ is of finite type and Tukey' s lemma applies.

(c) The maximal set found in (b) is a basis, as it is independent, and if there were a vector not in its span, then, according to (a), the set would not be maximal.

Supplementary Exercises

1.

Theorem (General principle of recursive definition). Let J be a well-ordered set; let C be a set. Let $\mathcal{F}$ be the set of all functions mapping sections of J into C. Given a function $\rho : \mathcal{F} \to C$, there exists a unique function $h : J \to C$ such that $h(\alpha) = \rho(h|S_\alpha)$ for each $\alpha \in J$.

[*Hint:* Follow the pattern outlined in Exercise 10 of §10.]

In Exercise 10 of §10, we are asked to prove a specific case of this theorem for a particular choice of ρ. Our prove of that result is, in fact, for this more general case. See Exercise 10 of §10.

2.

(a) Let J and E be well-ordered sets; let $h : J \to E$. Show the following two statements are equivalent:

(i) h is order preserving and its image is E or a section of E.

(ii) $h(\alpha) = smallest[E - h(S_\alpha)]$ for all α.

[*Hint:* Show that each of these conditions implies that $h(S_\alpha)$ is a section of E; conclude that it must be the section by $h(\alpha)$.]

(b) If E is a well-ordered set, show that no section of E has the order type of E, nor do two different sections of E have the same order type. [*Hint:* Given J, there is at most one order-preserving map of J into E whose image is E or a section of E.]

(a) (i) implies (ii). Let B be the set of $x \in J$ such that $h(S_x) = S_{h(x)}$, and suppose for some $\alpha \in J$, $S_\alpha \subset B$. h is order preserving, therefore, for $\beta \in S_\alpha$, $h(\beta) < h(\alpha)$, and $h(S_\alpha) \subset S_{h(\alpha)}$. Now, since $h(J)$ is E or a section of E, $h(\alpha) \in h(J)$ implies that for all $\delta \in S_{h(\alpha)}$, $\delta \in h(J)$, and there exists $\beta \in J$ such that $h(\beta) = \delta$. If $\beta \geq \alpha$, then $h(\beta) \geq h(\alpha) \notin S_{h(\alpha)}$, therefore, $\beta \in S_\alpha$, and $\delta \in h(S_\alpha)$. We conclude that $S_{h(\alpha)} = h(S_\alpha)$. By transfinite induction, $B = J$, and for all $\alpha \in J$, $h(\alpha)$ is the smallest element of E not in $S_{h(\alpha)} = h(S_\alpha)$.

(ii) implies (i). Let B be the set of $x \in J$ such that $h(S_x) = S_{h(x)}$, and suppose for some $\alpha \in J$, $S_\alpha \subset B$. If $h(\alpha) \leq h(\beta)$ for some $\beta \in S_\alpha \subset B$, then $h(\alpha) \in S_{h(\beta)} \cup \{h(\beta)\}$ $= h(S_\beta) \cup \{h(\beta)\} \subset h(S_\alpha)$, contradicting its definition, hence, $h(\alpha) > h(\beta)$ for all $\beta \in S_\alpha$, and $h(S_\alpha) \subset S_{h(\alpha)}$. At the same time, by definition, if $\delta \in S_{h(\alpha)}$, then $\delta < h(\alpha)$, $\delta \in h(S_\alpha)$, implying $S_{h(\alpha)} \subset h(S_\alpha)$. We conclude that $S_{h(\alpha)} = h(S_\alpha)$. By transfinite induction, $B = J$. This implies that for every $\alpha, \beta \in J$ such $\beta < \alpha$, $h(\beta) \in h(S_\alpha) = S_{h(\alpha)}$, and $h(\beta) < h(\alpha)$. Hence, h is order preserving. Further, suppose $h(J) \neq E$. Let us extend J by one element $x \notin J$, $J' = J \cup \{x\}$, and assume that for all $\alpha \in J$, $\alpha < x$. J' is well-ordered. Consider $h' : J' \to E$ such that $h'|J = h$, and $h'(x) = smallest[E - h(J)]$. Then h' satisfies (ii), and as we already shown, $h'(S_x) = h(J) = S_{h'(x)} = S_{smallest[E-h(J)]}$. This shows that the image of J under h is either the whole E or a section of E by the smallest element not in the image.

