Math 227
Suggested solutions to Homework Set 1

Problem 1. (a) We have:

(i) $[-1,1]$ has properties P2 and P3: indeed, if we have real numbers x_1, x_2, x_3 satisfying $x_i \in [-1,1] \Leftrightarrow 0 \leqslant |x_i| \leqslant 1$ for $i = 1,2,3$, then $0 \leqslant |x_1 x_2| = |x_1| \cdot |x_2| \leqslant 1 \Leftrightarrow x_1 x_2 \in [-1,1]$ and $0 \leqslant |-x_3| \leqslant 1 \Leftrightarrow -x_3 \in [-1,1]$.
On the other hand, $1 + \frac{1}{2} = \frac{3}{2} \notin [-1,1]$, and similarly $\left(\frac{1}{2}\right)^{-1} = 2 \notin [-1,1]$, so $[-1,1]$ does not have properties P1 and P4.

(ii) $\{-1,0,1\}$ has properties P2, P3 and P4, but does not have property P1 since, for instance, $1+1 = 2 \notin \{-1,0,1\}$.

(iii) $\mathbb{R} \setminus \mathbb{Q}$ has properties P3 and P4 since, for any real number r, we have $r \in \mathbb{Q} \Leftrightarrow -r \in \mathbb{Q}$, and if moreover $r \neq 0$, then $r \in \mathbb{Q} \Leftrightarrow r^{-1} \in \mathbb{Q}$. However, $\mathbb{R} \setminus \mathbb{Q}$ does not have properties P1 and P2 since, for instance $\sqrt{2} + (-\sqrt{2}) = 0 \in \mathbb{Q}$ and $\sqrt{2} \cdot \sqrt{2} = 2 \in \mathbb{Q}$.

(iv) $\{0\}$ has all 4 properties (regarding property P4, it has this one because it has no non-zero elements, so the implication "if an element is non-zero, then its multiplicative inverse is also in the set" is vacuously satisfied).

(v) $\mathbb{N}_0$ has properties P1 and P2. It does not have properties P3 and P4 since, for instance, -2 and $\frac{1}{2}$ are not in $\mathbb{N}_0$.

(vi) $\mathbb{Z}$ has properties P1, P2 and P3. It does not have property P4 since, for instance, $\frac{1}{2}$ is not in $\mathbb{Z}$.

(vii) $\mathbb{R} \setminus \{0\}$ has properties P2, P3 and P4: indeed, if we multiply two non-zero real numbers, the result is a non-zero number again, while if $r \in \mathbb{R} \setminus \{0\}$ then $-r \neq 0$ too, and similarly r^{-1} exists and is non-zero.
On the other hand, for any $r \in \mathbb{R} \setminus \{0\}$, $-r \in \mathbb{R} \setminus \{0\}$ too, as we just observed, but $r + (-r) = 0 \notin \mathbb{R} \setminus \{0\}$, which shows that $\mathbb{R} \setminus \{0\}$ does not have property P1.

(viii) $S_8 = \left\{ r \in \mathbb{R} : \exists\ q_1, q_2 \in \mathbb{Q} \text{ such that } r = q_1 + q_2\sqrt{5} \right\}$ has all 4 properties.

Indeed, if $r_1, r_2 \in S_8$, then we can write

$$r_1 = q_1 + q_2\sqrt{5} \quad \text{and} \quad r_2 = q_3 + q_4\sqrt{5}$$

for some $q_1, q_2, q_3, q_4 \in \mathbb{Q}$. But then

$$r_1 + r_2 = (q_1 + q_2\sqrt{5}) + (q_3 + q_4\sqrt{5}) = (q_1 + q_3) + (q_2 + q_4)\sqrt{5} \in S_8$$

since $q_1 + q_3,\ q_2 + q_4 \in \mathbb{Q}$, which shows that S_8 is closed under addition. Similarly,

$$r_1 \cdot r_2 = (q_1 + q_2\sqrt{5}) \cdot (q_3 + q_4\sqrt{5}) = (q_1q_3 + 5q_2q_4) + (q_1q_4 + q_2q_3)\sqrt{5} \in S_8$$

since $q_1q_3 + 5q_2q_4,\ q_1q_4 + q_2q_3$, which shows that S_8 is closed under multiplication.

Also, $-r_1 = (-q_1) + (-q_2)\sqrt{5} \in S_8$, given that $-q_1,\ -q_2 \in \mathbb{Q}$, which shows that S_8 is closed under taking additive inverses.

