Math 3124 Exam 1 Solutions

Feb 18, 2004

1. Let $\alpha : S \to T$ be a map.
   (a) (3 pts) Define what it means for α to be one-to-one.

   α is one-to-one if for all $x, y \in S$ such that $\alpha(x) = \alpha(y)$, $x = y$.

   (b) (3 pts) Define what it means for α to be onto.

   α is onto if for all $y \in T$ there exists $x \in S$ such that $\alpha(x) = y$.

   (c) (3 pts) Define what it means for α to have an inverse.

   α has an inverse $\beta : T \to S$ if $\alpha \circ \beta = \iota_T$ and $\beta \circ \alpha = \iota_S$.

   (d) (10 pts) Prove that α has an inverse if and only if α is one-to-one and onto. You may use any result from lecture, the textbook, or the homework, except for the theorem which says exactly what you are asked to prove.

   Proof: Suppose α has an inverse β. Then $\beta \circ \alpha = \iota_S$, which is one-to-one, hence α is one-to-one by Theorem 2.1 in Durbin. Also, $\alpha \circ \beta = \iota_T$, which is onto, hence α is onto by the same theorem.
   Conversely, let α be one-to-one and onto. This means that every element of T has a unique preimage with respect to α. So we can construct a map $\beta : T \to S$ by setting $\beta(t) = s$ where $\alpha(s) = t$ for each $t \in T$.
   We claim β is the inverse of α. For any $s \in S$, $\beta \circ \alpha(s) = \beta(\alpha(s)) = s$ because $\beta(\alpha(s))$ is the unique preimage of $\alpha(s)$ w.r.t. α, which is s. For any $t \in T$, $\alpha \circ \beta(t) = \alpha(\beta(t)) = t$ because $\beta(t)$ is a preimage of t w.r.t. α, so α must map it to t.

2. (10 pts) Let S be a set of n elements. How many different commutative operations are there on S? (Hint: What does commutativity mean in terms of the Cayley table? Count Cayley tables.)

   A commutative operation has to a Cayley table which is symmetric w.r.t. reflection across its diagonal. Clearly, different Cayley tables correspond to different operations. So we can reduce the problem to counting Cayley tables with this symmetry.

   When constructing such a Cayley table, we are free to choose anything for the entries on and above the diagonal, whereas the entries below the diagonal are determined by the symmetry. So we have n choices for each of $n + (n-1) + \cdots + 1 = n(n+1)/2$ entries. This yields $n^{n(n+1)/2}$ different operations.

3. (7 pts each) Prove or disprove the following.
   (a) If G is a group and $g, x, y \in G$ such that $gx = gy$, then $x = y$.

   Proof: Multiply both sides on the left by g^{-1}:

   $$g^{-1}gx = g^{-1}gy \implies ex = ey \implies x = y.$$

(b) If $*$ is a commutative operation on the set S, then $*$ is also associative.

This is false. Counterexample: let $S = \mathbb{R}$ and $m * n = (m+n)/2$. This is clearly a commutative operation. But it is not associative, e.g.

$$(0 * 0) * 1 = \frac{1}{2} \qquad \text{but} \qquad 0 * (0 * 1) = \frac{1}{4}.$$

(c) Let S be a set with an operation $*$ and T a subset of S which is closed under $*$. If $*$ is associative on S, then it is also associative on T.

Proof: We need to show that

$$(x * y) * z = x * (y * z) \qquad \forall\, x, y, z \in T.$$

But any such x, y, z are also in S, so the above relation holds by associativity of $*$ on S.

4. (15 pts) **Extra credit problem.** This is a hard problem. Attempt it only when you are done with everything else.

Let S be a nonempty set with an associative operation $*$. Suppose that

(a) there exists a left identity $e \in S$ such that $e * x = x$ for all $x \in S$,

(b) for each $x \in S$ there exists an $x' \in S$ such that $x' * x = e$ (notice this is not quite a left inverse because e may not be an identity).

Prove that S is a group. (Hint: prove first that if $y * y = y$ then $y = e$, then that $x * x' = e$, and finally that e is also a right identity.)

Claim: If $y \in S$ such that $y * y = y$, then $y = e$.
Proof: $y' * (y * y) = y' * y \implies (y' * y) * y = e \implies e * y = e \implies y = e.$

Claim: For all $x \in S$, $x * x' = e$.
Proof: $(x * x') * (x * x') = x * (x' * x) * x' = x * e * x' = x * (e * x') = x * x'$. So by the previous claim $x * x' = e$.

Claim: For all $x \in S$, $x * e = x$.
Proof: $x * e = x * (x' * x) = (x * x') * x = e * x = x.$