Math 127
Suggested solutions to Homework Set 2

Problem 1. (i) Consider an arbitrary $x \in \mathbb{R}$. By the way the 'new' addition on $\mathbb{R}$ is defined, we have

$$x \oplus (-1) = x + (-1) + 1 = x, \quad \text{and similarly} \quad (-1) \oplus x = (-1) + x + 1 = x.$$

Thus -1 acts as the neutral element of the 'new' addition, and since this is unique, we can conclude that $0' = -1$.

(ii) We observe that the element $1'$ should be a real number r_1 which satisfies

$$x = r_1 \odot x = 2r_1 x + 2r_1 + 2x + 1$$

for every $x \in \mathbb{R}$.

Applying this with $x = 0$, we see that we must have

$$0 = 2r_1 + 1 \quad \Rightarrow \quad r_1 = -\frac{1}{2} = -0.5.$$

We can now verify: given an arbitrary element $y \in \mathbb{R}$, we have

$$(-0.5) \odot y = 2(-0.5)y + 2(-0.5) + 2y + 1 = -y + (-1) + 2y + 1 = y,$$

as we wanted [it's also not hard to see that $(-0.5) \odot y = y \odot (-0.5)$].

Thus $1' = -0.5$.

(iii) Let y_0 stand for the 'new' additive inverse of 5. Then y_0 should satisfy

$$5 \oplus y_0 = y_0 \oplus 5 = 0' = -1.$$

We also note that, according to how the 'new' addition is defined,

$$y_0 \oplus 5 = y_0 + 5 + 1 = y_0 + 6.$$

Thus we need to have

$$y_0 + 6 = -1 \quad \Rightarrow \quad y_0 = -7.$$

We can also double check:

$$(-7) \oplus 5 = -7 + 5 + 1 = -1 = 0' = 5 \oplus (-7).$$

(iv) Let y_1 stand for the 'new' multiplicative inverse of 5. Then y_1 should satisfy

$$5 \odot y_1 = y_1 \odot 5 = 1' = -0.5.$$

We also note that, according to how the 'new' multiplication is defined,

$$y_1 \odot 5 = 2 \cdot y_1 \cdot 5 + 2 \cdot y_1 + 2 \cdot 5 + 1 = 12y_1 + 11.$$

Thus, we need to have

$$12y_1 + 11 = -0.5 \quad \Rightarrow \quad y_1 = -\frac{11.5}{12} = -\frac{23}{24}.$$

We can also double check:

$$\begin{aligned}\left(-\frac{23}{24}\right) \odot 5 &= 2 \cdot \left(-\frac{23}{24}\right) \cdot 5 \,+\, 2 \cdot \left(-\frac{23}{24}\right) \,+\, 2 \cdot 5 \,+\, 1 \\ &= 5 \cdot \left(-\frac{23}{12}\right) \,+\, \left(-\frac{23}{12}\right) \,+\, 11 = -\frac{23}{2} \,+\, 11 \\ &= -0.5 = 1' = 5 \odot \left(-\frac{23}{24}\right).\end{aligned}$$

(v) The answer here is no.

Observe that, for $(\mathbb{R}, \oplus, \odot)$ to be a subfield of $\mathbb{C}$ with the standard operations, we would need e.g. to have that $0' = 0_{\mathbb{C}}$.

But we showed in part (i) that this is not true since $0' = -1 \neq 0$. Hence, this new structure on $\mathbb{R}$ is not a subfield of the standard field structure on $\mathbb{C}$.

Problem 2. (i) We need to fill out the following tables of addition and multiplication so that the operations will satisfy the axioms of a field:

$+$	0	1	c	d
0				
1				
c				
d				

$\cdot$	0	1	c	d
0				
1				
c				
d				

.

Note that by the axioms for the existence of an additive and a multiplicative identity, as well as by the property "$0 \cdot x = 0$ for every x in the field" which follows from the field axioms, we have to start filling out the tables as follows:

(1)

$+$	0	1	c	d
0	0	1	c	d
1	1			
c	c			
d	d			

$\cdot$	0	1	c	d
0	0	0	0	0
1	0	1	c	d
c	0	c		
d	0	d		

(note that we filled out three columns too, and we did so as shown above, because we have to ensure commutativity as well).

Multiplication. We focus now on the table of multiplication. We recall the cancellation law as well, which we should make sure holds true if we want this table of multiplication to be that of a field: the law implies that the coloured part of the table below should have the property that different cells in the same row contain different non-zero elements, and analogously (because of commutativity as well) different cells in the same column contain different non-zero elements:

$\cdot$	0	1	c	d
0	0	0	0	0
1	0	1	c	d
c	0	c		
d	0	d		

.