Finally, if we assume that $r_1 \neq 0$, then we have that either q_1 or q_2 is non-zero (or both). But then we have that $q_1^2 - 5q_2^2 \neq 0$, which follows in all three cases, and in particular in the case that both q_1 and q_2 are non-zero, it follows because $\sqrt{5}$ is not a rational number. Using this, we can write

$$r_1^{-1} = \frac{1}{q_1 + q_2\sqrt{5}} = \frac{q_1 - q_2\sqrt{5}}{q_1^2 - 5q_2^2} = \frac{q_1}{q_1^2 - 5q_2^2} + \frac{-q_2}{q_1^2 - 5q_2^2}\sqrt{5} \in S_8$$

since $\frac{q_1}{q_1^2-5q_2^2}, \frac{-q_2}{q_1^2-5q_2^2} \in \mathbb{Q}$, which shows that S_8 is closed under taking multiplicative inverses.

(ix) $S_9 = \left\{ r \in \mathbb{R} : \exists\ p_1, p_2 \in \mathbb{Q} \text{ such that } r = p_1 - p_2\sqrt{20} \right\}$ has all 4 properties, and we could give a very similar justification to the one we gave for S_8.

Alternatively, we could note that $S_9 = S_8$. Indeed, if $s \in S_9$, then we can find $p_1, p_2 \in \mathbb{Q}$ such that $s = p_1 - p_2\sqrt{20}$. But then

$$p_1 - p_2\sqrt{20} = p_1 - p_2\sqrt{4 \cdot 5} = p_1 - 2p_2\sqrt{5} = p_1 + (-2p_2)\sqrt{5} \in S_8,$$

which shows that $S_9 \subseteq S_8$.

Conversely, if $r \in S_8$, then we can find $q_1, q_2 \in \mathbb{Q}$ such that $r = q_1 + q_2\sqrt{5}$. But then

$$q_1 + q_2\sqrt{5} = q_1 + \frac{q_2}{2}2\sqrt{5} = q_1 - \left(\frac{-q_2}{2}\right)\sqrt{20} \in S_9,$$

which shows that $S_8 \subseteq S_9$.

(x) $S_{10} = \{r \in \mathbb{R} : \exists\ s_1, s_2 \in \mathbb{Q} \text{ such that } r = s_1 + es_2\}$ has Properties P1 and P3: indeed, if $r_1, r_2 \in S_{10}$, then we can write

$$r_1 = s_1 + es_2 \quad \text{and} \quad r_2 = s_3 + es_4$$

for some $s_1, s_2, s_3, s_4 \in \mathbb{Q}$. But then

$$r_1 + r_2 = (s_1 + es_2) + (s_3 + es_4) = (s_1 + s_3) + e(s_2 + s_4) \in S_{10}$$

since $s_1 + s_3,\ s_2 + s_4 \in \mathbb{Q}$, which shows that S_{10} is closed under addition. Similarly, $-r_1 = (-s_1) + e(-s_2) \in S_{10}$, given that $-s_1, -s_2 \in \mathbb{Q}$, which shows that S_{10} is closed under taking additive inverses.

On the other hand, S_{10} does not have Properties P2 and P4.

To justify that it is not closed under multiplication, we note that $e = 0 + e \cdot 1 \in S_{10}$, but $e^2 = e \cdot e$ is not. Indeed, if we assumed towards a contradiction that e^2 were in S_{10}, then we should be able to write

$$e^2 = s_1 + es_2 \quad \text{for some } s_1, s_2 \in \mathbb{Q}.$$

We could then write $s_1 = \frac{m_1}{n_1}$ and $s_2 = \frac{m_2}{n_2}$ for some integers m_1, m_2, n_1, n_2, $n_1 n_2 \neq 0$, which would give

$$e^2 - \frac{m_2}{n_2}e - \frac{m_1}{n_1} = 0 \qquad \Leftrightarrow \qquad n_1 n_2 e^2 - m_2 n_1 e - m_1 n_2 = 0$$

and would show that e is a root of the non-zero polynomial

$$n_1 n_2 x^2 - m_2 n_1 x - m_1 n_2$$

with integer coefficients. We now recall that this contradicts the fact that e is a transcendental number, so our assumption that $e^2 \in S_{10}$ was incorrect.

Similarly we justify that $e^{-1} \notin S_{10}$ even though e is an element of S_{10}, which will show that S_{10} is not closed under taking multiplicative inverses.

Indeed, if we had

$$\frac{1}{e} = t_1 + et_2 \quad \text{for some } t_1, t_2 \in \mathbb{Q},$$

then we could remark that e satisfies the polynomial equation $t_2 e^2 + t_1 e - 1 = 0$, or in other words, it is a root of the non-zero polynomial $t_2 x^2 + t_1 x - 1$ which has rational coefficients. As before, we could then conclude that it is also a root of a non-zero polynomial with integer coefficients, which we know cannot happen.

(xi) $S_{11} = \left\{ r \in \mathbb{R} : \exists\, t_1, t_2, t_3 \in \mathbb{Q} \text{ such that } r = t_1 + t_2\sqrt[3]{2} + t_3\sqrt[3]{4} \right\}$ has all 4 properties.

