Solutions to selected exercises

1a, page 4

Consider a vacuously true condition proposition, say $p \to q$. By the definition of vacuously true, the hypothesis p is false. In particular, it is not the case that p is true and q is false. So the conditional proposition $p \to q$ is true by the definition of $\to$.

1b, page 4

In the notation of Definition 1.3.8, we have $p = (a \wedge b)$ and $q = (c \vee d)$ here. So the converse is $(c \vee d) \to (a \wedge b)$, the inverse is $\big(\neg(a \wedge b)\big) \to \big(\neg(c \vee d)\big)$, and the contrapositive is $\big(\neg(c \vee d)\big) \to \big(\neg(a \wedge b)\big)$.

1c, page 5

If a proposition is true, then it cannot be false because by definition no proposition can be both true and false.

If a proposition is not false, then it must be true because by definition no proposition can be neither true nor false.

1d, page 6

According to Convention 1.4.3, the compound expression $\neg p \to \neg q$ stands for $(\neg p) \to (\neg q)$.

- $\neg p$ evaluates to F according to the definition of $\neg$.
- $\neg q$ evaluates to T according to definition of $\neg$.
- $\neg p \to \neg q$ evaluates to T according to the definition of $\to$.

In summary,

$$\begin{array}{ccccc} \neg & p & \to & \neg & q \\ & \mathrm{T} & & & \mathrm{F} \\ \mathrm{F} & & & \mathrm{T} & \\ & & \mathrm{T} & & \end{array}$$

1e, page 6

(1) P and P evaluate to the same truth value under any substitution of propositions into the propositional variables.

(2) If P and Q evaluate to the same truth value under any substitution of propositions into the propositional variables, then so do Q and P.

(3) If P and Q evaluate to the same truth value under any substitution of propositions into the propositional variables, and Q and R evaluate to the same truth value under any substitution of propositions into the propositional variables, then so do P and R.

1f, page 8

No, as the following truth table shows.

p	q	r	$p \wedge q$	$(p \wedge q) \vee r$	$q \vee r$	$p \wedge (q \vee r)$
T	T	T	T	T	T	T
T	T	F	T	T	T	T
T	F	T	F	T	T	T
T	F	F	F	F	F	F
F	T	T	F	T	T	F
F	T	F	F	F	T	F
F	F	T	F	T	T	F
F	F	F	F	F	F	F

Actually, to justify a "no" answer, it suffices to give *one* row of this truth table in which the columns for $(p \wedge q) \vee r$ and $p \wedge (q \vee r)$ are different.

1g, page 8

One can prove the Associativity, the Commutativity, the Identity, and the Annihilator parts of Theorem 1.4.20 using the truth tables below.

p	q	r	$p \vee q$	$(p \vee q) \vee r$	$q \vee r$	$p \vee (q \vee r)$
T	T	T	T	T	T	T
T	T	F	T	T	T	T
T	F	T	T	T	T	T
T	F	F	T	T	F	T
F	T	T	T	T	T	T
F	T	F	T	T	T	T
F	F	T	F	T	T	T
F	F	F	F	F	F	F

p	q	r	$p \wedge q$	$(p \wedge q) \wedge r$	$q \wedge r$	$p \wedge (q \wedge r)$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	F	F	F	F
T	F	F	F	F	F	F
F	T	T	F	F	T	F
F	T	F	F	F	F	F
F	F	T	F	F	F	F
F	F	F	F	F	F	F

p	q	$p \vee q$	$q \vee p$	$p \wedge q$	$q \wedge p$
T	T	T	T	T	T
T	F	T	T	F	F
F	T	T	T	F	F
F	F	F	F	F	F

p	t	c	$p \vee c$	$p \wedge t$	$p \vee t$	$p \wedge c$
T	T	F	T	T	T	F
F	T	F	F	F	T	F

Alternatively, one can prove the associativity of $\wedge$ from that of $\vee$ as follows:

$$
\begin{aligned}
(p \wedge q) \wedge r &\equiv (\neg\neg p \wedge \neg\neg q) \wedge \neg\neg r && \text{by the Double Negative Law;}\\
&\equiv \neg(\neg p \vee \neg q) \wedge \neg\neg r && \text{by De Morgan's Laws;}\\
&\equiv \neg\big((\neg p \vee \neg q) \vee \neg r\big) && \text{by De Morgan's Laws;}\\
&\equiv \neg\big(\neg p \vee (\neg q \vee \neg r)\big) && \text{by the associativity of } \vee\text{;}\\
&\equiv \neg\neg p \wedge \neg(\neg q \vee \neg r) && \text{by De Morgan's Laws;}\\
&\equiv \neg\neg p \wedge (\neg\neg q \wedge \neg\neg r) && \text{by De Morgan's Laws;}\\
&\equiv p \wedge (q \wedge r) && \text{by the Double Negative Law.}
\end{aligned}
$$

One can also prove the commutativity of $\wedge$ from that of $\vee$ as follows:

$$\begin{aligned} p \wedge q &\equiv \neg\neg p \wedge \neg\neg q && \text{by the Double Negative Law;} \\ &\equiv \neg(\neg p \vee \neg q) && \text{by De Morgan's Laws;} \\ &\equiv \neg(\neg q \vee \neg p) && \text{by the commutativity of } \vee; \\ &\equiv \neg\neg q \wedge \neg\neg p && \text{by De Morgan's Laws;} \\ &\equiv q \wedge p && \text{by the Double Negative Law.} \end{aligned}$$

✐ 2a, page 15

(1) False: note that $\forall x \in \mathbb{Z} \;\; \neg(x > 0 \wedge x < 1)$ is true, but $\forall x \in \mathbb{R} \;\; \neg(x > 0 \wedge x < 1)$ is false.

(2) True, because every integer is a real number.

(3) True, because every integer is a real number.

(4) False: note that $\exists x \in \mathbb{R} \;\; (x > 0 \wedge x < 1)$ is true, but $\exists x \in \mathbb{R} \;\; (x > 0 \wedge x < 1)$ is false.

There are many other counterexamples for (1) and (4).

