Math 2111 Exam 1 Solutions

Oct 5, 2005

1. (16 pts)
   (a) Define what it means for an operation $\circ$ to be associative.

   An operation $\circ$ on the set S is *associative* if $(x \circ y) \circ z = x \circ (y \circ z)$ for all $x, y, z \in S$.

   (b) Define what it means for an operation $\circ$ to have an identity.

   An operation $\circ$ on a set S, has an identity $x \in S$ if $x \circ s = s$ for all $s \in S$ and $s \circ x = s$ for all $s \in S$.

   (c) Give the definition of a vector space over a field.

   A vector space over a field F is a nonempty set V which has an operation $+$ called addition and a function $\cdot : F \times V \to V$ called scalar multiplication such that
   1. $+$ is associative.
   2. $+$ is commutative.
   3. $+$ has an identity $\vec{0} \in V$ called the zero vector.
   4. Every $v \in V$ has an inverse $-v \in V$ w.r.t. $+$.
   5. $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$ for all $\alpha \in F$, $u, v \in V$.
   6. $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$ for all $\alpha, \beta \in F$, $v \in V$.
   7. $\alpha \cdot (\beta \cdot v) = (\alpha\beta) \cdot v$ for all $\alpha, \beta \in F$, $v \in V$.
   8. $1 \cdot v = v$ for all $v \in V$.

2. (10 pts) Give an example of each of the following. Be sure to justify your example.
   (a) An operation which is commutative but not associative.

   Let $x \circ y = xy - 1$ on $\mathbb{Z}$. Since
   $$x \circ y = xy - 1 = yx - 1 = y \circ x$$
   for all $x, y \in \mathbb{Z}$, this operation is commutative. But
   $$(x \circ y) \circ z = (xy - 1) \circ z = (xy - 1)z - 1 = xyz - z - 1$$
   $$x \circ (y \circ z) = x \circ (yz - 1) = x(yz - 1) - 1 = xyz - x - 1$$
   which are usually not equal. E.g.
   $$(0 \circ 0) \circ 1 = 0 - 1 - 1 = -2$$
   $$0 \circ (0 \circ 1) = 0 - 0 - 1 = -1$$

   (b) An operation which has no identity.

   Let $\circ$ be the same as in part (a). Suppose $y \in \mathbb{Z}$ is an identity. Then
   $$x = x \circ y = xy - 1$$
   for all x. So $y = (x + 1)/x$. In particular, if $x = 1$, we get $y = 2$ and if $x = 2$ we get $y = 3/2$. But $2 \neq 3/2$, so this is a contradiction. Hence no such y can exist.

3. (8 pts) Let $x \in \mathbb{Z}_n$. Show that if x is a zero divisor then x cannot have an inverse with respect to multiplication.

Since x is a zero divisor there must exist $y \neq \overline{0}$ such that $xy = \overline{0}$. If x had an inverse $z \in \mathbb{Z}_n$, then

$$y = \overline{1}y = (zx)y = z(xy) = z\overline{0} = \overline{0}$$

which is a contradiction.

Note: If you start with $x, y \in \mathbb{Z}_n$, you don't have to put a bar above them because they already denote elements of $\mathbb{Z}_n$. E.g. if $x = \overline{1}$, then $\overline{x}$ would be $\overline{\overline{1}}$, which makes no sense. If you start with $x, y \in \mathbb{Z}$ and you want to do arithmetic with the sets x and y represent in $\mathbb{Z}_n$, then you do have to put a bar above them. E.g. if $x = 5$, that is not an element of $\mathbb{Z}_n$, but $\overline{5}$ is. Usually, you can choose whichever notation you prefer, just be consistent.

Typically, if you are only doing arithmetic in $\mathbb{Z}_n$, it is more convenient to treat indeterminates as elements in $\mathbb{Z}_n$. If so, you should not use bars. If your argument requires doing some arithmetic in $\mathbb{Z}$ as well–for example because you want to say something is divisible by n, which makes no sense to say in $\mathbb{Z}_n$–then you would let your indeterminates be elements of $\mathbb{Z}$ and you would put a bar on them when you are working in $\mathbb{Z}_n$ and no bar when you are working in $\mathbb{Z}$. (See the argument in section 2.2 of the lecture notes for an example of this.)

In this problem you were told $x \in \mathbb{Z}_n$, so you don't have a choice. You need to treat x as an element of $\mathbb{Z}_n$, which means whatever x is, it already has a bar in it.

4. (8 pts) Let V be the vector space of all functions $\mathbb{R} \to \mathbb{R}$ over the field $\mathbb{R}$ with usual addition of functions as vector addition and the usual multiplication of functions by scalars as scalar multiplication. Let $C^1(\mathbb{R})$ denote the subset of all differentiable functions in V. Prove or disprove: $C^1(\mathbb{R})$ is a subspace of V.

