Long Quiz 2 - Solutions

December 02, 2020

Problem 1. Suppose (X, R) and (X', R') are ordered (linearly ordered) sets. A mapping $f : X \to X'$ is called an *isomorphism* from (X, R) to (X', R') iff

i) $f : X \to X'$ is bijective, and

ii) for all $x, y \in X$, $xRy \iff f(x)R'f(y)$.

Find an example of a linearly ordered set (A, R) and an isomorphism $f : A \to A$ such that $f(x) \neq x$ for all $x \in A$.

[Clearly describe (A, R) and show that it is a linearly ordered set. Define the map f and show that it is an isomorphism. Finally, prove that $f(x) \neq x$.]

Solution. Let $A = \mathbb{Z}$, the set of integers and $R =\leq=$ the usual order relation on the integers. Thus $(A, R) = (\mathbb{Z}, \leq)$.

We know that $x \leq x$ for all $x \in \mathbb{Z}$. So, $\leq$ is reflexive.

Suppose $x, y \in \mathbb{Z}$ such that $x \leq y$ and $y \leq x$. Then $x = y$. Thus $\leq$ is antisymmetric.

Suppose $x, y, z \in \mathbb{Z}$ such that $x \leq y$ and $y \leq z$. Then $x \leq z$. Thus $\leq$ is transitive.

Finally, suppose $x, y \in \mathbb{Z}$. Then either $x \leq y$ or $y \leq x$.

Thus $\leq$ is a linear ordering on $\mathbb{Z}$, that is, $(\mathbb{Z}, \leq)$ is a linearly ordered set.

We define $f : \mathbb{Z} \to \mathbb{Z}$ by $f(x) = x + 1$ for all $x \in \mathbb{Z}$.

Let $x, y \in \mathbb{Z}$ such that $f(x) = f(y)$. Then $x+1 = y+1$, which implies that $x = y$. So, f is injective.

Let $y \in \mathbb{Z}$. Then $y - 1 \in \mathbb{Z}$ and $f(y - 1) = y - 1 + 1 = y$. Thus f is surjective.

Hence f is bijective.

We note that for any $x, y \in \mathbb{Z}$, $x \leq y \iff x + 1 \leq y + 1$, that is, $f(x) \leq f(y)$.

Hence f is an isomorphism from $(Z, \leq)$ to $(\mathbb{Z}, \leq)$.

Finally, for any $x \in \mathbb{Z}$, $f(x) = x + 1 \neq x$. $\square$

Problem 2. Suppose R and S are binary relations on a set $A \neq \emptyset$. Show that $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$.

Solution. Let $x, y \in A$ such that $(x, y) \in (R \circ S)^{-1}$.

Then $(y, x) \in R \circ S$. This implies that there exists a $z \in A$ such that $(y, z) \in R$ and $(z, x) \in S$.

Now, $(y, z) \in R$ implies $(z, y) \in R^{-1}$ and $(z, x) \in S$ implies $(x, z) \in S^{-1}$.

Then $(x,z) \in S^{-1}$ and $(z,y) \in R^{-1}$ implies that $(x,y) \in S^{-1} \circ R^{-1}$. Thus

$$(R \circ S)^{-1} \subseteq S^{-1} \circ R^{-1}. \tag{1}$$

Conversely, let $x, y \in A$ such that $(x,y) \in S^{-1} \circ R^{1}$.

Then there exists $z \in A$ such that $(x,z) \in S^{-1}$ and $(z,y) \in R^{-1}$.

Now, $(x,z) \in S^{-1}$ implies that $(z,x) \in S$ and $(z,y) \in R^{-1}$ implies that $(y,z) \in R$.

Then $(y,z) \in R$ and $(z,x) \in S$ implies that $(y,x) \in R \circ S$. So $(x,y) \in (R \circ S)^{-1}$. Thus

$$S^{-1} \circ R^{-1} \subseteq (R \circ S)^{-1} \tag{2}$$

Combining (1) and (2), we have $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$. □

Problem 3. Suppose X is a finite set. Show that a function $f : X \to X$ is injective iff it is surjective.

Solution. We note that if $X = \emptyset$, then the empty function is the only function from X to X.

The empty function is injective, since if not, then there exist $x_1 \neq x_2 \in X$ such that $f(x_1) = f(x_2)$. But that is not possible as $X = \emptyset$.

The empty function is surjective, since if not, then there exists $y \in X$ such that $y \neq f(x)$ for all $x \in X$. But X is empty, so there cannot exists such a y.

