Math 227 Suggested solutions to Homework Set 2

Problem 1. (a) We check all the axioms of a commutative ring for \mathcal{R}_1 .

 $+_1$ is commutative: Consider two real polynomials $p, q \in \mathcal{P}$. There are $n \in \mathbb{N}$ and coefficients $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_n \in \mathbb{R}$ such that

$$p(x) = a_0 + a_1 x + \dots + a_n x^n, \qquad q(x) = b_0 + b_1 x + \dots + b_n x^n$$

(here we choose n to be larger than or equal to both the degree of the polynomial p and the degree of the polynomial q, so we may need to take some of the coefficients of higher-order terms equal to 0).

We then have

$$p(x) +_1 q(x) = (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_n + b_n)x^n$$

= $(b_0 + a_0) + (b_1 + a_1)x + \dots + (b_n + a_n)x^n = q(x) +_1 p(x),$

where the second equality holds because addition in \mathbb{R} is commutative, and where in the first and third equalities we also use generalised associativity of the addition in \mathbb{R} along with generalised commutativity.

 $+_1$ is associative: Consider three real polynomials $p, q, r \in \mathcal{P}$. There are $n \in \mathbb{N}$ and coefficients $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_n, c_0, c_1, \ldots, c_n \in \mathbb{R}$ such that

$$p(x) = a_0 + a_1 x + \dots + a_n x^n, q(x) = b_0 + b_1 x + \dots + b_n x^n,$$

 $r(x) = c_0 + c_1 x + \dots + c_n x^n$

(here we choose n to be larger than or equal to the maximum of the degrees of the polynomials p, q and r).

We then have

$$(p(x) +_1 q(x)) +_1 r(x)$$

$$= ((a_0 + b_0) + (a_1 + b_1)x + \dots + (a_n + b_n)x^n) + (c_0x + c_1x + \dots + c_nx^n)$$

$$= ((a_0 + b_0) + c_0) + ((a_1 + b_1) + c_1)x + \dots + ((a_n + b_n) + c_n)x^n$$

$$= (a_0 + (b_0 + c_0)) + (a_1 + (b_1 + c_1))x + \dots + (a_n + (b_n + c_n))x^n$$

$$= p(x) +_1 (q(x) + r(x)),$$

where we have used associativity of addition in \mathbb{R} for the third equality, and generalised associativity and commutativity of the addition in \mathbb{R} for the remaining equalities.

Neutral element of $+_1$: We check that this is the constant function 0. Consider a polynomial $p \in \mathcal{P}$. Then there are $n \in \mathbb{N}$ and coefficients $a_0, a_1, \ldots, a_n \in \mathbb{R}$ such that $p(x) = a_0 + a_1x + \cdots + a_nx^n$. We can then write

$$p(x) + \mathbf{0} = (a_0 + a_1 x + \dots + a_n x^n) + (0 + 0x + \dots + 0x^n)$$

= $(a_0 + 0) + (a_1 + 0)x + \dots + (a_n + 0)x^n = p(x),$

where we used that 0 is the neutral element of addition in \mathbb{R} .

Since p is an arbitrary polynomial in \mathcal{P} , it follows that $\mathbf{0}$ is the neutral element of $+_1$.

Additive inverses: For every polynomial $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathcal{P}$, we have that

$$p(x) + ((-a_0) + (-a_1)x + \dots + (-a_n)x^n) = (a_0 - a_0) + (a_1 - a_1)x + \dots + (a_n - a_n)x^n = \mathbf{0},$$

therefore p(x) has an additive inverse.

 \cdot_1 is commutative: Consider two real polynomials $p, q \in \mathcal{P}$. There are $n \in \mathbb{N}$ and coefficients $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_n \in \mathbb{R}$ such that

$$p(x) = a_0 + a_1 x + \dots + a_n x^n, \qquad q(x) = b_0 + b_1 x + \dots + b_n x^n.$$

We then have

$$p(x)\cdot_1 q(x) = \sum_{k=0}^{2n} \left(\sum_{\substack{0 \le i,j \le n \\ i+j=k}} a_i b_j\right) x^k = \sum_{k=0}^{2n} \left(\sum_{\substack{0 \le i,j \le n \\ i+j=k}} b_j a_i\right) x^k = q(x)\cdot_1 p(x),$$

where we use that multiplication in \mathbb{R} is commutative for the second equality, and we also use generalised commutativity and associativity of addition in \mathbb{R} to express the product of two polynomials by writing a double sum as above.

