Intro to Proofs: HW10

Aamod Varma

November 7, 2024

14.2

Problem 5

Proof. Consider the following set of irrationals,

$$\{\sqrt{2}/1, \sqrt{2}/2, \sqrt{2}/3, \dots\}$$

We can show a bijection from N to this set defined by $f(n) = \sqrt{2}/n$. And it is a subset of the irrationals as it contains only irrational numbers. □

Problem 8

Proof. 1. We know that Z is countably infinite and Q is countably infinite so it follows from the corollary that $Z \times Q$ is countable infinity.
2. We can constrict a mapping from $Z \times Q$ to $Z \times Z \times Z$ as follows $f(a, \frac{p}{q}) = (a, p, q)$ which is bijective. And we also know that $Z \times Z \times Z$ is countably infinite as Z is countably infinite hence $Z \times Q$ is countably infinite. □

Problem 13

Proof. For any arbitrary set X let us define a function that maps it to $p_{x_1} p_{x_2} \dots$. Where x_1, x_2 are the elements of X and p_{x_1} refers to the x_1th prime number.
This ensures that if $X_1 \neq X_2$ that $f(X_1) \neq f(X_2)$. Hence we have an injective function. So we can list out the elements of A making it countably infinite. □

14.3

Problem 2

Proof. We can define a function $f : C \to R \times R$ as follows $f(a+bi) = (a, b)$. We see that this is injective because $(a_1, b_2) = (a_2, b_2)$ implies $a_1 = a_2$, $b_1 = b_2$. Which must mean $a_1 + b_1 i = a_2 = b_2 i$ (by definition of addition in the complex plane). We show its surjective as for any (a, b) we can find $a + bi \in C$ such that $f(a + bi) = (a, b)$.
So we have $|C| = |R \times R|$. Because R is uncountable we know that $R \times R$ is uncountable. Hence C is uncountable

□

Problem 3

Proof. Consider $P(R)$. We know $P(R)$ is uncountable as it is a powerset of an infinite set. Howver $|R| < |P(R)|$ hence $|R| \neq |P(R)|$ □

Problem 7

Proof. Let us assume the contrary that $B - A$ is countable. Now we also know that A is countable. We know the union of two countable sets must be countable. Hence $A \cup (B - A)$ is countable. This is, $A \cup (B \cap \overline{A}) = B \cap B = B$. So B must be countable, but we know B is uncountable. Hence a contradiction. So $B - A$ must be uncountable. $\square$

Problem 8

Proof. We show that the set is uncoutable by showing there cannot be a mapping from the set to N. Consider the following mapping,

```
1 | a_1 a_2 a_3 ...
2 | b_1 b_2 b_3 ...
3 | c_1 c_2 c_3 ...
4 | d_1 d_2 d_3 ...
```

Now consider a sequence defined whose nth element is defined as 1 if $f(n) = 0$ where f gives the n element of sequence that the natural number n is mapped to.
Now by construction there is no natural number $n \in N$ such that maps to our sequence. Hence we show there cannot be a surjection which implies that it is uncountable. $\square$

Problem 10

Proof. Assume it is not injective. Then there exists $a_1 \neq a_2 \in A$ such that $f(a_1) = f(a_2)$. Now consider the set $A_0 = A - \{a_0\}$. Now for any $b \in B$ there still is $a \in A$ such that $f(a) = b$ as the element a_0 was mapped to is still mapped to by a_1. Hence it is still surjective. But we know that $|A| < |B|$ which makes it not surjective. We get a contradiction hence f must be injective.
Consider f from Z to N as follows $f(z) = |z|$. This is a surjection as for any $n \in N$ we have $n \in Z$ as well. But it is easy to see that it is not injective as z and $-z$ map to the same element despite being different. We also know that $|Z| = |N|$ $\square$

