MA2101S Homework 7

Qi Ji (A0167793L)

26th March 2018

Question 1

It is trivial that (i) $\implies$ (ii). $\square$

For (ii) $\implies$ (i), suppose (ii), let $\mathcal{B} = \{ v_1, \dots, v_n \}$ be a basis for V. Clearly these vectors are non-zero, so they are eigenvectors of φ. Then there exists eigenvalues $\lambda_1, \dots, \lambda_n \in K$ such that for any $i \in \{ 1, \dots, n \}$, $\varphi(v_i) = \lambda_i v_i$. As vectors in $\mathcal{B}$ form a basis, $v_1 + \cdots + v_n \neq 0$, then there exist an eigenvalue $c \in K$ such that

$$\begin{aligned} \varphi(v_1 + \cdots + v_n) &= c(v_1 + \cdots + v_n) \\ &= c\,v_1 + \cdots + c\,v_n \end{aligned}$$

but by linearity,

$$\varphi(v_1 + \cdots + v_n) = \lambda_1 v_1 + \cdots + \lambda_n v_n$$

Then by uniqueness of basis coefficients, $c = \lambda_1 = \cdots = \lambda_n$, then it becomes clear that $\varphi = c \cdot \mathrm{id}_V$. $\square$

Question 2

(a) **False.**

Counter-example. Set $K = \mathbb{R}$, $V = \mathbb{R}^2$, taking all matrices with respect to standard basis, set

$$B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad v = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

We can now compute that $ABv = A0 = 0$, which means v is an eigenvector of AB with eigenvalue 0, but $BAv = B \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ which is not a scalar multiple of v. $\square$

(b) **True.**

Proof. Let $\lambda \in K$ be an eigenvalue of AB, then $\exists v \in V \setminus \{ 0_V \}$ such that

$$AB\,v = \lambda\,v.$$

- Case $\lambda = 0$, then AB is singular $\implies$ BA is not invertible too, which lets us conclude that $\lambda = 0$ is also an eigenvalue of BA.

- Case $\lambda \neq 0$, then $Bv \neq 0_V$, then pre-multiplying by B gives

$$BA\,(Bv) = \lambda\,(Bv)$$

which shows that λ is also an eigenvalue of BA with eigenvector Bv. □

Question 3

(a) **True.**

Claim. Let v be an eigenvector of φ corresponding to eigenvalue λ. For any $n \in \mathbb{N}$, $\varphi^n\,v = \lambda^n\,v$.

Proof (of Claim). It is given that $\varphi\,v = \lambda\,v$. Suppose $\varphi^{n-1}\,v = \lambda^{n-1}v$, then $\varphi^n\,v = \varphi^{n-1}(\varphi v) = \varphi^{n-1}(\lambda\,v) = \lambda\,\varphi^{n-1}\,v$ by linearity. Applying induction hypothesis gives us the conclusion that $\varphi^n\,v = \lambda^n\,v$. □

Proof (of 3a). Let $\lambda \in \mathbb{C}$ be an eigenvalue of φ, so $\exists v \in V \setminus \{\,0\,\}\,.\,\varphi\,v = \lambda\,v$. Let $f(T) \in \mathbb{C}[T]$ be given by

$$f(T) = \sum_{i=0}^{\deg(f)} f_i\,T^i.$$

Evaluating f at φ gives us an endomorphism,

$$\begin{aligned}
f(\varphi) &= \sum_{i=0}^{\deg(f)} f_i\,\varphi^i && \text{in } \operatorname{End}(V)\\
f(\varphi)\,v &= \sum_{i=0}^{\deg(f)} f_i\,\varphi^i\,v && \text{in } V\\
&= \sum_{i=0}^{\deg(f)} f_i\,\lambda^i\,v && \text{by Claim}\\
&= f(\lambda)\,v
\end{aligned}$$

this shows that $f(\lambda) \in \mathbb{C}$ is an eigenvalue of $f(\varphi)$. □

(b) **True.**

Proof. Let a be an eigenvalue of $f(\varphi)$, so

$$\exists v \in V \setminus \{\,0\,\}\,.\,(f(\varphi) - aI)\,v = 0.$$

Consider the polynomial $f(T) - a \in \mathbb{C}[T]$, by Fundamental Theorem of Algebra, there exists

$\lambda_1, \ldots, \lambda_k, c \in \mathbb{C}$ such that

$$f(T) - a = c \cdot \prod_{i=1}^{k} (T - \lambda_i) \quad \text{in } \mathbb{C}[T] \tag{$\dagger$}$$

evaluating at φ gives

$$f(\varphi) - aI = c \cdot \prod_{i=1}^{k} (\varphi - \lambda_i I) \quad \text{in } \mathrm{End}_{\mathbb{C}}(V)$$