Indeed, if $r_1, r_2 \in S_{11}$, then we can write

$$r_1 = t_1 + t_2\sqrt[3]{2} + t_3\sqrt[3]{4} \quad \text{and} \quad r_2 = t_4 + t_5\sqrt[3]{2} + t_6\sqrt[3]{4}$$

for some $t_i \in \mathbb{Q}$, $1 \leqslant i \leqslant 6$. But then

$$\begin{aligned} r_1 + r_2 &= (t_1 + t_2\sqrt[3]{2} + t_3\sqrt[3]{4}) + (t_4 + t_5\sqrt[3]{2} + t_6\sqrt[3]{4}) \\ &= (t_1 + t_4) + (t_2 + t_5)\sqrt[3]{2} + (t_3 + t_6)\sqrt[3]{4} \in S_{11} \end{aligned}$$

since $t_1 + t_4, t_2 + t_5$ and $t_3 + t_6$ are in $\mathbb{Q}$.

Similarly,

$$\begin{aligned} r_1 \cdot r_2 &= (t_1 + t_2\sqrt[3]{2} + t_3\sqrt[3]{4}) \cdot (t_4 + t_5\sqrt[3]{2} + t_6\sqrt[3]{4}) \\ &= (t_1t_4 + 2t_2t_6 + 2t_3t_5) + (t_1t_5 + t_2t_4 + 2t_3t_6)\sqrt[3]{2} + (t_1t_6 + t_3t_4 + t_2t_5)\sqrt[3]{4} \in S_{11} \end{aligned}$$

since $t_1t_4 + 2t_2t_6 + 2t_3t_5, t_1t_5 + t_2t_4 + 2t_3t_6$ and $t_1t_6 + t_3t_4 + t_2t_5$ are in $\mathbb{Q}$.

Moreover,

$$-r_1 = (-t_1) + (-t_2)\sqrt[3]{2} + (-t_3)\sqrt[3]{4} \in S_{11}.$$

Thus, S_{11} is closed under addition, multiplication and under taking additive inverses.

It remains to verify that S_{11} is closed under taking multiplicative inverses whenever possible: consider a non-zero element r of S_{11}; then $r = a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{4}$ with $a_1, a_2, a_3 \in \mathbb{Q}$ and **not all of them zero**.

We start with a few observations:

- $(\sqrt[3]{2})^{-1}$ is in S_{11}, since

$$(\sqrt[3]{2})^{-1} = \frac{1}{2}\sqrt[3]{4} = 0 + 0 \cdot \sqrt[3]{2} + \frac{1}{2} \cdot \sqrt[3]{4}.$$

- Similarly, $(\sqrt[3]{4})^{-1}$ is in S_{11}, since

$$(\sqrt[3]{4})^{-1} = \frac{1}{2}\sqrt[3]{2} = 0 + \frac{1}{2} \cdot \sqrt[3]{2} + 0 \cdot \sqrt[3]{4}.$$

- For every $q \in \mathbb{Q} \setminus \{0\}$, q^{-1} in S_{11} since

$$q^{-1} = q^{-1} + 0 \cdot \sqrt[3]{2} + 0 \cdot \sqrt[3]{4}.$$

- If s is a non-zero element of S_{11}, and we already know that the multiplicative inverse of s is in S_{11}, then we have that

  sr has a multiplicative inverse in S_{11}
  if and only if r has a multiplicative inverse in S_{11}.

  Indeed, if $(sr)^{-1} = s^{-1}r^{-1}$ is contained in S_{11}, then $r^{-1} = s \cdot s^{-1}r^{-1}$ is also contained in S_{11}, since S_{11} satisfies Property P2, and conversely if r^{-1} is contained in S_{11}, then $(sr)^{-1} = s^{-1}r^{-1}$ is also contained in S_{11} (recall that we already know that s^{-1} is contained in S_{11}).

With these in mind, we note that it suffices to prove $r^{-1} = (a_1+a_2\sqrt[3]{2}+a_3\sqrt[3]{4})^{-1}$ is contained in S_{11} only in the case that $a_1 = 1$. Indeed, in all other cases we can remark the following:

- if $a_1 \neq 0$ but also $a_1 \neq 1$, then we can instead investigate whether $\frac{1}{a_1}r$ has a multiplicative inverse in S_{11}, which from the last remark above is equivalent to r having a multiplicative inverse in S_{11};
- if $a_1 = 0$, then we know that we must have $a_2 \neq 0$ or $a_3 \neq 0$.
  In cases that $a_2 \neq 0$, we can instead investigate whether

  $$\frac{1}{2a_2}\sqrt[3]{4}r = 1 + \frac{a_3}{a_2}\sqrt[3]{2} + \frac{a_1}{2a_2}\sqrt[3]{4} = 1 + \frac{a_3}{a_2}\sqrt[3]{2}$$

  has a multiplicative inverse in S_{11}, which is equivalent to r having a multiplicative inverse in S_{11}.
  Similarly, in cases that $a_3 \neq 0$, we can instead investigate whether

  $$\frac{1}{2a_3}\sqrt[3]{2}r = 1 + \frac{a_2}{2a_3}\sqrt[3]{4}$$

  has a multiplicative inverse in S_{11}.