Indeed, if we look at a row corresponding to a non-zero element x and at different cells within this row, one of them should contain the product $x \cdot y$ for some $y \in \mathbb{F}_4$ and the other cell should contain the product $x \cdot z$ for some $z \in \mathbb{F}_4$, $z \neq y$. But the cancellation law gives

$$\text{if } x \neq 0, \quad \text{then } x \cdot y = x \cdot z \quad \Rightarrow \quad y = z,$$

$$\text{or equivalently:} \quad \text{if } x \neq 0, \quad \text{then } y \neq z \quad \Rightarrow \quad x \cdot y \neq x \cdot z.$$

This shows that we can only use the elements 1 and d to fill out the rest of the third row in the above table: $c \cdot c$ should be equal to either 1 or d, and similarly $c \cdot d$ should be equal to either 1 or d and different from $c \cdot c$.

But $c \cdot d$ cannot be equal to d either, given that the fourth column already contains d. Therefore, we must have $c \cdot d = 1$, and this also implies that $c \cdot c = d$.

Recalling commutativity as well, we are forced to set $d \cdot c = 1$. This finally leaves one possibility for $d \cdot d$: $d \cdot d = c$.

Below is the fully completed table of multiplication:

$\cdot$	0	1	c	d
0	0	0	0	0
1	0	1	c	d
c	0	c	d	1
d	0	d	1	c

.

Remark 1 *(to be used in part (ii)).* Simply by how we completed the table, we have made sure

- that multiplication in this structure is commutative;
- that there exists an identity element, the element 1;
- that every element different from 0 has a multiplicative inverse (given that in every row in the coloured part of the table above there is a cell containing 1).

<u>Addition.</u> We now turn our attention to the table of addition. We start with the following claim (and give a justification for it at the end of part (i); recall that the hint given for Problem 2 essentially suggested we use this claim with or without proof).

Claim 1. $1 + 1 = 0$. *(Observe that this immediately gives that $\mathbb{Z}_2$ is a subfield of the structure $\mathbb{F}_4$ which we are trying to define; indeed, the result of adding or multiplying any other combination of the elements 0 and 1 has already been determined in the first step of filling out the tables (see* (1)*), and coincides with how these two elements interact in $\mathbb{Z}_2$.)*

Accepting the validity of the claim for now, we can fill out one more cell in the table of addition, but in fact we also get two more cells immediately: indeed, we must have that $c + c = 0$ because we can write

$$c + c = 1 \cdot c + 1 \cdot c = (1 + 1) \cdot c = 0 \cdot c = 0$$

(note that we can write the 2nd equality here, because we expect, and also want to make sure, the distributive law will hold at the end). Similarly, $d + d = 0$.

This leads to the following table:

$+$	0	1	c	d
0	0	1	c	d
1	1	0		
c	c		0	
d	d			0

.

We are now essentially done: note that the third cell in the second row should be filled out with either c or d (given that we want to make sure the cancellation law for addition holds). However, because it belongs to the third column as well, which already contains c, this cell can only be filled out with d.

This also shows that the last cell in the same row must be filled out with c (and by commutativity, which we also want to ensure, we get the full second column as well).

Similarly we argue for the last cell in the third row, and the third cell in the last row, both of which must be filled out with 1.

Below is the fully completed table of addition:

$+$	0	1	c	d
0	0	1	c	d
1	1	0	d	c
c	c	d	0	1
d	d	c	1	0

.

Remark 2 *(to be used in part (ii)).* Simply by how we completed the table, we have made sure

- that addition in this structure is commutative;
- that there exists a neutral element, the element 0;
- that every element has an additive inverse (given that in every row of the table there is a cell containing 0).

We finish part (i) by justifying Claim 1. We will do so using proof by contradiction.

Proof of Claim 1. Note that, if we want to make sure the cancellation law holds, $1+1$ cannot be equal to 1, so it can only be $0, c$ or d.

Assume that $1+1=c$ and that there is still a way to fill out the table of addition so that $\mathbb{F}_4$ with this table and the table of multiplication we have above has a field structure. We will show that these two assumptions cannot hold true at the same time.

If $1+1=c$, then this leaves two possibilities for $1+c$ (given how we've completed so far the second row of the table): it's either equal to 0 or d.

Case 1: set $1+c=0$. Then we are left with only one possibility for $1+d$ (again given how we've completed the second row so far): $1+d=d$. This however will violate the cancellation law since we also have $0+d=d$.

Case 2: set $1+c=d$. Then $1+d$ has to be equal to 0. But then, since we have assumed that we can continue completing the table so that commutativity and the distributive law will hold at the end (and given the table of multiplication we've already uniquely determined so that it satisfies the field properties), we can write

$$0 = 0 \cdot c = (1+d) \cdot c = 1 \cdot c + d \cdot c = c + 1 = 1 + c = d.$$

This clearly contradicts one of our initial assumptions, that $d \neq 0$.

