How Many Elements?
For each of these, how many elements are in the set? If the set has infinitely many elements, say so.

(a) \( A = \{1, 2, 3, 2\} \)

\textit{Solution:} 3

(b) \( B = \{\emptyset, \{\emptyset\}, \{\emptyset\}, \{\}, \{\}, \{\}, \ldots\} \)

\textit{Solution:}

\[ B = \{\emptyset, \{\emptyset\}, \{\emptyset\}, \{\}, \{\}, \{\}, \ldots\} = \{\emptyset\} \]

So, there are two elements in \( B \).

(c) \( C = A \times (B \cup \{7\}) \)

\textit{Solution:} \( C = \{1, 2, 3\} \times \emptyset, \{\emptyset\}, 7\} = \{(a, b) \mid a \in \{1, 2, 3\}, b \in \emptyset, \{\emptyset\}, 7\} \). It follows that there are \( 3 \times 3 = 9 \) elements in \( C \).

(d) \( D = \emptyset \)

\textit{Solution:} 0.

(e) \( E = \{\emptyset\} \)

\textit{Solution:} 1.

(f) \( F = \mathcal{P}(\{\emptyset\}) \)

\textit{Solution:} \( 2^1 = 2 \). The elements are \( F = \emptyset, \{\emptyset\} \).

\textbf{Set = Set}

Prove the following set identities.
(a) Let the universal set be \( \mathcal{U} \). Prove \( \overline{X} = X \) for any set \( X \).

**Solution:** We want to prove that \( S = \overline{S} \).

\[
S = \{ x : x \in S \}
\]
\[
= \{ x : \neg(x \in S) \} \quad \text{[Negation]}
\]
\[
= \{ x : (x \notin S) \} \quad \text{[Definition of \( \notin \)]}
\]
\[
= \{ x : (x \notin \overline{S}) \} \quad \text{[Definition of \( \overline{S} \)]}
\]
\[
= \{ x : x \in \overline{S} \} \quad \text{[Definition of \( \overline{S} \)]}
\]
\[
= \overline{S}
\]

It follows that \( S = \overline{S} \).

(Note that if we did not have a universal set, this whole proof would be garbage.)

(b) Prove \( (A \oplus B) \oplus B = A \) for any sets \( A, B \).

**Solution:**

\[
(A \oplus B) \oplus B = \{ x : x \in (A \oplus B) \oplus B \} \quad \text{[Set Comprehension]}
\]
\[
= \{ x : (x \in A \oplus x \in B) \oplus (x \in B) \} \quad \text{[Definition of \( \oplus \)]}
\]
\[
= \{ x : x \in A \oplus (x \in B \oplus x \in B) \} \quad \text{[Associativity of \( \oplus \)]}
\]
\[
= \{ x : x \in A \oplus (F) \} \quad \text{[Definition of \( \oplus \)]}
\]
\[
= \{ x : x \in A \} \quad \text{[Definition of \( \oplus \)]}
\]
\[
= A \quad \text{[Set Comprehension]}
\]

(c) Prove \( A \cup B \subseteq A \cup B \cup C \) for any sets \( A, B, C \).

**Solution:** Let \( x \) be arbitrary.

\[
x \in A \cup B \quad \rightarrow \quad (x \in A \cup B) \vee (x \in C) \quad \text{[Definition of \( \cup \)]}
\]
\[
\quad \rightarrow \quad x \in (A \cup B) \cup C
\]

Thus, since \( x \in A \cup B \rightarrow x \in (A \cup B) \cup C \), it follows that \( A \cup B \subseteq A \cup B \cup C \), by definition of subset.

(d) Let the universal set be \( \mathcal{U} \). Prove \( A \cap \overline{B} \subseteq A \setminus B \) for any sets \( A, B \).

**Solution:** Let \( x \) be arbitrary.

\[
x \in A \cap \overline{B} \quad \rightarrow \quad x \in A \land x \in \overline{B} \quad \text{[Definition of \( \cap \)]}
\]
\[
\quad \rightarrow \quad x \in A \land x \notin B \quad \text{[Definition of \( \overline{B} \)]}
\]
\[
\quad \rightarrow \quad x \in A \setminus B \quad \text{[Definition of \( \setminus \)]}
\]

Thus, since \( x \in A \cap \overline{B} \rightarrow x \in A \setminus B \), it follows that \( A \cap \overline{B} \subseteq A \setminus B \), by definition of subset.
Casting Out Nines

Let $n \in \mathbb{N}$. Prove that if $n \equiv 0 \pmod{9}$, then the sum of the digits of $n$ is a multiple of 9.

Solution: Suppose $n \equiv 0 \pmod{9}$, where $n = (x_m x_{m-1} \cdots x_1 x_0)_{10}$ (This is because we are working with a base-10 number). Then, it follows that $\sum_{i=0}^{m} x_i 10^i \equiv 0 \pmod{9}$. Note that $10 \equiv 1 \pmod{9}$.

So, the previous summation is the same as $\sum_{i=0}^{m} x_i i \equiv 0 \pmod{9}$. Simplifying, we see that $\sum_{i=0}^{m} x_i \equiv 0 \pmod{9}$, which is what we were trying to prove.

Modular Arithmetic

(a) Prove that if $a \mid b$ and $b \mid a$, where $a$ and $b$ are integers, then $a = b$ or $a = -b$.

Solution: Suppose $a \mid b$ and $b \mid a$, where $a, b$ are integers. By definition of divides, we have $b = ka, a = jb$ for some integers $k, j$. Combining these equations, we see that $a = j(ka)$. We go by cases on if $a$ is zero or not.

Case 1: $a = 0$. Then, we have $b = k \cdot 0 = 0$. So, $a = b = 0$, and the theorem holds.

Case 2: $a \neq 0$. Then, dividing both sides by $a$, we get $1 = jk$. So, $\frac{1}{j} = k$. Note that $j$ and $k$ are integers, which is only possible if $j, k \in \{1, -1\}$. It follows that $b = -a$ or $b = a$, as required. Since the theorem is true in both cases, it is true.

(b) Prove that if $n \mid m$, where $n$ and $m$ are integers greater than 1, and if $a \equiv b \pmod{m}$, where $a$ and $b$ are integers, then $a \equiv b \pmod{n}$.

Solution: Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$. By definition of divides, we have $m = kn$ for some $k \in \mathbb{Z}$. By definition of congruence, we have $m \mid a - b$, which means that $a - b = mj$ for some $j \in \mathbb{Z}$. Combining the two equations, we see that $a - b = (knj) = n(kj)$. By definition of congruence, we have $a \equiv b \pmod{n}$, as required.