Thus, for the remaining argument, we assume that $r = 1+a_2\sqrt[3]{2}+a_3\sqrt[3]{4}$, and we aim to find $s = x_1 + x_2\sqrt[3]{2} + x_3\sqrt[3]{4} \in S_{11}$ such that

$$1 = r\cdot s = (x_1+2a_3x_2+2a_2x_3)+(a_2x_1+x_2+2a_3x_3)\sqrt[3]{2}+(a_3x_1+a_2x_2+x_3)\sqrt[3]{4}.$$

This is equivalent to solving the linear system

$$\left\{ \begin{array}{rcrcrcl} x_1 & + & 2a_3x_2 & + & 2a_2x_3 & = & 1 \\ a_2x_1 & + & x_2 & + & 2a_3x_3 & = & 0 \\ a_3x_1 & + & a_2x_2 & + & x_3 & = & 0 \end{array} \right\} \qquad (1)$$

in $\mathbb{Q}$. But

$$\begin{pmatrix} 1 & 2a_3 & 2a_2 \\ a_2 & 1 & 2a_3 \\ a_3 & a_2 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2a_3 & 2a_2 \\ 0 & 1-2a_2a_3 & 2(a_3-a_2^2) \\ 0 & a_2-2a_3^2 & 1-2a_2a_3 \end{pmatrix},$$

and it remains to check that the last matrix is invertible, and thus that it has 3 pivots.

We can consider two cases here:

Case 1: $1-2a_2a_3=0$**.** Then $2a_2a_3=1 \Rightarrow a_3=\frac{1}{2a_2}$, and thus we get

$$a_3-a_2^2=\frac{1}{2a_2}-a_2^2=\frac{1-2a_2^3}{2a_2}\neq 0,$$

given that $1-2a_2^3=0$ would imply $a_2=\left(\frac{1}{2}\right)^{1/3}$, which contradicts that $a_2\in\mathbb{Q}$.
Similarly,

$$a_2-2a_3^2=a_2-\frac{1}{2a_2^2}=\frac{2a_2^3-1}{2a_2^2}\neq 0,$$

and thus the last matrix is row equivalent to

$$\begin{pmatrix} 1 & 2a_3 & 2a_2 \\ 0 & a_2-2a_3^2 & 0 \\ 0 & 0 & 2(a_3-a_2^2) \end{pmatrix}$$

which has 3 pivots.

Case 2: $1-2a_2a_3\neq 0$**.** Then

$$\begin{pmatrix} 1 & 2a_3 & 2a_2 \\ 0 & 1-2a_2a_3 & 2(a_3-a_2^2) \\ 0 & a_2-2a_3^2 & 1-2a_2a_3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2a_3 & 2a_2 \\ 0 & 1 & \frac{2(a_3-a_2^2)}{1-2a_2a_3} \\ 0 & \frac{a_2-2a_3^2}{1-2a_2a_3} & 1 \end{pmatrix}$$
$$\sim \begin{pmatrix} 1 & 2a_3 & 2a_2 \\ 0 & 1 & \frac{2(a_3-a_2^2)}{1-2a_2a_3} \\ 0 & 0 & p_3 \end{pmatrix}$$

$$\text{where } \; p_3=1-\frac{2(a_2-2a_3^2)(a_3-a_2^2)}{(1-2a_2a_3)^2}.$$

We will now justify why $p_3 \neq 0$, and hence why it is the 3rd pivot of the last matrix: $p_3 = 0$ would be equivalent to

$$\begin{aligned} 0 &= (1-2a_2a_3)^2 - 2(a_2 - 2a_3^2)(a_3 - a_2^2) \\ &= 1 + 4a_2^2a_3^2 - 4a_2a_3 - 2a_2a_3 - 4a_2^2a_3^2 + 2a_2^3 + 4a_3^3 \\ &= 1 - 6a_2a_3 + 2a_2^3 + 4a_3^3. \end{aligned}$$

Clearly, if $a_2 = a_3 = 0$, this wouldn't hold, so we can assume that at least one of a_2, a_3 is non-zero.
Moreover, we can check that if exactly one of them were non-zero, while the other one were zero, again we would get a contradiction because $p_3 = 0$ would imply that either $\left(\frac{1}{2}\right)^{1/3}$ or $\left(\frac{1}{4}\right)^{1/3}$ is in $\mathbb{Q}$.

