Homework Assignment 1

Due: Friday, January 28

1. Let S and T be sets, and suppose that $T \subseteq S$. Describe the following sets, proving the correctness of your answers.
   In (a) and (b) we use the following obvious fact, which we will call **Fact 1**. If $T \subseteq S$, then $x \in T$ implies $x \in S$.

   (a) $T \cap S$.

   Proof. Notice that $x \in T$ and $x \in S$ if and only if $x \in T$. Indeed, the righthand direction is trivial and the lefthand direction is precisely Fact 1. Therefore $T \cap S = T$. □

   (b) $T \cup S$.

   Proof. Observe that $x \in T$ or $x \in S$ if and only if $x \in S$. Indeed, the lefthand direction is trivial and the righthand direction is Fact 1. Therefore $T \cup S = S$. □

   (c) $T \cap (S \setminus T)$

   Proof. If $x \in S \setminus T$, then $x \notin T$, so that nothing can be in both T and $S \setminus T$. Therefore the intersection is empty: $T \cap (S \setminus T) = \emptyset$. □

   (d) $T \cup (S \setminus T)$.

   Proof. Let x be any element of S. Then x is either in T ($x \in T$), or it isn't ($x \in S \setminus T$). Therefore the union is all of S: $T \cup (S \setminus T) = S$. □

2. Let S be a set with 3 elements (say $\{0,1,2\}$) and T be a set with 5 elements (say $\{a,b,c,d,e\}$).

   (a) Give an example of an injection $f : S \to T$.

   Proof. Let $f(0) = a, f(1) = b, f(2) = c$. Since all 3 elements of S map to different elements of T, this map is injective. □

   (b) Give an example of a surjection $g : T \to S$.

   Proof. Let $g(a) = 0, g(b) = 1, g(c) = g(d) = g(e) = 2$. Since all 3 elements of S are in the image of g, this map is surjective. □

   (c) Can there be a bijection between S and T? Why or why not?

   Proof. No there cannot be any. Indeed, if $f : S \to T$ is any map, it can only have at most 3 elements of T in its image, so it cannot possibly hit all 5. □

3. A subset $T \subset S$ is called a *proper subset* if $T \neq S$. This is often denoted $T \subsetneq S$. Give an example of a set S and a bijection between S and a *proper* subset of S.

Proof. We see from 2(c) that this cannot possibly be true for finite sets, so we must pass to infinite sets. We give one such example, but there are many many others.

Let $\mathbb{N} = \{1, 2, 3, \cdots\}$ be the natural numbers, and let $2\mathbb{N} = \{2, 4, 6, 8, \cdots\}$. Then certainly $2\mathbb{N} \subsetneq \mathbb{N}$. Then let $f : \mathbb{N} \to 2\mathbb{N}$ be the multipliction by 2 function $f(x) = 2x$. Bijectivity is obvious: for injectivity notice that if $x \neq y$ then $2x \neq 2y$, and for surjectivity observe that every even number is 2 times some number. (Alternatively, one could see that the inverse is clearly given by division by 2, and then appeal to 4(c)). □

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

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

Proof. Suppose f has a left inverse $g : T \to S$ we will show injectivity. Let $x, y \in S$, and suppose that $f(x) = f(y)$. Therefore $g(f(x)) = g(f(y))$. But $g \circ f$ is the identity function, so $x = y$ proving injectivity.

Conversely, suppose f is injective. We construct a left inverse $g : T \to S$. For $t \in T$, we need to say what g does to t. There are two cases to consider:

(i) If $t = f(s)$ for some s: the we define $g(t) = s$ (this is well defined because if t also equals $f(s')$ for some s', the injectivity of f shows that $s = s'$ to begin with).

(ii) If $t \neq f(s)$ for any s: then any element of $s_0 \in S$ will do, just define $g(t) = s_0$ (for the attentive reader: here is where we use nonemptyness of S). We then observe that $g(f(s)) = s$ by definition, so that $g \circ f = \mathrm{id}_S$ and therefore g is indeed a left inverse. □

(b) Show that f is surjective if and only if it has a right inverse

Proof. Let $g : T \to S$ be a right inverse of f. We will show surjectivity. Let $t \in T$. Then $t = f(g(t))$ since g is a right inverse, so that t is in the image of f. This proves surjectivity.

Conversely, we define a right inverse to f as follows. Let $t \in T$. We must define what g does to t. Since f is surjective, $t = f(s)$ for some $s \in S$. Choose any such s, and define $g(t) = s$. Then $f(g(t)) = f(s) = t$ by definition and indeed g is a right inverse. □

(c) Show that f is bijective if and only if it has an inverse.

