

Part A.

1. Define $f : \mathbb{Z}[\sqrt{2}] \rightarrow M$ by $f(m + n\sqrt{2}) = \begin{bmatrix} m & n \\ 2n & m \end{bmatrix}$. We have

$$\begin{aligned} f((m + n\sqrt{2}) + (r + s\sqrt{2})) &= f((m + r) + (n + s)\sqrt{2}) = \begin{bmatrix} m + r & n + s \\ 2(n + s) & m + r \end{bmatrix} \\ &= \begin{bmatrix} m & n \\ 2n & m \end{bmatrix} + \begin{bmatrix} r & s \\ 2s & r \end{bmatrix} = f(m + n\sqrt{2}) + f(r + s\sqrt{2}) \end{aligned}$$

and

$$\begin{aligned} f((m + n\sqrt{2})(r + s\sqrt{2})) &= f((mr + 2ns) + (ms + nr)\sqrt{2}) = \begin{bmatrix} mr + 2ns & ms + nr \\ 2(ms + nr) & mr + 2ns \end{bmatrix} \\ &= \begin{bmatrix} m & n \\ 2n & m \end{bmatrix} \begin{bmatrix} r & s \\ 2s & r \end{bmatrix} = f(m + n\sqrt{2})f(r + s\sqrt{2}). \end{aligned}$$

Hence, f is a ring homomorphism.

Since $\begin{bmatrix} m & n \\ 2n & m \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ iff $m = n = 0$, we have $\ker f = \{0\}$ and so f is one-to-one. If $\begin{bmatrix} m & n \\ 2n & m \end{bmatrix} \in M$ then $m, n \in \mathbb{Z}$, and then $m + n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Moreover,

$$f(m + n\sqrt{2}) = \begin{bmatrix} m & n \\ 2n & m \end{bmatrix}$$

and thus f is onto. Hence f is an isomorphism of rings. \square

2. (a) Let $(a, b) \in \mathbb{Z}_{21} \oplus \mathbb{Z}_{35}$. Then $|(a, b)| = \text{lcm}(|a|, |b|)$. So, when $|(a, b)| = 7$ we have two cases:

Case 1: $|a| = 7$ and $|b| = 1$ or 7 . Since \mathbb{Z}_{21} has a unique cyclic group of order 7 and any cyclic group of order 7 has six generators, there are six choices for a . Similarly, there are seven choices for b (one for $|b| = 1$ and six for $|b| = 7$). This gives 42 choices for (a, b) .

Case 2: $|a| = 1$ and $|b| = 7$. Since \mathbb{Z}_{35} has a unique cyclic group of order 7 and any cyclic group of order 7 has six generators, there are six choices for b . There is only one choice for a . So, this case yields six more possibilities for (a, b) .

Thus $\mathbb{Z}_{21} \oplus \mathbb{Z}_{35}$ has $42 + 6 = 48$ elements of order 7.

(b) Because each cyclic group of order 7 has six elements of order 7 and no two of the cyclic subgroups can have an element of order 7 in common, there must be $48/6 = 8$ cyclic subgroups of order 7. \square

3. (a) We know that a homomorphism $f : \mathbb{Z}_{42} \rightarrow \mathbb{Z}_{12}$ is determined by its action on a generator of \mathbb{Z}_{42} . Assume that $f(1) = a$, for some $a \in \mathbb{Z}_{12}$. Then $|a|$ divides $|\mathbb{Z}_{12}| = 12$ and $|\mathbb{Z}_{42}| = 42$ (why?), so $|a|$ divides $\text{gcd}(12, 42) = 6$.

Case 1: If $|a| = 1$, then $a = 0$.

Case 2: If $|a| = 2$, then $a = 6$.

Case 3: If $|a| = 3$, then $a = 4$ or $a = 8$.

Case 4: If $|a| = 6$, then $a = 2$ or $a = 10$.

Notice that if $f(1) = a$, then $f(x) = f(x \cdot 1) = xf(1) = xa$, for all $x \in \mathbb{Z}$, because f is operation preserving. Therefore, the homomorphisms from \mathbb{Z}_{42} to \mathbb{Z}_{12} are:

$$f_1(x) = 0 \quad f_2(x) = 6x \quad f_3(x) = 4x \quad f_4(x) = 8x \quad f_5(x) = 2x \quad f_6(x) = 10x$$

None of the above functions are onto, since none of the possible values for a is a generator for \mathbb{Z}_{12} . Thus there are no homomorphisms from \mathbb{Z}_{42} onto \mathbb{Z}_{12} .