✐ 2b, page 16

(3) Note that the following are true.

$$\begin{array}{rcll} \neg\forall x \in D \;\; P(x) & \leftrightarrow & \neg\forall x \; \big(x \in D \to P(x)\big) & \text{by Definition 2.2.1(5).} \\ \neg\forall x \; \big(x \in D \to P(x)\big) & \leftrightarrow & \exists x \; \neg\big(x \in D \to P(x)\big) & \text{by part (1).} \\ \exists x \; \neg\big(x \in D \to P(x)\big) & \leftrightarrow & \exists x \; \big(x \in D \wedge \neg P(x)\big) & \text{by Example 1.4.23.} \\ \exists x \; \big(x \in D \wedge \neg P(x)\big) & \leftrightarrow & \exists x \in D \;\; \neg P(x) & \text{by Definition 2.2.4(5).} \end{array}$$

From these, we deduce that $\neg\forall x \in D \;\; P(x)$ is true if and only if $\exists x \in D \;\; \neg P(x)$ is true.

(4) Note that the following are true.

$$\begin{array}{rcll} \neg\exists x \in D \;\; P(x) & \leftrightarrow & \neg\exists x \; \big(x \in D \wedge P(x)\big) & \text{by Definition 2.2.4(5).} \\ \neg\exists x \; \big(x \in D \wedge P(x)\big) & \leftrightarrow & \forall x \; \neg\big(x \in D \wedge P(x)\big) & \text{by part (2).} \\ \forall x \; \neg\big(x \in D \wedge P(x)\big) & \leftrightarrow & \forall x \; \big(\neg(x \in D) \vee \neg P(x)\big) & \text{by De Morgan's Laws.} \\ \forall x \; \big(\neg(x \in D) \vee \neg P(x)\big) & \leftrightarrow & \forall x \; \big(x \in D \to \neg P(x)\big) & \text{by the Implication part of Theorem 1.4.20.} \\ \forall x \; \big(x \in D \to \neg P(x)\big) & \leftrightarrow & \forall x \in D \;\; \neg P(x) & \text{by Definition 2.2.1(5).} \end{array}$$

From these, we deduce that $\neg\exists x \in D \;\; P(x)$ is true if and only if $\forall x \in D \;\; \neg P(x)$ is true.

✐ 2c, page 19

(3) We have the following equivalences by Theorem 2.3.1.

$$\begin{array}{rcl} \neg\exists x \; \exists y \; Q(x,y) & \leftrightarrow & \forall x \; \neg\exists y \; Q(x,y). \\ \forall x \; \neg\exists y \; Q(x,y) & \leftrightarrow & \forall x \; \forall y \; \neg Q(x,y). \end{array}$$

From these, we deduce that $\neg\exists x \; \exists y \; Q(x,y)$ is true if and only if $\forall x \; \forall y \; \neg Q(x,y)$ is true.

(4) We have the following equivalences by Theorem 2.3.1.

$$\begin{array}{rcl} \neg\exists x \; \forall y \; Q(x,y) & \leftrightarrow & \forall x \; \neg\forall y \; Q(x,y). \\ \forall x \; \neg\forall y \; Q(x,y) & \leftrightarrow & \forall x \; \exists y \; \neg Q(x,y). \end{array}$$

From these, we deduce that $\neg\exists x \; \forall y \; Q(x,y)$ is true if and only if $\forall x \; \exists y \; \neg Q(x,y)$ is true. $\square$

✐ 2d, page 20

(1)
- This reads "there exists x in D such that, for every y in E, $xy = 0$".
- Alternatively, one can express this as "there is an element x of D which, when multiplied to any element y of E, gives a product of 0".
- This is **true** because if we choose the element 0 of D, then no matter which element y of E we multiply it to, we get a product of 0.

(2)
- This reads "for every y in E, there is x in D such that $xy = 0$".
- Alternatively, one can express this as "no matter which element y of E is given, one can always multiply it to an element x of D to get 0".
- This is **true** because no matter which element y of E is given, we can always multiply it to the element 0 of D to get 0.

(3)
- This reads "there exists x in D such that, for every y in E, $xy < 0$".
- Alternatively, one can express this as "there is an element x of D which, when multiplied to any element y of E, gives a negative product".
- This is **false** because no element x of D, when multiplied to any element y of E, always gives a negative product: let us consider all the elements of D one by one.
  - For the element -1 of D, when we multiply it to the element -1 of E, we get a non-negative product.
  - For the elements 0 and 1 of D, when we multiply them to the element 1 of E, we get non-negative products.

  There are other counterexamples.

(4)
- This reads "for every y in E, there exists x in D such that $xy < 0$".
- Alternatively, one can express this as "one can make any element y of E negative by multiplying it to some element x of D."
- This is **true**, as one can verify exhaustively for each element of E.
  - For the elements 1 and 2 of E, one can multiply them to the element -1 of D to make a negative product.
  - For the elements -1 and -2 of E, one can multiply them to the element 1 of D to make a negative product.

(5)
- This reads "there exist x_1, x_2 in D such that $x_1 + x_2 = 2$".
- Alternatively, one can express this as "there are two (possibly equal) elements x_1, x_2 of D whose sum is 2".
- This is **true** because 1 is an element of D and $1 + 1 = 2$.

(6)
- In view of Theorem 2.4.9(1), its negation $\neg\forall y_1, y_2 \in E \;\; y_1 = y_2$ is equivalent to $\exists y_1, y_2 \in E \;\; y_1 \neq y_2$.
- This negation reads "there exist y_1, y_2 in E such that $y_1 \neq y_2$".
- Alternatively, one can express this negation as "there are two different elements y_1, y_2 of E".
- This negation is true: for example, the numbers 1 and 2 are different elements of E.
- So the given proposition is **false**, because its negation is true.

✐ 3a, page 24

No. In the case when p is a false proposition and q is a true proposition, we have both $p \to q$ and $\neg p$ true, but $\neg q$ is false.

✎ 3b, page 27

(1) Suppose n is even. Use the definition of even integers to find an integer x such that $n = 2x$. Then $-n = -2x = 2(-x)$ where $-x$ is an integer. So $-n$ is even.