Proof. Suppose that $g : T \to S$ is a two sided inverse for f. Then it is a left inverse—proving the injectivity of f by part (a)—and a right inverse—proving the surjectivity of f by part (b)—so we are done, so f is bijective.

Conversely, suppose f is bijective. Then it has a left inverse $g_\ell : S \to T$ by part (a) and a right inverse $g_r : S \to T$ by part (b). If we show that $g_\ell = g_r$, then it must be a two sided inverse. Fix $t \in T$. Then $t = f(g_r(t))$. But since g_ℓ is a left inverse, applying it to both sides gives:

$$g_\ell(t) = g_\ell(f(g_r(t)) = g_r(t).$$

□

(d) Show that if f has a (two-sided) inverse, that inverse is unique.

Proof. In fact, the same proof as the second paragraph of part 2 works, letting g_ℓ and g_r be two inverses to f. □

Remark. *Because of part (c) and (d) of the question 4, we see that if f is bijective, then f has a unique inverse, which we call the inverse of f and denote by f^{-1}.*

5. Let S and T be finite sets and suppose that $|S| = |T|$. Let $f : S \to T$ be a function. Prove that

$$f \text{ is injective } \Leftrightarrow f \text{ is surjective } \Leftrightarrow f \text{ is bijective.}$$

Proof. Let $|S| = |T| = n$. We begin by showing that if f is injective if and only if f is surjective. First assume f is injective. Then, since every element of S must be mapped under f to a different element of T, that the image of f must contain at least n elements. Since T has only n elements, the image of f must be all of T. Contrapositively, suppose f is not injective. In particular, we know $f(x) = f(y)$ for some $x \neq y$ in S. But this means that the image of f can contain at most $n - 1$ elements, and therefore f cannot be surjective.

It remains to show that f is surjective if and only if it is bijective. If f is surjective, we know by the previous paragraph that it must be injective as well, so it is bijective. Conversely, if f is bijective it is surjective by definition, and we are done. □

6. 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 have 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 show the 3 conditions for being an equivalence relation hold.

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.

□

(c) Show that parts (a) and (b) give a bijection between the sets:

$$\{\text{Equivalence relations on } S\} \longleftrightarrow \{\text{Partitions of } S\}.$$

(Hint: Part (a) gives a function from the left to the right. Part (b) gives a function from the right to the left. Show that these are inverses to eachother).

Proof. Denote by $f : \{\text{Equivalence relations on } S\} \to \{\text{Partitions of } S\}$ the function from part (a) taking equivalence classes, and let $g : \{\text{Partitions of } S\} \to \{\text{Equivalence relation on } S\}$ be the function from part (b) building an equivalence relation out of a partition. The goal is to show that $f \circ g$ and $g \circ f$ are both the identity function.

Let's begin with $f \circ g$. We start with a partition $\{X_i\}$, for an equivalence class $\sim$ based on this partition, and then take the equivalence classes $\{[a]\}$ of this relation. For this to be the identity is saying that these two partitions are actually the same partition, that is: $\{X_i\} = \{[a]\}$. This follows from the following observation. If $a \in X_i$, then $X_i = [a]$. Indeed, $[a] = \{b : b \sim a\}$. But by the definition of $\sim$, $b \sim a$ if and only if $b \in X_i$. So $[a] = X_i$. Therefore the equivalence classes are of $\sim$ are precisely the elements of the partition we started with.

We next show that $g \circ f$ is the identity. We start with an equivalence relation $\sim$, take its equivalence classes $\{[a]\}$, and then form an equivalnece relation $\sim'$ from this partition as in part (b). Then $a \sim b$ if and only if $b \in [a]$ if and only if $a \sim' b$, and so $\sim$ and $\sim'$ are the same equivalence relation. □

7. Let $a, b, c \in \mathbb{Z}$. Prove the following divisibility facts.

(a) If $a|b$ and $a|c$ then $a|(b + c)$

Proof. We know $b = ka$ and $c = \ell a$. Thus $b + c = ka + \ell a = (k + \ell)a$ and we win. □

(b) If $a|b$ then $a|bc$.

Proof. We know $b = ka$. So $bc = kac = (kc)a$ and we win. □

8. In this exercise we prove the existence and uniqueness of division with remainder. Let $a, b \in \mathbb{Z}$, and suppose that $b \neq 0$. We start with existence.

(a) We begin by considering the set of numbers $a - bq$ as q varies over the integers. Prove that the set

$$S = \{a - bq : q \in \mathbb{Z}\},$$

has at least one nonnegative element.