 \cdot_1 is associative: Consider three real polynomials $p, q, r \in \mathcal{P}$. There are $n \in \mathbb{N}$ and coefficients $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_n, c_0, c_1, \ldots, c_n \in \mathbb{R}$ such that

$$p(x) = a_0 + a_1 x + \dots + a_n x^n, q(x) = b_0 + b_1 x + \dots + b_n x^n,$$

 $r(x) = c_0 + c_1 x + \dots + c_n x^n.$

We then have

$$(p(x) \cdot_{1} q(x)) \cdot_{1} r(x) = \left(\sum_{k=0}^{2n} \left(\sum_{\substack{0 \le i, j \le n \\ i+j=k}} a_{i} b_{j} \right) x^{k} \right) \cdot_{1} (c_{0} + c_{1}x + \dots + c_{n}x^{n})$$

$$= \sum_{l=0}^{3n} \left(\sum_{\substack{0 \le k \le 2n, 0 \le t \le n \\ k+t=l}} \left(\sum_{\substack{0 \le i, j \le n \\ i+j=k}} a_{i} b_{j} \right) \cdot c_{t} \right) x^{l}$$

$$= \sum_{l=0}^{3n} \left(\sum_{\substack{0 \le i \le n, 0 \le k' \le 2n \\ i+k'=l}} a_{i} \cdot \left(\sum_{\substack{0 \le j, t \le n \\ j+t=k'}} b_{j} c_{t} \right) \right) x^{l}$$

$$= p(x) \cdot_{1} (q(x) \cdot_{1} r(x)),$$

where we use the associativity of multiplication in \mathbb{R} , as well as the distributive law, in order to get the third equality.

Neutral element of \cdot_1 : We check that this is the constant function **1**. Consider a polynomial $p \in \mathcal{P}$. Then there are $n \in \mathbb{N}$ and coefficients $a_0, a_1, \ldots, a_n \in \mathbb{R}$ such that $p(x) = a_0 + a_1x + \cdots + a_nx^n$. We can then write

$$p(x) \cdot_1 \mathbf{1} = (a_0 + a_1 x + \dots + a_n x^n) \cdot_1 (1 + 0x + \dots + 0x^n)$$

= $(a_0 \cdot 1) + (a_1 \cdot 1)x + \dots + (a_n \cdot 1)x^n = p(x),$

where we used that 1 is the neutral element of multiplication in \mathbb{R} .

Since p is an arbitrary polynomial in \mathcal{P} , it follows that $\mathbf{1}$ is the neutral element of \cdot_1 .

Distributive law: We first note that it suffices to check either the left distributive property or the right distributive property, given that we have already verified that \cdot_1 is commutative; we check the right distributive property here.

Consider three real polynomials $p, q, r \in \mathcal{P}$. There are $n \in \mathbb{N}$ and coefficients $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_n, c_0, c_1, \ldots, c_n \in \mathbb{R}$ such that

$$p(x) = a_0 + a_1 x + \dots + a_n x^n, q(x) = b_0 + b_1 x + \dots + b_n x^n,$$

 $r(x) = c_0 + c_1 x + \dots + c_n x^n.$

We then have

$$(p(x) +_1 q(x)) \cdot_1 r(x)$$

$$= ((a_0 + b_0) + (a_1 + b_1)x + \dots + (a_n + b_n)x^n) \cdot_1 (c_0 + c_1x + \dots + c_nx^n)$$

$$= \sum_{k=0}^{2n} \left(\sum_{\substack{0 \le i, j \le n \\ i+j=k}} (a_i + b_i)c_j \right) x^k$$

$$= \sum_{k=0}^{2n} \left(\left(\sum_{\substack{0 \le i, j \le n \\ i+j=k}} a_ic_j \right) + \left(\sum_{\substack{0 \le i, j \le n \\ i+j=k}} b_ic_j \right) \right) x^k = p(x) \cdot_1 r(x) +_1 q(x) \cdot_1 r(x),$$

where we use the distributive law in \mathbb{R} , as well as generalised commutativity and associativity of addition in \mathbb{R} , to get the third equality.

We conclude that \mathcal{R}_1 is a commutative ring.

(b) We check the ring axioms for addition and for multiplication in the case of \mathcal{R}_2 now.

We first note that addition of polynomials in \mathcal{R}_2 is the same operation as addition in \mathcal{R}_1 , therefore the properties we verified before still hold:

- $+_2$ is commutative.
- \bullet +₂ is associative.
- There exists a neutral element of $+_2$, and it is the constant function 0.
- For every polynomial $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathcal{P}$, we can define the polynomial $\widetilde{p}(x) = (-a_0) + (-a_1)x + \cdots + (-a_n)x^n$, and we can check that it is the additive inverse of p(x): $p(x) + 2\widetilde{p}(x) = 0$.

We now check the ring axioms concerning multiplication:

·₂ is associative: Consider three real polynomials $p, q, r \in \mathcal{P}$. Then, for every $a \in \mathbb{R}$ we have

$$((p \cdot_2 q) \cdot_2 r)(a) = ((p \circ q) \circ r)(a) = (p \circ q)(r(a))$$
$$= p(q(r(a))) = p((q \circ r)(a)) = (p \circ (q \circ r))(a) = (p \cdot_2 (q \cdot_2 r))(a),$$

therefore the functions $(p \cdot_2 q) \cdot_2 r$ and $p \cdot_2 (q \cdot_2 r)$ coincide.