(b) We want to check whether any of the homomorphisms between the (additive) groups \mathbb{Z}_{42} and \mathbb{Z}_{12} found in (a) are ring homomorphisms. If such an f is then

$$a = f(1) = f(1 \cdot 1) = f(1) \cdot f(1) = a^2$$

Out of the six possible a 's listed above we get

$$0^2 = 0 \quad 6^2 = 0 \neq 6 \quad 4^2 = 4 \quad 8^2 = 4 \neq 8 \quad 2^2 = 4 \neq 2 \quad 10^2 = 4 \neq 10$$

and thus the only candidates to be ring homomorphisms are $f_1(x) = 0$ and $f_3(x) = 4x$. f_1 is clearly a homomorphism of rings, and

$$f_3(xy) = 4(xy) = 4^2(xy) = (4x)(4y) = f(x)f(y)$$

which means that f_3 is also a homomorphism of rings. \square

4. Since $\det(A) = 3^k \neq 0$, for all $A \in H$ then $H \subseteq G$. Moreover, $\det(I) = 1 = 3^0$, and thus the identity matrix lives in H .

Let $A, B \in H$ then $\det(A) = 3^k$ and $\det(B) = 3^t$, for some $k, t \in \mathbb{Z}$. Then

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = \det(A)\det(B)^{-1} = 3^k \cdot 3^{-t} = 3^{k-t}$$

Since $k - t \in \mathbb{Z}$, then $AB^{-1} \in H$. It follows that $H \leq G$.

In order to show that $H \trianglelefteq G$ we let $A \in H$ (with $\det(A) = 3^k$) and $B \in G$ (with $\det(B) = n \neq 0$) and we want to show that $BAB^{-1} \in H$. Note that

$$\det(BAB^{-1}) = \det(B)\det(A)\det(B^{-1}) = \det(B)\det(A)\det(B)^{-1} = n \cdot 3^k \cdot n^{-1} = 3^k$$

which implies that $BAB^{-1} \in H$. \square

5. We know that the subgroups of $(\mathbb{Z}_n, +)$ look like $\langle [d] \rangle$, where $d|n$. But

$$\langle [d] \rangle = \{[d]k; k \in \mathbb{Z}\} = \{[dk]; k \in \mathbb{Z}\} = \{[dk]; [k] \in \mathbb{Z}_n\} = \{[d][k]; [k] \in \mathbb{Z}_n\} = ([d])\mathbb{Z}_n = ([d])$$

where $([d])$ denotes the ideal generated by $[d]$.

Note that we are using that \mathbb{Z}_n is a commutative ring with one to get that $([d])\mathbb{Z}_n = ([d])$.

6. (\implies) If R is a field and $I \neq \{0\}$ is an ideal in R , then there exists $a \in I, a \neq 0$. Since R is a field, every nonzero element is a unit, and therefore $1 = a^{-1}a \in I$, since I is an ideal. Hence for all $r \in R$ we have $r = r \cdot 1 \in I$, and $I = R$.

(\impliedby) R is a commutative ring with one, so to show that R is a field we only need to show that all nonzero elements in R are units. Let $0 \neq a \in R$ and consider $I = (a)$, the principal ideal generated by a . Note that, since R is a commutative ring with one, then $(a) = Ra$.

$I \neq \{0\}$ since $0 \neq a \in I$. If $\{0\}$ and R are the only ideals in R , then we must have $I = R$. But R is a ring with one, hence $1 \in I$. In other words, there exists $r \in R$ such that $1 = ra$. Hence $r = a^{-1}$ (using that R is a commutative ring), and thus a is a unit. \square

7. (a) First note that $(xH)^{11} = x^{11}H = eH = H$, by hypothesis. Hence $|xH|$ divides 11. But since G/H is a group of order 24, we must also have that $|xH|$ divides 24. Since $\gcd(11, 24) = 1$, it must be the case that $|xH| = 1$. That is, $xH = H$. It follows that $x \in H$, as required.

(b) As $(123)H(123)^{-1} = (123)H(132) = \{e, (14)(23)\} \neq H$, then H is not normal in A_4 . \square

8. If G is isomorphic to all its non-trivial cyclic subgroups then it must be cyclic, as it would be isomorphic to all its non-trivial cyclic subgroups. Hence,

- If G is infinite we are done, as $G \cong \mathbb{Z}$.

