Math 402 Homework 3

Alexandre Lipson

January 29, 2025

Problem 1. Which of the following are subrings of $M(\mathbb{R})$ and which have identity?

a) $\begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix}$, $r \in \mathbb{Q}$.

This is a subset of $M(\mathbb{R})$ and contains the zero matrix.
This set is closed under addition as $\mathbb{Q}$ is closed under addition.
Similarly, this set has an additive inverse given that $-r \in \mathbb{Q}$ as well.
This set is closed under multiplication because multiplication maps only to the zero matrix.
This set does not have an identity because all multiplication maps to zero, so there cannot be an element 1 such that $\forall a$, $1 \cdot a = a$ because we already have $1 \cdot a = 0$. Since this the ring axioms hold for this set, then this set forms a subring of $M(\mathbb{R})$.

b) $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $a, b, c \in \mathbb{Z}$.

The addition properties of closure, an inverse, and a zero, are satisfied as in $\mathbb{Z}$.
Furthermore, we see that the multiplication of two elements from this set produce only a zero in the bottom left entry of the product matrix, and a linear combination of other elements of $\mathbb{Z}$ elsewhere. Thus the set is closed under multiplication because $\mathbb{Z}$ is closed under linear combinations and the bottom left entry remains zero.
This set contains an identity element which is the 2×2 matrix identity I. Since the ring axioms and identity hold for this set, then it forms a subring with identity.

c) $\begin{pmatrix} a & b \\ c & 0 \end{pmatrix}$, $a, b, c \in \mathbb{R}$.

This set is not closed under multiplication. Consider the bottom right entry of a product matrix, it can be nonzero and therefore an element not belonging to this set.
So, this set does not form a subring.

d) $\begin{pmatrix} a & 0 \\ a & 0 \end{pmatrix}$, $a \in \mathbb{R}$.

This set is closed under addition and has both a zero and an additive inverse given as in $\mathbb{R}$.
Consider multiplication for $a, b \in \mathbb{R}$,

$$\begin{pmatrix} a & 0 \\ a & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ ab & 0 \end{pmatrix}.$$

We see that multiplication is closed as it is for scalars in $\mathbb{R}$, and also that we have the identity

element $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$. Since this set conforms to the axioms of a ring and also has identity, then it is a subring with identity.

e) $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, $a \in \mathbb{R}$.

We see that this set is just a scalar matrix of the form aI where I is the 2×2 identity matrix. So, this set is closed under addition and multiplication and there exists both additive and multiplicative inverses and identities given that the same holds for scalars $a \in \mathbb{R}$.
Thus, this set forms a subfield of $M(\mathbb{R})$, and therefore a subring with identity as well.

f) $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, $a \in \mathbb{R}$.

This set is closed under addition, has a zero, and has an additive inverse, given as in $\mathbb{R}$.
This set is closed under multiplication as the only entry in a product matrix will be the top left and $\mathbb{R}$ is closed under multiplication.
The identity element is given by $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.
Since this set conforms to the ring axioms and has an identity, then it is a subring with identity.

Problem 2. Let S be the set of all rationals that can be written with an odd denominator.
Prove that S is a subring of $\mathbb{Q}$ and that S is not a field.

Proof of subring. First, we see that S is a subset of Q because all rationals that can be written with an odd denominator are also themselves rationals in the first place.

S has a zero element because 0 can be expressed as $0 = \frac{0}{1}$.

S has an additive inverse because, $\forall x \in S$, $-x$ will have the same odd denominator where $x + (-x) = 0$.

Since we can add two rational numbers by cross-multiplying their denominators, such a sum will have the product of odd numbers as a denominator. Since the product of two odd numbers is odd, then the sum of two elements in S can be written with an odd denominator. So, S is closed under addition.

Similarly, the product of two elements in S, where denominators are multiplied together, will also have an odd denominator. So, S is closed under multiplication.

Since S is closed under addition and multiplication, has an additive inverse, and has a zero element, then the ring axioms hold for S, so S is a subring of $\mathbb{Q}$ □

Proof of not a field. We will show that some elements in S do not have multiplicative inverses.

Consider $\frac{2}{1} \in S$. Note that $\left(\frac{1}{2}\right)^{-1} = \frac{1}{2} \notin S$ because the denominator 2 is not odd.

So, $\exists a \in S \ : \ a^{-1} \notin S \implies S$ is not a field. □

Problem 3. $kI = \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix}$, $k \in \mathbb{R}$ is a scalar matrix.

a) Prove that the set of scalar matrices is a subring of $M(\mathbb{R})$.

b) Show that $\forall A \in M(\mathbb{R})$, $KA = AK$ where K is a scalar matrix.

c) Show that, for $K \in M(\mathbb{R})$, $\forall A \in M(\mathbb{R})$, $KA = AK \implies K$ is a scalar matrix.

