Student Information

Full Name : Mithat Can Timurcan
Id Number : 2581064

Answer 1

a)

- Assume that the set $C \subseteq \mathbb{R}^n$ is a convex set.
- Since C is a convex set, we have the following:

$$\forall x_1, x_2 \in C, t \in [0,1] \quad tx_1 + (1-t)x_2 \in C$$

- We're going to use mathematical induction to prove that for a fixed $m > 3$, any linear combination of m points in the set C is also in the set C.
- **Base Case ($m = 3$):**
  - Consider three points x_1, x_2, x_3 in the convex set C. We want to prove that for any non-negative weights $\lambda_1, \lambda_2, \lambda_3$ such that $\sum_{i=1}^{3} \lambda_i = 1$, the convex combination $\sum_{i=1}^{3} \lambda_i x_i$ is also in C.
  - Since C is convex, the line segment between any two points in C lies in C. We can use this property to prove the base case.
  - Consider the convex combination $\lambda_1 x_1 + \lambda_2 x_2$. Without loss of generality, let's look at the combination of the first two points:

$$\lambda_1 x_1 + \lambda_2 x_2$$

  - Since $\lambda_1 + \lambda_2 = 1$, this is a convex combination of x_1 and x_2. By the convexity of C, this combination is in C.
  - Now, consider the combination of this result with the third point:

$$\lambda_3(\lambda_1 x_1 + \lambda_2 x_2) + (1-\lambda_3)x_3 = \lambda_3\lambda_1 x_1 + \lambda_3(1-\lambda_1)x_2 + (1-\lambda_3)x_3$$

  - Since $\lambda_3\lambda_1 + \lambda_3(1-\lambda_1) + (1-\lambda_3) = 1$, this is a convex combination of $\lambda_1 x_1 + \lambda_2 x_2$ and x_3. Therefore, it is also in C.
  - Hence, we've proved that the base case holds.
- **Inductive Step ($m = 3$):**
  - Assume the property holds for some k (i.e., for any k points in C, their convex combination is in C). We want to prove it for $k + 1$.

- Consider $k+1$ points $x_1, x_2, \ldots, x_{k+1}$ in C. We can use the inductive hypothesis on the first k points:

$$\sum_{i=1}^{k} \lambda_i x_i \in C$$

- Now, for the $k+1$-th point x_{k+1}, we can use the base case ($m = 3$):

$$\lambda_{k+1} x_{k+1} + (1 - \lambda_{k+1}) \left(\sum_{i=1}^{k} \lambda_i x_i \right)$$

- Since $\lambda_{k+1} \geq 0$ and $\sum_{i=1}^{k+1} \lambda_i = 1$, this is a convex combination of x_{k+1} and $\sum_{i=1}^{k} \lambda_i x_i$. By the base case, this convex combination is in C. Therefore, the property holds for $k+1$.

- By mathematical induction, we've proved that for a fixed $m > 3$, any linear combination of m points in the set C is also in the set C.

b)

- Assume that the functions f and g are convex functions.
- Since f and g are a convex functions, we have the following:

$$\forall x_1, x_2 \in \mathbb{R}^n, t \in [0,1] \quad f(tx_1 + (1-t)x_2) \leq tf(x_1) + (1-t)f(x_2)$$
$$\forall x_1, x_2 \in \mathbb{R}^n, t \in [0,1] \quad g(tx_1 + (1-t)x_2) \leq tg(x_1) + (1-t)g(x_2)$$

- Let's consider the functions:

$$f(x) = x^4, \; g(x) = x^2 - 4 \text{ and their composition } h(x) = f(g(x)) = (x^2 - 4)^4$$

- Pick $x_1 = 1/3$, $x_2 = 1/4$ and $t = 0.5$:

$$h(tx_1 + (1-t)x_2) = h(0.5 \times 1/3 + 0.5 \times 1/4) = h(7/48) = ((7/48)^2 - 1)^4$$
$$th(x_1) + (1-t)h(x_2) = 0.5((1/3)^2 - 1) + 0.5((1/4)^2 - 1)$$

- Comparing these results:

$$((7/48)^2 - 1)^4 \approx 0.9176$$
$$0.5((1/3)^2 - 1)^4 + 0.5((1/4)^2 - 1)^4 \approx 0.6983$$

- Since $((7/48)^2 - 1)^4 > 0.5((1/3)^2 - 1)^4 + 0.5((1/4)^2 - 1)^4$, the inequality in the definition doesn't hold. Hence while f and g are convex functions, their composite function $f(g(x))$ may not be convex.

c)