(2) Suppose n is odd. Use the definition of odd integers to find an integer x such that $n = 2x + 1$. Then $-n = -(2x + 1) = 2(-x - 1) + 1$ where $-x - 1$ is an integer. So n is odd.

✎ 3c, page 28

(1) We deduced n is odd from the assumption that n is not even. This uses Proposition 3.2.17.

(2) We deduced n^2 is not even from our knowledge that n^2 is odd. This uses Proposition 3.2.21.

✎ 3d, page 28

Proof. We show that $\forall x \in \mathbb{Z}\ \ 2x \neq 1$. Take any $z \in \mathbb{Z}$. By trichotomy, we have $z > 0$ or $z = 0$ or $z < 0$.

Case 1: suppose $z > 0$. Then $z \in \mathbb{N}$. So

$$\begin{array}{lll} & z \geqslant 1 & \text{by the discreteness of } \mathbb{N}; \\ \therefore & 2z \geqslant 2 \times 1 = 2 > 1 & \\ \therefore & 2z \neq 1 & \text{by the irreflexivity of } <. \end{array}$$

Case 2: suppose $z \leqslant 0$. Then $2z \leqslant 2 \times 0 = 0 < 1$. So $2z \neq 1$ by the irreflexivity of $<$. □

✎ 3e, page 30

Let us read the two steps in Strong MI as follows.

(base step) show that $P(i)$ is true for each integer i satisfying $b \leqslant i \leqslant c$;

(induction step) for each integer $k \geqslant c$, use the hypothesis that $P(i)$ is true for each integer i satisfying $b \leqslant i \leqslant k$ to show that $P(k + 1)$ is also true.

Consider the case when $c = b - 1$.

- For the base step, there is nothing to prove, because no integer i satisfies $b \leqslant i \leqslant c = b - 1$.
- Consider the induction step when $k = c$. The hypothesis we can use is $P(i)$ is true for each integer i satisfying $b \leqslant i \leqslant c = b - 1$. However, there is no such i. So there is no hypothesis one can use to show $P(b)$. In other words, one simply needs to show that $P(b)$ is true here (without assuming anything).
- In the induction step when $k = c + 1$, one needs to show $P(b) \to P(b + 1)$.
- In the induction step when $k = c + 2$, one needs to show $P(b) \wedge P(b + 1) \to P(b + 2)$.
- Etc.

We deduce that $P(b), P(b + 1), P(b + 2), \ldots$ are all true by a series of modus ponens.

✎ 3f, page 31

Proof. Note that $2^{a_1-a_2}b_1 = b_2$. As b_2 is odd, it cannot be even by Proposition 3.2.17. So $a_1 \leqslant a_2$. Similarly, we know $b_1 = 2^{a_2-a_1}b_2$. As b_2 is odd, it cannot be even by Proposition 3.2.17. So $a_2 \leqslant a_1$. Combining the two inequalities, we have $a_1 = a_2$. As $2^{a_1} = 2^{a_2} \neq 0$, we deduce from $2^{a_1}b_1 = 2^{a_2}b_2$ that $b_1 = b_2$. □

✎ 4a, page 34

(1) We want to prove that $E = \mathbb{Z}^+$, where $E = \{x+1 : x \in \mathbb{Z}_{\geqslant 0}\}$.

Proof. $(\Rightarrow)$ Let $z \in E$. Use the definition of E to find $x \in \mathbb{Z}_{\geqslant 0}$ such that $x+1 = z$. Then $x \in \mathbb{Z}$ and $x \geqslant 0$ by the definition of $\mathbb{Z}_{\geqslant 0}$. As $x \in \mathbb{Z}$, we know $x+1 \in \mathbb{Z}$ because $\mathbb{Z}$ is closed under $+$. As $x \geqslant 0$, we know $x+1 \geqslant 0+1 = 1 > 0$. So $z = x+1 \in \mathbb{Z}^+$ by the definition of $\mathbb{Z}^+$.

$(\Leftarrow)$ Let $z \in \mathbb{Z}^+$. Then $z \in \mathbb{Z}$ and $z > 0$. Define $x = z-1$. As $z \in \mathbb{Z}$, we know $x \in \mathbb{Z}$ because $\mathbb{Z}$ is closed under $-$. As $z > 0$, we know $x = z-1 > 0-1 = -1$, and thus $x \geqslant 0$ as $x \in \mathbb{Z}$. So $x \in \mathbb{Z}_{\geqslant 0}$ by the definition of $\mathbb{Z}_{\geqslant 0}$. Hence the definition of E tells us $z = x+1 \in E$. □

(2) We want to prove that $F = \mathbb{Z}$, where $F = \{x-y : x, y \in \mathbb{Z}_{\geqslant 0}\}$.

Proof. $(\Rightarrow)$ Let $z \in F$. Use the definition of F to find $x, y \in \mathbb{Z}_{\geqslant 0}$ such that $x-y = z$. Then $x, y \in \mathbb{Z}$ by the definition of $\mathbb{Z}_{\geqslant 0}$. So $z = x-y \in \mathbb{Z}$ as $\mathbb{Z}$ is closed under $-$.

$(\Leftarrow)$ Let $z \in \mathbb{Z}$.

- Case 1: suppose $z \geqslant 0$. Let $x = z$ and $y = 0$. Then $x, y \in \mathbb{Z}_{\geqslant 0}$. So $z = z - 0 = x - y \in F$ by the definition of F.
- Case 2: suppose $z < 0$. Let $x = 0$ and $y = -z$. Then $x, y \in \mathbb{Z}_{\geqslant 0}$ as $z < 0$. So $z = 0 - (-z) = x - y \in F$ by the definition of F.

So $z \in F$ in all the cases. □

✎ 4b, page 35

- $\{1\} \in C$ but $\{1\} \not\subseteq C$;
- $\{2\} \notin C$ but $\{2\} \subseteq C$;
- $\{3\} \in C$ and $\{3\} \subseteq C$; and
- $\{4\} \notin C$ and $\{4\} \not\subseteq C$.