Proof of a. First, we see that $\forall k \in \mathbb{R}$, $kI \subset M(\mathbb{R})$.

Next, scalar matrices are closed under addition, have a zero element, and have an additive inverse as in $\mathbb{R}$.

Since we can write scalar matrices as kI where I is the identity matrix, then products are of the form $(aI)(bI) = (ab)(II) = (ab)I$. So, scalar matrices are closed under multiplication.

Therefore, the set of scalar matrices forms of subring of $M(\mathbb{R})$. □

Proof of b. Let $K = kI$ where $k \in \mathbb{R}$ and I is the 2×2 identity matrix.

Then,

$$KA = (kI)A = k(IA) = kA = k(AI) = A(kI) = AK.$$

□

Proof of c. Let $K = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. First, let $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

Then,

$$\begin{aligned} KA &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} \\ AK &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \\ KA = AK &\implies \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \\ &\implies b = 0 \wedge c = 0. \end{aligned}$$

Now, let $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

$$\begin{aligned} KA &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix} \\ AK &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \\ KA = AK &\implies \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix} = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \\ &\implies a = d. \end{aligned}$$

Therefore, $K = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI$, which is a scalar matrix. □

Problem 4. Prove Theorem 3.1.
Let R, S be rings.

i) Define addition and multiplication on the Cartesian product $R \times S$ by

$$(r, s) + (r', s') = (r + r', s + s')$$
$$(r, s) \cdot (r', s') = (r \cdot r', s \cdot s').$$

Then $R \times S$ is a ring.

ii) R, S commutative $\implies$ $R \times S$ commutative.

iii) R, S with identity $\implies$ $R \times S$ with identity.

Proof of i. The closure and inverse of addition are retained from the properties of addition in the rings R and S.

We add only elements from R to other such elements and the same with S. Explicitly, we could also write

$$(r, s) \bigoplus_{R \times S} (r', s') = (r \bigoplus_R r', s \bigoplus_S s').$$

The zero element of $R \times S$ is given by $(0_R, 0_S)$ where

$$(r, s) + (0_R, 0_S) = (r + 0_R, s + 0_S) = (r, s).$$

Similarly, the closure under multiplication is retained as well. □

Proof of ii. R, S commutative implies that $rr' = r'r$ and $ss' = s's$. Then,

$$(r, s)(r', s') = (rr', ss') = (r'r, s's) = (r', s')(r, s).$$

□

Proof of iii. R, S with identity gives that there are both 1_R and 1_S. Then, $1_{R \times S} = (1_R, 1_S)$. We see that, for left multiplication,

$$(r, s)(1_R, 1_S) = (r \cdot 1_R, s \cdot 1_S) = (r, s).$$

The same holds for right multiplication given that $1 \cdot a = a = a \cdot 1$.

□

Problem 5. Let $\mathbb{Q}(\sqrt{2}) = \{r + s\sqrt{2} \mid r, s \in \mathbb{Q}\}$. Show that $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{R}$.

This is special case of Problem 6 where $d = 2 > 0$.

Problem 6. Let $d \in \mathbb{Z}$ be not a perfect square. Show $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{C}$.

Proof. Since d is not a perfect square, then $\sqrt{d}$ cannot be simplified.

Note that $d < 0 \implies \sqrt{d} = i\sqrt{(-d)} \in \mathbb{C}$, so $\mathbb{Q}(\sqrt{d})$ would contain complex elements. If $d \geq 0$, then we still have $\mathbb{Q}(\sqrt{d}) \subset \mathbb{R} \subset \mathbb{C}$. Thus, $\mathbb{Q}(\sqrt{d}) \subset \mathbb{C}$.

$\mathbb{Q}(\sqrt{d})$ is closed under addition as in $\mathbb{Q}$,

$$(a + b\sqrt{d}) + (a' + b'\sqrt{d}) = (a + a') + (b + b')\sqrt{d}.$$

For closure under multiplication, consider

$$\begin{aligned}(a + b\sqrt{d})(a' + b'\sqrt{d}) &= aa' + ab'\sqrt{d} + ba'\sqrt{d} + bb'(\sqrt{d})^2 \\ &= (aa' + bb'd) + (ab' + ba')\sqrt{d}.\end{aligned}$$

Since the product of $d \in \mathbb{Z}$ with elements is $\mathbb{Q}$ belongs to $\mathbb{Q}$ and $\mathbb{Q}$ is closed under addition and multiplication, then $\mathbb{Q}(\sqrt{d})$ is closed under multiplication.

