Review for Exam 2

1. Sample problems

Problem 1:

a. Give an example of a function $f : \mathbb{Z} \to \mathbb{Z}$ which is injective but not surjective.

b. Give an example of a function $g : \mathbb{Z} \to \mathbb{Z}$ which is surjective but not injective.

Solution for 1a:
Let $f : \mathbb{Z} \to \mathbb{Z}$ be given by the rule $f(x) = 2x$. The image of f is the set of even integers, which is a proper subset of $\mathbb{Z}$; thus f is not surjective. But f is injective: if $x, x' \in \mathbb{Z}$ and $f(x) = f(x')$ then $2x = 2x'$. Cancellation of the factor 2 then implies that $x = x'$. This demonstrates that f is injective.

Solution for 1b:
Let $g : \mathbb{Z} \to \mathbb{Z}$ be given by the rule

$$g(x) = \begin{cases} x \text{ if } x \geq 0 \\ x+1 \text{ if } x < 0 \end{cases}.$$

Note that $g(0) = g(-1) = 0$; this shows that g is *not injective*. On the other hand, let $y \in \mathbb{Z}$. If $y \geq 0$ then $y = g(y)$ while if $y < 0$ then $y = g(y-1)$. This shows that g is *surjective*.

Problem 2: We have seen that for finite sets A and B, we have

$$(\heartsuit) \quad |A \cup B| = |A| + |B| - |A \cap B|.$$

Now, let A, B, C be finite sets.

a. Suppose that

$$|A \cup B \cup C| = |A| + |B| + |C|.$$

Prove that $A \cap B = \emptyset$, $A \cap C = \emptyset$ and $B \cap C = \emptyset$.

b. If $A \cap B \cap C = \emptyset$, is it true that $|A \cup B \cup C| = |A| + |B| + |C|$? Justify your response with a proof or a counter-example.

Solution for 2a:
Note that $A \cup B \cup C = A \cup (B \cup C)$. Thus (♥) shows that

$$|A \cup B \cup C| = |A| + |B \cup C| - |A \cap (B \cup C)|.$$

Another application of (♥) shows that $|B \cup C| = |B| + |C| - |B \cap C|$.

Thus we find

$$|A \cup B \cup C| = |A| + |B| + |C| - |B \cap C| - |A \cap (B \cup C)|.$$

Since $|A \cup B \cup C| = |A| + |B| + |C|$ by hypothesis, and since for any finite set, $|X|$ is non-negative, we now deduce that $|B \cap C| = 0$ and $|A \cap B \cup C| = 0$. In particular, $B \cap C = \emptyset$.

Now, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. A further application of (♥) now shows that

$(*)$ $\quad 0 = |A \cap (B \cup C)| = |(A \cap B) \cup (A \cap C)| = |A \cap B| + |A \cap C| - |(A \cap B) \cap (A \cap C)|.$

Since $B \cap C = \emptyset$, we know that $(A \cap B) \cap (A \cap C) = \emptyset$. Thus $(*)$ shows that

$$0 = |A \cap B| + |A \cap C|.$$

Thus $A \cap B = A \cap C = \emptyset$ as required.

Solution for 2b:
It is not true that $A \cap B \cap C = \emptyset \Rightarrow |A \cup B \cup C| = |A| + |B| + |C|$.

Indeed, let $A = \{1, 2\}, B = \{2, 3\}, C = \{3, 4\}$. Then $A \cap B \cap C = \emptyset$. But $A \cup B \cup C = \{1, 2, 3, 4\}$ so that

$$|A \cup B \cup C| = 4 < 6 = |A| + |B| + |C|.$$

Problem 3: Let S be a finite set having $n \in \mathbb{N}$ elements, let $d \in \mathbb{N}$.

A sequence of elements of S of length d is a list $a_0, a_1, \ldots, a_{d-1}$ where $a_j \in S$ for each j.

Let $T_{\leq d}$ be the set of all sequences of elements of S of length $\leq d$.

Give an expression for the cardinality $|T_{\leq d}|$ in terms of d and n.

Solution for 3:
The number of sequences of elements of S of length equal to d is given by n^d, since there are n choices for each of the d entries in the sequence.