As it is known that LHS is singular, by multiplicativity of determinant, RHS is necessarily singular, so (at least) one of $\varphi - \lambda_i I$ is singular, so

$$\exists \lambda \in \{ \lambda_1, \ldots, \lambda_k \} .\ \det(\varphi - \lambda I) = 0$$

which implies that λ is an eigenvalue of φ, then evaluating $(\dagger)$ at λ gives

$$f(\lambda) - a = c \cdot 0 \implies a = f(\lambda). \qquad \square$$

Question 4

(a) **True.**

Proof. Let $f(T) \in \mathbb{C}[T]$ be given by

$$f(T) := T^k - 1.$$

then $f(A) = A^k - 1_n = 0$ in $\mathbb{M}_n(\mathbb{C})$, so f annihilates A. We see that f has the following factorisation in $\mathbb{C}[T]$

$$T^k - 1 = \prod_{j=0}^{k-1} \left(T - e^{j \cdot 2\pi i / k}\right)$$

Let $m(T) \in \mathbb{C}[T]$ be the minimal polynomial of A, then it is necessary that $m(T) \mid f(T)$. As $f(T)$ splits completely into distinct linear factors, $m(T)$ also has this property. This means that A is diagonalisable. $\square$

(b) **False.**

Counter-example. Consider $A := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in \mathbb{M}_2(\mathbb{C})$. $A^2 = 0$ is certainly diagonalisable, but A is already in Jordan canonical form and is not diagonalisable. $\square$

Question 5

Definition. For any $z \in \mathbb{C}$ that is algebraic over $\mathbb{Q}$, let the **minimal polynomial** of z refer to the (necessarily unique) monic generator of the ideal of polynomials over $\mathbb{Q}$ which annihilates z. (ie. The lowest degree monic polynomial with rational coefficients which has z as a root.)

Lemma. Let $f \in \mathbb{Q}[T]$, let $z \in \mathbb{C}$ be algebraic over $\mathbb{Q}$ with $f(z) = 0$, then m_z divides f in $\mathbb{Q}[T]$.

Proof (Lemma). First apply division algorithm in $\mathbb{Q}[T]$, so $\exists q, r \in \mathbb{Q}[T]$ such that

$$f(T) = q(T) \cdot m_z(T) + r(T) \quad \text{in } \mathbb{Q}[T],$$

with $\deg(r) < \deg(m_z)$. Then evaluation at z gives

$$0 = q(z) \cdot 0 + r(z) \quad \text{in } \mathbb{C}.$$

By minimality of m_z, r is necessarily the zero polynomial. Hence $m_z \mid f$. $\square$

Proof (Q5). Let $n = \dim_{\mathbb{Q}} V$. When $n = 0$, the conclusion trivially holds, so suppose $n \neq 0$. Fix any ordered basis, and let $A \in \mathbb{M}_n(\mathbb{Q})$ be the matrix representation of φ. Let $f(T) \in \mathbb{Q}[T]$ be the characteristic polynomial of A. We know that $\deg(f) = n$.

The polynomial $T^p - 1$ can also be factorised in $\mathbb{Q}[T]$ like so

$$T^p - 1 = (T - 1)\left(T^{p-1} + \cdots + T + 1\right) \quad \text{in } \mathbb{Q}[T]$$

Let $m(T) \in \mathbb{Q}[T]$ be given by $m(T) := T^{p-1} + \cdots + T + 1$. Evaluation at φ gives

$$\varphi^p - \mathrm{id}_V = 0 = (\varphi - \mathrm{id}_V) m(\varphi) \quad \text{in } \mathrm{End}(V)$$

as $(\varphi - \mathrm{id}_V)v = 0$ implies $v = 0_V$, we have $m(\varphi) = 0$ in $\mathrm{End}(V)$. So m annihilates φ, and similarly also annihilates its matrix representation A.

Now consider the field of complex numbers, and the corresponding linear map $\mathbb{C}^n \to \mathbb{C}^n$ that A characterises. Because m annihilates A, for any of its eigenvalues $\lambda \in \mathbb{C}$, $m(\lambda) = 0$ (corollary of 3a). As it is given that m is irreducible over $\mathbb{Q}$, m will be the minimal polynomial of λ.

Lastly, proceed to repeatedly apply lemma to obtain the result that

$$f(T) = m(T)^k \cdot l \quad \text{for some } k \in \mathbb{N} \setminus \{0\}, l \in \mathbb{Q} \setminus \{0\}.$$

Choose any root $\lambda \in \mathbb{C}$ of $f(T)$, then because λ is an eigenvalue of A, by Lemma we have $m \mid f$ in $\mathbb{Q}[T]$, so $\exists q \in \mathbb{Q}[T].\ f = m \cdot q$.