Neutral element of \cdot_2 : We check that this is the polynomial u(x) = x. Consider a polynomial $p \in \mathcal{P}$. Then there are $n \in \mathbb{N}$ and coefficients $a_0, a_1, \ldots, a_n \in \mathbb{R}$ such that $p(x) = a_0 + a_1x + \cdots + a_nx^n$. We can then write

$$(p \cdot_2 u)(x) = a_0 + a_1 u(x) + \dots + a_n (u(x))^n = a_0 + a_1 x + \dots + a_n x^n = p(x).$$

Similarly,

$$(u \cdot_2 p)(x) = u(p(x)) = p(x).$$

Since p is an arbitrary polynomial in \mathcal{P} , it follows that u(x) = x is the neutral element of \cdot_2 .

Finally, we check that the right distributive property holds true in \mathcal{R}_2 , while the left distributive property fails.

Consider three real polynomials $p, q, r \in \mathcal{P}$. There are $n \in \mathbb{N}$ and coefficients $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_n, c_0, c_1, \ldots, c_n \in \mathbb{R}$ such that

$$p(x) = a_0 + a_1 x + \dots + a_n x^n,$$
 $q(x) = b_0 + b_1 x + \dots + b_n x^n,$ $r(x) = c_0 + c_1 x + \dots + c_n x^n.$

We then have

$$(p(x) +2 q(x)) \cdot2 r(x) = ((a_0 + b_0) + (a_1 + b_1)x + \dots + (a_n + b_n)x^n) \circ r(x)$$

$$= (a_0 + b_0) + (a_1 + b_1)r(x) + \dots + (a_n + b_n)(r(x))^n$$

$$= (a_0 + a_1r(x) + \dots + a_n(r(x))^n) + (b_0 + b_1r(x) + \dots + b_n(r(x))^n)$$

$$= (p \cdot2 r)(x) + (q \cdot2 r)(x),$$

which we can justify by viewing the coefficients as constant polynomials as well, and then viewing addition of them and multiplication with powers of r(x) as the operations in \mathcal{R}_1 (whose properties we studied in part (a)); then, by the distributive law in \mathcal{R}_1 and by generalised commutativity and associativity of addition in \mathcal{R}_1 , we get the third equality here.

Since the polynomials p, q and r that we considered are arbitrary, we conclude that the right distributive property holds in \mathcal{R} .

On the other hand, if we choose $p(x) = x^2$, q(x) = x, r(x) = x + 1, then

$$p(x) \cdot_2 (q(x) +_2 r(x)) = p(x) \circ (q(x) +_2 r(x)) = p(q(x) + r(x)) = p(2x + 1)$$

$$= (2x + 1)^2 = 4x^2 + 4x + 1 \neq 2x^2 + 2x + 1$$

$$= (x)^2 + (x + 1)^2 = p(q(x)) + p(r(x))$$

$$= (p(x) \cdot_2 q(x)) +_2 (p(x) \cdot_2 r(x)).$$

This shows that the left distributive property does not hold for any three real polynomials in \mathcal{P} .

(c) We first deal with \mathcal{R}_1 . We are looking for polynomials $p \in \mathcal{P}$ such that there exists $q \in \mathcal{P}$ with

$$p(x) \cdot_1 q(x) = q(x) \cdot_1 p(x) = 1;$$
 (1)

in fact, since we have already confirmed that \cdot_1 is commutative, it suffices to ask for what polynomials p, q we have $p(x) \cdot_1 q(x) = 1$.

Clearly, p(x) cannot be the constant function $\mathbf{0}$ (because then the product of p(x) with any other polynomial in \mathcal{P} would be equal to the constant function $\mathbf{0}$), so we can find $n \geq 0$ and coefficients $a_0, a_1, \ldots, a_n \in \mathbb{R}$ with $a_n \neq 0$ so that

$$p(x) = a_0 + a_1 x + \dots + a_n x^n.$$

Similarly, if a polynomial q exists such that (1) holds true, then q cannot be equal to the constant function $\mathbf{0}$. Thus we would be able to find $m \ge 0$ and coefficients $b_0, b_1, \ldots, b_m \in \mathbb{R}$ with $b_m \ne 0$ so that

$$q(x) = b_0 + b_1 x + \dots + b_m x^m$$

and so that

$$p(x) \cdot_1 q(x) = (a_0 + a_1 x + \dots + a_n x^n) \cdot_1 (b_0 + b_1 x + \dots + b_m x^m)$$
$$= \sum_{k=0}^{n+m} \left(\sum_{\substack{0 \le i \le n, \ 0 \le j \le m \\ i+j-k}} a_i b_j \right) x^k.$$

For the latter product to be equal to 1, we need $n = \deg(p) = 0$, and similarly $m = \deg(q) = 0$.

Therefore, the only polynomials that could have a multiplicative inverse in \mathcal{R}_1 are the non-zero constant polynomials.

We now check that every non-zero constant polynomial has a multiplicative inverse in \mathcal{R}_1 , and thus that the invertible elements of \mathcal{R}_1 are precisely the elements of $\mathcal{P}_0 \setminus \{\mathbf{0}\}$.

Consider a non-zero constant polynomial $p \in \mathcal{P}$; then $p(x) = a_0$ with $a_0 \in \mathbb{R}$, $a_0 \neq 0$. But then, if we set $q(x) = a_0^{-1}$, this is another constant polynomial, for which we have

$$p(x) \cdot_1 q(x) = a_0 \cdot a_0^{-1} = 1.$$

Thus the non-zero constant polynomial we considered has a multiplicative inverse in \mathcal{R}_1 , and since this was arbitrary the conclusion we wanted follows.

