Math 127
Homework Problem Set 1

Problem 1. (i) For every non-zero element of $\mathbb{Z}_{11}$, find its multiplicative inverse.
(ii) Show that $\mathbb{Z}_{18}$ is not a field. Same for $\mathbb{Z}_{57}$.

Problem 2. Exactly two of the following structures are fields.

1. The set $\mathbb{Z}_3^2$, that is, the set of ordered pairs (a, b) with both a and b in $\mathbb{Z}_3$, with coordinate-wise addition, and multiplication given by $(a, b)(c, d) = (ac - bd, ad + bc)$.
2. The set $\mathbb{Z}_5^2$ with addition and multiplication defined in the same way as above.
3. The set of numbers of the form $a + \sqrt{5}\, b$ where $a, b \in \mathbb{Q}$, with usual addition and multiplication (note that all these numbers are real numbers, so we can add or multiply any two of them in the standard way; first check though that the result of these operations is again a number of the given form).
4. The set $\mathbb{Z}_3 \times \mathbb{Z}_7$, that is, the set of ordered pairs (r, s) with $r \in \mathbb{Z}_3$ and $s \in \mathbb{Z}_7$, with coordinate-wise addition and multiplication.

(i) Determine which two are fields, and (ii) verify that the other two are commutative rings too (but not fields). Justify your answer fully.
[*Hint.* You may wish to find first what the identity element in each case should be. Also, check carefully the associativity property and the distributive law.]

Problem 3. Let $\mathcal{R}$ be a commutative ring.
(i) Prove that $0 \cdot x = 0$ for all $x \in \mathcal{R}$. [*Hint.* Recall the proof of the corresponding fact for fields.]
(ii) Suppose x, y are elements of $\mathcal{R}$ such that $xy = 0$ and $x \neq 0$. Show that y is not invertible (that is, it does not have a multiplicative inverse).

Problem 4. For each of the following lines or planes, which are defined via a linear equation (or a pair of linear equations), give an equivalent vector equation.

(i) The line $\ell_1 = \big\{(x, y) \in \mathbb{R}^2 \mid 3x + 4y + 2 = 0\big\}$.

(ii) The line ℓ_2 in $\mathbb{R}^3$ defined by the system of linear equations

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

(iii) The plane $\mathcal{P}_1 = \big\{(x,y,z) \in \mathbb{R}^3 \mid 2y-x-z=0\big\}$.

(iv) The plane $\mathcal{P}_2 = \big\{(x,y,z) \in \mathbb{R}^3 \mid x-3y+z+6=0\big\}$.

Problem 5. (i) Prove that $\langle \bar{u}, \bar{v}+\bar{w}\rangle = \langle \bar{u}, \bar{v}\rangle + \langle \bar{u}, \bar{w}\rangle$ for every three vectors $\bar{u}, \bar{v}$ and $\bar{w}$ in $\mathbb{R}^n$.
(ii) Suppose $\bar{u}_1, \bar{v}_1$ and $\bar{w}_1$ are three vectors in $\mathbb{R}^n$ such that $\langle \bar{u}_1, \bar{v}_1\rangle \cdot \langle \bar{u}_1, \bar{w}_1\rangle \neq 0$. Show that we can find **non-zero** $t, s \in \mathbb{R}$ so that the vector $t\bar{v}_1 + s\bar{w}_1$ is orthogonal to $\bar{u}_1$.

Problem 6. Let $\bar{u} = \begin{pmatrix} 1 \\ -2 \\ 3 \\ 0 \\ 1 \end{pmatrix}$, $\bar{v} = \begin{pmatrix} -2 \\ 2 \\ 1 \\ -1 \\ 1 \end{pmatrix}$, $\bar{w} = \begin{pmatrix} 1 \\ 0 \\ -5 \\ 2 \end{pmatrix}$ and $\bar{z} = \begin{pmatrix} -8 \\ 0 \\ 5 \\ 0 \end{pmatrix}$
(where the coordinates are real numbers).
(i) Compute the following expressions if they are well-defined:
$2\bar{u}+15\bar{v}$, $\langle \bar{u}, \bar{v}\rangle$, $2\bar{u}+3\bar{v}+4\bar{w}$, $\langle \bar{u}, \bar{v}\rangle + \bar{v}$, $\langle \bar{u}+\bar{v}, \bar{z}\rangle$, $\big\langle \langle \bar{u}+\bar{v}, \bar{v}\rangle \bar{u}, \bar{u}-\bar{v}\big\rangle$, $\big\langle \langle \bar{u}+\bar{v}, \bar{u}\rangle, \bar{w}\big\rangle$, $\Big(\sum_{k=1}^{3} \langle \bar{u}+k\bar{v}, \bar{u}\rangle \bar{w}\Big) + 30\bar{z}$.
(ii) Among all the vectors you found or the ones that are given in the statement, are any two orthogonal to each other? Find all such pairs (if any exist).

Math 127
Suggested solutions to Homework Set 1

Problem 1. (i) We need to look at the multiplication table of $\mathbb{Z}_{11}$:

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[0]											
[1]											
[2]											
[3]											
[4]											
[5]											
[6]											
[7]											
[8]											
[9]											
[10]											

We already know what its first row looks like, but we ignore this as we only care about non-zero elements. We also don't need to fill out the second row, as we already know that $[1]^{-1} = [1]$.

We move on to the third row (the row corresponding to [2]):

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[2]	[0]	[2]	[4]	[6]	[8]	[10]	[12]	[14]	[16]	[18]	[20]

which is the same as

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[2]	[0]	[2]	[4]	[6]	[8]	[10]	[1]	[3]	[5]	[7]	[9]

We thus see that $[2]^{-1} = [6]$, which also gives us that $[6]^{-1} = [2]$.

Similarly, we complete the rows corresponding to [3] and to [5]:

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[2]	[0]	[2]	[4]	[6]	[8]	[10]	[1]	[3]	[5]	[7]	[9]
[3]	[0]	[3]	[6]	[9]	[1]	[4]	[7]	[10]	[2]	[5]	[8]
[4]											
[5]	[0]	[5]	[10]	[4]	[9]	[3]	[8]	[2]	[7]	[1]	[6]

which gives that $[3]^{-1} = [4]$ and that $[5]^{-1} = [9]$. This also shows that $[4]^{-1} = [3]$ (which is why we didn't have to fill out the row corresponding to $[4]$ after all), and analogously $[9]^{-1} = [5]$.

We now complete the row corresponding to $[7]$:

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[9]$	$[10]$
$[2]$	$[0]$	$[2]$	$[4]$	$[6]$	$[8]$	$[10]$	$[1]$	$[3]$	$[5]$	$[7]$	$[9]$
$[3]$	$[0]$	$[3]$	$[6]$	$[9]$	$[1]$	$[4]$	$[7]$	$[10]$	$[2]$	$[5]$	$[8]$
$[4]$											
$[5]$	$[0]$	$[5]$	$[10]$	$[4]$	$[9]$	$[3]$	$[8]$	$[2]$	$[7]$	$[1]$	$[6]$
$[7]$	$[0]$	$[7]$	$[3]$	$[10]$	$[6]$	$[2]$	$[9]$	$[5]$	$[1]$	$[8]$	$[4]$

which gives that $[7]^{-1} = [8]$ and $[8]^{-1} = [7]$.

The only remaining non-zero element is $[10]$, which necessarily will be its own multiplicative inverse too; we can verify this by computing $10 \cdot 10 = 100 = 11 \cdot 9 + 1$, which shows that $[10] \cdot [10] = [10 \cdot 10] = [1]$.

What we found is summarised in the following table:

x	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[9]$	$[10]$
x^{-1}	$[1]$	$[6]$	$[4]$	$[3]$	$[9]$	$[2]$	$[8]$	$[7]$	$[5]$	$[10]$

.

Alternative solution to (i) using Bézout's identity: Just as an example, we will confirm that $[7]^{-1} = [8]$ using an alternative method which relies on Bézout's identity. This method may be more helpful to use if we are asked the same question in a different $\mathbb{Z}_p$ with p really large: e.g. if we are asked to find the multiplicative inverse of 7 in $\mathbb{Z}_{1031}$ (note that 1031 is the 173-th prime number, as we can find with a simple internet search).

We recall that $\gcd(7, 11) = 1$ and that Bézout's identity tells us that we can find $t, s \in \mathbb{Z}$ such that

$$7t + 11s = 1 \tag{1}$$

(observe that this is an identity involving integers). This would imply that, in $\mathbb{Z}_{11}$, we have

$$\begin{aligned} [7t + 11s] = [1] \;&\Rightarrow\; [7t] = [7t] + [0] = [7t] + [11s] = [1] \\ &\Rightarrow\; [7] \cdot [t] = [1] \;\Rightarrow\; [7]^{-1} = [t]. \end{aligned}$$

Therefore, to find the multiplicative inverse of $[7]$ in $\mathbb{Z}_{11}$, it suffices to find t and s such that (1) will hold. We can do so by consecutive applications of

Euclidean division:

$$\begin{aligned} 11 &= 7 \cdot 1 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1. \end{aligned}$$

Once we end up with a line where the remainder is equal to $1 = \gcd(7, 11)$, we start reversing the process, and writing each remainder as a linear combination of the dividend and the divisor:

$$\begin{aligned} 1 = 4 - 3 \cdot 1 = 4 - (7 - 4 \cdot 1) \cdot 1 &= 4 \cdot 2 - 7 \cdot 1 \\ &= (11 - 7 \cdot 1) \cdot 2 - 7 \cdot 1 = 11 \cdot 2 - 7 \cdot 3 \\ &= 11 \cdot 2 + 7 \cdot (-3). \end{aligned}$$

Therefore (1) holds with $t = -3$ and $s = 2$. By the discussion above, this implies that $[7]^{-1} = [-3] = [8]$.

(ii) We recall the following Proposition that we proved in class:

Let $\mathbb{F}$ be a field, and let $x, y \in \mathbb{F}$. Then, if $x \cdot y = 0$, we must have $x = 0$ or $y = 0$ (or both).

Therefore, if we find two elements x, y of $\mathbb{Z}_{18}$, both of them non-zero, such that $x \cdot y = 0$, this will imply that $\mathbb{Z}_{18}$ is not a field (because, if it were, then according to the Proposition we shouldn't be able to find such elements). We can choose $x = [3]$ and $y = [6]$. Then, both x and y are non-zero, and $x \cdot y = [3] \cdot [6] = [3 \cdot 6] = [0]$, as claimed.

We will use the same approach to prove that $\mathbb{Z}_{57}$ is not a field: we choose $x' = [6]$ and $y' = [19]$ in $\mathbb{Z}_{57}$. Then, both x' and y' are non-zero, and $x' \cdot y' = [6] \cdot [19] = [114] = [2 \cdot 57] = [0]$. This completes the proof that $\mathbb{Z}_{57}$ is not a field.

Problem 2. We check below that all four structures are commutative rings, and that structure 1 and structure 3 are also fields (whereas structures 2 and 4 are not fields); we check structures 1, 2 and 4 first, and finally structure 3.

1. We check that $\mathbb{Z}_3^2$ with the operations of addition and multiplication defined as in the statement is a field. We first confirm that the operations are well-defined: if $(a,b),(c,d) \in \mathbb{Z}_3^2$, then $a,b,c,d \in \mathbb{Z}_3$, and so $a+c \in \mathbb{Z}_3$ and $b+d \in \mathbb{Z}_3$, which shows that $(a+c, b+d) \in \mathbb{Z}_3^2$; similarly, $ac-bd \in \mathbb{Z}_3$ and $ad+bc \in \mathbb{Z}_3$, which shows that $(ac-bd, ad+bd) \in \mathbb{Z}_3^2$.

We now check the properties of these operations.

Addition is commutative: For any two elements $(a,b),(c,d) \in \mathbb{Z}_3^2$, we have that

$$(a,b)+(c,d) = (a+c, b+d) \quad \text{and} \quad (c,d)+(a,b) = (c+a, d+b).$$

But since addition in $\mathbb{Z}_3$ is commutative, it holds that $a+c = c+a$ and $b+d = d+b$. Hence $(a,b)+(c,d) = (c,d)+(a,b)$.

Addition is associative: For any three elements $(a,b),(c,d),(f,g) \in \mathbb{Z}_3^2$, we have that

$$\big((a,b)+(c,d)\big)+(f,g) = (a+c, b+d)+(f,g) = \big((a+c)+f, (b+d)+g\big)$$
$$\text{and} \quad (a,b)+\big((c,d)+(f,g)\big) = (a,b)+(c+f, d+g) = \big(a+(c+f), b+(d+g)\big).$$

Since addition in $\mathbb{Z}_3$ is associative, it holds that $(a+c)+f = a+(c+f)$ and $(b+d)+g = b+(d+g)$. Therefore, $\big((a,b)+(c,d)\big)+(f,g) = (a,b)+\big((c,d)+(f,g)\big)$.

Neutral element: We first need to determine which element could be the neutral element of addition: we are looking for an element $(c,d) \in \mathbb{Z}_3^2$ such that, for every $(a,b) \in \mathbb{Z}_3^2$, we will have $(c,d)+(a,b) = (a,b)$. But $(c,d)+(a,b) = (c+a, d+b)$, so we need to have $c+a = a$ and $d+b = b$. This is satisfied if $c = 0$ and $d = 0$. We can now verify directly that $(0,0)+(a,b) = (a,b)$ for every $(a,b) \in \mathbb{Z}_3^2$ by noting that $(0,0)+(a,b) = (0+a, 0+b)$.

Additive inverses: For every $(a,b) \in \mathbb{Z}_3^2$ we need to find an element (c,d) such that $(a,b)+(c,d) = (0,0)$. We fix an element (a,b) and note that $(a,b)+(c,d) = (a+c, b+d)$, so in order to have $a+c = 0$ and $b+d = 0$ it must hold that $c = -a$ (the additive inverse of a in $\mathbb{Z}_3$) and $d = -b$. We check that indeed $(a,b)+(-a,-b) = (0,0)$.

Multiplication is commutative: For any two elements $(a,b),(c,d) \in \mathbb{Z}_3^2$, we have that

$$(a,b)(c,d) = (ac-bd, ad+bc) \quad \text{and} \quad (c,d)(a,b) = (ca-db, cb+da).$$

Since both addition and multiplication in $\mathbb{Z}_3$ are commutative, it holds that $ac-bd = ca-db$ and $ad+bc = bc+ad = cb+da$. Hence $(a,b)(c,d) = (c,d)(a,b)$.

Multiplication is associative: For any three elements $(a,b),(c,d),(f,g) \in \mathbb{Z}_3^2$, we have that

$$\big((a,b)(c,d)\big)(f,g) = (ac-bd, ad+bc)(f,g)$$
$$= \big((ac-bd)f - (ad+bc)g, (ac-bd)g + (ad+bc)f\big)$$

$$\text{and} \quad (a,b)\big((c,d)(f,g)\big) = (a,b)(cf-dg, cg+df)$$
$$= \big(a(cf-dg) - b(cg+df), a(cg+df) + b(cf-dg)\big).$$

Using the facts that addition in $\mathbb{Z}_3$ is commutative and associative, and that multiplication in $\mathbb{Z}_3$ is associative and also distributes over addition, we can write

$$(ac-bd)f - (ad+bc)g = (ac)f - (bd)f - (ad)g - (bc)g$$
$$= a(cf) - a(dg) - b(cg) - b(df) = a(cf-dg) - b(cg+df),$$

and similarly $(ac-bd)g + (ad+bc)f = (ac)g - (bd)g + (ad)f + (bc)f$
$$= a(cg) + a(df) + b(cf) + b(-dg) = a(cg+df) + b(cf-dg).$$

Therefore, $\big((a,b)(c,d)\big)(f,g) = (a,b)\big((c,d)(f,g)\big)$.

Identity element: We first need to determine which element could be the identity element: we are looking for an element $(c,d) \in \mathbb{Z}_3^2$ such that, for every $(a,b) \in \mathbb{Z}_3^2$, we will have $(c,d)(a,b) = (a,b)$. But $(c,d)(a,b) = (a,b)(c,d) = (ac-bd, ad+bc)$, so we need to have

$$\left\{ \begin{array}{l} ac-bd = a \\ ad+bc = b \end{array} \right\}.$$

To determine values for c and d it is easier to fix some specific non-zero element (a,b) initially, e.g. $(a,b) = (2,0)$. Then we need to have $2c = 2$ and $2d = 0$ for some $c,d \in \mathbb{Z}_3$, which implies a unique solution for c and d: $(c,d) = (1,0)$.

We can now verify directly that $(1,0)(a,b) = (a,b)$ for every $(a,b) \in \mathbb{Z}_3^2$ by noting that $(1,0)(a,b) = (1a-0b, 1b+0a) = (1a, 1b)$.

Distributive law: For any three elements $(a,b),(c,d),(f,g) \in \mathbb{Z}_3^2$, we have that

$$\big((a,b)+(c,d)\big)(f,g) = (a+c,b+d)(f,g) = \big((a+c)f-(b+d)g,(a+c)g+(b+d)f\big)$$

$$\begin{aligned}\text{while } \ (a,b)(f,g)+(c,d)(f,g) &= (af-bg,ag+bf)+(cf-dg,cg+df)\\ &= \big((af-bg)+(cf-dg),(ag+bf)+(cg+df)\big).\end{aligned}$$

Using the facts that addition in $\mathbb{Z}_3$ is commutative and associative, and that multiplication in $\mathbb{Z}_3$ is associative and also distributes over addition, we can write

$$(a+c)f-(b+d)g = (af+cf)-(bg+dg) = (af-bg)+(cf-dg),$$
$$\text{and } \ (a+c)g+(b+d)f = (ag+cg)+(bf+df) = (ag+bf)+(cg+df).$$

Therefore, $\big((a,b)+(c,d)\big)(f,g) = (a,b)(f,g)+(c,d)(f,g)$.

We can conclude that $\mathbb{Z}_3^2$ with the given operations is a commutative ring. It remains to check the existence of a multiplicative inverse for any non-zero element of this structure.

Multiplicative inverses: For every non-zero element $(a,b) \in \mathbb{Z}_3^2$ we need to find an element (c,d) such that $(a,b)(c,d) = (1,0)$. We fix an element (a,b) and note that $(a,b)(c,d) = (ac-bd, ad+bc)$, so we need to have

$$\left\{ \begin{array}{l} ac-bd = 1 \\ ad+bc = 0 \end{array} \right\}.$$

To solve this system, we consider three cases, with the first one being the most difficult:

Case 1: $a \neq 0$, $b \neq 0$. In this case, we can multiply both sides of the second linear equation by ba^{-1} to get an equivalent linear system:

$$\left\{ \begin{array}{l} ac-bd = 1 \\ ad+bc = 0 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} ac-bd = 1 \\ bd+a^{-1}b^2c = 0 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} (a+a^{-1}b^2)c = 1 \\ bd+a^{-1}b^2c = 0 \end{array} \right\}.$$

We could now solve for c in the first equation if we knew that $a+a^{-1}b^2$ is not zero: we can write

$$a+a^{-1}b^2 = a^{-1}a^2+a^{-1}b^2 = a^{-1}(a^2+b^2),$$

so it suffices (why?) to check that $a^2+b^2 \neq 0$. But in the case we are analysing here, a is a non-zero element of $\mathbb{Z}_3$, so it is either

1 or 2, and hence $a^2 = 1$ (since $1^1 = 1 = 2^2$ in $\mathbb{Z}^3$); for the same reason $b^2 = 1$, therefore $a^2 + b^2 = 2 \neq 0$. We can thus continue solving the linear system above:

$$\left\{ \begin{array}{c} c = (a + a^{-1}b^2)^{-1} \\ bd + a^{-1}b^2c = 0 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{c} c = (a + a^{-1}b^2)^{-1} \\ bd = -a^{-1}b^2c \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{c} c = (a + a^{-1}b^2)^{-1} \\ d = -a^{-1}b(a + a^{-1}b^2)^{-1} \end{array} \right\}.$$

We conclude that in the case that $a \neq 0$ and $b \neq 0$, the element (a, b) of $\mathbb{Z}_3^2$ has a multiplicative inverse.

Case 2: $a = 0$. In this case necessarily $b \neq 0$ (given that $(a, b) \neq (0, 0)$). Again, we need to find a solution to the system of linear equations $ac - bd = 1$ and $ad + bc = 0$, which now simplify to

$$\left\{ \begin{array}{c} -bd = 1 \\ bc = 0 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{c} d = -b^{-1} \\ c = 0 \end{array} \right\}.$$

Therefore in this case as well the element (a, b) has a multiplicative inverse.

Case 3: $b = 0$. This case is completely analogous to the previous one: in this case necessarily $a \neq 0$. The linear system we need to solve this time is

$$\left\{ \begin{array}{c} ac = 1 \\ ad = 0 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{c} c = a^{-1} \\ d = 0 \end{array} \right\}.$$

Therefore, in this final case too the system has a solution and thus the element (a, b) has a multiplicative inverse.

We finally observe that these three cases cover all possibilities for what values a and b can take, therefore we have checked that every non-zero (a, b) in $\mathbb{Z}_3^2$ has a multiplicative inverse.

2. We check that $\mathbb{Z}_5^2$ with the operations of addition and multiplication defined as in the statement is a commutative ring but not a field. We first confirm that the operations are well-defined: if $(a, b), (c, d) \in \mathbb{Z}_5^2$, then $a, b, c, d \in \mathbb{Z}_5$, and so $a + c \in \mathbb{Z}_5$ and $b + d \in \mathbb{Z}_5$, which shows that $(a + c, b + d) \in \mathbb{Z}_5^2$; similarly, $ac - bd \in \mathbb{Z}_5$ and $ad + bc \in \mathbb{Z}_5$, which shows that $(ac - bd, ad + bd) \in \mathbb{Z}_5^2$.

We now check the properties of these operations.

Addition is commutative: We can repeat the argument above for the corresponding property, except that now we will use the fact that addition in $\mathbb{Z}_5$ is commutative.

Addition is associative: We can repeat the argument above for the corresponding property, except that now we will use the fact that addition in $\mathbb{Z}_5$ is associative.

Neutral element: We can check that $(0,0)+(a,b) = (a,b)$ for every $(a,b) \in \mathbb{Z}_5^2$ by noting that $(0,0) + (a,b) = (0+a, 0+b) = (a,b)$.

Additive inverses: We can check that, for every $(a,b) \in \mathbb{Z}_5^2$, $(a,b)+(-a,-b) = (0,0)$ (where $-a$ is the additive inverse of a in $\mathbb{Z}_5$ and $-b$ the additive inverse of b) by noting that $(a,b)+(-a,-b) = (a+(-a), b+(-b)) = (0,0)$.

Multiplication is commutative: We can repeat the argument above for the corresponding property, except that now we will use the fact that addition and multiplication in $\mathbb{Z}_5$ are commutative.

Multiplication is associative: We can repeat the argument above for the corresponding property, except that now we will use the fact that addition in $\mathbb{Z}_5$ is commutative and associative, while multiplication in $\mathbb{Z}_5$ is associative and also distributes over addition.

Identity element: We can check that $(1,0)(a,b) = (a,b)$ for every $(a,b) \in \mathbb{Z}_5^2$ by noting that $(1,0)(a,b) = (1a - 0b, 1b + 0a) = (1a, 1b) = (a,b)$.

Distributive law: We can repeat the argument above for the corresponding property, except that now we will use the fact that addition in $\mathbb{Z}_5$ is commutative and associative, while multiplication in $\mathbb{Z}_5$ is associative and also distributes over addition.

We can conclude that $\mathbb{Z}_5^2$ with the given operations is a commutative ring.

It remains to check that it is not a field. We could try to adapt the argument for showing the existence of multiplicative inverses which we have above and try to see what needs to be different. It is not hard to confirm that Cases 2 and 3 would work in the same way. However in Case 1, where $a \neq 0$ and $b \neq 0$, in order to solve the system

$$\left\{ \begin{array}{l} ac - bd = 1 \\ ad + bc = 0 \end{array} \right\},$$

we need at some step to ensure that the element $a^2 + b^2 \neq 0$. This is not always true in $\mathbb{Z}_5$ as we can see for instance if $a = 2$ and $b = 1$: $a^2 + b^2 = 2^2 + 1^2 = 4 + 1 = 0$. This should make us suspect that the element $(2,1)$ is not invertible.

We can verify this by observing that $(2,1)(1,2) = (0,0)$ (given that $(2,1)(1,2) = (2 \cdot 1 - 1 \cdot 2,\ 2^2 + 1^2)$). But $(1,2) \neq 0$ and according to

HW1, Pb3(ii), if $yx = 0$ and $x \neq 0$ then y is not invertible (here we choose $y = (2, 1)$ and $x = (1, 2)$). (*Alternatively, we could recall a proposition we proved in class, that in every field* $\mathbb{F}$*, if* $x, y \in \mathbb{F}$ *satisfy* $xy = 0$ *then* $x = 0$ *or* $y = 0$*; given that in* $\mathbb{Z}_5^2$ *with the given operations* $(2, 1)(1, 2) = (0, 0)$ *with both* $(2, 1)$ *and* $(1, 2)$ *being non-zero, we see that this structure cannot be a field.*)

4. We check that $\mathbb{Z}_3 \times \mathbb{Z}_7$ with the operations of addition and multiplication defined as in the statement is a commutative ring but not a field. We first confirm that the operations are well-defined: if $(a, b), (c, d) \in \mathbb{Z}_3 \times \mathbb{Z}_7$, then $a, c \in \mathbb{Z}_3$ and $b, d \in \mathbb{Z}_7$, and so $a + c \in \mathbb{Z}_3$ and $b + d \in \mathbb{Z}_7$, which shows that $(a + c, b + d) \in \mathbb{Z}_3 \times \mathbb{Z}_7$; similarly, $ac \in \mathbb{Z}_3$ and $bd \in \mathbb{Z}_7$, which shows that $(ac, bd) \in \mathbb{Z}_3 \times \mathbb{Z}_7$.

We now check the properties of these operations.

Addition is commutative: We can repeat the argument above for the corresponding property, except that now we will use the fact that both addition in $\mathbb{Z}_3$ and addition in $\mathbb{Z}_7$ are commutative.

Addition is associative: We can repeat the argument above for the corresponding property, except that now we will use the fact that both addition in $\mathbb{Z}_3$ and addition in $\mathbb{Z}_7$ are associative.

Neutral element: We can check that $(0, 0)+(a, b) = (a, b)$ for every $(a, b) \in \mathbb{Z}_3 \times \mathbb{Z}_7$ by noting that $(0, 0) + (a, b) = (0 + a, 0 + b) = (a, b)$ (note that here the first coordinate of $(0, 0)$ is the neutral element of addition in $\mathbb{Z}_3$, while the second element is the neutral element in $\mathbb{Z}_7$).

Additive inverses: We can check that, for every $(a, b) \in \mathbb{Z}_3 \times \mathbb{Z}_7$, $(a, b) + (-a, -b) = (0, 0)$ (where $-a$ is the additive inverse of a in $\mathbb{Z}_3$ and $-b$ the additive inverse of b in $\mathbb{Z}_7$) by noting that $(a, b) + (-a, -b) = (a + (-a), b + (-b)) = (0, 0)$.

Multiplication is commutative: For any two elements $(a, b), (c, d) \in \mathbb{Z}_3 \times \mathbb{Z}_7$, we have that

$$(a, b)(c, d) = (ac, bd) \quad \text{and} \quad (c, d)(a, b) = (ca, db).$$

But since multiplication in $\mathbb{Z}_3$ is commutative, it holds that $ac = ca$; analogously, since multiplication in $\mathbb{Z}_7$ is commutative, we have that $bd = db$. Hence $(a, b)(c, d) = (c, d)(a, b)$.

Multiplication is associative: For any three elements $(a,b),(c,d),(f,g) \in \mathbb{Z}_3 \times \mathbb{Z}_7$, we have that

$$\begin{aligned} \big((a,b)(c,d)\big)(f,g) &= (ac,bd)(f,g) = \big((ac)f,(bd)g\big) \\ \text{and}\quad (a,b)\big((c,d)(f,g)\big) &= (a,b)(cf,dg) = \big(a(cf),b(dg)\big). \end{aligned}$$

Since addition in $\mathbb{Z}_3$ is associative, it holds that $(ac)f = a(cf)$; similarly, since addition in $\mathbb{Z}_7$ is associative, it holds that $(bd)g = b(dg)$. Therefore, $\big((a,b)(c,d)\big)(f,g) = (a,b)\big((c,d)(f,g)\big)$.

Identity element: We first need to determine which element could be the identity element (that is, the neutral element of multiplication): we are looking for an element $(c,d) \in \mathbb{Z}_3 \times \mathbb{Z}_7$ such that, for every $(a,b) \in \mathbb{Z}_3 \times \mathbb{Z}_7$, we will have $(c,d)(a,b) = (a,b)$. But $(c,d)(a,b) = (ca,db)$, so we need to have $ca = a$ and $db = b$. This is satisfied if $c = 1$ (the identity element in $\mathbb{Z}_3$) and $d = 1$ (the identity element in $\mathbb{Z}_7$). We can now verify directly that $(1,1)(a,b) = (a,b)$ for every $(a,b) \in \mathbb{Z}_3 \times \mathbb{Z}_7$ by noting that $(1,1)(a,b) = (1a,1b)$.

Distributive law: For any three elements $(a,b),(c,d),(f,g) \in \mathbb{Z}_3 \times \mathbb{Z}_7$, we have that

$$\begin{aligned} \big((a,b)+(c,d)\big)(f,g) &= (a+c,b+d)(f,g) = \big((a+c)f,(b+d)g\big) \\ \text{and}\quad \big((a,b)(f,g)\big) + \big((c,d)(f,g)\big) &= (af,bg)+(cf,dg) = \big(af+cf,bg+dg\big). \end{aligned}$$

Since multiplication in $\mathbb{Z}_3$ distributes over addition, it holds that $(a+c)f = af+cf$; similarly, since multiplication in $\mathbb{Z}_7$ distributes over addition, it holds that $(b+d)g = bg+dg$. Therefore, $\big((a,b)+(c,d)\big)(f,g) = \big((a,b)(f,g)\big) + \big((c,d)(f,g)\big)$.

We can conclude that $\mathbb{Z}_3 \times \mathbb{Z}_7$ with the given operations is a commutative ring.

It remains to check that it is not a field. We observe that both $(2,0)$ and $(0,4)$ are non-zero elements, and that $(2,0)(0,4) = (0,0)$, thus $\mathbb{Z}_3 \times \mathbb{Z}_7$ cannot be a field.

3. Let us denote by $\mathbb{Q}(\sqrt{5})$ the set of real numbers of the form $a + \sqrt{5}\,b$ with $a,b \in \mathbb{Q}$. We will show that $\mathbb{Q}(\sqrt{5})$ with the usual operations of addition and multiplication of real numbers is a field (and hence a subfield of $\mathbb{R}$).

We first check that $\mathbb{Q}(\sqrt{5})$ is closed under usual addition and multiplication, that is, for any two elements $x,y \in \mathbb{Q}(\sqrt{5})$, $x+y \in \mathbb{Q}(\sqrt{5})$ and $xy \in \mathbb{Q}(\sqrt{5})$.

Indeed, we recall that, if $x, y \in \mathbb{Q}(\sqrt{5})$, then by definition of the set there are some $a, b, c, d \in \mathbb{Q}$ such that $x = a + \sqrt{5}\, b$ and $y = c + \sqrt{5}\, d$. But then

$$x + y = (a + \sqrt{5}\, b) + (c + \sqrt{5}\, d) = (a + c) + \sqrt{5}(b + d) \in \mathbb{Q}(\sqrt{5})$$

given that $a + c, b + d \in \mathbb{Q}$. Similarly,

$$xy = (a+\sqrt{5}\, b)(c+\sqrt{5}\, d) = ac+\sqrt{5}\, bc+\sqrt{5}\, ad+5bd = (ac+5bd)+\sqrt{5}\, (ad+bc) \in \mathbb{Q}(\sqrt{5})$$

given that $ac + 5bd, ad + bc \in \mathbb{Q}$.

