Sets, Logic and Categories
Solutions to Exercises: Chapter 2

2.1 Prove that the ordered sum and lexicographic product of totally ordered (resp., well-ordered) sets is totally ordered (resp., well-ordered).

This involves checking the axioms, case-by-case. For the ordinal sum, we simplify the notation by using X and Y in place of $X \times \{0\}$ and $Y \times \{1\}$, assuming that X and Y are disjoint.

(a) Call the three clauses of the definition (1), (2), (3).

Irreflexivity: $z < z$ cannot be as a result of (3); if $z \in X$ then $z \not< z$ since X is ordered; and if $z \in Y$ then $z \not< z$ since Y is ordered.

Trichotomy: Suppose that $z_1 \neq z_2$. If $z_1, z_2 \in X$, then one of $z_1 < z_2$ and $z_2 < z_1$ holds since X is totally ordered. Similarly if $z_1, z_2 \in Y$. If, say, $z_1 \in X$ and $z_2 \in Y$, then $z_1 < z_2$ by (3).

Transitivity: Suppose that $z_1 < z_2$ and $z_2 < z_3$. If $z_1, z_2, z_3 \in X$, then $z_1 < z_3$ since X is ordered. So assume that at least one of the points is in Y. Similarly, we can assume that at least one is in X. Without loss of generality, $z_2 \in X$. Then $z_1 \in X$ and $z_3 \in Y$, so $z_1 < z_3$.

(b) Call the two clauses (1) and (2).

Irreflexivity: Clear.

Trichotomy: Suppose that $z_1 = (x_1, y_1) \neq z_2 = (x_2, y_2)$. If $y_1 \neq y_2$, then without loss $y_1 < y_2$, so $z_1 < z_2$ by (1). If $y_1 = y_2$, then $x_1 \neq x_2$ (property of ordered pairs); without loss, $x_1 < x_2$, and so $z_1 < z_2$ by (2).

Transitivity: Suppose that $z_1 < z_2$ and $z_2 < z_3$, where $z_i = (x_i, y_i)$. If y_1, y_2, y_3 are not all equal then (by considering four sub-cases) $y_1 < y_3$, so $z_1 < z_3$ by (1). Otherwise, the ordering of the z_i is the same as that of the x_i by (2), and transitivity for X implies the result.

Now suppose that X and Y are well-ordered.

(a) Let $S \subseteq X \cup Y$, $S \neq \emptyset$. If $S \cap X \neq \emptyset$ then, since X is well-ordered, there is a least element s of $S \cap X$. By (1), $s < y$ for all $y \in S \cap Y$; so s is the least element of S. On the other hand, if $S \cap X = \emptyset$ then $S \subseteq Y$, and so S has a least element since Y is well-ordered.

(b) Let $S \subseteq X \times Y$, $S \neq \emptyset$. Let

$$U = \{y \in Y : (\exists x \in X) \text{ with } (x, y) \in S\}.$$

Then $U \neq \emptyset$, so U has a least element u. Now let

$$T = \{x \in X : (x, u) \in S\}.$$

Then T has a least element t. We claim that (t, u) is the least element of S. If $(x, y) \in S$, $(x, y) \neq (t, u)$, then either $y \neq u$ (whence $u < y$, and $(t, u) < (x, y)$ by (1)), or $y = u$, $x \neq t$ (whence $t < x$, and $(t, u) < (x, y)$ by (2)).

2.2 Let X be any set, and define X^* to be the set of all finite sequences of elements of X. Prove that, if X can be well-ordered, then so can X^*. Show that dictionary order on the set X^* is never a well-ordering if $|X| > 1$.

If X is well-ordered, then X^2 is well-ordered: take it to be the lexicographic product of the ordered set X with itself. By induction, X^n is well-ordered for all $n \geq 1$. Now X^0 has just one element, namely the empty sequence. Now take the ordered sum of the well-ordered sets X^n for all n; that is, if $s \in X^n$ and $t \in X^m$, put $s < t$ if either $n < m$, or $n = m$ and $s < t$ as element of X^n.

