15-251: Great Theoretical Ideas In Computer Science

Recitation 13 Solutions

Forget about groups?

$(A, \circ)$ is defined as a group when the following four conditions are met:
1. Closure: for all $x, y \in A$, $x \circ y \in A$
2. Associativity: for all $x, y, z \in A$, $(x \circ y) \circ z = x \circ (y \circ z)$.
3. Identity: there is an $e \in A$ such that for all $x \in A$, $x \circ e = e \circ x = x$.
4. Inverses: for every $x \in A$, there is a $y \in A$ such that $x \circ y = y \circ x = e$.

We define $(A, \circ)$ as abelian (commutative) if for every $x, y \in A$, $x \circ y = y \circ x$.

(a) Is $\mathbb{Z}^+$ equipped with the following function a group? If $a \neq b$ then $f(a, b) = \max(a, b)$. Otherwise, $f(a, b) = 1$.

Closure: yes
Associativity: consider $x = y = 3$ and $z = 2$.
$(3 \circ 3) \circ 2 = 1 \circ 2 = 2$
$3 \circ (3 \circ 2) = 3 \circ 3 = 1$
Identity $e = 1$.
Inverses $a^{-1} = a$.

Mighty Morphin'

We define a homomorphism from a group $(A, \circ)$ to a group $(B, *)$ as a function $f : A \to B$ such that for every $x, y \in A$, $f(x \circ y) = f(x) * f(y)$. $(A, \circ)$ is homomorphic to $(B, *)$ if and only if there is a homomorphism from $(A, \circ)$ to $(B, *)$.
We define an isomorphism as a bijective homomorphism. Two groups are isomorphic if there is an isomorphism between them. They are essentially "the same" group, just with different labels.
We define an automorphism as an isomorphism between a group and itself.

(a) If f is a homomorphism from a group A to a group B, and e_A is the identity of A, is $f(e_A)$ the identity of B?

Let e_B be the identity of B.
Let $x \in A$.
$e_B * f(x) = f(x) = f(e_A \circ x) = f(e_A) * f(x)$.
Multiply on the right by $(f(x))^{-1}$.
$e_B = f(e_A)$.

(b) If f is a homomorphism from a group A to a group B, and $x \in A$, if $f(x^{-1}) = f(x)^{-1}$?

Let $x \in A$.
From before:
$e_B = f(e_A)$
Definition of inverses:
$f(x) * f(x)^{-1} = f(x \circ x^{-1})$
Homomorphism property:
$f(x) * f(x)^{-1} = f(x) * f(x^{-1})$
Canceling:
$f(x)^{-1} = f(x^{-1})$

(c) Is $(\mathbb{Z}, +)$ homomorphic to $(\mathbb{Q}, +)$?

Yes. $f(x) = x$.

(d) Is $(\mathbb{Z}, +)$ isomorphic to $(\mathbb{Q}, +)$?

No.
Assume f is an isomorphism.
Let $y = f(1)/2$. This gives us $y + y = f(1)$.
Let $x \in \mathbb{Z}$ such that $f(x) = y$.
$f(x) + f(x) = f(1)$.
By the homomorphism property:
$f(x + x) = f(1)$.
f is an inverse:
$x + x = 1$.
$x = 1/2$, but $x \in \mathbb{Z}$. Contradiction.

(e) Is $(\mathbb{R}, +)$ isomorphic to $(\mathbb{Q}, +)$?

No. Different cardinalities.

(f) Let A be a group. Let B be the set of automorphisms on A. Does B under functional composition form a group?

Closure:
Consider two automorphisms f and g. The composition of f and g will be a permutation. $f(g(x * x)) = f(g(x) * g(x)) = f(g(x)) * f(g(x))$, so $f \circ g$ is a homomorphism. Therefore $f \circ g$ is an automorphism.
Associativity: trivial.
Identity: If $f(x)$ is the identity function, it is a permutation. $f(x * x) = x * x = f(x) * f(x)$, so f is a homomorphism. The identity function is an identity.
Inverses: If $f(x)$ is an automorphism, then $f(x * x) = f(x) * f(x)$. Let $y = f(x)$. $f(f^{-1}(y) * f^{-1}(y)) = y * y$. Apply f^{-1} to both sides: $f^{-1}(y) * f^{-1}(y) = f^{-1}(y * y)$.

(g) A fixed point in a function f is a value x such that $f(x) = x$. Let $k \in \mathbb{N}$. Let A be the set of permutations of $\{1, \ldots, n\}$ with exactly k fixed points. For which value(s) of k is A under composition a group?

If $k = n$, then there is a single permutation, which forms a group.
If $k = n - 1$, then the first $n - 1$ fixed points fix the last point, and there are no permutations. Not a group.
Otherwise let $f(x)$ and $g(x)$ be as follows:
$f = (1, 2, 3, 4, \ldots, k, n, k + 1, k + 2, \ldots, n - 1)$.
$g = (1, 2, 3, 4, \ldots, k, k + 2, k + 3, \ldots, n, k + 1)$.
$f \circ g = (1, 2, 3, 4, \ldots, k, k+1, k+2, \ldots, n)$, so $f \circ g$ is the identity, and has n fixed points instead of k. Not a group.
This has at least

Induction

Consider the following proofs. What went wrong?

(a) Let $P(n)$ be the statement that every graph with n vertices and minimum degree of one is connected.
Claim: for all $n \geq 2$, $P(n)$.
Base Case:
$P(2)$ is trivial.
Induction hypothesis:
Assume $P(n)$ for some n.
Induction Step:
Start with a graph G with n vertices and min degree of one. By the IH, G is connected. Add a vertex v to G to form G'. The minimum degree in G' should be one, so we add one edge from v to a vertex u. Because G was connected, and there is an edge connecting v to the original graph, G' is connected.
QED

Fundamentally, the issue lies in the concept of "adding" to the original object. We want to show that if every object of size n has a property, then every object of size $n + 1$ has a property. If we start with an object of size n, and add something, there is no guarantee that we will form every possible object of size $n + 1$. Consider the graph $G = (\{1, 2, 3, 4\}, \{\{1, 2\}, \{3, 4\}\})$. There is no graph with min degree 1 to which we can add a vertex and form G.

Instead, the correct approach is to prove the claim directly.
1. Assume the induction hypothesis.
2. Take an arbitrary object G of size $n + 1$.
3. Contract that object or remove a node from it, to form G' of size n.
4. Argue that G' is a valid structure, so the IH applies to G'.
5. Argue why the claim applies to G.

In this proof, step 4 would have revealed the problem, as it is false.

(b) Let $P(n)$ be the statement that every binary tree with n nodes (including leaves) has a height of $n - 1$.

Base case:
$P(1)$ is trivial.
Assume $P(n)$ from some n.
Let T be an arbitrary n-node binary tree. By the IH, the height of T is $n-1$. Add a leaf off the bottom of T to form T'. The new tree has $n+1$ nodes and a height of n, so we conclude $P(n+1)$.
QED.

The same problem as before, but more pronounced.