Math 445, Fall 2009 Exercise Set #2 Solutions

1. [#1, page 26] Let A be a countable set and suppose there exists a function $f\colon A \to B$ which is surjective. Prove that B is also countable. (Recall that a set is *countable* if there is a bijection with the set of natural numbers $\mathbb{N}$.)

Proof. If A is finite, and there exists a surjection $f\colon A \to B$, then B is also finite.

So, we may assume that A is infinite. Choose a bijection $\phi\colon \mathbb{N} \to A$. It will suffice to show that $f \circ \phi\colon \mathbb{N} \to B$ surjective implies that B is countable.

We define an injection $\psi\colon B \to \mathbb{N}$ as follows: for each $b \in B$ let $K(b) \subset \mathbb{N}$ be the set of all pre-images of b. That is,

$$K(b) = \{n \in \mathbb{N} \mid f(n) = b\}$$

Then $K(b) \subset \mathbb{N}$ has a least element, which we denote by $\psi(b) \in K(b)$. The mapping $b \mapsto \psi(b)$ defines a map $\psi\colon B \to \mathbb{N}$. It is well-defined since $f \circ \phi$ is onto. Note that $f \circ \phi(\psi(b)) = b$. This implies that ψ is injective: if $\psi(b) = \psi(b')$ then $b = f \circ \phi(\psi(b)) = f \circ \phi(\psi(b')) = b'$. □

5. [#1, page 31] Prove that the set of positive real numbers has cardinal c. (Recall that c is the cardinal of the real number line $\mathbb{R}$.)

Proof. We just need to show there exists a bijection $f\colon (0, \infty) \to \mathbb{R}$. For example, for $0 < x < \infty$, set $f(x) = \ln(x)$. The function $y = \ln(x)$ has inverse $x = e^y$ so it is injective. The domain of e^y is all $y \in \mathbb{R}$, so the range of $\ln(x)$ is all of $\mathbb{R}$. Thus, f is one-to-one and onto. □

2. [#4, page 26] Show that the set $\mathbb{N}$ of natural numbers can be represented as a union $\mathbb{N} = \cup A_i$ of an infinite number of disjoint *infinite* sets.

Proof. There are many solutions to this problem. Here is one. Let $\{p_1, p_2, \ldots\}$ be a list of all the primes, with $p_i \geq 2$. For $i \geq 1$, let $A_i = \{p_i^n \mid n = 1, 2, \ldots\}$. Then A_i is an infinite set. Also, $A_i \cap A_j = \emptyset$ unless $p_i = p_j$ which implies $i = j$. Finally, there are an infinite number of composite integers, those integers with more than one distinct prime factor. Let $A_0 = \{n \in \mathbb{N} \mid n \text{ is composite}\}$. Then we have

$$\mathbb{N} = A_0 \cup A_1 \cup A_2 \cup \cdots$$

□

3. [#10, page 27] Let A be an infinite set, $B \subset A$ a finite subset, and $C = A - B$ the complement of B in A. Prove there exists a one-to-one correspondence between A and C.

Proof. A is infinite and B is finite, so C is again infinite. Thus, C contains a countably infinite subset, $H = \{g_1, g_2, \ldots\} \subset C$. The idea of the proof is to use the "Hilbert Hotel Principle" to squeeze B into the subset H. Let $B = \{b_1, b_2, \ldots, b_m\}$.

Define a bijection $f\colon A \to C$ by setting:

For $a \in C - H$ define $f(a) = a \in C - H$.

For $b_i \in B$ define $f(b_i) = g_i \in C$.

For $g_j \in H$ define $f(g_j) = g_{m+j} \in H \subset C$.

The map is one-to-one by definition. To show that it is onto, first note that is maps $C - H$ onto $C - H$ by definition. Then for H, the map f sends B to the beginning of the set H, and sends the entire subset H shifted onto the remainder of H. So, f maps $B \cup H$ bijectively to H. Combining the two cases, this shows that f is onto C. □

4. [#11*, page 27] Let A be an uncountable set, $B \subset A$ a countable subset, and $C = A - B$ the complement of B in A. Prove there exists a one-to-one correspondence between A and C.

Proof. The idea of this problem is similar to #3 above, except that we have to squeeze in an infinite subset, not just a finite subset.

A is uncountable and B is countable, so C is again uncountable. Thus, C contains a countably infinite subset, $H = \{g_1, g_2, \ldots\} \subset C$. The idea of the proof is to use the "Hilbert Hotel Principle" to squeeze the countable subset B into the countably infinite subset H. For example, we can map two copies of $\mathbb{N}$ into itself, one as the even integers, the other as the odd integers. We will squeeze in B along the even indices. Let $B = \{b_1, b_2, \ldots\}$.

Define a bijection $f \colon A \to C$ by setting:

For $a \in C - H$ define $f(a) = a \in C - H$.

For $b_i \in B$ define $f(b_i) = g_{2i} \in C$.

For $g_j \in H$ define $f(g_j) = g_{2j-1} \in H \subset C$.

B is mapped onto the subset of C with even indices, and C is mapped onto the subset of itself with odd indices. So, f maps $B \cup C$ onto C. This shows that f maps A onto $A - B$.