Thus the only function from X to X, where $X = \emptyset$ is injective and surjective. Hence a function from $X = \emptyset$ to itself is injective iff it is surjective.

Now suppose $X \neq \emptyset$.

If $X = \{x\}$, a singleton, then the only injective function from X to X is the identity function that maps x to itself. This is also the only surjective function. Thus the only injective function is also the only surjective function from X to itself. Hence a function from X to itself, where $|X| = 1$ is injective iff it is surjective.

Now, let $|X| \geq 2$ and suppose $X = \{x_1, x_2, \ldots, x_n\}$.

Suppose $f : X \to X$ is injective.

We need to show that f is surjective. Suppose the contrary.

Since f is not surjective, there exists $x_i \in X$, $1 \leq i \leq n$ such that $f(x_j) \neq x_i$ for all $1 \leq j \leq n$.

Thus f maps the n distinct elements of X into the $n-1$ distinct elements in $X \setminus \{x_i\}$. This implies that at least two of the elements in X must be mapped to one element of $X \setminus \{x_i\}$. So f is not injective. This is a contradiction. Hence f is surjective.

Conversely, suppose $f : X \to X$ is surjective.

We need to show that f is injective. Suppose the contrary.

Since f is not injective, there exist $x_i, x_j \in X$, where $1 \leq i < j \leq n$ such that $f(x_i) = f(x_j)$.

Let $f(x_i) = f(x_j) = x_k \in X$ for some $1 \leq k \leq n$. Since f is a function the pre-images of distinct images are distinct, in other words $f^{-1}(\{x_s\}) \cap f^{-1}(\{x_t\}) = \emptyset$ for all $1 \leq s \neq t \leq n$. Also, since f is surjective, each element of X has at least one pre-image in X.

Now, since x_k has at least 2 pre-images in X, this implies that there are at most $n-2$ distinct pre-images available for the $n-1$ elements in $X \setminus \{x_k\}$. This implies that not all elements in $X \setminus \{x_k\}$ can have distinct pre-images.

This contradicts the fact that f is a function. Hence f must be injective.

Thus for any finite X, a function $f : X \to X$ is injective iff it is surjective. $\square$

Problem 4. Let p be a prime and let $k \geq 1$ be a natural number. Prove that for $k < p$, $\binom{p}{k}$ is divisible by p.

Solution. We know that

$$\binom{p}{k} = \frac{\prod_{i=0}^{k-1}(p-i)}{k!}.$$

Now, since $k \geq 1$, the product in the numerator of the expression on the right hand side of the above equation is not an empty product, that is, $\prod_{i=0}^{k-1}(p-i) \neq 1$. Thus $p = (p-0)$ is a factor in the product in the numerator.

Now, $\binom{p}{k}$ is the number of k-element subsets of a p-element set, and hence is a natural number. Thus $k!$ divides $\prod_{i=0}^{k-1}(p-i)$. However, since p is a prime and $k < p$, $k, (k-1), \ldots, 3, 2$ do not divide p. Thus $k!$ must divide $\prod_{i=1}^{k-1}(p-i)$.

Let $\frac{\prod_{i=1}^{k-1}(p-i)}{k!} = l \in \mathbb{Z}^+$. Then $\binom{p}{k} = p \cdot l$. Thus $\binom{p}{k}$ is divisible by p. $\square$

Problem 5. Prove the Binomial Theorem, i.e.,

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k, \text{ where } n \in \mathbb{N},$$

by induction on n.

Solution. Base case: $n = 0$

We note that $(1+x)^0 = 1$ and $\sum_{k=0}^{n} \binom{n}{k} x^k = \binom{0}{0} x^0 = 1$. Thus the equation holds for $n = 0$.