We can give a completely analogous argument which will show that we cannot set $1+1=d$ either (check this yourselves).

Therefore, this shows that we must set $1+1=0$ in order to be able to get a table of a field at the end.

This completes part (i).

(ii) First we check the axioms concerning only addition. Recalling Remark 2, we observe that we have already ensured three of these axioms by how we filled out the table, and now it only remains to check that addition is associative.

In other words, we have to show that, for every $x, y, z \in \mathbb{F}_4$, $(x+y)+z = x+(y+z)$. We do so by grouping the many different combinations of x, y, z we have to consider into a few main cases.

Case 1: one of $\boldsymbol{x, y, z}$ is 0. For convenience, we break this case into 3 smaller cases:

- $\underline{x=0}$ Then we have $(x+y)+z = (0+y)+z = y+z = 0+(y+z)$.
- $\underline{y=0}$ Then we have $(x+0)+z = x+z = x+(0+z)$.
- $\underline{z=0}$ Then we have $(x+y)+0 = x+y = x+(y+0)$.

Case 2: $\boldsymbol{x = y = z}$. Then $(x+y)+z = (x+x)+x = x+(x+x)$ simply by commutativity.

Case 3: two of $\boldsymbol{x, y, z}$ are equal and $\neq 0$, the third one different and $\neq 0$. Observe that here the set $\{x, y, z\}$ contains two of the elements of the set $\{1, c, d\}$; we set w for the remaining element of $\{1, c, d\}$ which is not equal to any of x, y, z. Again we break this case into smaller cases.

$\underline{x = y \neq z}$ Note that in this subcase we have $x+y = x+x = 0$, while

$$y+z = w, \quad x+w = y+w = z$$

(why? note that here y, z, w are three different elements, and $\{y, z, w\} = \{1, c, d\}$, so these equalities follow from the table of addition that we have above, **regardless of which of $\boldsymbol{y, z, w}$ is equal to 1 or $\boldsymbol{c}$ or $\boldsymbol{d}$**).

Therefore, we can write $(x+y)+z = (x+x)+z = 0+z = z$, while $x+(y+z) = x+w = z$, showing that the two expressions $(x+y)+z$ and $x+(y+z)$ are equal.

$\underline{x = z \neq y}$ In this subcase $x+y = w$, and similarly $y+z = z+y = x+y = w$, while $w+z = z+w = y$ (why? try to convince yourselves about it giving a similar justification to the one in the subcase above).

Therefore, we can write $(x+y)+z = w+z = y$, while $x+(y+z) = x+w = z+w = y$ too, as we wanted.

$\underline{x \neq y = z}$ In this subcase $x+y = w$ and $w+y = w+z = x$, while $y+z = z+z = 0$. Therefore, $(x+y)+z = w+z = x$, while $x+(y+z) = x+0 = x$ too, as we wanted.

Case 4: x, y, z are three different elements, and $x, y, z \in \{1, c, d\}$. In this case we have $\{x, y, z\} = \{1, c, d\}$, and hence $x + y = z$ and $y + z = x$. We also have $x + x = z + z = 0$.

Therefore, we can write $(x + y) + z = z + z = 0 = x + x = x + (y + z)$, as we wanted.

It is not hard to see that every combination of x, y, z from $\mathbb{F}_4$ belongs to one of the above cases (some of them may even belong to more than one cases). We have thus shown that addition, in the way we defined it, is associative.

We turn to the axioms concerning multiplication only. Recalling Remark 1, we observe that we have already ensured three of these axioms by how we filled out the table. We have also made sure that $0 \cdot x = x \cdot 0 = 0$ for every $x \in \mathbb{F}_4$.

It only remains to check that multiplication is associative. In other words, we have to show that, for every $x, y, z \in \mathbb{F}_4$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. We do so by considering a few main cases again.

Case 1: one of x, y, z is 0. For convenience, we break this case into 3 smaller cases:

$\underline{x = 0}$ Then we have $(x \cdot y) \cdot z = (0 \cdot y) \cdot z = 0 \cdot z = 0$, while $x \cdot (y \cdot z) = 0 \cdot (y \cdot z) = 0$, therefore $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ in this case.

$\underline{y = 0}$ Then we have $(x \cdot 0) \cdot z = 0 \cdot z = 0$, while $x \cdot (0 \cdot z) = x \cdot 0 = 0$ too, as we wanted.

$\underline{z = 0}$ Then we have $(x \cdot y) \cdot 0 = 0$, while $x \cdot (y \cdot 0) = x \cdot 0 = 0$ too, as we wanted.

Case 2: one of x, y, z is 1. We break this case into 3 smaller cases:

$\underline{x = 1}$ Then we have $(x \cdot y) \cdot z = (1 \cdot y) \cdot z = y \cdot z = 1 \cdot (y \cdot z) = x \cdot (y \cdot z)$.