We now deal with \mathcal{R}_2 . We are looking for polynomials $p \in \mathcal{P}$ such that there exists $q \in \mathcal{P}$ with

$$p(x) \cdot_2 q(x) = q(x) \cdot_2 p(x) = x.$$
 (2)

We recall that this is equivalent to having

$$p(q(x)) = (p \circ q)(x) = (q \circ p)(x) = q(p(x)) = x.$$

We now note that, if either p or q is a constant polynomial, then $p \circ q$ or $q \circ p$ respectively will be a constant polynomial too. Therefore, we must have $\deg(p) \geqslant 1$ for p to potentially have a multiplicative inverse, and we should also have $\deg(q) \geqslant 1$ if q were to be the multiplicative inverse of p.

We can thus find $n, m \in \mathbb{N}$ and coefficients $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_m \in \mathbb{R}$ with $a_n b_m \neq 0$ and such that

$$p(x) = a_0 + a_1 x + \dots + a_n x^n, \qquad q(x) = b_0 + b_1 x + \dots + b_m x^m.$$

If either n or m were greater than 1, then we would have $deg(p \circ q) = nm > 1$, and so it wouldn't be possible for $p \cdot_2 q = p \circ q$ to be equal to a degree 1 polynomial.

Therefore, the only polynomials that could have a multiplicative inverse in \mathcal{R}_2 are the polynomials of degree 1.

We now check that every polynomial of degree 1 has a multiplicative inverse in \mathcal{R}_2 , and thus that the invertible elements of \mathcal{R}_2 are precisely the elements of $\mathcal{P}_1 \setminus \mathcal{P}_0$.

Consider a polynomial $p \in \mathcal{P}$ of degree 1; then $p(x) = a_0 + a_1 x$ with $a_0, a_1 \in \mathbb{R}$, $a_1 \neq 0$. But then, if we set $q(x) = \frac{-a_0}{a_1} + \frac{1}{a_1}x$, this is another polynomial of degree 1, for which we have

$$p(x) \cdot_2 q(x) = p(q(x)) = a_0 + a_1 q(x) = a_0 + a_1 \left(\frac{-a_0}{a_1} + \frac{1}{a_1}x\right) = x,$$

and also $q(x) \cdot_2 p(x) = q(p(x)) = \frac{-a_0}{a_1} + \frac{1}{a_1}(a_0 + a_1x) = x.$

Thus the polynomial p of degree 1 that we considered has a multiplicative inverse in \mathcal{R}_2 , and since this was arbitrary the conclusion we wanted follows.

Summarising, we have verified that the elements of \mathcal{P} with a multiplicative inverse in \mathcal{R}_1 are the polynomials in $\mathcal{P}_0 \setminus \{\mathbf{0}\}$, while those with a multiplicative inverse in \mathcal{R}_2 are the polynomials in $\mathcal{P}_1 \setminus \mathcal{P}_0$. Clearly, $\mathcal{P}_0 \setminus \{\mathbf{0}\} \neq \mathcal{P}_1 \setminus \mathcal{P}_0$ (in fact, they even have no common elements).

Problem 2. Consider two arbitrary vectors $\bar{x}, \bar{y} \in V_1$, and $r \in \mathbb{F}$. We then have

$$(\mu_1 f_1 + \mu_2 f_2)(\bar{x} + \bar{y}) = (\mu_1 f_1)(\bar{x} + \bar{y}) + (\mu_2 f_2)(\bar{x} + \bar{y})$$
 (by definition of sum of functions)
$$= \mu_1 \cdot f_1(\bar{x} + \bar{y}) + \mu_2 \cdot f_2(\bar{x} + \bar{y})$$
 (by definition of scalar multiplication for functions)
$$= \mu_1 \cdot (f_1(\bar{x}) + f_1(\bar{y})) + \mu_2 \cdot (f_2(\bar{x}) + f_2(\bar{y}))$$
 (because f_1, f_2 are linear)
$$= (\mu_1 \cdot f_1(\bar{x}) + \mu_1 \cdot f_1(\bar{y})) + (\mu_2 \cdot f_2(\bar{x}) + \mu_2 \cdot f_2(\bar{y}))$$

$$= (\mu_1 f_1)(\bar{x}) + (\mu_1 f_1)(\bar{y}) + (\mu_2 f_2)(\bar{x}) + (\mu_2 f_2)(\bar{y})$$

$$= (\mu_1 f_1)(\bar{x}) + (\mu_2 f_2)(\bar{x})) + ((\mu_1 f_1)(\bar{y}) + (\mu_2 f_2)(\bar{y}))$$

$$= (\mu_1 f_1 + \mu_2 f_2)(\bar{x}) + (\mu_1 f_1 + \mu_2 f_2)(\bar{y}),$$

which shows the additivity of $\mu_1 f_1 + \mu_2 f_2$.