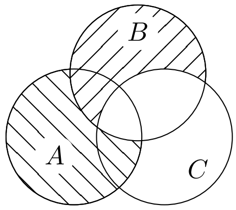
✎ 4c, page 38

Let $z \in A$. In particular, we know $z \in A$ or $z \in B$. So $z \in A \cup B$ by the definition of $\cup$.

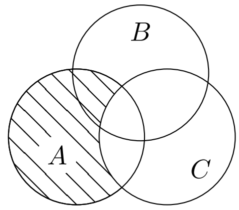
✎ 4d, page 39

Assume $A \subseteq B$ and $A \subseteq C$. Take any $z \in A$. Then $z \in B$ and $z \in C$ as $A \subseteq B$ and $A \subseteq C$ by assumption. So $z \in B \cap C$ by the definition of $\cap$. As the choice of z in A was arbitrary, this shows $A \subseteq B \cap C$. □

4e, page 39



$(A \setminus B) \cup (B \setminus C)$



$A \setminus C$

No. For a counterexample, let $A = C = \varnothing$ and $B = \{1\}$. Then

$$(A \setminus B) \cup (B \setminus C) = \varnothing \cup \{1\} = \{1\} \neq \varnothing = A \setminus C.$$

4f, page 39

Ideas. (1) The set of all sets?

(2) $\Bigg\{\bigg\{\Big\{\big\{\{\dots\ \dots\}\big\}\Big\}\bigg\}\Bigg\}$?

4g, page 39

Maybe, but is it better?

Proof. Take any set R. Split into two cases.

- Case 1: assume $R \in R$. Then $\neg(R \notin R)$. So $\neg(R \in R \Rightarrow R \notin R)$. Hence
$$\exists x \ \neg(x \in R \quad \Leftrightarrow \quad x \notin x).$$
- Case 2: assume $R \notin R$. Then $\neg(R \in R)$. So $\neg(R \notin R \Rightarrow R \in R)$. Hence
$$\exists x \ \neg(x \in R \quad \Leftrightarrow \quad x \notin x).$$

In either case, we showed $\neg\forall x \ (x \in R \Leftrightarrow x \notin x)$. So the proof is finished. □

5a, page 44

Let $P(n)$ be the predicate

> For all ordered n-tuples $(x_1, x_2, \dots, x_n)$ and $(y_1, y_2, \dots, y_n)$,
> $$(x_1, x_2, \dots, x_n) = (y_1, y_2, \dots, y_n) \quad \Leftrightarrow \quad x_1 = y_1 \text{ and } x_2 = y_2 \text{ and } \dots \text{ and } x_n = y_n.$$

over $\mathbb{Z}_{\geqslant 2}$.

(Base step) $P(2)$ is true by the definition of ordered pairs.

(Induction step) Let $k \in \mathbb{Z}_{\geqslant 2}$ such that $P(k)$ is true, i.e., all ordered k-tuples $(x_1, x_2, \dots, x_k)$ and $(y_1, y_2, \dots, y_k)$,

$$(x_1, x_2, \dots, x_k) = (y_1, y_2, \dots, y_k) \quad \Leftrightarrow \quad x_1 = y_1 \text{ and } x_2 = y_2 \text{ and } \dots \text{ and } x_k = y_k.$$

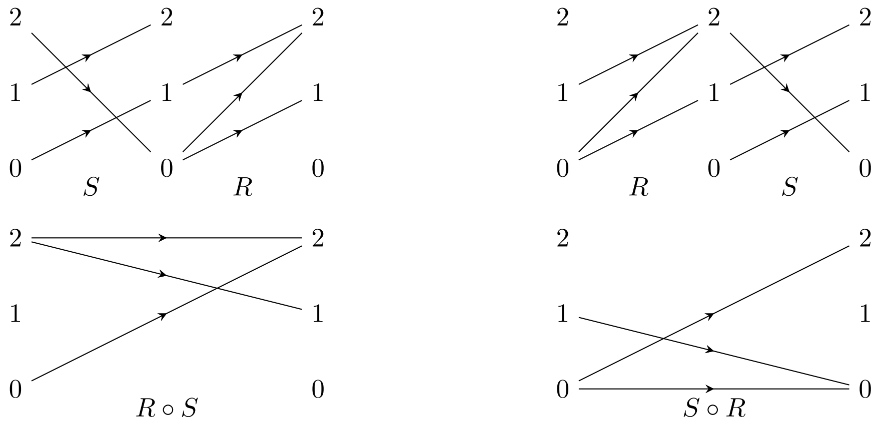
For all $(k+1)$-tuples $(x_1, x_2, \ldots, x_{k+1})$ and $(y_1, y_2, \ldots, y_{k+1})$,

$$
\begin{array}{lll}
 & (x_1, x_2, \ldots, x_k, x_{k+1}) = (y_1, y_2, \ldots, y_k, y_{k+1}) & \\
\Leftrightarrow & \big((x_1, x_2, \ldots, x_k), x_{k+1}\big) = \big((y_1, y_2, \ldots, y_k), y_{k+1}\big) & \text{by Definition 5.1.10(2);} \\
\Leftrightarrow & (x_1, x_2, \ldots, x_k) = (y_1, y_2, \ldots, y_k) \text{ and } x_{k+1} = y_{k+1} & \text{by Definition 5.1.1;} \\
\Leftrightarrow & x_1 = y_1 \text{ and } x_2 = y_2 \text{ and } \ldots \text{ and } x_k = y_k \text{ and } x_{k+1} = y_{k+1} & \\
 & & \text{by the induction hypothesis.}
\end{array}
$$

This shows $P(k+1)$ is true.

Hence $\forall n \in \mathbb{Z}_{\geqslant 2}$ $P(n)$ is true by MI. □

5b, page 46



No. For instance, we have $(2,2) \in R \circ S$ because $(2,0) \in S$ and $(0,2) \in R$, but $(2,2) \notin S \circ R$ because no $y \in A$ makes $(2,y) \in R$ and $(y,2) \in S$. (There are exactly three other counterexamples.)