$\underline{y = 1}$ Then we have $(x \cdot 1) \cdot z = x \cdot z = x \cdot (1 \cdot z)$.

$\underline{z = 1}$ Then we have $(x \cdot y) \cdot 1 = x \cdot y = x \cdot (y \cdot 1)$.

It remains to check the cases where $x, y, z \in \{c, d\}$. There are two main cases here:

Case 3: $x = y = z$. Then $(x \cdot x) \cdot x = x \cdot (x \cdot x)$ simply by commutativity.

Case 4: $\{x, y, z\} = \{c, d\}$. In other words, in this case we have two of x, y, z being equal to each other and equal either to c or d, and the third element of x, y, z being equal to the remaining element of $\{c, d\}$.

We will break this case into 3 smaller cases and we will use the fact that $c \cdot c = d$, $d \cdot d = c$ and $c \cdot d = d \cdot c = 1$.

$\underline{x = y \neq z}$ Given the products above, we can see that, **regardless of whether $x = c$ or $x = d$**, we have that $x \cdot y = x \cdot x = z$, $z \cdot z = x$, and $x \cdot z = y \cdot z = 1$. Therefore, we have

$$(x \cdot y) \cdot z = z \cdot z = x, \qquad \text{while} \;\; x \cdot (y \cdot z) = x \cdot 1 = x,$$

which shows what we wanted in this case.

$\underline{x \neq y = z}$ Similarly here we have $x \cdot y = x \cdot z = 1$, while $x \cdot x = y = z$, $y \cdot z = z \cdot z = x$. Therefore, we have

$$(x \cdot y) \cdot z = 1 \cdot z = z, \qquad \text{while} \;\; x \cdot (y \cdot z) = x \cdot x = z,$$

which shows what we wanted.

$\underline{x = z \neq y}$ Here we have $x \cdot y = 1 = y \cdot z$. Therefore,

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

as we wanted.

We have now checked all cases regarding associativity of multiplication, so we can conclude that multiplication in $\mathbb{F}_4$, in the way that we defined it, is associative.

It remains to check that the distributive law holds. In other words, we have to check that, for every $x, y, z \in \mathbb{F}_4$, $(x + y) \cdot z = x \cdot z + y \cdot z$. We do so by considering cases.

Case 1: $z = 0$. Then $(x+y) \cdot z = (x+y) \cdot 0 = 0 = x \cdot 0 + y \cdot 0 = x \cdot z + y \cdot z$, as we wanted.

Case 2: $z = 1$. Then $(x+y) \cdot z = (x+y) \cdot 1 = x+y = x \cdot 1 + y \cdot 1 = x \cdot z + y \cdot z$, as we wanted.

Case 3: one of x, y is equal to 0. Note that it suffices to check this case when $x = 0$ (indeed, if $y = 0$ instead, then, using commutativity, we will be able to write $(x+y) \cdot z = (y+x) \cdot z$ and $x \cdot z + y \cdot z = y \cdot z + x \cdot z$, and then just repeat the proof we give below with the roles of x and y interchanged).

But if $x = 0$, then $(x+y) \cdot z = (0+y) \cdot z = y \cdot z = 0 \cdot z + y \cdot z = x \cdot z + y \cdot z$.

Case 4: $x = y$. Then $x+y = 0$, while $x \cdot z = y \cdot z$, and hence $x \cdot z + y \cdot z = 0$ as well (recall the table of addition we ended up with). Therefore, $(x + y) \cdot z = 0 \cdot z = 0 = x \cdot z + y \cdot z$.

Case 5: $z \in \{c, d\}$ and $x, y \in \{1, c, d\}$ and $x \neq y$. We consider three smaller cases here:

<u>x, y, z are all different</u> Then necessarily one of x, y is equal to 1 (why?). Similarly to Case 3 above, it suffices to assume that $x = 1$ (and therefore that $\{y, z\} = \{c, d\}$).

We also have that $x + y = z$ and that $y \cdot z = c \cdot d$ or $= d \cdot c$ (by commutativity the two products are equal anyway), therefore $y \cdot z = 1$. Finally, $z \cdot z = y$ regardless of whether $z = c$ or $z = d$.

We thus have $(x+y) \cdot z = z \cdot z = y$, while $x \cdot z + y \cdot z = 1 \cdot z + y \cdot z = z + 1 = y$, again regardless of whether $z = c$ or $z = d$. This shows that the two expressions $(x + y) \cdot z$ and $x \cdot z + y \cdot z$ are equal.

<u>one of x, y is equal to z, while the other one is $= 1$</u> Similarly to Case 3 above, or the previous subcase, we note that it suffices to assume that $x = z$, and hence $x \in \{c, d\}$, while $y = 1$.