- Let A function $f(.) : S \subseteq \mathbb{R}^n \to \mathbb{R}$ is a convex function be s and S is convex set and the function $g(t) = f(x + tv)$ is a convex function for all $t \in \mathbb{R}$ such that $x + tv \in S$ be r.
- We need to show that $s \to r$ and $r \to s$, then we're done.
- $s \to r$.
  - Assume that $f(.) : S \subseteq \mathbb{R}^n \to \mathbb{R}$ is a convex function.
  - If $f(.)$ is a convex function and defined on S, then S must be a convex set since the domain of a convex function is also a convex set by the definition of convexity.
  - Now let's consider $g(x) = f(x + tv)$. We need to show that $g(t)$ is convex $\forall t$ such that $x + tv \in S$.
  - Let $y_1 = x + t_1 v$ and $y_2 = x + t_2 v$ be two points in S where t_1, t_2 such that $y_1, y_2 \in S$.
  - Consider $z = \lambda y_1 + (1 - \lambda) y_2$, where λ is a convex linear combination coefficient. ($\lambda \in [0, 1]$)

$$
\begin{aligned}
z &= \lambda(x + t_1 v) + (1 - \lambda)(x + t_2 v) \\
z &= x + (\lambda t_1 + (1 - \lambda) t_2) v
\end{aligned}
$$

  - Since S is a convex set, $x + (\lambda t_1 + (1 - \lambda) t_2) v \in S$ and by the convexity of $f(.)$, we can say that $g(t) = f(x + tv)$ is also convex.
  - $s \to r$ has been proved.
- $r \to s$.
  - Assume that S is a convex set and $g(t) = f(x + tv)$ is a convex function for all $t \in \mathbb{R}$ such that $x + tv \in S$.
  - In order to show $f(.)$ is a convex function, we need to consider two arbitrary points x_1, x_2 in the domain of f and show the inequality $f(\lambda x_1 + (1 - \lambda) x_2) \leq \lambda f(x_1) + (1 - \lambda) f(x_2)$ holds for $\forall \lambda \in [0, 1]$.
  - Consider x_1, x_2 in the domain of $f(.)$. Let λ be a convex linear combination coefficient ($\lambda \in [0, 1]$).
  - Now, let's consider $z = \lambda x_1 + (1 - \lambda) x_2$
  - Since S is convex, by the definition we can say that $z \in S$. Therefore we can also use the convexity of $g(t) = f(x + tv)$ for t such that $x + tv = z$.

$$g(t) = f(x + tv) = f(\lambda x_1 + (1 - \lambda) x_2)$$

  - And by the convexity of $g(t)$ we can obtain:

$$f(\lambda x_1 + (1 - \lambda) x_2) \leq \lambda f(x_1) + (1 - \lambda) f(x_2)$$

  - Therefore, $r \to s$ is also proved.

Answer 2

a)

- (i) where X is uncountable.
  - Let's denote this set as Σ.
  - Consider X as the set of real numbers. Since $X - X = \emptyset$, we can say that $X \in \Sigma$. However, it's complement $\emptyset$ is not in Σ since $X - \emptyset = X$ and X is not finite.
  - Therefore, the given set Σ is not σ-algebra on X when X is uncountable.
- (ii) where X is countably infinite.
  - Let's denote this set as Σ.
  - Consider X as the set of natural numbers. Since $X - X = \emptyset$, we can say that $X \in \Sigma$. However, it's complement $\emptyset$ is not in Σ since $X - \emptyset = X$ and X is not finite.
  - Therefore, the given set Σ is not σ-algebra on X when X is countably infinite.
- (iii) where X is finite.
  - Let's denote this set as Σ and check the conditions.
  - X is in Σ since $X - X = \emptyset$ is finite and $\emptyset$ is also in Σ since $X - \emptyset = X$ is finite.
  - If A is in Σ, then $X - A$ is either finite or $\emptyset$. The complement of $X - A$ is A, which is also a finite set in Σ.
  - If $A_1, A_2, \ldots$ are in Σ, then their complements $X - A_1, X - A_2$, are finite or $\emptyset$. The union of these sets corresponds to the complement of the union $A = A_1 \cup A_2 \cup \ldots$, which is also in Σ.
  - Therefore, the given set Σ is a σ-algebra on X when X is finite.

b)

- (i) where X is uncountable.
  - Let's denote this set as Σ.
  - Consider X as the set of real numbers and $U = \mathbb{R} - \mathbb{N}$. Since $X - U = \mathbb{N}$, we can say that $U \in \Sigma$. However, it's complement $\mathbb{N}$ is not in Σ since $X - \mathbb{N} = \mathbb{R} - \mathbb{N}$ and $\mathbb{R} - \mathbb{N}$ is uncountable.
  - Therefore, the given set Σ is not σ-algebra on X when X is uncountable.
- (ii) where X is countably infinite.
  - Let's denote this set as Σ and check the conditions.
  - X is in Σ since $X - X = \emptyset$ is countable and $\emptyset$ is also in Σ since $X - \emptyset = X$ is countable.

