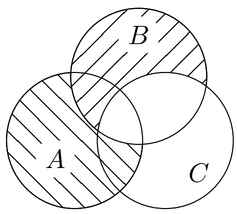
Answers to selected exercises

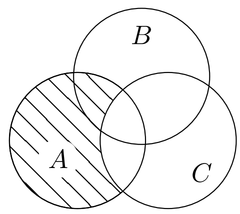
5a, page 3

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

5b, page 7



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



$A \setminus C$

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

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

6a, page 9

We show $\{|x| : x \in \mathbb{Q}\} = \mathbb{Q}_{\geqslant 0}$.

Proof. 1. $(\subseteq)$

- 1.1. Let $z \in \{|x| : x \in \mathbb{Q}\}$.
- 1.2. Find $x \in \mathbb{Q}$ such that $z = |x|$.
- 1.3. 1.3.1. Case 1: Suppose $x \geqslant 0$.
  - 1.3.2. Then $z = |x| = x \in \mathbb{Q}_{\geqslant 0}$ by the definition of $|\cdot|$.
- 1.4. 1.4.1. Case 2: Suppose $x < 0$.
  - 1.4.2. Then $z = |x| = -x$ by the definition of $|\cdot|$.
  - 1.4.3. As $x < 0$, we know $-x > 0$.
  - 1.4.4. As $x \in \mathbb{Q}$, we know $-x \in \mathbb{Q}$.
  - 1.4.5. Thus $z = -x \in \mathbb{Q}_{\geqslant 0}$.
- 1.5. In either case, we have $z \in \mathbb{Q}_{\geqslant 0}$.

2. $(\supseteq)$

- 2.1. Let $z \in \mathbb{Q}_{\geqslant 0}$.
- 2.2. Then the definition of $|\cdot|$ implies $z = |z| \in \{|x| : x \in \mathbb{Q}\}$. □

✎ 6b, page 9

We only show (1) here. The proof of (2) is similar.

Proof. 1. We know $\lfloor x \rfloor \in \mathbb{Z}$ by the definition of $\lfloor x \rfloor$.

2. As $\lfloor x \rfloor + 1 \in \mathbb{Z}$ and $\lfloor x \rfloor + 1 > \lfloor x \rfloor$, it follows from the largestness of $\lfloor x \rfloor$ that $\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1$.
3. Now let us show uniqueness: let $y \in \mathbb{Z}$ such that $y \leqslant x < y + 1$.
4. 4.1. Suppose $\lfloor x \rfloor < y$.
   4.2. Then $\lfloor x \rfloor + 1 \leqslant y$ as $\lfloor x \rfloor, y \in \mathbb{Z}$.
   4.3. This implies $x < \lfloor x \rfloor + 1 \leqslant y \leqslant x$ by line 2 and line 3, which is a contradiction.
5. So $\lfloor x \rfloor \geqslant y$.
6. Similarly, one shows $\lfloor x \rfloor \leqslant y$.
7. Thus $\lfloor x \rfloor = y$. $\square$

✎ 6c, page 9

It does not make f assign any value in the codomain $\mathbb{Q}$ to the element $1/2$ of the domain $\mathbb{Q}$. (Recall $2^{1/2} = \sqrt{2} \notin \mathbb{Q}$.)

✎ 6d, page 9

It does not make g assign any value in the codomain $\mathbb{Q}$ to the element -1 of the domain $\mathbb{Q}$.

✎ 6e, page 9

It makes $h(1/2) = 1 \neq 2 = h(2/4)$, although $1/2 = 2/4$.

✎ 6f, page 13

Only the top-middle, the bottom-left and the bottom-right diagrams represent functions. Of these, the first is a surjection but not an injection; the second is an injection but not a surjection; and the third is both an injection and a surjection. Thus only the last one is a bijection.

✎ 6g, page 14

The following are true statements:

$$g(0) = 0, \quad g(\{0\}) = \{0\}, \quad g^{-1}(\{0\}) = \{0\}.$$

Each of the following has a type mismatch error because there is a number on one side of the equation, and a set on the other side:

$$g(0) = \{0\}, \quad g(\{0\}) = 0, \quad g^{-1}(\{0\}) = 0.$$

The following refer to the inverse of g, which does not exist in view of Example 6.2.8 or Example 6.2.11, and Theorem 6.2.18:

$$g^{-1}(0) = 0, \quad g^{-1}(0) = \{0\}.$$

✎ 7a, page 19

On line 3.2.7, it is implicitly assumed that some participant stayed in the meeting throughout. This is not true when $k = 1$.

7b, page 23

$$\begin{aligned}
a_n &= a_{n-1} + n && \text{by the definition of } a_{n-1};\\
&= a_{n-2} + (n-1) + n && \text{by the definition of } a_{n-2};\\
&\;\vdots\\
&= a_1 + 2 + 3 + \cdots + (n-1) + n && \text{by the definition of } a_2;\\
&= 1 + 2 + 3 + \cdots + (n-1) + n && \text{by the definition of } a_1;\\
&= \frac{1}{2} n(n+1) && \text{by Example 7.1.3.}
\end{aligned}$$

7c, page 25

Structural induction over S. To prove that $\forall n \in S \;\; P(n)$ is true, where each $P(n)$ is a proposition, it suffices to:

(base step) show that $P(1)$ is true; and

(induction step) show that $\forall x \in S \;\; \big(P(x) \Rightarrow P(2x) \wedge P(3x)\big)$ is true.

