Problem 1. *Let $f : A \to B$. Then:*

a) f is injective if and only if it has a left inverse.

b) f is surjective if and only if it has a right inverse.

c) f is bijective if and only if it has a left and right inverse.

d) If $|A| = |B| = n \in \mathbb{Z}_{\geq 0}$ then f is injective if and only if f is surjective if and only if f is bijective.

Proof.

a) Suppose that f is injective. This implies that $f^{-1}(f(a)) = \{a\}$ for all $a \in A$ since by the definition of injectivity if $f(a_0) = f(a_1)$ then $a_0 = a_1$. Define $g : B \to A$ as $g(b) = f^{-1}(a)$ where $b \in f(A)$. If $b \notin f(A)$ then send it to any arbitrary $a \in A$. Then $g \circ f(a) = f^{-1}(f(a)) = a$ which implies that $g \circ f = id_A$ and that g is a left inverse of f.

Now suppose that there exists a function $g : B \to A$ such that $g \circ f = id_A$. Let $a_0, a_1 \in A$ such that $f(a_0) = f(a_1)$. Then $g \circ f(a_0) = a_0 = a_1 = g \circ f(a_1)$ which is the definition of injectivity.

Therefore f is injective if and only if it has a left inverse.

b) Suppose that f is surjective. Then given $b \in B$ there exists an $a \in A$ such that $f(a) = b$. Define a function $g : B \to A$ via $g(b) = a$ where a fulfills $f(a) = b$. Then $f \circ g(b) = b$ by definition which implies that g is a right inverse of f.

Now suppose that there exists a function $g : B \to A$ such that $f \circ g = id_B$. Then given $b \in B$ let $a = g(b)$. Then $f(a) = f \circ g(b) = b$. Since this holds for all elements of b f is surjective.

Therefore f is surjective if and only if it has a right inverse.

c) Suppose that f is a bijection. Then it is both injective and surjective which by the previous statements in the proposition implies that f has both a left and right inverse.

Otherwise suppose that f has a left and right inverse. Then via the previous statements in the proposition we know that f is both injective and surjective and thus a bijection.

To show that the left and right inverse are unique let g, h be a left and right inverse for f respectively. Then

$$g = g \circ id_B = g \circ (f \circ h) = (g \circ f) \circ h = id_A \circ h = h$$

Therefore f is a bijection if and only if it has a left and right inverse. Moreover these inverses are equal.

d) Suppose that $|A| = |B| = 1$. Then there is only one function $f : A \to B$ defined as $f(a_0) = b_0$. As such the function f is injective, surjective and bijective.

Next assume for sets of size n that a function is injective if and only if it is surjective if and only if it is bijective. Let $|A| = |B| = n + 1$.

First consider the case where f is bijective. Then by definition f is also injective and surjective.

Next, if f is injective then take the pair (a_n, b_n), where $f(a_n) = b_n$. Since f is injective the restriction $f|_{a_n}$ will be well defined since no other element of A maps to b_n. However via our inductive hypothesis this implies that $f|_{A\setminus\{a_n\}}$ is also bijective and surjective. Reintroduce (a_n, b_n) to $f|_{A\setminus\{a_n\}}$ and this will maintain injectivity and surjectivity since no other element will map to b_n and b_n is mapped to by a_n.

Finally suppose that f is surjective. Then given any $b \in B$ we can find an $a \in A$ that maps to it. There must be at least one $b_i \in B$ such that $f^{-1}(b_i) = a_i$ since if the pullback for every element was greater than 1 we would have $|A| > 2|B|$ which contradicts our assumption. Now we can take the restriction $f_{A \setminus \{a_i\}}$ which will still be surjective. Which by our inductive hypothesis implies that $f_{A \setminus \{a_i\}}$ is injective and bijective. Reintroduce pair (a_i, b_i) to f and for the same reasoning as above we preserve injectivity, surjectivity, and bijectivity.

Therefore via induction, if $|A| = |B| = n \in \mathbb{Z}_{>0}$ then a function $f : A \to B$ is injective if and only if it is surjective if and only if it is bijective.

$\square$

Problem 2. *Let $\sim$ be an equivalence relation of the set A. For any $a, b \in A$,*

a) $a \sim b$ if and only if $\bar{a} = \bar{b}$.

b) if $\bar{a} \neq \bar{b}$, then $\bar{a} \cap \bar{b} = \phi$

Proof.

a) Suppose that $a \sim b$. Without loss of generality let $c \in \bar{a}$. Then $c \sim a$ which implies that $c \sim b$ by transitivity and as such $c \in \bar{b}$ Therefore if $a \sim b$ then $\bar{a} = \bar{b}$.

   Now suppose that $\bar{a} = \bar{b}$. Since $a \in \bar{a}$ and $b \in \bar{b}$ by reflexivity we know that $a, b \in \bar{b}$ and as such $a \sim b$.

   Therefore $a \sim b$ if and only if $\bar{a} = \bar{b}$.

b) Suppose that $\bar{a} \neq \bar{b}$ and that there existed a $c \in \bar{a} \cap \bar{b}$. Then $a \sim c$ and $c \sim b$ which would imply that $a \sim b$ by transitivity and that $\bar{a} = \bar{b}$ by the previous part of the proposition which is a contradiction.

   Therefore if $\bar{a} \neq \bar{b}$ then $\bar{a} \cap \bar{b} = \phi$

$\square$

Problem 3. *Let n be a fixed positive integer. Then*

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} | 1 \leq a \leq n \textit{ and } a, n \textit{ are relatively prime}\}$$

Proof. Let $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then $\bar{a}$ has a multiplicative inverse $\bar{\alpha}$ such that $\bar{a}\bar{\alpha} = \bar{1}$. This means that $a\alpha = kn + 1$ where $k \in \mathbb{Z}$. Rearrange and we get $\alpha a + kn = 1$ which implies that the $\gcd(a, n) = 1$.

Otherwise suppose that a, n are relatively prime. Then using the extended Euclidean algorithm we can get $\alpha, \beta \in \mathbb{Z}$ such that $\alpha a + \beta n = 1$. Rearrange to get $\alpha a = (-\beta)n + 1$ and rewrite mod n for $\bar{\alpha}\bar{a} = \bar{1}$ which implies that $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ $\square$