Suppose that $a, b \in X$ with $a < b$. Then, in the dictionary order on X^*, we have the infinite decreasing sequence

$$b > ab > aab > aaab > aaaab > \cdots$$

2.3 According to our definition, any natural number can be described in symbols as a sequence whose terms are the empty set $\emptyset$, opening and closing curly brackets $\{$ and $\}$, and commas ,. For example, the number 4 is

$$\{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\},\{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\}\}$$

with eight occurrences of $\emptyset$, eight of each sort of bracket, and seven commas. How many occurrences of each symbol are there in the expression for the number n?

For $n \geq 1$, if $\{X\}$ is the sequence of symbols representing n, then $n+1$ is represented by $\{X,\{X\}\}$. So, if a_n, b_n, c_n, d_n are the numbers of empty set symbols, left braces, right braces, and commas respectively, then

$$a_{n+1} = 2a_n, \quad b_{n+1} = 2b_n, \quad c_{n+1} = 2c_n, \quad d_{n+1} = 2d_n + 1,$$

with initial conditions

$$a_1 = 1, \quad b_1 = 1, \quad c_1 = 1, \quad ,d_1 = 0.$$

By induction, the solutions are

$$a_n = 2^{n-1}, \quad b_n = 2^{n-1}, \quad c_n = 2^{n-1}, \quad d_n = 2^{n-1} - 1,$$

for $n \geq 1$. Of course, for $n = 0$ we have $a_0 = 1$ and $b_0 = c_0 = d_0 = 0$.

2.4 Prove the properties of addition and multiplication of natural numbers used in Section 1.8.

We have to prove the following, for all natural numbers a, b, c:

(a) $a + b = b + a$;

(b) $a + (b + c) = (a + b) + c$;

(c) $a + 0 = a$;

(d) $a + c = b + c$ implies $a = b$;

(e) $a < b$ implies $a + c < b + c$;

(f) $ab = ba$;

(g) $a(bc) = (ab)zc$;

(h) $a1 = a$;

(i) $ac = bc$ and $c \neq 0$ imply $a = b$;

(j) $ac < bc$ and $c \neq 0$ imply $a < b$.

(a) The proof is by induction on b. (This is induction on the well-ordered set ω, that is, ordinary 'mathematical induction'.) Both the base case and the inductive step require induction on a. This double induction takes great care!

Base case: we have to show that $a + 0 = 0 + a$. Since $a + 0 = a$ by definition, we must show that $0 + a = a$. This is true for $a = 0$. Su suppose that $0 + a = a$. Then $0 + s(a) = s(0 + a) = s(a)$. So the statement is true, by induction on a.

Inductive step: we have to show that if $a+b = b+a$ for some fixed b then $a+s(b) = s(b) + a$. Again this is proved by induction on a. Clearly it holds for $a = 0$, as in the previous paragraph. So suppose that $a + s(b) = s(b) + a$. Then

$$s(a) + s(b) = s(s(a) + b) = s(s(a + b)) = s(a + s(b)) = s(s(b) + a) = s(b) + s(a)$$

(some steps have been omitted!)

So the statement is proved.

(b) Proof by induction on c. For $c = 0$, we have

$$(a + b) + 0 = a + b = a + (b + 0).$$

So assume the result for c. Then

$$(a + b) + s(c) = s((a + b) + c) = s(a + (b + c)) = a + s(b + c) = a + (b + s(c)).$$

The result is proved.

(c) This is true by definition.

(d) First a lemma: *if s(a)=s(b), then* $a = b$. For suppose that $s(a) = s(b)$, that is, $a \cup \{a\} = b \cup \{b\}$. If $a \neq b$, then $a \in b$ and $b \in a$, which is impossible. So $a = b$.

