Solutions to Homework #9.

1. Problem 3(b)(d) from Section 5.2 (make sure to prove your answer)

Solution: In both parts of the problem we will denote the given relation simply as $\sim$ (ignoring the notations introduced in the book). Also, we will explicitly describe the equivalence class of each element, even though this was not formally asked in the book.

3(b): First we check that $\sim$ is an equivalence relation. Take any $(x, y) \in \mathbb{R} \times \mathbb{R}$. Since $x = x$, by definition we have $(x, y) \sim (x, y)$, so $\sim$ is reflexive.

Now take two points $(x, y), (z, w) \in \mathbb{R} \times \mathbb{R}$, and suppose that $(x, y) \sim (z, w)$. By definition this means $x = z$. But then also $z = x$ and hence $(z, w) \sim (x, y)$. Thus, $\sim$ is reflexive.

Finally, take three points $(x, y), (z, w), (u, v) \in \mathbb{R} \times \mathbb{R}$, and suppose that $(x, y) \sim (z, w)$ and $(z, w) \sim (u, v)$. By definition of $\sim$ this means $x = z$ and $z = u$. By transitivity of equality we get $x = u$ and hence $(x, y) \sim (u, v)$. Thus, $\sim$ is transitive.

Now we describe the equivalence classes. Fix a point $(a, b) \in \mathbb{R} \times \mathbb{R}$. By definition its equivalence class is

$$\begin{aligned}[(a, b)] &= \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid (x, y) \sim (a, b)\} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = a\} \\ &= \{\text{all points on the plane whose first coordinate is equal to } a\}.\end{aligned}$$

Geometrically, each equivalence class here is a vertical line.

3(d): Proof of the fact that $\sim$ is an equivalence relation is analogous to 3(b). Let us now describe the equivalence classes. Take any $(a, b) \in \mathbb{R} \times \mathbb{R}$. Then

$$[(a, b)] = \{(x, y) \in \mathbb{R}\times\mathbb{R} \mid (x, y) \sim (a, b)\} = \{(x, y) \in \mathbb{R}\times\mathbb{R} \text{ s.t. } |x+y| = |a+b|\}.$$

Since $|a + b| \geq 0$, the equality $|x + y| = |a + b|$ holds $\iff$ $x + y = |a + b|$ or $x + y = -|a + b|$. Each of the equations $x + y = |a + b|$ and $x + y = -|a + b|$ defines a line with slope -1 passing through the point $(a + b, 0)$ in the first case and $-(a + b, 0)$ in the second case. Note that if $a + b = 0$, the two lines are the same; otherwise they are different.

Thus, if $a + b \neq 0$, the equivalence class $[(a, b)]$ is the union of two lines with slope -1 passing through $(a + b, 0)$ and $-(a + b, 0)$, respectively. If $a + b = 0$, the equivalence class $[(a, b)]$ is the line with slope -1 passing through $(0, 0)$.

2. Define a relation $\sim$ on $\mathbb{Z}$ by $x \sim y \iff x^2 \equiv y^2 \mod 5$ (that is, $x \sim y \iff 5 \mid (y^2 - x^2)$). Prove that $\sim$ is an equivalence relation and describe the equivalence classes with respect to $\sim$: find the number of distinct equivalence classes and explicitly describe the elements in each class.

Solution: (1) reflexivity: For any x we have $x^2 - x^2 = 0$. Since $5 \mid 0$, we have $x \sim x$.

(2) symmetry: Take any $x, y \in \mathbb{Z}$, and suppose that $x \sim y$, so that $5 \mid (y^2 - x^2)$. By divisibility properties we have $5 \mid c(y^2 - x^2)$ for any $c \in \mathbb{Z}$. In particular, this is true for $c = -1$. Since $(-1)(y^2 - x^2) = x^2 - y^2$, we deduce that $5 \mid (x^2 - y^2)$ and hence $y \sim x$.