14.4

Problem 1

Proof. If $A \subseteq B$ then $|A| \leq |B|$. And if there is an injection from $B \to A$ then that implies that $|B| \leq |A|$. Both these imply that $|A| = |B|$ $\square$

Problem 6

Proof. We know that $|N \times N| = |N| = \aleph_0$. This means there exists f which is a bijection from $N \times N$ to N. Now let us construct a bijection g defined on $P(N \times N)$ to $P(N)$. Defined as follows,

$$g(X) = \{f(x) : x \in X\}$$

Now we show this is a bijective function.
First consider two sets X_1, X_2, we need to show that $g(X_1) = g(X_2) \Rightarrow X_1 = X_2$.
We have,

$$\{f(x_1) : x_1 \in X_1\} = \{f(x_2) : x_2 \in X_2\}$$

First consider $x_1 \in X_1$ this means that $f(x_1) \in g(X_1)$. Now because the sets are equal means $\exists x_2 \in X_2$ such that $f(x_2) = f(x_1)$. However because f is injective we have $x_1 = x_2$ or $x_1 \in X_2$. This means that $X_1 \subseteq X_2$
Now we can similarly show that $X_2 \subseteq X_1$ which implies that $X_1 = X_2$
Now we need to show that g is surjective.
Consider an arbitrary Y in $P(Z)$. We need to show there is an $X \in P(N)$ such that $g(X) = Y$.
We know that because f is surjective, for any $y \in Y, \exists x \in N$ such that $f(x) = y$. Hence we define,

$$X = \{x : f(x) \in Y\}$$

Now because of how we define X we have,

$$g(X) = \{f(x) : x \in X\}$$

but $x \in X$ such that $f(x) \in Y$. Hence if $y \in g(X)$ then $\exists x \in X$ such that $f(x) = y$. But this means that $x \in X$ which implies that $f(x) \in Y$ or $y \in Y$ which shows that $f(x) \subseteq Y$.
Similarly, if $y \in Y$ we have $x \in X$ such that $f(x) = y$. But based on how $g(X)$ is defined we have $f(x)$ if $x \in X$ but $f(x) = y$ so $y \in g(X)$ hence $Y \subseteq g(X)$ or $g(X) = Y$
This shows surjection. So we have defined a bijective function fro $P(N)$ to $P(Z)$ showing their cardinality is the same.

$\square$

Problem 22

Proof. First we show its defined for addition. So let $[a] = [a']$ and $[b] = [b']$ we want to show that $[a + b] = [a' + b']$
By definition we know that $a - a' = k_1 n$ and $b - b' = k_2 n$. Adding them both we have,

$$a + b - (a' + b') = n(k_1 + k_2)$$

Or $[a + b] = [a' + b']$
We show its defined for multiplication. So we need to show that $[ab] = [a'b']$.

So we have,

$$a - a' = k_1 n \Rightarrow a = k_1 n + a'$$

$$b - b' = k_2 n \Rightarrow b = k_2 n + b'$$

So,

$$ab = k_1 n b' + k_1 k_2 n^2 + k_2 n a' + a'b'$$

$$ab - a'b' = n(k_1 b' + k_1 k_2 n + k_2 a')$$

So $[ab] = [a'b']$ □

Problem 23

Proof. We show that $([a] + [b]) + [c] = [a] + ([b] + [c])$
We have,

$$\begin{aligned}([a] + [b]) + [c] &= [a + b] + c \\ &= ([a + b]) + [c] \\ &= ([a + (b + c)] \\ &= [a] + [b + c] \\ &= [a] + ([b] + [c])\end{aligned}$$

Similarly we have $[ab][c] = [a][bc]$ □

Problem 24

Proof. Let $a(b + c) \equiv m \pmod{n}$
This means that $a(b + c) - m = kn$ for some k, So we have,

$$ab + bc - m = kn$$

for some k which means that,

$$ab + bc \equiv m \bmod n$$

So we have $a(b + c)ab + ac \pmod{n}$ □