Math 212, Assignment 5

Solutions

All questions are equally weighted. They will be marked for correctness and clarity of explanation.

1. Consider the set $\mathbb{R}^3$ with componentwise addition, and with multiplication defined by

$$(x, y, z) \cdot (x', y', z') = (0, yy', 0).$$

Is $\mathbb{R}^3$ a ring with these operations? If so, is it commutative? Does it have an identity? If it has an identity, determine which elements are units.

Solution: Addition is associative, we have

$$\begin{aligned}
((x_1,\ & y_1, z_1) + (x_2, y_2, z_2)) + (x_3, y_3, z_3) \\
&= (x_1 + x_2, y_1 + y_2, z_1 + z_2) + (x_3, y_3, z_3) \\
&= ((x_1 + x_2) + x_3, (y_1 + y_2) + y_3, (z_1 + z_2) + z_3) \\
&= (x_1 + (x_2 + x_3), y_1 + (y_2 + y_3), z_1 + (z_2 + z_3)) \quad \text{since addition is associative in } \mathbb{R} \\
&= (x_1, y_1, z_1) + (x_2 + x_3, y_2 + y_3, z_2 + z_3) \\
&= (x_1, y_1, z_1) + ((x_2, y_2, z_2) + (x_3, y_3, z_3)).
\end{aligned}$$

Similarly, addition is commutative:

$$(x, y, z) + (x', y', z') = (x + x', y' + y', z + z') = (x' + x, y' + y, z' + z) = (x', y', z') + (x, y, z).$$

The identity for addition is $(0, 0, 0)$, and the additive inverse of (x, y, z) is $(-x, -y, -z)$.

Therefore $\mathbb{R}^3$ is an abelian group with componentwise addition.

Next, we check that multiplication is associative:

$$\begin{aligned}
((x_1, y_1, z_1) \cdot (x_2, y_2, z_2)) \cdot (x_3, y_3, z_3) &= (0, y_1 y_2, 0) \cdot (x_3, y_3, z_3) \\
&= (0, (y_1 y_2) y_3, 0) \\
&= (0, y_1 (y_2 y_3), 0) \\
&= (x_1, y_1, z_1) \cdot (0, y_2 y_3, 0) \\
&= (x_1, y_1, z_1) \cdot ((x_2, y_2, z_2) \cdot (x_3, y_3, z_3)).
\end{aligned}$$

We now show that multiplication is also commutative (this will help later when we prove that the distributive law holds).

$$(x, y, z) \cdot (x', y', z') = (0, yy', 0) = (0, y'y, 0) = (x', y', z') \cdot (x, y, z)$$

Now we show that the distributive law holds:

$$
\begin{aligned}
(x_1, \quad & y_1, z_1) \cdot [(x_2, y_2, z_2) + (x_3, y_3, z_3)] \\
&= (x_1, y_1, z_1) \cdot (x_2 + x_3, y_2 + y_3, z_2 + z_3) \\
&= (0, y_1(y_2 + y_3), 0) \\
&= (0, y_1y_2 + y_1y_3, 0) \\
&= (0, y_1y_2, 0) + (0, y_1y_3, 0) \\
&= (x_1, y_1, z_1) \cdot (x_2, y_2, z_2) + (x_1, y_1, z_1) \cdot (x_3, y_3, z_3),
\end{aligned}
$$

and since both operations are commutative, it follows from the above that

$$[(x_2, y_2, z_2) + (x_3, y_3, z_3)] \cdot (x_1, y_1, z_1) = (x_2, y_2, z_2) \cdot (x_1, y_1, z_1) + (x_3, y_3, z_3) \cdot (x_1, y_1, z_1).$$

We have now shown that $\mathbb{R}^3$, with the given operations, is a commutative ring.

There is no identity, since, for example, there is no $(x, y, z) \in \mathbb{R}^3$ such that

$$(0, y, 0) = (1, 1, 1) \cdot (x, y, z) = (1, 1, 1).$$

Since there is no identity, inverses for $\cdot$ are not defined.

