MATH 108 Winter 2019 - **Problem Set 7 solutions**

due March 8

1. (a) Prove (with the Axiom of Choice) that every infinite set has a countably infinite subset.

   Let A be an infinite set. $\mathcal{P}(A) \setminus \{\emptyset\}$ is a collection of nonempty sets, so by the Axiom of Choice there is a choice function $c : \mathcal{P}(A) \setminus \{\emptyset\} \to A$ with $c(B) \in B$. Define injective function $f : \mathbb{N}_1 \to A$ as follows. For each $n \in \mathbb{N}_1$, let $f(n) = c(A \setminus \{f(1), \ldots, f(n-1)\})$. The resulting function f is injective since each value is chosen to be distinct from the previous ones. Therefore $\text{im}(f)$ is a countably infinite subset of A.

   (b) Prove that every infinite set has a proper subset with the same cardinality.

   For A an infinite set, by part (a), there is a countably infinite subset $B \subseteq A$. Since B is countably infinite, we can write the elements as $B = \{x_1, x_2, x_3, \ldots\}$. Let $g : B \to B \setminus \{x_1\}$ be the bijective function defined by $g(x_k) = x_{k+1}$ for each $k \in \mathbb{N}_1$. Then define $h : A \to A \setminus \{x_1\}$ by

$$h(x) = \begin{cases} g(x) & \text{if } x \in B \\ x & \text{if } x \notin B \end{cases}.$$

   h is also bijective, so $|A| = |A \setminus \{x_1\}|$.

2. Prove that the set of irrational numbers, $\mathbb{R} \setminus \mathbb{Q}$, is uncountable.

   Suppose $\mathbb{R} \setminus \mathbb{Q}$ is countable. We know that $\mathbb{Q}$ is countable and that the union of two countable sets is countable. Therefore

$$\mathbb{R} = (\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q}$$

   is also countable. But this contradicts the fact that $\mathbb{R}$ is uncountable. Therefore $\mathbb{R} \setminus \mathbb{Q}$ is uncountable.

3. Let $\mathbb{N}_0^\infty$ denote the set of all infinite sequences of nonnegative integers,

$$\mathbb{N}_0^\infty = \{(a_1, a_2, a_3, \ldots) \mid a_1, a_2, a_3, \ldots \in \mathbb{N}_0\}.$$

   Use Cantor's diagonalization argument to prove that $\mathbb{N}_0^\infty$ is uncountable.

   For any function $f : \mathbb{N}_1 \to \mathbb{N}_0^\infty$, we will construct a new sequence

$$s = (s_1, s_2, s_3, \ldots) \in \mathbb{N}_0^\infty$$

   that is not in the image of f, proving that f is not surjective. For each $n \in \mathbb{N}_1$, let $f(n) = (a_{n1}, a_{n2}, a_{n3}, \ldots)$. Choose s_n to be some nonnegative integer that is different from a_{nn}. We can for example choose $s_n = 0$ if $a_{nn} \neq 0$ and $s_n = 1$ if $a_{nn} = 0$. The resulting sequence has $s \neq f(n)$ for all $n \in \mathbb{N}_1$ because they have different nth entries. Therefore $s \notin \text{im}(f)$. We conclude that there are no surjective functions from $\mathbb{N}_1$ to $\mathbb{N}_0^\infty$, so $\mathbb{N}_0^\infty$ is uncountable.

4. Prove that the following sets have cardinality $\mathfrak{c}$.

   (a) The set of all functions from $\mathbb{N}_1$ to $\{0,1\}$.

   Denote this set A. Let $f : \mathcal{P}(\mathbb{N}_1) \to A$ map each subset $B \subseteq \mathbb{N}_1$ to its characteristic function $\chi_B : \mathbb{N}_1 \to \{0,1\}$. Recall that

   $$\chi_B(n) = \begin{cases} 1 \text{ if } n \in B \\ 0 \text{ if } n \notin B \end{cases}.$$

   Suppose that $f(B_1) = f(B_2)$, so $\chi_{B_1} = \chi_{B_2}$. For each $n \in \mathbb{N}_1$, $\chi_{B_1}(n) = 1$ if and only if $\chi_{B_2}(n) = 1$. Therefore $n \in B_1$ if and only if $n \in B_2$, implying that $B_1 = B_2$. This proves that f is injective.

   For any $g \in A$, define the set $B = \{n \in \mathbb{N}_1 \mid g(n) = 1\}$. Then $f(B) = g$. Therefore f is surjective. Since $f : \mathcal{P}(\mathbb{N}_1) \to A$ is a bijection, $|A| = |\mathcal{P}(\mathbb{N}_1)| = \mathfrak{c}$.

   (b) The closed interval $[0,1]$.