Let w be the other element in $\{c, d\}$ which is different from x and z. Then $x + y = x + 1 = w$, $w \cdot z = 1$, while $x \cdot z = z \cdot z = w$, $y \cdot z = 1 \cdot z = z$ and $w + z = 1$.

Therefore, $(x + y) \cdot z = w \cdot z = 1$, while $x \cdot z + y \cdot z = w + z = 1$ too, as we wanted.

<u>one of x, y is equal to z, and $\{x, y\} = \{c, d\}$</u> Again, it suffices to assume that $x = z$, while $y \neq x$.

In this case $y \in \{c, d\}$, hence y is the element in $\{c, d\}$ which is different from x and z.

But then $x \cdot z = z \cdot z = y$, while $y \cdot z = 1$. Similarly, $x+y = 1$, while $y+1 = z$. Therefore, $(x+y) \cdot z = 1 \cdot z = z$, while $x \cdot z + y \cdot z = y+1 = z$ too, as we wanted.

It is not hard to see that every combination of x, y, z from $\mathbb{F}_4$ belongs to one of the above cases (again some of them may belong to more than one cases), and therefore that we have fully checked the distributive law holds.

Problem 3. (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) $S_9 = \{r \in \mathbb{R} : \exists\ p_1, p_2 \in \mathbb{Q}$ such that $r = p_1 - p_2\sqrt{20}\}$ 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) $S_{10} = \{r \in \mathbb{R} : \exists\ s_1, s_2 \in \mathbb{Q}$ 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.

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

- it contains the additive identity,
- it contains the multiplicative identity,
- 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 the subsets S_8 and S_9 (which in fact are the same set, and hence the same subfield of $\mathbb{R}$).

Problem 4. (i) We need to find two different points P_0, P_1 on ℓ_1.

To find the first point, we could set $x = 0$ and solve for y in the linear equation representing ℓ_1: we must have

$$4y + 2 = 0 \quad \Rightarrow \quad 4y = -2 \quad \Rightarrow \quad y = -1/2.$$

Thus the point $P_0(0, -1/2)$ is contained in ℓ_1.

To find the second point, we could set $y = 0$ and solve for x (note that this point will be different from P_0 since P_0 has non-zero second coordinate): we must have

$$3x + 2 = 0 \quad \Rightarrow \quad 3x = -2 \quad \Rightarrow \quad x = -2/3.$$

Thus the point $P_1(-2/3, 0)$ is also contained in ℓ_1.

If we denote the point $(0,0)$ in $\mathbb{R}^2$ by O, then by the above we see that a vector equation for ℓ_1 is

$$\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = \overrightarrow{OP_0} + t\overrightarrow{P_0P_1} = \left(\begin{smallmatrix} 0 \\ -1/2 \end{smallmatrix}\right) + t\begin{pmatrix} -2/3 \\ 1/2 \end{pmatrix}, \qquad t \in \mathbb{R}.$$

(ii) We need to find two different points P_0, P_1 on ℓ_2. We first try to transform the system of linear equations representing ℓ_2 to an equivalent but slightly simpler one: here we can simply add both sides of the two linear equations to get a new one, which will be simpler as it will only involve the unknowns x and z, and which we can use in place of one of the original equations (while also keeping the other one).

$$\left\{ \begin{array}{c} x - y + 3z = 0 \\ x + y - z - 2 = 0 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{c} x - y + 3z = 0 \\ 2x + 2z - 2 = 0 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{c} x - y + 3z = 0 \\ x + z - 1 = 0 \end{array} \right\}.$$

Now, to find a point on ℓ_2, we could set $x = 0$ and solve for z in the second linear equation in the last system, and then solve for y in the first equation (after plugging in the values for x and z which we will already have): by the second equation we see that

$$z - 1 = 0 + z - 1 = 0 \quad \Rightarrow \quad z = 1,$$

and then by the first equation we obtain that

$$-y + 3 = 0 - y + 3 \cdot 1 = 0 \quad \Rightarrow \quad y = 3.$$

Thus the point $P_0(0, 3, 1)$ is contained in ℓ_2.

To find a second point, we could set $z = 0$ and solve for x in the second equation, and then solve for y in the first equation (note that this point will be different from P_0 since P_0 has non-zero third coordinate): by the second equation we must have

$$x - 1 = 0 \quad \Rightarrow \quad x = 1,$$

and then by the first equation we see that

$$1 - y = 0 \quad \Rightarrow \quad y = 1.$$

Thus the point $P_1(1, 1, 0)$ is also contained in ℓ_2.

If we denote the point $(0, 0, 0)$ in $\mathbb{R}^3$ by O, then by the above we see that a vector equation for ℓ_2 is

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \overrightarrow{OP_0} + t\overrightarrow{P_0P_1} = \begin{pmatrix} 0 \\ 3 \\ 1 \end{pmatrix} + t\begin{pmatrix} 1 \\ -2 \\ -1 \end{pmatrix}, \qquad t \in \mathbb{R}.$$

(iii) We need to find three different points P_1, P_2 and P_3 in $\mathcal{P}_1$ which are also not collinear.