Proof. The goal is to show that there is some q with $a - bq \geq 0$. Solving for q gives $q \geq (a/b)$ if $b \geq 0$ or $q \leq (a/b)$ if $b \leq 0$. In each case we can find some $q \in \mathbb{Z}$ satisfying the inequality. □

(b) Let r be the minimal nonnegative element of S. Show that $0 \leq r < |b|$.

Proof. By assumption $r \geq 0$ and $r = a - bq$ for some q. Suppose $r \geq |b|$. Then

$$r - |b| = a - bq - |b| = a - b(q \pm 1)$$

is another nonnegative element of S, and it is smaller than r, contradicting the minimality of r. So we cannot have $r \geq |b|$ completing the proof. □

(c) Use (b) to conclude that $a = bq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < |b|$. This proves existence.

Proof. Letting $r = a - bq$ be the minimal element of the set, then $a = bq + r$ and by the previous exercise $0 \leq r < |b|$. □

(d) Show that the division with remainder from part (c) is unique. That is, suppose there are $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that

$$a = bq_1 + r_1 \quad \text{and} \quad a = bq_2 + r_2.$$

Suppose further that $0 \leq r_i < |b|$ for $i = 1, 2$. Then show $q_1 = q_2$ and $r_1 = r_2$.

Proof. Perhaps swapping 1 and 2 we may assume without loss of generality that $r_1 \geq r_2$. The equation $bq_1 + r_1 = bq_2 + r_2$ can be rewritten as

$$r_1 - r_2 = b(q_2 - q_1).$$

Therefore $r_1 - r_2$ is a multiple of b, and $0 \leq r_1 - r_2 < |b|$, so the only possibility is that $r_1 - r_2 = 0$ and we have $r_1 = r_2$. Subbing into the equation above gives:

$$0 = b(q_2 - q_1),$$

and since $b \neq 0$ we have $q_2 - q_1 = 0$ so that $q_2 = q_1$. □

9. In this exercise we prove the Euclidean algorithm works.

(a) Suppose $a, b \in \mathbb{N}$ are two positive integers, and let $a = bq + r$ for $0 \leq r < b$ (as in the previous exercise). Show that:

$$\gcd(a, b) = \gcd(b, r).$$

Proof. If we can prove that the common divisors of a and b agree with the common divisors of b and r, then they will certainly share the greatest one. Therefore we show this.
Suppose $d|a$ and $d|b$. Then (by problem 7) $d|(a-bq)$ which is r, and therefore is a common divisor of b and r. Conversely, if $d|b$ and $d|r$, then $d|(bq+r)$ which is a so it is a common divisor of b and a. □

(b) Let $a \neq 0$ be an integer. What is $\gcd(a, 0)$? Justify your answer.

Proof. Notice that any $d|0$, since $d \cdot 0 = 0$. Therefore the common divisors of a and 0 are just the divisors of a, of which $|a|$ is plainly the largest one. □

(c) Prove the correctness of the Euclidean algorithm. That is, suppose $a, b \in \mathbb{N}$ are two positive integers, and suppose you iterate the division algorithm as follows:

$$\begin{aligned} a &= bq_0 + r_0 && 0 \leq r_0 < b \\ b &= r_0 q_1 + r_1 && 0 \leq r_1 < r_0 \\ r_0 &= r_1 q_2 + r_2 && 0 \leq r_2 < r_1 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n && 0 \leq r_n < r_{n-1} \\ r_{n-1} &= r_n q_{n+1}. \end{aligned}$$

Show that $\gcd(a, b) = r_n$.

Proof. Applying parts (a) and (b) we see that:

$$\gcd(a, b) = \gcd(b, r_0) = \gcd(r_0, r_1) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n.$$

□

10. Let d be the greatest common divisor of 792 and 275. Using Euclid's algorithm, find d and write $d = 792x + 275y$ for some x and y.

Proof.

$$\begin{aligned} 792 &= 275 * 2 + 242 \\ 275 &= 242 * 1 + 33 \\ 242 &= 33 * 7 + 11 \\ 33 &= 11 * 3 + 0 \end{aligned}$$

Therefore $\gcd(792, 275) = 11$. Working our way up we see:

$$\begin{aligned} 11 &= 242 - 33 * 7 \\ &= 242 - (275 - 242) * 7 \\ &= 242 * 8 - 275 * 7 \\ &= (792 - 275 * 2) * 8 - 275 * 7 \\ &= 792 * 8 - 275 * 23. \end{aligned}$$

□