Induction on c. If $a + 0 = b + 0$, then obviously $a = b$, so the induction starts. Now suppose that it is true for c, and suppose that $a + s(c) = b + s(c)$. Then $s(a + c) = s(b + c)$. By our lemma, $a + c = b + c$. By the inductive hypothesis, $a = b$.

(e) Again the proof is by induction on c. The result is trivial for $c = 0$.

This time the required lemma is: if $s(a) < s(b)$ then $a < b$. Now $s(a) < s(b)$ means $a \cup \{a\} \subset b \cup \{b\}$, so that $a \in b$ or $a = b$. The first is impossible (since then $s(a) = s(b)$, so $a \in b$, which means $a < b$ as required.

Nw suppose that $a + s(c), b + s(c)$, that is, $s(a + c) < s(b + c)$. By the lemma, $a + c < b + c/$ by the inductive hypothesis, $a < b$ as required.

(f)–(j): These are multiplicative analogues of (a)–(e); the proofs are similar.

2.5 Prove that the two definitions of ordinal addition and multiplication agree.

For addition, we have to show that the sets $\alpha+\beta$ and $(\alpha\times\{0\})\cup(\beta\times\{1\})$ are isomorphic. This can be shown by transfinite induction on β.

- For $\beta=0$, the isomorphism between $\alpha\times\{0\}$ and α is clear: just throw away the tag!
- Let $\beta=s(\gamma)$ and assume that $\alpha+\gamma$ and $(\alpha\times\{0\})\cup(\gamma\times\{1\})$ are isomorphic. Then the sets $\alpha+\beta$ and $(\alpha\times\{0\})\cup(\beta\times\{1\})$ are obtained by adding a greatest element to each of them, and so are isomorphic.
- Suppose that β is a limit ordinal, and that $\alpha+\gamma$ and $(\alpha\times\{0\})\cup(\gamma\times\{1\})$ are isomorphic for all $\gamma<\alpha$. Then the union of these isomorphisms is the required isomorphism between $\alpha+\beta$ and $(\alpha\times\{0\})\cup(\beta\times\{1\})$.

For multiplication, we have to show that $\alpha\cdot\beta$ and $\alpha\times\beta$ are isomorphic. Again we use induction on β.

- If $\beta=0$, both sides are zero (the empty set).
- If $\beta=s(\gamma)$, then $\beta=\gamma\cup\{\gamma\}$. Assume that $\alpha\cdot\gamma$ is isomorphic to $\alpha\times\gamma$. Then

  $$\alpha\cdot\beta=\alpha\cdot\gamma+\alpha\cong\alpha\times\gamma\cup\alpha\times\{\gamma\}=\alpha\times\beta,$$

  since the elements of $\alpha\times\{\gamma\}$ are greater than those in $\alpha\times\gamma$.
- If β is a limit ordinal, then take the union of the (unique) isomorphisms between $\alpha\cdot\gamma$ and $\alpha\times\gamma$ for $\gamma<\beta$.

2.6 Prove the following properties of ordinal arithmetic:

(a) $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$.

(b) $(\alpha+\beta)\cdot\gamma=\alpha\cdot\gamma+\beta\cdot\gamma$.

(c) $\alpha^{\beta+\gamma}=\alpha^{\beta}\cdot\alpha^{\gamma}$.

(a) By induction on γ. Suppose that $\gamma=0$. Then

$$(\alpha+\beta)+0=\alpha+\beta=\alpha+(\beta+0).$$

Suppose that $\gamma=s(\delta)$, and assume that $(\alpha+\beta)+\delta=\alpha+(\beta+\delta)$. Then

$$\begin{aligned}(\alpha+\beta)+s(\delta) &= s((\alpha+\beta)+\delta)\\ &= s(\alpha+(\beta+\delta))\\ &= \alpha+s(\beta+\delta)\\ &= \alpha+(\beta+s(\delta)).\end{aligned}$$