From these, it now immediately follows that both addition and multiplication in $\mathbb{Q}(\sqrt{5})$ are commutative and associative, and also that they satisfy the distributive law. This is due to the fact that if, for instance, we know that

$$\textit{for all } x, y, z \in \mathbb{R},\ (x + y)z = xz + yz,$$

then we also have that

$$\textit{for all } x, y, z \in \mathbb{Q}(\sqrt{5}),\ (x + y)z = xz + yz$$

(given that any element of $\mathbb{Q}(\sqrt{5})$ is also an element of $\mathbb{R}$).

Moreover, $0 \in \mathbb{Q}(\sqrt{5})$ (since $0 \in \mathbb{Q}$ and we can write $0 = 0 + \sqrt{5} \cdot 0$), therefore there is a neutral element of addition in $\mathbb{Q}(\sqrt{5})$. Similarly, $1 \in \mathbb{Q}(\sqrt{5})$ (since $0, 1 \in \mathbb{Q}$ and we can write $1 = 1 + \sqrt{5} \cdot 0$), therefore there is an identity element in $\mathbb{Q}(\sqrt{5})$.

Finally, for every $x = a + \sqrt{5}\, b \in \mathbb{Q}(\sqrt{5})$ the element $-x$ (the additive inverse of x in $\mathbb{R}$) is also in $\mathbb{Q}(\sqrt{5})$, given that

$$-x = -(a + \sqrt{5}\, b) = -a - \sqrt{5}\, b = (-a) + \sqrt{5}\, (-b)$$

and $-a, -b \in \mathbb{Q}$ when a, b are rationals.

Similarly, for every non-zero $x = a + \sqrt{5}\, b \in \mathbb{Q}(\sqrt{5})$ the element $1/x$ (the multiplicative inverse of x in $\mathbb{R}$) is also in $\mathbb{Q}(\sqrt{5})$, given that

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

and both $a/(a^2 - 5b^2)$ and $(-b)/(a^2 - 5b^2)$ are in $\mathbb{Q}$ when a, b are rationals. Note that here we could multiply and divide by $a - \sqrt{5}\, b$ because this number is non-zero. Indeed, if it were equal to zero, then we would have

$$a = \sqrt{5}\, b \Rightarrow$$
$$\text{either } b = 0, \text{ and hence } a = 0 \text{ too,} \qquad \text{or } b \neq 0 \text{ and } \sqrt{5} = a/b,$$

with both conclusions here leading to contradictions (we have assumed that $(a, b) \neq (0, 0)$ since $a + \sqrt{5}\, b \neq 0$, and on the other hand $\sqrt{5}$ cannot be equal to a/b when $b \neq 0$ because $a/b \in \mathbb{Q}$). Note finally that, since both $(a + \sqrt{5}\, b)$ and $(a - \sqrt{5}\, b)$ here are non-zero, $a^2 - 5b^2 = (a + \sqrt{5}\, b)(a - \sqrt{5}\, b)$ is also non-zero, and thus the expression that we found above for $1/x$ is correct.

We conclude that $\mathbb{Q}(\sqrt{5})$ is a field.

Problem 3. (i) **Note.** *We will repeat, word for word essentially, the proof of the corresponding fact for fields, which we did in class (this is because the only properties we needed to use there are properties that a commutative ring also has).*

We have that

$$\begin{aligned} 0 \cdot x + x &= 0 \cdot x + 1 \cdot x && \text{(since there is an identity element denoted here by 1)} \\ &= (0+1) \cdot x && \text{(by the distributive law)} \\ &= 1 \cdot x && \text{(0 is the neutral element)} \\ &= x && \text{(1 is the identity element).} \end{aligned}$$

We conclude that we have $0 \cdot x + x = x$.

We now add $-x$ to both sides of this identity (we can do so because every element in $\mathcal{R}$ has an additive inverse, so we can find the additive inverse $-x$ of x):

$$\begin{aligned} 0 \cdot x &= 0 + 0 \cdot x && \text{(0 is the neutral element)} \\ &= 0 \cdot x + 0 && \text{(addition is commutative)} \\ &= 0 \cdot x + (x + (-x)) && (-x \text{ is exactly the element for which we have } x + (-x) = 0) \\ &= (0 \cdot x + x) + (-x) && \text{(addition is associative)} \\ &= x + (-x) && \text{(by the above identity)} \\ &= 0. \end{aligned}$$

(ii) We will give a proof by contradiction. Let us consider $x, y \in \mathcal{R}$ such that $xy = 0$ and $x \neq 0$. Assume towards a contradiction that y is invertible. Then we can find its multiplicative inverse y^{-1} and we can multiply by it both sides of the equality $xy = 0$; using part (i) as well we get that

$$\begin{aligned} 0 &= 0 \cdot y^{-1} \\ &= (x \cdot y) \cdot y^{-1} && \text{(by the assumption } xy = 0) \\ &= x \cdot (y \cdot y^{-1}) && \text{(multiplication is associative)} \\ &= x \cdot 1 && (y^{-1} \text{ is exactly the element for which we have } y \cdot y^{-1} = 1) \\ &= 1 \cdot x && \text{(multiplication is commutative)} \\ &= x && \text{(1 is the identity element).} \end{aligned}$$

We conclude that $x = 0$, which contradicts our assumption that $x \neq 0$. This shows that the assumption we made, that y is invertible, is incorrect.

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

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

(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) We have

$$2\bar{u} + 15\bar{v} = \begin{pmatrix} 2 \\ -4 \\ 6 \\ 0 \\ 2 \end{pmatrix} + \begin{pmatrix} -30 \\ 30 \\ 15 \\ -15 \\ 15 \end{pmatrix} = \begin{pmatrix} -28 \\ 26 \\ 21 \\ -15 \\ 17 \end{pmatrix},$$

$$\langle \bar{u}, \bar{v} \rangle = 1 \cdot (-2) + (-2) \cdot 2 + 3 \cdot 1 + 0 \cdot (-1) + 1 \cdot 1 = -2,$$

$$2\bar{u} + 3\bar{v} + 4\bar{w} \text{ is not defined}$$
(*attempting to add vectors of different dimension*),

$$\langle \bar{u}, \bar{v} \rangle + \bar{v} \text{ is not defined}$$
(*attempting to add vectors of different dimension given that the dot product* $\langle \bar{u}, \bar{v} \rangle$ *is a real number*),

$$\langle \bar{u} + \bar{v}, \bar{z} \rangle \text{ is not defined}$$
(*attempting to take dot product of vectors of different dimension*).

Moreover, to compute $\big\langle \langle \bar{u} + \bar{v}, \bar{v} \rangle \bar{u}, \bar{u} - \bar{v} \big\rangle$, we observe that

$$\bar{u} + \bar{v} = \begin{pmatrix} -1 \\ 0 \\ 4 \\ -1 \\ 2 \end{pmatrix}, \quad \langle \bar{u} + \bar{v}, \bar{v} \rangle = (-1) \cdot (-2) + 0 \cdot 2 + 4 \cdot 1 + (-1) \cdot (-1) + 2 \cdot 1 = 9,$$

$$9\bar{u} = \begin{pmatrix} 9 \\ -18 \\ 27 \\ 0 \\ 9 \end{pmatrix}, \quad \bar{u} - \bar{v} = \begin{pmatrix} 3 \\ -4 \\ 2 \\ 1 \\ 0 \end{pmatrix},$$

$$\text{and finally } \big\langle \langle \bar{u} + \bar{v}, \bar{v} \rangle \bar{u}, \bar{u} - \bar{v} \big\rangle = \big\langle 9\bar{u}, \bar{u} - \bar{v} \big\rangle =$$
$$9 \cdot 3 + (-18) \cdot (-4) + 27 \cdot 2 + 0 \cdot 1 + 9 \cdot 0 = 153.$$

Finally, to compute $\big(\sum_{k=1}^{3} \langle \bar{u} + k\bar{v}, \bar{u} \rangle \bar{w}\big) + 30\bar{z}$, we first need to compute $\langle \bar{u} + k\bar{v}, \bar{u} \rangle$ for every $k = 1, 2, 3$. Alternatively, we could first observe that

$$\sum_{k=1}^{3} \langle \bar{u} + k\bar{v}, \bar{u} \rangle \bar{w} = \left(\sum_{k=1}^{3} \langle \bar{u} + k\bar{v}, \bar{u} \rangle \right) \bar{w}$$
$$= \left(\sum_{k=1}^{3} \big(\langle \bar{u}, \bar{u} \rangle + k \langle \bar{v}, \bar{u} \rangle \big) \right) \bar{w} = \big(3\langle \bar{u}, \bar{u} \rangle + (1 + 2 + 3) \langle \bar{v}, \bar{u} \rangle \big) \bar{w}.$$

Therefore, we need to find $\langle \bar{u}, \bar{u} \rangle$ and $\langle \bar{v}, \bar{u} \rangle$:

$$\langle \bar{u}, \bar{u} \rangle = 1^2 + (-2)^2 + 3^2 + 0^2 + 1^2 = 15,$$
$$\langle \bar{v}, \bar{u} \rangle = (-2) \cdot 1 + 2 \cdot (-2) + 1 \cdot 3 + (-1) \cdot 0 + 1 \cdot 1 = -2.$$

We obtain that

$$\left(\sum_{k=1}^{3}\langle\bar{u}+k\bar{v},\bar{u}\rangle\bar{w}\right)+30\bar{z}=\big(3\cdot 15+6\cdot(-2)\big)\bar{w}+30\bar{z}$$
$$=33\bar{w}+30\bar{z}=\begin{pmatrix}33\\0\\-165\\66\end{pmatrix}+\begin{pmatrix}-240\\0\\150\\0\end{pmatrix}=\begin{pmatrix}-207\\0\\-15\\66\end{pmatrix}.$$

(ii) We already saw in the previous part that $\langle\bar{v},\bar{u}\rangle=-2\neq 0$. We also compute:

$$\langle\bar{u},2\bar{u}+15\bar{v}\rangle=\langle\bar{u},2\bar{u}\rangle+\langle\bar{u},+15\bar{v}\rangle=2\langle\bar{u},\bar{u}\rangle+15\langle\bar{u},\bar{v}\rangle=2\cdot 15+15\cdot(-2)=0,$$

where we used properties of the dot product and the dot products $\langle\bar{u},\bar{u}\rangle$ and $\langle\bar{v},\bar{u}\rangle$ that we found before. Similarly,

$$\langle\bar{v},2\bar{u}+15\bar{v}\rangle=\langle\bar{v},2\bar{u}\rangle+\langle\bar{v},+15\bar{v}\rangle=2\langle\bar{v},\bar{u}\rangle+15\langle\bar{v},\bar{v}\rangle=2\cdot(-2)+15\cdot 11=161,$$

where we used that $\langle\bar{v},\bar{v}\rangle=11$.

We conclude that among the 5-dimensional vectors which we found or were given in the statement, there is only one pair of orthogonal vectors, the pair $\bar{u}$ and $2\bar{u}+15\bar{v}$.

Similarly, we find that

$$\langle\bar{w},\bar{z}\rangle=-33,$$

$$\text{while }\left\langle\left(\sum_{k=1}^{3}\langle\bar{u}+k\bar{v},\bar{u}\rangle\bar{w}\right)+30\bar{z},\bar{w}\right\rangle=\langle 33\bar{w}+30\bar{z},\bar{w}\rangle$$
$$=33\langle\bar{w},\bar{w}\rangle+30\langle\bar{z},\bar{w}\rangle=33\cdot 30+30\cdot(-33)=0,$$

where we also used that $\langle\bar{w},\bar{w}\rangle=30$. Finally,

$$\left\langle\left(\sum_{k=1}^{3}\langle\bar{u}+k\bar{v},\bar{u}\rangle\bar{w}\right)+30\bar{z},\bar{z}\right\rangle=\langle 33\bar{w}+30\bar{z},\bar{z}\rangle$$
$$=33\langle\bar{w},\bar{z}\rangle+30\langle\bar{z},\bar{z}\rangle=33\cdot(-33)+30\cdot 89=-1089+2670\neq 0,$$

where we also used that $\langle\bar{z},\bar{z}\rangle=(-8)^2+5^2=89$. We conclude that among the 4-dimensional vectors, there is only one pair of orthogonal vectors, the pair $\bar{w}$ and $\big(\sum_{k=1}^{3}\langle\bar{u}+k\bar{v},\bar{u}\rangle\bar{w}\big)+30\bar{z}$.

Math 127
Homework Problem Set 2

Problem 1. Let $n > 1$ be a natural number. Consider the set $\mathbb{R}^n$ of all n-tuples $\bar{x} = (x_1, x_2, \ldots, x_n)$ all of whose components are real numbers.

Define the operations of addition and of multiplication of two n-tuples by doing them coordinate-wise. In other words,

$$(\bar{x}, \bar{y}) \in \mathbb{R}^n \times \mathbb{R}^n \quad \mapsto \quad \bar{x} + \bar{y} \stackrel{\text{def}}{=} (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n) \in \mathbb{R}^n,$$
$$(\bar{x}, \bar{y}) \in \mathbb{R}^n \times \mathbb{R}^n \quad \mapsto \quad \bar{x} \cdot \bar{y} \stackrel{\text{def}}{=} (x_1 y_1, x_2 y_2, \ldots, x_n y_n) \in \mathbb{R}^n.$$

Show that $\mathbb{R}^n$ with these operations is a commutative ring. Show also that it is not a field.

Problem 2. (*Cancellation laws for addition and multiplication*) Let $\mathbb{F}$ be a field. For any three elements $a, b, c \in \mathbb{F}$ show the following.
(i) (*Cancellation law for addition*) If $a + b = a + c$, then $b = c$.
(ii) (*Cancellation law for multiplication*) If $ab = ac$ and moreover $a \neq 0$, then $b = c$.

If you like Sudoku-type puzzles, then the next problem is precisely for you! Otherwise.... well, it's just one more homework problem.

Problem 3. There is essentially only one field $\mathbb{F}_4$ with exactly 4 elements. Note that among these elements we must have the neutral element 0 of addition, as well as the identity element 1 (the neutral element of multiplication). Note also that these have to be different elements (why?). This shows that $\mathbb{F}_4 = \{0, 1, c, d\}$.

(i) Explain how the operations of addition and multiplication must be defined (so that $\mathbb{F}_4$ becomes a field) by completing their tables, and give reasons for your choices:

$+$	0	1	c	d
0				
1				
c				
d				

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

(ii) Subsequently, verify that all the axioms of a field are satisfied.

[*Hint.* Recall that, by standard properties of fields (axioms or facts we have already derived

from the axioms), one row and one column of the table of addition are predetermined, and so are two rows and two columns of the table of multiplication (which are these rows and columns?).

Make a note also of what the cancellation laws (see Problem 2 above) should give you: in the table of addition every element of $\mathbb{F}$ should appear exactly once in each row and each column (why? convince yourselves that this claim is equivalent to the cancellation law for addition); on the other hand, in the table of multiplication something similar holds for the part of the table that corresponds only to non-zero elements. It may also help you to go back to tables of addition and multiplication that we worked out for other examples (or that you perhaps completed for problems of HW1), and confirm these claims.

Finally, even though this choice can also be justified, it may be helpful to start with the assumption that $\mathbb{Z}_2$ is a subfield of this field (what would this imply for the tables?).]

Problem 4. (i) Prove that $\langle \bar{x}, \bar{x} \rangle \geqslant 0$ for every $\bar{x} \in \mathbb{R}^n$.
(ii) Prove that $\langle \bar{x}, \bar{x} \rangle = 0 \Leftrightarrow \bar{x} = \bar{0}$. [*Note.* The symbol "$\Leftrightarrow$" means "if and only if".]

Problem 5. In $\mathbb{R}^n$ set $\bar{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}$, $\bar{e}_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix}$, $\ldots$, $\bar{e}_{n-1} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}$, $\bar{e}_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$.
These are called the *standard basis vectors* of $\mathbb{R}^n$.
For instance, in $\mathbb{R}^2$ there are two standard basis vectors: $\bar{e}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\bar{e}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, while in $\mathbb{R}^3$ there are three: $\bar{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\bar{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ and $\bar{e}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$.
(i) Show that any vector $\bar{x}$ in $\mathbb{R}^n$ is a linear combination of $\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_n$. In other words, $\mathrm{span}(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_n) = \mathbb{R}^n$.
(ii) Show that, for every $1 \leqslant i \leqslant n$, $\|\bar{e}_i\| = 1$. Moreover, show that, for every $1 \leqslant i, j \leqslant n$ with $i \neq j$, $\langle \bar{e}_i, \bar{e}_j \rangle = 0$.

Problem 6. Consider the following sets of vectors from $\mathbb{R}^5$:

$$S_1 = \left\{ \begin{pmatrix} 1 \\ -2 \\ 0 \\ 0.5 \\ 0 \end{pmatrix}, \begin{pmatrix} 6 \\ -12 \\ 7 \\ 3 \\ -7 \end{pmatrix} \right\}, \qquad S_2 = \left\{ \begin{pmatrix} 2 \\ -4 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -2 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \\ 3 \\ -0.5 \\ -3 \end{pmatrix} \right\},$$

$$S_3 = \left\{ \begin{pmatrix} 1 \\ -2 \\ -1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -1 \\ 0.5 \\ 1 \end{pmatrix} \right\}, \qquad S_4 = \left\{ \begin{pmatrix} 1 \\ -2 \\ 0 \\ 0.5 \\ 0 \end{pmatrix}, \begin{pmatrix} 6 \\ 12 \\ -7 \\ -3 \\ 7 \end{pmatrix} \right\}.$$

Exactly two of them have the same span: find which two, and also justify why the span of each of the remaining sets is different (recall that the scalars are taken from $\mathbb{R}$).

Problem 7. Consider the following vectors from $\mathbb{Z}_7^4$:

$$\begin{pmatrix} 6 \\ 2 \\ 0 \\ 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 \\ 3 \\ 5 \\ 4 \end{pmatrix},$$

$$\begin{pmatrix} 2 \\ 3 \\ 1 \\ 5 \end{pmatrix}, \qquad \begin{pmatrix} 2 \\ 5 \\ 2 \\ 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 \\ 2 \\ 2 \\ 2 \end{pmatrix}, \qquad \begin{pmatrix} 1 \\ 4 \\ 3 \\ 1 \end{pmatrix}.$$

Show that only two of the vectors in the second line are linear combinations of the vectors in the first line (where the scalars are taken from $\mathbb{Z}_7$).

Math 127
Suggested solutions to Homework Set 2

Problem 1. We check that $\mathbb{R}^n$ with coordinate-wise addition and multiplication satisfies all axioms of a commutative ring.

Addition is commutative: Consider two elements $\bar{x}, \bar{y} \in \mathbb{R}^n$. By definition, we have that the i-th component of $\bar{x} + \bar{y}$ is $x_i + y_i$. Similarly, the i-th component of $\bar{y} + \bar{x}$ is $y_i + x_i$. Since addition in $\mathbb{R}$ is commutative, it holds that $x_i + y_i = y_i + x_i$ for every index i. This shows that $\bar{x} + \bar{y}$ and $\bar{y} + \bar{x}$ have the same i-th component for every i, and hence $\bar{x} + \bar{y} = \bar{y} + \bar{x}$.

Addition is associative: Consider three elements $\bar{x}, \bar{y}, \bar{z} \in \mathbb{R}^n$. By definition, we have that the i-th component of $(\bar{x} + \bar{y}) + \bar{z}$ is $(x_i + y_i) + z_i$. Similarly, the i-th component of $\bar{x} + (\bar{y} + \bar{z})$ is $x_i + (y_i + z_i)$. Since addition in $\mathbb{R}$ is associative, it holds that $(x_i + y_i) + z_i = x_i + (y_i + z_i)$ for every index i. This shows that $(\bar{x} + \bar{y}) + \bar{z}$ and $\bar{x} + (\bar{y} + \bar{z})$ have the same i-th component for every i, and hence $(\bar{x} + \bar{y}) + \bar{z} = \bar{x} + (\bar{y} + \bar{z})$.

Neutral element: We check that $\bar{0} = (0, 0, \ldots, 0)$ (the n-tuple all of whose components are equal to $0 \in \mathbb{R}$) is the neutral element of addition. Indeed, for every $\bar{x} \in \mathbb{R}^n$,

$$\bar{0} + \bar{x} = (0 + x_1, 0 + x_2, \ldots, 0 + x_n) = (x_1, x_2, \ldots, x_n) = \bar{x}.$$

Additive inverses: Consider an element $\bar{x} \in \mathbb{R}^n$, and set $\bar{w}$ to be the n-tuple with i-th component $w_i = -x_i$ (each x_i is a real number, so it has an additive inverse in $\mathbb{R}$). Then $\bar{w}$ is the additive inverse of $\bar{x}$:

$$\begin{aligned} \bar{x} + \bar{w} &= (x_1 + w_1, x_2 + w_2, \ldots, x_n + w_n) \\ &= \big(x_1 + (-x_1), x_2 + (-x_2), \ldots, x_n + (-x_n)\big) = \bar{0}. \end{aligned}$$

Multiplication is commutative: Consider two elements $\bar{x}, \bar{y} \in \mathbb{R}^n$. By definition, we have that the i-th component of $\bar{x} \cdot \bar{y}$ is $x_i y_i$. Similarly, the i-th component of $\bar{y} \cdot \bar{x}$ is $y_i x_i$. Since multiplication in $\mathbb{R}$ is commutative, it holds that $x_i y_i = y_i x_i$ for every index i. This shows that $\bar{x} \cdot \bar{y}$ and $\bar{y} \cdot \bar{x}$ have the same i-th component for every i, and hence $\bar{x} \cdot \bar{y} = \bar{y} \cdot \bar{x}$.

Multiplication is associative: Consider three elements $\bar{x}, \bar{y}, \bar{z} \in \mathbb{R}^n$. By definition, we have that the i-th component of $(\bar{x} \cdot \bar{y}) \cdot \bar{z}$ is $(x_i y_i) z_i$. Similarly, the i-th component of $\bar{x} \cdot (\bar{y} \cdot \bar{z})$ is $x_i (y_i z_i)$. Since multiplication in $\mathbb{R}$ is associative, it holds that $(x_i y_i) z_i = x_i (y_i z_i)$ for every index i. This shows that $(\bar{x} \cdot \bar{y}) \cdot \bar{z}$ and $\bar{x} \cdot (\bar{y} \cdot \bar{z})$ have the same i-th component for every i, and hence $(\bar{x} \cdot \bar{y}) \cdot \bar{z} = \bar{x} \cdot (\bar{y} \cdot \bar{z})$.

Identity element: We check that $\bar{1} = (1, 1, \ldots, 1)$ (the n-tuple all of whose components are equal to $1 \in \mathbb{R}$) is the neutral element of multiplication. Indeed, for every $\bar{x} \in \mathbb{R}^n$,

$$\bar{1} \cdot \bar{x} = (1 \cdot x_1, 1 \cdot x_2, \ldots, 1 \cdot x_n) = (x_1, x_2, \ldots, x_n) = \bar{x}.$$

Distributive law: Consider three elements $\bar{x}, \bar{y}, \bar{z} \in \mathbb{R}^n$. By definition, we have that the i-th component of $(\bar{x} + \bar{y}) \cdot \bar{z}$ is $(x_i + y_i) z_i$. Similarly, the i-th component of $\bar{x} \cdot \bar{z} + \bar{y} \cdot \bar{z}$ is $x_i z_i + y_i z_i$. Since multiplication distributes over addition in $\mathbb{R}$, it holds that $(x_i + y_i) z_i = x_i z_i + y_i z_i$ for every index i. This shows that $(\bar{x} + \bar{y}) \cdot \bar{z}$ and $\bar{x} \cdot \bar{z} + \bar{y} \cdot \bar{z}$ have the same i-th component for every i, and hence $(\bar{x} + \cdot \bar{y}) \cdot \bar{z} = \bar{x} \cdot \bar{z} + \bar{y} \cdot \bar{z}$.

The above show that $\mathbb{R}^n$ with coordinate-wise addition and coordinate-wise multiplication is a commutative ring.

We finally check that it is not a field. Given that $n > 1$ by our assumptions, we can find non-zero n-tuples whose first component is 0: for instance, the element $(0, 1, \ldots, 1)$ (all of whose components are 1 except for the first one which is 0) is a non-zero element. Consider now any other element $\bar{x} \in \mathbb{R}^n$. Then

$$(0, 1, \ldots, 1) \cdot \bar{x} = (0 \cdot x_1, 1 \cdot x_2, \ldots, 1 \cdot x_n) = (0, x_2, \ldots, x_n) \neq \bar{1},$$

no matter what $\bar{x}$ is. This shows that there is no multiplicative inverse of $(0, 1, \ldots, 1)$ in $\mathbb{R}^n$, and hence this structure fails to be a field.

Problem 2. (i) Consider three elements $a, b, c \in \mathbb{F}$, and suppose that

$$a + b = a + c.$$

We recall that there is an element $-a \in \mathbb{F}$ such that $a + (-a) = (-a) + a = 0$. We add to both sides of the above equality the element $-a$: using the associativity of addition as well, we can write

$$(-a)+(a+b) = (-a)+(a+c) \;\Rightarrow\; ((-a)+a)+b = ((-a)+a)+c \;\Rightarrow\; 0+b = 0+c.$$

Given that 0 is the neutral element of addition, the last equality implies $b = c$, as we wanted.

Since the elements a, b, c were arbitrary, the proof is complete.

(ii) Consider three elements $a, b, c \in \mathbb{F}$ such that $a \neq 0$, and suppose that

$$ab = ac.$$

Since $a \neq 0$, we recall that there is an element $a^{-1} \in \mathbb{F}$ such that $aa^{-1} = a^{-1}a = 1$. We multiply both sides of the above equality by the element a^{-1}: using the associativity of multiplication as well, we can write

$$a^{-1}(ab) = a^{-1}(ac) \quad\Rightarrow\quad (a^{-1}a)b = (a^{-1}a)c \quad\Rightarrow\quad 1b = 1c.$$

Given that 1 is the neutral element of multiplication, the last equality implies $b = c$, as we wanted.

Since the elements a, b, c with $a \neq 0$ were arbitrary, the proof is complete.

Problem 3. (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:

$+$	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		

(1)

(note that we filled out three columns too, and moreover 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).

Addition. 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 3 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 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: $x = y = z$. Then $(x + y) + z = (x + x) + x = x + (x + x)$ simply by commutativity.

Case 3: two of 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 y, z, w is equal to 1 or c or 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:

x, y, z are all different

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.

one of x, y is equal to z, while the other one is $= 1$

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.

one of x, y is equal to z, and $\{x, y\} = \{c, d\}$

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 4. (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. if $\bar{x} = \bar{0}$, then $\langle \bar{x}, \bar{x} \rangle = 0$; 2. if $\bar{x} \neq \bar{0}$, 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 5. (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 $i \neq j$,

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

Problem 6. We will show that $\text{span}(S_1) = \text{span}(S_2)$ by showing that $\text{span}(S_1) \subseteq \text{span}(S_2)$ and $\text{span}(S_2) \subseteq \text{span}(S_1)$.

Afterwards, we will also check that $\text{span}(S_1) \neq \text{span}(S_3)$ and $\text{span}(S_1) \neq \text{span}(S_4)$.

To show that $\text{span}(S_1) \subseteq \text{span}(S_2)$, it suffices to check that

$$\begin{pmatrix} 1 \\ -2 \\ 0 \\ 0.5 \\ 0 \end{pmatrix} \in \text{span}(S_2) \qquad \text{and} \qquad \begin{pmatrix} 6 \\ -12 \\ 7 \\ 3 \\ -7 \end{pmatrix} \in \text{span}(S_2). \tag{2}$$

Indeed, if we find $\lambda_1, \mu_1, \kappa_1, \lambda_2, \mu_2, \kappa_2 \in \mathbb{R}$ so that

$$\begin{pmatrix} 1 \\ -2 \\ 0 \\ 0.5 \\ 0 \end{pmatrix} = \lambda_1 \cdot \begin{pmatrix} 2 \\ -4 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \mu_1 \cdot \begin{pmatrix} 0 \\ 0 \\ -2 \\ 0 \\ 2 \end{pmatrix} + \kappa_1 \cdot \begin{pmatrix} -1 \\ 2 \\ 3 \\ -0.5 \\ -3 \end{pmatrix}$$

$$\text{and} \quad \begin{pmatrix} 6 \\ -12 \\ 7 \\ 3 \\ -7 \end{pmatrix} = \lambda_2 \cdot \begin{pmatrix} 2 \\ -4 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \mu_2 \cdot \begin{pmatrix} 0 \\ 0 \\ -2 \\ 0 \\ 2 \end{pmatrix} + \kappa_2 \cdot \begin{pmatrix} -1 \\ 2 \\ 3 \\ -0.5 \\ -3 \end{pmatrix}$$

then for an arbitrary vector $\bar{v} \in \text{span}(S_1)$,

$$\bar{v} = \alpha \cdot \begin{pmatrix} 1 \\ -2 \\ 0 \\ 0.5 \\ 0 \end{pmatrix} + \beta \cdot \begin{pmatrix} 6 \\ -12 \\ 7 \\ 3 \\ -7 \end{pmatrix} \qquad \text{for some } \alpha, \beta \in \mathbb{R},$$

we will be able to write

$$\bar{v} = \alpha \cdot \left[\lambda_1 \cdot \begin{pmatrix} 2 \\ -4 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \mu_1 \cdot \begin{pmatrix} 0 \\ 0 \\ -2 \\ 0 \\ 2 \end{pmatrix} + \kappa_1 \cdot \begin{pmatrix} -1 \\ 2 \\ 3 \\ -0.5 \\ -3 \end{pmatrix} \right]$$
$$+ \beta \cdot \left[\lambda_2 \cdot \begin{pmatrix} 2 \\ -4 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \mu_2 \cdot \begin{pmatrix} 0 \\ 0 \\ -2 \\ 0 \\ 2 \end{pmatrix} + \kappa_2 \cdot \begin{pmatrix} -1 \\ 2 \\ 3 \\ -0.5 \\ -3 \end{pmatrix} \right]$$
$$= \big(\alpha \cdot \lambda_1 + \beta \cdot \lambda_2\big) \cdot \begin{pmatrix} 2 \\ -4 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \big(\alpha \cdot \mu_1 + \beta \cdot \mu_2\big) \cdot \begin{pmatrix} 0 \\ 0 \\ -2 \\ 0 \\ 2 \end{pmatrix} + \big(\alpha \cdot \kappa_1 + \beta \cdot \kappa_2\big) \cdot \begin{pmatrix} -1 \\ 2 \\ 3 \\ -0.5 \\ -3 \end{pmatrix},$$

and this will show that $\bar{v} \in \text{span}(S_2)$ as well.

We proceed to verify (2). We notice that

$$\begin{pmatrix} 1 \\ -2 \\ 0 \\ 0.5 \\ 0 \end{pmatrix} = 0.5 \cdot \begin{pmatrix} 2 \\ -4 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \tag{3}$$

which shows the first part of (2).