- If G is finite then $G \cong \mathbb{Z}_n$, for some n . If n were not prime, then there would be a prime q dividing n . Consider $H = \langle [q] \rangle$. This is a subgroup of \mathbb{Z}_n of order n/q . We get a contradiction because if G were isomorphic to H then $n = n/q$ and that is false. So, n must be prime, and G is isomorphic to \mathbb{Z}_p , for some prime p . \square

Part B.

1. Let $\mathbf{v} \in \mathbb{R}^n$ and $M \in M_n(\mathbb{R}) \setminus \{0\}$ be such that $M\mathbf{v} = \mathbf{0}$. Since $M \neq 0$ then there is a vector \mathbf{w} such that $M\mathbf{w} \neq \mathbf{0}$. Consider N to be any matrix mapping \mathbf{v} to \mathbf{w} .

Why does such a matrix exist? One way to think about it is to create two matrices: A that maps \mathbf{v} to, let us say, $(1, 0, 0 \cdots, 0)$ and B (invertible) mapping \mathbf{w} to $(1, 0, 0 \cdots, 0)$. Then $N = B^{-1}A$ would map \mathbf{v} to \mathbf{w} .

It follows that $(MN)\mathbf{v} = M(N\mathbf{v}) = M\mathbf{w} \neq \mathbf{0}$.

2. (a) We need to show that T preserves addition and scalar multiplication of matrices. Let $A, B \in M_2(\mathbb{C})$ and $c \in \mathbb{C}$. Then we have

$$\begin{aligned} T(A+B) &= (A+B) + (A+B)^T \\ &= (A+B) + (A^T + B^T) \\ &= (A+A^T) + (B+B^T) \\ &= T(A) + T(B) \end{aligned}$$

and

$$T(cA) = (cA) + (cA)^T = c(A) + c(A^T) = c(A+A^T) = cT(A).$$

Therefore, T is a linear transformation.

- (b) Let $B \in M_2(\mathbb{C})$ such that $B^T = B$ (i.e. B is a symmetric matrix). Then consider $A = \frac{1}{2}B$ and observe that

$$A + A^T = \frac{1}{2}B + \left(\frac{1}{2}B\right)^T = \frac{1}{2}B + \frac{1}{2}B^T = \frac{1}{2}B + \frac{1}{2}B = B$$

and thus $T(A) = B$.

These calculations show that the range of T contains all matrices in $M_2(\mathbb{C})$ such that $B = B^T$. Moreover, notice that

$$T(A)^T = (A + A^T)^T = A^T + (A^T)^T = A^T + A = T(A)$$

and thus the range of T is *exactly* the set of all matrices in $M_2(\mathbb{C})$ such that $B = B^T$.

- (c) We have that

$$\begin{aligned} \ker T &= \{A \in M_2(\mathbb{C}) : T(A) = \mathbf{0}\} \\ &= \{A \in M_2(\mathbb{C}) : A + A^T = \mathbf{0}\} \\ &= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{C}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\} \\ &= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{C}) : \begin{bmatrix} 2a & b+c \\ c+b & 2d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\}. \end{aligned}$$

Thus if $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \ker T$, then $2a = b + c = 2d = 0$, or equivalently, $a = d = 0$ and $c = -b$, for some $b \in \mathbb{R}$. Therefore, $\ker T = \left\{ \begin{bmatrix} 0 & b \\ -b & 0 \end{bmatrix} : b \in \mathbb{C} \right\}$. □

3. (a) Let $A, B \in W$ and $c \in \mathbb{R}$. Clearly, $W \subseteq M_2(\mathbb{R})$ and $0 \in W$. Now using that the trace is an additive function we get

$$\text{tr}(A - B) = \text{tr}(A) - \text{tr}(B) = 0 - 0 = 0$$

$$\text{tr}(cA) = c \text{tr}(A) = c \cdot 0 = 0$$

implies that W is a subspace of $M_2(\mathbb{R})$

(b) Since $M_2(\mathbb{R})$ has dimension four and there are matrices in $M_2(\mathbb{R}) \setminus W$ (for instance the identity matrix), then $\dim(W) \leq 3$. Note that S contains three elements, all of them in W . Hence, if they were linearly independent then they would be forced to form a basis of W . But this is immediate, as

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = x \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} + y \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + z \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} x & y \\ z & -x \end{bmatrix}$$

yields $x = y = z = 0$.