So we must have that both a_2, a_3 are non-zero. Furthermore, we can write

$$a_2 = \frac{m_2}{n_2} \quad \text{and} \quad a_3 = \frac{m_3}{n_3}$$

with $m_2, m_3, n_2, n_3 \in \mathbb{Z}$, and such that $\gcd(m_2, n_2) = \gcd(m_3, n_3) = 1$ *(note that we can always choose to write a_2 and a_3 in such a way; compare also with the proof that $\sqrt{2}$ is irrational, which is in the same spirit as the argument that follows).*
Then

$$\begin{gathered} 1 - 6a_2a_3 + 2a_2^3 + 4a_3^3 = 0 \quad \Leftrightarrow \\ (n_2n_3)^3 - 6m_2m_3(n_2n_3)^2 + 2m_2^3n_3^3 + 4m_3^3n_2^3 = 0 \quad \Leftrightarrow \\ (n_2n_3)^3 = 2\left[3m_2m_3(n_2n_3)^2 - m_2^3n_3^3 - 2m_3^3n_2^3\right]. \end{gathered}$$

From this we see that 2 must divide n_2n_3. If we suppose that 2 divides only n_3, then we would get that both m_3 and n_2 are odd, and thus $4m_3^3n_2^3$ is not a multiple of 8. But at the same time,

$$\begin{aligned} &n_3 \text{ is a multiple of } 2 \ \Rightarrow\ n_3^2 \text{ is a multiple of 4, while } 2n_3^2 \text{ and } n_3^3 \text{ are multiples of 8} \\ &\Rightarrow\ 4m_3^3n_2^3 = 6m_2m_3(n_2n_3)^2 - 2m_2^3n_3^3 - (n_2n_3)^3 \ \text{ is a multiple of 8,} \end{aligned}$$

which is a contradiction.
Similarly we arrive at a contradiction if we assume that 2 divides only n_2.

But then, if we consider the largest power k_2 of 2 that divides n_2 and also the largest power k_3 that divides n_3, we see that

$(n_2n_3)^3$ is a multiple of $2^{3(k_1+k_2)}$, while none of the summands in the expression

$$6m_2m_3(n_2n_3)^2 - 2m_2^3n_3^3 - 4m_3^3n_2^3$$

is divided by $2^{3(k_1+k_2)}$, but only by smaller powers of 2.
We conclude that we **cannot** have

$$(n_2n_3)^3 = 2\left[3m_2m_3(n_2n_3)^2 - m_2^3n_3^3 - 2m_3^3n_2^3\right],$$

and thus $p_3 \neq 0$. In other words, we've just seen that in Case 2 as well, the linear system in (1) has no pivot in the last column, and therefore it is consistent.

We conclude that the linear system (1) is always consistent, and thus the number $1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{4}$ has a multiplicative inverse in S_{11} as we wanted.

(b) We recall that a subset of $\mathbb{R}$ is a subfield if and only if

- it has at least two elements,
- it is closed under addition,
- it is closed under multiplication,
- it is closed under taking additive inverses,
- and it is closed under taking multiplicative inverses (whenever possible).

So from the above subsets, only the ones that have all 4 properties and also have at least two elements are subfields of $\mathbb{R}$: these are subsets $S_8 = S_9$ and S_{11}.

We finally note that, since $S_8 = S_9$, the sets described in parts (viii) and (ix) are isomorphic fields and one isomorphism is the identity map. Another isomorphism we could define is the function

$$f\left(q_1 + q_2\sqrt{5}\right) := q_1 - q_2\sqrt{5} = q_1 - \frac{q_2}{2}\sqrt{20}\,.$$

First of all, we note that this is a well-defined function: given that the set $\{1, \sqrt{5}\}$ is $\mathbb{Q}$-linearly independent (why?), each number in S_8 can be written in a unique way as $q_1 + q_2\sqrt{5}$ with $q_1, q_2 \in \mathbb{Q}$.

Moreover, the above function satisfies:

- $f(1) = 1$,
- $f\big((q_1 + q_2\sqrt{5}) + (q_3 + q_4\sqrt{5})\big) = f\big((q_1 + q_3) + (q_2 + q_4)\sqrt{5}\big) = (q_1 + q_3) - \frac{q_2+q_4}{2}\sqrt{20} = \big(q_1 - \frac{q_2}{2}\sqrt{20}\big) + \big(q_3 - \frac{q_4}{2}\sqrt{20}\big) = f\big(q_1 + q_2\sqrt{5}\big) + f\big(q_3 + q_4\sqrt{5}\big)$,
- and $f\big((q_1 + q_2\sqrt{5}) \cdot (q_3 + q_4\sqrt{5})\big) = f\big((q_1q_3 + 5q_2q_4) + (q_1q_4 + q_2q_3)\sqrt{5}\big) = (q_1q_3 + 5q_2q_4) - \frac{q_1q_4+q_2q_3}{2}\sqrt{20} = \big(q_1 - \frac{q_2}{2}\sqrt{20}\big) \cdot \big(q_3 - \frac{q_4}{2}\sqrt{20}\big) = f\big(q_1 + q_2\sqrt{5}\big) \cdot f\big(q_3 + q_4\sqrt{5}\big)$,

so f is a field homomorphism.