Next we also note that

$$\begin{pmatrix} 6 \\ -12 \\ 7 \\ 3 \\ -7 \end{pmatrix} = \begin{pmatrix} 6 \\ -12 \\ 0 \\ 3 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 7 \\ 0 \\ -7 \end{pmatrix} = 3 \cdot \begin{pmatrix} 2 \\ -4 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \left(-\frac{7}{2}\right) \cdot \begin{pmatrix} 0 \\ 0 \\ -2 \\ 0 \\ 2 \end{pmatrix}, \tag{4}$$

which shows the second part of (2).

Combining all the above, we conclude that $\text{span}(S_1) \subseteq \text{span}(S_2)$.

Similarly, to show that $\text{span}(S_2) \subseteq \text{span}(S_1)$, it suffices to check that

$$\begin{pmatrix} 2 \\ -4 \\ 0 \\ 1 \\ 0 \end{pmatrix} \in \text{span}(S_1), \quad \begin{pmatrix} 0 \\ 0 \\ -2 \\ 0 \\ 2 \end{pmatrix} \in \text{span}(S_1) \quad \text{and} \quad \begin{pmatrix} -1 \\ 2 \\ 3 \\ -0.5 \\ -3 \end{pmatrix} \in \text{span}(S_1). \quad (5)$$

Observe that (3) quickly implies the first part of (5):

$$\begin{pmatrix} 1 \\ -2 \\ 0 \\ 0.5 \\ 0 \end{pmatrix} = 0.5 \cdot \begin{pmatrix} 2 \\ -4 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad \Rightarrow \quad \begin{pmatrix} 2 \\ -4 \\ 0 \\ 1 \\ 0 \end{pmatrix} = 2 \cdot \begin{pmatrix} 1 \\ -2 \\ 0 \\ 0.5 \\ 0 \end{pmatrix}.$$

Combining this with (4) as well, we obtain the second part of (5):

$$(4) \;\Rightarrow\; \left(-\frac{7}{2}\right) \cdot \begin{pmatrix} 0 \\ 0 \\ -2 \\ 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 6 \\ -12 \\ 7 \\ 3 \\ -7 \end{pmatrix} - 3 \cdot \begin{pmatrix} 2 \\ -4 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 6 \\ -12 \\ 7 \\ 3 \\ -7 \end{pmatrix} - 6 \cdot \begin{pmatrix} 1 \\ -2 \\ 0 \\ 0.5 \\ 0 \end{pmatrix}$$

$$\Rightarrow \quad \begin{pmatrix} 0 \\ 0 \\ -2 \\ 0 \\ 2 \end{pmatrix} = \left(-\frac{2}{7}\right) \cdot \begin{pmatrix} 6 \\ -12 \\ 7 \\ 3 \\ -7 \end{pmatrix} + \frac{12}{7} \cdot \begin{pmatrix} 1 \\ -2 \\ 0 \\ 0.5 \\ 0 \end{pmatrix}. \quad (6)$$

Finally we note that

$$\begin{pmatrix} -1 \\ 2 \\ 3 \\ -0.5 \\ -3 \end{pmatrix} = \begin{pmatrix} -1 \\ 2 \\ 0 \\ -0.5 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 3 \\ 0 \\ -3 \end{pmatrix} = (-1) \cdot \begin{pmatrix} 1 \\ -2 \\ 0 \\ 0.5 \\ 0 \end{pmatrix} + \left(-\frac{2}{3}\right) \cdot \begin{pmatrix} 0 \\ 0 \\ -2 \\ 0 \\ 2 \end{pmatrix},$$

which combined with (6) gives the third part of (5) (why?).

We conclude that $\text{span}(S_2) \subseteq \text{span}(S_1)$, and therefore that $\text{span}(S_2) = \text{span}(S_1)$.

We now check that $\text{span}(S_3) \neq \text{span}(S_1)$. It suffices to check that

$$\begin{pmatrix} 0 \\ 0 \\ -1 \\ 0.5 \\ 1 \end{pmatrix} \notin \text{span}(S_1),$$

because then we will have an element of $\text{span}(S_3)$ which is not in $\text{span}(S_1)$, so definitely the two linear spans will not coincide.

We equivalently show that the linear system

$$\left\{ \begin{array}{rcrcl} t & + & 6s & = & 0 \\ -2t & - & 12s & = & 0 \\ & & 7s & = & -1 \\ 0.5t & + & 3s & = & 0.5 \\ & & -7s & = & 1 \end{array} \right\}$$

is inconsistent.

Looking at the 3rd equation, we see that we must have $s = -1/7$. Combining this with the 1st equation, we also see that we must have $t = -6s = 6/7$. But then

$$0.5t + 3s = 0.5\,\frac{6}{7} + 3\left(-\frac{1}{7}\right) = \frac{3}{7} - \frac{3}{7} = 0 \neq 0.5,$$

which shows that we cannot satisfy the 1st, 3rd and 4th equations at the same time.

Similarly we check that $\text{span}(S_4) \neq \text{span}(S_1)$. Given that

$$\begin{pmatrix} 1 \\ -2 \\ 0 \\ 0.5 \\ 0 \end{pmatrix} \in S_1 \cap S_4,$$

we are essentially led to show

$$\text{either that } \begin{pmatrix} 6 \\ 12 \\ -7 \\ -3 \\ 7 \end{pmatrix} \notin \text{span}(S_1), \qquad \text{or that } \begin{pmatrix} 6 \\ -12 \\ 7 \\ 3 \\ -7 \end{pmatrix} \notin \text{span}(S_4).$$

Here we check the former by showing that the linear system

$$\left\{\begin{array}{rcrcr} t & + & 6s & = & 6 \\ -2t & - & 12s & = & 12 \\ & & 7s & = & -7 \\ 0.5t & + & 3s & = & -3 \\ & & -7s & = & 7 \end{array}\right\}$$

is inconsistent.

Looking at the 3rd equation, we see that we must have $s = -1$. Combining this with the 2nd equation, we also see that we must have $-2t + 12 = -2t - 12s = 12 \Rightarrow -2t = 0 \Rightarrow t = 0$. But then

$$t + 6s = 6s = -6 \neq 6,$$

which shows that we cannot satisfy the 1st, 2nd and 3rd equations at the same time.

This completes the solution of Problem 6.

Problem 7. We check first whether there are $t_1, s_1 \in \mathbb{Z}_7$ such that

$$\begin{pmatrix} 2 \\ 3 \\ 1 \\ 5 \end{pmatrix} = t_1 \cdot \begin{pmatrix} 6 \\ 2 \\ 0 \\ 1 \end{pmatrix} + s_1 \cdot \begin{pmatrix} 1 \\ 3 \\ 5 \\ 4 \end{pmatrix} = \begin{pmatrix} 6t_1 + s_1 \\ 2t_1 + 3s_1 \\ 5s_1 \\ t_1 + 4s_1 \end{pmatrix}.$$

This is equivalent to finding a solution to the following system of linear equations:

$$\left\{ \begin{array}{rcrcl} 6t_1 & + & s_1 & = & 2 \\ 2t_1 & + & 3s_1 & = & 3 \\ & & 5s_1 & = & 1 \\ t_1 & + & 4s_1 & = & 5 \end{array} \right\}.$$

Looking at the 3rd equation, we note that we should have $5s_1 = 1 \Leftrightarrow s_1 = 5^{-1} = 3$ (recall that we are working in $\mathbb{Z}_7$).

Combining this with the 4th equation, we note that we should have $t_1 + 4 \cdot 3 = 5 \Leftrightarrow t_1 = 0$.

Therefore, there is only one choice of values for t_1 and s_1 that would satisfy the 3rd and the 4th equations at the same time: $t_1 = 0$ and $s_1 = 3$.

Given that $2 \neq 3 = 6 \cdot 0 + 3$, we conclude that $\begin{pmatrix} 2 \\ 3 \\ 1 \\ 5 \end{pmatrix}$ cannot be written as a linear combination of the given vectors.

Next we check whether there are $t_2, s_2 \in \mathbb{Z}_7$ such that

$$\begin{pmatrix} 2 \\ 5 \\ 2 \\ 0 \end{pmatrix} = t_2 \cdot \begin{pmatrix} 6 \\ 2 \\ 0 \\ 1 \end{pmatrix} + s_2 \cdot \begin{pmatrix} 1 \\ 3 \\ 5 \\ 4 \end{pmatrix} = \begin{pmatrix} 6t_2 + s_2 \\ 2t_2 + 3s_2 \\ 5s_2 \\ t_2 + 4s_2 \end{pmatrix}.$$

This is equivalent to finding a solution to the following system of linear equations:

$$\left\{ \begin{array}{rcrcl} 6t_2 & + & s_2 & = & 2 \\ 2t_2 & + & 3s_2 & = & 5 \\ & & 5s_2 & = & 2 \\ t_2 & + & 4s_2 & = & 0 \end{array} \right\}.$$

Looking at the 3rd equation, we note that we should have $5s_2 = 2 \Leftrightarrow s_2 = 2 \cdot 5^{-1} = 6$.

Combining this with the 4th equation, we note that we should have $t_2 + 4 \cdot 6 = 0 \Leftrightarrow t_2 = -4 \cdot 6 = -3 = 4$.

Therefore, there is only one choice of values for t_2 and s_2 that would satisfy the 3rd and the 4th equations at the same time: $t_2 = 4$ and $s_2 = 6$.

We now check whether this choice of values for t_2 and s_2 solves the system: we note that

$$6 \cdot 4 + 6 = 3 + 6 = 2 \quad \text{and} \quad 2 \cdot 4 + 3 \cdot 6 = 1 + 4 = 5.$$

We conclude that we can write $\begin{pmatrix} 2 \\ 5 \\ 2 \\ 0 \end{pmatrix}$ as a linear combination of the given vectors.

Next we check whether there are $t_3, s_3 \in \mathbb{Z}_7$ such that

$$\begin{pmatrix} 0 \\ 2 \\ 2 \\ 2 \end{pmatrix} = t_3 \cdot \begin{pmatrix} 6 \\ 2 \\ 0 \\ 1 \end{pmatrix} + s_3 \cdot \begin{pmatrix} 1 \\ 3 \\ 5 \\ 4 \end{pmatrix} = \begin{pmatrix} 6t_3 + s_3 \\ 2t_3 + 3s_3 \\ 5s_3 \\ t_3 + 4s_3 \end{pmatrix}.$$

This is equivalent to finding a solution to the following system of linear equations:

$$\left\{ \begin{array}{rcrcl} 6t_3 & + & s_3 & = & 0 \\ 2t_3 & + & 3s_3 & = & 2 \\ & & 5s_3 & = & 2 \\ t_3 & + & 4s_3 & = & 2 \end{array} \right\}.$$

Looking at the 3rd equation, we note that we should have $5s_3 = 2 \Leftrightarrow s_3 = 2 \cdot 5^{-1} = 6$.

Combining this with the 4th equation, we note that we should have $t_3 + 4 \cdot 6 = 2 \Leftrightarrow t_3 = 2 - 4 \cdot 6 = 2 - 3 = -1 = 6$.

Therefore, there is only one choice of values for t_3 and s_3 that would satisfy the 3rd and the 4th equations at the same time: $t_3 = 6$ and $s_3 = 6$.

We now check whether this choice of values for t_3 and s_3 solves the system: we note that

$$6 \cdot 6 + 6 = 1 + 6 = 0 \quad \text{and} \quad 2 \cdot 6 + 3 \cdot 6 = 5 + 4 = 2.$$

We conclude that we can write $\begin{pmatrix} 0 \\ 2 \\ 2 \\ 2 \end{pmatrix}$ as a linear combination of the given vectors.

Finally, we verify that there are no $t_4, s_4 \in \mathbb{Z}_7$ such that

$$\begin{pmatrix} 1 \\ 4 \\ 3 \\ 1 \end{pmatrix} = t_4 \cdot \begin{pmatrix} 6 \\ 2 \\ 0 \\ 1 \end{pmatrix} + s_4 \cdot \begin{pmatrix} 1 \\ 3 \\ 5 \\ 4 \end{pmatrix} = \begin{pmatrix} 6t_4 + s_4 \\ 2t_4 + 3s_4 \\ 5s_4 \\ t_4 + 4s_4 \end{pmatrix}.$$

If there were, we should be able to find a solution to the following system of linear equations:

$$\left\{\begin{array}{rcrcl} 6t_4 & + & s_4 & = & 1 \\ 2t_4 & + & 3s_4 & = & 4 \\ & & 5s_4 & = & 3 \\ t_4 & + & 4s_4 & = & 1 \end{array}\right\}.$$

Looking at the 3rd equation, we note that we should have $5s_4 = 3 \Leftrightarrow s_4 = 3 \cdot 5^{-1} = 2$.

Combining this with the 4th equation, we also obtain that $t_4 + 4 \cdot 2 = 1 \Leftrightarrow t_4 = 1 - 4 \cdot 2 = 0$.

Therefore, there is only one choice of values for t_4 and s_4 that would satisfy the 3rd and the 4th equations at the same time: $t_4 = 0$ and $s_4 = 2$.

Given that $1 \neq 2 = 6 \cdot 0 + 2$, we conclude that this last system is inconsistent and therefore $\begin{pmatrix} 1 \\ 4 \\ 3 \\ 1 \end{pmatrix}$ cannot be written as a linear combination of the given vectors.

Math 127
Homework Problem Set 3

Problem 1. (i) Let $\mathcal{R}$ be a ring (not necessarily commutative, that is, multiplication in $\mathcal{R}$ may or may not be commutative). Consider $a, b, c \in \mathcal{R}$ and show the following:

$$-a = (-1) \cdot a, \qquad -(b \cdot c) = (-b) \cdot c = b \cdot (-c).$$

(Note that here e.g. $-a$ denotes the additive inverse of a, while -1 denotes the additive inverse of the multiplicative identity 1, and $(-1) \cdot a$ denotes the product of -1 and a; similarly $-(b \cdot c)$ denotes the additive inverse of the product $b \cdot c$, while $(-b) \cdot c$ denotes the product of $-b$ and c.)

[*Hint.* You may wish to first give a proof in a commutative ring $\mathcal{R}$, and then check that the proof can be adapted to work even when $\mathcal{R}$ is non-commutative. Similarly you can check (and it will be useful to do so because you may need it in part (i) as well) that in any ring $\mathcal{R}$ we have:

$$0 \cdot x = x \cdot 0 = 0 \quad \text{for all } x \in \mathcal{R},$$

and that any proof you came up with in the commutative case can be adapted to work in the general case as well.]

(ii) Let $\mathbb{F}$ be a field, and let x be a non-zero element of $\mathbb{F}$ (recall that then we know that x has a multiplicative inverse). Show that $-x$ has a multiplicative inverse too, and that

$$(-x)^{-1} = -(x^{-1}).$$

(iii) Let $m > 1$ be a positive integer (not necessarily a prime), and consider the ring $\mathbb{Z}_m$. Let $[k], [l]$ be two invertible elements of $\mathbb{Z}_m$. Show that their product $[k] \cdot [l]$ is also invertible, and that

$$\big([k] \cdot [l]\big)^{-1} = [k]^{-1} \cdot [l]^{-1}.$$

(iv) Does part (iii) have a corresponding version in any commutative ring $\mathcal{R}$? If yes, how would you state the corresponding fact? (If yes, you only need to give a corresponding statement, not prove it.)

What if $\mathcal{R}$ is a non-commutative ring?

Problem 2. Let $\mathbb{F}$ be a field, and suppose there is $c \in \mathbb{F}$ which is non-zero and satisfies $c + c = 0$. Show that for every $x \in \mathbb{F}$ we have $x + x = 0$.

Problem 3. Use Gaussian elimination (or in other words, row reduction) to solve the following linear systems.

(i) $$\left\{\begin{array}{rcl} 3x_1 - 6x_2 + 7x_3 &=& 0 \\ -x_1 + 2x_2 - 3x_3 &=& -2 \\ 2x_1 + 0x_2 + 4x_3 &=& 1 \end{array}\right\} \quad \text{(coefficients from } \mathbb{R}\text{)}.$$

(ii) $$\left\{\begin{array}{rcrcrcrcl} 2x_1 &+& 3x_2 &+& x_3 &+& x_4 &=& 1 \\ -x_1 &+& 3x_2 &-& 3x_3 &+& 4x_4 &=& 3 \\ 0x_1 &+& x_2 &+& 4x_3 &-& x_4 &=& 1 \end{array}\right\} \quad \text{(coefficients from } \mathbb{Z}_5\text{)}.$$

Problem 4. Give an example of an inconsistent and underdetermined system of linear equations in at least 3 unknowns, where none of the equations is a multiple of another equation in the system, and also all equations have at least two non-zero coefficients (you can choose to work over any field you want, but specify what field you chose, and also explain why your example has the required properties).

Problem 5. Assume that the following matrices are augmented matrices of certain systems of linear equations. In each case, use the matrix to determine the general form of the solutions: that is, to which $\mathbb{F}^n$ the solutions belong (namely what is $\mathbb{F}$ and what is n).

Furthermore, determine which of these matrices correspond to an upper triangular system (equivalently, which of these matrices are in row echelon form), and use each such matrix to find the size of the set of solutions of the system: that is, determine whether it is the empty set, or an infinite set, or a nonempty finite set (and if it is a nonempty finite set, determine exactly its size). Justify your answers.

Do not try to find any of these solutions.

$$A_1 = \begin{pmatrix} 2 & -3.5 & 17 & 0 & 9 & 1 & 2 & 0 \\ 0 & 2 & 3 & -4 & 100 & 20 & 5 & 6 \\ 0 & 0 & 35 & 4 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 4 & 0 & 7 & -25 & 0.5 \\ 0 & 0 & 0 & 0 & 0 & 8 & 0 & 113 \end{pmatrix} \in \mathbb{R}^{5\times 8},$$

$$A_2 = \begin{pmatrix} 0 & 1 & 2 & 0 & 9 \\ 0 & -11 & 8 & -4 & 0 \\ 0 & 0 & 3 & 4 & 1 \\ 0 & 0 & 0 & 4 & 12 \end{pmatrix} \in \mathbb{Z}_{13}^{4\times 5}, \qquad A_3 = \begin{pmatrix} 4 & 1 & 0 & 6 & 3 \\ 0 & 0 & -3 & 4 & 2 \\ 0 & 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 0 & 3 \end{pmatrix} \in \mathbb{Z}_7^{4\times 5},$$

$$A_4 = \begin{pmatrix} 3 & 1 & 4 & 0 & 5 & 0 \\ 0 & 2 & -3 & 4 & 5 & 0 \\ 0 & 0 & 0 & 4 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in \mathbb{Z}_7^{4\times 6}, \qquad A_5 = \begin{pmatrix} 2 & -0.75 & 8 & 0 & 7 & 0 \\ 0 & 13 & 4 & -4 & 7 & 2 \\ 0 & 0 & -99 & 0.25 & 3 & 0 \\ 0 & 0 & 0 & 5 & 0 & 1 \\ 0 & 0 & 0 & 0 & 7 & -12 \end{pmatrix} \in \mathbb{Q}^{5\times 6}.$$

Problem 6. This problem has two parts involving a square matrix A. In each part, find $A^2 = A \cdot A$. Moreover, use Gaussian elimination to determine whether A^2 is invertible (you do not have to find its inverse).

[*Hint.* Does it suffice to determine whether A is invertible? See also Problem 1 of this homework set.]

(i) $$A = \begin{pmatrix} 1 & -1 & 1 \\ 11 & 4 & 2 \\ 2 & -2 & 3 \end{pmatrix} \in \mathbb{R}^{3\times 3}.$$

(ii) $$A = \begin{pmatrix} 1 & 2 & 3 & 1 \\ 2 & 4 & 1 & 3 \\ 0 & 0 & 0 & 1 \\ 3 & 1 & 0 & 0 \end{pmatrix} \in \mathbb{Z}_5^{4\times 4}.$$

Problem 7. Let $\mathbb{F}$ be any of the fields we have discussed so far. Give a general proof that multiplication of matrices in $\mathbb{F}^{2\times 2}$ is not commutative.

That is, give an example (that would work in any of the fields $\mathbb{F}$ we have discussed) of two matrices $A, B \in \mathbb{F}^{2\times 2}$ such that $AB \neq BA$, and verify this.

Math 127
Suggested solutions to Homework Set 3

Problem 1. (i) We will use the fact that, for every $x \in \mathcal{R}$,

$$0 \cdot x = x \cdot 0 = 0.$$

Even though this is not necessary here, we include a brief justification for completeness.

The equality $0 \cdot x = 0$ has already been proven in HW1, Pb3 (even though we were working there in a commutative ring, the proof can go through without using that multiplication is commutative, as long as we have a right distributive law):

$$\begin{aligned} 0 \cdot x + x &= 0 \cdot x + 1 \cdot x && \text{(1 is the identity element)} \\ &= (0+1) \cdot x && \text{(by the right distributive law)} \\ &= 1 \cdot x && \text{(0 is the neutral element)} \\ &= x && \text{(1 is the identity element).} \end{aligned}$$

We conclude that we have $0 \cdot x + x = x$, and add now $-x$, the additive inverse of x, to both sides:

$$\begin{aligned} 0 \cdot x &= 0 \cdot x + 0 && \text{(0 is the neutral element)} \\ &= 0 \cdot x + (x + (-x)) && \text{($-x$ is exactly the element for which we have $x + (-x) = 0$)} \\ &= (0 \cdot x + x) + (-x) && \text{(addition is associative)} \\ &= x + (-x) && \text{(by the above identity)} \\ &= 0. \end{aligned}$$

Similarly, by using the left distributive law in $\mathcal{R}$ now, we have that

$$\begin{aligned} x \cdot 0 + x &= x \cdot 0 + x \cdot 1 && \text{(1 is the identity element)} \\ &= x \cdot (0+1) && \text{(by the left distributive law)} \\ &= x \cdot 1 && \text{(0 is the neutral element)} \\ &= x && \text{(1 is the identity element).} \end{aligned}$$

Thus again we have $x \cdot 0 + x = x$, and we can add $-x$ to both sides now to conclude that $x \cdot 0 = 0$ too.

Using this, we can prove that $(-1) \cdot a = -a = a \cdot (-1)$ (and thus also that -1 commutes with every element in $\mathcal{R}$). We have that

$$\begin{aligned} a + (-1) \cdot a &= 1 \cdot a + (-1) \cdot a && \text{(1 is the identity element)} \\ &= (1 + (-1)) \cdot a && \text{(by the right distributive law)} \\ &= 0 \cdot a && \text{(-1 is the additive inverse of 1)} \\ &= 0 && \text{(by the above fact).} \end{aligned}$$

We now check that this implies that $(-1) \cdot a$ is the additive inverse of a:

$$\begin{aligned} -a &= -a + 0 && \text{(0 is the neutral element)} \\ &= -a + \big(a + (-1) \cdot a\big) && \text{(by what we just proved)} \\ &= (-a + a) + (-1) \cdot a && \text{(addition is associative)} \\ &= 0 + (-1) \cdot a && \text{($-a$ is the additive inverse of a)} \\ &= (-1) \cdot a && \text{(0 is the neutral element).} \end{aligned}$$

Similarly,

$$\begin{aligned} a + a \cdot (-1) &= a \cdot 1 + a \cdot (-1) && \text{(1 is the identity element)} \\ &= a \cdot (1 + (-1)) && \text{(by the left distributive law)} \\ &= a \cdot 0 && \text{(-1 is the additive inverse of 1)} \\ &= 0 && \text{(by the above fact).} \end{aligned}$$

This implies in the same way as above that $a \cdot (-1) = -a$.

We can now prove the second claim of part (i): for every $b, c \in \mathcal{R}$, we have by the first claim that

$$\begin{aligned} -(b \cdot c) &= (-1) \cdot (b \cdot c) \\ &= \big((-1) \cdot b\big) \cdot c && \text{(multiplication is associative)} \\ &= (-b) \cdot c && \text{(by the first claim again).} \end{aligned}$$

Similarly,

$$\begin{aligned} -(b \cdot c) &= \big((-1) \cdot b\big) \cdot c && \text{(as before)} \\ &= \big(b \cdot (-1)\big) \cdot c && \text{(-1 commutes with b)} \\ &= b \cdot \big((-1) \cdot c\big) && \text{(multiplication is associative)} \\ &= b \cdot (-c) && \text{(by the first claim again).} \end{aligned}$$

(ii) We will make use of the second claim of part (i), which remains valid in the field $\mathbb{F}$, since $\mathbb{F}$ is also a ring. By the assumption that $x \neq 0$, we know that x has a multiplicative inverse, denoted by x^{-1}. We therefore get that

$$x \cdot (-x^{-1}) = -(x \cdot x^{-1}) = -1.$$

This implies that

$$\begin{aligned} 1 &= -(-1) && \text{(1 is the additive inverse of -1)} \\ &= -\big(x \cdot (-x^{-1})\big) && \text{(by the equality we just checked)} \\ &= (-x) \cdot (-x^{-1}) && \text{(by the second claim of part (i))} \end{aligned}$$

and moreover

$$= (-x^{-1}) \cdot (-x) \qquad \text{(multiplication is commutative in } \mathbb{F}\text{).}$$

It follows that $-x$ has a multiplicative inverse and that this is equal to $-(x^{-1})$.

(iii) We have that

$$\begin{aligned}
\big([k]\cdot[l]\big)\cdot\big([k]^{-1}\cdot[l]^{-1}\big) &= \big([k]\cdot[l]\big)\cdot\big([l]^{-1}\cdot[k]^{-1}\big) && \text{(multiplication is commutative in } \mathbb{Z}_m) \\
&= \big[\big([k]\cdot[l]\big)\cdot[l]^{-1}\big]\cdot[k]^{-1} && \text{(multiplication is associative)} \\
&= \big[[k]\cdot\big([l]\cdot[l]^{-1}\big)\big]\cdot[k]^{-1} && \text{(multiplication is associative)} \\
&= \big([k]\cdot 1\big)\cdot[k]^{-1} && ([l]^{-1} \text{ stands for the multiplicative inverse of } [l]) \\
&= [k]\cdot[k]^{-1} && (1 \text{ is the identity element}) \\
&= 1 && ([k]^{-1} \text{ stands for the multiplicative inverse of } [k]).
\end{aligned}$$

Therefore, $[k]\cdot[l]$ has a multiplicative inverse, which is equal to $[k]^{-1}\cdot[l]^{-1}$.

(iv) Both questions have an affirmative answer: we can adapt the statement of part (iii) to give a more general statement saying that the product of two invertible elements in a commutative ring $\mathcal{R}$ (or more generally a ring $\mathcal{R}$) is invertible.

The following statements, which can be proven in a similar way to above, with only a couple of adjustments in the case of a general ring, are the corresponding versions we want:

Statement 1. Let $\mathcal{R}$ be a commutative ring, and let r, s be two invertible elements of $\mathcal{R}$. Then the product $r\cdot s$ is also invertible, and its multiplicative inverse is the element $r^{-1}\cdot s^{-1}$.

Statement 2. Let $\mathcal{R}$ be a ring (not necessarily commutative), and let x, y be two invertible elements of $\mathcal{R}$. Then the product $x\cdot y$ is also invertible, and its multiplicative inverse is the element $y^{-1}\cdot x^{-1}$.

Problem 2. By the assumptions there is $c \in \mathbb{F}$, $c \neq 0$, such that $c + c = 0$. We can then write

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

using the fact that 1 is the multiplicative identity, as well as the distributive law. But $c \neq 0$, therefore the equality $(1 + 1) \cdot c = 0$ implies that $1 + 1 = 0$.

Consider now any $x \in \mathbb{F}$. We can write

$$x + x = 1 \cdot x + 1 \cdot x = (1 + 1) \cdot x = 0 \cdot x = 0,$$

where we also used the property that $0 \cdot z = 0$ for all $z \in \mathbb{F}$.

Since x was arbitrary, the proof is complete.

Problem 3. (i) We have

$$\left\{\begin{array}{rcrcrcr} 3x_1 & - & 6x_2 & + & 7x_3 & = & 0 \\ -x_1 & + & 2x_2 & - & 3x_3 & = & -2 \\ 2x_1 & & & + & 4x_3 & = & 1 \end{array}\right\} \begin{array}{c} E_2+\frac{1}{3}E_1\to E_2' \\ E3-\frac{2}{3}E1\to E_3' \\ \Longleftrightarrow \end{array}$$

$$\left\{\begin{array}{rcrcrcr} 3x_1 & - & 6x_2 & + & 7x_3 & = & 0 \\ & & & & -\frac{2}{3}x_3 & = & -2 \\ & & 4x_2 & - & \frac{2}{3}x_3 & = & 1 \end{array}\right\} \begin{array}{c} E_2\leftrightarrow E_3 \\ \Longleftrightarrow \end{array}$$

$$\left\{\begin{array}{rcrcrcr} 3x_1 & - & 6x_2 & + & 7x_3 & = & 0 \\ & & 4x_2 & - & \frac{2}{3}x_3 & = & 1 \\ & & & & -\frac{2}{3}x_3 & = & -2 \end{array}\right\}.$$

The last equivalent system is upper triangular/staircase, and it has no pivot in the last column, so we can solve it using back substitution. From the third equation we get that $x_3 = 3$. Combining this with the second equation we also get that $4x_2 - 2 = 1 \Rightarrow x_2 = 3/4$. Finally, combining these with the first equation we get that $3x_1 - 6\frac{3}{4} + 21 = 0 \Rightarrow 3x_1 = -\frac{42-9}{2} = -\frac{33}{2} \Rightarrow x_1 = -\frac{11}{2}$.

We conclude that the system has a unique solution, the solution

$$(x_1, x_2, x_3) = \big(-\tfrac{11}{2}, \tfrac{3}{4}, 3\big).$$

(ii) We have

$$\left\{\begin{array}{rcrcrcrcr} 2x_1 & + & 3x_2 & + & x_3 & + & x_4 & = & 1 \\ -x_1 & + & 3x_2 & - & 3x_3 & + & 4x_4 & = & 3 \\ & & x_2 & + & 4x_3 & - & x_4 & = & 1 \end{array}\right\} \begin{array}{c} E_2+3E_1\to E_2' \\ \Longleftrightarrow \end{array}$$

$$\left\{\begin{array}{rcrcrcrcr} 2x_1 & + & 3x_2 & + & x_3 & + & x_4 & = & 1 \\ & & 2x_2 & & & + & 2x_4 & = & 1 \\ & & x_2 & + & 4x_3 & - & x_4 & = & 1 \end{array}\right\} \begin{array}{c} E_3+2E_2\to E_3' \\ \Longleftrightarrow \end{array}$$

$$\left\{\begin{array}{rcrcrcrcr} 2x_1 & + & 3x_2 & + & x_3 & + & x_4 & = & 1 \\ & & 2x_2 & & & + & 2x_4 & = & 1 \\ & & & & 4x_3 & + & 3x_4 & = & 3 \end{array}\right\} \begin{array}{c} 3E_1\to E_1',\ 3E_2\to E_2' \\ 4E3\to E_3' \\ \Longleftrightarrow \end{array}$$

$$\left\{\begin{array}{rcrcrcrcr} x_1 & + & 4x_2 & + & 3x_3 & + & 3x_4 & = & 3 \\ & & x_2 & & & + & x_4 & = & 3 \\ & & & & x_3 & + & 2x_4 & = & 2 \end{array}\right\}.$$

The last equivalent system is upper triangular/staircase, and it has no pivot in the last column, therefore it is consistent. In addition, it has no pivot in the fourth column, but it has pivots in all previous columns. Therefore x_4 is

the only free variable, and the system has more than one solutions (in this case it has $|\mathbb{Z}_5| = 5$ solutions).