1. Case q has no roots in $\mathbb{C}$, by our earlier assumption that f nonzero, q is a constant polynomial.
2. Case q has a root, say $z \in \mathbb{C}$, then $f(z) = 0$, which means z is an eigenvalue of A. Using the same argument, we obtain that z is also a root of $m(T)$ and by Lemma, $m \mid q$. Then $\exists q'(T) \in \mathbb{Q}[T]$ such that $f = m^2 \cdot q'$. Repeat this process until $q_k(T)$ is degree 0, and we obtain the result stated earlier.

Then taking degrees,

$$\deg(f) = k\ \deg(m) \implies n = k(p-1) \text{ for some } k \in \mathbb{N} \setminus \{\, 0 \,\},$$

which shows $p - 1 \mid \dim_{\mathbb{Q}} V$. □

Question 6

Proof. Rewriting the recurrence equation in matrix form gives us that for any $n \geq 1$,

$$\begin{pmatrix} P_{n+1} \\ P_n \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} P_n \\ P_{n-1} \end{pmatrix}$$

recursive expansion gives that for any $n \geq 0$,

$$\begin{aligned} \begin{pmatrix} P_{n+1} \\ P_n \end{pmatrix} &= \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} P_1 \\ P_0 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{aligned}$$

Finding a closed form formula for Pell numbers reduces to diagonalising the matrix $A := \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$. Let $f(t) \in \mathbb{R}[t]$ be characteristic polynomial of A,

$$\begin{aligned} f(t) &= (2-t)(-t) - 1 \\ &= t^2 - 2t - 1 \end{aligned}$$

Roots of f are $\frac{2 \pm \sqrt{8}}{2} = 1 \pm \sqrt{2}$. Let $\alpha := 1 + \sqrt{2}$ and $\beta := 1 - \sqrt{2}$, note that they can be characterised as solutions of the equation $t^2 = 2t + 1$. Using this property, it becomes clear that $\begin{pmatrix} \alpha \\ 1 \end{pmatrix}$ is an eigenvector (with eigenvalue α), because

$$\begin{aligned}
\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ 1 \end{pmatrix} &= \begin{pmatrix} 2\alpha + 1 \\ \alpha \end{pmatrix} \\
&= \begin{pmatrix} \alpha^2 \\ \alpha \end{pmatrix} \\
&= \alpha \begin{pmatrix} \alpha \\ 1 \end{pmatrix}
\end{aligned}$$

As β has the same characterising property, the same computation will also show that $\begin{pmatrix} \beta \\ 1 \end{pmatrix}$ is an eigenvector for eigenvalue β. Since the eigenspace has enough dimensions, A is diagonalisable, in fact

$$\begin{aligned}
A &= \begin{pmatrix} \alpha & \beta \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ 1 & 1 \end{pmatrix}^{-1} \\
A^n &= \begin{pmatrix} \alpha & \beta \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}^n \begin{pmatrix} \alpha & \beta \\ 1 & 1 \end{pmatrix}^{-1} \\
&= \frac{1}{\alpha - \beta} \begin{pmatrix} \alpha & \beta \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \alpha^n & 0 \\ 0 & \beta^n \end{pmatrix} \begin{pmatrix} 1 & -\beta \\ -1 & \alpha \end{pmatrix}
\end{aligned}$$

substituting that into our original expression for $\begin{pmatrix} P_{n+1} \\ P_n \end{pmatrix}$, we can derive the closed form,

$$\begin{aligned}
\begin{pmatrix} P_{n+1} \\ P_n \end{pmatrix} &= A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
&= \frac{1}{\alpha - \beta} \begin{pmatrix} \alpha & \beta \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \alpha^n & 0 \\ 0 & \beta^n \end{pmatrix} \begin{pmatrix} 1 & -\beta \\ -1 & \alpha \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
&= \frac{1}{\alpha - \beta} \begin{pmatrix} \alpha^{n+1} & \beta^{n+1} \\ \alpha^n & \beta^n \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \\
&= \frac{1}{\alpha - \beta} \begin{pmatrix} \alpha^{n+1} - \beta^{n+1} \\ \alpha^n - \beta^n \end{pmatrix}
\end{aligned}$$

then we have

$$\begin{aligned}
P_n &= \frac{1}{\alpha - \beta}(\alpha^n - \beta^n) \\
&= \frac{1}{2\sqrt{2}} \cdot \alpha^n - \frac{1}{2\sqrt{2}} \cdot \beta^n
\end{aligned}$$

and $\alpha = 1 + \sqrt{2}, \beta = 1 - \sqrt{2}, c = \frac{1}{2\sqrt{2}}, d = -\frac{1}{2\sqrt{2}}$ can all be verified to be real numbers. $\square$