6a, page 52

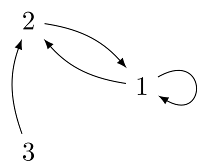
- R is reflexive as $x \leqslant x$ for all $x \in \mathbb{Q}$;
- R is not symmetric as $0 \leqslant 1$ but $1 \not\leqslant 0$, for example;
- R is transitive as $x \leqslant y$ and $y \leqslant z$ imply $x \leqslant z$ for all $x, y, z \in \mathbb{Q}$.

6b, page 52

- R' is not reflexive as $0 \not< 0$, for example;
- R' is not symmetric as $0 < 1$ but $1 \not< 0$, for example;
- R' is transitive as $x < y$ and $y < z$ imply $x < z$ for all $x, y, z \in \mathbb{Q}$.

6c, page 52

The arrow diagram below represents the relation R in the exercise:



This relation is not reflexive because $2 \not R 2$. It is not symmetric because $3 \mathrel{R} 2$ but $2 \not R 3$. It is not transitive because $2 \mathrel{R} 1$ and $1 \mathrel{R} 2$ but $2 \not R 2$.

✐ 6d, page 52

Proof. ($\Rightarrow$) Assume R is transitive. Let $(x,z) \in R \circ R$. Use the definition of $R \circ R$ to find $y \in A$ such that $(x,y) \in R$ and $(y,z) \in R$. This means $x \mathrel{R} y$ and $y \mathrel{R} z$. So $x \mathrel{R} z$ by the transitivity of R. Hence $(x,z) \in R$.

($\Leftarrow$) Assume $R \circ R \subseteq R$. Let $x, y, z \in A$ such that $x \mathrel{R} y$ and $y \mathrel{R} z$. This means $(x,y) \in R$ and $(y,z) \in R$. So $(x,z) \in R \circ R$ by the definition of $R \circ R$. Our assumption then implies $(x,z) \in R$. Hence $x \mathrel{R} z$. □

✐ 6e, page 54

Yes, as shown below.

Proof. We know $x \in [x]$ by Lemma 6.3.5(1). So $x \in S \cap [x]$ by the hypothesis. This implies $S \cap [x] \neq \varnothing$. Hence $S = [x]$ by Lemma 6.3.6. □

✐ 6f, page 55

The divisibility relation on $\mathbb{Z}$ is not antisymmetric because $1 \mid -1$ and $-1 \mid 1$, but $1 \neq -1$.

✐ 6g, page 56

The divisibility relation on $\mathbb{Z}^+$ is antisymmetric, as shown below. So it is a partial order by Example 6.1.8. It is not total because $2 \nmid 3$ and $3 \nmid 2$.

Proof of antisymmetry. Let us first show that if $a, b \in \mathbb{Z}^+$ such that $a \mid b$, then $a \leqslant b$. Let $a, b \in \mathbb{Z}^+$ such that $a \mid b$. Then the definition of divisibility gives $k \in \mathbb{Z}$ such that $b = ak$. Note $k = b/a > 0$ as both a and b are positive. Since $k \in \mathbb{Z}$, this implies $k \geqslant 1$. Thus $b = ak \geqslant a \times 1 = a$, as required.

Now let $a, b \in \mathbb{Z}^+$ such that $a \mid b$ and $b \mid a$. Then the previous paragraph tells us $a \leqslant b$ and $b \leqslant a$. So $a = b$. □

✐ 6h, page 56

We use the version of Strong MI with $c = b - 1$ given by Exercise 3.2.25.

Proof. Let $P(n)$ be the predicate "$n \notin S$" over $\mathbb{Z}_{\geqslant b}$.

(Induction step) Let $k \in \mathbb{Z}_{\geqslant b-1}$ such that $P(b), P(b+1), \ldots, P(k)$ are true, i.e., that $b, b+1, \ldots, k \notin S$. If $k+1 \in S$, then $k+1$ is the smallest element of S because $S \subseteq \mathbb{Z}_{\geqslant b}$, which contradicts our assumption. So $k+1 \notin S$. This means $P(k+1)$ is true.

Hence $\forall n \in \mathbb{Z}_{\geqslant b}\ \ P(n)$ is true by Strong MI. □

✐ 7a, page 61

Only (b), (c), (d) and (f) represent functions.

✐ 7b, page 63

Proposition 7.3.1 implies

- $\mathrm{id}_B \circ f$ is a function $A \to B$; and
- $(\mathrm{id}_B \circ f)(x) = \mathrm{id}_B(f(x)) = f(x)$ for all $x \in A$.

So $\mathrm{id}_B \circ f = f$ by Proposition 7.2.7. □

✎ 7c, page 63

(1) Yes, because $(f \circ f)(x) = f(f(x)) = f(1231) = 1231 = f(x)$ for all $x \in \mathbb{Z}$ in this case.

(2) Yes, because $(f \circ f)(x) = f(f(x)) = f(x)$ for all $x \in \mathbb{Z}$ in this case.

(3) No, because $(f \circ f)(1) = f(f(1)) = f(-1) = 1 \neq -1 = f(1)$ in this case.

(4) No, because $(f \circ f)(0) = f(f(0)) = f(1) = 4 \neq 1 = f(0)$ in this case.

(5) No, because $(f \circ f)(2) = f(f(2)) = f(4) = 16 \neq 4 = f(2)$ in this case.

✎ 7d, page 64

(b) is a surjection but not an injection; (c) is neither a surjection nor an injection; (d) is an injection but not a surjection; and (f) is both an injection and a surjection. Thus only the last one is a bijection.