Each of these solutions can be found via back substitution after we assign a value to x_4, so we can parametrise the solution set S_2 as follows: if $x_4 = \mu$ with μ some element of $\mathbb{Z}_5$, then $x_3 = 2 - 2\mu$, $x_2 = 3 - \mu$, and

$$x_1 = 3 - 4(3 - \mu) - 3(2 - 2\mu) - 3\mu = 2\mu.$$

In other words,

$$S_2 = \big\{(2\mu, 3 - \mu, 2 - 2\mu, \mu) : \mu \in \mathbb{Z}_5\big\}.$$

Problem 4. One example is the following system with coefficients from $\mathbb{R}$:

$$\left\{\begin{array}{rcrcrcrcl} x_1 & + & x_2 & + & x_3 & + & x_4 & = & 8 \\ x_1 & + & 2x_2 & + & 2x_3 & + & 2x_4 & = & 4 \\ & & x_2 & + & x_3 & + & x_4 & = & 4 \end{array}\right\}.$$

This system has 3 equations (with the desired properties) and 4 unknowns, so it is underdetermined. To see that it is inconsistent, note that

$$\left\{\begin{array}{rcrcrcrcl} x_1 & + & x_2 & + & x_3 & + & x_4 & = & 8 \\ x_1 & + & 2x_2 & + & 2x_3 & + & 2x_4 & = & 4 \\ & & x_2 & + & x_3 & + & x_4 & = & 4 \end{array}\right\} \quad \overset{E_2-E_1\to E_2'}{\Longleftrightarrow}$$

$$\left\{\begin{array}{rcrcrcrcr} x_1 & + & x_2 & + & x_3 & + & x_4 & = & 8 \\ & & x_2 & + & x_3 & + & x_4 & = & -4 \\ & & x_2 & + & x_3 & + & x_4 & = & 4 \end{array}\right\} \quad \overset{E_3-E_2\to E_3'}{\Longleftrightarrow}$$

$$\left\{\begin{array}{rcrcrcrcr} x_1 & + & x_2 & + & x_3 & + & x_4 & = & 8 \\ & & x_2 & + & x_3 & + & x_4 & = & -4 \\ & & & & & & 0x_4 & = & 8 \end{array}\right\}.$$

Thus the last equivalent system contains an inconsistent equation, the equation $0x_4 = 8$, and so it is inconsistent too.

Problem 5. 1. A_1 has 8 columns. Given that it is the augmented matrix of a linear system, its last column is the column of the constant terms. Therefore, the corresponding system is in 7 unknowns, and thus the solutions to it, if any exist, will be vectors in $\mathbb{R}^7$.

A_1 is in row echelon form, or equivalently the corresponding system is upper triangular/staircase. Indeed, all the rows of the matrix are non-zero, and the first non-zero entry of the first row is 2 in the first column, the first non-zero entry of the second row is 2 in the second column, the first non-zero entry of the third row is 35 in the third column, the first non-zero entry of the fourth row is 4 in the fourth column, and finally the first non-zero entry of the fifth row is 8 in the sixth column; given that each such entry is to the right of the previous first non-zero entries, the matrix is indeed in REF and these entries are its pivots.

We finally observe that there is no pivot in the fifth, seventh and eighth columns. The latter shows that the corresponding system is consistent, while the former show that there are two free variables. Therefore the system has infinitely many solutions (given that $\mathbb{R}$ is infinite).

2. A_2 has 5 columns. Therefore, the corresponding system is in 4 unknowns, and thus the solutions to it, if any exist, will be vectors in $\mathbb{Z}_{13}^4$.

A_2 is not in row echelon form; equivalently the corresponding system is not upper triangular/staircase. Indeed, the first non-zero entry of the first row and the first non-zero entry of the second row are both in the second column, which does not agree with the definition of a matrix in REF.

3. A_3 has 5 columns. Therefore, the corresponding system is in 4 unknowns, and thus the solutions to it, if any exist, will be vectors in $\mathbb{Z}_7^4$.

A_3 is in row echelon form, or equivalently the corresponding system is upper triangular/staircase. Indeed, all the rows of the matrix are non-zero, and the first non-zero entry of the first row is 4 in the first column, the first non-zero entry of the second row is -3 in the third column, the first non-zero entry of the third row is 4 in the fourth column, and the first non-zero entry of the fourth row is 3 in the last column; given that each such entry is to the right of the previous first non-zero entries, the matrix is indeed in REF and these entries are its pivots.

We finally observe that the last pivot being in the last column implies that the corresponding system is inconsistent.

4. A_4 has 6 columns. Therefore, the corresponding system is in 5 unknowns, and thus the solutions to it, if any exist, will be vectors in $\mathbb{Z}_7^5$.

A_4 is in row echelon form, or equivalently the corresponding system is upper triangular/staircase. Indeed, the only zero row of the matrix is the

last one, while the first non-zero entry of the first row is 3 in the first column, the first non-zero entry of the second row is 2 in the second column, and the first non-zero entry of the third row is 4 in the fourth column; given that each such entry is to the right of the previous first non-zero entries, the matrix is indeed in REF and these entries are its pivots.

We now observe that there is no pivot in the third, fifth and sixth columns. The latter shows that the corresponding system is consistent, while the former show that there are two free variables. Therefore the system has more than one solutions, and in fact has $7^2 = 49$ solutions (given that $|\mathbb{Z}_7| = 7$).

5. A_5 has 6 columns. Therefore, the corresponding system is in 5 unknowns, and thus the solutions to it, if any exist, will be vectors in $\mathbb{Q}^5$.

A_5 is in row echelon form, or equivalently the corresponding system is upper triangular/staircase. Indeed, all the rows of the matrix are non-zero, and the first non-zero entry of the first row is 2 in the first column, the first non-zero entry of the second row is 13 in the second column, the first non-zero entry of the third row is -99 in the third column, the first non-zero entry of the fourth row is 5 in the fourth column, and finally the first non-zero entry of the fifth row is 7 in the fifth column; given that each such entry is to the right of the previous first non-zero entries, the matrix is indeed in REF and these entries are its pivots.

We finally observe that there is no pivot in the last column, but there is a pivot in each of the remaining columns. These show that the corresponding system is consistent and has no free variables, therefore it has a unique solution.

Problem 6. (i) We have

$$A^2 = \begin{pmatrix} -8 & -7 & 2 \\ 59 & 1 & 25 \\ -14 & -16 & 7 \end{pmatrix}.$$

Next, we observe that it suffices to check that A is invertible in order to determine whether A^2 is invertible. Indeed we have the following

Claim. A^2 is invertible if and only if A is invertible. *(This claim can be proven in several different ways, although it is not necessary in this problem to give a proof; below one is given for completeness and it is based only on the definition of invertibility.)*

Proof of Claim. If A is invertible, then A^{-1} exists and we can check that $(A^2)^{-1} = A^{-1}A^{-1} = \left(A^{-1}\right)^2$ (this is a special case of Problem 1(iv) in this homework set).
Conversely, if A^2 is invertible, then there should exist $B \in \mathbb{R}^{3\times 3}$ such that $A^2B = I_3 = BA^2$. But this would imply that $A(AB) = I_3 = (BA)A$, so A would have both a right inverse C_1 ($C_1 = AB$ here) and a left inverse C_2 ($C_2 = BA$ here). But in such a case, the two inverses are equal given that

$$C_1 = I_3C_1 = (C_2A)C_1 = C_2(AC_1) = C_2I_3 = C_2.$$

Therefore A would be invertible too. □

We now check whether A is invertible. By one of the main theorems about matrix arithmetic, it suffices to check whether a Row Echelon Form of A has 3 pivots. But

$$A = \begin{pmatrix} 1 & -1 & 1 \\ 11 & 4 & 2 \\ 2 & -2 & 3 \end{pmatrix} \overset{\substack{R_2-11R_1 \\ R_3-2R_1}}{\sim} \begin{pmatrix} 1 & -1 & 1 \\ 0 & 15 & -9 \\ 0 & 0 & 1 \end{pmatrix},$$

and the last matrix is in REF and has 3 pivots. Therefore, A is invertible, and so is A^2.

(ii) We have

$$A^2 = \begin{pmatrix} 3 & 1 & 0 & 0 \\ 4 & 3 & 0 & 0 \\ 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Analogously to part (i), we observe that, in order to check whether A^2 is invertible, it would suffice to check if A is invertible. However here it may be

more efficient to work directly with A^2 (given that A^2 has more zero entries than A). We note that

$$A^2 = \begin{pmatrix} 3 & 1 & 0 & 0 \\ 4 & 3 & 0 & 0 \\ 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \xrightarrow[R_3 - R_1]{R_2 - 3R_1} \begin{pmatrix} 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \xrightarrow{R_2 \leftrightarrow R_4} \begin{pmatrix} 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Therefore, A^2 is not invertible since at least one Row Echelon Form of it does not have 4 pivots (in fact this shows that all Row Echelon Forms of A^2 have only 2 pivots).

Problem 7. In each of the fields we have discussed there is a neutral element of addition, denoted by 0, and a neutral element of multiplication, denoted by 1, which are different. In fact, given that $\mathbb{Z}_2$ is one of the fields we have discussed, and that $\mathbb{Z}_2$ only has two elements, this implies that 0 and 1 are the only elements we can be sure to have in the field.

Let $\mathbb{F}$ now be one of these fields, and let $0_{\mathbb{F}}$ be the neutral element of addition in $\mathbb{F}$, $1_{\mathbb{F}}$ be the neutral element of multiplication in $\mathbb{F}$. Consider the matrices

$$A = \begin{pmatrix} 0_{\mathbb{F}} & 1_{\mathbb{F}} \\ 0_{\mathbb{F}} & 0_{\mathbb{F}} \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 0_{\mathbb{F}} & 1_{\mathbb{F}} \\ 1_{\mathbb{F}} & 0_{\mathbb{F}} \end{pmatrix}.$$

Then

$$AB = \begin{pmatrix} 1_{\mathbb{F}} & 0_{\mathbb{F}} \\ 0_{\mathbb{F}} & 0_{\mathbb{F}} \end{pmatrix}, \qquad \text{while} \qquad BA = \begin{pmatrix} 0_{\mathbb{F}} & 0_{\mathbb{F}} \\ 0_{\mathbb{F}} & 1_{\mathbb{F}} \end{pmatrix}.$$

Since the $(1,1)$-entry of AB is different from the corresponding entry of BA, the two matrices are different.

Math 127
Homework Problem Set 4

Problem 1. (i) Consider the following matrices:

$$A = \begin{pmatrix} 1 & 1 & -4 \\ 11 & -5 & 7 \end{pmatrix} \in \mathbb{R}^{2\times 3}, \quad B = \begin{pmatrix} -1 & -2 \\ 10 & 9 \\ 8 & -6 \end{pmatrix} \in \mathbb{R}^{3\times 2}, \quad \bar{c} = \begin{pmatrix} 1 & -5 \end{pmatrix} \in \mathbb{R}^{1\times 2},$$

$$D = \begin{pmatrix} -3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 8 \end{pmatrix} \in \mathbb{R}^{3\times 3}, \quad E = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 2 & 2 \\ 1 & 0 & 3 \end{pmatrix} \in \mathbb{Z}_5^{3\times 3}, \quad \bar{u} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \in \mathbb{Z}_5^{3\times 1}.$$

Find all products of any two (different) matrices from above that make sense, as well as the following expressions, again if they are defined: $AB + I_2$, $A(I_3 + B)$, $AB\bar{c}$, $I_3 + (E^2 - E) \cdot (I_3 - E)^{-1}$ (is it possible to simplify any of the expressions you are asked to find, in order to do fewer and easier computations? can you simplify regardless of what the given matrices are?).

(ii) Using Gauss-Jordan elimination, check that only one of the following matrices is invertible and find its inverse:

$$A_1 = \begin{pmatrix} 1 & 1 & 6 & 4 \\ 2 & 3 & 2 & 5 \\ 2 & 2 & 2 & 2 \\ 3 & 2 & 5 & 4 \end{pmatrix} \in \mathbb{Z}_7^{4\times 4}, \qquad A_2 = \begin{pmatrix} 0.5 & -0.5 & 3 & 2 \\ -1 & 1.5 & -3 & -1 \\ 0 & 0.5 & 3 & 1 \\ -3 & 1 & 0 & -4 \end{pmatrix} \in \mathbb{R}^{4\times 4}.$$

Problem 2. We saw in class on an example that, if a real square matrix has a zero row, then it cannot be invertible. Prove the corresponding fact for square matrices that have a zero column.

That is, consider $n > 1$ and a matrix $A \in \mathbb{F}^{n\times n}$ (where $\mathbb{F} = \mathbb{R}$ or any other field out of the ones we have discussed so far), and suppose that A has at least one zero column. Prove that A is not invertible.

Problem 3. Prove the Distributive Law for matrices. That is, given a field $\mathbb{F}$ and positive integers m, n, k, l, prove that, for any matrices $A, B \in \mathbb{F}^{m\times n}$, $C \in \mathbb{F}^{n\times k}$ and $E \in \mathbb{F}^{l\times m}$, we have that

$$\big(A + B\big)C = AC + BC, \qquad E\big(A + B\big) = EA + EB.$$

[*Clarification.* Here you will have to rely on the axioms of a field to prove the desired conclusions.

Observe though that, already in the definition we gave of how we multiply two matrices with appropriate sizes, we used generalised associativity (in fact we already relied on this property when giving the definition of the dot product).

In other words, for this problem, and for similar problems about concepts like the dot product or multiplication of matrices (thus for all other problems in this homework set too), generalised associativity and generalised commutativity are among the basic properties we can now simply refer to (if we have to) and then apply.]

Problem 4. (i) Let $\mathbb{F}$ be a field, and let $U, U' \in \mathbb{F}^{n\times n}$ be two upper triangular matrices. Prove that $U + U'$ and UU' are also upper triangular.
(ii) Similarly, let $L, L' \in \mathbb{F}^{n\times n}$ be two lower triangular matrices. Prove that $L + L'$ and LL' are also lower triangular.

We have already seen in HW3 that multiplication of matrices in, say, $\mathbb{Z}_5^{2\times 2}$ is not commutative. The following problem allows us to generalise this conclusion to multiplication of matrices of any size.

We use the following **terminology**: if A, B are two matrices in $\mathbb{F}^{n\times n}$, we say that A, B *commute* if $AB = BA$.

Problem 5. (I) Let $n > 1$ and $\mathbb{F}$ a field. Show that any two diagonal matrices in $\mathbb{F}^{n\times n}$ commute.
(II) In the following two parts of the problem, the point is to come up with one or two examples of pairs of upper triangular matrices A, B in $\mathbb{Z}_5^{3\times 3}$ that **do not commute**.

(a) Can you pick the pair of matrices A, B so that none of the diagonal entries is 0? Justify your answer.

(b) Show that you can pick A, B so that at least for one of them the $(3, 3)$ entry is 0. [*Hint.* It may help to also revisit HW3, Pb7, and see if you could have worked with upper triangular matrices there.]

(III) Try to generalise what you did in part (II)b in order to also prove that, for any $n \geqslant 4$, multiplication of upper triangular matrices in $\mathbb{Z}_5^{n\times n}$ is not commutative.

The following problem is about a special class of square matrices with real entries, called *stochastic* matrices.

These matrices appear in numerous applications and are very useful in several areas of Mathematics and other disciplines (as for example Probability Theory, Statistics, Mathematical Finance, Communications Theory or Evolutionary Biology). They allow us to encode the possible ways in which certain probabilistic/stochastic phenomena can evolve over time, and how likely each of these ways is: for instance, questions like

"If we have a standard deck of 52 cards, how likely is it
for, say, 5 consecutive cards to be of the same colour or the same suit
after one shuffle of the deck, or two shuffles, or eight shuffles, and so on?"

can be answered with the use of stochastic matrices.

Problem 6. Let $n > 1$. A square matrix $Q = \left(q_{ij}\right)_{1 \leqslant i,j \leqslant n} \in \mathbb{R}^{n \times n}$ is called *stochastic* (or sometimes *row stochastic*) if:

- all the entries q_{ij} are non-negative numbers, and
- for each row the total sum of the entries contained in it is 1, that is, for every $1 \leqslant i_0 \leqslant n$,

$$\sum_{j=1}^{n} q_{i_0,j} = 1.$$

Consider a stochastic matrix $Q_3 \in \mathbb{R}^{3 \times 3}$, and show that $Q_3^2 = Q_3 \cdot Q_3$ is also stochastic. Moreover, show that the same is true for a stochastic matrix $Q_4 \in \mathbb{R}^{4 \times 4}$.

[*Remark.* This problem is a good instance of how we can rearrange a sum using generalised commutativity and associativity, with the purpose of simplifying it, when the summation is over more than one index.

Although the problem doesn't ask for this, is it possible to generalise your approach in order to prove the conclusion for a stochastic matrix of any size?]

Problem 7. (*Bonus problem: write your own proof!*) By adapting the proofs of Proposition 1 and of Theorem 1 that we discussed in class, prove the following important result:

Theorem. *Let $LS0$ be a homogeneous and underdetermined linear system with m non-trivial equations in n unknowns, and coefficients coming from a given field $\mathbb{F}$ (recall that underdetermined means that $n > m$).*

Prove that $LS0$ has at least one solution that is different from the trivial solution.

In other words:
(I) By adapting the proof of Theorem 1, show that $LS0$ can be replaced by an equivalent homogeneous and underdetermined upper triangular/staircase system $LS1$ via finitely many applications of Gaussian elimination.

[Note that you no longer need to prove that every type of application of Gaussian elimination gives an equivalent system to $LS0$, as this follows from Theorem 1 for an arbitrary linear system (without requiring the additional properties of $LS0$); however you should analyse what Gaussian elimination does to a homogeneous system.]

(II) By relying on the proof of Proposition 1, justify why the homogeneous and underdetermined upper triangular/staircase system $LS1$ has more than one solutions, and hence at least one solution different from the trivial one.

Math 127
Suggested solutions to Homework Set 4

Problem 1. (i) The products $A\bar{c}$, $B\bar{c}$, BD, $\bar{c}B$, $\bar{c}D$, DA, $D\bar{c}$ and $\bar{u}E$ are not defined because the dimensions don't match. Similarly, the products AE, EA, BE, EB, $\bar{c}E$, $E\bar{c}$, DE, ED, $A\bar{u}$, $\bar{u}A$, $B\bar{u}$, $\bar{u}B$, $\bar{c}\bar{u}$, $\bar{u}\bar{c}$, $D\bar{u}$, $\bar{u}D$ are not defined simply because the entries of the matrices we are trying to multiply in each case come from different fields none of which is a subfield of the other.

Thus the only products that are defined are the following:

$$AB = \begin{pmatrix} -23 & 31 \\ -5 & -109 \end{pmatrix}, \quad BA = \begin{pmatrix} -23 & 9 & -10 \\ 109 & -35 & 23 \\ -58 & 38 & -74 \end{pmatrix},$$

$$\bar{c}A = \begin{pmatrix} -54 & 26 & -39 \end{pmatrix}, \quad AD = \begin{pmatrix} -3 & 2 & -32 \\ -33 & -10 & 56 \end{pmatrix},$$

$$DB = \begin{pmatrix} 3 & 6 \\ 20 & 18 \\ 64 & -48 \end{pmatrix}, \quad \text{and} \quad E\bar{u} = \begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix}.$$

Moreover, $A(I_3 + B)$ is not defined because $I_3 + B$ is not defined given that B does not have the same number of columns as I_3. Similarly, $AB\bar{c}$ is not defined because AB has 2 columns while $\bar{c}$ has 1 row.

On the other hand,

$$AB + I_2 = \begin{pmatrix} -22 & 31 \\ -5 & -108 \end{pmatrix}.$$

Finally, if we can show that $I_3 - E$ is invertible, then the last expression will make sense, and we will be able to write

$$\begin{aligned} I_3 + (E^2 - E) \cdot (I_3 - E)^{-1} &= I_3 + E(E - I_3) \cdot (I_3 - E)^{-1} \\ &= I_3 + E \cdot \big((-1) \cdot (I_3 - E)\big) \cdot (I_3 - E)^{-1} = I_3 - E \end{aligned}$$

where we used associativity and the distributive law for matrix multiplication as well as properties of multiplication of a matrix by a scalar following from Question 3 of the Review and Practice File for the 2nd Midterm.

Thus it remains to check whether $I_3 - E$ is invertible. But

$$I_3 - E = \begin{pmatrix} 0 & 1 & 0 \\ 0 & -1 & -2 \\ -1 & 0 & -2 \end{pmatrix} \sim \begin{pmatrix} -1 & 0 & -2 \\ 0 & -1 & -2 \\ 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} -1 & 0 & -2 \\ 0 & -1 & -2 \\ 0 & 0 & -2 \end{pmatrix} = \begin{pmatrix} 4 & 0 & 3 \\ 0 & 4 & 3 \\ 0 & 0 & 3 \end{pmatrix},$$

so there exists a Row Echelon Form of $I_3 - E$ with 3 pivots, showing the matrix is invertible.

(ii) We have that

$$\left(\begin{array}{cccc|cccc} 1 & 1 & 6 & 4 & 1 & 0 & 0 & 0 \\ 2 & 3 & 2 & 5 & 0 & 1 & 0 & 0 \\ 2 & 2 & 2 & 2 & 0 & 0 & 1 & 0 \\ 3 & 2 & 5 & 4 & 0 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|cccc} 1 & 1 & 6 & 4 & 1 & 0 & 0 & 0 \\ 0 & 1 & -3 & 4 & -2 & 1 & 0 & 0 \\ 0 & 0 & -3 & 1 & -2 & 0 & 1 & 0 \\ 0 & -1 & 1 & -1 & -3 & 0 & 0 & 1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccc|cccc} 1 & 1 & 6 & 4 & 1 & 0 & 0 & 0 \\ 0 & 1 & -3 & 4 & -2 & 1 & 0 & 0 \\ 0 & 0 & -3 & 1 & -2 & 0 & 1 & 0 \\ 0 & 0 & -2 & 3 & -5 & 1 & 0 & 1 \end{array}\right) = \left(\begin{array}{cccc|cccc} 1 & 1 & 6 & 4 & 1 & 0 & 0 & 0 \\ 0 & 1 & 4 & 4 & 5 & 1 & 0 & 0 \\ 0 & 0 & 4 & 1 & 5 & 0 & 1 & 0 \\ 0 & 0 & 5 & 3 & 2 & 1 & 0 & 1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccc|cccc} 1 & 1 & 6 & 4 & 1 & 0 & 0 & 0 \\ 0 & 1 & 4 & 4 & 5 & 1 & 0 & 0 \\ 0 & 0 & 4 & 1 & 5 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 4 & 1 \end{array}\right),$$

therefore A_1 is not invertible because it has a Row Echelon Form with fewer than 4 pivots.

On the other hand,

$$\left(\begin{array}{cccc|cccc} 0.5 & -0.5 & 3 & 2 & 1 & 0 & 0 & 0 \\ -1 & 1.5 & -3 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0.5 & 3 & 1 & 0 & 0 & 1 & 0 \\ -3 & 1 & 0 & -4 & 0 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|cccc} 0.5 & -0.5 & 3 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0.5 & 3 & 3 & 2 & 1 & 0 & 0 \\ 0 & 0.5 & 3 & 1 & 0 & 0 & 1 & 0 \\ 0 & -2 & 18 & 8 & 6 & 0 & 0 & 1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccc|cccc} 0.5 & -0.5 & 3 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0.5 & 3 & 3 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & -2 & -2 & -1 & 1 & 0 \\ 0 & 0 & 30 & 20 & 14 & 4 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|cccc} 0.5 & -0.5 & 3 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0.5 & 3 & 3 & 2 & 1 & 0 & 0 \\ 0 & 0 & 3 & 2 & 1.4 & 0.4 & 0 & 0.1 \\ 0 & 0 & 0 & -2 & -2 & -1 & 1 & 0 \end{array}\right),$$

thus A_2 is invertible.

Moreover, to find its inverse we continue to do elementary row operations until we get to its RREF, which should be I_4:

$$\left(\begin{array}{cccc|cccc} 0.5 & -0.5 & 3 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0.5 & 3 & 3 & 2 & 1 & 0 & 0 \\ 0 & 0 & 3 & 2 & 1.4 & 0.4 & 0 & 0.1 \\ 0 & 0 & 0 & -2 & -2 & -1 & 1 & 0 \end{array}\right) \sim \left(\begin{array}{cccc|cccc} 0.5 & -0.5 & 3 & 0 & -1 & -1 & 1 & 0 \\ 0 & 0.5 & 3 & 0 & -1 & -0.5 & 1.5 & 0 \\ 0 & 0 & 3 & 0 & -0.6 & -0.6 & 1 & 0.1 \\ 0 & 0 & 0 & -2 & -2 & -1 & 1 & 0 \end{array}\right)$$

$$\sim \left(\begin{array}{cccc|cccc} 0.5 & -0.5 & 0 & 0 & -0.4 & -0.4 & 0 & -0.1 \\ 0 & 0.5 & 0 & 0 & -0.4 & 0.1 & 0.5 & -0.1 \\ 0 & 0 & 3 & 0 & -0.6 & -0.6 & 1 & 0.1 \\ 0 & 0 & 0 & -2 & -2 & -1 & 1 & 0 \end{array}\right)$$

$$\sim \left(\begin{array}{cccc|cccc} 0.5 & 0 & 0 & 0 & -0.8 & -0.3 & 0.5 & -0.2 \\ 0 & 0.5 & 0 & 0 & -0.4 & 0.1 & 0.5 & -0.1 \\ 0 & 0 & 3 & 0 & -0.6 & -0.6 & 1 & 0.1 \\ 0 & 0 & 0 & -2 & -2 & -1 & 1 & 0 \end{array}\right) \sim \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & -1.6 & -0.6 & 1 & -0.4 \\ 0 & 1 & 0 & 0 & -0.8 & 0.2 & 1 & -0.2 \\ 0 & 0 & 1 & 0 & -0.2 & -0.2 & \frac{1}{3} & \frac{1}{30} \\ 0 & 0 & 0 & 1 & 1 & 0.5 & -0.5 & 0 \end{array}\right).$$

In conclusion,

$$A_2^{-1} = \begin{pmatrix} -1.6 & -0.6 & 1 & -0.4 \\ -0.8 & 0.2 & 1 & -0.2 \\ -0.2 & -0.2 & \frac{1}{3} & \frac{1}{30} \\ 1 & 0.5 & -0.5 & 0 \end{pmatrix}.$$

Problem 2. Let $n > 1$ and consider a matrix $A \in \mathbb{F}^{n\times n}$ with at least one zero column. Let j_0, $1 \leqslant j_0 \leqslant n$, be such that $A_{\cdot,j_0}$ is a zero column.

Consider now an arbitrary matrix $B \in \mathbb{F}^{n\times n}$, and let us write $A = \big(a_{ij}\big)_{1\leqslant i,j\leqslant n}$, $B = \big(b_{ij}\big)_{1\leqslant i,j\leqslant n}$.

The (j_0, j_0)-entry of the matrix BA is equal to

$$\sum_{s=1}^{n} b_{j_0,s}a_{s,j_0} = \sum_{s=1}^{n} b_{j_0,s} \cdot 0 = 0.$$

Therefore, $BA \neq I_n$, since the (j_0, j_0)-entry of I_n is equal to 1. Since B was arbitrary, this shows that no matrix in $\mathbb{F}^{n\times n}$ can be the multiplicative inverse of A, and therefore that A is not invertible.

Problem 3. Consider matrices $A, B \in \mathbb{F}^{m\times n}$ and $C \in \mathbb{F}^{n\times k}$. Write

$$A = \big(a_{ij}\big)_{\substack{1\leqslant i\leqslant m,\\ 1\leqslant j\leqslant n}} \quad B = \big(b_{ij}\big)_{\substack{1\leqslant i\leqslant m,\\ 1\leqslant j\leqslant n}} \quad \text{and} \quad C = \big(c_{rs}\big)_{\substack{1\leqslant r\leqslant n.\\ 1\leqslant s\leqslant k}}$$

Then $A + B = \big(a_{ij} + b_{ij}\big)_{\substack{1\leqslant i\leqslant m,\\ 1\leqslant j\leqslant n}}$, and therefore the product $(A + B)C$ is defined and is in $\mathbb{F}^{m\times k}$. Fix $1 \leqslant i \leqslant m$ and $1 \leqslant s \leqslant k$. The (i, s)-entry of $(A + B)C$ is equal to

$$\sum_{j=1}^{n}(a_{ij} + b_{ij})c_{js}. \tag{1}$$

Moving on, AC and BC are also defined and they are both in $\mathbb{F}^{m\times k}$. The (i, s)-entry of AC is equal to $\sum_{j=1}^{n} a_{ij}c_{js}$, while the (i, s)-entry of BC is equal to $\sum_{j=1}^{n} b_{ij}c_{js}$. Therefore the (i, s)-entry of $AC + BC$ is equal to

$$\left(\sum_{j=1}^{n} a_{ij}c_{js}\right) + \left(\sum_{j=1}^{n} b_{ij}c_{js}\right). \tag{2}$$

We now compare (1) and (2): by the distributive law in $\mathbb{F}$, we have that

$$\sum_{j=1}^{n}(a_{ij} + b_{ij})c_{js} = \sum_{j=1}^{n}\big(a_{ij}c_{js} + b_{ij}c_{js}\big)$$

which, by generalised commutativity and associativity in $\mathbb{F}$, is in turn

$$= \left(\sum_{j=1}^{n} a_{ij}c_{js}\right) + \left(\sum_{j=1}^{n} b_{ij}c_{js}\right).$$

In other words, the (i, s)-entry of $(A + B)C$ is equal to the (i, s)-entry of $AC + BC$. Since the indices i and s were arbitrary, we conclude that every entry of $(A+B)C$ is equal to the corresponding entry of $AC+BC$, and thus that $(A + B)C = AC + BC$.

Next we also consider a matrix $E \in \mathbb{F}^{l\times m}$ and write

$$E = \big(e_{tu}\big)_{\substack{1\leqslant t\leqslant l\\ 1\leqslant u\leqslant m}}.$$

$E(A + B)$ is defined and is in $\mathbb{F}^{l\times n}$. Fix $1 \leqslant t \leqslant l$ and $1 \leqslant j \leqslant n$. Then the (t, j)-entry of $E(A + B)$ is equal to

$$\sum_{u=1}^{m} e_{tu}(a_{uj} + b_{uj}). \tag{3}$$

Similarly EA and EB are defined and they are in $\mathbb{F}^{l\times n}$. The (t,j)-entry of EA is equal to $\sum_{u=1}^{m} e_{tu}a_{uj}$, while the (t,j)-entry of EB is equal to $\sum_{u=1}^{m} e_{tu}b_{uj}$. Therefore the (t,j)-entry of $EA+EB$ is equal to

$$\left(\sum_{u=1}^{m} e_{tu}a_{uj}\right) + \left(\sum_{u=1}^{m} e_{tu}b_{uj}\right). \tag{4}$$

We now compare (3) and (4): by the distributive law in $\mathbb{F}$, we have that

$$\sum_{u=1}^{m} e_{tu}(a_{uj}+b_{uj}) = \sum_{u=1}^{m}\left(e_{tu}a_{uj}+e_{tu}b_{uj}\right)$$

which, by generalised commutativity and associativity in $\mathbb{F}$, is in turn

$$= \left(\sum_{u=1}^{m} e_{tu}a_{uj}\right) + \left(\sum_{u=1}^{m} e_{tu}b_{uj}\right).$$

In other words, the (t,j)-entry of $E(A+B)$ is equal to the (t,j)-entry of $EA+EB$. Since the indices t and j were arbitrary, we conclude that every entry of $E(A+B)$ is equal to the corresponding entry of $EA+EB$, and thus that $E(A+B)=EA+EB$.

