Homework Assignment 1

Selected Solutions

3. Let S and T be two sets, and $f : S \to T$ a function between them.

   (a) Show that f is bijective *if and only if* there exists a function $g : T \to S$ so that $g \circ f = \mathrm{id}_S$ and $f \circ g = \mathrm{id}_T$.

   Proof. Righthand Direction:

   Suppose f is bijective (that is, injective and surjective). We construct the inverse g. To describe g we say what it does to an element $t \in T$. Since f is surjective, there is some $s \in S$ so that $f(s) = t$. Furthermore, since f is injective, s is unique (if $f(s') = t$ then $s = s'$). We define $g(t) = s$.

   Applying f to both sides of the equation shows $f(g(t)) = g(s) = t$ by our choice of s, so that $f \circ g = \mathrm{id}_T$. In turn applying f shows $f(g(s)) = g(t) = s$ by the definition of g, so that $g \circ f = \mathrm{id}_S$. (Note to grader: They should show that $f \circ g$ and $g \circ f$ are the identity, but it is ok to use words, or even just say it is immediate by the definition of g if they define g correctly).

   Lefthand Direction:

   Assume there is an inverse g. We must show f is injective and surjective. For injectivity note if $f(x) = f(y)$, then $g(f(x)) = g(f(y))$, so that

   $$x = \mathrm{id}_T(x) = g(f(x)) = g(f(y)) = \mathrm{id}_T(y) = y.$$

   For surjectivity, fix $t \in T$. Then:

   $$t = \mathrm{id}_T(t) = g(f(t)).$$

   so that it is in the image of f. □

   (b) The function g constructed above is called the *inverse* of f and is sometimes denoted f^{-1}. Show that this terminology is justified by proving that g is *unique*. That is, show that if some other h served as an inverse for f then g.

   Proof. Assume there is some other h so that $h \circ f = \mathrm{id}_T$ and $f \circ h = \mathrm{id}_S$. We must show $h = g$. Note first that:

   $$g \circ f = \mathrm{id}_T = h \circ f.$$

   Now compose both sides of the equation above with g to so that $g \circ f \circ g = h \circ f \circ g$. But then:

   $$g = g \circ \mathrm{id}_S = g \circ f \circ g = h \circ f \circ g = h \circ \mathrm{id}_S = h.$$

   □

4. Show that equivalence relations are partitions are equivalent. Explicitly, let S be a set, construct a natural bijection between the partitions on S and the equivalence relations on S in the following way.

   (a) Let $\sim$ be an equivalence relation. Show that the equivalence classes of $\sim$ form a partition of S.

Proof. We must show the three conditions of partition hold.

(i) Let $\overline{a}$ be the equivalence class of a. Then it is nonempty because in particular it contains a (using that $a \sim a$ by reflexivity).

(ii) Fix $a \in S$. Then again by reflexivity $a \in \overline{a}$ so it is in some equivalence class. In particular, the union of the equivalence classes is all of S.

(iii) We must show that distinct equivalence classes of empty intersection. We first prove a helper result.

Lemma 1. *If $a \sim b$ then $\overline{a} = \overline{b}$.*

Proof. Suppose $c \in \overline{a}$. This means $c \sim a$. By transitivity $c \sim b$, and since $\sim$ is symmetric $b \sim c$. Therefore $c \in \overline{b}$ and so $\overline{a} \subseteq \overline{b}$. The reverse containment is identical. □

We will show the contrapositive, that is we will assume $\overline{a}$ and $\overline{b}$ have nonempty intersection, and deduce that they are equal. Suppose c lies in their intersection. Then $c \sim a$ and $c \sim b$. Since $\sim$ is symmetric and transitive $a \sim b$, and so by the Lemma $\overline{a} = \overline{b}$

□

(b) Conversely, let X_i be a partition of S. Show that the relation $\sim$ given by the rule

$$x \sim y \text{ if } x, y \in X_i \text{ for the same } i$$

is an equivalence relation for S.

Proof. We must show that the equivalence relation is reflexive, symmetric, and transitive.

(i) Fix any a. a is in some X_i since the X_i cover S so $a \sim a$. This shows reflexivity.

(ii) Fix a and b. If $a \sim b$ the $a, b \in X_i$ for the same i, but containment does not depend on order, so $b, a \in X_i$ as well. Thus $b \sim a$ showing that $\sim$ is symmetric.

(iii) Suppose $a \sim b$ and $b \sim c$. By the first assumption $a, b \in X_i$, and by the second $b, c \in X_j$. In particular $b \in X_i \cap X_j$, and since these sets form a partition $i = j$. In particular, $a, c \in X_i$ and $a \sim c$. This show transitivity and completes the proof.

□

6. Fix a nonzero integer $m \in \mathbb{Z}$. Show that congruence modulo m forms an equivalence relation on $\mathbb{Z}$.

Proof. We must show the relation is reflexive, symmetric, and transitive.

(i) Since $a - a = 0 = 0 \cdot m$ we have that $m|(a-a)$ so that $a \equiv a (\operatorname{mod} m)$.

(ii) Suppose $a \equiv b (\operatorname{mod} m)$. Then $m|(b-a)$. Therefore $m|(a-b)$ (indeed, if $b - a = km$ then $a - b = -km$), and so $b \equiv a (\operatorname{mod} m)$.

(iii) Suppose $a \equiv b (\operatorname{mod} m)$ and $b \equiv c (\operatorname{mod} m)$. Then $m|(b-a)$ and $m|(c-b)$. We've show that if m divides 2 things it divides their sum, so m divides $(b-a)+(c-b) = (c-a)$, and in particular $a \equiv b (\operatorname{mod} m)$.

□

7. Let a and b be integers. Show that $a^2 + b^2$ does not have a remainder of 3 when divided by four. (Hint: First show that the squares of elements in $\mathbb{Z}/4\mathbb{Z}$ are just $\overline{0}$ and $\overline{1}$.)

Proof. The congruence classes in $\mathbb{Z}/4\mathbb{Z}$ are $\overline{0}, \overline{1}, \overline{2}, \overline{3}$. Their squares are

$$\begin{aligned} & \overline{0} \\ \overline{1}^2 = & \overline{1} \\ \overline{2}^2 = \overline{4} = & \overline{0} \\ \overline{3}^2 = \overline{9} = & \overline{1} \end{aligned}$$

Therefore, modulo 4, $a^2 + b^2$ is one of:

$$\begin{aligned} \overline{0} + \overline{0} = & \overline{0} \\ \overline{0} + \overline{1} = & \overline{1} \\ \overline{1} + \overline{0} = & \overline{1} \\ \overline{1} + \overline{1} = & \overline{2} \end{aligned}$$

none of which are $\overline{3}$. $\square$

8. Let p be a prime number. Show that the product of two nonzero elements in $\mathbb{Z}/p\mathbb{Z}$ is again nonzero.

Proof. Recall that $\overline{a}\mathbb{Z}/m\mathbb{Z}$ is 0 if and only if $m|a$. We will show the contrapositive. Fix $\overline{a}$ and $\overline{b}$ in $\mathbb{Z}/p\mathbb{Z}$. If $\overline{ab} = 0$ then $p|ab$. Since p is prime, this means that $p|a$ or $p|b$. Therefore $\overline{a} = 0$ or $\overline{b} = 0$. $\square$