Moreover,

$$(\mu_1 f_1 + \mu_2 f_2)(r\bar{x}) = (\mu_1 f_1)(r\bar{x}) + (\mu_2 f_2)(r\bar{x})$$
 (by definition of sum of functions)
$$= \mu_1 \cdot f_1(r\bar{x}) + \mu_2 \cdot f_2(r\bar{x})$$
 (by definition of scalar multiplication for functions)
$$= \mu_1 \cdot (r \cdot f_1(\bar{x})) + \mu_2 \cdot (r \cdot f_2(\bar{x}))$$
 (because f_1, f_2 are linear)
$$= (\mu_1 r) \cdot f_1(\bar{x}) + (\mu_2 r) \cdot f_2(\bar{x})$$

$$= (r\mu_1) \cdot f_1(\bar{x}) + (r\mu_2) \cdot f_2(\bar{x})$$

$$= r \cdot (\mu_1 \cdot f_1(\bar{x})) + r \cdot (\mu_2 \cdot f_2(\bar{x}))$$

$$= r \cdot ((\mu_1 f_1)(\bar{x}) + (\mu_2 f_2)(\bar{x}))$$

$$= r \cdot (\mu_1 f_1 + \mu_2 f_2)(\bar{x}).$$

Combining the above, we conclude that $\mu_1 f_1 + \mu_2 f_2$ is a linear map from V_1 to V_2 .

Problem 3. We first use Gaussian elimination to find a Row Echelon Form of A:

The last matrix, matrix A', is in Row Echelon Form, and has 3 pivots. Therefore, we can conclude that rank(A) = 3.

Moreover, we see that the pivot columns of A' are $C_1(A')$, $C_3(A')$ and $C_5(A')$, and we recall (or alternatively can check directly by doing back substitution) that these form a maximal linearly independent subset of the columns of A'. Therefore, as we discussed in class (in fact, as we saw in the proof of Main Theorem C), a maximal linearly independent subset of the columns of A, and hence a basis of CS(A), is the set

$$\left\{C_1(A), C_3(A), C_5(A)\right\} = \left\{ \begin{pmatrix} 7\\0\\10\\0\\3 \end{pmatrix}, \begin{pmatrix} 9\\3\\5\\4 \end{pmatrix}, \begin{pmatrix} 4\\6\\8\\0\\5 \end{pmatrix} \right\}.$$

On the other hand, we recall that a basis for RS(A) is the set of non-zero rows of A'. Given though that here we want to find a basis formed from rows of A, we proceed in a similar way to above by considering A^T instead and by

finding a Row Echelon Form of it:

The last matrix, matrix B, is in Row Echelon Form. Its pivot columns are $C_1(B)$, $C_2(B)$ and $C_4(B)$. Therefore, analogously to what we noted previously, a maximal linearly independent subset of the columns of A^T , and hence a basis of $CS(A^T) = RS(A)$, is the set

$$\left\{R_1(A), R_2(A), R_4(A)\right\} = \left\{C_1(A^T), C_2(A^T), C_4(A^T)\right\} = \left\{\begin{pmatrix} 7\\2\\0\\1\\4 \end{pmatrix}, \begin{pmatrix} 0\\0\\3\\2\\6 \end{pmatrix}, \begin{pmatrix} 0\\0\\5\\7\\0 \end{pmatrix}\right\}.$$

Finally, by Main Theorem D we know that

$$\operatorname{nullity}(A) = \#\{\operatorname{columns of } A\} - \operatorname{rank}(A) = 5 - 3 = 2.$$

We also recall that the linear system $A\bar{x} = \bar{0}$ is equivalent to the linear system $A'\bar{x} = \bar{0}$, and that Nullspace(A) coincides with the common solution set of these systems.

To find a basis for Nullspace(A), or equivalently for the solution set of the linear system $A'\bar{x} = \bar{0}$, we note that this system has 2 free variables, the variables x_2 and x_4 . We also recall that a basis for the solution set of $A'\bar{x} = \bar{0}$ can be chosen to be the subset of solutions we get when we set one of the free variables equal to 1 and the remaining free variables equal to 0.

In this case, we can set

•
$$x_2 = 1, x_4 = 0$$
, which corresponds to the solution $\bar{x} = \begin{pmatrix} 6 \\ 1 \\ 0 \\ 0 \end{pmatrix}$;

•
$$x_2 = 0, x_4 = 1$$
, which corresponds to the solution $\bar{x} = \begin{pmatrix} 3 \\ 0 \\ 3 \\ 1 \\ 0 \end{pmatrix}$.