Problem 4. (i) Consider two upper triangular matrices $U, U' \in \mathbb{F}^{n\times n}$, and write

$$U = \big(u_{ij}\big)_{1\leqslant i,j\leqslant n}, \qquad U' = \big(u'_{ij}\big)_{1\leqslant i,j\leqslant n}.$$

By the definition of upper triangular matrix, we know that $u_{ij} = 0 = u'_{ij}$ if $i > j$.

We set $A = U + U'$, $B = UU'$, and we write

$$A = \big(a_{ij}\big)_{1\leqslant i,j\leqslant n}, \qquad B = \big(b_{ij}\big)_{1\leqslant i,j\leqslant n}.$$

To check that both A and B are upper triangular, we use the definition again: we need to check that $a_{ij} = 0$ if $i > j$, and similarly that $b_{ij} = 0$ if $i > j$.

But whenever $i > j$ we have that $a_{ij} = u_{ij} + u'_{ij} = 0 + 0 = 0$, thus we can conclude that A is upper triangular.

On the other hand,

$$\begin{aligned} b_{ij} = \sum_{r=1}^{n} u_{ir}u'_{rj} &= \sum_{\substack{1\leqslant r\leqslant n\\ i>r}} u_{ir}u'_{rj} + \sum_{\substack{1\leqslant r\leqslant n\\ i\leqslant r}} u_{ir}u'_{rj} \\ &= \sum_{\substack{1\leqslant r\leqslant n\\ i>r}} 0\cdot u'_{rj} + \sum_{\substack{1\leqslant r\leqslant n\\ i\leqslant r}} u_{ir}u'_{rj} = \sum_{\substack{1\leqslant r\leqslant n\\ i\leqslant r}} u_{ir}u'_{rj}. \end{aligned}$$

It remains to note that, **if $i > j$**, then $r \geqslant i$ implies that $r > j$, therefore the final sum above is also equal to 0:

$$b_{ij} = \sum_{\substack{1\leqslant r\leqslant n\\ i>r}} u_{ir}u'_{rj} + \sum_{\substack{1\leqslant r\leqslant n\\ i\leqslant r}} u_{ir}u'_{rj} = \sum_{\substack{1\leqslant r\leqslant n\\ i\leqslant r}} u_{ir}u'_{rj} = \sum_{\substack{1\leqslant r\leqslant n\\ i\leqslant r}} u_{ir}\cdot 0 = 0.$$

We conclude that B is upper triangular too.

(ii) Consider two lower triangular matrices $L, L' \in \mathbb{F}^{n\times n}$. Our proof here will be completely analogous to the above argument. We write

$$L = \big(l_{ij}\big)_{1\leqslant i,j\leqslant n}, \qquad L' = \big(l'_{ij}\big)_{1\leqslant i,j\leqslant n}.$$

By the definition of lower triangular matrix, we know that $l_{ij} = 0 = l'_{ij}$ if $i < j$.

We set $C = L + L'$, $E = LL'$, and we write

$$C = \big(c_{ij}\big)_{1\leqslant i,j\leqslant n}, \qquad E = \big(e_{ij}\big)_{1\leqslant i,j\leqslant n}.$$

To check that both C and E are lower triangular, we use the definition again: we need to check that $c_{ij} = 0$ if $i < j$, and similarly that $e_{ij} = 0$ if $i < j$.

But whenever $i < j$ we have that $c_{ij} = l_{ij} + l'_{ij} = 0 + 0 = 0$, thus we can conclude that C is lower triangular.

On the other hand,

$$\begin{aligned} e_{ij} = \sum_{r=1}^{n} l_{ir} l'_{rj} &= \sum_{\substack{1 \leqslant r \leqslant n \\ i < r}} l_{ir} l'_{rj} + \sum_{\substack{1 \leqslant r \leqslant n \\ i \geqslant r}} l_{ir} l'_{rj} \\ &= \sum_{\substack{1 \leqslant r \leqslant n \\ i < r}} 0 \cdot l'_{rj} + \sum_{\substack{1 \leqslant r \leqslant n \\ i \geqslant r}} l_{ir} l'_{rj} = \sum_{\substack{1 \leqslant r \leqslant n \\ i \geqslant r}} l_{ir} l'_{rj}. \end{aligned}$$

It remains to note that, **if $\boldsymbol{i < j}$**, then $r \leqslant i$ implies that $r < j$, therefore the final sum above is also equal to 0:

$$e_{ij} = \sum_{\substack{1 \leqslant r \leqslant n \\ i < r}} l_{ir} l'_{rj} + \sum_{\substack{1 \leqslant r \leqslant n \\ i \geqslant r}} l_{ir} l'_{rj} = \sum_{\substack{1 \leqslant r \leqslant n \\ i \geqslant r}} l_{ir} l'_{rj} = \sum_{\substack{1 \leqslant r \leqslant n \\ i \geqslant r}} l_{ir} \cdot 0 = 0.$$

We conclude that E is lower triangular too.

Problem 5. (I) Suppose $D, D' \in \mathbb{F}^{n\times n}$ are two diagonal matrices. Write

$$D = (d_{ij})_{1\leqslant i,j\leqslant n}\,, \qquad D = \left(d'_{ij}\right)_{1\leqslant i,j\leqslant n}$$

and recall that $d_{ij} = 0 = d'_{ij}$ if $i \neq j$.

We first observe that DD' and $D'D$ are both diagonal matrices. We could check this directly, or we could refer to Problem 4 of this homework: we recall that a matrix is diagonal if and only if it is both upper triangular and lower triangular.

But then we know that D and D' are upper triangular, so as we showed in Problem 4 the matrices DD' and $D'D$ are upper triangular. Similarly, we can conclude that the latter matrices are lower triangular, therefore in the end DD' and $D'D$ are both diagonal.

It now suffices to check that the corresponding entries of DD' and $D'D$ on the diagonal coincide: consider $1 \leqslant i \leqslant n$ and note that the (i,i)-entry of DD' is the dot product of the i-th row of D and the i-th column of D', that is, the (i,i)-entry of DD' is equal to

$$\sum_{r=1}^{n} d_{ir}d'_{ri} = d_{ii}d'_{ii} + \sum_{r\neq i} d_{ir}d'_{ri} = d_{ii}d'_{ii}.$$

Similarly the (i,i)-entry of $D'D$ is equal to

$$\sum_{r=1}^{n} d'_{ir}d_{ri} = d'_{ii}d_{ii} + \sum_{r\neq i} d'_{ir}d_{ri} = d'_{ii}d_{ii}.$$

By commutativity of multiplication in $\mathbb{F}$, we have that $d_{ii}d'_{ii} = d'_{ii}d_{ii}$.

Since i was arbitrary, we conclude that the corresponding diagonal entries of DD' and $D'D$ coincide, and hence that the matrices are equal.

(II) (a) The answer is yes. Suppose

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then

$$AB = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{while} \quad BA = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Therefore $AB \neq BA$.

(b) Set

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Then

$$AB = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \text{while} \quad BA = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Therefore $AB \neq BA$.

(III) We will use the matrices A, B from part (b) to create larger upper triangular matrices $\widetilde{A}, \widetilde{B}$ contained in $\mathbb{Z}_5^{n\times n}$ that do not commute either.

Set

$$\widetilde{A} = \left(\begin{array}{ccc|ccc} & & & 0 & \cdots & 0 \\ & A & & 0 & \ddots & 0 \\ & & & 0 & \cdots & 0 \\ \hline 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{array}\right) = \left(\begin{array}{ccc|ccc} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 \\ \hline 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{array}\right)$$

and $\widetilde{B} = \left(\begin{array}{ccc|ccc} & & & 0 & \cdots & 0 \\ & B & & 0 & \ddots & 0 \\ & & & 0 & \cdots & 0 \\ \hline 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{array}\right) = \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 \\ \hline 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{array}\right).$

We can check that

$$\widetilde{A}\widetilde{B} = \left(\begin{array}{ccc|ccc} & & & 0 & \cdots & 0 \\ & AB & & 0 & \ddots & 0 \\ & & & 0 & \cdots & 0 \\ \hline 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{array}\right) \neq \left(\begin{array}{ccc|ccc} & & & 0 & \cdots & 0 \\ & BA & & 0 & \ddots & 0 \\ & & & 0 & \cdots & 0 \\ \hline 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{array}\right) = \widetilde{B}\widetilde{A}.$$

More simply, the $(1,2)$-entry of $\widetilde{A}\widetilde{B}$ is the dot product of the 1st row of $\widetilde{A}$ and the 2nd column of $\widetilde{B}$, so it is equal to 0, while the $(1,2)$-entry of $\widetilde{B}\widetilde{A}$ is the dot product of the 1st row of $\widetilde{B}$ and the 2nd column of $\widetilde{A}$, so it is equal to 1. This shows that the two products cannot be equal.

Problem 6. We suppose $Q_3 \in \mathbb{R}^{3\times 3}$ is a stochastic matrix, and we write

$$Q_3 = \big(q_{ij}\big)_{1\leqslant i,j\leqslant 3}.$$

Consider $1 \leqslant i_0 \leqslant 3$. For each $1 \leqslant j \leqslant 3$, the (i_0, j)-entry of $Q_3^2 = Q_3 \cdot Q_3$ is by definition equal to

$$\sum_{s=1}^{3} q_{i_0,s} q_{s,j}.$$

Therefore, to verify that Q_3^2 is stochastic, we need to check that

$$\sum_{j=1}^{3} \left(\sum_{s=1}^{3} q_{i_0,s} q_{s,j} \right) = 1.$$

But because of generalised commutativity and associativity in $\mathbb{R}$, we could sum over the index j first:

$$\begin{aligned} \sum_{j=1}^{3} \left(\sum_{s=1}^{3} q_{i_0,s} q_{s,j} \right) &= \sum_{j=1}^{3} \sum_{s=1}^{3} q_{i_0,s} q_{s,j} \\ &= \sum_{s=1}^{3} \sum_{j=1}^{3} q_{i_0,s} q_{s,j} = \sum_{s=1}^{3} q_{i_0,s} \cdot \left(\sum_{j=1}^{3} q_{s,j} \right), \end{aligned}$$

where the latter equality follows by distributivity because $q_{i_0,s}$ is a common factor in the inner sum.

We now use the assumption that Q_3 is stochastic: for every $1 \leqslant s \leqslant 3$, this gives that $\sum_{j=1}^{3} q_{s,j} = 1$.

We can thus continue rewriting the double sum we started with as follows:

$$\sum_{j=1}^{3} \left(\sum_{s=1}^{3} q_{i_0,s} q_{s,j} \right) = \sum_{s=1}^{3} q_{i_0,s} \cdot \left(\sum_{j=1}^{3} q_{s,j} \right) = \sum_{s=1}^{3} q_{i_0,s} \cdot 1 = \sum_{s=1}^{3} q_{i_0,s} = 1,$$

where we use the assumption that Q_3 is a stochastic matrix one more time.

The proof of the corresponding fact for a stochastic matrix $Q_4 \in \mathbb{R}^{4\times 4}$ is completely analogous: write

$$Q_4 = \big(\tilde{q}_{ij}\big)_{1\leqslant i,j\leqslant 4}.$$

Consider $1 \leqslant i_0 \leqslant 4$. For each $1 \leqslant j \leqslant 4$, the (i_0, j)-entry of $Q_4^2 = Q_4 \cdot Q_4$ is by definition equal to

$$\sum_{s=1}^{4} \tilde{q}_{i_0,s} \tilde{q}_{s,j}.$$

Therefore, to verify that Q_4^2 is stochastic, we need to check that

$$\sum_{j=1}^{4}\left(\sum_{s=1}^{4}\tilde{q}_{i_0,s}\tilde{q}_{s,j}\right)=1.$$

But because of generalised commutativity and associativity in $\mathbb{R}$, we could sum over the index j first:

$$\begin{aligned}\sum_{j=1}^{4}\left(\sum_{s=1}^{4}\tilde{q}_{i_0,s}\tilde{q}_{s,j}\right)&=\sum_{j=1}^{4}\sum_{s=1}^{4}\tilde{q}_{i_0,s}\tilde{q}_{s,j}\\&=\sum_{s=1}^{4}\sum_{j=1}^{4}\tilde{q}_{i_0,s}\tilde{q}_{s,j}=\sum_{s=1}^{4}\tilde{q}_{i_0,s}\cdot\left(\sum_{j=1}^{4}\tilde{q}_{s,j}\right),\end{aligned}$$

where the latter equality follows by distributivity because $\tilde{q}_{i_0,s}$ is a common factor in the inner sum.

We now use the assumption that Q_4 is stochastic: for every $1\leqslant s\leqslant 4$, this gives that $\sum_{j=1}^{4}\tilde{q}_{s,j}=1$.

We can thus continue rewriting the double sum we started with as follows:

$$\sum_{j=1}^{4}\left(\sum_{s=1}^{4}\tilde{q}_{i_0,s}\tilde{q}_{s,j}\right)=\sum_{s=1}^{4}\tilde{q}_{i_0,s}\cdot\left(\sum_{j=1}^{4}\tilde{q}_{s,j}\right)=\sum_{s=1}^{4}\tilde{q}_{i_0,s}\cdot 1=\sum_{s=1}^{4}\tilde{q}_{i_0,s}=1,$$

where we use the assumption that Q_4 is a stochastic matrix one more time.

Side note: It may have become clear by now that we only need to slightly adjust the (very similar) arguments above in order to justify the most general analogous statement we can get here, that for every $n\geqslant 2$ and every stochastic matrix $Q\in\mathbb{R}^{n\times n}$, the matrix Q^2 is also stochastic.

Indeed, fix some $n\geqslant 2$ and consider a stochastic matrix $Q\in\mathbb{R}^{n\times n}$. For notational convenience, write

$$Q=\left(q_{ij}\right)_{1\leqslant i,j\leqslant n}.$$

For every $1\leqslant i_0\leqslant n$, and every $1\leqslant j\leqslant n$, the (i_0,j)-entry of Q^2 is

$$\sum_{s=1}^{n}q_{i_0,s}q_{s,j}.$$

Therefore, we need to check that

$$\sum_{j=1}^{n}\left(\sum_{s=1}^{n}q_{i_0,s}q_{s,j}\right)=1.$$

But

$$\begin{aligned}
\sum_{j=1}^{n}\left(\sum_{s=1}^{n} q_{i_0,s}q_{s,j}\right) &= \sum_{s=1}^{n}\sum_{j=1}^{n} q_{i_0,s}q_{s,j} \\
&= \sum_{s=1}^{n} q_{i_0,s}\cdot\left(\sum_{j=1}^{n} q_{s,j}\right) && \text{(the entries of the } s\text{-th row of } Q \text{ add up to 1)} \\
&= \sum_{s=1}^{n} q_{i_0,s}\cdot 1 = \sum_{s=1}^{n} q_{i_0,s} = 1. && \text{(the entries of the } i_0\text{-th row of } Q \text{ add up to 1)}
\end{aligned}$$

This completes the proof of the general statement.

Problem 7. (I) Let us write

$$LS0: \left\{ \begin{array}{ccc} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = & 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n & = & 0 \\ \vdots \qquad\qquad \ddots \qquad\qquad \vdots & & \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & = & 0 \end{array} \right\}.$$

We first show that any application of the method of Gaussian elimination replaces the homogeneous and underdetermined linear system $LS0$ by another homogeneous and underdetermined linear system.

Case 1: If we use a Type 1 operation, say we multiply the i-th equation Eq_i by a non-zero constant c, the i-th equation of the new system is

$$c\big(a_{i1}x_1+a_{i2}x_2+\cdots+a_{in}x_n\big) = c\cdot 0 \;\Leftrightarrow\; ca_{i1}x_1+ca_{i2}x_2+\cdots+ca_{in}x_n = 0.$$

Therefore the constant term of this equation is again 0, while all the other equations are the same as in $LS0$, so their constant terms are 0 too. In other words, the new system is homogeneous. At the same time, it is underdetermined because the number of equations remains the same, and is less than the number of unknowns.

Case 2: If we use a Type 2 operation, say we replace the i-th equation Eq_i by $Eq_i - dEq_j$, where $j \neq i$ and d is some element of $\mathbb{F}$, then the i-th equation of the new system is

$$\begin{aligned} &\big(a_{i1}x_1+a_{i2}x_2+\cdots+a_{in}x_n\big)-d\big(a_{j1}x_1+a_{j2}x_2+\cdots+a_{jn}x_n\big) = 0-d\cdot 0 \\ &\quad\Leftrightarrow\quad (a_{i1}-da_{j1})x_1 + (a_{i2}-da_{j2})x_2 + \cdots + (a_{in}-da_{jn})x_n = 0. \end{aligned}$$

Therefore its constant term is 0. Again, all the other equations are the equations Eq_r, $r \neq i$, of $LS0$, so their constant terms are also 0. Therefore, the new system is homogeneous as well.

Finally, since we replace Eq_i by the equation above, while we keep the remaining equations, their number of non-trivial equations doesn't increase (it either stays the same, or it can happen that the new Eq_i is trivial), and thus the new system is underdetermined again.

Case 3: If we use a Type 3 operation, say we swap the positions of Eq_i and Eq_j, then the equations we have are the same as before, they are just given in a different order. Therefore, all the constant terms are still 0, and the new system is homogeneous and underdetermined.

Observe now that the only assumptions we used about $LS0$ are the assumptions that it is homogeneous and underdetermined. Therefore, we essentially showed that any application of Gaussian elimination replaces a homogeneous and underdetermined linear system with m non-trivial equations by another homogeneous and underdetermined linear system with at most m non-trivial equations in the same set of unknowns.

We now recall that Theorem 1 states that we can replace $LS0$ by an equivalent upper triangular/staircase system $LS1$ via finitely many applications of Gaussian elimination.

By what we showed above, after the first application we will have a new homogeneous and underdetermined system (with at most m non-trivial equations in our n unknowns), while similarly if at some step we have ended up with a homogeneous system with at most m non-trivial equations in these n unknowns, at the next step we will have another homogeneous system with at most m non-trivial equations in the same unknowns. By induction, it follows that $LS1$ is also homogeneous and has at most m non-trivial equations, so it is underdetermined too.

(II) By part (I) we know that $LS0$ is equivalent to an upper triangular/staircase system $LS1$ which is homogeneous and underdetermined, so it suffices to show that $LS1$ has more than one solutions.

Given that $LS1$ is homogeneous, the last column, that is, the column of constant terms, contains only zero entries, therefore we cannot have a pivot there. But by Proposition 1 we know then that $LS1$ is consistent.

Moreover, we know that the number of pivots in a staircase system equals the number of non-trivial equations. Therefore, $LS1$ can have at most m pivots. But since the number of unknowns is $n > m$, there exists at least one unknown which has no pivot coefficient (otherwise the number of pivots should be $\geqslant n > m$, which we just explained cannot happen). In other words, there exists at least one free variable, say the variable x_i for some $1 \leqslant i \leqslant n$, and by Proposition 1 again we know that, if we assign **a non-zero value** to x_i (and also choose values for any other free variables we have), we can then find a solution to $LS1$. Such a solution will necessarily be different from the trivial solution (given that we set x_i equal to a non-zero element).

Math 127
Homework Problem Set 5

In the first problem you are given six statements, for each one of which you are asked to decide whether it is correct or not, and to give a rigorous justification for your answer. All the statements begin in a very similar way (with the quantifier "for every"), but be careful that different statements may require a substantially different approach/proof technique. The primary goal of the problem is to have you recognise what you need to prove and what is a suitable way of proving it in each case.

For this problem, we use the following convention: **Type 1 elementary matrices** are all those elementary matrices that correspond to multiplying a row by a non-zero constant, **Type 2 elementary matrices** are those that correspond to adding a multiple of one row to another row, and **Type 3 elementary matrices** are those that correspond to swapping two rows.

Problem 1. TRUE OR FALSE? For each of the following statements, decide whether it is correct or not, and give a proof of the statement or of its negation accordingly. $\mathbb{F}$ could be any of the fields we have discussed.

1. Every two Type 3 elementary matrices in $\mathbb{F}^{2\times 2}$ commute.
2. Every two Type 3 elementary matrices in $\mathbb{F}^{3\times 3}$ commute.
3. For every two elementary matrices A, B in $\mathbb{Z}_5^{15\times 15}$ we have that, if A and B are both Type 1 or both Type 2, then $AB = BA$.
4. For every upper triangular matrix $U \in \mathbb{R}^{6\times 6}$ and for every $\bar{b} \in \mathbb{R}^{6\times 1}$, we have that $(U \mid \bar{b})$ corresponds to an upper triangular system.
5. For every upper triangular matrix $U' \in \mathbb{R}^{6\times 6}$ and for every $\bar{b} \in \mathbb{R}^{6\times 1}$, we have that, if all diagonal entries of U' are non-zero, then $(U' \mid \bar{b})$ corresponds to an upper triangular system.
6. For every Type 1 elementary matrix $A \in \mathbb{R}^{4\times 4}$, there is a Type 2 elementary matrix $B \in \mathbb{R}^{4\times 4}$ such that $B \neq I_4$, and such that $AB = BA$.

In mathematics, a *relation* $\mathcal{R}$ on a non-empty set S is a mathematical concept allowing us to "link" certain elements of S (possibly motivated by a certain interesting property we want to study, and which is supposed to be shared by "linked" elements, and not shared by elements that have not been "linked").

Formally, a (binary) relation $\mathcal{R}$ on S is a subset of $S \times S$, that is, it is a set of ordered pairs with components from S. For instance, $\mathcal{R}_1 = \{(m,n) : m, n \in \mathbb{N},\ m \text{ divides } n\}$ is a relation on $\mathbb{N}$, while $\mathcal{R}_2 = \{(0,1),(1,2),(2,4),(3,3)\}$ is a relation on $\mathbb{Z}_5$ (of course the latter relation may not be particularly meaningful).

Notation. If two elements a, b in S are "linked" in $\mathcal{R}$, the most common ways of denoting this are

$$(a,b) \in \mathcal{R} \qquad \text{or} \qquad a \,\mathcal{R}\, b \qquad \text{or} \qquad a \sim b.$$

There are some types of binary relations that can be really useful.

Definition. A binary relation $\mathcal{R}$ on a non-empty set S is called an *equivalence relation* if:

- for every $a \in S$, we have that $a \,\mathcal{R}\, a$ (we say $\mathcal{R}$ is *reflexive*);
- for every $a, b \in S$, if $a \,\mathcal{R}\, b$, then $b \,\mathcal{R}\, a$ as well (we say $\mathcal{R}$ is *symmetric*);
- for every $a, b, c \in S$, if $a \,\mathcal{R}\, b$ and $b \,\mathcal{R}\, c$, then $a \,\mathcal{R}\, c$ as well (we say $\mathcal{R}$ is *transitive*).

Side Remark. Not every interesting relation in Mathematics has to be an equivalence relation. For example, the relation $\mathcal{R}_1$ above, which is reflexive and transitive, but not symmetric, or the relation

$$\mathcal{R}_3 = \big\{(x,y) : x, y \in \mathbb{R}, x < y\big\} = \big\{(x,y) : x, y \in \mathbb{R}, y - x > 0\big\},$$

which only satisfies the transitive property out of the above three, but fully encodes the standard ordering in $\mathbb{R}$, offer us a lot of useful information.

Problem 2. (a) Let $\mathbb{F}$ be a field, and m, n be positive integers. Show that *row equivalence* of matrices in $\mathbb{F}^{m\times n}$ is an equivalence relation on $\mathbb{F}^{m\times n}$. Recall that we say that $A \in \mathbb{F}^{m\times n}$ is row equivalent to $B \in \mathbb{F}^{m\times n}$ (and we write $A \sim B$) if there are some $k \geqslant 1$ and some elementary matrices $\mathcal{E}_1, \mathcal{E}_2, \ldots, \mathcal{E}_k \in \mathbb{F}^{m\times m}$ so that

$$B = \mathcal{E}_k \cdots \mathcal{E}_2 \mathcal{E}_1 A.$$

(b) Let $m > 1$ be a positive integer. Recall that congruence modulo m is a relation on $\mathbb{Z}$ defined as follows: $k \equiv l (\mathrm{mod}\, m)$ if and only if m divides $l - k$. Show that this is an equivalence relation.

Problem 3. (a) Let $\mathbb{F}$ be a field, n a positive integer, and suppose that A is a square matrix in $\mathbb{F}^{n\times n}$ with the property that, for every $\bar{b} \in \mathbb{F}^n$, the vector equation $A\bar{x} = \bar{b}$ is consistent (that is, it has at least one solution).

Prove that, for every $\bar{b}$, the vector equation $A\bar{x} = \bar{b}$ has a *unique* solution.

[**Remark 1.** This is Question 10 (II) from the 2nd Midterm Review and Practice File (one possible approach for this part is suggested in the second version of the file). Recall that combining this part with part (I) of the same question will allow you to also conclude that A is invertible.]

(b) Use part (a) combined with Remark 1 to prove the following: given $C \in \mathbb{F}^{n\times n}$, if there exists a matrix D in $\mathbb{F}^{n\times n}$ such that $CD = I_n$, then C is invertible (in other words, for a

square matrix C, it suffices to know that C has a right inverse in order to conclude that C has an inverse).

[**Remark 2.** How strong this property of multiplication in $\mathbb{F}^{n\times n}$ is, can be appreciated even more once we get to see examples of other non-commutative rings that fail to have the corresponding property.

Note that you can use part (a) to show part (b) even if you haven't proven part (a).]

Problem 4. Let V be a vector space over a field $\mathbb{F}$, and let u, v, w be vectors in V.
(a) Using the definition of linear span, show that

$$\operatorname{span}(u, v, w) = \operatorname{span}(u - v, v, w).$$

(b) Give an example showing that we can have

$$\operatorname{span}(u, v, w) \neq \operatorname{span}(u - v, v - u, w).$$

(c) What about

$$\operatorname{span}(u, v, w) = \operatorname{span}(u - v, v - w, w - u)\,?$$

Is it always true, or not always? Justify your answer.

Problem 5. (a) Determine which of the following sets are linearly independent and which are not. Justify your answer.

$$S_1 = \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \right\} \subset \mathbb{Z}_3^4 \quad \text{(scalars from } \mathbb{Z}_3\text{)},$$

$$S_2 = \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \right\} \subset \mathbb{R}^4 \quad \text{(scalars from } \mathbb{R}\text{)},$$

$$S_3 = \left\{ \begin{pmatrix} 0.5 \\ -0.5 \\ 3 \\ 2 \end{pmatrix}, \begin{pmatrix} -1 \\ 1.5 \\ -3 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0.5 \\ 3 \\ 1 \end{pmatrix}, \begin{pmatrix} -3 \\ 1 \\ 0 \\ -4 \end{pmatrix} \right\} \subset \mathbb{R}^4 \quad \text{(scalars from } \mathbb{R}\text{)},$$

$$S_4 = \left\{ x^2 + x,\ x^2 + 3x + 1,\ 5x - 2,\ 3x + 7 \right\} \subset \mathcal{P}_2 \quad \text{(scalars from } \mathbb{R}\text{)},$$

where $\mathcal{P}_2$ is the vector space of polynomials of degree at most 2 with real coefficients.

(b) Is any of these sets a basis of the space they are a subset of? Is any of them a spanning set? Justify your answer.

Also, for any of these sets that is not a basis, show how you can construct a basis of the corresponding space using as many vectors from the given set as possible.

Math 127
Suggested solutions to Homework Set 5

Problem 1. Statement 1 is true. The identity matrix in $\mathbb{F}^{2\times 2}$ only has two rows, so we can only swap these two to get an elementary matrix of Type 3. In other words, there is only one Type 3 elementary matrix in $\mathbb{F}^{2\times 2}$, and this is the matrix P_{12}.

Therefore, if both A and B are equal to P_{12}, clearly $AB = BA$.

Statement 2 is false. It suffices to give a counterexample: take one matrix to be P_{12} and the other matrix to be P_{13}; these are both understood to be elementary matrices in $\mathbb{F}^{3\times 3}$, so in other words

$$P_{12} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad P_{13} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Recalling that multiplying by P_{ij} from the left corresponds to swapping the i-th and the j-th rows of the matrix on the right, we get

$$P_{12}P_{13} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = P_{13}P_{12}.$$

Statement 3 is false. To disprove it, we would need to find a pair of elementary matrices $A, B \in \mathbb{Z}_5^{15\times 15}$ which are **both** of the same type, that type being either Type 1 or Type 2, and which do not commute. Indeed, we can rewrite Statement 3 using mathematical logic syntax as follows:

$$\forall A, B \in \mathbb{Z}_5^{15\times 15} \Big[\big[(A, B \text{ are Type 1}) \text{ or } (A, B \text{ are Type 2})\big] \quad \Rightarrow \quad (AB = BA)\Big],$$

so its negation would be

$$\exists A, B \in \mathbb{Z}_5^{15\times 15} \Big[\big[(A, B \text{ are Type 1}) \text{ or } (A, B \text{ are Type 2})\big] \quad \text{and} \quad (AB \neq BA)\Big].$$

But recall that Type 1 elementary matrices are all diagonal matrices, and we have proven in HW4, Pb5(I) that any two diagonal matrices coming from the same space commute. So our only hope of finding a pair of elementary

matrices of the same type that disproves Statement 3 (or in other words confirms its negation) is to look for suitable Type 2 matrices.

Take one matrix to be $E_{1,2;2}$ (that is, the matrix we get by adding twice the 2nd row of I_{15} to its 1st row and replacing the 1st row by the result), and let the other matrix be $E_{2,1;2}$ (that is, the matrix we get by adding twice the 1st row of I_{15} to its 2nd row and replacing the 2nd row by the result). In other words,

$$E_{1,2;2} = \begin{pmatrix} - \ \bar{e}_1 + 2\bar{e}_2 \ - \\ \text{---} \ \bar{e}_2 \ \text{---} \\ \text{---} \ \bar{e}_3 \ \text{---} \\ \vdots \\ \text{---} \ \bar{e}_{15} \ \text{---} \end{pmatrix} = \begin{pmatrix} | & | & | & & | \\ \bar{e}_1 & 2\bar{e}_1 + \bar{e}_2 & \bar{e}_3 & \cdots & \bar{e}_{15} \\ | & | & | & & | \end{pmatrix},$$

while

$$E_{2,1;2} = \begin{pmatrix} \text{---} \ \bar{e}_1 \ \text{---} \\ - \ \bar{e}_2 + 2\bar{e}_1 \ - \\ \text{---} \ \bar{e}_3 \ \text{---} \\ \vdots \\ \text{---} \ \bar{e}_{15} \ \text{---} \end{pmatrix} = \begin{pmatrix} | & | & | & & | \\ \bar{e}_1 + 2\bar{e}_2 & \bar{e}_2 & \bar{e}_3 & \cdots & \bar{e}_{15} \\ | & | & | & & | \end{pmatrix}.$$

To check that $E_{1,2;2}E_{2,1;2} \neq E_{2,1;2}E_{1,2;2}$, it suffices to check that there is at least one pair of indices i, j such that the (i, j)-entries of the two product matrices are different (in other words, we don't need to find all the entries of the two products). We can take $i = j = 1$. The $(1, 1)$-entry of $E_{1,2;2}E_{2,1;2}$ is equal to $\langle \bar{e}_1 + 2\bar{e}_2, \bar{e}_1 + 2\bar{e}_2 \rangle = \langle \bar{e}_1, \bar{e}_1 \rangle + \langle 2\bar{e}_2, 2\bar{e}_2 \rangle = 0$, while the $(1, 1)$-entry of $E_{2,1;2}E_{1,2;2}$ is equal to $\langle \bar{e}_1, \bar{e}_1 \rangle = 1$.

