MATH 108 Fall 2019 - **Problem Set 6 solutions**

due November 8

1. For each pair of sets A and B, and subset $\Gamma \subseteq A \times B$ determine if Γ is the graph of a function from A to B. Justify your answer.

   (a) $A = B = \mathbb{R}$ and $\Gamma = \{(x, y) \in \mathbb{R}^2 \mid x = y^2\}$.
   No. Both $(1, 1)$ and $(1, -1)$ are in Γ.

   (b) $A = B = \mathbb{R}$ and $\Gamma = \{(x, y) \in \mathbb{R}^2 \mid y = x^2\}$.
   Yes. For each $x \in \mathbb{R}$, there is exactly one pair, (x, x^2), with first coordinate x.

   (c) $A = B = \mathbb{R}$ and $\Gamma = \{(x, y) \in \mathbb{R}^2 \mid y = \sqrt{x}\}$.
   No. There is no y such that $(-1, y) \in \Gamma$.

   (d) $A = B = \mathbb{Z}$ and $\Gamma = \{(n, 0) \mid n \in \mathbb{Z}\}$.
   Yes. For each $n \in \mathbb{Z}$, there is exactly one pair, $(n, 0)$, with first coordinate n.

   (e) $A = \mathbb{Z}$, $B = \{0\}$ and $\Gamma = \{(n, 0) \mid n \in \mathbb{Z}\}$.
   Yes. For each $n \in \mathbb{Z}$, there is exactly one pair, $(n, 0)$, with first coordinate n.

   (f) $A = B = \mathbb{Z}/5\mathbb{Z}$ and $\Gamma = \{(a, b) \mid a = \overline{2}b\}$.
   Yes. $\Gamma = \{(\overline{0}, \overline{0}), (\overline{2}, \overline{1}), (\overline{4}, \overline{2}), (\overline{1}, \overline{3}), (\overline{3}, \overline{4})\}$. There is exactly one pair with first coordinate equal to each element of $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

2. For each function f, determine if it is injective. If yes, find a *left-inverse* of f, which is a function g such that $g \circ f$ is the identity.

   (a) $f : \mathbb{R} \to \mathbb{R}^2$ defined by $f(x) = (x, x)$.
   Injective. Let $g : \mathbb{R}^2 \to \mathbb{R}$ be the function defined by $g(x, y) = x$.

   (b) $f : \mathbb{R}^2 \to \mathbb{R}$ defined by $f(x, y) = x + y$.
   Not injective. For example $f(0, 1) = f(1, 0) = 1$.

   (c) $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = 2x$.
   Injective. Let $g : \mathbb{Z} \to \mathbb{Z}$ be the function defined by $g(x) = x/2$ if x is even, and $g(x) = 0$ if x is odd.

   (d) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = e^x$.
   Injective. Let $g : \mathbb{R} \to \mathbb{R}$ be the function defined by $g(x) = \ln(x)$ if $x > 0$, and $g(x) = 0$ if $x \leq 0$.

   (e) $f : \mathbb{Z} \to \{0\}$ defined by $f(x) = 0$.
   Not injective. For example $f(0) = f(1) = 0$.

3. Let $f : A \to B$ and $g : B \to C$.

(a) Prove that if $g \circ f$ is injective then f is injective.

Assume that $g \circ f$ is injective and that $f(x) = f(y)$ for some $x, y \in A$. Applying g to both sides of the equation gives $g(f(x)) = g(f(y))$. Since $g \circ f$ is injective, we have $x = y$. Therefore f is injective.

(b) Give an example of f and g where $g \circ f$ is injective but g is not injective.

Let $A = C = \{1\}$ and $B = \{1, 2\}$. Define $f : A \to B$ by $f(1) = 1$ and $g : B \to C$ by $g(1) = g(2) = 1$. Then $g \circ f$ is the identity function on $\{1\}$, which is injective, but g is not injective.

4. Let S be a set with partial order $\sqsubseteq$ and T be a set with partial order $\preceq$. A function $f : S \to T$ is called *order-embedding* if it satisfies the property that $x \sqsubseteq y$ if and only if $f(x) \preceq f(y)$. Prove that if f is order-embedding then f injective.

Assume that f is order-embedding and that $f(x) = f(y)$ for some $x, y \in S$. Since the relation $\preceq$ on T is reflexive, we have $f(x) \preceq f(y)$ and $f(y) \preceq f(x)$. By the order-embedding property, this implies that $x \sqsubseteq y$ and $y \sqsubseteq x$. Then since the relation $\sqsubseteq$ on S is antisymmetric, it must be that $x = y$. Therefore f is injective.

5. Let a and m be integers with $0 < a < m$. Let $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ be the function defined by $f(\overline{x}) = \overline{a} \cdot \overline{x}$. Prove that f is injective if and only if $\gcd(a, m) = 1$.

For the forward direction, we proceed by contraposition. Assume that $\gcd(a, m) = d > 1$. We can write $m = dx$ where x is a positive integer with $x < m$, so $\overline{x} \neq \overline{0}$. Since a is divisible by d, we have ax divisible by $dx = m$, so

$$f(\overline{x}) = \overline{ax} = \overline{0} = f(\overline{0})$$

so f is not injective.

For the backward direction, assume that $\gcd(a, m) = 1$. Suppose that $f(\overline{x}) = f(\overline{y})$ for some integers x, y. Therefore

$$ax \equiv ay \pmod{m}.$$

We want to show that a can be canceled from both sides, to get $x \equiv y \pmod{m}$. Unfortunately we can't use the Cancellation Law or Euclid's Lemma since m is not necessarily prime.

By Bezout's Identity, there exist $s, t \in \mathbb{Z}$ such that $as + tm = 1$, so $as \equiv 1 \pmod{m}$. In other words, $\overline{s}$ is the multiplicative inverse of $\overline{a}$ in $\mathbb{Z}/m\mathbb{Z}$. So we have

$$sax \equiv say \pmod{m},$$

$$1 \cdot x \equiv 1 \cdot y \pmod{m}.$$

Therefore $\overline{x} = \overline{y}$, so f is injective.