To find the first point, we could set $x = 0$ and $y = 0$ and solve for z in the linear equation representing $\mathcal{P}_1$: we get $z = 0$ (indeed the origin O is contained in $\mathcal{P}_1$).

To find a second point, we set $x = 1$ and $y = 1$ and solve for z: we must have

$$2 - 1 - z = 2 \cdot 1 - 1 - z = 0 \quad \Rightarrow \quad 1 - z = 0 \quad \Rightarrow \quad z = 1.$$

Thus the point $P_2(1, 1, 1)$ is contained in $\mathcal{P}_1$.

Next we note that all points contained in the line determined by $P_1 = O$ and P_2 have first two coordinates equal (in fact they have all three coordinates equal). Indeed, one vector equation for this line is

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = t\,\overrightarrow{OP_2} = t\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} t \\ t \\ t \end{pmatrix}, \qquad t \in \mathbb{R}.$$

Thus to find a third point in $\mathcal{P}_1$ that is also <u>not</u> on the line determined by P_1 and P_2, we could set $x = 2$ and $y = 1$; then we must have $-z = 2 \cdot 1 - 2 - z = 0 \Rightarrow z = 0$. Thus the point $P_3(2, 1, 0)$ is contained in $\mathcal{P}_1$ and we have that the points $P_1 = O, P_2$ and P_3 are not collinear.

In such a case, we know that a vector equation for $\mathcal{P}_1$ is

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = t\,\overrightarrow{OP_2} + s\,\overrightarrow{OP_3} = t\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + s\begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}, \qquad t, s \in \mathbb{R}.$$

(iv) We need to find three different points P_1, P_2 and P_3 in $\mathcal{P}_2$ which are also not collinear.

To find the first point, we could set $x = 0$ and $y = 0$ and solve for z in the linear equation representing $\mathcal{P}_2$: we get $z = -6$. Thus the point $P_1(0, 0, -6)$ is contained in $\mathcal{P}_2$.

To find a second point, we set $x = 1$ and $y = 1$ and solve for z: we must have

$$1 - 3 + z + 6 = 1 - 3 \cdot 1 + z + 6 = 0 \quad \Rightarrow \quad z + 4 = 0 \quad \Rightarrow \quad z = -4.$$

Thus the point $P_2(1, 1, -4)$ is contained in $\mathcal{P}_2$.

Next we note that all points contained in the line determined by P_1 and P_2 have first two coordinates equal. Indeed, one vector equation for this line is

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \overrightarrow{OP_1} + t\,\overrightarrow{P_1P_2} = \begin{pmatrix} 0 \\ 0 \\ -6 \end{pmatrix} + t \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} t \\ t \\ -6+2t \end{pmatrix}, \qquad t \in \mathbb{R}.$$

Thus to find a third point in $\mathcal{P}_2$ that is also <u>not</u> on the line determined by P_1 and P_2, we could set $x = 1$ and $y = 0$: then we must have

$$1 + z + 6 = 0 \quad \Rightarrow \quad z + 7 = 0 \quad \Rightarrow \quad z = -7.$$

Thus the point $P_3(1, 0, -7)$ is contained in $\mathcal{P}_2$ and we have that the points P_1, P_2 and P_3 are not collinear.

In such a case, we know that a vector equation for $\mathcal{P}_2$ is

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \overrightarrow{OP_1} + t\,\overrightarrow{P_1P_2} + s\,\overrightarrow{P_1P_3} = \begin{pmatrix} 0 \\ 0 \\ -6 \end{pmatrix} + t \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix} + s \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \qquad t, s \in \mathbb{R}.$$

Problem 5. (i) We consider three arbitrary vectors $\bar{u} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}$, $\bar{v} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$ and $\bar{w} = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}$ in $\mathbb{R}^n$. We first observe that

$$\bar{v} + \bar{w} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} + \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} v_1+w_1 \\ v_2+w_2 \\ \vdots \\ v_n+w_n \end{pmatrix}.$$

Therefore

$$\langle \bar{u}, \bar{v} + \bar{w} \rangle = \sum_{i=1}^{n} u_i(v_i + w_i). \tag{2}$$

At the same time,

$$\langle \bar{u}, \bar{v} \rangle + \langle \bar{u}, \bar{w} \rangle = \left(\sum_{i=1}^{n} u_i v_i \right) + \left(\sum_{i=1}^{n} u_i w_i \right) = \sum_{i=1}^{n} \big(u_i v_i + u_i w_i \big) \tag{3}$$

where the second equality follows from the commutativity and the associativity of addition in $\mathbb{R}$.