4. Let $q_1 = p_1$, and

$$\langle p_2, q_1 \rangle = \int_0^1 (2t-1)(1) dt = (t^2 - t) \Big|_0^1 = 0$$

So, p_2 and q_1 are already orthogonal. Hence, $p_2 = q_2$. Now we compute

$$\langle p_3, q_1 \rangle = \int_0^1 (12t^2)(1) dt = (4t^3) \Big|_0^1 = 4$$

$$\langle q_1, q_1 \rangle = \int_0^1 (1)(1) dt = t \Big|_0^1 = 1$$

$$\langle p_3, q_2 \rangle = \int_0^1 (12t^2)(2t-1) dt = 2$$

$$\langle q_2, q_2 \rangle = \int_0^1 (12t^2)^2 dt = \frac{1}{6}(2t-1)^3 \Big|_0^1 = \frac{1}{3}$$

Then, the projection of p_3 onto $W_2 = \text{span}\{q_1, q_2\}$ is given by

$$\frac{\langle p_3, q_1 \rangle}{\langle q_1, q_1 \rangle} q_1 + \frac{\langle p_3, q_2 \rangle}{\langle q_2, q_2 \rangle} q_2 = \frac{4}{1} q_1 + \frac{2}{1/3} q_2 = 4q_1 + 6q_2$$

Hence,

$$q_3 = p_3 - (4q_1 + 6q_2)$$

and thus $q_3(t) = 12t^2 - 4 - 6(2t-1) = 12t^2 - 12t + 2$. It follows that the orthogonal basis is $\{q_1, q_2, q_3\}$.

5. (a) Let $\mathbf{p}, \mathbf{q} \in \mathcal{P}_2$ and $c \in \mathbb{R}$. Then

$$T(\mathbf{p} + \mathbf{q}) = \begin{bmatrix} (\mathbf{p} + \mathbf{q})(0) \\ (\mathbf{p} + \mathbf{q})(2) \end{bmatrix} = \begin{bmatrix} \mathbf{p}(0) \\ \mathbf{p}(2) \end{bmatrix} + \begin{bmatrix} \mathbf{q}(0) \\ \mathbf{q}(2) \end{bmatrix} = T(\mathbf{p}) + T(\mathbf{q})$$

$$T(c\mathbf{p}) = \begin{bmatrix} (c\mathbf{p})(0) \\ (c\mathbf{p})(2) \end{bmatrix} = \begin{bmatrix} c(\mathbf{p}(0)) \\ c(\mathbf{p}(2)) \end{bmatrix} = c \begin{bmatrix} \mathbf{p}(0) \\ \mathbf{p}(2) \end{bmatrix} = cT(\mathbf{p}).$$

Hence, T is a linear transformation.

(b) Using the definition of the kernel of a linear transformation, we have:

$$\begin{aligned} \text{Ker}(T) &= \left\{ \mathbf{p} \in \mathcal{P}_2 \mid T(\mathbf{p}) = \begin{bmatrix} \mathbf{p}(0) \\ \mathbf{p}(2) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\} \\ &= \left\{ a + bt + ct^2 \in \mathcal{P}_2 \mid \begin{bmatrix} a \\ a + 2b + 4c \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\} \\ &= \{ a + bt + ct^2 \in \mathcal{P}_2 \mid a = 0, a + 2b + 4c = 0 \} \end{aligned}$$

If $a = 0$, the equation $a+2b+4c = 0$ is equivalent to $b+2c = 0$, or to $b = -2c$, where c is free. Therefore, we arrive at:

$$\text{Ker}(T) = \{(-2c)t + ct^2 \mid c \in \mathbb{R}\} = \text{Span}\{-2t + t^2\}$$

which implies that $\{-2t + t^2\}$ forms a basis for $\text{Ker}(T)$.

(c) The standard basis for \mathcal{P}_2 is $\{1, t, t^2\}$, thus we need to compute the images under T of the polynomials $1, t$ and t^2 .

$$\begin{aligned} T(1) &= \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\ T(t) &= \begin{bmatrix} 0 \\ 2 \end{bmatrix} \\ T(t^2) &= \begin{bmatrix} 0 \\ 4 \end{bmatrix} \end{aligned}$$

Therefore the matrix for T relative to the basis $\{1, t, t^2\}$ for \mathcal{P}_2 and the standard basis for \mathbb{R}^2 is $\begin{bmatrix} 1 & 0 & 0 \\ 1 & 2 & 4 \end{bmatrix}$. □

6. (a) True. Matrices A and A^T have the same characteristic polynomial, because

$$\det(A^T - \lambda I) = \det(A^T - (\lambda I)^T) = \det(A - \lambda I)^T = \det(A - \lambda I)$$

and thus the same eigenvalues, counting multiplicities.