(b) By (a), if $h : S_\alpha \to E$ is an order preserving map, then it must be given by (ii), and using the principle of the recursive definition (Exercise 1) there is only one such function. So, it must be the identity function ("another" order preserving function), which is not bijective. For two sections, one must be a subsection of the other.

3.

Let J and E be well-ordered sets; suppose there is an order-preserving map $k: J \to E$. Using Exercises 1 and 2, show that J has the order type of E or a section of E. [*Hint:* Choose $e_0 \in E$. Define $h: J \to E$ by the recursion formula

$$h(\alpha) = smallest[E - h(S_\alpha)] \text{ if } h(S_\alpha) \neq E,$$

and $h(\alpha) = e_0$ otherwise. Show that $h(\alpha) < k(\alpha)$ for all α; conclude that $h(S_\alpha) \neq E$ for all α.]

Note that we cannot directly apply Exercise 2, as there is a condition in (a)(i) of that exercise that requires h to map J onto E or a section of E. And this assumption is not given for k. In fact, this is exactly what we want from an order preserving map from J into E, so, we construct another order preserving function h satisfying this condition, as suggested in the hint.

First, we need to formally show that h is well-defined. This is pretty much straightforward using Exercise 1. For any $S_\alpha \subset J$ and $f: S_\alpha \to E$ define $\rho(f) = smallest[E - f(S_\alpha)]$ if $f(S_\alpha) \neq E$, or $\rho(f) = e_0$ otherwise. Then ρ is well-defined, and it uniquely defines h satisfying the recursive formula.

Second, we use the existence of the order-preserving function k to show that a) h must be bounded above by k, b) no section is mapped by h onto E, and c) using Exercise 2, h is an order-preserving function that maps J onto E or its section.

a) Let B be the subset of $\alpha \in J$ such that the inequality $h(\alpha) \leq k(\alpha)$ holds. If $S_\alpha \subset B$ then for every $\beta \in S_\alpha$, $k(\alpha) > k(\beta) \geq h(\beta)$, so $k(\alpha)$ is an element that is greater than all elements in $h(S_\alpha)$, but $h(\alpha)$ is the smallest element that is greater than all elements in $h(S_\alpha)$ provided there is at least one such element, and there is one, namely, $k(\alpha)$, hence, $h(\alpha) \leq k(\alpha)$. By transfinite induction, $B = J$.

b) If for some $\alpha \in J$, $h(S_\alpha) = E$, then there is some $\beta < \alpha$ such that $k(\alpha) = h(\beta) \leq k(\beta)$. Contradiction. Therefore, $h(S_\alpha) \neq E$ for all $\alpha \in J$.

c) Now, since $h(S_\alpha) \neq E$ for all $\alpha \in J$, h is defined by the expression 2(a)(ii), and by Exercise 2(a), h is an order preserving function mapping J onto E or its section. Since h is order preserving, it is injective, so h is an order preserving bijection from J onto E or its section.

4.

Use Exercises 1-3 to prove the following:

(a) If A and B are well-ordered sets, then exactly one of the following three conditions holds: A and B have the same order type, or A has the order type of a section of B, or B has the order type of a section of A. [*Hint:* Form a well-ordered set containing both A and B, as in Exercise 8 of §10; then apply the preceding exercise.]

(b) Suppose that A and B are well-ordered sets that are uncountable, such that every section of A and of B is countable. Show A and B have the same order type.

(a) At least one of the three conditions holds. Consider the well-ordered union C of A and B as in Exercise 8 of §10, where every element of A is less than every element of B. Then, the identity function is an order preserving mapping from B into C. Using Exercise 3, there is an order preserving bijection h from B onto a section S_x of C or onto C itself. If x is in A, then S_x is a subset of A, and B has the order type of a section of A. If x equals the smallest element z of B, then $S_x = S_z$ equals A, and B has the order type of A. Otherwise, there is $b \in B$ such that $h(b) = z$, and, according to Exercise 2(a), $h(S_b) = S_{h(b)} = S_z = A$, implying there is an order preserving bijection of A with the section S_b of B.