2. Prove that the set
$$S = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{R} \right\}$$
is a subring of $M_2(\mathbb{R})$ with its usual addition and multiplication. Is S a commutative ring? Does it have an identity? If so, find the identity and determine which elements are units of S.

Solution: First of all, the zero matrix is in S (with $a = b = c = 0$) and so S is not empty. Let
$$A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}, B = \begin{bmatrix} d & e \\ 0 & f \end{bmatrix}$$
be two elements of S. We must check that $A - B$ and AB are both in S:
$$A - B = \begin{bmatrix} a - d & b - e \\ 0 & c - f \end{bmatrix}$$
is obviously in S and
$$AB = \begin{bmatrix} ad & ae + cf \\ 0 & df \end{bmatrix}$$
which is also obviously in S.

To see that S is not commutative, note that $\begin{bmatrix} 1 & 2 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ 0 & 1 \end{bmatrix}$ while $\begin{bmatrix} 2 & 1 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 0 & 3 \end{bmatrix}$.

Of course the usual identity matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is in S.

To determine which elements are units, note that $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ has an inverse if and only if $ac \neq 0$.

Therefore the units of S are the elements $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ such that a and c are both non-zero.

3. For each of the following, decide if the set S is a subring of the real numbers, with its usual operations of addition and multiplication. If it is, give a proof, and if not, explain why.

   (a) $S = \{\frac{n}{4} : n \in \mathbb{Z}\}$

   Solution:
   This set S is not a subring of $\mathbb{R}$, since S is not closed under multiplication. For example, $\frac{1}{4} \in S$, but $\left(\frac{1}{4}\right)^2 = \frac{1}{16} \notin S$, since there is no integer n such that $\frac{1}{16} = \frac{n}{4}$.

   (b) $S = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Z}\}$.

   Solution:
   Note that we can write the elements of S as $a + b(2^{1/3}) + c(2^{2/3})$, for $a, b, c \in \mathbb{Z}$. Of course S is a subset of $\mathbb{R}$. To see that it is a subring of R, note first that $0 \in S$, so S is non-empty. Next we take two arbitrary elements of S, say $a + b(2^{1/3}) + c(2^{2/3})$ and $e + e(2^{1/3}) + f(2^{2/3})$. Then

   $$[a + b(2^{1/3}) + c(2^{2/3})] - [d + e(2^{1/3}) + f(2^{2/3})] = (a - d) + (b - e)(2^{1/3}) + (c - f)(2^{2/3}),$$

   which is in S because $a, b, c, d, e, f \in \mathbb{Z}$ and $\mathbb{Z}$ is closed under subtraction. Finally,

   $$[a+b(2^{1/3})+c(2^{2/3})][d+e(2^{1/3})+f(2^{2/3})] = (ad+ebf+2ce)+(ae+bd+2cf)2^{1/3}+(af+be+cd)2^{2/3},$$

   which is in S because $\mathbb{R}$ is closed under addition and multiplication.

4. TRUE or FALSE. (If true, give a proof and if false, give an explicit counterexample.)

If R is a field and S is a subring of R, then S is also a field.

Solution:

False. $\mathbb{Q}$ is a field and $\mathbb{Z}$ is a subring, but not a subfield.

More generally, if R is any integral domain which is not a field, it is a subring of its field of quotients.

5. Let R be a commutative ring with identity $1 \neq 0$, and suppose the cancellation rule holds in R. That is, for all $a, b, c \in R$, with $a \neq 0$, if $ab = ac$ then $b = c$. Prove that if R is finite, then R is a field.

Solution:

First we show that R has no zero divisors. Suppose $ab = 0$, where $a \neq 0$. Then $ab = a0$, so, by the cancellation law, $b = 0$.

