MA1100(T) - Basic Discrete Mathematics (T) Suggested Solutions

Written by : Maximus Pung Jun
Audited by : Teoh Tze Tzun

(Semester 1 : AY2022/23)

Question 1

(a) *Proof.* Define $g : A \to \text{Maps}(B, C)$ by $g(a) = \{(b, c) \in B \times C : b \in B \text{ and } f(a, b) = c\}$. First, we want to show that g is a function. See that for all $a \in A$ and $b \in B$, $f(a, b)$ is well defined, as f is a function. So, it also follows that g is a function. Now, we want to show that g is unique. So, suppose g_1 and g_2 are functions that map A to $\text{Maps}(B, C)$, such that $g_1(a)(b) = f(a, b)$ and $g_2(a)(b) = f(a, b)$, for all $b \in B$. So, one has $g_1(a) = g_2(a)$. Since both g_1 and g_2 have the same domain, codomain and $f(x) = g(x)$ for all $x \in A$, we conclude that $g_1 = g_2$ as desired. □

(b) *Proof.* Let f be one-to-one. Now suppose $g(a_1) = g(a_2)$. Fix some $b \in B$. See that $g(a_1)(b) = g(a_2)(b)$. So, $f(a_1, b) = f(a_2, b)$. Since f is one-to-one, one has $a_1 = a_2$ as desired. □

Question 2

Proof. ($\to$) Suppose $\gcd(a, b)$ divides c. By Bezout's Identity, one can fix integers $n, m \in \mathbb{Z}$ such that $\gcd(a, b) = an + mb$. Now fix some integer $k \in \mathbb{Z}$ such that $c = k(an + mb)$. It follows that $-mb = akn - c$. Now let $x = ak$. So, $-mb = ax - c$. Since $-m \in \mathbb{Z}$, it follows that b divides $ax - c$ for some integer x.

($\leftarrow$) Suppose there exists some $x \in \mathbb{Z}$ such that b divides $ax - c$. Fix some $k \in \mathbb{Z}$ such that $kb = ax - c$. See that $c = ax - kb$. Now observe that $\gcd(a, b)$ divides both a and b. Since x and $-k$ are integers, one has $\gcd(a, b)$ divides $ax - kb = c$ as desired. □

Question 3

(a) *Proof.* WLOG, suppose $x \leq y$. Then $n \cdot x \leq n \cdot y$. Observe that $\min\{n \cdot x, n \cdot y\} = n \cdot x$, and $n \cdot \min\{x, y\} = n \cdot x$. So, $\min\{n \cdot x, n \cdot y\} = n \cdot \min\{x, y\}$ as desired. □

(b) *Proof.* Let $a = \prod\{p^{e_a(p)} : e_a(p) \neq 0\}$ and $b = \prod\{p^{e_b(p)} : e_b(p) \neq 0\}$. So, $a^n = \prod\{p^{n \cdot e_a(p)} : e_a(p) \neq 0\}$ and $b^n = \prod\{p^{n \cdot e_b(p)} : e_b(p) \neq 0\}$.

$$\begin{aligned}
\gcd(a^n, b^n) &= \prod\{p^{\min\{n \cdot e_a(p), n \cdot e_b(p)\}}\} \\
&= \prod\{p^{n \cdot \min\{e_a(p), e_b(p)\}}\} \\
&= (\prod\{p^{\min\{e_a(p), e_b(p)\}}\})^n \\
&= (\gcd(a, b))^n
\end{aligned}$$

□

Question 4

Define $f_b : \mathbb{Z} \to \mathbb{Z}$ by $f_b(a) = a + b$.

- To show that $\pi \circ f_b = \pi$, see that $a \sim f_b(a)$ for all $a \in \mathbb{Z}$. So, $\pi(a) = \pi \circ f_b(a)$. Since the domain of π and $\pi \circ f_b$ are the same, we conclude that $\pi \circ f_b = \pi$ as desired.
- It is clear that $f_b \neq \mathrm{id}_{\mathbb{Z}}$.
- To show that f_b is one-to-one, let $f_b(a_1) = f_b(a_2)$. So, $a_1 + b = a_2 + b$. Thus, one has $a_1 = a_2$ as desired.