Finally, $f \circ f = id_{S_8}$, which implies (as we see in Problem 5 of this homework, by combining both its parts) that f is bijective. Therefore, f is a field isomorphism.

On the other hand, S_{11} is not isomorphic to S_8 (this is not necessary to justify here, but one way we could do so is to observe that, if they were isomorphic as fields, then they should also be isomorphic as vectors spaces over $\mathbb{Q}$; however, $\dim_{\mathbb{Q}} S_8 = 2$ while $\dim_{\mathbb{Q}} S_{11} = 3$, so the two vector spaces cannot be isomorphic).

Problem 2. (i) Since S_1 contains at least one element, we can find $x \in S_1$. Since S_1 is closed under taking additive inverses, we have that $-x$ is also in S_1. Finally, because S_1 is closed under addition too, we have that $0_{\mathbb{F}} = x + (-x)$ is also in S_1.

(ii) Since S_2 contains at least one non-zero element, we can find $y \in S_2$ with $y \neq 0_{\mathbb{F}}$. Given that $\mathbb{F}$ is a field, we know that y has a multiplicative inverse y^{-1}, and since S_2 is closed under taking multiplicative inverses, y^{-1} is in S_2 as well. Finally, because S_2 is closed under multiplication too, we have that $1_{\mathbb{F}} = y \cdot y^{-1}$ is also in S_2.

Problem 3. (a) As stated in the remark preceding this problem, it suffices to verify the following properties:

1. $1_{\mathcal{R}_2} \in \text{Range}(\phi)$,
2. $\text{Range}(\phi)$ is closed under the addition in $\mathcal{R}_2$,
3. $\text{Range}(\phi)$ is closed under the multiplication in $\mathcal{R}_2$,
4. $\text{Range}(\phi)$ is closed under taking additive inverses.

By definition of a ring homomorphism, we have that $\phi(1_{\mathcal{R}_1}) = 1_{\mathcal{R}_2}$, therefore $1_{\mathcal{R}_2} \in \text{Range}(\phi)$.

We now check property 2: let $u, v \in \text{Range}(\phi)$; we have to show that $u+v \in \text{Range}(\phi)$ too. We can find $x, y \in \mathcal{R}_1$ so that $u = \phi(x)$ and $v = \phi(y)$. But then, by the additivity of ϕ, we see that

$$u + v = \phi(x) + \phi(y) = \phi(x + y) \in \text{Range}(\phi),$$

as we wanted.

Similarly we check property 3: let $u, v \in \text{Range}(\phi)$ as above; we have to show that $u + v \in \text{Range}(\phi)$ too. If $u = \phi(x)$ and $v = \phi(y)$ as before, then by the multiplicativity of ϕ, we get that

$$u \cdot v = \phi(x) \cdot \phi(y) = \phi(x \cdot y) \in \text{Range}(\phi),$$

as we wanted.

Finally, we check property 4: let $w \in \text{Range}(\phi)$; we have to show that $-w \in \text{Range}(\phi)$ too.

First we check that $\phi(0_{\mathcal{R}_1}) = 0_{\mathcal{R}_2}$. As before, we can find $z \in \mathcal{R}_1$ so that $w = \phi(z)$. But then

$$\begin{aligned} &\phi(z) + \phi(0_{\mathcal{R}_1}) = \phi(z + 0_{\mathcal{R}_1}) = \phi(z) = \phi(z) + 0_{\mathcal{R}_2} \\ \Rightarrow \quad &\phi(0_{\mathcal{R}_1}) = (-\phi(z)) + \phi(z) + \phi(0_{\mathcal{R}_1}) = (-\phi(z)) + \phi(z) + 0_{\mathcal{R}_2} = 0_{\mathcal{R}_2}. \end{aligned}$$

Note now that

$$\begin{aligned} &w + \phi(-z) = \phi(z) + \phi(-z) = \phi(z + (-z)) = \phi(0_{\mathcal{R}_1}) = 0_{\mathcal{R}_2}, \\ \Rightarrow \quad &-w = -w + 0_{\mathcal{R}_2} = -w + w + \phi(-z) = \phi(-z) \in \text{Range}(\phi), \end{aligned}$$

as we wanted.