Now, let a be any non-zero element of R. Consider the set $\{ax : x \neq 0\} \subseteq R$. Since R has no zero divisors, none of these elements is 0. Furthermore, by the cancellation law, they are all distinct, since

$$ax_1 = ax_2 \Rightarrow x_1 = x_2.$$

It follows that each element of $R - \{0\}$ appears exactly once among the elements $\{ax : x \neq 0\}$. In particular, the element 1 appears. That is, there is some $x \in R - \{0\}$ such that $ax = 1$. Therefore a has is a unit.

Since this holds for any nonzero a, it follows that R is a field.

6. Prove that $F = \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$, with ordinary addition and multiplication, is a field.

Solution: First, we show that F is a subring of $\mathbb{R}$. Using $a = b = 0$, it is clear that F contains 0 and is non-empty.

Now, we let $x = a + b\sqrt{5}, y = c + d\sqrt{5}$ be two elements of F $(a, b, c, d \in \mathbb{Q})$ and show that both $x - y$ and xy are in F.

$$x - y = (a - c) + (b - d)\sqrt{5}.$$

As a, b, c, d are all rational numbers, so are $a - c$ and $b - d$, so $x - y$ is in F.

$$\begin{aligned} xy &= (a + b\sqrt{5})(c + d\sqrt{5}) \\ &= ac + ad\sqrt{5} + bc\sqrt{5} + bd\sqrt{5}^2 \\ &= (ac + 5bd) + (bc + ad)\sqrt{5}. \end{aligned}$$

As a, b, c, d are all rational numbers, so are $ac + 5bd$ and $ad + bc$.

The last step is to check that every element of F, $a + b\sqrt{5} \neq 0$, has an inverse which lies in F. It certainly has one in $\mathbb{R}$, but we must check it is in F. Notice that $a + b\sqrt{5} \neq 0$ means that a, b are not both 0.

$$\begin{aligned}
\frac{1}{a+b\sqrt{5}} &= \frac{1}{a+b\sqrt{5}}\frac{a-b\sqrt{5}}{a-b\sqrt{5}} \\
&= \frac{a-b\sqrt{5}}{a^2-(b\sqrt{5})^2} \\
&= \frac{a-b\sqrt{5}}{a^2-5b^2} \\
&= \frac{a}{a^2-5b^2} + \frac{-b}{a^2-5b^2}\sqrt{5}
\end{aligned}$$

As a, b are rational numbers, $a^2 - 5b^2 \neq 0$ and $\frac{a}{a^2-5b^2}$ and $\frac{-b}{a^2-5b^2}$ are both rational numbers. So the inverse of $a + b\sqrt{5}$ lies in F.

7. Let $R = \{i + j\sqrt{5} : i, j \in \mathbb{Z}\}$, and let Q be the field of quotients of R.

   (a) Prove that if $[a, b]$ is in Q, then there exists c in R and $k \in \mathbb{Z}$, $k \neq 0$, such that $[a, b] = [c, k]$.

   Solution:
   Let $a = i + j\sqrt{5}, b = m + n\sqrt{5}$, i, j, m, n in $\mathbb{Z}$, be the two elements of R. We assume that $b \neq 0$, which means m and n are not both 0. From this, we know that

   $$m^2 - 5n^2 = (m + \sqrt{5}n)(m - \sqrt{5}n)$$

   is nonzero.
   Let
   $$c = (i + j\sqrt{5})(m - n\sqrt{5}) = (im - 5jn) + (jm - in)\sqrt{5}$$
   which is obviously in R and let $k = m^2 - 5n^2$, which is obviously in $\mathbb{Z}$.
   We claim that $[a, b] = [c, k]$. To verify this, we cross-multiply:

   $$\begin{aligned}
   bc &= (m + n\sqrt{5})(m - n\sqrt{5})(i + j\sqrt{5}) \\
   &= (m^2 - 5n^2)(i + j\sqrt{5}) \\
   &= ka.
   \end{aligned}$$

   This completes the proof.

(b) Define an isomorphism from the field F of problem 6 to Q. You do not need to prove it is an isomorphism, but use part (a) to prove it is surjective.