This shows $E_{1,2;2}E_{2,1;2} \neq E_{2,1;2}E_{1,2;2}$, as we wanted.

Statement 4 is false. An upper triangular matrix $U = (u_{ij})_{i,j} \in \mathbb{R}^{6\times 6}$ needs to satisfy $u_{ij} = 0$ if $i > j$, and that is the only requirement (that is, the values the diagonal entries and the entries above the diagonal could take are not restricted). We could thus choose

$$U = \begin{pmatrix} 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 3 & 0 & 1 & 2 \\ 0 & 0 & 2 & 1 & 3 & -1 \\ 0 & 0 & 0 & 2 & 5 & 0 \\ 0 & 0 & 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \bar{b} = \begin{pmatrix} 0 \\ 1 \\ 2 \\ -1 \\ \pi \\ \sqrt{e} \end{pmatrix}.$$

But the linear system with augmented matrix

$$\left(U \mid \bar{b}\right) = \left(\begin{array}{cccccc|c} 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 & 1 & 2 & 1 \\ 0 & 0 & 2 & 1 & 3 & -1 & 2 \\ 0 & 0 & 0 & 2 & 5 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & -2 & \pi \\ 0 & 0 & 0 & 0 & 0 & 1 & \sqrt{e} \end{array}\right)$$

has the following properties: the first non-zero coefficient of the second equation is **to the left** of the first non-zero coefficient of the first equation, and also the first non-zero coefficient of the third equation is **directly below** the first non-zero coefficient of the second equation. Either one of these properties violates the definition of an upper triangular/staircase system.

Statement 5 is true. Consider an upper triangular matrix $U' = (u'_{ij})_{i,j} \in \mathbb{R}^{6\times 6}$ with all diagonal entries non-zero. Then, for any $\bar{b} \in \mathbb{R}^{6\times 1}$, the linear system with augmented matrix $(U' \mid \bar{b})$ satisfies the following:

(a) all its equations are non-trivial/non-zero, given that in the i-th row we certainly have the non-zero entry u'_{ii};

(b) the first non-zero coefficient of the i-th equation is the coefficient u'_{ii}, given that the entries $u'_{i1}, u'_{i2}, \ldots, u'_{i,i-1}$ of $(U' \mid \bar{b})$ are zero since U' is upper triangular, while the entry u'_{ii} is non-zero by the additional assumption we have;

(c) if $r < i$, then u'_{ii}, the first non-zero coefficient of the i-th equation, is to the right of u'_{rr}, the first non-zero coefficient of the r-th equation which comes before the i-th equation.

By properties (a) and (c), we see that the linear system is upper triangular/staircase (and we can further conclude by property (b) that its pivots are the coefficients u'_{ii}).

Since U' was an arbitrary upper triangular matrix with all diagonal entries non-zero, we have shown that Statement 5 is true.

Statement 6 is true. Consider a Type 1 elementary matrix $A \in \mathbb{R}^{4\times 4}$. Suppose $A = D_{i;\lambda}$, that is, the diagonal matrix all of whose diagonal entries are equal to 1 except the i-th diagonal entry which is equal to some non-zero constant $\lambda \in \mathbb{R}$.

Since each matrix in $\mathbb{R}^{4\times 4}$ has 4 rows, we can find two indices $r, s \in \{1, 2, 3, 4\}$ both of which are different from i. In other words, we choose two indices $r, s \in \{1, 2, 3, 4\} \setminus \{i\}$. We will show that the Type 2 elementary matrix $E_{rs;1} \in \mathbb{R}^{4\times 4}$ commutes with A.

Note that $E_{rs;1}$ is the matrix that we get by adding the s-th row of I_4 (which is equal to the row vector $\bar{e}_s$) to its r-th row (which is equal to the row vector $\bar{e}_r$), and replacing the r-th row by the result $\bar{e}_r + \bar{e}_s$; thus $E_{rs;1} \neq I_4$. Nevertheless, for every $j \neq r$, the j-th row of $E_{rs;1}$ and the j-th row of I_4 are equal.

We now check: the product $AE_{rs;1} = D_{i;\lambda}E_{rs;1}$ is the matrix we get by multiplying the i-th row of $E_{rs;1}$ by λ, and leaving all other rows unchanged. But $i \neq r$ by our choice of r, s, therefore the i-th row of $E_{rs;1}$ is equal to the row vector $\bar{e}_i$, and hence the i-th row of $AE_{rs;1}$ is equal to $\lambda\bar{e}_i$. Moreover, the r-th row of $AE_{rs;1}$ is equal to the r-th row of $E_{rs;1}$, and equal to $\bar{e}_r + \bar{e}_s$. Finally, for every $j \notin \{i, r\}$, the j-th row of $AE_{rs;1}$ is equal to the j-th row of $E_{rs;1}$, and equal to $\bar{e}_j$.

On the other hand, the product $E_{rs;1}A = E_{rs;1}D_{i;\lambda}$ is the matrix we get by adding the s-th row of $D_{i;\lambda}$ to its r-th row, and by replacing the r-th row by the result. Since $i \notin \{r, s\}$, the s-th row of $D_{i;\lambda}$ is the row vector $\bar{e}_s$ and the r-th row of $D_{i;\lambda}$ is the row vector $\bar{e}_r$; therefore the r-th row of the new matrix $E_{rs;1}D_{i;\lambda}$ is equal to $\bar{e}_r + \bar{e}_s$, while the s-th row is the same as before. Moreover, all other rows of the new matrix are equal to the corresponding rows of $D_{i;\lambda}$, therefore the i-th row of $E_{rs;1}D_{i;\lambda}$ is equal to $\lambda\bar{e}_i$, while, for any $j \notin \{i, r, s\}$, the j-th row of $E_{rs;1}D_{i;\lambda}$ is equal to $\bar{e}_j$.

We conclude that the corresponding rows of the matrices $AE_{rs;1}$ and $E_{rs;1}A$ are equal, so the two matrices are equal.

Since A was an arbitrary Type 1 elementary matrix in $\mathbb{R}^{4\times 4}$, we have shown that Statement 6 is true.

Problem 2. (a) We have to check that row equivalence on $\mathbb{F}^{m\times n}$ is reflexive, symmetric and transitive.

Reflexivity: we need to check that, for any $A \in \mathbb{F}^{m\times n}$, $A \sim A$. But for any $A \in \mathbb{F}^{m\times n}$, we have that $A = D_{1;1}A$, which gives the desired conclusion (*we are using the notation $D_{i;\lambda}$ here in the same way as in Problem 1, Statement 6 above: $D_{i;\lambda}$ is the diagonal matrix $\in \mathbb{F}^{m\times m}$ all of whose diagonal entries are equal to 1 except the i-th diagonal entry which is equal to some $\lambda \neq 0$; this is an elementary matrix, and in fact, if $\lambda = 1$, it is equal to I_m*).

Symmetry: we need to check that, for any $A, B \in \mathbb{F}^{m\times n}$, if $A \sim B$, then $B \sim A$. Consider two matrices $A, B \in \mathbb{F}^{m\times n}$ satisfying $A \sim B$. Then, by definition there is some $k \geqslant 1$ and there are elementary matrices $\mathcal{E}_1, \mathcal{E}_2, \ldots, \mathcal{E}_k \in \mathbb{F}^{m\times m}$ so that

$$B = \mathcal{E}_k \cdots \mathcal{E}_2 \mathcal{E}_1 A.$$

We now recall that elementary matrices are all invertible, and the inverses are also elementary matrices. Therefore, we can write

$$\begin{aligned} A &= \mathcal{E}_1^{-1}\mathcal{E}_2^{-1}\cdots\mathcal{E}_k^{-1}\big(\mathcal{E}_k \cdots \mathcal{E}_2\mathcal{E}_1 A\big) \\ &= \mathcal{E}_1^{-1}\mathcal{E}_2^{-1}\cdots\mathcal{E}_k^{-1} B, \end{aligned}$$

which shows that $B \sim A$, since, for every $1 \leqslant j \leqslant k$, $\mathcal{E}_j^{-1}$ is an elementary matrix.

Transitivity: we need to check that, for any $A, B, C \in \mathbb{F}^{m\times n}$, if $A \sim B$ and $B \sim C$, then $A \sim C$. Consider three matrices $A, B, C \in \mathbb{F}^{m\times n}$ satisfying $A \sim B$ and $B \sim C$. Then, there are some integers $k_1, k_2 \geqslant 1$ and there are elementary matrices $\mathcal{E}_1, \mathcal{E}_2, \ldots, \mathcal{E}_{k_1}$, $\widetilde{\mathcal{E}}_1, \widetilde{\mathcal{E}}_2, \ldots, \widetilde{\mathcal{E}}_{k_2} \in \mathbb{F}^{m\times m}$ so that

$$B = \mathcal{E}_{k_1} \cdots \mathcal{E}_2 \mathcal{E}_1 A, \quad \text{and} \quad C = \widetilde{\mathcal{E}}_{k_2} \cdots \widetilde{\mathcal{E}}_2 \widetilde{\mathcal{E}}_1 B.$$

Combining these two assumptions, we have that

$$C = \widetilde{\mathcal{E}}_{k_2} \cdots \widetilde{\mathcal{E}}_2 \widetilde{\mathcal{E}}_1 \left(\mathcal{E}_{k_1} \cdots \mathcal{E}_2 \mathcal{E}_1 A\right) = \big(\widetilde{\mathcal{E}}_{k_2} \cdots \widetilde{\mathcal{E}}_2 \widetilde{\mathcal{E}}_1 \cdot \mathcal{E}_k \cdots \mathcal{E}_2 \mathcal{E}_1\big) A,$$

which shows that $A \sim C$ as we wanted.

We conclude that row equivalence on $\mathbb{F}^{m\times n}$ is an equivalence relation.

(b) Fix an integer $m > 1$. We have to check that congruence modulo m is reflexive, symmetric and transitive.

Reflexivity: we need to check that, for any $k \in \mathbb{Z}$, $k \equiv k (\mathrm{mod}\, m)$. But for any k, $k - k = 0$, therefore m divides $k - k$.

Symmetry: we need to check that, for any $k, l \in \mathbb{Z}$, if $k \equiv l (\mathrm{mod}\, m)$, then $l \equiv k (\mathrm{mod}\, m)$. Consider two integers $k, l \in \mathbb{Z}$ satisfying $k \equiv l (\mathrm{mod}\, m)$. Then, by how congruence modulo m is defined, we have that m divides $l - k$. This means that there is some $s \in \mathbb{Z}$ such that $l - k = s \cdot m$. But then

$$k - l = -(l - k) = -s \cdot m = (-s) \cdot m,$$

which shows that $k - l$ is also a multiple of m. Therefore, $l \equiv k (\mathrm{mod}\, m)$, as we wanted.

Transitivity: we need to check that, for any $k, l, r \in \mathbb{Z}$, if $k \equiv l (\mathrm{mod}\, m)$ and $l \equiv r (\mathrm{mod}\, m)$, then $k \equiv r (\mathrm{mod}\, m)$. Consider three integers $k, l, r \in \mathbb{Z}$ satisfying $k \equiv l (\mathrm{mod}\, m)$ and $l \equiv r (\mathrm{mod}\, m)$. Then m divides both $l - k$ and $r - l$. In other words, there are $s_1, s_2 \in \mathbb{Z}$ such that $l - k = s_1 \cdot m$ and $r - l = s_2 \cdot m$. We then have that

$$r - k = r - l + l - k = (l - k) + (r - l) = s_1 \cdot m + s_2 \cdot m = (s_1 + s_2) \cdot m,$$

which shows that $r - k$ is also a multiple of m. Therefore, $k \equiv r (\mathrm{mod}\, m)$ as we wanted.

We conclude that congruence modulo m is an equivalence relation on $\mathbb{Z}$.

Problem 3. (a) We will give a proof by contradiction. Assume that there exists some $\bar{b}_0 \in \mathbb{F}^n$ such that the vector equation/linear system $LS1: A\bar{x} = \bar{b}_0$ does not have a unique solution.

Given that we know it is consistent, we can conclude that it has more than one solutions.

But this can happen only if an equivalent staircase system $\widetilde{LS1}: \widetilde{A}\bar{x} = \bar{b}_1$ has free variables (and no pivot in the last column of course). Recall that we find such an equivalent system by doing Gaussian elimination; in matrix notation/terminology, we can find k elementary matrices $\mathcal{E}_1, \mathcal{E}_2, \ldots, \mathcal{E}_k$ for some $k \geqslant 1$ so that

$$(\widetilde{A} \mid \bar{b}_1) = \mathcal{E}_k \cdots \mathcal{E}_2 \mathcal{E}_1 (A \mid \bar{b}_0) = \big(\mathcal{E}_k \cdots \mathcal{E}_2 \mathcal{E}_1 A \mid \mathcal{E}_k \cdots \mathcal{E}_2 \mathcal{E}_1 \bar{b}_0\big),$$

and so that $(\widetilde{A} \mid \bar{b}_1)$ is in Row Echelon Form.

Since $\widetilde{LS1}$ has free variables and no pivot in the last column, the augmented matrix $(\widetilde{A} \mid \bar{b}_1)$ must have fewer than n pivots. Given that this matrix has n rows, it must have some zero rows (we recall that the number of pivots of a matrix in REF equals the number of its non-zero rows). Moreover, given that the zero rows must be at the bottom, we can conclude that the last row is certainly zero. This implies that the last row of $\widetilde{A}$ is also zero.

Consider now the linear system $LS2: \widetilde{A}\bar{x} = \bar{e}_n$. This is inconsistent since its last equation is of the form

$$0x_1 + 0x_2 + \cdots + 0x_n = 1.$$

We can find an equivalent linear system with coefficient matrix A by reversing the steps of Gaussian elimination that we considered above. Indeed, the system

$$\widetilde{LS2}: \; A\bar{x} = \mathcal{E}_1^{-1}\mathcal{E}_2^{-1} \cdots \mathcal{E}_k^{-1}\bar{e}_n$$

is equivalent to $LS2$ because the corresponding augmented matrices are row equivalent:

$$\begin{aligned}\big(A \mid \mathcal{E}_1^{-1}\mathcal{E}_2^{-1} \cdots \mathcal{E}_k^{-1}\bar{e}_n\big) &= \big(\mathcal{E}_1^{-1}\mathcal{E}_2^{-1} \cdots \mathcal{E}_k^{-1}\widetilde{A} \mid \mathcal{E}_1^{-1}\mathcal{E}_2^{-1} \cdots \mathcal{E}_k^{-1}\bar{e}_n\big) \\ &= \mathcal{E}_1^{-1}\mathcal{E}_2^{-1} \cdots \mathcal{E}_k^{-1}\big(\widetilde{A} \mid \bar{e}_n\big) \;\sim\; \big(\widetilde{A} \mid \bar{e}_n\big).\end{aligned}$$

Thus the solution sets of the two systems coincide, or in other words $\widetilde{LS2}$ is inconsistent. But this contradicts the assumption that, for every $\bar{b} \in \mathbb{F}^n$ the system $A\bar{x} = \bar{b}$ is consistent.

We conclude that our initial assumption, that there exists some $\bar{b}_0 \in \mathbb{F}^n$ for which the system $A\bar{x} = \bar{b}_0$ does not have a unique solution, was incorrect.

(b) According to Remark 1, if we show that

$$\text{for every } \bar{u} \in \mathbb{F}^n, \text{ the linear system } C\bar{y} = \bar{u} \text{ is consistent,} \tag{1}$$

we will be done (because in part (a) we saw that (1) implies that at least one such system has a unique solution (in fact we showed that every such a system has a unique solution), and this in turn implies that the coefficient matrix C is invertible according to Question 10 (I) from the 2nd Midterm Review and Practice File).

Fix now some $\bar{u} \in \mathbb{F}^n$. We have that $CD = I_n$, and therefore if we set $\bar{w} = D\bar{u}$, we will have

$$C\bar{w} = C(D\bar{u}) = (CD)\bar{u} = I_n\bar{u} = \bar{u}.$$

In other words, $\bar{w}$ is a solution to the system $C\bar{y} = \bar{u}$.

Since $\bar{u}$ was arbitrary, we have shown (1).

Problem 4. (i) By definition we have that

$$\begin{aligned}\operatorname{span}(u,v,w) &= \{\lambda_1 u + \lambda_2 v + \lambda_3 w : \lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}\} \\ \text{and } \operatorname{span}(u-v,v,w) &= \{\mu_1(u-v) + \mu_2 v + \mu_3 w : \mu_1, \mu_2, \mu_3 \in \mathbb{F}\}.\end{aligned}$$

We will show that

$$\operatorname{span}(u,v,w) \subseteq \operatorname{span}(u-v,v,w) \quad \text{and} \quad \operatorname{span}(u-v,v,w) \subseteq \operatorname{span}(u,v,w).$$

To prove the first inclusion, consider a vector $z \in \operatorname{span}(u,v,w)$. Then there exist $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}$ so that

$$z = \lambda_1 u + \lambda_2 v + \lambda_3 w.$$

We need to find $\mu_1, \mu_2, \mu_3 \in \mathbb{F}$ so that z can be written as $\mu_1(u-v)+\mu_2 v+\mu_3 w$ too.

If we set $\mu_1 = \lambda_1$, $\mu_2 = \lambda_1 + \lambda_2$ and $\mu_3 = \lambda_3$, then we will have

$$\begin{aligned}\mu_1(u-v) + \mu_2 v + \mu_3 w &= \lambda_1(u-v) + (\lambda_1+\lambda_2)v + \lambda_3 w \\ &= \lambda_1 u - \lambda_1 v + \lambda_1 v + \lambda_2 v + \lambda_3 w \\ &= \lambda_1 u + \lambda_2 v + \lambda_3 w = z.\end{aligned}$$

This shows that $z \in \operatorname{span}(u-v,v,w)$. Since we started with an arbitrary $z \in \operatorname{span}(u,v,w)$, we have proven the first inclusion.

To prove the second inclusion, we similarly start by considering a vector $z' \in \operatorname{span}(u-v,v,w)$. Then there exist $\mu_1', \mu_2', \mu_3' \in \mathbb{F}$ so that

$$z' = \mu_1'(u-v) + \mu_2' v + \mu_3' w.$$

We need to find $\lambda_1', \lambda_2', \lambda_3' \in \mathbb{F}$ so that z' can be written as $\lambda_1' u + \lambda_2' v + \lambda_3' w$ too.

If we set $\lambda_1' = \mu_1'$, $\lambda_1' = \mu_2' - \mu_1'$ and $\lambda_3' = \mu_3'$, then we have

$$\begin{aligned}\lambda_1' u + \lambda_2' v + \lambda_3' w &= \mu_1' u + (\mu_2' - \mu_1')v + \mu_3' w \\ &= \mu_1' u + \mu_2' v - \mu_1' v + \mu_3' w \\ &= \mu_1' u - \mu_1' v + \mu_2' v + \mu_3' w \\ &= \mu_1'(u-v) + \mu_2' v + \mu_3' w = z'.\end{aligned}$$

This shows that $z' \in \operatorname{span}(u,v,w)$. Since we started with an arbitrary $z' \in \operatorname{span}(u-v,v,w)$, we have shown the second inclusion too.

Combining the two, we get the equality of the two spans.

(ii) Consider the vector space $\mathbb{R}^3$ over $\mathbb{R}$, and set $u = \bar{e}_1$, $v = \bar{e}_2$ and $w = \bar{e}_3$.

Then $\text{span}(u, v, w) = \mathbb{R}^3$. On the other hand, $\text{span}(u - v, v - u, w) = \text{span}(\bar{e}_1 - \bar{e}_2, \bar{e}_2 - \bar{e}_1, \bar{e}_3)$, so every vector $\bar{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ in the latter span satisfies $x_1 = -x_2$. This shows that $\bar{e}_1 \notin \text{span}(u - v, v - u, w)$, and thus we obtain that

$$\text{span}(\bar{e}_1, \bar{e}_2, \bar{e}_3) \neq \text{span}(\bar{e}_1 - \bar{e}_2, \bar{e}_2 - \bar{e}_1, \bar{e}_3).$$

(iii) The equality is **not** always true.

To verify this, let us consider again the vector space $\mathbb{R}^3$ over $\mathbb{R}$, and let's set $u = \bar{e}_1$, $v = \bar{e}_1 + \bar{e}_2$ and $w = \bar{e}_1 + \bar{e}_2 + \bar{e}_3$.

Then we can check that all the standard basis vectors of $\mathbb{R}^3$ are in $\text{span}(u, v, w) = \text{span}(\bar{e}_1,\ \bar{e}_1 + \bar{e}_2,\ \bar{e}_1 + \bar{e}_2 + \bar{e}_3)$, and thus $\text{span}(\bar{e}_1,\ \bar{e}_1 + \bar{e}_2,\ \bar{e}_1 + \bar{e}_2 + \bar{e}_3) = \mathbb{R}^3$.

On the other hand, $\text{span}(u - v, v - w, w - u) = \text{span}(-\bar{e}_2,\ -\bar{e}_3,\ \bar{e}_2 + \bar{e}_3)$. Therefore every vector $\bar{y} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$ in this span will have first coordinate $y_1 = 0$. This shows that $\bar{e}_1$ cannot be in this span, and hence

$$\text{span}(\bar{e}_1,\ \bar{e}_1 + \bar{e}_2,\ \bar{e}_1 + \bar{e}_2 + \bar{e}_3) \neq \text{span}(-\bar{e}_2,\ -\bar{e}_3,\ \bar{e}_2 + \bar{e}_3).$$

Problem 5. (a) Let $A_1 \in \mathbb{Z}_3^{4\times 3}$ be the matrix whose columns are the vectors in S_1:

$$A_1 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix},$$

and let us consider the linear system $A_1\bar{x} = \bar{0}$ where $\bar{0} \in \mathbb{Z}_3^4$ and $\bar{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$.

We recall that S_1 is linearly independent if and only if the system $A_1\bar{x} = \bar{0}$ has only one solution, the trivial solution. Thus it suffices to check the latter. We look at the augmented matrix of the system:

$$(A_1 \mid \bar{0}) = \left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{array}\right) \xrightarrow[R_4 - R_1 \to R_4']{R_3 - R_1 \to R_3'} \left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

$$\xrightarrow{R_3 + R_2 \to R_3'} \left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

This shows that the equivalent staircase system we have gotten has a free variable, the variable x_3, so this system, and hence also the original system, has more than one solutions.

We conclude that S_1 is linearly dependent.

Let $A_2 \in \mathbb{R}^{4\times 3}$ be the matrix whose columns are the vectors in S_2 and let us consider the linear system $A_2\bar{x} = \bar{0}$ where $\bar{0} \in \mathbb{R}^4$ and $\bar{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$. It suffices to check whether this system has a unique solution or not.

We have that

$$(A_2 \mid \bar{0}) = \left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{array}\right) \xrightarrow[R_4 - R_1 \to R_4']{R_3 - R_1 \to R_3'} \left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

$$\xrightarrow{R_3 - \frac{1}{2}R_2 \to R_3'} \left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & -\frac{3}{2} & 0 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

This shows that all variables are pivot variables of the equivalent staircase system we have gotten, therefore this system, and hence also the original system, has a unique solution.

We conclude that S_2 is linearly independent.

Let $A_3 \in \mathbb{R}^{4\times 4}$ be the matrix whose columns are the vectors in S_3 and let us consider the linear system $A_3\bar{x} = \bar{0}$ where $\bar{0} \in \mathbb{R}^4$ and $\bar{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$. It suffices to check whether this system has a unique solution or not.

We have that

$$(A_3 \mid \bar{0}) = \left(\begin{array}{cccc|c} 0.5 & -1 & 0 & -3 & 0 \\ -0.5 & 1.5 & 0.5 & 1 & 0 \\ 3 & -3 & 3 & 0 & 0 \\ 2 & -1 & 1 & -4 & 0 \end{array}\right) \xrightarrow[R_4-4R_1]{R_2+R_1,\ R_3-6R_1} \left(\begin{array}{cccc|c} 0.5 & -1 & 0 & -3 & 0 \\ 0 & 0.5 & 0.5 & -2 & 0 \\ 0 & 3 & 3 & 18 & 0 \\ 0 & 3 & 1 & 8 & 0 \end{array}\right)$$

$$\xrightarrow[R_4-6R_2\to R_4']{R_3-6R_2\to R_3'} \left(\begin{array}{cccc|c} 0.5 & -1 & 0 & -3 & 0 \\ 0 & 0.5 & 0.5 & -2 & 0 \\ 0 & 0 & 0 & 30 & 0 \\ 0 & 0 & -2 & 20 & 0 \end{array}\right) \xrightarrow{R_3 \leftrightarrow R_4} \left(\begin{array}{cccc|c} 0.5 & -1 & 0 & -3 & 0 \\ 0 & 0.5 & 0.5 & -2 & 0 \\ 0 & 0 & -2 & 20 & 0 \\ 0 & 0 & 0 & 30 & 0 \end{array}\right).$$

This shows that all variables are pivot variables of the equivalent staircase system we have gotten, therefore this system, and hence also the original system, has a unique solution.

We conclude that S_3 is linearly independent.

Finally, we look at the arbitrary linear combination of the vectors in S_4: consider $\lambda_i \in \mathbb{R}$, $1 \leqslant i \leqslant 4$; then

$$\begin{aligned} &\lambda_1(x^2+x) + \lambda_2(x^2+3x+1) + \lambda_3(5x-2) + \lambda_4(3x+7) \\ &\qquad = (\lambda_2 - 2\lambda_3 + 7\lambda_4) + (\lambda_1 + 3\lambda_2 + 5\lambda_3 + 3\lambda_4)x + (\lambda_1+\lambda_2)x^2. \end{aligned}$$

Suppose now that such a combination equals the zero polynomial $\mathbf{0}$. We recall that this can happen if and only if the coefficient of each monomial x^k in the latter expression is equal to 0; that is, we want

$$\lambda_2 - 2\lambda_3 + 7\lambda_4 \;=\; \lambda_1 + 3\lambda_2 + 5\lambda_3 + 3\lambda_4 \;=\; \lambda_1 + \lambda_2 \;=\; 0.$$

To find combinations of values for the λ_i that would satisfy this, we solve the system

$$\left\{\begin{array}{rcrcrcl} & & \lambda_2 & - & 2\lambda_3 & + & 7\lambda_4 = 0 \\ \lambda_1 & + & 3\lambda_2 & + & 5\lambda_3 & + & 3\lambda_4 = 0 \\ \lambda_1 & + & \lambda_2 & & & & = 0 \end{array}\right\}.$$

This is equivalent to

$$\left\{\begin{array}{rcrcrcrcl} \lambda_1 & + & \lambda_2 & & & & & = & 0 \\ \lambda_1 & + & 3\lambda_2 & + & 5\lambda_3 & + & 3\lambda_4 & = & 0 \\ & & \lambda_2 & - & 2\lambda_3 & + & 7\lambda_4 & = & 0 \end{array}\right\} \Leftrightarrow \left\{\begin{array}{rcrcrcrcl} \lambda_1 & + & \lambda_2 & & & & & = & 0 \\ & & 2\lambda_2 & + & 5\lambda_3 & + & 3\lambda_4 & = & 0 \\ & & \lambda_2 & - & 2\lambda_3 & + & 7\lambda_4 & = & 0 \end{array}\right\}$$

$$\Leftrightarrow \left\{\begin{array}{rcrcrcrcl} \lambda_1 & + & \lambda_2 & & & & & = & 0 \\ & & 2\lambda_2 & + & 5\lambda_3 & + & 3\lambda_4 & = & 0 \\ & & & & -4.5\lambda_3 & + & 5.5\lambda_4 & = & 0 \end{array}\right\}.$$

The last equivalent system we got is staircase, and has one free variable (the variable x_4). Therefore, it has more than one solutions, and so does the original system.

Alternatively, we could have simply observed that the original system is homogeneous and underdetermined (it has 3 equations in 4 unknowns), therefore, by the Theorem stated in HW4, Problem 7, we know that it has more than one solutions.

We thus obtain that there is a choice of values for $\lambda_1, \lambda_2, \lambda_3$ and λ_4, so that not all of them are zero, and so that

$$\lambda_1(x^2+x) + \lambda_2(x^2+3x+1) + \lambda_3(5x-2) + \lambda_4(3x+7) = \mathbf{0}.$$

As a consequence we get that S_4 is a linearly dependent subset of $\mathcal{P}_2$.

Alternative justification for S_4: We can check that

$$(-3)\cdot(5x-2) + 5\cdot(3x+7) = 41 \;\Rightarrow$$
$$\frac{2}{3}(3x+7) - \frac{11}{3\cdot 41}\big((-3)\cdot(5x-2) + 5\cdot(3x+7)\big) = 2x + \frac{14}{3} - \frac{11}{3} = 2x+1 \;\Rightarrow$$
$$(x^2+x) + \frac{11}{41}(5x-2) + \frac{9}{41}(3x+7) = x^2+3x+1.$$

In other words, one of the polynomials in S_4 is a linear combination of the others, and hence, as we have seen in class, S_4 is linearly dependent.

(b) We have just seen that the sets S_1 and S_4 are not linearly independent, therefore they cannot be bases.

S_2 is linearly independent, so it suffices to check whether it is also a spanning set of $\mathbb{R}^4$, that is, if $\mathbb{R}^4 = \text{span}(S_2)$. But recall that $\mathbb{R}^4 = \text{span}(\bar{e}_i : 1 \leqslant i \leqslant 4)$, thus, as we have seen in previous problems, it suffices to check

whether each $\bar{e}_i$ is in $\text{span}(S_2)$. We can check these simultaneously:

$$(A_2 \mid I_4) = \left(\begin{array}{ccc|c:c:c:c} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \underbrace{\begin{array}{l} R_3 - R_1 \to R_3' \\ R_4 - R_1 \to R_4' \end{array}} \left(\begin{array}{ccc|c:c:c:c} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & -1 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 1 \end{array}\right)$$

$$\underbrace{R_3 - \tfrac{1}{2}R_2 \to R_3'} \left(\begin{array}{ccc|c:c:c:c} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & -\frac{3}{2} & -1 & -\frac{1}{2} & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 1 \end{array}\right).$$

This shows that $\bar{e}_1$ and $\bar{e}_4$ are not in $\text{span}(S_2)$ (while $\bar{e}_2$ and $\bar{e}_3$ are). We conclude that S_2 is not a spanning set.

We also observe that, as discussed in class, $S_2 \cup \{\bar{e}_1\}$ is linearly independent too. We check again whether this is a spanning set of $\mathbb{R}^4$, and hence a basis: from what we showed above, we immediately obtain that

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & -\frac{3}{2} & -1 & 0 \\ 0 & 0 & 0 & -1 & 1 \end{array}\right).$$

Thus $\bar{e}_4$ is in $\text{span}(S_2 \cup \{\bar{e}_1\})$. Since we already saw that $\bar{e}_2, \bar{e}_3 \in \text{span}(S_2) \subseteq \text{span}(S_2 \cup \{\bar{e}_1\})$, and since $\bar{e}_1 \in S_2 \cup \{\bar{e}_1\} \subseteq \text{span}(S_2 \cup \{\bar{e}_1\})$, we can conclude that $S_2 \cup \{\bar{e}_1\}$ spans $\mathbb{R}^4$, and thus it is also a basis of $\mathbb{R}^4$.

Similarly, S_3 is linearly independent, so it suffices to check, in an analogous way to above, whether it is also a spanning set of $\mathbb{R}^4$.