Now, $|T_{\leq d}| = \sum_{i=1}^{d} n^i$.

Problem 4: Let $f : X \to Y$ be a function. Define a relation $\sim$ on X by the rule: $x \sim x'$ if and only if $f(x) = f(x')$.

a. Show that $\sim$ is an equivalence relation.

b. For $x \in X$, show that the equivalence class $[x]$ is equal to $f^{-1}(f(x))$.

Solution for 4:

a.
- reflexive: If $x \in X$, then $f(x) = f(x) \Rightarrow x \sim x$.
- symmetric: For $x, y \in X$, $x \sim y \Rightarrow f(x) = f(y) \Rightarrow f(y) = f(x) \Rightarrow y \sim x$.
- transitive: For $x, y, z \in X$,

$$\begin{aligned} x \sim y \text{ and } y \sim z &\Rightarrow f(x) = f(y) \text{ and } f(y) = f(z) \\ &\Rightarrow f(x) = f(z) \Rightarrow x \sim z. \end{aligned}$$

b. Recall that $[x] = \{z \in X \mid x \sim z\}$ and $f^{-1}(f(x)) = \{z \in X \mid f(x) = f(z)\}$.

We now see that $[x] = f^{-1}(f(x))$. Indeed, for $z \in X$ we have

$$z \in [x] \Leftrightarrow x \sim z \Leftrightarrow f(x) = f(z) \Leftrightarrow z \in f^{-1}(f(x)).$$

Problem 5: Let $n \in \mathbb{N}$ and write $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$. For $(a, b), (a', b') \in \mathbb{Z}^2$ we consider the relation

$$(a, b) \equiv (a', b') (\mathrm{mod}\, n) \text{ provided that } a \equiv a' (\mathrm{mod}\, n) \text{ and } b \equiv b' (\mathrm{mod}\, n).$$

a. Show that this relation is an equivalence relation on $\mathbb{Z}^2$.

b. Show that there are n^2 equivalence classes in $\mathbb{Z}^2$ for this relation.

Solution for 5:

a.
- reflexive: For $(a,b) \in \mathbb{Z}^2$, $a \equiv a (\mathrm{mod}\, n)$ and $b \equiv b (\mathrm{mod}\, n)$ since $\equiv (\mathrm{mod}\, n)$ is an equivalence relation on $\mathbb{Z}$. Thus $(a,b) \sim (a,b)$.
- symmetric: Let $(a,b),(c,d) \in \mathbb{Z}^2$ and suppose that $(a,b) \sim (c,d)$. Since $\equiv (\mathrm{mod}\, n)$ is a symmetric relation on $\mathbb{Z}$, we see that

  $$a \equiv c (\mathrm{mod}\, n) \text{ and } b \equiv d (\mathrm{mod}\, n) \Rightarrow c \equiv a (\mathrm{mod}\, n) \text{ and } d \equiv b (\mathrm{mod}\, n).$$

  This now shows that $(c,d) \sim (a,b)$.
- transitive: Let $(a,b),(c,d),(e,f) \in \mathbb{Z}^2$ with $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$.

  The first assumption shows that

  $$a \equiv c (\mathrm{mod}\, n) \text{ and } b \equiv d (\mathrm{mod}\, n),$$

  and the second assumption shows that

  $$c \equiv e (\mathrm{mod}\, n) \text{ and } d \equiv f (\mathrm{mod}\, n).$$

  Since $\equiv (\mathrm{mod}\, n)$ is a transitive relation on $\mathbb{Z}$, we deduce that

  $$a \equiv e (\mathrm{mod}\, n) \text{ and } b \equiv f (\mathrm{mod}\, n).$$

  This confirms that $(a,b) \sim (d,f)$ as required.

b. Recall that we write $\mathbb{Z}_n$ for the set of equivalence class in $\mathbb{Z}$ for the relation $\equiv (\mathrm{mod}\, n)$. We know that $|\mathbb{Z}_n| = n$.