Finally, suppose that γ is a limit ordinal, and that $(\alpha+\beta)+\delta = \alpha+(\beta+\delta)$ for all $\delta < \gamma$. Then

$$\begin{aligned} (\alpha+\beta)+\gamma &= \bigcup_{\delta<\gamma}(\alpha+\beta)+\delta \\ &= \bigcup_{\delta<\gamma}\alpha+(\beta+\delta) \\ &= \alpha+\bigcup_{\delta<\gamma}(\beta+\delta) \\ &= \alpha+(\beta+\gamma). \end{aligned}$$

(b) **This question is incorrect — it should read**

$$\gamma\cdot(\alpha+\beta) = \gamma\cdot\alpha+\gamma\cdot\beta.$$

This can be proved by induction on β, or by using the result of Exercise 2.5, as follows.

$$\begin{aligned} \gamma\cdot(\alpha+\beta) &\cong \gamma\times(\alpha+\beta) \\ &= \gamma\times((\alpha\times\{0\})\cup(\beta\times\{1\})) \\ &\cong (\gamma\times\alpha\times\{0\})\cup(\gamma\times\beta\times\{1\}) \\ &\cong (\gamma\times\alpha)+(\gamma\times\beta). \end{aligned}$$

(You should check carefully that, at each stage, the obvious bijection is an order-isomorphism.) So the ordinals $\gamma\cdot(\alpha+\beta)$ and $(\gamma\times\alpha)+(\gamma\times\beta)$ are isomorphic.

For a counterexample to the version stated, note that

$$(\omega+1)\cdot 2 = (\omega+1)+(\omega+1) = \omega\cdot 2+1$$

(since $1+\omega = \omega$), not $\omega\cdot 2+2$.

(c) Proof by induction on γ:

- The result is clear if $\gamma = 0$, since $\alpha^0 = 1$.
- Suppose that $\gamma = s(\delta)$. Then

$$\begin{aligned} \alpha^{\beta+s(\delta)} &= \alpha^{s(\beta+\delta)} \\ &= \alpha^{\beta+\delta}\cdot\alpha \\ &= \alpha^{\beta}\cdot\alpha^{\delta}\cdot\alpha \\ &= \alpha^{\beta}\cdot\alpha^{s(\delta)}. \end{aligned}$$

- If γ is a limit ordinal, take the union.

2.7 (a) Show that, if $\gamma+\alpha = \gamma+\beta$, then $\alpha = \beta$.
(b) Show that, if $\gamma\cdot\alpha = \gamma\cdot\beta$ and $\gamma \neq 0$, then $\alpha = \beta$.

(a) The identity map from $\gamma+\alpha$ to $\gamma+\beta$ maps γ to γ and induces an isomorphism from α to β. Now isomorphic ordinals are equal, by Theorem 2.3.

(b) Suppose that $\alpha < \beta$; say $\beta = \alpha+\delta$ for some $\delta > 0$. Then $\gamma\cdot\beta = \gamma\cdot\alpha+\gamma\cdot\delta$. Now it cannot be the case that $\gamma\cdot\beta = \gamma\cdot\alpha$; for the isomorphism would map $\gamma\cdot\alpha$ to a proper section of itself. Similarly, $\beta < \alpha$ is impossible. So $\alpha = \beta$.

2.8 Let $(X_i)_{i\in I}$ be a family of non-empty sets. Prove that, under either of the following conditions, the cartesian product $\prod_{i\in I} X_i$ is non-empty:

(a) $X_i = X$ for all $i \in I$;

(b) X_i is well-ordered for all $i \in I$.

(a) For each $x \in X$, the function f given by $f(i) = x$ for all $i \in I$ is a choice function. This shows that the cartesian product is at least as large as X.

(b) Let x_i be the least element of X_i. Then the function f given by $f(i) = x_i$ for all $i \in I$ is a choice function.

2.9 Let X be a subset of the set of real numbers, which is well-ordered by the natural order on $\mathbb{R}$. Prove that X is finite or countable.