We now observe that, because of the distributive law in $\mathbb{R}$, $u_i(v_i + w_i) = u_i v_i + u_i w_i$ for every index i. Thus, combining (2) and (3), we get

$$\langle \bar{u}, \bar{v} + \bar{w} \rangle = \sum_{i=1}^{n} u_i(v_i + w_i) = \sum_{i=1}^{n} \big(u_i v_i + u_i w_i \big) = \langle \bar{u}, \bar{v} \rangle + \langle \bar{u}, \bar{w} \rangle.$$

(ii) We want to find non-zero $t, s \in \mathbb{R}$ such that $0 = \langle \bar{u}_1, t\bar{v}_1 + s\bar{w}_1 \rangle$. From part (i) and also the property of the dot product which we proved in class and states that $\langle \bar{x}, \lambda \bar{y} \rangle = \lambda \langle \bar{x}, \bar{y} \rangle$ for every two vectors x, y in $\mathbb{R}^n$ and every scalar λ, we obtain

$$\langle \bar{u}_1, t\bar{v}_1 + s\bar{w}_1 \rangle = \langle \bar{u}_1, t\bar{v}_1 \rangle + \langle \bar{u}_1, s\bar{w}_1 \rangle = t\langle \bar{u}_1, \bar{v}_1 \rangle + s\langle \bar{u}_1, \bar{w}_1 \rangle.$$

Thus we want to find non-zero $t, s \in \mathbb{R}$ such that

$$t\langle \bar{u}_1, \bar{v}_1 \rangle + s\langle \bar{u}_1, \bar{w}_1 \rangle = 0.$$

Since we have the assumption that $\langle \bar{u}_1, \bar{v}_1 \rangle \neq 0$ and $\langle \bar{u}_1, \bar{w}_1 \rangle \neq 0$, we can solve this linear equation in the unknown t, s by setting t equal to some non-zero value and then solving for s: if e.g. $t = 1$, then we must have

$$0 = \langle \bar{u}_1, \bar{v}_1 \rangle + s\langle \bar{u}_1, \bar{w}_1 \rangle \quad \Rightarrow \quad s = -\frac{\langle \bar{u}_1, \bar{v}_1 \rangle}{\langle \bar{u}_1, \bar{w}_1 \rangle}.$$

We also remark that this s has to be non-zero.

We conclude that, for $t = 1$ and $s = -\frac{\langle \bar{u}_1, \bar{v}_1 \rangle}{\langle \bar{u}_1, \bar{w}_1 \rangle}$, the vector $t\bar{v}_1 + s\bar{w}_1$ is orthogonal to $\bar{u}_1$, as we wanted.

Problem 6. (i) Let $\bar{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$. We recall that

$$\langle \bar{x}, \bar{x} \rangle = x_1^2 + x_2^2 + \cdots + x_n^2 = \sum_{i=1}^{n} x_i^2.$$

We also recall that, for any real number a, its square a^2 is nonnegative (that is, $a^2 \geqslant 0$).

Moreover, if we add finitely many nonnegative real numbers $a_1, a_2, \ldots, a_n$, the result is again a nonnegative number: that is, if $a_1, a_2, \ldots, a_n \in \mathbb{R}$ with $a_i \geqslant 0$ for every index i, then $a_1 + a_2 + \cdots + a_n \geqslant 0$ (although this is not necessary to justify here, this last fact can be shown using mathematical induction in the number n of the summands: indeed, the base case can be $n = 2$, in which case we have

$$a_1 \geqslant 0 \text{ and } a_2 \geqslant 0 \quad \Rightarrow \quad a_1 + a_2 \geqslant a_1 + 0 = a_1 \geqslant 0$$

using fundamental properties of the ordering in $\mathbb{R}$; then we assume that the claim is true when we add n nonnegative real numbers $a_1, a_2, \ldots, a_n$ with $n \geqslant 2$, and show that it remains true when we add $n+1$ nonnegative real numbers: if $a_1, a_2, \ldots, a_n, a_{n+1} \in \mathbb{R}$ with $a_i \geqslant 0$ for every index i, then

$$\begin{aligned} a_1 + a_2 + \cdots + a_n + a_{n+1} &= (a_1 + a_2 + \cdots + a_n) + a_{n+1} \\ &\geqslant (a_1 + a_2 + \cdots + a_n) + 0 = a_1 + a_2 + \cdots + a_n \geqslant 0 \end{aligned}$$

with the last inequality following from our inductive hypothesis).

Combining the above, we conclude that $\langle \bar{x}, \bar{x} \rangle = x_1^2 + x_2^2 + \cdots + x_n^2 \geqslant 0$. Since $\bar{x}$ was an arbitrary vector in $\mathbb{R}^n$, the proof is complete.

