Type your answers to the following questions and submit a PDF file to Blackboard. One page per problem.

Problem 1. [5pts] Consider our definitions of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. Recall that $A \subseteq B$ means "A is a subset of B" and $A \not\subseteq B$ means "A is not a subset of B."

Prove that

(a) $\mathbb{Z} \subseteq \mathbb{Q}$,

Proof. Let $i \in \mathbb{Z}$ be an arbitrary integer. Then $\frac{i}{1}$ is a rational number in $\mathbb{Q}$, and $i = \frac{i}{1}$. □

(b) $\mathbb{Q} \not\subseteq \mathbb{Z}$,

Proof. $\frac{1}{2}$ is a rational number in $\mathbb{Q}$, but it is not an integer, so $\frac{1}{2} \notin \mathbb{Z}$. □

(c) $\mathbb{R} \not\subseteq \mathbb{Q}$,

Proof. $\sqrt{2}$ is a real number, but as we know from class it is irrational. □

(d) $\mathbb{R} \subseteq \mathbb{C}$,

Proof. Let x be a real number. Then $x + 0i$ is a complex number in $\mathbb{C}$, and $x = x + 0i$. □

and (e) $\mathbb{C} \not\subseteq \mathbb{R}$.

Proof. i is a complex number in $\mathbb{C}$, but $i = \sqrt{-1}$ and for every real number $x \in \mathbb{R}$, $x^2 \geq 0$, so since $i^2 < 0$, i is not a real number. □

(We would also accept that we know i is imaginary and not a real number, but giving a reason is always nice.)

Problem 2. [5pts] Prove that if $A \subseteq B$, then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Proof. Let $S \in \mathcal{P}(A)$ be an arbitrary element of $\mathcal{P}(A)$. By the definition of $\mathcal{P}(A)$, S is a subset of A. Therefore, for every element $x \in S$, the element x is also in A. Since $A \subset B$, the element $x \in A$ is also an element $x \in B$. Therefore, S is also a subset of B. Hence, S is an element of $\mathcal{P}(B)$ and $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. $\square$

Problem 3. [5pts] Let A and B be sets. Prove that $|A \cup B| = |A| + |B| - |A \cap B|$, using the following steps:

1. Prove that if E and F are disjoint sets (i.e. $E \cap F = \varnothing$) then $|E \cup F| = |E| + |F|$.

   Proof. Since $E \cap F = \varnothing$, each element of $E \cup F$ is in exactly one of E or F (not both). There are $|E|$ such elements that are in E and $|F|$ such elements that are in F. Thus, there are $|E| + |F|$ elements total in $E \cup F$. $\square$

2. Prove that $|A \cup B| = |A| + |B \setminus A|$.

   Proof. Note that $A \cap (B \setminus A) = \varnothing$. Therefore, by the previous part (with $E = A$ and $F = B \setminus A$), $|A \cup (B \setminus A)| = |A| + |B \setminus A|$. It remains to show that $A \cup (B \setminus A) = A \cup B$, which holds since

   $$A \cup (B \setminus A) = A \cup (B \cap \overline{A}) = (A \cup \overline{A}) \cap (A \cup B) = \mathcal{U} \cap (A \cup B) = A \cup B.$$

   $\square$

3. Prove that $|B \setminus A| = |B| - |A \cap B|$.

   Proof. Note that $|B \setminus A| = |B| - |A \cap B|$ if and only if $|B| = |B \cap A| + |B \setminus A|$. Since $(B \cap A) \cap (B \setminus A) = \varnothing$, we can apply the first part with $E = B \cap A$ and $F = B \setminus A$ to find that $|(B \cap A) \cup (B \setminus A)| = |B \cap A| + |B \setminus A|$. It remains to show that $B = (B \cap A) \cup (B \setminus A)$, but this holds since any element $x \in B$ is either in A or not in A, so it is in $B \cap A$ or $B \setminus A$. (You can also use Set Identities, if you want.) $\square$

4. Conclude that $|A \cup B| = |A| + |B| - |A \cap B|$.

   Proof. From previous parts, we see that

   $$|A \cup B| = |A| + |B \setminus A| = |A| + |B| - |A \cap B|.$$

   $\square$

Problem 4. [5pts] Let $\mathcal{U} = \{1, 2, 3, 4, 5, 6, 7\}$, $A = \{1, 3, 5, 7\}$, $B = \{4, 5, 6, 7\}$. Determine the following sets:

- $\overline{A} = \{2, 4, 6\}$
- $A \cap B = \{5, 7\}$
- $A \cup B = \{1, 3, 4, 5, 6, 7\}$
- $A \setminus B = \{1, 3\}$
- $A \triangle B = \{1, 3, 6\}$

Problem 5. [5pts] Let A and B be sets. Prove that $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$.

Proof. We prove both $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$ and $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$ to show equality.