No more than one of the three conditions hold. If A has the order type of a section of B (there is an order preserving bijection $h : A \to S_b \subset B$), then A and B cannot have the same order type (there is an order preserving bijection $g : B \to A$), and B cannot have the order type of a section of A (there is an order preserving bijection $g : B \to S_a \subset A$), as in both cases this would imply that there is an order preserving bijection $g \circ h : A \to S_{g(b)}$ of A with the section $S_{g(b)}$ of A, which is not possible according to Exercise 2(b).

(b) This follows from (a) and the fact that there is no bijection of a countable set with an uncountable set.

5.

Let X be a set; let $\mathcal{A}$ be the collection of all pairs $(A, <)$, where A is a subset of X and $<$ is a well-ordering of A. Define

$$(A, <) \prec (A', <')$$

if $(A, <)$ *equals* a section of $(A', <')$.

(a) Show that $\prec$ is a strict partial order on $\mathcal{A}$.

(b) Let $\mathcal{B}$ be a subcollection of $\mathcal{A}$ that is simply ordered by $\prec$. Define B' to be the union of the sets B, for all $(B, <) \in \mathcal{B}$; and define $<'$ to be the union of the relations $<$, for all $(B, <) \in \mathcal{B}$. Show that $(B', <')$ is a well-ordered set.

(a) No $(A, <)$ equals its own section, and if $(A, <)$ equals a section of $(B, <')$, which equals a section of $(C, <")$, then $(A, <)$ equals a section of $(C, <")$. So, non-reflexivity and transitivity hold.

(b) Let $x_1, x_2 \in (B', <')$. Then, for $i \in \{1, 2\}$ there exists $x_i \in (A_i, <_i)$. Without loss of generality, suppose $(A_2, <_2)$ equals a section of $(A_1, <_1)$. Then, both points x_1 and x_2 are in $(A_1, <_1)$, and at least one of $x_1 <_1 x_2$, $x_1 = x_2$ and $x_2 <_1 x_1$ holds. Hence, we have comparability. Further, $x < x$ does not hold in any $(A, <) \in \mathcal{B}$, hence, $x <' x$ does not hold, and $<'$ is irreflexive. For any three elements $x_1, x_2, x_3 \in (B', <')$ such that $x_1 <' x_2 <' x_3$, consider $(A_i, <_i)_{i=1,2}$ such that $x_1 <_1 x_2$ and $x_2 <_2 x_3$, and suppose that $(A_{3-i}, <_{3-i})$ is a section of $(A_i, <_i)$ (i equals 1 or 2), then $x_1 <_i x_2 <_i x_3$, implying $x_1 <_i x_3$ and $x_1 <' x_3$, hence, $<'$ is transitive. To sum up, $<'$ is an order on B'. For any nonempty subset A of B', let $x \in A$, and $(B, <) \in \mathcal{B}$ be such that $x \in (B, <)$. Then, for $y \in A$, $y <' x$ iff $y < x$ and $y \in B$, and the $<$ -smallest element of $(B \cap A, <)$ is the $<'$ -smallest element of $(A, <')$.

6.

Use Exercises 1 and 5 to prove the following:

Theorem. The maximum principle is equivalent to the well-ordering theorem.

Given the maximum principle and a nonempty set X we need to construct a well-ordering on X. Consider the strict partial order on the collection $\mathcal{A}$ of well-ordered subsets of X as in Exercise 5. The collection $\mathcal{A}$ is not empty as, for example, there are finite well-ordered subsets of X. By the maximum principle, there exists a maximal ordered subcollection $\mathcal{B}$ of $\mathcal{A}$. Take the union of all subsets of X in $\mathcal{B}$, a well-ordered subset $(B', <')$ of X (Exercise 5(b)). If there is $x \notin B'$, then $(B' \cup \{x\}, <")$, where $<"$ is the extension of $<'$ defined by $b < x$ for all $b \in B'$, is a well-ordered subset of X, and it is strictly $\prec$-greater than any subset in $\mathcal{B}$, as $B' = S_x$. But this contradicts the maximality of $\mathcal{B}$, as $(B' \cup \{x\}, <") \notin \mathcal{B}$. So, $X = B'$ and $<'$ is a well-ordering on X.