Next, we have the zero element $0 + 0\sqrt{d} = 0$.

We have the additive inverse of any $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ as $(-a) + (-b)\sqrt{d})$, where

$$(a + b\sqrt{d}) + ((-a) + (-b)\sqrt{d}) = (a + (-a)) + (b + (-b))\sqrt{d} = 0 + 0\sqrt{d} = 0.$$

We also have the multiplicative identity element $1 + 0\sqrt{d}$, where $\forall a, b \in \mathbb{Q}$

$$(1 + 0\sqrt{d})(a + b\sqrt{d}) = a + b\sqrt{d}.$$

For the multiplicative inverse, we have that $(a + b\sqrt{d})(a' + b'\sqrt{d}) = (aa' + bb'd) + (ab' + ba')\sqrt{d}$ from above.

So, $(aa' + bb'd) + (ab' + ba')\sqrt{d} = 1 + 0\sqrt{d} \implies ab + ba' = 0 \wedge aa' + bb'd = 1$.

Set $b' = \frac{-ba'}{a}$ so that we have,

$$\begin{aligned}aa' + b\left(\frac{-ba'}{a}\right)d &= 1 \\ a'\left(a - \frac{b^2d}{a}\right) &= 1 \\ a'(a^2 - b^2d) &= a \\ a' &= \frac{a}{a^2 - b^2d} \\ b' &= -\frac{b}{a}\left(\frac{a}{a^2 - b^2d}\right) \\ &= -\frac{b}{a^2 - b^2d}.\end{aligned}$$

So, $(a + b\sqrt{d})^{-1} = \frac{1}{a^2 - b^2d}(a - b\sqrt{d})$. Note that this is very similar to the inverse in $\mathbb{C}$!

Since $\frac{1}{a^2 - b^2d}(a - b\sqrt{d}) \in \mathbb{Q}(\sqrt{d})$, then every element in $\mathbb{Q}(\sqrt{d})$ has an inverse.

Since $\mathbb{Q}(\sqrt{d}) \subset \mathbb{C}$ satisfies the ring axioms (with the ordinary add. & mul. ops. as in $\mathbb{C}$) and has both a multiplicative inverse and identity, then it is a subring and subfield of $\mathbb{C}$. $\square$

Problem 7. In $M(\mathbb{C})$, let $\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $\mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

Let the set $\mathbb{H}$ of real quaternions be

$$a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} = \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}, \quad a, b, c, d \in \mathbb{R}.$$

a) Prove

i) $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}$

ii) $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$

iii) $\mathbf{jk} = -\mathbf{kj} = \mathbf{i}$

iv) $\mathbf{ki} = -\mathbf{ik} = \mathbf{j}$

b) Show $\mathbb{H}$ is non-commutative and has an identity.

c) Show that $\mathbb{H}$ is a division ring.

d) Show that $x^2 = -\mathbf{1}$ has infinitely many solutions in $\mathbb{H}$.

Proof of a. (i) Since $\mathbf{i}$ is a diagonal matrix, its square is the matrix with diagonal entries squared. So, $\mathbf{i}^2 = \begin{pmatrix} (i)^2 & 0 \\ 0 & (i)^2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\mathbf{1}$.

For $\mathbf{j}^2$ and $\mathbf{k}^2$, antidiagonal 2×2 matrices square to a diagonal matrix with the entries as products of each original entry. So, $\mathbf{j}^2 = \begin{pmatrix} 1\cdot(-1) & 0 \\ 0 & (-1)\cdot 1 \end{pmatrix} = -\mathbf{1}$ and $\mathbf{k}^2 = \begin{pmatrix} i\cdot i & 0 \\ 0 & i\cdot i \end{pmatrix} = -\mathbf{1}$.

(ii) $\mathbf{ij} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \mathbf{k} = -\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = -\mathbf{ji}$

(iii) $\mathbf{jk} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \mathbf{i} = -\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -\mathbf{kj}$

(iv) $\mathbf{ki} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \mathbf{j} = -\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = -\mathbf{ik}$

□

Proof of b. Since matrix multiplication is non-commutative, then multiplication in $\mathbb{H}$, where $x \in \mathbb{H}$ is written in 2×2 matrix form, is also non-commutative.

Since we can express the 2×2 identity matrix I as $1\mathbf{1} + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$, then $1_{\mathbb{H}} = I$. □

Proof on c. Let $M = a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$. Let $|M| = a^2 + b^2 + c^2 + d^2$. Let $N = \frac{1}{|M|}(a\mathbf{1} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k})$.