(3) transitivity. Take any $x, y, z \in \mathbb{Z}$, and suppose that $x \sim y$ and $y \sim z$, so that $5 \mid (y^2 - x^2)$ and $5 \mid (z^2 - y^2)$. Using the divisibility property $((c \mid a) \wedge (c \mid b)) \Rightarrow (c \mid (a + b))$, we get $5 \mid ((y^2 - x^2) + (z^2 - y^2)) = z^2 - x^2$, so $x \sim z$.

By definition for any $a \in \mathbb{Z}$ we have

$$[a] = \{x \in \mathbb{Z} \text{ s.t. } x \sim a\} = \{x \in \mathbb{Z} \text{ s.t. } a \sim x\} = \{x \in \mathbb{Z} \text{ s.t. } 5 \mid (x^2 - a^2)\}$$

(The second equality above holds since $\sim$ is symmetric).

Next observe that since $x^2 - a^2 = (x - a)(x + a)$, we have

$$5 \mid (x^2 - a^2) \iff 5 \mid (x - a) \text{ or } 5 \mid (x + a).$$

The "$\Rightarrow$" holds by Euclid's lemma (since 5 is prime) and "$\Leftarrow$" holds by the divisibility property "$(u \mid v) \Rightarrow (u \mid vw)\, \forall w \in \mathbb{Z}$". Thus,

$$\begin{aligned}
[a] &= \{x \in \mathbb{Z} \text{ s.t. } 5 \mid (x - a) \text{ or } 5 \mid (x + a)\} \\
&= \{x \in \mathbb{Z} \text{ s.t. } x - a = 5k \text{ or } x + a = 5k \text{ for some } k \in \mathbb{Z}\} \\
&= \{x \in \mathbb{Z} \text{ s.t. } x = 5k + a \text{ or } x = 5k - a \text{ for some } k \in \mathbb{Z}\}.
\end{aligned}$$

In particular, we get $[0] = \{\text{all multiples of } 5\}$;

$$\begin{aligned}
[1] &= \{\text{all integers of the form } 5k + 1 \text{ or } 5k - 1 \text{ with } k \in \mathbb{Z}\} \\
&= \{\text{all integers of the form } 5k + 1 \text{ or } 5k + 4 \text{ with } k \in \mathbb{Z}\}
\end{aligned}$$

(the set of all integers of the form $5k - 1$ with $k \in \mathbb{Z}$ is the same as the set of all integers of the form $5k + 4$ with $k \in \mathbb{Z}$ since we can write $5k - 1$ as $5(k - 1) + 4$ and $5k + 4$ as $5(k + 1) - 1$). Similarly,

$$\begin{aligned}
[2] &= \{\text{all integers of the form } 5k + 2 \text{ or } 5k - 2 \text{ with } k \in \mathbb{Z}\} \\
&= \{\text{all integers of the form } 5k + 2 \text{ or } 5k + 3 \text{ with } k \in \mathbb{Z}\}
\end{aligned}$$

From the above description we see that the classes $[0], [1]$ and $[2]$ are distinct and their union is the set of all integers (the division with remainder theorem tells us that any integer has the form $5k$, $5k+1$, $5k+2$, $5k+3$ or $5k+4$ for some $k \in \mathbb{Z}$). Since distinct equivalence classes cannot overlap, there is no room for any additional equivalence classes, so we have the total of 3 distinct equivalence classes: $[0], [1]$ and $[2]$.

3. For each of the following functions determine whether it is injective and whether it is surjective (include detailed justifications):

(a) $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$
(b) $f : \mathbb{R} \to \mathbb{R}_{\geq 0}$ given by $f(x) = x^2$
(c) $f : \mathbb{Q}_{\geq 0} \to \mathbb{Q}_{\geq 0}$ given by $f(x) = x^2$
(d) $f : \mathbb{R}_{\geq 0} \to [0, 1)$ given by $f(x) = \frac{x}{x+1}$. Here $[0, 1)$ is the half-open interval $\{x \in \mathbb{R} \mid 0 \leq x < 1\}$.

Solution: (a) Neither injective nor surjective. The function f is not injective since $1 \neq -1$ but $f(1) = f(-1) = 1$. The function f is not surjective since -1 lies in the codomain of f, but there is no $x \in \mathbb{R}$ such that $x^2 = -1$.