The map is one-to-one by definition. To show that it is onto, first note that is maps $C - H$ onto $C - H$ by definition. Then for H, the map f sends B to the elements with even indices in the set H, and sends the entire subset H shifted onto the subset of H with odd indices. So, f maps $B \cup H$ bijectively to H. Combining the two cases, this shows that f is onto C. ☐

6. [#5, page 31] What is the cardinal number of the set of irrational numbers? Of the set of transcendental real numbers? (A real number is *transcendental* if it is not algebraic. A real number is *algebraic* if it is the solution of a non-trivial polynomial equation with integer coefficients.)

Proof. The irrational numbers are the complement $\mathbb{R} - \mathbb{Q}$, where $\mathbb{R}$ is uncountable and $\mathbb{Q}$ is countable. Then use Problem 4) above to see that there is a bijection between $\mathbb{R}$ and $\mathbb{R} - \mathbb{Q}$. So, the set of irrational numbers is again uncountable.

The integers $\mathbb{Z}$ are a countable set. A polynomial with integer coefficients can be written as

$$p(x) = \alpha_n \cdot x^n + \alpha_{n-1} \cdot x^{n-1} + \cdots \alpha_1 \cdot x + \alpha_0$$

where $(\alpha_0, \alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^{n+1}$. For each degree $n > 0$ there exists a countably infinite number of such polynomials. Each polynomial equation of degree n has at most n roots, so the number of solutions to all such polynomials of degree n is again countably infinite. There are a countably infinite number of degrees of such polynomials, so there are a countably infinite number of algebraic numbers. Denote the algebraic numbers by $\mathbb{A}$.

The set of transcendental numbers are the complement $\mathbb{R} - \mathbb{A}$, where $\mathbb{R}$ is uncountable and $\mathbb{A}$ is countable. Then use Problem 4) above to see that there is a bijection between $\mathbb{R}$ and $\mathbb{R} - \mathbb{A}$. So, the set of transcendental numbers is again uncountable. ☐

[Note: Very few transcendental numbers are known explicitly. The proofs that e and π are transcendental are difficult. The above argument shows that all but a countable number of irrational numbers are transcendental. Read more in the wikipedia entry for "transcendental numbers".]

7. [#2, page 39] Let L be a lattice in which every chain has an upper bound. Prove that L has a unique maximal element; that is, a top element. [You can assume Zorn's Lemma.]

Proof. L is a lattice, so it is partially ordered set, and for any two elements, $a, b \in$ there exists a least upper bound $a \cup b \in L$. We are given that every chain $C \subset L$ has an upper bound.

Intuitively, one might proceed by taking a chain $C \subset L$ and then let $u \in L$ be an upper bound. If u is not a top element for L, then there exist another $u' \in L$ with $u < u'$. Then $C' = C \cup \{u'\}$ is a new chain which is larger than C. This suggests that what we need to do is find a "top chain". Here's how:

Let $\mathcal{P}_c(L)$ denote the set of all subsets of L which are chains.

Order the chains by inclusion: for $C, C' \in \mathcal{P}_c(L)$ then $C \leq C'$ if $C \subset C'$. We want to apply Zorn's Lemma to this set of chains $\mathcal{P}_c(L)$. We must show that every chain in $\mathcal{P}_c(L)$ has a maximal element.

Given a chain (of chains) $\mathcal{B} = \{C_\alpha \mid \alpha \in \mathcal{A}\} \subset \mathcal{P}_c(L)$, define $C_0 = \bigcup_{\alpha \in \mathcal{A}} C_\alpha$.

We claim C_0 is again a chain: given $x, y \in C_0$ then for some $\alpha \in \mathcal{A}$, we have $x \in C_\alpha$ and for some $\beta \in \mathcal{A}$ we have $y \in C_\beta$. We assume that $\mathcal{B}$ is a chain, so either $C_\alpha \leq C_\beta$ or $C_\beta \leq C_\alpha$. Assume the former, then $C_\alpha \subset C_\beta$. Then both $x, y \in C_\beta$. As C_β is a chain, either $x \leq y$ or $y \leq x$. Thus, the partial order on L restricts to an order on the set C_0 so it is a chain. This shows that $C_0 \in \mathcal{P}_c(L)$.

We claim C_0 is an upper bound for the chain $\mathcal{B}$. Given any $C_\alpha \in \mathcal{B}$ then $C_\alpha \subset C_0$ be its construction. Hence, for the partial ordering on chains we have $C_\alpha \leq C_0$.

By Zorn's Lemma, there exists $C_* \in \mathcal{P}_c(L)$ which is a maximal element. By our assumption, there exists an upper bound $u \in L$ for the chain C_*.

We claim that u is a top element for L.

Given any $v \in L$ then there is a least upper bound $w = u \cup v \in L$. Suppose that $u < w$, then we can form a new chain $C'_* = C_* \cup \{w\}$ which is a strictly larger chain that C_*. This contradicts the maximality of C_*.

So, we must have $w \leq u$. But this implies $u \cup v \leq u$ and so by definition of the upper bound, $v \leq u \cup v \leq u$. So, $v \leq u$, as was to be shown. ☐