One can show by structural induction over S that

$$S = \{2^a 3^b : a, b \in \mathbb{Z}_{\geqslant 0}\}.$$

Thus $9, 12 \in S$ but $10, 11, 13 \notin S$ because

$$\begin{array}{lll}
9 = 2^0 \times 3^2, & 12 = 2^2 \times 3^1, & \\
10 = 2^1 \times 5, & 11 = 11, & 13 = 13
\end{array}$$

when each of these numbers is written as a product of prime numbers. Here we implicitly use the Fundamental Theorem of Arithmetic when we claim that certain numbers here cannot be written as $2^a 3^b$ for any $a, b \in \mathbb{Z}_{\geqslant 0}$.

8a, page 28

This is a discussion question in Tutorial 6.

8b, page 28

This is a discussion question in Tutorial 6.

8c, page 32

$(10101010)_2 = 170$ and $(777)_8 = 511$ and $(\mathrm{ABC})_{16} = 2748$.

8d, page 32

$(b, n) = (7, 1231)$

$$\begin{array}{r|l}
7 & 1231 \\ \hline
7 & 175 \quad \text{—}\; 6 \quad \to a_0 \\ \hline
7 & 25 \quad \text{—}\; 0 \quad \to a_1 \\ \hline
7 & 3 \quad \text{—}\; 4 \quad \to a_2 \\ \hline
 & 0 \quad \text{—}\; 3 \quad \to a_3
\end{array}$$

So $1231 = (3406)_7$.

✎ 8e, page 34

Proof. 1. Let $q = m \underline{\text{div}}\, n$ and $r = m \underline{\text{mod}}\, n$, so that $m = nq + r$ and $0 \leqslant r < n$.

2. ("if")
   2.1. Suppose $\gcd(m, n) = n$.
   2.2. Then $n \mid m$.
   2.3. So $n \mid r$ by the Closure Lemma as $r = m - nq$.
   2.4. Note $|n| = n \not\leqslant r = |r|$ as $n, r \geqslant 0$.
   2.5. Thus the contrapositive of Proposition 8.1.10 tells us $m \underline{\text{mod}}\, n = r = 0$.
3. ("Only if")
   3.1. Suppose $r = 0$.
   3.2. Then $m = qn + 0 = qn$.
   3.3. Thus $n \mid m$ by the definition of divisibility.
   3.4. As $n \mid n$ by Example 8.1.6, this implies n is a common divisor of m and n.
   3.5. So $n \leqslant \gcd(m, n)$ by the greatestness of gcd.
   3.6. Since $\gcd(m, n) \mid n$ and $n > 0$, Proposition 8.1.10 tells us that

$$\gcd(m, n) = |\gcd(m, n)| \leqslant |n| = n.$$

   3.7. Hence $\gcd(m, n) = n$. □

✎ 8f, page 34

Example 8.1.7 tells us that every integer is a divisor of 0. As every integer is a common divisor of 0 and 0, there is no greatest one.

✎ 8g, page 34

Proof. 1. Suppose p is prime.

2. As $m, p > 0$, we know $\gcd(m, p)$ exists and is positive by Remark 8.4.4.
3. The primality of p tells us that $\gcd(m, p) = 1$ or $\gcd(m, p) = p$.
4. Case 1: suppose $\gcd(m, p) = 1$.
   4.1. Then we are done.
5. Case 2: suppose $\gcd(m, p) = p$.
   5.1. Then $m \underline{\text{mod}}\, p = 0$ by Exercise 8.4.3.
   5.2. Thus $m = pq + 0 = pq$, where $p = m \underline{\text{div}}\, p \in \mathbb{Z}$.
   5.3. So $p \mid m$. □

✎ 8h, page 34

Proof. 1. We first show that every common divisor of m and n is a common divisor of $|m|$ and $|n|$.
   1.1. Let $d \in \mathbb{Z}$ such that $d \mid m$ and $d \mid n$.
   1.2. Then $d \mid -m$ and $d \mid -n$ by Lemma 8.1.9.
   1.3. Thus $d \,\big|\, |m|$ and $d \,\big|\, |n|$ as $|m| \in \{m, -m\}$ and $|n| \in \{n, -n\}$ by the definition of $|\cdot|$.

2. Next we show that every common divisor of $|m|$ and $|n|$ is a common divisor of m and n.
   2.1. Let $d \in \mathbb{Z}$ such that $d \,\big|\, |m|$ and $d \,\big|\, |n|$.
   2.2. Recall that $|m| = m$ or $|m| = -m$ by the definition of $|\cdot|$.
   2.3. If $|m| = m$, then $d \mid m$ by the choice of d.
   2.4. If $|m| = -m$, then $d \mid -(-m) = m$ by the choice of d and Lemma 8.1.9.
   2.5. So $d \mid m$ in all cases.
   2.6. Recall that $|n| = n$ or $|n| = -n$ by the definition of $|\cdot|$.
   2.7. Similarly, if $|n| = n$, then $d \mid n$ by the choice of d.
   2.8. If $|n| = -n$, then $d \mid -(-n) = n$ by the choice of d and Lemma 8.1.9.
   2.9. So $d \mid n$ in all cases. □