- If A is in Σ, then $X - A$ is either countable or is all of X. The complement of $X - A$ is A, which is also a countable set in Σ since $A \subseteq X$.
- If $A_1, A_2, ...$ are in Σ, then their complements $X - A_1, X - A_2$, are either countable or are all of X. The union of these sets corresponds to the complement of the union $A = A_1 \cup A_2 \cup ...$, which is also in Σ since union of countable sets is also countable.
- Therefore, the given set Σ is a σ-algebra on X when X is countably infinite.

- (iii) where X is finite.
  - Let's denote this set as Σ and check the conditions.
  - X is in Σ since $X - X = \emptyset$ is countable and $\emptyset$ is also in Σ since $X - \emptyset = X$ and X is countable.
  - If A is in Σ, then $X - A$ is either finite or $\emptyset$, therefore countable. The complement of $X - A$ is A, which is also a countable set in Σ.
  - If $A_1, A_2, ...$ are in Σ, then their complements $X - A_1, X - A_2$, are finite or $\emptyset$, therefore countable. The union of these sets corresponds to the complement of the union $A = A_1 \cup A_2 \cup ...$, which is also countable set in Σ.
  - Therefore, the given set Σ is a σ-algebra on X when X is finite.

c)

- (i) where X is uncountable.
  - Let's denote this set by Σ.
  - Consider X as the set of real numbers. Let $U = \{1, ..., n\}$ then $X - U = \mathbb{R} - \{1, ..., n\}$ which is infinite, therefore it's in Σ. However, it's complement $\mathbb{R} - \{1, ..., n\}$ is not in Σ since $\mathbb{R} - (\mathbb{R} - \{1, ..., n\}) = \{1, ..., n\}$ which is not infinite or Σ or X.
  - Therefore, the given set Σ is not a σ-algebra on X when X is uncountable.
- (ii) where X is countably infinite.
  - Let's denote this set by Σ.
  - Consider X as the set of national numbers. Let $U = \{1, ..., n\}$ then $X - U = \mathbb{N} - \{1, ..., n\}$ which is infinite, therefore it's in Σ. However, it's complement $\mathbb{N} - \{1, ..., n\}$ is not in Σ since $\mathbb{N} - (\mathbb{N} - \{1, ..., n\}) = \{1, ..., n\}$ which is not infinite or Σ or X.
  - Therefore, the given set Σ is not a σ-algebra on X when X is countably infinite.
- (iii) where X is finite.
  - Let's denote this set by Σ.
  - Since X is finite, $X - U$ will also be finite. Therefore Σ will only include X itself and the $\emptyset$.

- X is in Σ.
- Σ is closed under complementation. The complement of X is the $\emptyset$ which is also in Σ and vice versa.
- Σ is closed under countable unions. The union of X and $\emptyset$ is X which is also in Σ.
- Therefore, the given set Σ is a σ-algebra on X when X is finite.

Answer 3

a)

- Let $ax \equiv b (\text{mod } p)$ has a solution for x be s and $gcd(a, p)|b$ be r.
- We need to show that $s \rightarrow r$ and $r \rightarrow s$, then we're done.
- $s \rightarrow r$.
  - Assume that $ax \equiv b (\text{mod } p)$, then $ax = pt + b$, $\exists t \in \mathbb{Z}$.
  - $ax - pt = b$
  - Let $gcd(a, p) = d$ then $d|a$ and $d|p$.
  - We can also say that $d|ax$ and $d|pt \rightarrow d|(ax - pt)$.
  - $d|(ax - pt) \rightarrow d|b$.
  - We get $gcd(a, p)|b$. $s \rightarrow r$ has been proved.
- $r \rightarrow s$.
  - Assume that $d = gcd(a, p)$, then $\exists k, t \in \mathbb{Z}$ such that $ak + pt = d$ by Bezout's Identity.
  - $b = cd \rightarrow b = c(ak + pt) = a(ck) + p(ct)$
  - Therefore, we get a solution for $ax \equiv b (\text{mod } p)$.
  - $r \rightarrow s$ has been proved.

b)

- Assume we have the pair of congruences:

$$\begin{aligned} a_1x &\equiv b_1 \pmod{p_1} \\ a_2x &\equiv b_2 \pmod{p_2} \end{aligned}$$

- We are given the conditions $\gcd(p_1, p_2) = 1$, $\gcd(a_1, p_1) \mid b_1$, and $\gcd(a_2, p_2) \mid b_2$.
- Let $d = \gcd(p_1, p_2)$. Since $d = \gcd(p_1, p_2) = 1$, we can apply Bezout's Identity to find integers m and n such that $mp_1 + np_2 = 1$.