We conclude that a basis for Nullspace(A) is the set

$$\left\{ \begin{pmatrix} 6\\1\\0\\0\\0 \end{pmatrix}, \begin{pmatrix} 3\\0\\3\\1\\0 \end{pmatrix} \right\}.$$

Problem 4. (a) For every matrix $\begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} \in \mathbb{R}^{2 \times 2}$,

$$f\left(\left(\begin{array}{cc} r_1 & r_2 \\ r_3 & r_4 \end{array}\right)\right) = \left(\begin{array}{cc} 3 & 2 \\ -2 & 1 \\ 0 & 4 \end{array}\right) \left(\begin{array}{cc} r_1 & r_2 \\ r_3 & r_4 \end{array}\right) = \left(\begin{array}{cc} 3r_1 + 2r_3 & 3r_2 + 2r_4 \\ -2r_1 + r_3 & -2r_2 + r_4 \\ 4r_3 & 4r_4 \end{array}\right).$$

We first note that f is <u>not</u> surjective, that is, Range $(f) \neq \mathbb{R}^{3\times 2}$. Indeed, consider the matrix

$$\left(\begin{array}{cc} 3 & 3\\ 2 & 2\\ 0 & 0 \end{array}\right) \in \mathbb{R}^{3\times 2},$$

and suppose that there were a matrix $\binom{r_1}{r_3} \binom{r_2}{r_4} \in \mathbb{R}^{2 \times 2}$ such that

$$\begin{pmatrix} 3r_1 + 2r_3 & 3r_2 + 2r_4 \\ -2r_1 + r_3 & -2r_2 + r_4 \\ 4r_3 & 4r_4 \end{pmatrix} = f \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ 2 & 2 \\ 0 & 0 \end{pmatrix}.$$

We would then need $r_3 = r_4 = 0$, which would then imply

$$3r_1 = 3, \ 3r_2 = 3, \ -2r_1 = 2, \ -2r_2 = 2 \quad \Rightarrow \quad r_1 = 1 = r_2 \text{ but also } r_1 = -1 = r_2.$$

Since the conclusions contradict each other, we obtain that there is no matrix $\binom{r_1}{r_3} \binom{r_2}{r_4} \in \mathbb{R}^{2 \times 2}$ whose image under f is the matrix $\binom{3}{2} \binom{3}{2} \binom{3}{0} \in \mathbb{R}^{3 \times 2}$.

Alternatively, we could use Main Theorem E to conclude that f is not surjective: the theorem tells us that

$$\dim_{\mathbb{R}} \mathrm{Range}(f) \leqslant \dim_{\mathbb{R}} \mathrm{Range}(f) + \dim_{\mathbb{R}} \mathrm{Ker}(f) = \dim_{\mathbb{R}} \mathbb{R}^{2 \times 2} = 4,$$

while $\dim_{\mathbb{R}} \mathbb{R}^{3 \times 2} = 6$. Thus we <u>cannot</u> have $\dim_{\mathbb{R}} \operatorname{Range}(f) = \dim_{\mathbb{R}} \mathbb{R}^{3 \times 2}$, and hence we <u>cannot</u> have $\operatorname{Range}(f) = \mathbb{R}^{3 \times 2}$.

We now check that f is injective:

$$\begin{pmatrix} 3r_1 + 2r_3 & 3r_2 + 2r_4 \\ -2r_1 + r_3 & -2r_2 + r_4 \\ 4r_3 & 4r_4 \end{pmatrix} = f\left(\begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix}\right) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\Rightarrow r_3 = r_4 = 0, \text{ which in turn imply } 3r_1 = 3r_1 + 2r_3 = 0$$

and $3r_2 = 3r_2 + 2r_4 = 0$ \Rightarrow $r_1 = r_2 = 0$ as well.

Therefore, $Ker(f) = \{O\}$, where O is the zero matrix in $\mathbb{R}^{2\times 2}$.

Clearly, a basis for Ker(f) is the empty set \emptyset . As for Range(f), we know that the arbitrary image of f is of the form

$$\begin{pmatrix} 3r_1 + 2r_3 & 3r_2 + 2r_4 \\ -2r_1 + r_3 & -2r_2 + r_4 \\ 4r_3 & 4r_4 \end{pmatrix}$$

$$= \begin{pmatrix} 3r_1 & 0 \\ -2r_1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 3r_2 \\ 0 & -2r_2 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 2r_3 & 0 \\ r_3 & 0 \\ 4r_3 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 2r_4 \\ 0 & r_4 \\ 0 & 4r_4 \end{pmatrix}$$

$$= r_1 \begin{pmatrix} 3 & 0 \\ -2 & 0 \\ 0 & 0 \end{pmatrix} + r_2 \begin{pmatrix} 0 & 3 \\ 0 & -2 \\ 0 & 0 \end{pmatrix} + r_3 \begin{pmatrix} 2 & 0 \\ 1 & 0 \\ 4 & 0 \end{pmatrix} + r_4 \begin{pmatrix} 0 & 2 \\ 0 & 1 \\ 0 & 4 \end{pmatrix}.$$

Therefore,

$$\operatorname{Range}(f) = \operatorname{span}\left(\left\{ \begin{pmatrix} 3 & 0 \\ -2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 3 \\ 0 & -2 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 1 & 0 \\ 4 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 0 & 1 \\ 0 & 4 \end{pmatrix} \right\}\right).$$