(b) Surjective, but not injective. The proof of non-injectivity is the same as in (a). For surjectivity note that this time the codomain is non-negative reals $\mathbb{R}_{\geq 0}$. If we take any $y \in \mathbb{R}_{\geq 0}$ and let $x = \sqrt{y}$ (which is defined since $y \geq 0$), then $f(x) = (\sqrt{y})^2 = y$. Thus, f hits every element in the codomain and thus f is surjective.

(c) Injective, but not surjective. Take any $a_1, a_2 \in \mathbb{Q}_{\geq 0}$ and suppose that $f(a_1) = f(a_2)$, so that $a_1^2 = a_2^2$. This means that $a_2 = \pm a_1$, but since a_1 and a_2 are both non-negative by assumption, we must have $a_2 = a_1$. Thus, $f(a_1) = f(a_2)$ implies $a_1 = a_2$ for all a_1, a_2 in the domain of f, so f is injective. The function f is not surjective since $\sqrt{2}$ is irrational and hence there is no $a \in \mathbb{Q}$ such that $a^2 = 2$ (in particular, no $a \in \mathbb{Q}_{\geq 0}$ such that $a^2 = 2$).

(d) Both injective and surjective. First we prove injectivity. Take any $a_1, a_2 \in \mathbb{R}_{\geq 0}$, and suppose that $f(a_1) = f(a_2)$, so that $\frac{a_1}{a_1+1} = \frac{a_2}{a_2+1}$. Cross multiplying, we get $a_1(a_2+1) = a_2(a_1+1)$, so $a_1a_2 + a_1 = a_1a_2 + a_2$ and hence $a_1 = a_2$.

Surjectivity: We need to show that for any $b \in [0, 1)$ there exists $a \in \mathbb{R}_{\geq 0}$ such that $\frac{a}{a+1} = b$; in other words, for any $b \in [0, 1)$ the equation $\frac{a}{a+1} = b$ can be solved for a with $a \in \mathbb{R}_{\geq 0}$.

Solving $\frac{a}{a+1} = b$, we get $a = (a+1)b = ab+b$, so $a(1-b) = b$ and $a = \frac{b}{1-b}$. Recall that by assumption $0 \leq b < 1$, so $0 < 1 - b \leq 1$. The inequalities

$b \geq 0$ and $1 - b > 0$ ensure that $\frac{b}{1-b} \geq 0$, so a defined by $a = \frac{b}{1-b}$ does lie in the domain of f. Let us now check that $f(a) = b$ for this a (which would complete the proof of surjectivity). We have

$$f(a) = f(\frac{b}{1-b}) = \frac{\frac{b}{1-b}}{\frac{b}{1-b} + 1} = \frac{b}{b + (1-b)} = b,$$

as desired.

4. Problem 5 in Section 6.1 (make sure to prove your answer)

Solution: The function f is not injective. For instance, $f(6) = f(2 \cdot 3) = 2 + 3 = 5 = f(5)$. We claim that f is surjective. By definition we need to show that for every $b \in \mathbb{N}$ there exists $n \in \mathbb{N}$ such that $f(n) = b$. We give a separate argument for b even and b odd.

Case 1: b is even. Then $b = 2k$ for some $k \in \mathbb{Z}$; moreover, $k \geq 1$ since $b \in \mathbb{N}$ by assumption. If we define $n = 2^k$, then $f(n) = \underbrace{2 + \ldots + 2}_{k \text{ times}} = 2k = b$.

Case 2: b is odd. Since $1 = f(1)$ and $3 = f(3)$, we can assume that $b \geq 5$. Let $k = \frac{b-3}{2}$ (note that $k \in \mathbb{N}$ since b is odd and $b \geq 5$). Then $b = 3 + 2k = 3 + \underbrace{2 + \ldots + 2}_{k \text{ times}}$ and hence $b = f(3 \cdot 2^k)$.

5. Problem 12 in Section 6.1.

Solution: (a) We need to show that for every $c \in C$ there exists $b \in B$ such that $g(b) = c$.