   I claim that the set X of equivalence classes for $\sim$ in $\mathbb{Z}^2$ is in bijection with $\mathbb{Z}_n \times \mathbb{Z}_n$. Once this bijection is established, it follows that the number of equivalence classes is given by $|X| = |\mathbb{Z}_n \times \mathbb{Z}_n| = n \cdot n = n^2$.

   Now, define $f : X \to \mathbb{Z}_n \times \mathbb{Z}_n$ by the rule $f([(a,b)]) = ([a]_n, [b]_n)$ for $(a,b) \in \mathbb{Z}^2$.

   We must confirm that f is *well-defined*. Well, if $(a,b) \sim (c,d)$ we must argue that $f([(a,b)]) = f([(c,d)])$. But $(a,b) \sim (c,d)$ implies that $a \equiv c (\mathrm{mod}\, n)$ and $b \equiv d (\mathrm{mod}\, n)$ and this shows that $[a]_n = [c]_n$ and $[b]_n = [d]_n$. Thus $f([(a,b)]) = ([a]_n, [b]_n) = ([c]_n, [d]_n) = f([(c,d)])$.

   On the other hand, we define $g : \mathbb{Z}_n \times \mathbb{Z}_n \to X$ by the rule $g([a]_n, [b]_n) = [(a,b)]$. Again we must argue that g is well-defined. Suppose $([a]_n, [b]_n) = ([c]_n, [d]_n)$ is an equality in $\mathbb{Z}_n \times \mathbb{Z}_n$. Thus $[a]_n = [c]_n$ and $[b]_n = [d]_n$. But this shows that $(a,b) \sim (b,d)$ so that $[(a,b)] = [(c,d)]$ in X, confirming that g is well-defined.

   Now, by definition we have

   $$(f \circ g)([a]_n, [b]_n) = f([(a,b)]) = ([a]_n, [b]_n) \text{ so that } f \circ g = \mathrm{id}_{\mathbb{Z}_n \times \mathbb{Z}_n}$$

   and

   $$(g \circ f)([(a,b)]) = g([a]_n, [b]_n) = [(a,b)] \text{ so that } g \circ f = \mathrm{id}_X .$$

   Thus f is a bijection $X \to \mathbb{Z}_n \times \mathbb{Z}_n$.

Problem 6: Let A and B be sets.

a. If A is finite and B is countably infinite, prove that the union $A \cup B$ is a countably infinite set.

b. Prove that there is a bijection between $A \sqcup A \sqcup A$ and $A \times \{0,1,2\}$.

c. Let $f : A \to B$ be an injective function, and suppose that A is infinite and not countable. Prove that B is infinite and not countable.

Solution for 6a:

a. Choosing a bijection between A and $I_n = \{0, 1, ..., n-1\}$ and a bijection between B and $\mathbb{N}$, we are reduced to prove that $I_n \sqcup \mathbb{N}$ is countably infinite. We just need to demonstrate a bijection between $I_n \sqcup \mathbb{N}$ and $\mathbb{N}$.

Define $f : I_n \sqcup \mathbb{N} \to \mathbb{N}$ by the rule

$$f(x) = \begin{cases} x \text{ if } x \in I_n \\ x + n \text{ otherwise.} \end{cases}$$

We argue that f is surjective. If $m \in \mathbb{N}$ and $m \geq n$, then $m - n \in \mathbb{N} \subset I_n \sqcup \mathbb{N}$, and $m = f(m-n)$.

If $m < n$ then $m \in I_n \subset I_n \sqcup \mathbb{N}$, and $m = f(m)$.

This shows in all cases that f is surjective.

Finally, we argue that f is injective. Before proceeding, we observe that for $x \in I_n \sqcup \mathbb{N}$ we have by definition:

$$(\heartsuit): \quad f(x) \in I_n \subset \mathbb{N} \text{ if and only if } x \in I_n \subset I_n \sqcup \mathbb{N}.$$

For this, suppose that $x, y \in I_n \sqcup \mathbb{N}$ and assume that $f(x) = f(y)$. If $f(x) = f(y) \in I_n$ observation $(\heartsuit)$ shows that $x, y \in I_n$. Now the definition of f shows that $x = y$.