   The inclusion map $i : [0,1] \to \mathbb{R}$ is injective, so $|[0,1]| \leq \mathfrak{c}$. The inclusion map $i : (0,1) \to [0,1]$ is injective, so $|[0,1]| \geq \mathfrak{c}$. By the Cantor-Schröder-Bernstein Theorem, $|[0,1]| = \mathfrak{c}$.

   (c) $\mathcal{P}(\mathbb{N}_1) \times \mathcal{P}(\mathbb{N}_1)$.

   The map $f : \mathcal{P}(\mathbb{N}_1) \to \mathcal{P}(\mathbb{N}_1) \times \mathcal{P}(\mathbb{N}_1)$ defined by $f(B) = (B, \emptyset)$ is injective, so $|\mathcal{P}(\mathbb{N}_1) \times \mathcal{P}(\mathbb{N}_1)| \geq |\mathcal{P}(\mathbb{N}_1)| = \mathfrak{c}$. The map $g : \mathcal{P}(\mathbb{N}_1) \times \mathcal{P}(\mathbb{N}_1) \to \mathcal{P}(\mathbb{Z})$ defined by

   $$g(A, B) = A \cup \{-x \mid x \in B\}$$

   is also injective. Therefore $|\mathcal{P}(\mathbb{N}_1) \times \mathcal{P}(\mathbb{N}_1)| \leq |\mathcal{P}(\mathbb{Z})|$. Since $|\mathbb{Z}| = |\mathbb{N}_1|$, it follows that $|\mathcal{P}(\mathbb{Z})| = |\mathcal{P}(\mathbb{N}_1)| = \mathfrak{c}$. By the Cantor-Schröder-Bernstein Theorem, $|\mathcal{P}(\mathbb{N}_1) \times \mathcal{P}(\mathbb{N}_1)| = \mathfrak{c}$.

5. Order the following cardinal numbers: $|(0,1)|$, $|[0,1]|$, $|\{0,1\}|$, $|\{0\}|$, $|\mathcal{P}(\mathbb{R})|$, $|\mathbb{Q}|$, $|\emptyset|$, $|\mathbb{R}^2|$, $|\mathcal{P}(\mathcal{P}(\mathbb{R}))|$, $|\mathbb{R}|$, $|\mathcal{P}(\mathbb{Q})|$.

   $|\emptyset| < |\{0\}| < |\{0,1\}| < |\mathbb{Q}| < |\mathbb{R}| = |(0,1)| = |[0,1]| = |\mathcal{P}(\mathbb{Q})| = |\mathbb{R}^2| < |\mathcal{P}(\mathbb{R})| < |\mathcal{P}(\mathcal{P}(\mathbb{R}))|$.

6. Determine whether each algebraic structure is a group. If no, which properties does it fail? If yes, is it abelian? Find an identity element if one exists.

   (a) $(\mathbb{N}_1, +)$.

   Not a group. $\mathbb{N}_1$ has no additive identity, and elements have no additive inverses. There are no identity elements.

   (b) $(\mathbb{Q}, \cdot)$.

   Not a group. 0 has no multiplicative inverse. The identity element is 1.

   (c) $(\mathbb{Q} \setminus \{0\}, \cdot)$.

   Group. It is abelian because $a \cdot b = b \cdot a$. The identity element is 1.

(d) $(\mathbb{Z}/4\mathbb{Z}, +)$.

Group. It is abelian because $\overline{x} + \overline{y} = \overline{x+y} = \overline{y} + \overline{x}$. The identity element is $\overline{0}$.

(e) $(\mathbb{Z}/4\mathbb{Z} \setminus \{\overline{0}\}, \cdot)$.

Not a group. Not even an algebraic structure, because $\overline{2} \cdot \overline{2} = \overline{0}$ is not in the set $\mathbb{Z}/4\mathbb{Z} \setminus \{\overline{0}\}$. Therefore the operation $\cdot$ is not well-defined.

(f) (The set of functions $\{1, 2, 3\} \to \{1, 2, 3\}$, composition).

Not a group. If function f is not injective, then it has no inverse. The identity element is the identity function $I_{\{1,2,3\}}$.

(g) (The set of bijective functions $\{1, 2, 3\} \to \{1, 2, 3\}$, composition).

Group. It is not abelian. For example let f be the function that switches 1 and 2, and g be the function that switches 2 and 3. Then $g \circ f(1) = 3$ but $f \circ g(1) = 2$. The identity element is the identity function $I_{\{1,2,3\}}$.

(h) (The set of 2×2 real matrices with determinant 1, matrix multiplication).

Group. It is not abelian. For example let

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Then

$$AB = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \quad BA = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}.$$

The identity element is the identity matrix,

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$