Take any $c \in C$. We are given that $g \circ f : A \to C$ is surjective, so there exists $a \in A$ s.t. $(g \circ f)(a) = c$, that is, $g(f(a)) = c$. Define $b = f(a)$. Then $b \in B$ (since f is a function from A to B) and $g(b) = c$, so b has required properties.

We now give an example showing that the converse fails. Let $A = \{1\}$, $B = C = \{1, 2\}$, and define $f : A \to B$ and $g : B \to C$ by $f(1) = 1$ and $g(b) = b$ for all $b \in B$. Then g is bijective, so in particular surjective, but $g \circ f$ is not surjective; in fact, there are no surjective functions from A to C since $|A| = 1 < 2 = |C|$.

(b) We need to show that for all $a_1, a_2 \in A$ the equality $f(a_1) = f(a_2)$ implies $a_1 = a_2$.

So suppose $a_1, a_2 \in A$ and $f(a_1) = f(a_2)$. Applying g to both sides, we get $g(f(a_1)) = g(f(a_2))$ or, equivalently, $(g \circ f)(a_1) = (g \circ f)(a_2)$. Since $g \circ f$ is injective by assumption, it follows that $a_1 = a_2$.

We now give an example showing that the converse fails. Let $A = B = \{1, 2\}$, $C = \{1\}$, and define $f : A \to B$ by $f(x) = x$ and $g : B \to C$ by $g(1) = g(2) = 1$. Then f is bijective, so in particular injective, but $g \circ f$

is not injective; in fact, there are no injective functions from A to C since $|A| = 2 > 1 = |C|$.

6. Let $f : A \to B$ be a function. Define a relation $\sim_f$ on A by $a \sim_f b \iff f(a) = f(b)$.

(a) Prove that $\sim_f$ is an equivalence relation

(b) Fix an integers $n \geq 2$, let $A = \mathbb{Z}$ and $B = \{0, 1, \ldots, n-1\}$. Construct a function $f : A \to B$ such that the equivalence classes with respect to the relation $\sim_f$ defined above are precisely the congruence classes mod n (that is, the equivalence classes with respect to $\equiv \mod n$). Your f should be given by a simple verbal description.

Solution: (a) The proof is analogous to Problem 1. In fact, both relations in Problem 1 are special cases of the relation described in this problem (in both cases we can take $A = \mathbb{R} \times \mathbb{R}$ and $B = \mathbb{R}$ with function $f : A \to B$ given by $f((x, y)) = x$ in Problem 3(b) and $f((x, y)) = |x + y|$ in Problem 3(d)).

Define $f : A \to B$ by $f(a) =$ the remainder of dividing a by n. From the first definition of congruences given in the book it is clear that the equivalence classes with respect to $\sim_f$ are precisely the congruence classes mod n.

7. Let A and B be non-empty finite sets, $n = |A|$ and $m = |B|$. Use the fundamental principle of counting to prove that

(a) The total number of functions from A to B is equal to m^n.

(b) The total number of injective functions from A to B is equal to $m(m-1)\ldots(m-n+1)$ if $m \geq n$ and is equal to 0 if $m < n$.

Solution: (a) Write $A = \{a_1, \ldots, a_n\}$. To define a function f from A to B we need to define $f(a_1), f(a_2), \ldots, f(a_n)$. Each of these values could be any element of B, so we have $m = |B|$ choices for $f(a_i)$ for each i (without any additional restrictions). By FPC, the number of choices for the sequence $(f(a_1), \ldots, f(a_n))$ is $\underbrace{m \cdot \ldots \cdot m}_{n \text{ times}} = m^n$.

(b) Again write $A = \{a_1, \ldots, a_n\}$. This time we have m choices for $f(a_1)$, $m-1$ choices for $f(a_2)$ (since $f(a_2)$ must be different from $f(a_1)$), $m-2$ choices for $f(a_3)$ (since $f(a_3)$ must be different from $f(a_1)$ and $f(a_2)$) etc. If $m \geq n$, we will $m-n+1$ choices for the last value $f(a_n)$ and hence the total number of ways to choose an injective function from A to B is $m(m-1)\ldots(m-n+1)$. If $m < n$, then we will have 0 choices for $f(a_{m+1})$, so there are no injective functions from A to B.