Combining all the above, we conclude that $\text{Range}(\phi)$ is a subring of $\mathcal{R}_2$.

(b) By part (a), we know that $\mathrm{Range}(\phi)$ is a subring of $\mathcal{R}_2$, so it remains to check that multiplication in $\mathrm{Range}(\phi)$ is commutative if we assume that multiplication in $\mathcal{R}_1 = \mathrm{Dom}(\phi)$ is commutative.

Consider $u, v \in \mathrm{Range}(\phi)$; we need to check that $u \cdot v = v \cdot u$. We can find $x, y \in \mathcal{R}_1$ such that $u = \phi(x)$ and $v = \phi(y)$. Since multiplication in $\mathcal{R}_1$ is commutative, we have that

$$x \cdot y = y \cdot x.$$

But this, combined with the fact that ϕ is a ring homomorphism, gives us the desired conclusion:

$$u \cdot v = \phi(x) \cdot \phi(y) = \phi(x \cdot y) = \phi(y \cdot x) = \phi(y) \cdot \phi(x) = v \cdot u.$$

(c) Recall that multiplication of matrices in $\mathbb{R}^{2\times 2}$ is not commutative, therefore $\mathbb{R}^{2\times 2}$ is a non-commutative ring. At the same time, $\mathbb{R}$ is a field, and therefore a commutative ring.

Define the following function from $\mathbb{R}$ to $\mathbb{R}^{2\times 2}$:

$$r \in \mathbb{R} \ \mapsto \ \phi(r) := \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}.$$

We verify that ϕ is a ring homomorphism. We immediately see that $\phi(1) = I_2$. Moreover, for every $r, s \in \mathbb{R}$, we have that

$$\phi(r+s) = \begin{pmatrix} r+s & 0 \\ 0 & r+s \end{pmatrix} = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} + \begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix} = \phi(r) + \phi(s),$$

and similarly

$$\phi(r \cdot s) = \begin{pmatrix} r \cdot s & 0 \\ 0 & r \cdot s \end{pmatrix} = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \cdot \begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix} = \phi(r) \cdot \phi(s).$$

We conclude that ϕ has the requested properties.

We finally observe that $\mathrm{Range}(\phi) = \left\{ \left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right) : r \in \mathbb{R} \right\} = \{ rI_2 : r \in \mathbb{R} \}$.

Problem 4. (a) Consider two arbitrary vectors $\bar{x}, \bar{y} \in V_1$, and $r \in \mathbb{F}$. Then, since f is linear, we have $f(\bar{x}+\bar{y}) = f(\bar{x}) + f(\bar{y})$ and $f(r\bar{x}) = rf(\bar{x})$. But then,

$$
\begin{aligned}
(g \circ f)(\bar{x}+\bar{y}) = g\big(f(\bar{x}+\bar{y})\big) &= g\big(f(\bar{x}) + f(\bar{y})\big) \\
&= g(f(\bar{x})) + g(f(\bar{y})) = (g \circ f)(\bar{x}) + (g \circ f)(\bar{y}),
\end{aligned}
$$

where we used that g is linear too.

Similarly,

$$(g \circ f)(r\bar{x}) = g\big(f(r\bar{x})\big) = g\big(rf(\bar{x})\big) = rg(f(\bar{x})) = r(g \circ f)(\bar{x}).$$

Since $\bar{x}, \bar{y} \in V_1$ and $r \in \mathbb{F}$ were arbitrary, we conclude that $g \circ f$ is linear.

(b) Consider arbitrary vectors $\bar{u}, \bar{v} \in V_2$ and $s \in \mathbb{F}$. We need to show that

$$h^{-1}(\bar{u}+\bar{v}) = h^{-1}(\bar{u}) + h^{-1}(\bar{v}) \quad \text{and} \quad h^{-1}(s\bar{u}) = sh^{-1}(\bar{u}).$$

For notational simplicity, let us write $h^{-1}(\bar{u}) = \bar{x} \in V_1$ and $h^{-1}(\bar{v}) = \bar{y} \in V_1$. By definition of the inverse function, we have that $h(\bar{x}) = \bar{u}$ and $h(\bar{y}) = \bar{v}$.

Moreover, since we know that h is linear, we can write

$$h(\bar{x}+\bar{y}) = h(\bar{x}) + h(\bar{y}) = \bar{u}+\bar{v} \quad \Rightarrow \quad h^{-1}(\bar{u}+\bar{v}) = \bar{x}+\bar{y} = h^{-1}(\bar{u}) + h^{-1}(\bar{v}).$$

Similarly, since h is linear,

$$h(s\bar{x}) = sh(\bar{x}) = s\bar{u} \quad \Rightarrow \quad h^{-1}(s\bar{u}) = s\bar{x} = sh^{-1}(\bar{u}).$$

Since $\bar{u}, \bar{v} \in V_2$ and $s \in \mathbb{F}$ were arbitrary, we conclude that h^{-1} is linear.