Given the well-ordering theorem and a nonempty set X together with a strict partial order $<$, we need to prove that there is a maximal ordered subset of X. Let $\prec$ be a well-ordering on X, and by the general principle of recursive definition (Exercise 1), we construct $h : X \to \mathcal{P}(X)$ using

$$\rho(f : S_x \to \mathcal{P}(X)) = \begin{cases} f(S_x) \cup \{x\} & \text{if } f(S_x) \cup \{x\} \text{ is } <\text{-ordered,} \\ f(S_x) & \text{otherwise.} \end{cases}$$

Then, $h(\alpha) = \rho(h|S_\alpha) = h(S_\alpha) \cup \{\alpha\}$ if it is $<$ -ordered, and $h(S_\alpha)$ otherwise (sections are all with respect to $\prec$). The idea is exactly as in the text: take all elements one-by-one in some order, and see if you can add each one to the existing ordered subset so that the resulting subset is still ordered. Note, that $h(\alpha)$ is an $<$ -ordered subset of X, and $h(S_\alpha)$ is always a suborder of $h(\alpha)$. Hence, the union $Z = \cup_{\alpha \in X} h(\alpha)$ is an ordered subset of X (this is similar but even either than Exercise 5(b)). Further, it is a maximal ordered subset of X. Indeed, if some $x \notin Z$, then $h(S_x) \cup \{x\} \subset Z \cup \{x\}$ is not ordered, neither is $Z \cup \{x\}$.

7.

Use Exercises 1-5 to prove the following:

Theorem. The choice axiom is equivalent to the well-ordering theorem.

Proof. Let X be a set; let c be a fixed choice function for the nonempty subsets of X. If T is a subset of X and $<$ is a relation on T, we say that $(T, <)$ is a ***tower*** in X if $<$ is a well-ordering of T and if for each $x \in T$,

$$x = c(X - S_x(T)),$$

where $S_x(T)$ is the section of T by x.

(a) Let $(T_1, <_1)$ and $(T_2, <_2)$ be two towers in X. Show that either these two ordered sets are the same, or one equals a section of the other. [*Hint:* Switching indices if necessary, we can assume that $h : T_1 \to T_2$ is order preserving and $h(T_1)$ equals either T_2 or a section of T_2. Use Exercise 2 to show that $h(x) = x$ for all x.]

(b) If $(T, <)$ is a tower in X and $T \neq X$, show there is a tower in X of which $(T, <)$ is a section.

(c) Let $\{(T_k, <_k) | k \in K\}$ be the collection of all towers in X. Let

$$T = \bigcup_{k \in K} T_k \text{ and } <= \bigcup_{k \in K} (<_k).$$

Show that $(T, <)$ is a tower in X. Conclude that $T = X$.

Given the choice axiom and a nonempty set X, we need to construct a well-ordering on X. The towers simply describe the construction of a well-ordering on X "step-by-step". Take *any* tower T, let x_1 be its smallest element, then the section of the tower by x_1, i.e. $S_{x_1}(T)$, is empty, therefore, the smallest element of any tower must be $x_1 = c(X)$. Now take the second to least element in T, x_2, the section $S_{x_2}(T)$ contains x_1 only, therefore, $x_2 = c(X - \{x_1\})$. And etc. So the proof is actually to show that the construction of the tower this way can be continued up to the whole set X (using transfinite induction or recursion along the way).

(a) There is an order preserving injection at least one way between the towers such that the image set of the injection is the whole range or a subsection of the range (Exercise 4(a)). So, as the hint suggests, "switching indices if necessary, there is an order preserving $h: T_1 \to T_2$ such that $h(T_1)$ equals T_2 or its section. Let Y be the set of elements $y \in T_1$ such that $h(y) = y$. If $S_x(T_1) \subset Y$, $x \in T_1$, then $S_x(T_1) = h(S_x(T_1)) = S_{h(x)}(T_2)$ (the fact proved in Exercise 4), and, therefore, $x = c(X - S_x(T_1))$ $= c(X - S_{h(x)}(T_2))$ $= h(x)$. By transfinite induction, $x = h(x)$ for all points in T_1.

(b) Take $x = c(X - T)$ and extend the relation $<$ on T to $T' = T \cup \{x\}$ by taking $<' = <$ on T and $z < x$ for all $z \in T$. Then, T' is well-ordered by $<'$, $T = S_x(T')$ and $z = c(X - S_z(T'))$ holds for all $z \in T'$ including $z = x$.