(b) True. If A is an $n \times n$ diagonalizable matrix, then A has n linearly independent eigenvectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ in \mathbb{R}^n . Since $\dim(\mathbb{R}^n) = n$, the set $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ forms a basis for \mathbb{R}^n , and therefore each vector in \mathbb{R}^n can be written as a linear combination of $\mathbf{v}_1, \dots, \mathbf{v}_n$.

(c) False. If A is a diagonal matrix with (at least one) 0 on the diagonal then the columns of A are not linearly independent (since a set of vectors containing the zero vector is linearly dependent). □

7. We find first $[T]_B$, the matrix of T relative to the standard basis $B = \{1, t\}$ for \mathcal{P}_1 . Since $T(1) = -2 + t$ and $T(t) = 1 + 2t$, the B -matrix of T has the following form:

$$[T]_B = \begin{bmatrix} -2 & 1 \\ 1 & 2 \end{bmatrix}$$

The eigenvalues of T are exactly the eigenvalues of the matrix $A = [T]_B$. The characteristic polynomial of A is $\chi_A = \lambda^2 - 5$, thus the eigenvalues of A (and hence the eigenvalues of T) are $\lambda = \pm\sqrt{5}$.

For $\lambda = \sqrt{5}$: $A - \sqrt{5}I = \begin{bmatrix} -2 - \sqrt{5} & 1 \\ 1 & 2 - \sqrt{5} \end{bmatrix}$ and the equation $(A - \sqrt{5}I)\mathbf{x} = \mathbf{0}$ amounts to

$$\begin{aligned} (-2 - \sqrt{5})x_1 + x_2 &= 0 & x_1 + (2 - \sqrt{5})x_2 &= 0 \end{aligned}$$

Observe that these two equations are equivalent.

So, $x_2 = (2 + \sqrt{5})x_1$, and x_1 free. The general solution to the equation $(A - \sqrt{5}I)\mathbf{x} = \mathbf{0}$ is $\mathbf{x} = x_1 \begin{bmatrix} 1 \\ 2 + \sqrt{5} \end{bmatrix}$, with $x_1 \in \mathbb{R}$.

This tells us that the eigenspace $V_{\lambda=\sqrt{5}}$ is 1-dimensional, and that if $\{p(t)\}$ is a basis for $V_{\lambda=\sqrt{5}}$, then the B -coordinate vector of $p(t)$ is $[p(t)]_B = \begin{bmatrix} 1 \\ 2 + \sqrt{5} \end{bmatrix}$.

Therefore, $\{p(t) = 1 + (2 + \sqrt{5})t\}$ is a basis for the eigenspace $V_{\lambda=\sqrt{5}}$ corresponding to the eigenvalue $\lambda = \sqrt{5}$.

The computations for $\lambda = -\sqrt{5}$ are similar. □

8. We will denote the change-of-coordinates matrix from the standard basis C to the basis B by $P_{B \leftarrow C}$.

The set B contains 2 vectors, and $\dim \mathcal{P}_1 = 2$, thus to show that B forms a basis for \mathcal{P}_1 it suffices to show that it is a linearly independent set.

If $a(t-1) + b(t+1) = 0 = 0t + 1$, for some scalars a and b , then $a + b = 0$ and $-a + b = 0$. Then $a = 0 = b$, implying that B is linearly independent and, therefore, a basis for \mathcal{P}_1 .

Recall that the change-of-coordinates matrix from the basis $C = \{1, t\}$ to the basis $B = \{t-1, t+1\}$ is given by $P_{B \leftarrow C} = \begin{bmatrix} [1]_B & [t]_B \end{bmatrix}$, so we need to find the B -coordinate vectors of the polynomials/vectors contained in the basis C .

Since $1 = -\frac{1}{2}(t-1) + \frac{1}{2}(t+1)$ we have $[1]_B = \begin{bmatrix} -1/2 \\ 1/2 \end{bmatrix}$.

Similarly, since $t = \frac{1}{2}(t-1) + \frac{1}{2}(t+1)$, it implies that $[t]_B = \begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix}$.

Then $P_{B \leftarrow C} = \begin{bmatrix} [1]_B & [t]_B \end{bmatrix} = \begin{bmatrix} -1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$. □