Question 5

(a) *Proof.* To show that G is well defined, one can fix some $f \in \bigcup_{n\in\mathbb{N}} \mathrm{Maps}([n], \mathbb{N})$. So, there exists some $n \in \mathbb{N}$ such that $f \in \mathrm{Maps}([n], \mathbb{N})$. So, $f : [n] \to \mathbb{N}$. Thus, range$(f) \subseteq \mathbb{N}$ and is finite. So, G is well defined. To show that G is onto, fix some $s \in \mathcal{P}_{\text{fin}}(\mathbb{N})$. Since s is finite, we can fix some $m \in \mathbb{Z}$ such that $s \approx [m]$. Fix bijection $g : [m] \to s$. We know that $s \subseteq \mathbb{N}$ and that s is finite. Thus, $g \in \mathrm{Maps}([m], \mathbb{N})$. Since $m \in \mathbb{N}$, one has $g \in \bigcup_{n\in\mathbb{N}} \mathrm{Maps}([n], \mathbb{N})$ as desired. □

(b) *Proof.* Since $\bigcup_{n\in\mathbb{N}} \mathrm{Maps}([n], \mathbb{N})$ is countably infinite, one can fix a bijection $B : \mathbb{N} \to \bigcup_{n\in\mathbb{N}} \mathrm{Maps}([n], \mathbb{N})$. Observe that $G \circ B : \mathbb{N} \to \mathcal{P}_{\text{fin}}(\mathbb{N})$ is onto. So, $\mathcal{P}_{\text{fin}}(\mathbb{N})$ is countably infinite. □

(c) *Proof.* Since A is countably infinite, one can fix a bijection $h : \mathbb{N} \to A$. Now, define $j : \mathcal{P}_{\text{fin}}(\mathbb{N}) \to \mathcal{P}_{\text{fin}}(A)$ by $j(X) = \{y \in A : h(n) = y, n \in X\}$. To show that j is onto, consider some $Y \in \mathcal{P}_{\text{fin}}(A)$. Now let $X = \{n \in \mathbb{N} : h^{-1}(y) = n, y \in Y\}$. Clearly $X \in \mathcal{P}_{\text{fin}}(\mathbb{N})$. So, j is onto. Since $\mathcal{P}_{\text{fin}}(\mathbb{N})$ is countably infinite, fix bijection $k : \mathbb{N} \to \mathcal{P}_{\text{fin}}(\mathbb{N})$. Observe that $j \circ k : \mathbb{N} \to \mathcal{P}_{\text{fin}}(A)$ is onto. So, $\mathcal{P}_{\text{fin}}(A)$ is countably infinite as desired. □

Question 6

(a) *Proof.* The Axiom of Choice states that there is a function $F : P \to \bigcup P$ such that for every $S \in P$, $F(S) \in S$. We know this as $\phi \notin P$. We will show that F is an injection. Let $F(S_1) = F(S_2)$. So, $F(S_1) \in S_1$ and $F(S_2) \in S_2$. So, we have $F(S_1) \in S_1$ and $F(S_1) \in S_2$. Since P is a partition, it must be the case that $S_1 = S_2$. So, F is an injection from P to $\bigcup P$. Thus, $P \preceq \bigcup P$ as desired. □

(b) *Proof.* Let $X = \{\{1\}, \{2\}, \{1, 2\}\}$. Observe that $\bigcup X = \{1, 2\}$. Now, $|X| = 3 > 2 = |\bigcup X|$. By the pigeonhole principle, $X \npreceq \bigcup X$. □

Question 7

Proof. Fix some $x \in \mathbb{R}$. Now define $A = \{y \in \mathbb{Q} : y \leq x\}$. We claim that $\sup(A) = x$. By the definition of A, see that $y \leq x$ for all $y \in A$. So, x is clearly an upper bound of A. We will now show that x is the **least** upper bound of A, i.e. the supremum of A. For the sake of a contradiction, fix $s \in \mathbb{R}$ such that $\sup(A) = s < x$. Since $s, x \in \mathbb{R}$, there exists a rational r such that $s < r < x$. By the definition of A, one has $r \in A$. However, we know that $s < r$. So s cannot possibly be an upper bound of A. Thus, $\sup(A) = x$ as desired. □