The well-ordered set X is isomorphic to a unique ordinal α; that is, $X = \{x_\beta : \beta < \alpha\}$, and $\beta < \gamma$ implies $x_\beta < x_\gamma$. Choose a real number q_β in the interval $(x_\beta, x_{s(\beta)})$ for all $\beta < \alpha$. (The apparent use of the Axiom of Choice here can be avoided: enumerate the rational numbers, and take the rational number with smallest index in this interval.)

These rational numbers are all distinct. For if $\beta < \gamma < \alpha$, then

$$q_\beta < x_{s(\beta)} \leq x_\gamma < q_\gamma.$$

So the cardinality of X does not exceed that of $\mathbb{Q}$.

2.10 (a) Show that any infinite ordinal can be written in the form $\lambda + n$, where λ is a limit ordinal and n a natural number.
(b) Show that any limit ordinal can be written in the form $\omega \cdot \alpha$ for some ordinal α.

(a) The proof is by induction. The conclusion is clear for a limit ordinal, so suppose that α is a successor ordinal, say $\alpha = s(\beta)$. By the inductive hypothesis, $\beta = \lambda + m$, where λ is a limit ordinal and m a natural number. Now

$$\alpha = \beta + 1 = (\lambda + m) + 1 = \lambda + (m+1),$$

which is of the required form.

(b) Let λ be a limit ordinal. By induction and part (a), every ordinal smaller than λ can be written in the form $\omega \cdot \beta + n$ for some ordinal β and natural number n. Let α be the set of all the ordinals β which occur in such expressions. Then we have $\beta < \alpha$, so $\omega \cdot \beta + n < \omega \cdot \alpha$; thus, $\lambda \leq \omega \cdot \alpha$. On the other hand, every ordinal less than $\omega \cdot \alpha$ has the form $\omega \cdot \beta + n$ for some $\beta < \alpha$; so $\omega \cdot \alpha \leq \lambda$, and we have equality.

2.11 Show that the set $\{m - \frac{1}{n} : m, n \in \mathbb{N}, m \geq 1, n \geq 2\}$ of rational numbers is isomorphic to ω^2. Find a set of rational numbers isomorphic to ω^3.

The ordinals less than ω^2 are those of the form $\omega \cdot m + n$. We have $\omega \cdot m + n < \omega \cdot m' + n'$ if and only if either $m < m'$, or $m = m'$ and $n < n'$. Now it is clear that the function mapping $\omega \cdot m + n$ to $(m+1) - \frac{1}{n+2}$ is an order-isomorphism between ω^2 and the given set. This amounts to showing that $(m+1)-\frac{1}{n+2}<(m'+1)-\frac{1}{n'+2}$ if and only if either $m<m'$, or $m=m'$ and $n<n'$.

To construct a set order-isomorphic to ω^3, we have to replace each interval in the above construction with a set of order-type ω. Now the interval from $(m+1)-\frac{1}{n+2}$ to $(m+1)-\frac{1}{n+3}$ has length $1/(n+2)(n+3)$; so take the set

$$\left\{(m+1)-\frac{1}{n+2}-\frac{1}{(n+2)(n+3)(p+2)}:m,n,p\in\omega\right\}.$$

Clearly this can be extended to construct ω^k for any $k\in\omega$.

2.12 Show that there are uncountably many non-isomorphic countable ordinals. Using the fact that every countable totally ordered set is isomorphic to a subset of $\mathbb{Q}$ (see Exercise 1.16), give another proof of Cantor's Theorem that the power set of a countable set is uncountable.

The set of countable ordinals is an ordinal, since every section of it is a countable ordinal. It cannot be a countable ordinal, else it would be smaller than itself. So it is uncountable.

By Exercise 1.17, every countable ordered set (and in particular every countable ordinal) is isomorphic to a subset of the ordered set $\mathbb{Q}$. So $\mathbb{Q}$ has uncountably many non-isomorphic subsets.