✎ 7e, page 65

Proof. Let $y \in B$. Define $x = f^{-1}(y)$. Then

$$\begin{aligned}
(f \circ f^{-1})(y) &= f(f^{-1}(y)) && \text{by Proposition 7.3.1;}\\
&= f(x) && \text{by the definition of } x;\\
&= y && \text{by Proposition 7.4.11, as } f^{-1}(y) = x;\\
&= \mathrm{id}_B(y) && \text{by the definition of } \mathrm{id}_B.
\end{aligned}$$

So $f \circ f^{-1} = \mathrm{id}_B$ by Proposition 7.2.7. □

✎ 8a, page 69

Proof of the converse to the Pigeonhole Principle. Suppose $n \leqslant m$. Define $f\colon A \to B$ by setting $f(x_i) = y_i$ for each $i \in \{1, 2, \ldots, n\}$. This definition is unambiguous because the x's are different. To show injectivity, suppose $i, j \in \{1, 2, \ldots, n\}$ such that $f(x_i) = f(x_j)$. The definition of f tells us $f(x_i) = y_i$ and $f(x_j) = y_j$. Then $y_i = f(x_i) = f(x_j) = y_j$. So $i = j$ because the y's are different. This implies $x_i = x_j$. □

Proof of a partial converse to the Dual Pigeonhole Principle. Suppose $n \geqslant m > 0$. Define $f\colon A \to B$ by setting, for each $i \in \{1, 2, \ldots, n\}$,

$$f(x_i) = \begin{cases} y_i, & \text{if } i \leqslant m;\\ y_m, & \text{otherwise.}\end{cases}$$

This definition is unambiguous because the x's are different. It is surjective because given any $y_i \in B$, we have $x_i \in A$ such that $f(x_i) = y_i$. □

Proof. (1) Suppose f and g are surjective. Let $z \in C$. Use the surjectivity of g to find $y \in B$ such that $z = g(y)$. Then use the surjectivity of f to find $x \in A$ such that $y = f(x)$. Now $z = g(y) = g(f(x)) = (g \circ f)(x)$ by Proposition 7.3.1, as required.

(2) Suppose f and g are injective. Let $x_1, x_2 \in A$ such that $(g \circ f)(x_1) = (g \circ f)(x_2)$. Then $g(f(x_1)) = g(f(x_2))$ by Proposition 7.3.1. The injectivity of g then implies $f(x_1) = f(x_2)$. So the injectivity of f tells us $x_1 = x_2$, as required. □

✐ 8b, page 70

Proof. To show that A has the same cardinality as $\mathrm{range}(f)$, it suffices to find a bijection $A \to \mathrm{range}(f)$. We use the function $f_0 \colon A \to \mathrm{range}(f)$ defined by setting $f_0(x) = f(x)$ for each $x \in A$.

(Well-defined) Let us first check that the definition of f_0 given indeed assigns every element of A exactly one element of $\mathrm{range}(f)$, as required by the definition of functions. Take any $x_0 \in A$. As $x_0 \in A$ and f is a function with domain A, there is exactly one object that is equal to $f(x_0)$. So we only need to check that this object is indeed an element of the codomain of f_0, i.e., $\mathrm{range}(f)$. Recall $\mathrm{range}(f) = \{f(x) : x \in A\}$ by definition. As $x_0 \in A$, we see that $f(x_0) \in \mathrm{range}(f)$, as required.

(Surjective) Take any $y \in \mathrm{range}(f)$. Use the definition of $\mathrm{range}(f)$ to find $x \in A$ such that $y = f(x)$. Then $y = f(x) = f_0(x)$ by the definition of f_0.

(Injective) Let $x_1, x_2 \in A$ such that $f_0(x_1) = f_0(x_2)$. Then the definition of f_0 tells us $f(x_1) = f(x_2)$. So $x_1 = x_2$ as f is injective. □

Additional comment. Sometimes when one defines a function, it is not immediately clear that the definition given indeed defines a function, i.e., that it defines an object satisfying the definition of functions. In such cases, a proof should be provided. In many other cases, it is clear that the definition given really defines a function, and so no additional explanation is needed.

✐ 8c, page 70

Proof. Let $n \in \mathbb{N}$ and $f \colon \mathbb{N} \to \{1, 2, \ldots, n\}$. Define $f_n \colon \{1, 2, \ldots, n+1\} \to \{1, 2, \ldots, n\}$ by setting $f_n(x) = f(x)$ for all $x \in \{1, 2, \ldots, n+1\}$. Then f_n is not injective by the Pigeonhole Principle. Let $x_1, x_2 \in \{1, 2, \ldots, n+1\}$ such that $x_1 \neq x_2$ but $f_n(x_1) = f_n(x_2)$. Then $f(x_1) = f(x_2)$ by the definition of f_n. This show f is not injective.

The paragraph above shows, in particular, that there is no bijection $\mathbb{N} \to \{1, 2, \ldots, n\}$, for any $n \in \mathbb{N}$. So $\mathbb{N}$ is infinite. □

✐ 8d, page 70

(1) True. This follows directly from Definition 8.2.1.

(2) False. The $f \colon \mathbb{N} \to \mathbb{N}$ satisfying $f(0) = 0$ and $f(x+1) = x$ for each $x \in \mathbb{N}$ is a surjection that is not an injection, but $\mathbb{N}$ has the same cardinality as $\mathbb{N}$.

(3) False. The $f \colon \mathbb{N} \to \mathbb{N}$ satisfying $f(x) = x + 1$ for each $x \in \mathbb{N}$ is an injection that is not a surjection, but $\mathbb{N}$ has the same cardinality as $\mathbb{N}$.

(4) False. The function $f \colon \{0, 1\} \to \{0, 1\}$ satisfying $f(0) = 0 = f(1)$ is neither a surjection nor an injection, but $\{0, 1\}$ has the same cardinality as $\{0, 1\}$.

✐ 9a, page 75

Proof. By symmetry, it suffices to show only one direction. Suppose A is countable. If A is finite, then B is also finite by Lemma 8.2.8; thus B is countable and we are done. So suppose A is infinite. Then A has the same cardinality as $\mathbb{N}$ by the definition of countability. Then the symmetry and the transitivity of same-cardinality tell us B has the same cardinality of $\mathbb{N}$. So B is countable. □

✎ 9b, page 76

Proof sketch. Suppose B is finite. Use the finiteness of B to find $n \in \mathbb{N}$ and a bijection $f\colon \{1,2,\ldots,n\} \to B$. Run the following procedure.