(c) In Exercise 5(b) we proved that the union of strictly ordered collection of well-ordered subsets is a well-ordered subset. Now, take any $x \in T$, there is a tower $(T_k, <_k)$ containing it. For any other tower $(T_l, <_l)$ containing x, either $(T_l, <_l)$ is a section of $(T_k, <_k)$, or $(T_k, <_k)$ is a section of $(T_l, <_l)$ (see (a)). So, $S_x(T)$ equals $S_x(T_k)$, and, therefore, $x = c(X - S_x(T_k))$ $= c(X - S_x(T))$. Therefore, $(T, <)$ is a tower in X. If $X \neq T$, then, by (b), there is another tower in X of which T is a section, which is not possible, as T is the union of all towers in X. Hence, T is a well-ordered tower such that $T = X$.

8.

Using Exercises 1-4, construct an uncountable well-ordered set, as follows. Let $\mathcal{A}$ be the collection of all pairs $(A, <)$, where A is a subset of $\mathbb{Z}_+$ and $<$ is a well-ordering of A. (We allow A to be empty.) Define $(A, <) \sim (A', <')$ if $(A, <)$ and $(A', <')$ have the same order type. It is trivial to show this is an equivalence relation. Let $[(A, <)]$ denote the equivalence class of $(A, <)$; let E denote the collection of these equivalence classes. Define

$$[(A, <)] \ll [(A', <')]$$

if $(A, <)$ has the order type of a *section* of $(A', <')$.

(a) Show that the relation $\ll$ is well defined and is a simple order on E. Note that the equivalence class $[(\emptyset, \emptyset)]$ is the smallest element of E.

(b) Show that if $\alpha = [(A, <)]$ is an element of E, then $(A, <)$ has the same order type as the section $S_\alpha(E)$ of E by α. [*Hint:* Define a map $f: A \to E$ by setting $f(x) = [(S_x(A), \text{restriction of } <)]$ for each $x \in A$.]

(c) Conclude that E is well-ordered by $\ll$.

(d) Show that E is uncountable. [*Hint:* If $h: E \to \mathbb{Z}_+$ is a bijection, then h gives rise to a well-ordering of $\mathbb{Z}_+$.]

(a) "Well defined" means that the relation does not depend on the choice of $(A, <)$ representing a class. It does not, as all pairs in one class have the same order type. Then, using Exercises 2(b) and 4(a), the relation is non-reflexive and every two equivalence classes are comparable. Finally, transitivity follows from the fact that a section of a section is a section.

(b) Define the map f as in the hint. This is an order preserving injection, as if $x < y$ then $S_x(A)$ is a section of $S_y(A)$. Moreover, for every $x \in A$, $f(x)$ is a subsection of A , so $f(x) \in S_\alpha(E)$. Now, if $[(B, <')] \ll \alpha$, then there is an order preserving bijection from B onto a section $S_\gamma(A)$, and $f(\gamma) = [(B, <')]$. Therefore, $f : A \to f(A) = S_{[(A,<)]}(E)$ is an order preserving bijection from $(A, <)$ onto $S_{[(A,<)]}(E)$.

(c) Take any element $\alpha = [(A, <)]$ of a nonempty subset $B \subset E$. If α is not the smallest element of B ($B \cap S_\alpha(E)$ is not empty), we show that there is one. $(A, <)$ has the same order type as $S_\alpha(E)$, and there is the order preserving bijection f defined in (b). Then, $f(smallest[f^{-1}(B \cap S_\alpha(E))])$ is the smallest element in B . (Simply said, by (b), every section of E is well-ordered, hence, so is E .)

(d) E is infinite, as $e_n = [(\{1, \ldots, n\}, <)] \in E$ for every $n \in \mathbb{Z}_+$, and for $m \neq n$, e_m and e_n have different order types (for example, Exercise 2(b)). Suppose E is countable and $h : E \to \mathbb{Z}_+$ is a bijection. Define the order $\prec$ on $\mathbb{Z}_+$ such that $x \prec y$ iff $h^{-1}(x) \ll h^{-1}(y)$. This is a well-ordering, and it has the same type as $\ll$ on E (h is an order preserving bijection). But from (b) we know that $[(\mathbb{Z}_+, \prec)]$ has the same order type as $S_{[(\mathbb{Z}_+,\prec)]}(E)$. Therefore, we conclude that $(E, \ll)$ has the same order type as one of its sections. Contradiction to Exercise 2(b). Hence, there is no bijection of E with $\mathbb{Z}_+$, and E is uncountable.