Induction hypothesis: Suppose the equation holds for some $n \in \mathbb{N}$. Thus

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

Induction step: We need to show that the equation holds for $n+1$. We note that

$$(1+x)^{n+1} = (1+x) \cdot (1+x)^n = (1+x) \sum_{k=0}^{n} \binom{n}{k} x^k,$$

by the induction hypothesis. Thus

$$\begin{aligned}(1+x)^{n+1} &= \sum_{k=0}^{n} \binom{n}{k} x^k + \sum_{k=0}^{n} \binom{n}{k} x^{k+1} \\ &= \binom{n}{0} x^0 + \left[\binom{n}{1} + \binom{n}{0}\right] x + \left[\binom{n}{2} + \binom{n}{1}\right] x^2 + \cdots + \\ &\quad \left[\binom{n}{n} + \binom{n}{n-1}\right] x^n + \binom{n}{n} x^{n+1}\end{aligned}$$

Now, we know that $\binom{n}{0} = 1 = \binom{n+1}{0}$, $\binom{n}{n} = 1 = \binom{n+1}{n+1}$, and for any $1 \leq k \leq n$,

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

Thus

$$\begin{aligned}(1+x)^{n+1} &= \binom{n+1}{0} x^0 + \binom{n+1}{1} x + \binom{n+1}{2} x^2 + \cdots + \binom{n+1}{n} x^n + \binom{n+1}{n+1} x^{n+1} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k.\end{aligned}$$

Thus the equation holds for $n+1$. Hence, by the principle of mathematical induction,

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k, \text{ for all } n \in \mathbb{N}$$

□

Problem 6. Find the coefficient of x^2y^8z in $(2x + y^2 - 5z)^7$.

Solution. We note that $x^2y^8z = x^2(y^2)^4z$. Now using the Multinomial theorem, we see that the coefficient of $(2x)^2(y^2)^4(-5z)$ in the expansion of $(2x + y^2 - 5z)^7$ is

$$\binom{7}{2,4,1} = \frac{7!}{2! \cdot 4! \cdot 1!} = 105.$$

Thus the x^2y^8z-term in the expansion of $(2x + y^2 - 5z)^7$ is

$$105 \cdot (2x)^2 \cdot (y^2)^4 \cdot (-5z) = 105 \cdot 4 \cdot (-5)x^2y^8z = -2100x^2y^8z.$$

Hence the coefficient of x^2y^8z in $(2x + y^2 - 5z)^7$ is -2100. □

Problem 7. How many bitstrings (that is, strings of 0s and 1s) of length 10 are there that contain an equal number of 0s and 1s?

Solution. We first note that the bitstrings of length 10 that contain an equal number of 0s and 1s have exactly 5 of each bit.

Thus the number of such strings will be

$$\frac{10!}{5! \cdot 5!} = 252.$$

□

Problem 8. Let N be an n-element set and M be an m-element set. Define a bijection between the set of all mappings $f : N \to M$ and the n-fold Cartesian product M^n. (Define a map and show that it is a bijection.)

Solution. We assume that $m, n \in \mathbb{Z}^+$.

Suppose $N = \{x_1, x_2, \ldots, x_n\}$. Let $F = \{f : N \to M\}$ = the set of all mappings from N to M.

We note that any mapping $f : N \to M$ is completely described by the images of the n elements of N, $f(x_1), f(x_2), \ldots, f(x_n)$.

Now, since $f(x_1), f(x_2), \ldots, f(x_n) \in M$, the n-tuple $(f(x_1), f(x_2), \ldots, f(x_n)) \in M^n$.

We then define a map $\Theta : F \to M^n$ as follows.

$$\Theta(f) = (f(x_1), f(x_2), \ldots, f(x_n))$$

Suppose $f_1 = f_2 \in F$. Then $f_1(x_i) = f_2(x_i)$ for each $1 \leq i \leq n$. Thus

$$\Theta(f_1) = (f_1(x_1), f_1(x_2), \ldots, f_1(x_n)) = (f_2(x_1), f_2(x_2), \ldots, f_2(x_n)) = \Theta(f_2).$$

Hence Θ is well-defined.

Now, let $f_1, f_2 \in F$ such that $\Theta(f_1) = \Theta(f_2)$. Thus

$$(f_1(x_1), f_1(x_2), \ldots, f_1(x_n)) = (f_2(x_1), f_2(x_2), \ldots, f_2(x_n)) = \Theta(f_2),$$

which implies that $f_1(x_i) = f_2(x_i)$ for all $1 \leq i \leq n$. Thus $f_1 = f_2$. Hence Θ is injective.

Now, suppose $(y_1, y_2, \ldots, y_n) \in M^n$. We can then define a map $f : N \to M$ as follows.

$$f(x_i) = y_i, \text{ for each } 1 \leq i \leq n$$

Clearly, $\Theta(f) = (f(x_1), f(x_2), \ldots, f(x_n)) = (y_1, y_2, \ldots, y_n)$. Thus Θ is surjective.

Hence Θ is a bijective map from $F = \{f : N \to M\}$ to M^n. □