We finally check that the spanning set for Range(f) that we just found is linearly independent too: if we have $\lambda_1, \lambda_2, \lambda_3$ and $\lambda_4 \in \mathbb{R}$ such that

$$\lambda_{1} \begin{pmatrix} 3 & 0 \\ -2 & 0 \\ 0 & 0 \end{pmatrix} + \lambda_{2} \begin{pmatrix} 0 & 3 \\ 0 & -2 \\ 0 & 0 \end{pmatrix} + \lambda_{3} \begin{pmatrix} 2 & 0 \\ 1 & 0 \\ 4 & 0 \end{pmatrix} + \lambda_{4} \begin{pmatrix} 0 & 2 \\ 0 & 1 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix},$$

$$\text{then } \begin{pmatrix} 3\lambda_{1} + 2\lambda_{3} & 3\lambda_{2} + 2\lambda_{4} \\ -2\lambda_{1} + \lambda_{3} & -2\lambda_{2} + \lambda_{4} \\ 4\lambda_{3} & 4\lambda_{4} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\Rightarrow f \begin{pmatrix} \begin{pmatrix} \lambda_{1} & \lambda_{2} \\ \lambda_{3} & \lambda_{4} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} \lambda_{1} & \lambda_{2} \\ \lambda_{3} & \lambda_{4} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ since we showed that } f \text{ is injective}$$

$$\Rightarrow \lambda_{1} = \lambda_{2} = \lambda_{3} = \lambda_{4} = 0.$$

We conclude that $\left\{ \begin{pmatrix} 3 & 0 \\ -2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 3 \\ 0 & -2 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 1 & 0 \\ 4 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 0 & 1 \\ 0 & 4 \end{pmatrix} \right\}$ is a basis for Range(f).

(b) We first look for a matrix representation for g: we want a matrix $B \in \mathbb{Z}_7^{3 \times 3}$ satisfying

$$g\left(\left(\begin{smallmatrix} x_1\\x_2\\x_3 \end{smallmatrix}\right)\right) = B\left(\begin{smallmatrix} x_1\\x_2\\x_3 \end{smallmatrix}\right)$$

for every $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{Z}_7^3$. We can verify that

$$B = \left(g(\bar{e}_1) \mid g(\bar{e}_2) \mid g(\bar{e}_3) \right) = \left(\begin{array}{ccc} 1 & 3 & 5 \\ 2 & 0 & 1 \\ 0 & 3 & 0 \end{array} \right)$$

is the matrix we want.

We now remark that, since $\dim_{\mathbb{Z}_7} \text{Dom}(g) = \dim_{\mathbb{Z}_7} \text{Codomain}(g) = 3$, Main Theorem E implies that g is injective if and only if g is surjective (see e.g. discussion from the January 23 Recitation file), so it suffices to check one of the two properties.

We check whether g is injective: this is equivalent to checking that the linear system

$$B\left(\begin{smallmatrix} x_1\\x_2\\x_3 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0\\0\\0 \end{smallmatrix}\right)$$

has only one solution, the trivial solution, which in this case is equivalent to B being invertible.

To check whether B is invertible, we use Gauss-Jordan elimination:

$$B = \begin{pmatrix} 1 & 3 & 5 \\ 2 & 0 & 1 \\ 0 & 3 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 5 \\ 0 & 1 & 5 \\ 0 & 3 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 5 \\ 0 & 1 & 5 \\ 0 & 0 & 6 \end{pmatrix}.$$

We thus see that a REF of B has 3 pivots (as many as its rows or columns), therefore B is invertible. Going back, this implies that g is injective, and therefore surjective too.

We conclude that $Ker(g) = {\bar{0}}$ and $Range(g) = \mathbb{Z}_7^3$, and also that g is bijective.

Clearly, a basis for Ker(g) is the empty set \emptyset , while a basis for $Range(g) = \mathbb{Z}_7^3$ is the standard basis $\{\bar{e}_1, \bar{e}_2, \bar{e}_3\}$ of \mathbb{Z}_7^3 .

Finally, we find the inverse of g by noting that the matrix representation of g^{-1} would be the matrix B^{-1} (see e.g. the discussion from the January 23 Recitation file). We start again from the Gauss-Jordan elimination steps we

did before:

$$\begin{pmatrix} 1 & 3 & 5 & | & 1 & 0 & 0 \\ 2 & 0 & 1 & | & 0 & 1 & 0 \\ 0 & 3 & 0 & | & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 5 & | & 1 & 0 & 0 \\ 0 & 1 & 5 & | & 5 & 1 & 0 \\ 0 & 3 & 0 & | & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 5 & | & 1 & 0 & 0 \\ 0 & 1 & 5 & | & 5 & 1 & 0 \\ 0 & 0 & 6 & | & 6 & 4 & 1 \end{pmatrix}$$
$$\sim \begin{pmatrix} 1 & 3 & 5 & | & 1 & 0 & 0 \\ 0 & 1 & 5 & | & 5 & 1 & 0 \\ 0 & 0 & 1 & | & 1 & 3 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 0 & | & 3 & 6 & 5 \\ 0 & 1 & 0 & | & 0 & 0 & 5 \\ 0 & 0 & 1 & | & 1 & 3 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & | & 3 & 6 & 4 \\ 0 & 1 & 0 & | & 0 & 0 & 5 \\ 0 & 0 & 1 & | & 1 & 3 & 6 \end{pmatrix}.$$

Therefore,

$$B^{-1} = \begin{pmatrix} 3 & 6 & 4 \\ 0 & 0 & 5 \\ 1 & 3 & 6 \end{pmatrix}$$
 and $g^{-1} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = B^{-1} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 3y_1 + 6y_2 + 4y_3 \\ 5y_3 \\ y_1 + 3y_2 + 6y_3 \end{pmatrix}$

for every $\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \in \mathbb{Z}_7^3$.