Solution:
Define $f : F \to Q$ as follows. Suppose that r, s are rational numbers. Say $r = \frac{i}{j}, s = \frac{k}{l}$, where i, j, k, l are integers and $j \neq 0, l \neq 0$. This means we can write

$$r + s\sqrt{5} = \frac{i}{j} + \frac{k}{l}\sqrt{5} = \frac{il + jk\sqrt{5}}{jl}.$$

This tells us how to define f: set

$$f(r + s\sqrt{5}) = [il + jk\sqrt{5}, jl].$$

This is well-defined because the fact that i, j, k, l are all integers means that both $il + jk\sqrt{5}$ and jl are in R and $jl \neq 0$.
To see that f is surjective, let $[a, b]$ be any element of Q, meaning a, b are in R and $b \neq 0$. We know that $[a, b] = [c, k]$ where c is in R and $k \neq 0$ is an integer. Write $c = i + j\sqrt{5}$, where i, j are integers. Clearly $x = \frac{i}{k} + \frac{j}{k}\sqrt{5}$ is in F and we claim that $f(x) = [c, k]$. To see this, we note that, by definition

$$f(x) = [ik + jk\sqrt{5}, k^2].$$

To verify that $f(x) = [c, k]$, we cross-multiply:

$$(ik + jk\sqrt{5})k = ik^2 + jk^2\sqrt{5} = (i + j\sqrt{5})k^2 = ck^2.$$

This completes the proof.

8. For each of the following subsets of the rational numbers, determine if the set has (i) a maximum, (ii) an upper bound, (iii) a least upper bound. (This means within the set of *rational* numbers.) In parts (i) and (iii) if the answer is yes, name one. In part (ii) if the answer is yes, name three.

(a) $\{\frac{1}{2n} : n = 1, 2, 3, \ldots\}$.

Solution: Maximum $\frac{1}{2}$. Upper bound $\frac{1}{2}, 1, 2$. Least upper bound $\frac{1}{2}$.

(b) $\{\frac{a}{b} \mid a, b \in \mathbb{Z}, 0 < a < b\}$.

Solution:

If $\frac{a}{b}$ is in the set, so $a < b$, then $a+1 < b+1$ and $\frac{a+1}{b+1}$ is also in the set and

$$\frac{a}{b} < \frac{a+1}{b+1}$$

because $a(b+1) = ab + a < ab + b = b(a+1)$. This means that the set has no maximum.
Since $a < b$, $\frac{a}{b} < 1$, so 1 is an upper bound. So are 2 and 3.
The least upper bound is 1.

(c) $\{\frac{n^3+5n}{n^2} : n = 1, 2, 3, \dots\}$.

Solution:
Note that $\frac{n^3+5n}{n^2} > \frac{n^3}{n^2} = n$. Since there is no number greater than every positive integer, the set has no upper bound and no maximum.

(d) $\{\frac{a}{b} : a, b \in \mathbb{Z}^+, a^2 + 3ab - b^2 < 0\}$. (You may assume there is no rational number r with $r^2 = 13$.)

Solution:
Observe that $a^2 - 3ab - b^2 < 0$ if and only if $\left(\frac{a}{b}\right)^2 - 3\frac{a}{b} - 1 < 0$. In other words, our set is all positive rational numbers x such that $x^2 - 3x - 1 < 0$. This polynomial is a quadratic. Its graph is an upward parabola with roots at $\frac{-3\pm\sqrt{9+4}}{2} = \frac{-3\pm\sqrt{13}}{2}$. Our set is all rational numbers x with

$$0 < x < \frac{-3+\sqrt{13}}{2}.$$

This set has no maximum: given any x in the set, there is a rational number y with $x < y < \frac{-3+\sqrt{13}}{2}$.
The set does have an upper bound. As $\sqrt{13} < 4$, $\frac{1}{2}$ is an upper bound as are 1 and 2.
The set has no least upper bound because if z is any rational number which is an upper bound, it must be greater than $\frac{-3+\sqrt{13}}{2}$ and we can find another rational number w with $\frac{-3+\sqrt{13}}{2} < w < z$.