(ii) We start with the following

Remark. One way to prove the equivalence

$$\langle \bar{x}, \bar{x} \rangle = 0 \Leftrightarrow \bar{x} = \bar{0}$$

is to prove the following two statements:

$$1. \quad \text{if } \bar{x} = \bar{0}, \text{ then } \langle \bar{x}, \bar{x} \rangle = 0; \qquad 2. \quad \text{if } \bar{x} \neq \bar{0}, \text{ then } \langle \bar{x}, \bar{x} \rangle \neq 0.$$

This is because the 2nd statement is the contrapositive of the statement $\langle \bar{x}, \bar{x} \rangle = 0 \Rightarrow \bar{x} = \bar{0}$, so they are logically equivalent (note that the contrapositive of

$$\langle \bar{x}, \bar{x} \rangle = 0 \quad \Rightarrow \quad \bar{x} = \bar{0}$$

is

$$\mathrm{NOT}\big(\bar{x} = \bar{0}\big) \quad \Rightarrow \quad \mathrm{NOT}\big(\langle \bar{x}, \bar{x} \rangle = 0\big),$$

which can be rewritten more simply as above).

To prove the 1st statement, we note that, if $\bar{x} = \bar{0}$, then

$$\langle \bar{x}, \bar{x} \rangle = \sum_{i=1}^{n} x_i^2 = \sum_{i=1}^{n} 0^2 = n \cdot 0 = 0.$$

To prove the 2nd statement, let us consider $\bar{x} \in \mathbb{R}^n$, $\bar{x} \neq 0$. Then necessarily there is an index i_0 such that $x_{i_0} \neq 0$, which implies that $x_{i_0}^2 > 0$. By the commutativity and associativity of addition, we have

$$\langle \bar{x}, \bar{x} \rangle = \sum_{i=1}^{n} x_i^2 = x_{i_0}^2 + \sum_{\substack{1 \leqslant i \leqslant n \\ i \neq i_0}} x_i^2.$$

Moreover, exactly as in part (i), we have that $\displaystyle\sum_{\substack{1 \leqslant i \leqslant n \\ i \neq i_0}} x_i^2 \geqslant 0$.

Therefore,

$$x_{i_0}^2 + \sum_{\substack{1 \leqslant i \leqslant n \\ i \neq i_0}} x_i^2 \geqslant x_{i_0}^2 + 0 = x_{i_0}^2 > 0.$$

We conclude that $\langle \bar{x}, \bar{x} \rangle > 0$, and hence that it is non-zero.

Problem 7. (i) Consider a vector $\bar{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-1} \\ x_n \end{pmatrix} \in \mathbb{R}^n$. Then we can write $\bar{x}$ as the sum of n vectors as follows:

$$\begin{aligned}
\bar{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-1} \\ x_n \end{pmatrix} &= \begin{pmatrix} x_1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ x_2 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 \\ 0 \\ \vdots \\ x_{n-1} \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ x_n \end{pmatrix} \\
&= x_1 \cdot \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \cdots + x_{n-1} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix} + x_n \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \\
&= x_1 \cdot \bar{e}_1 + x_2 \cdot \bar{e}_2 + \cdots + x_{n-1} \cdot \bar{e}_{n-1} + x_n \cdot \bar{e}_n.
\end{aligned}$$

This shows that $\bar{x}$ is a linear combination of the standard basis vectors in $\mathbb{R}^n$.

(ii) Let us denote by $(\bar{e}_i)_l$ the l-th component of $\bar{e}_i$ (given how the standard basis vectors were defined, we have $(\bar{e}_i)_i = 1$ and $(\bar{e}_i)_l = 0$ when $l \neq i$).

Therefore,

$$\|\bar{e}_i\|^2 = \langle \bar{e}_i, \bar{e}_i \rangle = \sum_{l=1}^{n} (\bar{e}_i)_l^2 = (\bar{e}_i)_i^2 + \sum_{\substack{1 \leqslant l \leqslant n \\ l \neq i}} (\bar{e}_i)_l^2 = 1 + \sum_{\substack{1 \leqslant l \leqslant n \\ l \neq i}} 0 = 1,$$

which shows that $\|\bar{e}_i\| = 1$.

Similarly, we check that, when $i \neq j$,

$$\begin{aligned}
\langle \bar{e}_i, \bar{e}_j \rangle = \sum_{l=1}^{n} (\bar{e}_i)_l \cdot (\bar{e}_j)_l &= (\bar{e}_i)_i \cdot (\bar{e}_j)_i + (\bar{e}_i)_j \cdot (\bar{e}_j)_j + \sum_{\substack{1 \leqslant l \leqslant n \\ l \notin \{i,j\}}} (\bar{e}_i)_l \cdot (\bar{e}_j)_l \\
&= 1 \cdot 0 + 0 \cdot 1 + \sum_{\substack{1 \leqslant l \leqslant n \\ l \notin \{i,j\}}} 0 = 0.
\end{aligned}$$