All we need to check is whether $C^1(\mathbb{R})$ is closed under addition and scalar multiplication (see Theorem 3.3 or your notes). So let $f(x), g(x)$ be differentiable functions. Then we learned in calculus that

$$\frac{d}{dx}(f + g) = \frac{df}{dx} + \frac{dg}{dx}.$$

Hence $(f + g)(x)$ is differentiable and so $f + g \in C^1(\mathbb{R})$ Let $\alpha \in \mathbb{R}$. We also learned in calculus that

$$\frac{d}{dx}(\alpha f) = \alpha \frac{df}{dx}.$$

Hence αf is also differentiable and so $\alpha f \in C^1(\mathbb{R})$. Therefore $C^1(\mathbb{R})$n is a subspace.

5. (8 pts) Let V be as in the previous problem. Let $S = \{p_1, p_2, p_3\}$, where

$$\begin{aligned} p_1(x) &= 2x^3 + 4x - 3 \\ p_2(x) &= x^3 - 3x + 1 \\ p_3(x) &= x^3 + 3x - 2. \end{aligned}$$

Is S a linearly independent set? If it is, prove that it is, if it is not, give a nontrivial linear combination of the elements in S equal to $\vec{0}$.

We need to solve

$$\begin{aligned} \alpha(2x^3 + 4x - 3) + \beta(x^3 - 3x + 1) + \gamma(x^3 + 3x - 2) &= 0 \\ (2\alpha + \beta + \gamma)x^3 + (4\alpha - 3\beta + 3\gamma)x + (-3\alpha + \beta + 2\gamma) &= 0 \end{aligned}$$

This gives the following set of linear equations:

$$2\alpha + \beta + \gamma = 0 \qquad (1)$$
$$4\alpha - 3\beta + 3\gamma = 0 \qquad (2)$$
$$-3\alpha + \beta + 2\gamma = 0 \qquad (3)$$

Using (2)-3(1) and (2)-2(1), we get

$$-2\alpha - 6\beta = 0 \implies \alpha = -3\beta \qquad \text{(2)-3(1)}$$
$$-5\beta + \gamma = 0 \implies \gamma = 5\beta \qquad \text{(2)-2(1)}$$

Substituting into (3)

$$-3(-3\beta) + \beta + 2(5\beta) = 0$$
$$0\beta = 0$$

This is true for any β, so we can choose $\beta = 1$. Then $\alpha = -3$ and $\gamma = 5$ and we have the following nontrivial linear combination:

$$-3(2x^3 + 4x - 3) + (x^3 - 3x + 1) + 5(x^3 + 3x - 2) = 0$$

6. **Extra credit problem.** Let $\circ$ be an operation on a set S with identity $e \in S$. For $x \in S$, an element $y \in S$ is called a *left inverse* of x if $y \circ x = e$.

   Now, let T be any nonempty set, and $M(T)$ the set of all functions $T \to T$. Let $\circ$ be composition of functions on $M(T)$.

   (a) (5 pts) Show that if $f \in M(T)$ has a left inverse $g \in M(T)$, then f is one-to-one.

   Let $f : T \to T$ have a left inverse $g : T \to T$ and let $x, y \in T$. If $f(x) = f(y)$, then $x = g(f(x)) = g(f(y)) = y$. Hence f is one-to-one.

   (b) (10 pts) Show that if $f \in M(T)$ is one-to-one then f has a left inverse $g \in M(T)$.

   Let $f : T \to T$ be a one-to-one function. Choose some element $t \in T$.
   Define the function $g : T \to T$ as follows. For $y \in T$, if there exists $x \in T$ such that $f(x) = y$, then set $g(y) = x$. Otherwise, set $g(y) = t$.
   We will now show that g is a left inverse of f. For $x \in T$, let $y = f(x)$. Since there exists an element $x \in T$ such that $f(x) = y$, in the definition of g we wouldn't have set $g(y) = t$. The problem is that we need to show that we would have set $g(y) = x$. By definition, $g(y)$ is such an element $z \in T$ that $f(z) = y$. We need to show $z = x$. This is true because f is one-to-one and $f(z) = f(x)$. So $g(f(x)) = x$. This can be done for any $x \in T$, hence $g \circ f$ is the identity function on T.

   Here is an example. Let $T = \mathbb{R}$ and $f(x) = e^x$. You know from calculus/precalculus that this is a one-to-one function. Let

   $$g(y) = \begin{cases} \ln(y) & \text{if } y > 0 \\ 0 & \text{if } y \leq 0 \end{cases}$$

   Since $e^x > 0$ for any $x \in \mathbb{R}$, $g \circ f(x) = g(f(x)) = \ln(e^x) = x$. So $g \circ f$ is the identity function on $\mathbb{R}$.
   Left inverses are not unique. The function below is also a left inverse of e^x.

   $$h(y) = \begin{cases} \ln(y) & \text{if } y > 0 \\ 1 & \text{if } y \leq 0 \end{cases}$$