If $f(x) = f(y) \notin I_n$, then $x, y \in \mathbb{N} \subset I_n \sqcup \mathbb{N}$ so that

$$f(x) = f(y) => x + n = y + n \Rightarrow x = y.$$

This shows in all cases that f is injective.

Since f is bijective, $I_n \sqcup \mathbb{N}$ is indeed countably infinite.

Solution for 6b:
An element $x \in A \sqcup A \sqcup A$ is either in the left, middle or right-hand copy of A. We define

$$f : A \sqcup A \sqcup A \to A \times \{0,1,2\}$$

by the rule

$$f(x) = \begin{cases} (x,0) \text{ if } x \text{ is in the left-hand copy of } A \\ (x,1) \text{ if } x \text{ is in the middle copy of } A \\ (x,2) \text{ if } x \text{ is in the right-hand copy of } A \end{cases}.$$

Then f is a bijection. (**NB**: recall that we **defined** the disjoint union using a product construction, so this problem is more-or-less just an invocation of the definition of the disjoint union.)

Solution for 6c:
We prove the contra-positive. Thus, we suppose the negation of "B is infinite and not countable." Thus we suppose: B is finite or countably infinite.

And we must prove the negation of "A is infinite and not countable." This we must prove: A is finite or countably infinite.

Now the required result just follows from the (given) observation (i) in problem 7.

Problem 7: We showed the following in class (and you may use these statements here):

Let A, B be sets.

i. If $f : A \to B$ is an injective function and if B is countable, then A is either finite or countably infinite.
ii. If $g : B \to A$ is a surjective function and if A is countable, then B is either finite or countably infinite.

a. Prove that if A is a countably infnte set and if $\sim$ is an equivalence relation on A, then the set of equivalence classes is either finite or countably infinite.
b. Show by example for some countable set(s) A with equivalence relation(s) $\sim$ that the set B of equivalence classes can be finite, and that B can be infinite.

Solution for 7:

a. Let X be the set of equivalence classes in A for the eq. relation $\sim$. There is a surjective function $f : A \to X$ given by $f(a) = [a]$. Since A is countably infinte, it follows from (ii) that X is countable infinite or finite, as required.

b. Note that $\mathbb{Z}$ is countably infinite. For any $n \in \mathbb{N}_{>0}$, the set of equivalence classes $\mathbb{Z}_n$ for the equivalence relation $\equiv (\mathrm{mod}\, n)$ is finite, since $|\mathbb{Z}_n| = n$.

On the other hand, take the trivial equivalence relation on $\mathbb{Z}$ just defined by equality: $x \sim y \Leftrightarrow x = y$. Then for each $x \in \mathbb{Z}$, the equivalence class $[x]$ is just the singleton set $\{x\}$. In particular, the set of equivalence classes is in bijection with $\mathbb{Z}$ and is hence (countably) infinite.

Problem 8: Find all solutions x to the following equations in $\mathbb{Z}_{14}$:

a. $[3]_{14} \cdot x + [2]_{14} = [6]_{14}$

(Note that $[3]_{14} \cdot [5]_{14} = [15]_{14} = [1]_{14}$.)

b. $[2]_{14} \cdot x = [2]_{14}$.

Solution for 8:

a. We need $[3] \cdot x = [4]$ in $\mathbb{Z}_{14}$. Since $[3] \cdot [5] = [1]$ in $\mathbb{Z}_{14}$, we see that the only solution is

$$x = [5] \cdot [3]x = [5] \cdot [4] = [20]_{14} = [6]_{14}.$$

b. To solve $[2] \cdot x = [2]$ in $\mathbb{Z}_{14}$, we can write $x = [z]$ for some $z \in \mathbb{Z}$ with $0 \leq z < 14$. Then $[2] \cdot x = [2z]$. So we must decide: for which z is $2z \equiv 2 (\mathrm{mod}\, 14)$?

We of course have the "obvious" solution $x = [1]_{14}$ (i.e. $z = 1$.)

Note that $2z < 28$, and the integers between 0 and 28 which are $\equiv 2 (\mathrm{mod}\, 14)$ are precisely: 2 and 16.

So: there is one further solution, namely: $x = [z] = [8]_{14}$.