Note, by the way, that for any $\alpha = [(A, <)] \in E$, $S_\alpha(E)$ has the same order type as $(A, <)$, and A is countable. Therefore, by Exercise 4(b), the constructed well-ordered set is the minimal uncountable well-ordered set.

> The same argument as in (d) can be applied to any other set X . We start by considering all possible well-orderings on subsets of X (including X itself and the empty set). We define the set E of the classes of well-ordered subsets having the same order type, define the well-ordering $\ll$ on E as before, and show that each element of each class has the same order type as the section of E by this class. Since E includes all possible well-orderings on X , neither one can have the same order type as the constructed well-ordering on E , otherwise E would have the same order type as one of its sections. Therefore, $(E, \ll)$ is a well-ordered set having greater cardinality than X (if they had the same cardinality there would be a bijection giving rise to a well-ordering on X having the same order type as E ; the argument is the same as in (d)).
>
> For example, let us start with the empty set $X_1 = \emptyset$. It has one well-ordered subset, and $E_1 = \{[(\emptyset, \emptyset)]\}$. Let us denote $[(\emptyset, \emptyset)]$ by the symbol 1 . Now, $\ll_1$ on E_1 is empty, hence, we have a one-element well-ordered set $(E_1, \ll_1) = (\{1\}, \emptyset)$. Further, let the one element set $X_2 = E_1 = \{1\}$. Then, there are two well-ordered subsets of X_2 , and
>
> $$E_2 = \{[(\emptyset, \emptyset)], [(\{1\}, \emptyset)]\},$$

where $[(\emptyset, \emptyset)] \ll_2 [(\{1\}, \emptyset)]$ as $(\emptyset, \emptyset)$ has the order type of $(S_1(\{1\}) = \emptyset, \emptyset)$. Let us denote $[(\{1\}, \emptyset)]$ by the symbol 2. The constructed $(E_2, \ll_2) = (\{1, 2\}, \{(1, 2)\})$ is a well-ordered two-element set, where $1 \ll_2 2$. Now, having a two-element set $X_3 = E_2 = \{1, 2\}$, there are five well-ordered subsets of X_3 (can you name them all?), but only three classes of equivalent well-orderings (this is where the equivalence of well-orderings starts mattering). Moreover, the type of the order depends only on the number of elements in the subset (Theorem 10.1), and for different numbers of elements we have different orders (Exercise 2(b)). Hence, as representatives for the classes of equivalent well-orderings we can choose $\emptyset$, $\{1\}$ and $\{1, 2\}$. Therefore, we have

$$E_3 = \{[(\emptyset, \emptyset)], [(\{1\}, \emptyset)], [(\{1, 2\}, \{(1, 2)\})]\}.$$

Let us denote $[(\{1, 2\}, \{(1, 2)\})]$ by the symbol 3. Then, clearly, $1 \ll_3 2 \ll_3 3$. The constructed $(E_3, \ll_3) = (\{1, 2, 3\}, \{(1, 2), (1, 3), (2, 3)\})$ is a well-ordered three-element set. We can continue this way. Having an $(n-1)$-element set $X_n = \{1, 2, \ldots, n-1\}$, the set of all well-ordered subsets of X_n consists of approximately $(n-1)!e$ ($n > 1$) well-ordered subsets, where each class of equivalent k-element subsets consists of $k!$ subsets. Then, the set $E_n = \{1, 2, \ldots, n-1, [(X_n, <)]\}$ where $<$ is the usual order. We denote $[(X_n, <)]$ by n. Then,

$$(E_n, \ll_n) = (X_{n+1} = \{1, 2, \ldots, n\}, <).$$

Now, let X_ω be the set of all $[(X_n, <)] = n$, $X_\omega = \{1, 2, \ldots\}$. Then, the classes of equivalent well-ordered subsets of X_ω include all finite well-orderings, i.e. $1, 2, \ldots$, as well as all order types of countably infinite well-orderings. What we prove in (d) is that there are uncountably many countably infinite order types, and E_ω is uncountable.