We will show that N is the inverse of M, i.e., $MN = 1$. Note that the product of any basis with the basis $\mathbf{1}$ remains the same.

$$\begin{aligned}
MN &= (a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})\frac{1}{|M|}(a\mathbf{1} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) \\
&= \frac{1}{|M|}(a^2\mathbf{1} - ab\mathbf{i} - ac\mathbf{j} - ad\mathbf{k} \\
&+ ab\mathbf{i} - b^2\mathbf{i}^2 - bc\mathbf{ij} - bd\mathbf{ik} \\
&+ ac\mathbf{j} - bc\mathbf{ji} - c^2\mathbf{j}^2 - cd\mathbf{jk} \\
&+ ad\mathbf{k} - bd\mathbf{ki} - cd\mathbf{kj} - d^2\mathbf{k}^2) \\
&= \frac{1}{|M|}(a^2\mathbf{1} - b^2(-\mathbf{1}) - c^2(-\mathbf{1}) - d^2(-\mathbf{1}) \\
&= \frac{a^2 + b^2 + c^2 + d^2}{a^2 + b^2 + c^2 + d^2} = 1.
\end{aligned}$$

□

Proof of d. Consider $x = 0\mathbf{1} + b\mathbf{i} + c\mathbf{j} - d\mathbf{k}$ where $b^2 + c^2 + d^2 = 1$.

Then,

$$\begin{aligned}
x^2 &= (b\mathbf{i} + c\mathbf{j} - d\mathbf{k})(b\mathbf{i} + c\mathbf{j} - d\mathbf{k}) \\
&= b^2\mathbf{i}^2 + bc\mathbf{ij} - bd\mathbf{ik} \\
&+ bc\mathbf{ji} + c^2\mathbf{j}^2 - cd\mathbf{jk} \\
&- bd\mathbf{ki} - cd\mathbf{kj} + d^2\mathbf{k}^2 \\
&= b^2(-\mathbf{1}) + c^2(-\mathbf{1}) + d^2(-\mathbf{1}) \\
&= (b^2 + c^2 + d^2)(-\mathbf{1}).
\end{aligned}$$

But, with the vector length condition $b^2 + c^2 + d^2 = 1$, the above becomes just $-\mathbf{1}$.

So, any x satisfying the unit distance with zero $\mathbf{1}$ part will hold for $x^2 = -\mathbf{1}$.

Thus, $x^2 = -\mathbf{1}$ has infinitely many solutions because $b^2 + c^2 + d^2 = 1$ has infinitely many solutions. □

Problem 8. Find inverses for the following elements in the ring of quaternions.

i) $\mathbf{i}$. Using Problem 7c, for $x = (\mathbf{a}1 + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) \in \mathbb{H}$, we have that

$$x^{-1} = \frac{a\mathbf{1} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}}{a^2 + b^2 + c^2 + d^2}.$$

So, $(\mathbf{i})^{-1} = -\mathbf{i}$.

ii) $\mathbf{j}$. As before, $-\mathbf{j}$.

iii) $\mathbf{k}$. Again, $-\mathbf{k}$.

iv) $\mathbf{1} + \mathbf{i}$. Taking note of the vector magnitude, we have $\frac{1}{2}(\mathbf{1} - \mathbf{i})$.

v) $\mathbf{j}+\mathbf{k}$. As above, $-\frac{1}{2}(\mathbf{j}+\mathbf{k})$.

vi) $\mathbf{1}+\mathbf{i}+\mathbf{j}+\mathbf{k}$. With a magnitude of 4, we have $\frac{1}{4}(\mathbf{1}-\mathbf{i}-\mathbf{j}-\mathbf{k})$.

Problem 9. Let R be a ring. Prove $\forall a \in R$, $a \cdot 0 = 0$.

Proof. Since R is a ring, then it has an additive identity 0. By the additive identity, $0 = 0 + 0$.

By the axiom of distributivity,

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

But, we can take $a \cdot 0$ from both sides,

$$0 = a \cdot 0.$$

□

Problem 10. Prove or disprove: The set of units in a ring R with identity is a subring of R.

This statement does not hold.

For an example, consider the ring $\mathbb{Z}$ with units $\{1, -1\}$. This set is not closed under addition, $1+(-1) = 0 \notin \{1, -1\}$.

Proposition 1. The set of units in a ring R with identity cannot form a subring of R.

Proof. Recall the definition of a unit in R with identity, $a \in R$ is a unit if it has an inverse in R.

The units of R will never include 0 because 0 is not an inverse. So, this new subset of units will not be able to satisfy the additive identity axiom.

Since the subset of units of R does not contain zero, then it cannot satisfy the ring addition axioms and therefore is not a ring.

So, the subset of units of R is not a subring of R either. □