Alternatively, we could remark that we have already found a REF of A_3 which has 4 pivots (as many as the rows of A_3). This implies that, for any $\bar{b} \in \mathbb{R}^4$, the linear system $A_3\bar{x} = \bar{b}$ has a solution (since the augmented matrix $(A_3 \mid \bar{b})$ of the system has a row equivalent matrix $\widetilde{C}$ with first 4 columns equal to this REF of A_3, and hence the equivalent system corresponding to $\widetilde{C}$ is staircase (no matter what the last column is) and does not have a pivot in the last column).

We conclude that S_3 is a basis of $\mathbb{R}^4$.

Finally we check whether S_1 and/or S_4 are spanning sets of their respective spaces.

Regarding S_1, we follow a similar strategy to above: it suffices to check whether all the standard basis vectors of $\mathbb{Z}_3^4$ are in $\text{span}(S_1)$. Let us note first

of all that, from what we have already seen, we can write

$$\left(\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right).$$

Therefore the vector $\begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$ is a linear combination of the other two vectors in S_1, and if we set

$$\widetilde{S}_1 = \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 1 \\ 0 \end{pmatrix} \right\},$$

we will have $\operatorname{span}(S_1) = \operatorname{span}(\widetilde{S}_1)$. Thus, it will suffice to check whether $\widetilde{S}_1$ spans $\mathbb{Z}_3^4$.

We write

$$\left(\begin{array}{cc|c:c:c:c} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|c:c:c:c} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|c:c:c:c} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 & 1 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 \end{array}\right).$$

This shows that none of the standard basis vectors of $\mathbb{Z}_3^4$ are in $\operatorname{span}(\widetilde{S}_1) = \operatorname{span}(S_1)$, so S_1 is not a spanning set of $\mathbb{Z}_3^4$ (and clearly neither is $\widetilde{S}_1$).

On the other hand, $\widetilde{S}_1$ is a linearly independent subset of S_1, since it contains two vectors which are not parallel to each other, and given that S_1 is not linearly independent itself, $\widetilde{S}_1$ is a maximal linearly independent subset of S_1. We will now try to construct a basis of $\mathbb{Z}_3^4$ which contains $\widetilde{S}_1$.

By what we already saw, the set $\widetilde{S}_1 \cup \{\bar{e}_1\}$ is linearly independent. Based on the row equivalences we showed above, we can continue writing:

$$\left(\begin{array}{ccc|c:c:c} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|c:c:c} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 & 1 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|c:c:c} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 1 \end{array}\right).$$

This again implies that none of the remaining standard basis vectors is in $\operatorname{span}\big(\widetilde{S}_1 \cup \{\bar{e}_1\}\big)$, so the set $\widetilde{S}_1 \cup \{\bar{e}_1, \bar{e}_2\}$ is also linearly independent. But now we have that

$$\left(\begin{array}{cccc|c:c} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c:c} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 1 \end{array}\right),$$

therefore $\bar{e}_3$ and $\bar{e}_4$ are in $\operatorname{span}\big(\widetilde{S}_1 \cup \{\bar{e}_1, \bar{e}_2\}\big)$.

We conclude that $\widetilde{S}_1 \cup \{\bar{e}_1, \bar{e}_2\}$ is both linearly independent and a spanning set of $\mathbb{Z}_3^4$, thus it is a basis of $\mathbb{Z}_3^4$.

It remains to ask the analogous questions about S_4: we need to check whether every polynomial $p \in \mathcal{P}_2$, namely every polynomial of the form $p(x) = a_0 + a_1 x + a_2 x^2$ with $a_0, a_1, a_2 \in \mathbb{R}$, can be written in the form

$$\begin{aligned}\lambda_1(x^2+x) + \lambda_2(x^2+3x+1) + \lambda_3(5x-2) + \lambda_4(3x+7) \\ = (\lambda_2 - 2\lambda_3 + 7\lambda_4) + (\lambda_1 + 3\lambda_2 + 5\lambda_3 + 3\lambda_4)x + (\lambda_1 + \lambda_2)x^2.\end{aligned}$$

Equivalently, we need to check whether the system

$$\left\{\begin{array}{rcrcrcrcl} & & \lambda_2 & - & 2\lambda_3 & + & 7\lambda_4 & = & a_0 \\ \lambda_1 & + & 3\lambda_2 & + & 5\lambda_3 & + & 3\lambda_4 & = & a_1 \\ \lambda_1 & + & \lambda_2 & & & & & = & a_2 \end{array}\right\} \tag{2}$$

has a solution. By what we already showed, we have

$$\left\{\begin{array}{rcrcrcrcl} \lambda_1 & + & \lambda_2 & & & & & = & a_0 \\ \lambda_1 & + & 3\lambda_2 & + & 5\lambda_3 & + & 3\lambda_4 & = & a_1 \\ & & \lambda_2 & - & 2\lambda_3 & + & 7\lambda_4 & = & a_2 \end{array}\right\} \Leftrightarrow \left\{\begin{array}{rcrcrcrcl} \lambda_1 & + & \lambda_2 & & & & & = & \tilde{a}_0 \\ & & 2\lambda_2 & + & 5\lambda_3 & + & 3\lambda_4 & = & \tilde{a}_1 \\ & & & & -4.5\lambda_3 & + & 5.5\lambda_4 & = & \tilde{a}_2 \end{array}\right\}$$

for some $\tilde{a}_0, \tilde{a}_1, \tilde{a}_2 \in \mathbb{R}$, therefore, regardless of what a_0, a_1, a_2 are (or equivalently what $\tilde{a}_0, \tilde{a}_1, \tilde{a}_2$ are), the corresponding system in (2) is consistent. We conclude that S_4 is a spanning set of $\mathcal{P}_2$.

Moreover, we can see from above that, if we set $\lambda_4 = 0$, then there is a unique choice of values for λ_1, λ_2 and λ_3 that solves the system. This implies two things:

- the subset $\widetilde{S}_4 = \big\{x^2 + x,\ x^2 + 3x + 1,\ 5x - 2\big\}$ is a spanning set of $\mathcal{P}_2$ as well;
- $\widetilde{S}_4$ is linearly independent (this follows if we start with $a_0 = a_1 = a_2 = 0$ in (2)).

We conclude that $\widetilde{S}_4$ is a maximal linearly independent subset of S_4, and a basis of $\mathcal{P}_2$.

Math 127
Homework Problem Set 6

Problem 0. *(Practice Problem, not to be submitted)* (a) Consider the complex numbers $z = 3 + 4\mathbf{i}$ and $w = 2 - 3\mathbf{i}$. Compute $z + w,\ zw,\ z/w,\ z \cdot \overline{w},\ \operatorname{Re} z,\ \operatorname{Im} z,\ |z|$, and $\arg(z)$.
(b) Determine whether the following matrix from $\mathbb{C}^{3\times 3}$ is invertible or not:

$$A = \begin{pmatrix} 1 & \boldsymbol{i} & 3+4\boldsymbol{i} \\ -\boldsymbol{i} & 1 & 3-4\boldsymbol{i} \\ 2+\boldsymbol{i} & 4+2\boldsymbol{i} & 3+12\boldsymbol{i} \end{pmatrix}.$$

Problem 1. Let κ, λ, μ be unknown constants/parameters allowed to take values in $\mathbb{C}$. Consider the following linear system with coefficients from $\mathbb{C}$:

$$\left\{ \begin{array}{rcrcrcl} x_1 & + & 2x_2 & + & (\boldsymbol{i}-1)x_3 & = & 0 \\ -3x_1 & + & (\kappa^6-5)x_2 & + & (3+3\boldsymbol{i})x_3 & = & \lambda^2 \\ & & & & (\mu^3-1)x_3 & = & \lambda \end{array} \right\}.$$

Find all combinations of κ, λ, μ, if any exist, for which the corresponding system has infinitely many solutions (list explicit values). Justify your answer.

Problem 2. (a) Find a matrix $B \in \mathbb{R}^{2\times 2}$ such that $B^2 = -I_2$.
(b) Define a field isomorphism from $\mathbb{C}$ to the space of matrices

$$\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$$

with the standard addition and multiplication, and verify your answer. This gives one more representation of the complex numbers.

Problem 3. Let $\mathbb{F}$ be a field. We have seen in Question 3 from the 2nd Midterm Review and Practice File that the space $\mathbb{F}^{m\times n}$ (with standard matrix addition, and scalar multiplication defined as stated in that question) is a vector space over $\mathbb{F}$.

Find a basis for this space and thus determine its dimension too.

Problem 4. (a) View $\mathbb{R}$ as a vector space over itself. Show that the sets

$$\{\sqrt{2}, \sqrt{5}\}, \qquad \{\sqrt{2}, \sqrt{5}, \sqrt{7}\}$$

are linearly dependent.

(b) View $\mathbb{R}$ as a vector space over $\mathbb{Q}$. Prove that two of the following sets are linearly independent, while the remaining set is linearly dependent:

$$\{\sqrt{2}, \sqrt{5}, \sqrt{7}\}, \qquad \{\sqrt{2}, \sqrt{6}, \sqrt{8}\}, \qquad \{\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{10}\}.$$

[*Note/Hint.* You may use the fact, which will be discussed in more detail in MATH 227, that, for any integer k which is not a square of another integer, $\sqrt{k}$ is irrational.]

(c) Let $\mathbb{F}_4$ be the field with 4 elements which you constructed in HW2, Problem 3, and recall that $\mathbb{Z}_2$ is a subfield of this field (why?). What is the dimension of the vector space $\mathbb{F}_4^{2\times 2}$ over $\mathbb{Z}_2$? Justify your answer. (See also Problem 3 above.)

Problem 5. Let V be a vector space over a field $\mathbb{F}$, and suppose $\dim_{\mathbb{F}} V = n$. Consider a linearly independent set $S \subseteq V$ with size $|S| = n$. Prove that S is a basis of V.

Problem 6. Explain why (a) through (d) are the same problem essentially, and choose whichever way you want to solve the problem.

(a) Solve the following system of linear equations with coefficients from $\mathbb{R}$:

$$\left\{\begin{array}{rrr} 3x_1 + 2x_2 & +x_3 = & 9 \\ x_1 & -2x_3 = & -8 \\ 2x_1 & -2x_3 = & -6 \end{array}\right\}.$$

(b) Consider the vectors $\bar{u} = \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix}$, $\bar{v} = \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}$, $\bar{w} = \begin{pmatrix} 1 \\ -2 \\ -2 \end{pmatrix}$, and $\bar{b} = \begin{pmatrix} 9 \\ -8 \\ -6 \end{pmatrix}$ in $\mathbb{R}^3$. Determine whether $\bar{b}$ is in the linear span of $\bar{u}$, $\bar{v}$, and $\bar{w}$. If yes, write explicitly the linear combination(s) showing this.

(c) Let

$$A = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 0 & -2 \\ 2 & 0 & -2 \end{pmatrix} \in \mathbb{R}^{3\times 3} \quad \text{and} \quad \bar{b} = \begin{pmatrix} 9 \\ -8 \\ -6 \end{pmatrix} \in \mathbb{R}^3.$$

Solve the equation $A\bar{x} = \bar{b}$ for the unknown vector $\vec{x} \in \mathbb{R}^3$.

(d) Define $f\colon \mathbb{R}^3 \to \mathbb{R}^3$ by $f\left(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}\right) = \begin{pmatrix} 3x_1 + 2x_2 + x_3 \\ x_1 - 2x_3 \\ 2x_1 - 2x_3 \end{pmatrix}$. Determine whether $\begin{pmatrix} 9 \\ -8 \\ -6 \end{pmatrix}$ is in the range of f, and, if it is, find all its preimages.

Problem 7. (a) For each of the following functions, determine whether it is linear, injective and/or surjective (give brief justifications). The spaces that appear as domains or codomains of these functions should be understood as the standard vector spaces we have seen (over the largest possible scalar field in each case).

(i) $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ given by $f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = \begin{pmatrix} -x_1 \\ x_2 \end{pmatrix}$

(ii) $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ given by $f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = \begin{pmatrix} x_1 + x_2 \\ x_1 x_2 \end{pmatrix}$

(iii) $f\colon \mathbb{Z}_3^2 \to \mathbb{Z}_3^2$ given by $f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = \begin{pmatrix} x_1 - x_2 \\ x_1 x_2 \end{pmatrix}$

(iv) $f\colon \mathbb{R}^2 \to \mathbb{R}$ given by $f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = x_1 + x_2$

(v) $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ given by $f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = \begin{pmatrix} x_1 + 1 \\ x_2 + 2 \end{pmatrix}$

(vi) $f\colon \mathbb{Z}_5^3 \to \mathbb{Z}_5^3$ given by $f\left(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}\right) = \begin{pmatrix} x_2 \\ x_3 \\ x_1 \end{pmatrix}$

(vii) $f\colon \mathbb{R}^3 \to \mathbb{R}^{2\times 2}$ given by $f\left(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}\right) = \begin{pmatrix} x_1 & x_2 \\ 0 & x_3 \end{pmatrix}$

(viii) $f\colon \mathbb{R}^3 \to \mathbb{R}^{2\times 2}$ given by $f\left(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}\right) = \begin{pmatrix} x_1 & x_2 \\ 1 - x_3 & x_3 \end{pmatrix}$

(b) For any of the functions in parts (i)-(vi) that is linear, find a matrix representation.

Math 127
Suggested solutions to Homework Set 6

Problem 0. (a) We have

$$z + w = (3 + 4\boldsymbol{i}) + (2 - 3\boldsymbol{i}) = 5 + \boldsymbol{i},$$
$$zw = (3 + 4\boldsymbol{i})(2 - 3\boldsymbol{i}) = 3 \cdot 2 - 4 \cdot (-3) + 3 \cdot (-3)\boldsymbol{i} + 4 \cdot 2\boldsymbol{i} = 18 - \boldsymbol{i},$$

$$\frac{z}{w} = z\, w^{-1} = z\, \frac{\overline{w}}{|w|^2} = (3 + 4\boldsymbol{i})\, \frac{2 + 3\boldsymbol{i}}{(\mathrm{Re}(w))^2 + (\mathrm{Im}(w))^2} =$$
$$= \frac{3 \cdot 2 - 4 \cdot 3 + 3 \cdot 3\boldsymbol{i} + 4 \cdot 2\boldsymbol{i}}{13} = -\frac{6}{13} + \frac{15}{13}\boldsymbol{i},$$

$$z \cdot \overline{w} = (3 + 4\boldsymbol{i})(2 + 3\boldsymbol{i}) = 3 \cdot 2 - 4 \cdot 3 + 3 \cdot 3\boldsymbol{i} + 4 \cdot 2\boldsymbol{i} = -6 + 15\boldsymbol{i},$$

$$\mathrm{Re}(z) = 3, \quad \mathrm{Im}(z) = 4, \quad |z| = \sqrt{z \cdot \overline{z}} = \sqrt{(\mathrm{Re}(z))^2 + (\mathrm{Im}(z))^2} = 5, \quad \arg(z) = \arctan(4/3).$$

(b) It suffices to look at a Row Echelon Form of A, and see how many pivots (equivalently, how many non-zero rows) it has:

$$A = \begin{pmatrix} 1 & \boldsymbol{i} & 3 + 4\boldsymbol{i} \\ -\boldsymbol{i} & 1 & 3 - 4\boldsymbol{i} \\ 2 + \boldsymbol{i} & 4 + 2\boldsymbol{i} & 3 + 12\boldsymbol{i} \end{pmatrix} \xrightarrow[R_3 - (2+\boldsymbol{i})R_1 \to R_3']{R_2 + \boldsymbol{i}R_1 \to R_2'} \begin{pmatrix} 1 & \boldsymbol{i} & 3 + 4\boldsymbol{i} \\ 0 & 0 & -1 - \boldsymbol{i} \\ 0 & 5 & 1 + \boldsymbol{i} \end{pmatrix}$$
$$\xrightarrow{R_2 \leftrightarrow R_3} \begin{pmatrix} 1 & \boldsymbol{i} & 3 + 4\boldsymbol{i} \\ 0 & 5 & 1 + \boldsymbol{i} \\ 0 & 0 & -1 - \boldsymbol{i} \end{pmatrix}.$$

The last matrix is in REF, and has 3 pivots (as many as the total number of its rows or columns), therefore it is invertible and so is A.

Problem 1. We have that

$$\left\{\begin{array}{rcrcrcl} x_1 & + & 2x_2 & + & (\boldsymbol{i}-1)x_3 & = & 0 \\ -3x_1 & + & (\kappa^6-5)x_2 & + & (3+3\boldsymbol{i})x_3 & = & \lambda^2 \\ & & & & (\mu^3-1)x_3 & = & \lambda \end{array}\right\} \quad \Leftrightarrow$$

$$\left\{\begin{array}{rcrcrcl} x_1 & + & 2x_2 & + & (\boldsymbol{i}-1)x_3 & = & 0 \\ & & (\kappa^6+1)x_2 & + & 6\boldsymbol{i}\,x_3 & = & \lambda^2 \\ & & & & (\mu^3-1)x_3 & = & \lambda \end{array}\right\}.$$

We consider two cases:

Case 1: $\kappa^6+1=0$. Then none of the coefficients of the variable x_2 can be a pivot coefficient, therefore x_2 is certainly a free variable. This implies that, if the system is consistent, then it will have infinitely many solutions (since the field $\mathbb{C}$ where the coefficients are coming from is infinite).

But

$$\left\{\begin{array}{rcrcrcl} x_1 & + & 2x_2 & + & (\boldsymbol{i}-1)x_3 & = & 0 \\ & & & & 6\boldsymbol{i}\,x_3 & = & \lambda^2 \\ & & & & (\mu^3-1)x_3 & = & \lambda \end{array}\right\} \quad \Leftrightarrow$$

$$\left\{\begin{array}{rcrcrcl} x_1 & + & 2x_2 & + & (\boldsymbol{i}-1)x_3 & = & 0 \\ & & & & 6\boldsymbol{i}\,x_3 & = & \lambda^2 \\ & & & & 0x_3 & = & \lambda+\lambda^2(\mu^3-1)\frac{\boldsymbol{i}}{6} \end{array}\right\},$$

so for the system to be consistent we need

$$\lambda+\lambda^2(\mu^3-1)\frac{\boldsymbol{i}}{6}=0 \quad \Leftrightarrow$$
$$\lambda=0 \quad \text{or} \quad \big[\mu^3-1\neq 0 \ \text{ and } \ \lambda=6\boldsymbol{i}(\mu^3-1)^{-1}\big].$$

Case 2: $\kappa^6+1\neq 0$. Then the system has at least two pivot variables, the variables x_1 and x_2, so we need the last row to be zero: indeed, if it were not zero, then

- either the third variable would also be a pivot variable, so the coefficient matrix would be invertible and the system would have a unique solution,
- or there would be a pivot in the last column, so the system would be inconsistent.

On the other hand, if the last row is zero, then the system is consistent and the variable x_3 is a free variable, so the system has infinitely many solutions.

Thus, in this case we need

$$\mu^3 - 1 = 0 \qquad \text{and} \qquad \lambda = 0.$$

Combining all the above, we see that the system has infinitely many solutions if and only if:

$$\begin{gathered}\big[\kappa^6 + 1 = 0 \ \text{ and } \ \lambda = 0\big] \qquad \text{or} \\ \big[\kappa^6 + 1 = 0 \ \text{ and } \ \mu^3 - 1 \neq 0 \ \text{ and } \ \lambda = 6\boldsymbol{i}(\mu^3 - 1)^{-1}\big] \quad \text{or} \\ \big[\kappa^6 + 1 \neq 0 \ \text{ and } \ \mu^3 - 1 = 0 \ \text{ and } \ \lambda = 0\big].\end{gathered}$$

It remains to check for what complex values κ we have $\kappa^6 + 1 = 0$, and similarly for what complex values μ we have $\mu^3 - 1 = 0$.

To solve for κ in $\kappa^6 + 1 = 0 \Leftrightarrow \kappa^6 = -1$, we first solve the corresponding equation $\tilde{\kappa}^6 = 1$. We recall that the polynomial $x^6 - 1$ has 6 complex roots, the numbers

$$\rho_j = e^{2\pi \boldsymbol{i} \frac{j}{6}}, \qquad j = 0, 1, 2, \ldots, 5.$$

Next we find one specific solution to the equation $\kappa^6 = -1$: we note that $-1 = e^{\boldsymbol{i}\pi}$, therefore one solution is the number

$$\kappa_0 = e^{\boldsymbol{i}\pi/6} = \cos(\pi/6) + \boldsymbol{i}\sin(\pi/6) = \frac{\sqrt{3}}{2} + \frac{1}{2}\boldsymbol{i}.$$

Given these, we can conclude that the solutions of the equation $\kappa^6 = -1$ are the numbers

$$\kappa_0 \rho_j = e^{\boldsymbol{i}\pi/6} e^{2\pi \boldsymbol{i} \frac{j}{6}} = e^{2\pi \boldsymbol{i} \frac{2j+1}{12}}, \qquad j = 0, 1, 2, \ldots, 5.$$

Similarly, the polynomial $x^3 - 1$ has 3 complex roots, the numbers

$$\tilde{\rho}_j = e^{2\pi \boldsymbol{i} \frac{j}{3}}, \qquad j = 0, 1, 2.$$

Summarising all the above, we have that the given system has infinitely many solutions in one of the following three cases and in only these:

$$\begin{gathered}\left[\kappa \in \left\{e^{2\pi \boldsymbol{i} \frac{2j+1}{12}} : j = 0, 1, \ldots, 5\right\} \ \text{ and } \ \lambda = 0\right] \qquad \text{or} \\ \left[\kappa \in \left\{e^{2\pi \boldsymbol{i} \frac{2j+1}{12}} : j = 0, 1, \ldots, 5\right\} \ \text{ and } \ \mu \notin \left\{e^{2\pi \boldsymbol{i} \frac{j}{3}} : j = 0, 1, 2\right\} \ \text{ and } \ \lambda = 6\boldsymbol{i}(\mu^3 - 1)^{-1}\right] \quad \text{or} \\ \left[\kappa \notin \left\{e^{2\pi \boldsymbol{i} \frac{2j+1}{12}} : j = 0, 1, \ldots, 5\right\} \ \text{ and } \ \mu \in \left\{e^{2\pi \boldsymbol{i} \frac{j}{3}} : j = 0, 1, 2\right\} \ \text{ and } \ \lambda = 0\right].\end{gathered}$$

Problem 2. (a) We set

$$B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Then we can check that

$$B^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

as we wanted.

(b) We note that the space of matrices

$$\mathcal{R}_2 = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\},$$

which is a subset of $\mathbb{R}^{2\times 2}$, is closed under addition as well as multiplication:

$$\text{if } C = \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix},\ C_2 = \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix},$$
$$\text{then } C_1C_2 = \begin{pmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -a_2b_1 - a_1b_2 & -b_1b_2 + a_1a_2 \end{pmatrix} \in \mathcal{R}_2.$$

Moreover, it contains the zero matrix and I_2, as well as the additive inverse of each one of its elements:

$$\text{if } C = \begin{pmatrix} a & b \\ -b & a \end{pmatrix},\ \text{then } -C = \begin{pmatrix} -a & -b \\ b & -a \end{pmatrix} \in \mathcal{R}_2 \text{ as well.}$$

Thus $\mathcal{R}_2$ is a subring of $\mathbb{R}^{2\times 2}$.

By a proposition discussed in class, it suffices to define a ring isomorphism f from $\mathbb{C}$ to $\mathcal{R}_2$. Indeed, then we will be able to conclude that $\mathcal{R}_2$ is a field too, and hence that f is a field isomorphism.

We define f as follows: for every $z \in \mathbb{C}$, we set

$$f(z) = f\big(\mathrm{Re}(z) + \mathrm{Im}(z)\boldsymbol{i}\big) := \begin{pmatrix} \mathrm{Re}(z) & \mathrm{Im}(z) \\ -\mathrm{Im}(z) & \mathrm{Re}(z) \end{pmatrix}.$$

It remains to check that f is a ring isomorphism, or in other words that it is a ring homomorphism and it is bijective.

For every $z_1, z_2 \in \mathbb{C}$, we have

$$\begin{aligned} f(z_1 + z_2) &= \begin{pmatrix} \mathrm{Re}(z_1 + z_2) & \mathrm{Im}(z_1 + z_2) \\ -\mathrm{Im}(z_1 + z_2) & \mathrm{Re}(z_1 + z_2) \end{pmatrix} \\ &= \begin{pmatrix} \mathrm{Re}(z_1) + \mathrm{Re}(z_2) & \mathrm{Im}(z_1) + \mathrm{Im}(z_2) \\ -\mathrm{Im}(z_1) - \mathrm{Im}(z_2) & \mathrm{Re}(z_1) + \mathrm{Re}(z_2) \end{pmatrix} = f(z_1) + f(z_2), \end{aligned}$$

and similarly

$$\begin{aligned} f(z_1 \cdot z_2) &= \begin{pmatrix} \operatorname{Re}(z_1 \cdot z_2) & \operatorname{Im}(z_1 \cdot z_2) \\ -\operatorname{Im}(z_1 \cdot z_2) & \operatorname{Re}(z_1 \cdot z_2) \end{pmatrix} \\ &= \begin{pmatrix} \operatorname{Re}(z_1) \cdot \operatorname{Re}(z_2) - \operatorname{Im}(z_1) \cdot \operatorname{Im}(z_2) & \operatorname{Re}(z_1) \cdot \operatorname{Im}(z_2) + \operatorname{Re}(z_2) \operatorname{Im}(z_1) \\ -\operatorname{Re}(z_1) \cdot \operatorname{Im}(z_2) - \operatorname{Re}(z_2) \operatorname{Im}(z_1) & \operatorname{Re}(z_1) \cdot \operatorname{Re}(z_2) - \operatorname{Im}(z_1) \cdot \operatorname{Im}(z_2) \end{pmatrix} \\ &= f(z_1) \cdot f(z_2). \end{aligned}$$

Finally, $f(1_{\mathbb{C}}) = I_2$.

We finally check that f is a bijection.

f is injective: Consider $z_1, z_2 \in \mathbb{C}$ with $f(z_1) = f(z_2)$. We need to show that $z_1 = z_2$. By the definition of f, we have

$$\begin{pmatrix} \operatorname{Re}(z_1) & \operatorname{Im}(z_1) \\ -\operatorname{Im}(z_1) & \operatorname{Re}(z_1) \end{pmatrix} = \begin{pmatrix} \operatorname{Re}(z_2) & \operatorname{Im}(z_2) \\ -\operatorname{Im}(z_2) & \operatorname{Re}(z_2) \end{pmatrix}.$$

This implies that the corresponding entries are equal, and hence that $\operatorname{Re}(z_1) = \operatorname{Re}(z_2)$ and $\operatorname{Im}(z_1) = \operatorname{Im}(z_2)$. But then $z_1 = \operatorname{Re}(z_1) + \operatorname{Im}(z_1)\boldsymbol{i} = \operatorname{Re}(z_2) + \operatorname{Im}(z_2)\boldsymbol{i} = z_2$, as we wanted.

f is surjective: Consider C in $\mathcal{R}_2$, the codomain of f. We need to show that C is the image under f of some element in $\mathbb{C}$.

We can find $a, b \in \mathbb{R}$ such that

$$C = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

But then $a + b\boldsymbol{i} \in \mathbb{C}$ and $f(a + b\boldsymbol{i}) = C$, as we wanted.

Problem 3. For every $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$, define the matrix S_{ij} to be the matrix whose (i,j)-entry is equal to 1, while all other entries are equal to 0.

We will show that the set $\mathcal{B}_0 = \{S_{ij} : 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\}$ is a basis of $\mathbb{F}^{m\times n}$.

Let us first show that $\mathcal{B}_0$ is a spanning set of $\mathbb{F}^{m\times n}$. Consider an arbitrary matrix $A \in \mathbb{F}^{m\times n}$, $A = (a_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}$. Then

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots\cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots\cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots\cdots & a_{3n} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots\cdots & a_{mn} \end{pmatrix}$$

$$= \begin{pmatrix} a_{11} & 0 & 0 & \cdots\cdots & 0 \\ 0 & 0 & 0 & \cdots\cdots & 0 \\ 0 & 0 & 0 & \cdots\cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots\cdots & 0 \end{pmatrix} + \begin{pmatrix} 0 & a_{12} & a_{13} & \cdots\cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots\cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots\cdots & a_{3n} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots\cdots & a_{mn} \end{pmatrix}$$

$$= a_{11}S_{11} + \begin{pmatrix} 0 & a_{12} & 0 & \cdots\cdots & 0 \\ 0 & 0 & 0 & \cdots\cdots & 0 \\ 0 & 0 & 0 & \cdots\cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots\cdots & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & a_{13} & \cdots\cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots\cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots\cdots & a_{3n} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots\cdots & a_{mn} \end{pmatrix}$$

$$= \cdots\cdots\cdots$$

$$= \sum_{j=1}^{n} a_{1j}S_{1j} + \begin{pmatrix} 0 & 0 & 0 & \cdots\cdots & 0 \\ a_{21} & 0 & 0 & \cdots\cdots & 0 \\ 0 & 0 & 0 & \cdots\cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots\cdots & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & \cdots\cdots & 0 \\ 0 & a_{22} & a_{23} & \cdots\cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots\cdots & a_{3n} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots\cdots & a_{mn} \end{pmatrix}$$

$$= \cdots\cdots\cdots = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}S_{ij}.$$

Thus we see that any matrix $A \in \mathbb{F}^{m\times n}$ can be written as a linear combination of the matrices S_{ij}, or in other words that $\mathcal{B}_0$ is a spanning set of $\mathbb{F}^{m\times n}$.

We now check that it is linearly independent too. Suppose that λ_{ij},

$1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$, are scalars that satisfy

$$\sum_{i=1}^{m} \sum_{j=1}^{n} \lambda_{ij} S_{ij} = \boldsymbol{O},$$

where $\boldsymbol{O}$ is the zero matrix in $\mathbb{F}^{m \times n}$. By reversing what we did before, we can see that

$$\sum_{i=1}^{m} \sum_{j=1}^{n} \lambda_{ij} S_{ij} = \big(\lambda_{ij}\big)_{\substack{1 \leqslant i \leqslant m, \\ 1 \leqslant j \leqslant n}}$$

thus for this matrix to be equal to the zero matrix we need to have $\lambda_{ij} = 0$ for every $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$. We conclude that $\mathcal{B}_0$ is linearly independent.

By combining the above, we see that $\mathcal{B}_0$ is a basis of the space $\mathbb{F}^{m \times n}$ over the field $\mathbb{F}$, and hence its size $m \cdot n$ is the dimension of the space.

Problem 4. (a) To show that each of the two sets is not $\mathbb{R}$-linearly independent, we need to check that 0 can be written as a linear combination of the elements in the set with coefficients that are not all zero.

For the first set, we can use the coefficients $\lambda_1 = \sqrt{5}$, $\lambda_2 = -\sqrt{2}$: we have that $\lambda_1 \cdot \sqrt{2} + \lambda_2 \cdot \sqrt{5} = 0$, as we wanted.

For the second set, we can use the same coefficients as before as well as $\lambda_3 = 0$: we have that $\lambda_1 \cdot \sqrt{2} + \lambda_2 \cdot \sqrt{5} + \lambda_3 \cdot \sqrt{7} = 0$, as we wanted.

(b) We first show that the set $\left\{\sqrt{2}, \sqrt{5}, \sqrt{7}\right\}$ is $\mathbb{Q}$-linearly independent. Suppose $p_1, p_2, p_3 \in \mathbb{Q}$ are such that $p_1 \cdot \sqrt{2} + p_2 \cdot \sqrt{5} + p_3 \cdot \sqrt{7} = 0$. We need to show that $p_1 = p_2 = p_3 = 0$.