1. Initialize $i = 0$.
2. While $A \setminus \{g_1, g_2, \ldots, g_i\} \neq \varnothing$ do:

   2.1. Let m_{i+1} be the smallest element in
   $$\big\{m \in \{1,2,\ldots,n\} : f(m) \in A \setminus \{g_1, g_2, \ldots, g_i\}\big\}.$$

   2.2. Set $g_{i+1} = f(m_{i+1})$.

   2.3. Increment i to $i + 1$.

On the one hand, suppose we are at line 2.2 when this procedure is run. Then the loop condition tells us $A \setminus \{g_1, g_2, \ldots, g_i\} \neq \varnothing$. If $a_i \in A \setminus \{g_1, g_2, \ldots, g_i\}$, then $a_i = f(m)$ for some $m \in \{1,2,\ldots,n\}$ because f is a surjection $\{1,2,\ldots,n\} \to B$ and $A \subseteq B$. This says $\{m \in \{1,2,\ldots,n\} : f(m) \in A \setminus \{g_1, g_2, \ldots, g_i\}\} \neq \varnothing$. So m_{i+1} must exist by the Well-Ordering Principle.

On the other hand, by the choices of m_{i+1} and g_{i+1} on lines 2.2 and 2.1,

$$\text{each } g_{i+1} \in A \setminus \{g_1, g_2, \ldots, g_i\}. \tag{$*$}$$

Case 1: this procedure stops after finitely many steps. Then a run results in

$$m_1, m_2, \ldots, m_\ell \quad \text{and} \quad g_1, g_2, \ldots, g_\ell$$

where $\ell \in \mathbb{N}$. Define $g\colon \{1,2,\ldots,\ell\} \to A$ by setting $g(i) = g_i$ for all $i \in \{1,2,\ldots,\ell\}$.

Notice $A \setminus \{g_1, g_2, \ldots, g_\ell\} = \varnothing$ as the stopping condition is reached. This says any element of A is equal to some g_i, thus some $g(i)$. So g is surjective. We know g is injective by $(*)$.

As g is a bijection $\{1,2,\ldots,\ell\} \to A$, we deduce that A is finite.

Case 2: this procedure does not stop. Then a run results in

$$m_1, m_2, m_3, \ldots \quad \text{and} \quad g_1, g_2, g_3, \ldots.$$

Define $g\colon \mathbb{N} \to A$ by setting $g(i) = g_{i+1}$ for all $i \in \mathbb{N}$. As one can verify, this g is a bijection $\mathbb{N} \to A$. Recall that f is a bijection $\{1,2,\ldots,n\} \to B$. So Proposition 7.4.3 tells us f^{-1} is a bijection $B \to \{1,2,\ldots,n\}$. Define $h\colon \mathbb{N} \to \{1,2,\ldots,n\}$ by setting $h(i) = f^{-1}(g(i))$ for all $i \in \mathbb{N}$. This h is injective because, if $i, j \in \mathbb{N}$ such that $h(i) = h(j)$, then

$$\begin{array}{llr} & f^{-1}(g(i)) = f^{-1}(g(j)) & \text{by the definition of } h. \\ \therefore & g(i) = g(j) & \text{as } f^{-1} \text{ is injective.} \\ \therefore & i = j & \text{as } g \text{ is injective.} \end{array}$$

This contradicts Exercise 8.2.7. Therefore, this case is not possible. ☐

✎ 9c, page 77

Proof. As f is an injection $A \to B$, Exercise 8.2.5 implies that A has the same cardinality as $\operatorname{range}(f)$. Since A is infinite, Lemma 8.2.8 tells us $\operatorname{range}(f)$ is also infinite. Recall from Remark 7.2.3(2) that $\operatorname{range}(f) \subseteq B$. Hence B is infinite too by Proposition 9.2.6(1). ☐

✎ 9d, page 77

Given any function $f\colon A \to \mathcal{P}(A)$, we will produce an element of $\mathcal{P}(A)$ that is not equal to $f(x)$ for any $x \in A$. This will show that there is no surjection $f\colon A \to \mathcal{P}(A)$, and thus A cannot have the same cardinality as $\mathcal{P}(A)$.

Let $f\colon A \to \mathcal{P}(A)$. Define $R = \{x \in A : x \notin f(x)\}$. Then $R \in \mathcal{P}(A)$ by the definition of power sets. We claim that $R \neq f(x)$ for any $x \in A$. We prove this by contradiction. Suppose we have $a \in A$ such that $R = f(a)$. From the definition of R,

$$\forall x \in A \ \ \big(x \in R \quad \Leftrightarrow \quad x \notin f(x)\big). \tag{†}$$

As $R = f(a)$, applying (†) to $x = a$ gives

$$a \in f(a) \quad \Leftrightarrow \quad a \notin f(a). \tag{‡}$$

Split into two cases.

- Case 1: assume $a \in f(a)$. Then $a \notin f(a)$ by the $\Rightarrow$ part of (‡). This contradicts our assumption that $a \in f(a)$.
- Case 2: assume $a \notin f(a)$. Then $a \in f(a)$ by the $\Leftarrow$ part of (‡). This contradicts our assumption that $a \notin f(a)$.

In either case, we get a contradiction. This completes the proof of the claim and thus of the remark. □

✎ 9e, page 78

According to the definition of countability, we need to show that $\mathcal{P}(A)$ is infinite, and that $\mathcal{P}(A)$ does not have the same cardinality as $\mathbb{N}$.

Let $f\colon A \to \mathcal{P}(A)$ defined by setting $f(a) = \{a\}$ for each $a \in A$. Then f is injective because if $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$, then $\{a_1\} = \{a_2\}$, and thus $a_1 = a_2$ by the definition of set equality. As A is infinite, Corollary 9.2.7(1) tells us that $\mathcal{P}(A)$ is infinite too.

As A is countable and infinite, it must have the same cardinality as $\mathbb{N}$ by the definition of countability. However, Theorem 9.3.1 tells us A does not have the same cardinality as $\mathcal{P}(A)$. Thus $\mathcal{P}(A)$ cannot have the same cardinality as $\mathbb{N}$ by Proposition 8.2.4. □

✎ 10a, page 82

($\subseteq$) Let $x \in A \setminus B$. Then $x \in A$ and $x \notin B$ by the definition of $\setminus$. The latter implies $x \notin A$ or $x \notin B$. So it is not the case that x is both in A and in B by De Morgan's Laws. Thus the definition of $\cap$ tells us $x \notin A \cap B$. As $x \in A$, we deduce that $x \in A \setminus (A \cap B)$ according to the definition of $\setminus$.