- Now, consider the following linear combination:

$$c = m \cdot p_1 \cdot b_2 + n \cdot p_2 \cdot b_1$$

- By rearranging the terms, we get:

$$c \equiv m \cdot p_1 \cdot b_2 \pmod{p_1}$$
$$c \equiv n \cdot p_2 \cdot b_1 \pmod{p_2}$$

- Now, let's consider $a = a_1 \cdot p_2 \cdot b_2 + a_2 \cdot p_1 \cdot b_1$. Notice that a is a linear combination of a_1 and a_2 with coefficients being multiples of p_1 and p_2.

- Now, let's show that $x = c$ satisfies both congruences:

$$a_1 \cdot x = a_1 \cdot (m \cdot p_1 \cdot b_2 + n \cdot p_2 \cdot b_1)$$
$$a_2 \cdot x = a_2 \cdot (m \cdot p_1 \cdot b_2 + n \cdot p_2 \cdot b_1)$$

- Now, consider these expressions modulo p_1 and p_2. It will be found that they are congruent to b_1 and b_2 modulo p_1 and p_2 respectively.

- Therefore, $x = c$ is a solution to the system of congruences $a_1x \equiv b_1 \pmod{p_1}$ and $a_2x \equiv b_2 \pmod{p_2}$ when $\gcd(p_1, p_2) = 1$, $\gcd(a_1, p_1) \mid b_1$, and $\gcd(a_2, p_2) \mid b_2$.

c)

- To prove that the given system of congruences has a solution of the form $x \equiv c \pmod{\Pi}$, where $\Pi = p_1p_2 \dots p_k$, $\gcd(p_1, \dots, p_k) = 1$, and $\gcd(a_i, p_i) \mid b_i$ for some $c \in \mathbb{Z}$ and $i = 1, \dots, k$, we can use the Chinese Remainder Theorem.

- The Chinese Remainder Theorem states that if $m_1, m_2, \dots, m_k$ are pairwise coprime integers (i.e., $\gcd(m_i, m_j) = 1$ for all $i \neq j$), and $a_1, a_2, \dots, a_k$ are any integers, then the system of simultaneous congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

  has a unique solution modulo $M = m_1m_2 \dots m_k$.

- Now, let's relate this to the given system of congruences:

$$\begin{aligned} a_1x &\equiv b_1 \pmod{p_1} \\ a_2x &\equiv b_2 \pmod{p_2} \\ &\vdots \\ a_kx &\equiv b_k \pmod{p_k} \end{aligned}$$

- Note that the conditions $\gcd(p_1, \ldots, p_k) = 1$ and $\gcd(a_i, p_i) \mid b_i$ for each i are satisfied.
- Now, set $m_1 = p_1, m_2 = p_2, \ldots, m_k = p_k$. Since $\gcd(p_i, p_j) = 1$ for $i \neq j$, the conditions of the Chinese Remainder Theorem are met.
- By Chinese Remainder Theorem, the system of congruences has a unique solution x modulo $M = p_1 p_2 \ldots p_k = \Pi$. Therefore, there exists a solution of the form $x \equiv c \pmod{\Pi}$.

Answer 4

a)

- Let's denote the set $\prod_{i \in \mathbb{Z}^+} X$ as X^T. Then we'll assume that this set is countable. Since it's countable, there should exist such a function $f : \mathbb{Z}^+ \to X^T$ which is surjective.
- For a defined function f, we have $f(n) = (x_{n1}, x_{n2}, ..., x_{nn}, ...)$ where each $x_{ij} \in \{a, ..., z\}$.
- Then we can consider $y = (y_1, y_2, ...) \in X^T$ defined by

$$y_n = \begin{cases} c & \text{if } x_{nn} \neq c \\ t & \text{if } x_{nn} = c \end{cases}$$

- Such defined y is not mapped to by our function f, it differs from each $f(n)$ by at least one coordinate. Therefore, f is not surjective, we get a contradiction. The set X^T is not countable.

b)

- Let $\{Y_i\}_{i \in \mathbb{Z}^+}$ be a family of sets, each of which is countably infinite. We want to determine whether the set $S = \bigcup_{i \in \mathbb{Z}^+} Y_i$ is countable or not.
- To show whether S is countable or not, we need to check if we can construct a function $f : \mathbb{Z}^+ \to S$ which is surjective.
- Since each Y_i is countably infinite, we can list its elements as $Y_i = \{y_{i1}, y_{i2}, y_{i3}, ...\}$. Now, we can create a function that maps the elements of each set:

$$\begin{aligned} f(1) &= y_{11}, \\ f(2) &= y_{21}, \\ f(3) &= y_{12}, \\ f(4) &= y_{31}, \\ f(5) &= y_{22}, \\ f(6) &= y_{13}, \end{aligned}$$

  and so on.
- Therefore, by using Cantor's diagonal argument, we can say that $S = \bigcup_{i \in \mathbb{Z}^+} Y_i$ is countable.