Problem 5. We recall that A is invertible if and only if the linear system $A\bar{x} = \bar{0}$, where $\bar{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ and $\bar{0} \in \mathbb{F}^n$, has only the trivial solution.

If we now assume that A is not invertible, then the linear system $A\bar{x} = \bar{0}$ has a non-zero solution. Therefore, there is a non-zero vector $\bar{u} \in \mathbb{F}^n$ such that

$$A\bar{u} = \bar{0} = 0 \cdot \bar{u}.$$

This shows that \bar{u} is an eigenvector of A corresponding to eigenvalue 0.

Conversely, if we assume that 0 is an eigenvalue of A, then we know that there exists a non-zero vector $\bar{v} \in \mathbb{F}^n$ such that $A\bar{v} = 0 \cdot \bar{v} = \bar{0}$. But then the linear system $A\bar{x} = \bar{0}$ has more than one solutions, which shows that A is not invertible.

Combining the above, we get that

A is not invertible if and only if 0 is an eigenvalue of A.

By taking contrapositives of the two implications forming this equivalence, we get the equivalence we wanted.

Problem 6. By our assumption, there exists a non-zero vector $\bar{u} \in \mathbb{R}^n$ such that

$$A\bar{u} = \lambda \cdot \bar{u}$$
.

We now have

- 1. $(2A)\bar{u} = 2(\bar{A}u) = 2(\lambda \cdot \bar{u}) = (2\lambda) \cdot \bar{u}$, therefore \bar{u} is an eigenvector of 2A corresponding to eigenvalue 2λ .
- 2. $(A + I_n)\bar{u} = A\bar{u} + I_n\bar{u} = \lambda \cdot \bar{u} + \bar{u} = \lambda \cdot \bar{u} + 1 \cdot \bar{u} = (\lambda + 1) \cdot \bar{u}$, which shows that \bar{u} is an eigenvector of $A + I_n$ corresponding to eigenvalue $\lambda + 1$.
- 3. $(A^2)\bar{u} = (A\cdot A)\bar{u} = A(A\bar{u}) = A(\lambda\cdot\bar{u}) = \lambda\cdot(A\bar{u}) = \lambda\cdot(\lambda\cdot\bar{u}) = \lambda^2\cdot\bar{u}$, which shows that \bar{u} is an eigenvector of A^2 corresponding to eigenvalue λ^2 .
- 4. Similarly to part (3), and starting from it and using mathematical induction, we can show that, for every k > 2, \bar{u} is an eigenvector of A^k corresponding to eigenvalue λ^k . But then, for every $m \ge 0$ and for every set of coefficients $b_0, b_1, \ldots, b_m \in \mathbb{R}$, we have for the polynomial $p(x) = b_0 + b_1 x + \cdots + b_m x^m$ that

$$(p(A))\bar{u} = (b_{m}A^{m} + b_{m-1}A^{m-1} + \dots + b_{1}A + b_{0}I_{n})\bar{u}$$

$$= (b_{m}A^{m})\bar{u} + (b_{m-1}A^{m-1})\bar{u} + \dots + (b_{1}A)\bar{u} + (b_{0}I_{n})\bar{u}$$

$$= b_{m}(A^{m}\bar{u}) + b_{m-1}(A^{m-1}\bar{u}) + \dots + b_{1}(A\bar{u}) + b_{0} \cdot \bar{u}$$

$$= b_{m} \cdot (\lambda^{m} \cdot \bar{u}) + b_{m-1} \cdot (\lambda^{m-1} \cdot \bar{u}) + \dots + b_{1} \cdot (\lambda \cdot \bar{u}) + b_{0} \cdot \bar{u}$$

$$= (b_{m}\lambda^{m}) \cdot \bar{u} + (b_{m-1}\lambda^{m-1}) \cdot \bar{u} + \dots + (b_{1}\lambda) \cdot \bar{u} + b_{0} \cdot \bar{u}$$

$$= (b_{m}\lambda^{m} + b_{m-1}\lambda^{m-1} + \dots + b_{1}\lambda + b_{0}) \cdot \bar{u} = p(\lambda) \cdot \bar{u}.$$

Thus, \bar{u} is an eigenvector of the matrix p(A) corresponding to eigenvalue $p(\lambda)$.

5. By the assumption,

$$A\bar{u} = \lambda \cdot \bar{u} \quad \Rightarrow \quad \frac{1}{\lambda}(A\bar{u}) = \bar{u}$$

$$\Rightarrow \quad A\left(\frac{1}{\lambda} \cdot \bar{u}\right) = \bar{u} \quad \Rightarrow \quad \frac{1}{\lambda} \cdot \bar{u} = A^{-1}\left(A\left(\frac{1}{\lambda} \cdot \bar{u}\right)\right) = A^{-1}\bar{u}.$$

Thus, \bar{u} is an eigenvector of the matrix A^{-1} corresponding to eigenvalue $1/\lambda$.