($\supseteq$) Let $x \in A \setminus (A \cap B)$. Then $x \in A$ and $x \notin A \cap B$ by the definition of $\setminus$. In view of the definition of $\cap$, the latter implies that it is not the case that x is both in A and in B. So either $x \notin A$ or $x \notin B$ by De Morgan's Laws. As $x \in A$, we deduce that $x \notin B$. So $x \in A \setminus B$ by the definition of $\setminus$. □

✎ 10b, page 83

Let C be the set of all countable sets and I be the set of all infinite sets here. Note that all sets are either countable or infinite because finite sets are by definition countable. So $|C \cup I| = 40$. Also, by the Inclusion–Exclusion Rule,

$$\begin{aligned} |C \cup I| &= |C| + |I| - |C \cap I| \\ &= 12 + 31 - |C \cap I|. \end{aligned}$$

Hence, the number of sets that are both countable and infinite here is

$$|C \cap I| = 12 + 31 - |C \cup I| = 12 + 31 - 40 = 3.$$

✎ 10c, page 89

Define $\Gamma = \{\mathrm{B}, \mathrm{I}_1, \mathrm{C}, \mathrm{O}_1, \mathrm{N}_1, \mathrm{D}, \mathrm{I}_2, \mathrm{T}, \mathrm{I}_3, \mathrm{O}_2, \mathrm{N}_2, \mathrm{A}, \mathrm{L}\}$. In view of the General Multiplication Rule,

$$\begin{pmatrix}\text{number of}\\ \text{permutations}\\ \text{of } \Gamma\end{pmatrix} = \begin{pmatrix}\text{number of}\\ \text{permutations of}\\ \text{BICONDITIONAL}\end{pmatrix} \times \begin{pmatrix}\text{number of}\\ \text{ways to}\\ \text{arrange}\\ \mathrm{I}_1, \mathrm{I}_2, \mathrm{I}_3 \text{ into}\\ 3 \text{ positions}\end{pmatrix} \times \begin{pmatrix}\text{number of}\\ \text{ways to}\\ \text{arrange}\\ \mathrm{O}_1, \mathrm{O}_2 \text{ into}\\ 2 \text{ positions}\end{pmatrix} \times \begin{pmatrix}\text{number of}\\ \text{ways to}\\ \text{arrange}\\ \mathrm{N}_1, \mathrm{N}_2 \text{ into}\\ 2 \text{ positions}\end{pmatrix}.$$

$$\therefore \qquad 13! = \begin{pmatrix}\text{number of}\\ \text{permutations of}\\ \text{BICONDITIONAL}\end{pmatrix} \times 3! \times 2! \times 2! \qquad \text{by Corollary 10.3.7.}$$

From this, we see that the number of permutations of BICONDITIONAL is $\frac{13!}{3!\,2!\,2!} = 13!/24$.

✎ 11a, page 94

Note that, in G, there is no edge between the left vertices, and there is no edge between the right vertices. So vertices in a path in G must alternate between the left vertices and the right vertices. As 1 and 3 are both on the left, the length of the path between 1 and 3 must be even, and so be at least 2. So such a path must have length 2 or 4 because there are only 6 vertices in the graph, and paths cannot "use" the same vertex twice or more.

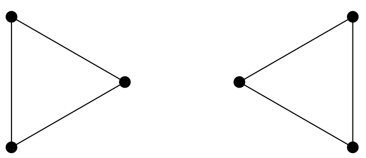
Case 1: consider those paths between 1 **and** 3 **of length** 2**.** There are 3 choices for the remaining vertex from $\{\mathrm{a}, \mathrm{b}, \mathrm{c}\}$. So there are exactly 3 such paths.

Case 2: consider those paths between 1 **and** 3 **of length** 4**.** Such a path contains one more left vertex and two more right vertices. This left vertex must be 2 because this is the only remaining vertex on the left. For the two right vertices, they can be any two distinct ones from $\{\mathrm{a}, \mathrm{b}, \mathrm{c}\}$, and order matters for these two vertices. So there are $P(3, 2) = 3 \times 2 = 6$ such paths.

In total, there are exactly $3 + 6 = 9$ paths between 1 and 3 in G.

✎ 11b, page 97

As one can verify exhaustively, (a) and (b) are drawings of connected graphs. It is clear that (d) is a drawing of graph that is not connected. That (c) is a drawing of a graph that is not connected can be more easily seen by redrawing the same graph as follows:



✎ 12a, page 103

- By splitting into a $\Rightarrow$ part and a $\Leftarrow$ part, we used Technique 3.2.9 to prove a biconditional proposition.
- We used Technique 3.2.3 to prove the $\Rightarrow$ part.
- The $\Leftarrow$ part is proved using contraposition, i.e., Technique 3.2.7.
- In the $\Leftarrow$ part, to prove that there is an edge e in G such that $(\mathrm{V}(G), \mathrm{E}(G) \setminus \{e\})$ remains connected, we produced a witness e; this is Technique 3.2.1.

- In the $\Leftarrow$ part, we split into two cases: one when $x_1x_k \notin \mathrm{E}(P)$, the other when $x_1x_k \in \mathrm{E}(P)$; this uses Technique 3.2.11.

- Etc.

✎ 12b, page 104

- We used Strong MI, i.e., Technique 3.2.23.

- In the base step, we used a proof by contradiction, i.e., Technique 3.2.16, to show that G does not have a loop.

- Etc.

✎ 12c, page 105

- We used an algorithmic proof, i.e., Technique 9.2.3, to produce a subgraph H_k of G $|\mathrm{V}(G)| = |\mathrm{V}(H_k)| = |\mathrm{E}(H_k)|$.

- Etc.

✎ 12d, page 108

- We used a counting argument here, i.e., Technique 10.3.16.

- Etc.

✎ 12e, page 108

- We used a counting argument here, i.e., Technique 10.3.16.

- Etc.