We can write:

$$\begin{aligned} p_1 \cdot \sqrt{2} + p_2 \cdot \sqrt{5} + p_3 \cdot \sqrt{7} = 0 \quad &\Rightarrow \quad \text{(multiply both sides by } \sqrt{2}\text{)} \\ p_2\sqrt{10} + p_3\sqrt{14} = -2p_1 \quad &\Rightarrow \quad \text{(square both sides)} \\ 10p_2^2 + 14p_3^2 + 2p_2p_3\sqrt{140} = 4p_1^2 \quad &\Rightarrow \\ p_2p_3\sqrt{140} \in \mathbb{Q}. \end{aligned}$$

But 140 is not the square of an integer, therefore, according to the given hint, $\sqrt{140}$ is irrational, and the only way the last line holds true is if $p_2p_3 = 0 \Rightarrow p_2 = 0$ or $p_3 = 0$.

But then going back to the second equality, we get that $p_2\sqrt{10} + p_3\sqrt{14} \in \mathbb{Q}$ and at most one of p_2, p_3 can be non-zero. Given that $\sqrt{10}$ and $\sqrt{14}$ are also irrational, this can only happen if both p_2 and p_3 are equal to zero. But then, combining this with the first equality, we also get that $p_1 = 0$.

Next we show that the set $\left\{\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{10}\right\}$ is also $\mathbb{Q}$-linearly independent. Since we already saw that $\left\{\sqrt{2}, \sqrt{5}, \sqrt{7}\right\}$ is $\mathbb{Q}$-linearly independent, by a theorem we proved in class (Theorem 1 from the November 27 Lecture Notes) it suffices to show that $\sqrt{10}$ is not in the linear span of $\left\{\sqrt{2}, \sqrt{5}, \sqrt{7}\right\}$ (if the scalars are coming from $\mathbb{Q}$).

Assume towards a contradiction that we could write $\sqrt{10}$ as a linear combination of $\sqrt{2}, \sqrt{5}$ and $\sqrt{7}$ using coefficients from $\mathbb{Q}$; in other words, assume there are $q_1, q_2, q_3 \in \mathbb{Q}$ such that

$$\sqrt{10} = q_1 \cdot \sqrt{2} + q_2 \cdot \sqrt{5} + q_3 \cdot \sqrt{7}. \tag{1}$$

Then we can write

$$\begin{aligned} q_1 \cdot \sqrt{2} + q_2 \cdot \sqrt{5} = \sqrt{10} - q_3\sqrt{7} \quad &\Rightarrow \quad \text{(square both sides)} \\ 2q_1^2 + 5q_2^2 + 2q_1q_2\sqrt{10} = 10 + 7q_3^2 - 2q_3\sqrt{70} \quad &\Rightarrow \\ q_1q_2\sqrt{10} + q_3\sqrt{70} \in \mathbb{Q} \quad &\Rightarrow \quad \text{(square the expression)} \\ 10q_1^2q_2^2 + 70q_3^2 + 2q_1q_2q_3\sqrt{700} \in \mathbb{Q} \quad &\Rightarrow \\ q_1q_2q_3\sqrt{700} \in \mathbb{Q}. \end{aligned}$$

Since 700 is not the square of an integer, the last line can hold true only if $q_1q_2q_3 = 0 \Rightarrow q_1q_2 = 0$ or $q_3 = 0$.

But then returning to the third line above, we see that $q_1q_2\sqrt{10}+q_3\sqrt{70} \in \mathbb{Q}$ and at most one of q_1q_2, q_3 can be non-zero. Given that $\sqrt{10}$ and $\sqrt{70}$ are also irrational, this can only happen if both q_1q_2 and q_3 are equal to zero.

With these in mind, we look again at (1): it gives us

$$q_1 \cdot \sqrt{2} + q_2 \cdot \sqrt{5} = \sqrt{10} \quad \Rightarrow \quad q_1 \cdot \sqrt{20} + q_2 \cdot \sqrt{50} = 10 \in \mathbb{Q}$$

with at most one of q_1, q_2 being non-zero. Given that $\sqrt{20}, \sqrt{50}$ are both irrational (since they are not squares of integers), we conclude that q_1, q_2 are both zero.

In other words, (1) can be rewritten as $\sqrt{10} = 0$, which is absurd, and shows that assuming (1) can be true for some $q_1, q_2, q_3 \in \mathbb{Q}$ was incorrect.

Finally we check that $\{\sqrt{2}, \sqrt{6}, \sqrt{8}\}$ is not $\mathbb{Q}$-linearly independent. Indeed, set $\mu_1 = 2, \mu_2 = 0, \mu_3 = -1$. Then

$$\mu_1 \cdot \sqrt{2} + \mu_2 \cdot \sqrt{6} + \mu_3 \cdot \sqrt{8} = 2\sqrt{2} - \sqrt{8} = \sqrt{4 \cdot 2} - \sqrt{8} = 0,$$

as we wanted.

(c) We recall the tables of addition and multiplication for $\mathbb{F}_4$ that we came up with for HW2, Problem 3. We set $\mathbb{F}_4 = \{0, 1, c, d\}$ with the elements satisfying the following:

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

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

.

From this it follows that $\{1, c\}$ is a basis of $\mathbb{F}_4$ over the scalar field $\mathbb{Z}_2$. Indeed, in this setting the scalars can only be 0 or 1, and from the above tables we have that

$$0 \cdot 1 + 0 \cdot c = 0, \quad 1 \cdot 1 + 0 \cdot c = 1, \quad 0 \cdot 1 + 1 \cdot c = c,$$
$$1 \cdot 1 + 1 \cdot c = 1 + c = d.$$

These imply that a linear combination of 1 and c is equal to 0 only if both coefficients are equal to 0, giving the linear independence of $\{1, c\}$, and also shows that the linear span of $\{1, c\}$ is the entire field $\mathbb{F}_4$.

Using this, we will now construct a basis of $\mathbb{F}_4^{2\times 2}$ over $\mathbb{Z}_2$. Recall the matrices S_{ij} that we defined in Problem 3 above. We will check that the set

$$\mathcal{B}_1 = \big\{S_{ij}, cS_{ij} : 1 \leqslant i, j \leqslant 2\big\}$$

is linearly independent if we use scalars from $\mathbb{Z}_2$ and spans $\mathbb{F}_4^{2\times 2}$.

Indeed, consider a matrix $A \in \mathbb{F}_4^{2\times 2}$, $A = (a_{ij})_{1\leqslant i,j\leqslant 2}$. For every $1 \leqslant i, j \leqslant 2$, $a_{ij} \in \mathbb{F}_4$, and hence, from what we showed above, there exist $\lambda_{ij}, \mu_{ij} \in \mathbb{Z}_2$ so that

$$a_{ij} = \lambda_{ij} \cdot 1 + \mu_{ij} \cdot c.$$

But then, again as we showed above, we can write

$$\begin{aligned} A = \sum_{i=1}^{2}\sum_{j=1}^{2} a_{ij}S_{ij} &= \sum_{i=1}^{2}\sum_{j=1}^{2} \big(\lambda_{ij}1 + \mu_{ij}c\big)S_{ij} \\ &= \sum_{i=1}^{2}\sum_{j=1}^{2} \lambda_{ij}(S_{ij}) + \sum_{i=1}^{2}\sum_{j=1}^{2} \mu_{ij}(cS_{ij}). \end{aligned}$$

Thus A is in the linear span of $\mathcal{B}_1$ that we get if we use scalars from $\mathbb{Z}_2$. Since this matrix A was arbitrary, we get that $\mathcal{B}_1$ is a spanning set of the space $\mathbb{F}_4^{2\times 2}$ over $\mathbb{Z}_2$.

It remains to check that $\mathcal{B}_1$ is $\mathbb{Z}_2$-linearly independent. Suppose that λ_{ij}, μ_{ij}, $1 \leqslant i, j \leqslant 2$, are taken from $\mathbb{Z}_2$ and satisfy

$$\sum_{i=1}^{2}\sum_{j=1}^{2} \lambda_{ij}(S_{ij}) + \sum_{i=1}^{2}\sum_{j=1}^{2} \mu_{ij}(cS_{ij}) = \boldsymbol{O},$$

where $\boldsymbol{O}$ is the zero matrix in $\mathbb{F}_4^{2\times 2}$. As before, we can write

$$\sum_{i=1}^{2}\sum_{j=1}^{2} \lambda_{ij}(S_{ij}) + \sum_{i=1}^{2}\sum_{j=1}^{2} \mu_{ij}(cS_{ij}) = \big(\lambda_{ij} \cdot 1 + \mu_{ij} \cdot c\big)_{1\leqslant i,j\leqslant 2},$$

thus for this matrix to be equal to the zero matrix we need to have $\lambda_{ij} \cdot 1 + \mu_{ij} \cdot c = 0$ for every $1 \leqslant i, j \leqslant 2$. By the linear independence of $\{1, c\}$, we conclude that $\lambda_{ij} = \mu_{ij} = 0$ for every $1 \leqslant i, j \leqslant 2$. This shows that $\mathcal{B}_1$ is $\mathbb{Z}_2$-linearly independent.

We have therefore verified that $\mathcal{B}_1$ is a basis of $\mathbb{F}_4^{2\times 2}$ over $\mathbb{Z}_2$. It follows that the dimension of $\mathbb{F}_4^{2\times 2}$ over $\mathbb{Z}_2$ is equal to $|\mathcal{B}_1| = 8$.

Problem 5. By our assumptions we have that there is a basis $\mathcal{B}_0$ of V with size n (in fact, by the Main Theorem in the November 27 Lecture Notes, we know that every basis of V has size n).

Assume now towards a contradiction that S is not a basis of V. Since S is linearly independent by our assumptions, we must have that S is not a spanning set of V. That is, there exists some $w \in V$ that is not contained in $\text{span}(S)$.

But then w is not contained in S either, therefore the size of $S \cup \{w\}$ is $|S| + 1 = n + 1$. At the same time, by Theorem 1 from the November 27 Lecture Notes, $S \cup \{w\}$ is linearly independent. Thus we have a linearly independent subset of V that has size larger than the size of the basis $\mathcal{B}_0$. On the other hand, the proof of the Main Theorem that we gave relies on showing that this is impossible.

Therefore, we have reached an absurd conclusion, which shows that the assumption that S is not a spanning set of V was incorrect.

We can conclude that S is a spanning set of V, and hence a basis of V.

Problem 6. We show that (a) through (d) are the same problem essentially in the following way:

1. each solution $x_1 = \lambda_1, x_2 = \lambda_2$ and $x_3 = \lambda_3$ to the system in (a) gives a triple of coefficients that allow us to write the vector $\bar{b}$ as a linear combination of the vector $\bar{u}$, $\bar{v}$ and $\bar{w}$ as follows: $\bar{b} = \lambda_1\bar{u} + \lambda_2\bar{v} + \lambda_3\bar{w}$;

2. each way of writing $\bar{b}$ as a linear combination of the vector $\bar{u}$, $\bar{v}$ and $\bar{w}$ corresponds to a triple of coefficients $\lambda_1, \lambda_2, \lambda_3$ that make the equality $\bar{b} = \lambda_1\bar{u} + \lambda_2\bar{v} + \lambda_3\bar{w}$ true; this triple gives us a column vector $\begin{pmatrix}\lambda_1\\ \lambda_2\\ \lambda_3\end{pmatrix}$ which is a solution to the vector equation $A\bar{x} = \bar{b}$;

3. each solution to the vector equation $A\bar{x} = \bar{b}$ is a preimage under f of the vector $\bar{b}$;

4. each preimage $\begin{pmatrix}\lambda_1\\ \lambda_2\\ \lambda_3\end{pmatrix}$ of the vector $\bar{b}$ under f gives a solution to the system in (a) if we set $x_1 = \lambda_1, x_2 = \lambda_2$ and $x_3 = \lambda_3$.

We can thus conclude that the solution set to each of the problems (a) through (c) is essentially contained in the solution set of the subsequent problem, while the solution set to problem (d) is contained in the solution set of the system in (a). This implies that all these solutions sets coincide.

We begin by showing 1. Let us suppose that $x_1 = \lambda_1, x_2 = \lambda_2$ and $x_3 = \lambda_3$ is a solution to the system in (a). Then we have that

$$\begin{Bmatrix} 3\lambda_1 + 2\lambda_2 & +\lambda_3 = & 9 \\ \lambda_1 & -2\lambda_3 = & -8 \\ 2\lambda_1 & -2\lambda_3 = & -6 \end{Bmatrix} \quad \Rightarrow \quad \begin{pmatrix} 3\lambda_1 + 2\lambda_2 + \lambda_3 \\ \lambda_1 - 2\lambda_3 \\ 2\lambda_1 - 2\lambda_3 \end{pmatrix} = \begin{pmatrix} 9 \\ -8 \\ -6 \end{pmatrix}$$

$$\Rightarrow \quad \begin{pmatrix} 3\lambda_1 \\ \lambda_1 \\ 2\lambda_1 \end{pmatrix} + \begin{pmatrix} 2\lambda_2 \\ 0\lambda_2 \\ 0\lambda_2 \end{pmatrix} + \begin{pmatrix} \lambda_3 \\ -2\lambda_3 \\ -2\lambda_3 \end{pmatrix} = \begin{pmatrix} 9 \\ -8 \\ -6 \end{pmatrix}$$

$$\Rightarrow \quad \lambda_1 \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix} + \lambda_2 \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} + \lambda_3 \begin{pmatrix} 1 \\ -2 \\ -2 \end{pmatrix} = \begin{pmatrix} 9 \\ -8 \\ -6 \end{pmatrix},$$

that is, the scalars $\lambda_1, \lambda_2, \lambda_3$ make the equality $\bar{b} = \lambda_1\bar{u} + \lambda_2\bar{v} + \lambda_3\bar{w}$ true.

Next we show 2. Suppose $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ are coefficients for which the

equality $\bar{b} = \lambda_1\bar{u} + \lambda_2\bar{v} + \lambda_3\bar{w}$ holds true. Then

$$\lambda_1 \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix} + \lambda_2 \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} + \lambda_3 \begin{pmatrix} 1 \\ -2 \\ -2 \end{pmatrix} = \begin{pmatrix} 9 \\ -8 \\ -6 \end{pmatrix} \quad \Rightarrow$$

$$\begin{pmatrix} 3\lambda_1 \\ \lambda_1 \\ 2\lambda_1 \end{pmatrix} + \begin{pmatrix} 2\lambda_2 \\ 0\lambda_2 \\ 0\lambda_2 \end{pmatrix} + \begin{pmatrix} \lambda_3 \\ -2\lambda_3 \\ -2\lambda_3 \end{pmatrix} = \begin{pmatrix} 9 \\ -8 \\ -6 \end{pmatrix} \quad \Rightarrow \quad \begin{pmatrix} 3\lambda_1 + 2\lambda_2 + 1\lambda_3 \\ 1\lambda_1 + 0\lambda_2 - 2\lambda_3 \\ 2\lambda_1 + 0\lambda_2 - 2\lambda_3 \end{pmatrix} = \begin{pmatrix} 9 \\ -8 \\ -6 \end{pmatrix}$$

$$\Rightarrow A \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 0 & -2 \\ 2 & 0 & -2 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} = \begin{pmatrix} 9 \\ -8 \\ -6 \end{pmatrix} = \bar{b}.$$

Next we show 3. Suppose $\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix}$ is a solution to the vector equation $A\bar{x} = \bar{b}$. Then

$$\begin{pmatrix} 3 & 2 & 1 \\ 1 & 0 & -2 \\ 2 & 0 & -2 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} = \begin{pmatrix} 9 \\ -8 \\ -6 \end{pmatrix}$$

$$\Rightarrow \quad \begin{pmatrix} 3\lambda_1 + 2\lambda_2 + 1\lambda_3 \\ 1\lambda_1 + 0\lambda_2 - 2\lambda_3 \\ 2\lambda_1 + 0\lambda_2 - 2\lambda_3 \end{pmatrix} = \begin{pmatrix} 9 \\ -8 \\ -6 \end{pmatrix} \quad \Rightarrow \quad f\left(\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} \right) = \begin{pmatrix} 9 \\ -8 \\ -6 \end{pmatrix},$$

so $\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix}$ is mapped to $\begin{pmatrix} 9 \\ -8 \\ -6 \end{pmatrix}$ by f, and thus $\begin{pmatrix} 9 \\ -8 \\ -6 \end{pmatrix}$ is in the range of f.

Finally we show 4. Suppose $\begin{pmatrix} 9 \\ -8 \\ -6 \end{pmatrix}$ is in the range of f, and one of its preimages is the vector $\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix}$. Then

$$\begin{pmatrix} 3\lambda_1 + 2\lambda_2 + \lambda_3 \\ \lambda_1 - 2\lambda_3 \\ 2\lambda_1 - 2\lambda_3 \end{pmatrix} = f\left(\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} \right) = \begin{pmatrix} 9 \\ -8 \\ -6 \end{pmatrix} \quad \Rightarrow \quad \begin{Bmatrix} 3\lambda_1 + 2\lambda_2 & +\lambda_3 = & 9 \\ \lambda_1 & -2\lambda_3 = & -8 \\ 2\lambda_1 & -2\lambda_3 = & -6 \end{Bmatrix},$$

so one solution to the system in (a) is given by $x_1 = \lambda_1, x_2 = \lambda_2$ and $x_3 = \lambda_3$.

It remains to solve one version of the problem: we solve part (a). The augmented matrix of the system is

$$\left(\begin{array}{ccc|c} 3 & 2 & 1 & 9 \\ 1 & 0 & -2 & -8 \\ 2 & 0 & -2 & -6 \end{array} \right),$$

which is row equivalent to the following matrices:

$$\left(\begin{array}{ccc|c} 1 & 0 & -2 & -8 \\ 3 & 2 & 1 & 9 \\ 2 & 0 & -2 & -6 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & -2 & -8 \\ 0 & 2 & 7 & 33 \\ 0 & 0 & 2 & 10 \end{array}\right).$$

The last matrix is in REF and has 3 pivots with no pivot in the last column. Therefore, the corresponding linear system

$$\left\{\begin{array}{rcl} x_1 - 2x_3 &=& -8 \\ 2x_2 + 7x_3 &=& 33 \\ 2x_3 &=& 10 \end{array}\right\}$$

is upper triangular, and has a unique solution which we can find using back-substitution:

from the last equation we get $x_3 = 5$, which plugged into the first and second equations also gives $x_1 - 10 = -8 \Rightarrow x_1 = 2$,
$2x_2 + 35 = 33 \Rightarrow x_2 = -1$.

Problem 7. We have that:

(i) this f is linear, injective and surjective. Indeed, for every $\bar{x} = \left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right), \bar{y} = \left(\begin{smallmatrix} y_1 \\ y_2 \end{smallmatrix}\right) \in \mathbb{R}^2$ and every $r \in \mathbb{R}$ we have

$$f(\bar{x}+\bar{y}) = f\left(\begin{pmatrix} x_1+y_1 \\ x_2+y_2 \end{pmatrix}\right) = \begin{pmatrix} -x_1-y_1 \\ x_2+y_2 \end{pmatrix} = \begin{pmatrix} -x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} -y_1 \\ y_2 \end{pmatrix} = f(\bar{x}) + f(\bar{y})$$
$$\text{and} \quad f(r\bar{x}) = f\left(\begin{pmatrix} rx_1 \\ rx_2 \end{pmatrix}\right) = \begin{pmatrix} -rx_1 \\ rx_2 \end{pmatrix} = rf(\bar{x}),$$

thus f is linear.

Also, if $f(\bar{x}) = f(\bar{y})$, then

$$\begin{pmatrix} -x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -y_1 \\ y_2 \end{pmatrix} \quad \Rightarrow \quad x_1 = y_1 \ \text{ and } \ x_2 = y_2$$
$$\Rightarrow \quad \bar{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \bar{y},$$

thus f is injective.

Finally, given $\bar{z} = \left(\begin{smallmatrix} z_1 \\ z_2 \end{smallmatrix}\right) \in \mathbb{R}^2$, we have that $\left(\begin{smallmatrix} -z_1 \\ z_2 \end{smallmatrix}\right) \in \mathbb{R}^2$ too and

$$f\left(\begin{pmatrix} -z_1 \\ z_2 \end{pmatrix}\right) = \begin{pmatrix} -(-z_1) \\ z_2 \end{pmatrix} = \bar{z},$$

thus f is surjective.

(ii) this f is not linear, it is not injective and it is not surjective. Indeed,

$$f\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \quad \text{while} \quad f\left(\begin{pmatrix} 2 \\ 2 \end{pmatrix}\right) = \begin{pmatrix} 4 \\ 4 \end{pmatrix} \neq 2\begin{pmatrix} 2 \\ 1 \end{pmatrix} = 2f\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right),$$

thus f is not linear.

Also, $f\left(\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)\right) = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = f\left(\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)\right)$, thus f is not injective.

Finally, we show that $\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$ is not in the range of f. Assume towards a contradiction that there is $\left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right) \in \mathbb{R}^2$ such that

$$f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad \Leftrightarrow \qquad \begin{pmatrix} x_1+x_2 \\ x_1x_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Given that we want $x_1x_2 = 1$, none of the x_1, x_2 can be zero, and moreover either both of them are positive or both of them are negative. But if both of them were negative, then $x_1 + x_2 < 0$ and thus $\neq 1$. So

both x_1, x_2 need to be positive. But then $x_1 = x_1 + 0 < x_1 + x_2 = 1$, and similarly $x_2 < x_1 + x_2 = 1$. Thus $x_1, x_2 \in (0,1)$ and they satisfy $x_1 x_2 = 1 \Rightarrow x_2 = \frac{1}{x_1}$. These imply that

$$x_1 + x_2 = x_1 + \frac{1}{x_1} = \frac{x_1^2 + 1}{x_1} > \frac{1}{x_1} > 1 \quad \text{given that} \quad 0 < x_1 < 1,$$

which contradicts our assumption that $x_1 + x_2 = 1$.

(iii) this f is not linear, it is not injective and it is not surjective. Indeed,

$$f\left(\begin{pmatrix}1\\1\end{pmatrix}\right) = \begin{pmatrix}0\\1\end{pmatrix}, \quad \text{while} \quad f\left(\begin{pmatrix}2\\2\end{pmatrix}\right) = \begin{pmatrix}0\\1\end{pmatrix} \neq \begin{pmatrix}0\\2\end{pmatrix} = 2f\left(\begin{pmatrix}1\\1\end{pmatrix}\right),$$

thus f is not linear.

Also, we just saw that $f\left(\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)\right) = f\left(\left(\begin{smallmatrix}2\\2\end{smallmatrix}\right)\right)$, thus f is not injective.

Finally, we show that $\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$ is not in the range of f. Assume towards a contradiction that there is $\left(\begin{smallmatrix}x_1\\x_2\end{smallmatrix}\right) \in \mathbb{Z}_3^2$ such that

$$f\left(\begin{pmatrix}x_1\\x_2\end{pmatrix}\right) = \begin{pmatrix}1\\1\end{pmatrix} \qquad \Leftrightarrow \qquad \begin{pmatrix}x_1 - x_2\\x_1 x_2\end{pmatrix} = \begin{pmatrix}1\\1\end{pmatrix}.$$

Given that we want $x_1 x_2 = 1$, none of the x_1, x_2 can be zero, thus $x_1, x_2 \in \{1, 2\}$. Note moreover that if we had $x_1 \neq x_2$ combined with $x_1, x_2 \in \{1, 2\}$, then we would get $x_1 x_2 = 2 \neq 1$. Therefore we must have $x_1 = x_2$. This in turn implies that $x_1 - x_2 = 0$, which contradicts our assumption that $x_1 - x_2 = 1$.

(iv) this f is linear and surjective, but it is not injective. Indeed, for every $\bar{x} = \left(\begin{smallmatrix}x_1\\x_2\end{smallmatrix}\right), \bar{y} = \left(\begin{smallmatrix}y_1\\y_2\end{smallmatrix}\right) \in \mathbb{R}^2$ and every $r \in \mathbb{R}$ we have

$$\begin{aligned} f(\bar{x} + \bar{y}) = f\left(\begin{pmatrix}x_1 + y_1\\x_2 + y_2\end{pmatrix}\right) &= (x_1 + y_1) + (x_2 + y_2) \\ &= (x_1 + x_2) + (y_1 + y_2) = f(\bar{x}) + f(\bar{y}) \\ \text{and} \quad f(r\bar{x}) = f\left(\begin{pmatrix}rx_1\\rx_2\end{pmatrix}\right) &= rx_1 + rx_2 = r(x_1 + x_2) = rf(\bar{x}), \end{aligned}$$

thus f is linear.

Also, given $s \in \mathbb{R}$, we have that $f\left(\left(\begin{smallmatrix}s\\0\end{smallmatrix}\right)\right) = s + 0 = s$, thus f is surjective.

However, we also have $f\left(\left(\begin{smallmatrix}0\\s\end{smallmatrix}\right)\right) = s$, thus f is not injective (given that the vectors $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$, which are different, are mapped to the same element).

(v) this f is injective and surjective, but it is not linear. Indeed, $f(\bar{0}) = \binom{1}{2} \neq \bar{0}$, thus f is not linear.

On the other hand, if $f(\bar{x}) = f(\bar{y})$, then

$$\begin{pmatrix} x_1+1 \\ x_2+2 \end{pmatrix} = \begin{pmatrix} y_1+1 \\ y_2+2 \end{pmatrix} \quad \Rightarrow \quad x_1+1 = y_1+1 \ \text{ and } \ x_2+2 = y_2+2$$

$$\Rightarrow \quad x_1 = y_1 \ \text{ and } \ x_2 = y_2 \Rightarrow \quad \bar{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \bar{y},$$

thus f is injective.

Finally, given $\bar{z} = \binom{z_1}{z_2} \in \mathbb{R}^2$, we have that $\binom{z_1-1}{z_2-2} \in \mathbb{R}^2$ too and

$$f\left(\begin{pmatrix} z_1-1 \\ z_2-2 \end{pmatrix}\right) = \begin{pmatrix} (z_1-1)+1 \\ (z_2-2)+2 \end{pmatrix} = \bar{z},$$

thus f is surjective.

(vi) this f is linear, injective and surjective. Indeed, for every $\bar{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \bar{y} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \in \mathbb{Z}_5^3$ and every $s \in \mathbb{Z}_5$ we have

$$f(\bar{x}+\bar{y}) = f\left(\begin{pmatrix} x_1+y_1 \\ x_2+y_2 \\ x_3+y_3 \end{pmatrix}\right) = \begin{pmatrix} x_2+y_2 \\ x_3+y_3 \\ x_1+y_1 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_3 \\ x_1 \end{pmatrix} + \begin{pmatrix} y_2 \\ y_3 \\ y_1 \end{pmatrix} = f(\bar{x}) + f(\bar{y})$$

$$\text{and } \ f(s\bar{x}) = f\left(\begin{pmatrix} sx_1 \\ sx_2 \\ sx_3 \end{pmatrix}\right) = \begin{pmatrix} sx_2 \\ sx_3 \\ sx_1 \end{pmatrix} = sf(\bar{x}),$$

thus f is linear.

Also, if $f(\bar{x}) = f(\bar{y})$, then

$$\begin{pmatrix} x_2 \\ x_3 \\ x_1 \end{pmatrix} = \begin{pmatrix} y_2 \\ y_3 \\ y_1 \end{pmatrix} \quad \Rightarrow \quad x_2 = y_2, \quad x_3 = y_3 \ \text{ and } \ x_1 = y_1$$

$$\Rightarrow \quad \bar{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \bar{y},$$

thus f is injective.

Finally, given $\bar{z} = \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} \in \mathbb{Z}_5^3$, we have that $\begin{pmatrix} z_3 \\ z_1 \\ z_2 \end{pmatrix} \in \mathbb{Z}_5^3$ too and

$$f\left(\begin{pmatrix} z_3 \\ z_1 \\ z_2 \end{pmatrix}\right) = \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix},$$

as we wanted. Thus f is surjective.

(vii) this f is linear and injective, but it is not surjective. Indeed, for every $\bar{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \bar{y} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \in \mathbb{R}^3$ and every $r \in \mathbb{R}$ we have

$$f(\bar{x}+\bar{y}) = f\left(\begin{pmatrix} x_1+y_1 \\ x_2+y_2 \\ x_3+y_3 \end{pmatrix}\right) = \begin{pmatrix} x_1+y_1 & x_2+y_2 \\ 0 & x_3+y_3 \end{pmatrix}$$
$$= \begin{pmatrix} x_1 & x_2 \\ 0 & x_3 \end{pmatrix} + \begin{pmatrix} y_1 & y_2 \\ 0 & y_3 \end{pmatrix} = f(\bar{x}) + f(\bar{y})$$
$$\text{and} \quad f(r\bar{x}) = f\left(\begin{pmatrix} rx_1 \\ rx_2 \\ rx_3 \end{pmatrix}\right) = \begin{pmatrix} rx_1 & rx_2 \\ 0 & rx_3 \end{pmatrix} = \begin{pmatrix} rx_1 & rx_2 \\ r\cdot 0 & rx_3 \end{pmatrix} = rf(\bar{x}),$$

thus f is linear.

Also, if $f(\bar{x}) = f(\bar{y})$, then

$$\begin{pmatrix} x_1 & x_2 \\ 0 & x_3 \end{pmatrix} = \begin{pmatrix} y_1 & y_2 \\ 0 & y_3 \end{pmatrix} \quad \Rightarrow \quad x_1 = y_1, \quad x_2 = y_2 \ \text{ and } \ x_3 = y_3$$
$$\Rightarrow \quad \bar{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \bar{y},$$

thus f is injective.

Finally, note that $C = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ is not in the range of this f, thus f is not surjective.

(viii) this f is not linear and it is not surjective, but it is injective. Indeed, for every matrix $C = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in the range of f, we should have $c+d = 1$. But then the zero matrix cannot be in the range of f, which shows both that f is not linear (why?) and that it is not surjective.

On the other hand this f is injective: consider $\bar{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \bar{y} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \in \mathbb{R}^3$ that satisfy

$$f\left(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}\right) = f\left(\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}\right) \quad \Leftrightarrow \quad \begin{pmatrix} x_1 & x_2 \\ 1-x_3 & x_3 \end{pmatrix} = \begin{pmatrix} y_1 & y_2 \\ 1-y_3 & y_3 \end{pmatrix}.$$

Then we must have $x_1 = y_1, x_2 = y_2$ and $x_3 = y_3$, hence $\bar{x} = \bar{y}$.

(b) Note that out of the first six functions, the only ones that we found are linear are the functions in part (i), part (iv) and part (iv). We give a matrix representation for each one of these:

(i) Let

$$A_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{R}^{2\times 2}.$$

Then, for every $\bar{x} = \left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right) \in \mathbb{R}^2$, we have

$$A_1\bar{x} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -x_1 \\ x_2 \end{pmatrix} = f(\bar{x}).$$

(iv) Let

$$A_2 = \begin{pmatrix} 1 & 1 \end{pmatrix} \in \mathbb{R}^{1\times 2}.$$

Then, for every $\bar{x} = \left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right) \in \mathbb{R}^2$, we have

$$A_2\bar{x} = \begin{pmatrix} 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = x_1 + x_2 = f(\bar{x}).$$

(vi) Let

$$A_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \in \mathbb{Z}_5^{3\times 3}.$$

Then, for every $\bar{x} = \left(\begin{smallmatrix} x_1 \\ x_2 \\ x_3 \end{smallmatrix}\right) \in \mathbb{Z}_5^3$, we have

$$A_3\bar{x} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_3 \\ x_1 \end{pmatrix} = f(\bar{x}).$$