($\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$) Let $S \in \mathcal{P}(A) \cap \mathcal{P}(B)$. Thus $S \in \mathcal{P}(A)$ and $S \in \mathcal{P}(B)$. By definition of the power set, S is a subset of A and S is a subset of B. Therefore, every element of S is an element of A and an element of B. Hence S is a subset of $A \cap B$ and by definition of the power set, $S \in \mathcal{P}(A \cap B)$.

($\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$) Let $S \in \mathcal{P}(A \cap B)$. By definition of the power set, S is a subset of $A \cap B$. So every element of S is in both A and B. Then S is a subset of A and a subset of B. By definition of the power set, S is in $\mathcal{P}(A)$ and in $\mathcal{P}(B)$. Therefore, $S \in \mathcal{P}(A) \cap \mathcal{P}(B)$. $\square$

Problem 6. [10pts] Let A, B, and C be subsets of a universe $\mathcal{U}$. Use definitions of set operations and set identities to prove the following equality of sets:

$$((B \cap A) \cup (B \cap C)) \setminus (A \cap B \cap C) = (B \cap (A \triangle C))$$

$$\begin{aligned}
&((B \cap A) \cup (B \cap C)) \setminus (A \cap B \cap C) & \\
&= (B \cap (A \cup C)) \setminus (A \cap B \cap C) & \text{Distributive law} \\
&= (B \cap (A \cup C)) \cap \overline{(A \cap B \cap C)} & \text{Definition of set difference} \\
&= (B \cap (A \cup C)) \cap (\overline{A} \cup \overline{B} \cup \overline{C}) & \text{DeMorgan's law} \\
&= B \cap ((A \cup C) \cap (\overline{A} \cup \overline{B} \cup \overline{C})) & \text{Associative law} \\
&= B \cap ((A \cap (\overline{A} \cup \overline{B} \cup \overline{C})) \cup (C \cap (\overline{A} \cup \overline{B} \cup \overline{C}))) & \text{Distributive law} \\
&= B \cap ((A \cap \overline{A}) \cup (A \cap \overline{B}) \cup (A \cap \overline{C})) \cup (C \cap \overline{A}) \cup (C \cap \overline{B}) \cup (C \cap \overline{C})) & \text{Distributive law} \\
&= B \cap (\varnothing \cup (A \cap \overline{B}) \cup (A \cap \overline{C}) \cup (C \cap \overline{A}) \cup (C \cap \overline{B}) \cup \varnothing) & \text{Complementation law} \\
&= B \cap ((A \cap \overline{B}) \cup (A \cap \overline{C}) \cup (C \cap \overline{A}) \cup (C \cap \overline{B})) & \text{Identity law} \\
&= B \cap ((A \cap \overline{B}) \cup (A \setminus C) \cup (C \setminus A) \cup (C \cap \overline{B})) & \text{Definition of set difference} \\
&= B \cap ((A \triangle C) \cup (A \cap \overline{B}) \cup (C \cap \overline{B})) & \text{Definition of symm. diff. and comm. law} \\
&= (B \cap (A \triangle C)) \cup (B \cap (A \cap \overline{B})) \cup ((B \cap (C \cap \overline{B}))) & \text{Distributive law} \\
&= (B \cap (A \triangle C)) \cup (B \cap \overline{B} \cap A) \cup (B \cap \overline{B} \cap A) & \text{Commutative and Associative laws} \\
&= (B \cap (A \triangle C)) \cup (\varnothing \cap A) \cup (\varnothing \cap A) & \text{Complementation laws} \\
&= (B \cap (A \triangle C)) \cup \varnothing \cup \varnothing & \text{Domination law} \\
&= B \cap (A \triangle C) & \text{Identity law}
\end{aligned}$$

Problem 7. [5pts] Let $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, and $C = \{\pi, \phi, i\}$. Define functions $f : A \to B$ and $g : B \to C$ as

$$f(x) = \begin{cases} 2 & x = a \\ 3 & x = b \\ 4 & x = c \end{cases} \quad g(x) = \begin{cases} \pi & x = 1 \\ \phi & x = 2 \\ i & x = 3 \\ \pi & x = 4 \end{cases}$$

Consider each of the functions f, g, $g \circ f$ and determine if they are injective, surjective, or both.

- f : injective, not surjective.

  Since $f(a) = 2$, $f(b) = 3$, and $f(c) = 4$, every element of the domain is mapped to a distinct element of the codomain, so f is injective.

  Since no element is mapped to $1 \in B$, f is not surjective.

- g : surjective, not injective.

  Since $g(1) = g(4) = \pi$, g is not injective.

  Since $g(2) = \phi$, $g(3) = i$, and $g(4) = \pi$, g is surjective.

- $g \circ f$: injective and surjective.

  Since $(g \circ f)(a) = g(2) = \phi$, $(g \circ f)(b) = g(3) = i$, and $(g \circ f)(c) = g(4) = \pi$, every element of the domain is mapped to a distinct element of the codomain, and every element of the codomain is the image of an element of the domain, $g \circ f$ is both injective and surjective.

