Math 521A Exam 2 Solutions

Nov 2, 2009

1. (10 pts) Find all integers $n > 1$ such that $\phi(n) = 2$.

   Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the prime factorization of n. Then

   $$2 = \phi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1).$$

   Clearly no prime $p > 3$ can appear in the prime factorization, otherwise $p - 1 > 2$ appears as a factor in $\phi(n)$. So $n = 2^\alpha 3^\beta$. It is also clear that $\alpha \leq 2$ and $\beta \leq 1$, otherwise $2^{\alpha-1}$ or $3^{\beta-1}$ is already more than 2. Now there only five cases to check:

   $$\begin{aligned} \phi(3^1) &= 2 \\ \phi(2^1) &= 1 \\ \phi(2^1 3^1) &= 2 \\ \phi(2^2) &= 2 \\ \phi(2^2 3^1) &= 4 \end{aligned}$$

   So the integers we are looking for are 3, 4, and 6.

2. (5 pts each) Let $f : A \to B$ and $g : B \to C$ be functions.
   (a) Prove that if $g \circ f$ is one-to-one then f is one-to-one.

   Let $x_1, x_2 \in A$. If $f(x_1) = f(x_2)$, then $g \circ f(x_1) = g \circ f(x_1)$. Since $g \circ f$ is one-to-one, it follows $x_1 = x_2$. So $f(x_1) = f(x_2)$ implies $x_1 = x_2$. This shows f is one-to-one.

   (b) Prove that if $g \circ f$ is onto then g is onto.

   Since $f(A) \subseteq B$, $g \circ f(A) \subseteq g(B)$. But $g \circ f(A) = C$ because $g \circ f$ is onto and $g(B) \subseteq C$, so

   $$C = g \circ f(A) \subseteq g(B) \subseteq C \implies g(B) = C.$$

   That is g is onto.

3. Let $T = \{(x, y, z) \in \mathbb{R}^3 \mid (x, y, z) \neq (0, 0, 0)\}$. Define $\sim$ on T by $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ if there exists a nonzero real number λ such that $x_1 = \lambda x_2$, $y_1 = \lambda y_2$, and $z_1 = \lambda z_2$.
   (a) (8 pts) Show that $\sim$ is an equivalence relation.

   Reflexivity: Since $x = 1 \cdot x$, $y = 1 \cdot y$, and $z = 1 \cdot z$, $(x, y, z) \sim (x, y, z)$.

   Symmetry: If $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ then $x_1 = \lambda x_2$, $y_1 = \lambda y_2$, and $z_1 = \lambda z_2$ for some $\lambda \in \mathbb{R}^*$. Hence $\lambda^{-1} \in \mathbb{R}^*$ and $x_2 = \lambda^{-1} x_1$, $y_2 = \lambda^{-1} y_1$, and $z_2 = \lambda^{-1} z_1$. Therefore $(x_2, y_2, z_2) \sim (x_1, y_1, z_1)$.

   Transitivity: If $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ and $(x_2, y_2, z_2) \sim (x_3, y_3, z_3)$, then $x_1 = \lambda x_2$, $y_1 = \lambda y_2$, and $z_1 = \lambda z_2$ and $x_2 = \mu x_3$, $y_2 = \mu y_3$, and $z_2 = \mu z_3$ for some $\lambda, \mu \in \mathbb{R}^*$. Therefore $\lambda\mu \in \mathbb{R}^*$ and $x_1 = \lambda\mu x_3$, $y_1 = \lambda\mu y_3$, and $z_1 = \lambda\mu z_3$. Therefore $(x_1, y_1, z_1) \sim (x_3, y_3, z_3)$.

   (b) (2 pts) Give a geometric description of the equivalence class of (x, y, z).

   It is the line passing through (x, y, z) and the origin.

4. (a) (3 pts) Define equivalence class.

   See Definition 2.2.2.

   (b) (3 pts) Define partition.

   Let S be a nonempty set. A collection $\mathcal{P}$ of nonempty subsets of S is called a *partition* if

   (i) the subsets are pairwise disjoint and

   (ii) their union is all of S.

   Alternately, see Definition 2.2.4.

   (c) (10 pts) Let $\sim$ be an equivalence relation on the set S. Prove that the equivalence classes of $\sim$ form a partition of S.

   See the proof of Proposition 2.2.3 or the proof we gave in class.

5. (a) (3 pts) Define permutation.

   See Definition 2.3.1.

   (b) (5 pts) Give an example of a permutation on the set $\mathbb{R}$. Prove that your example is really a permutation.

   The identity function is one possible example. But here is a more interesting one. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = -x$. Then $f \circ f(x) = x$ for all $x \in \mathbb{R}$. So f has an inverse. Therefore f is one-to-one and onto, i.e. a permutation.

   (c) (3 pts) Compute

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 5 & 3 & 2 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 5 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 2 & 4 & 5 \end{pmatrix}$$

   (d) (3 pts) Compute

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 1 & 2 & 3 \end{pmatrix}^{-1}.$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 1 & 2 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 3 & 2 & 1 \end{pmatrix}$$

6. **Extra credit problem.** Let $f : A \to B$ be a function. We say $g : B \to A$ is a *left inverse* of f if $g \circ f = 1_A$ and is a *right inverse* of f if $f \circ g = 1_B$.

   (a) (5 pts) Construct an example of a function f which has a left inverse but no right inverse. Be sure to justify your example.

   Let $f, g : \mathbb{R} \to \mathbb{R}$ be $f(x) = e^x$ and $g(x) = \ln(x)$. Then $g \circ f(x) = \ln(e^x) = x$ for all $x \in \mathbb{R}$. So f has a left inverse.
   Suppose $h : \mathbb{R} \to \mathbb{R}$ were a right inverse of f. Then $f \circ h = 1_{\mathbb{R}}$, which is an onto function. By problem 2(b), f would have to be onto. But it is clearly not, as the values of f are all positive. So f cannot have a right inverse.

(b) (10 pts) Prove that f has a left inverse if and only if f is one-to-one.

Suppose f has a left inverse g. Then $g \circ f = 1_A$, which is a one-to-one function. By problem 2(a), f must also be one-to-one.
Conversely, suppose f is one-to-one. Define $g : B \to A$ as follows. First, pick an element $a \in A$. Now let $y \in B$. If $y \notin \text{im}(f)$ then let $g(y) = a$. If $y \in \text{im}(f)$, then there is an $x \in A$ such that $f(x) = y$. Since f is one-to-one, there is exactly one such $x \in A$, therefore letting $g(y) = x$ is well-defined.
We claim $g : B \to A$ is a left inverse of f. Let $x \in A$. Then $f(x) \in \text{im}(f)$. So $g(f(x))$ is by definition the element $x' \in A$ such that $f(x') = f(x)$. Since f is one-to-one, $x' = x$, and hence $g(f(x)) = x$. Therefore $g \circ f = 1_A$.