21-127 Homework 8

Christian Broms
Section J

Thursday 5th April, 2018

Complete the following problems. Fully justify each response.

1. A number is called *algebraic* if it is the root of a polynomial $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where each $a_i \in \mathbb{Z}$. Let $\mathcal{A}$ denote the set of algebraic numbers.

   (a) Prove that $\mathbb{Q} \subseteq \mathcal{A}$.

   Proof. Let $q \in \mathbb{Q}$ such that $q = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$. So our polynomial $p(x) = a_1 x - a_0$ can be written as $p(x) = bx - a$. Notice, $p(q) = p(\frac{a}{b}) = b \cdot \frac{a}{b} - a = 0$ and thus q is a root of $p(x)$. Thus $q \in \mathcal{A}$. Therefore, $\mathbb{Q} \subseteq \mathcal{A}$. ■

   (b) Prove that the set of all algebraic numbers is countably infinite.

   (Hint: First consider the possible roots of polynomials of degree k. Then use a union argument).

   Proof. Consider the set of polynomials of degree n as P_n. We can show that this set of polynomials is countable by constructing a bijection between P_n and $\mathbb{Z}^{n+1}$, so let $f : P_n \to \mathbb{Z}^{n+1}$, where $f(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) = (a_0, a_1 \ldots a_{n-1}, a_n)$. The codomain can be expressed as an expansion of the integers, where there are $\mathbb{Z} \times \mathbb{Z}^n$ instances. We know that $\mathbb{Z}$ is countably infinite, and the cartesian product of countably infinite sets yields a countably infinite set, so we conclude that P_n is countably infinite.

   Now, we know that a polynomial of degree n has a maximum of n roots. So, we need to prove that the set R of roots for any given polynomial is countably infinite. This can be easily derived from the fact that the set of polynomials of degree n is countably infinite. So, we can construct the set $\mathcal{A}$ of algebraic numbers as a union of the sets of roots for given polynomials p. Thus, $\mathcal{A} = \bigcup\limits_{p \in P} R_p$. Since this is a union of countably infinite sets, we can conclude that $\mathcal{A}$ is countably infinite. ■

2. (a) Let X be any set. Prove, using Cantor's Diagonalization Argument, that $|\mathcal{P}(X)| > |X|$.

   Proof. We want to show that for every function $f : X \to \mathcal{P}(X)$ there is a subset $A \subseteq X$ such that $A \notin \mathcal{P}(X)$, which shows that there is no bijection or surjection from X to $\mathcal{P}(X)$, and thus $|\mathcal{P}(X)| > |X|$.

   Assume that we have some function $f : X \to \mathcal{P}(X)$. Let the set $B = f(x)$. There are two possibilites: for each $x \in X$, either $x \in B$ or $x \notin B$. We build a subset from X, called A by selecting values from X such that $A = \{x \in X \mid x \notin B\}$.

   Notice that for each $x \in X$, $x \in B$ and $x \notin A$, OR $x \in A$ and $x \notin B$. We therefore have two distinct sets, A and B. Hence, it must be that $A \neq B$ since the two sets don't share any elements. We now know that there are elements in X, namely the set A, that do not map to any value in the codomain. Thus, we know that $A \notin \mathcal{P}(X)$, and can conclude that there is no surjection from X to $\mathcal{P}(X)$. Therefore, $|\mathcal{P}(X)| > |X|$. ■

   (b) Prove that $\mathcal{P}(X)$ is either finite or uncountably infinite.

   Proof. We can consider three distinct cases based off of the size of X.

   Case 1: X is finite. Let $|X| = n$ for some $n \in \mathbb{N}$. We know that $|\mathcal{P}(X)| = 2^n$. Therefore, $\mathcal{P}(X)$ is countably infinite because n is some finite number and 2^n is also some finite number, and there exists a bijection from 2^n to $\mathcal{P}(X)$, and thus the power set is finite.

   Case 2: X is countably infinite. Suppose that $|\mathcal{P}(X)| = |X|$. Then there exists some bijection, g from X to $\mathcal{P}(X)$, so $g : X \to \mathcal{P}(X)$. We will construct a set $T \in \mathcal{P}(X)$ such that there is no $t \in X$ with $g(t) = T$. Let $T = \{t \in X \mid t \notin g(t)\}$. Notice that $T \in \mathcal{P}(X)$ but there is no $x \in X$ such that $g(x) = T$. Therefore, there cannot be a bijection from X to $\mathcal{P}(X)$. Thus, $\mathcal{P}(X)$ is not countably infinite. Since $|\mathcal{P}(X)| > |X|$ and X is countably infinite, then $\mathcal{P}(X)$ is uncountably infinite because it is greater than a countably infinite set.

Case 3: X is uncountably infinite. Therefore, $\mathcal{P}(X)$ is uncountably infinite because it's size is greater than X, and uncountably infinite set because $|\mathcal{P}(X)| > |X|$.

Therefore, we conclude that $\mathcal{P}(X)$ can be either finite or uncountably infinite. ■

3. Let $f : X \to Y$ be a function. Define a relation R on X by $x_1 R x_2 \Leftrightarrow f(x_1) = f(x_2)$. Is this an equivalence relation? If so, prove it. If not, explain why not.

Proof. Yes, this is an equivalence relation.

Reflexivity: We know xRx since $f(x) = f(x)$.

Symmetry: Suppose $x_1 R x_2$. Then $f(x_1) = f(x_2)$ and $f(x_2) = f(x_1)$. Thus $x_2 R x_1$.

Transitivity: Suppose $x_1 R x_2$ and $x_2 R x_3$. Then $f(x_1) = f(x_2)$ and $f(x_2) = f(x_3)$. Therefore, $f(x_1) = f(x_2) = f(x_3)$ so $f(x_1) = f(x_3)$. Hence $x_1 R x_3$. ■