Problem 8. [10pts] Consider the following function $f : \mathbb{N} \to \mathbb{Z}$:

$$f(n) = (-1)^n \left(\frac{n}{2} + \frac{1}{4}\right) - \frac{1}{4}.$$

1. [1pt] Write out the elements $f(0)$, $f(1)$, $f(2)$, $f(3)$, $f(4)$, $f(5)$.

$$f(0) = 0, \quad f(1) = -1, \quad f(2) = 1, \quad f(3) = -2, \quad f(4) = 2, \quad f(5) = -3, \ldots$$

From this part, you should notice that the output differs depending on if the input is even or odd.

2. [4pts] Prove that f is injective.

Proof. First, I claim that $f(n) < 0$ when n is odd and $f(n) \geq 0$ when n is even. If $n = 2k$ for some integer $k \geq 0$, then $f(2k) = (-1)^{2k}(2k/2+1/4)-1/4 = (k+1/4)-1/4 = k \geq 0$. If $n = 2k+1$ for some integer $k \geq 0$, then $f(2k+1) = (-1)^{2k+1}((2k+1)/2+1/4)-1/4 = -k-1/2-1/4-1/4 = -(k+1) < 0$.

Now, assume n and m are natural numbers such that $f(n) = f(m)$.

If $f(n) \geq 0$, then both n and m are even. Then $n = 2k$ and $m = 2\ell$ for nonnegative integers k and ℓ. Thus,

$$(2k/2 + 1/4) - 1/4 = f(2k) = f(n) = f(m) = f(2\ell) = (2\ell/2 + 1/4) - 1/4.$$

However, this implies that $k = \ell$ by simple algebra (1/4's cancel, $2/2 = 1$). So $n = m$.

If $f(n) < 0$, then both n and m are odd. Then $n = 2k + 1$ and $m = 2\ell + 1$ for nonnegative integers k and ℓ. Thus,

$$-(k+1) = -((2k+1)/2+1/4)-1/4 = f(2k) = f(n) = f(m) = f(2\ell+1) = -((2\ell+1)/2+1/4)-1/4 = -(\ell+1).$$

However, this implies that $k = \ell$, so $n = m$. Therefore f is injective. □

3. [5pts] Prove that f is surjective.

Proof. Let y be an arbitrary integer.

If $y \geq 0$, then let $x = 2y$. Note that $f(2y) = (-1)^{2y}(2y/2 + 1/4) - 1/4 = y$.

If $y < 0$, then let $x = 2|y|-1$. Note that $f(2|y|-1) = (-1)^{2|y|-1}((2|y|-1)/2+1/4)-1/4 = -|y| = y$. □

4. [+5pts] Describe a function $g : \mathbb{Z} \to \mathbb{Q}$ that is surjective (and prove it is surjective).

   There are many ways to do this, and almost all of them are gross. This is the cleanest version I can think of.

   We will describe an algorithm that will take as input an integer i and will output a rational number, and the output of this algorithm defines $g(i)$.

Algorithm: Input an integer i.

If $i = 0$, then output $0/1$.

If $i < 0$, then output $-g(-i)$, so we must only consider positive integers.

If $i > 0$, then consider the (unsigned) binary representation of i as $i = \sum_{j=0}^{k} a_j 2^j$ for some $(k+1)$-tuple $(a_k, a_{k-1}, \ldots, a_1, a_0)$. Since $i > 0$, we can assume that $a_k = 1$ (by making $k = \lceil \log_2 i \rceil$). Let q be the minimum integer such that either $q > k$ or $a_{k-q} = 0$. Thus, the binary representation of i starts with q 1-digits, then either stops, or has a 0-digit followed by $k - q - 1$ more digits. Let $p = \sum_{j=0}^{k-q} a_j 2^j$.

Output $\frac{p}{q}$.

We claim that for every rational number $\frac{p}{q} \in \mathbb{Q}$, there exists an integer i where the algorithm outputs a rational number equal to $\frac{p}{q}$ when given i. We will assume that $q > 0$, since $q \neq 0$ and if $q < 0$ we can use the rational number $\frac{-p}{-q} = \frac{p}{q}$.

If $p = 0$, then the algorithm outputs $\frac{0}{1} = \frac{p}{q}$ when given 0.

If $p > 0$, then let $\sum_{j=0}^{t} a_j 2^j$ be a binary representation of the integer p, defining a $(t+1)$-tuple $(a_t, a_{t-1}, \ldots, a_1, a_0)$. We can further assume that $t = \lceil \log_2 p \rceil + 1$, so $a_t = 0$. Then, for $j \in \{t + 1, \ldots, t + q\}$, define $a_j = 1$. Then, let $i = \sum_{j=0}^{t+q} a_j 2^j$ and notice that this binary representation of i starts with q 1-digits, a zero digit, then the binary representation of p. Therefore, the algorithm will output $\frac{p}{q}$ when given the input i (in fact, it will output the fraction in this form, with exactly this p and q pair.)

If $p < 0$, then consider the i that outputs $\frac{-p}{q}$ and the algorithm given input $-i$ will output $\frac{p}{q}$.