Problem 5. (a) Let a_1, a_2 be elements in A satisfying $f_1(a_1) = f_1(a_2)$; we have to show that $a_1 = a_2$. But, if $f_1(a_1) = f_1(a_2)$, then $g_1\big(f_1(a_1)\big) = g_1\big(f_1(a_2)\big)$, and hence

$$a_1 = \mathrm{id}_A(a_1) = (g_1 \circ f_1)(a_1) = (g_1 \circ f_1)(a_2) = \mathrm{id}_A(a_2) = a_2.$$

Since a_1, a_2 are arbitrary, this shows that f_1 is injective.

(b) Let $b \in B$; we have to show that there is $a \in A$ such that $b = f_2(a)$. We have that

$$b = \mathrm{id}_B(b) = (f_2 \circ h_2)(b) = f_2(h_2(b)),$$

therefore $h_2(b) \in A$ is a preimage of b under f_2.

Since $b \in B$ was arbitrary, this shows that f_2 is surjective.

Problem 6. From the tables we note that $a_6 = 0_{\mathcal{A}}$ and $a_3 = 1_{\mathcal{A}}$.

We observe that the set $B = \{a_6, a_3\}$ is a subfield of $\mathcal{A}$ of size 2. Indeed, B is a subset that has two elements, and is closed under addition and multiplication given that we have

$$a_6 + a_6 = a_6 \in B, \quad a_6 + a_3 = a_3 + a_6 = a_3 \in B, \quad a_3 + a_3 = a_6 \in B,$$
$$\text{and} \quad a_6 \cdot a_6 = a_6 \cdot a_3 = a_3 \cdot a_6 = a_6 \in B, \quad a_3 \cdot a_3 = a_3 \in B.$$

Moreover, a_6 and a_3 are their own additive inverses, while a_3 is its own multiplicative inverse; thus B is closed under taking additive and multiplicative inverses.

Given the above, we can conclude that B is a subfield of $\mathcal{A}$.

We now verify that $\mathcal{A}$ has no subfield of size 4. From Problem 2 above, we know that if we had a subset C with at least two elements (and thus at least one non-zero element) which is closed under taking additive and multiplicative inverses, then this subset C needs to contain $0_{\mathcal{A}} = a_6$ and $1_{\mathcal{A}} = a_3$. Therefore, the only subsets of $\mathcal{A}$ that could be subfields with size 4 should contain a_6, a_3 and two more elements.

Let's suppose we have such a subset C_0. Clearly, it should also be closed under addition and multiplication to be a subfield of $\mathcal{A}$. But we can now check:

- if one more element of C_0 is the element a_1, then $a_2 = a_1 \cdot a_1$ should also be in C_0, and then $a_7 = a_1 \cdot a_2$ should be in C_0 too, which implies that C_0 should have at least 5 elements, contrary to our assumption;

- similarly, if one more element of C_0 is the element a_2, then $a_5 = a_2 \cdot a_2$ should also be in C_0, and then $a_8 = a_2 \cdot a_5$ should be in C_0 too, which implies that C_0 should have at least 5 elements, contrary to our assumption;

- if one more element of C_0 is the element a_4, then $a_7 = a_4 \cdot a_4$ should also be in C_0, and then $a_1 = a_4 \cdot a_7$ should be in C_0 too, which implies that C_0 should have at least 5 elements, contrary to our assumption;

- if one more element of C_0 is the element a_5, then $a_1 = a_5 \cdot a_5$ should also be in C_0, and then $a_4 = a_5 \cdot a_1$ should be in C_0 too, which implies that C_0 should have at least 5 elements, contrary to our assumption;

- if one more element of C_0 is the element a_7, then $a_8 = a_7 \cdot a_7$ should also be in C_0, and then $a_2 = a_7 \cdot a_8$ should be in C_0 too, which implies that C_0 should have at least 5 elements, contrary to our assumption;

- finally, if one more element of C_0 is the element a_8, then $a_4 = a_8 \cdot a_8$ should also be in C_0, and then $a_5 = a_8 \cdot a_4$ should be in C_0 too, which implies that C_0 should have at least 5 elements, contrary to our assumption.

We conclude that no subset of $\mathcal{A}$ which contains a_6 and a_3 and has 4 elements can be closed under multiplication, while a subset with 4 elements that does not contain both a_6 and a_3 will not be closed either under taking additive inverses or under taking multiplicative inverses (or will fail to have both properties). Combining these, we see that no subset of $\mathcal{A}$ that has 4 elements can be a subfield of $\mathcal{A}$.