So the full set of solutions is: $[1]_{14}$ and $[8]_{14}$.

Problem 9: Let $n \in \mathbb{N}$ and consider the mapping $f : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $f([x]_n) = [x]_n \cdot [x]_n$.

a. Show that f is well-defined.

(We obtained a result in class that implies that f is well-defined, but show the details here).

b. Is f injective? Is f surjective? Prove or disprove each statement.

Solution for 9:

a. Suppose that $[x]_n = [y]_n$ for $x, y \in \mathbb{Z}$ –i.e. that $x \equiv y (\mathrm{mod}\, n)$. To see that f is well-defined, we need to check that $f([x]) = f([y])$. Now, $f([x]) = [x] \cdot [x] = [x^2]$. So we must argue that $x^2 \equiv y^2 (\mathrm{mod}\, n)$. Let's write $x - y = k \cdot n$ for $k \in \mathbb{Z}$.

Then we have

$$x^2 - y^2 = (x-y)(x+y) = k \cdot n \cdot (x+y) \Rightarrow n \mid x^2 - y^2 \Rightarrow x^2 \equiv y^2 (\mathrm{mod}\, n).$$

This proves that f is indeed well-defined.

b. In general, f is neither surjective nor injective.

For example, if $n = 3$, then

$$f([0]) = [0], f([1]) = [1], f([2]) = [4]_3 = [1]_3.$$

Thus the image of f is $\{[0], [1]\}$ so that f is not surjective.

Moreover, $f([1]) = f([2])$ but $[1] \neq [2]$ so that f is not injective.

Problem 10: Assume that a_n is a sequence with $\lim_{n\to\infty} a_n = 1$. Prove that $(-1)^n a_n$ is not a Cauchy sequence.

Solution for 10:
Since a_n converges to 1, we may find $m_0 \in \mathbb{N}$ such that $n \geq m_0 \Rightarrow |a_n - 1| < 1/2$. Thus

$$-1/2 < a_n - 1 < 1/2 \Rightarrow 1/2 < a_n.$$

We now show that the sequence $(-1)^n \cdot a_n$ fails to be Cauchy.

We must prove that (♣) : $\exists \varepsilon > 0$ such that $\forall m \in \mathbb{N}$, $\exists n_1, n_2 \geq m$ such that

$$|(-1)^{n_1} \cdot a_{n_1} - (-1)^{n_2} \cdot a_{n_2}| \geq \varepsilon.$$

We take $\varepsilon = 1/2$. For any m, choose $n_1, n_2 \geq \max(m, m_0)$ with n_1 even and n_2 odd. Observe that $(-1)^n_1 \cdot a_{n_1} = a_{n_1}$ and $(-1)^n_2 \cdot a_{n_2} = -a_{n_2}$.

Then we have

$$\left|(-1)^{n_1} a_{n_1} - (-1)^{n_2} \cdot a_{n_2}\right| = \left|a_{n_1} + a_{n_2}\right| \geq |a_{n_1}| > 1/2.$$

This confirms (♣) and shows that $(-1)^n \cdot a_n$ is not Cauchy.

Problem 11: If a_n is a Cauchy sequence, prove that the sequence $b_n = a_n \cdot a_{2n}$ is a Cauchy sequence.

(You can use results from class/the notes - just give a brief description of the result you are using).

Solution for 11:
We know that the product of Cauchy sequences is again a Cauchy sequence. Thus to prove that b_n is Cauchy it is enough to know that a_n is Cauchy – which is true by hypothesis – and that a_{2n} is Cauchy.

Thus, it remains only to prove that a_{2n} is Cauchy.

Let $\varepsilon > 0$. Since a_n is Cauchy, we may choose $m \in \mathbb{N}$ such that

$$(*) : n_1, n_2 \geq m \Rightarrow |a_{n_1} - a_{n_2}| < \varepsilon.$$

Now for any $n_1, n_2 \geq m$, notice that $2n_1 \geq m$ and $2n_2 \geq m$.

Thus $(*)$ implies that

$$\left|a_{2n_1} - a_{2n_2}\right| < \varepsilon.$$

This confirms that a_{2n} is Cauchy.