Math 113 Homework 6 Solutions

Solutions by Guanyang Wang, with edits by Tom Church.

Exercises from the book.

Exercise 6.A.16 Suppose $u, v \in V$ are such that

$$\|u\| = 3, \|u + v\| = 4, \|u - v\| = 6.$$

What number does $\|v\|$ equal?

Answer. We will use the following two formulas.

$$\begin{aligned} ||u+v||^2 &= \langle u+v, u+v\rangle \\ &= \langle u, u\rangle + \langle u, v\rangle + \langle v, u\rangle + \langle v, v\rangle \\ &= ||u||^2 + 2\langle u, v\rangle + ||v||^2 \end{aligned}$$

since $\langle u, v\rangle = \langle v, u\rangle$ because V is over $\mathbb{R}$.

And,

$$\begin{aligned} ||u-v||^2 &= \langle u-v, u-v\rangle \\ &= \langle u, u\rangle + \langle u, -v\rangle + \langle -v, u\rangle + \langle -v, -v\rangle \\ &= ||u||^2 - 2\langle u, v\rangle + ||v||^2 \end{aligned}$$

again where the simplifications are justified because V is over $\mathbb{R}$.

Adding these two equations together, we get that

$$||u+v||^2 + ||u-v||^2 = 2||u||^2 + 2||v||^2$$

(This is called the parallelogram identity. Think of u and v as the sides of the parallelogram, and $u+v$ and $u-v$ as its diagonals.)

We are given that $||u+v|| = 4$, $||u-v|| = 6$ and $||u|| = 3$. Thus,

$$16 + 36 = 18 + 2||v||^2$$

implies that $||v||^2 = 17$. Therefore $||v|| = \sqrt{17}$. □

Exercise 6.B.5 On $\mathcal{P}_2(\mathbb{R})$, consider the inner product given by

$$\langle p, q\rangle = \int_0^1 p(x)q(x)\,dx$$

Apply the Gram-Schmidt Procedure to the basis $1, x, x^2$ to produce an orthonormal basis of $\mathcal{P}_2(\mathbb{R})$.

Proof. Denote $v_0 = 1, v_1 = x$ and $v_2 = x^2$. We use the formula 6.31. This gives us

$$e_0 = \frac{v_0}{||v_0||}$$

so we need to compute the norm of v_0. We have $||v_0||^2 = \langle v_0, v_0\rangle$. So we use that

$$\langle v_0, v_0\rangle = \int_0^1 1(x)1(x)dx = 1$$

to see that $||v_0|| = 1$. Therefore

$$e_0 = 1$$

Next, we need to find a constant a_1 s.t. $v_1 - ae_0$ is perpendicular to e_0. We have that

$$\begin{aligned}\langle v_1 - a_0e_0, e_0\rangle &= \int_0^1 (v_1(x) - a_0e_0(x))e_0(x)dx \\ &= \int_0^1 (x - a_0)1dx \\ &= \frac{1}{2} - a_0\end{aligned}$$

Thus,

$$\langle v_1 - ae_0, e_0\rangle = 0 \iff a_0 = \frac{1}{2}$$

So $f_1(x) = x - \frac{1}{2}$ is perpendicular to e_0. We need to scale it so that it has norm one. First we compute $||f_1(x)||^2$:

$$\langle f_1(x), f_1(x)\rangle = \int_0^1 (x - \frac{1}{2})(x - \frac{1}{2})\,dx = \frac{1}{12}$$

Thus, $||f_1(x)|| = \frac{1}{\sqrt{12}}$. We want $e_1 = \frac{f_1(x)}{||f_(x)||}$. Therefore,

$$e_1 = \sqrt{12}(x - \frac{1}{2}) = \sqrt{3}(2x - 1)$$

Lastly, we need to find constants a_2, b_2 s.t. $v_2 - a_2e_1 - b_2e_0$ is perpendicular to both e_1 and e_2. We have that

$$\begin{aligned}\langle v_2 - a_2e_1 - b_2e_0, e_0\rangle &= \langle v_2 - b_2e_0, e_0\rangle \\ &= \langle x^2 - b_2, 1\rangle \\ &= \int_0^1 x^2 - b_2dx \\ &= \frac{1}{3} - b_2\end{aligned}$$

So, $b_2 = \frac{1}{3}$.

Next,

$$\begin{aligned}\langle v_2 - a_2e_1 - b_2e_0, e_1\rangle &= \langle v_2 - a_2e_1, e_1\rangle \\ &= \langle v_2, e_1\rangle - a_2 \\ &= \langle x^2, \sqrt{12}(x - \frac{1}{2})\rangle - a_2 \\ &= \int_0^1 x^2\sqrt{12}(x - \frac{1}{2})\,dx - a_2 \\ &= \sqrt{12}\int_0^1 x^3 - \frac{1}{2}x^2dx - a_2 \\ &= \sqrt{12}\left(\frac{1}{4} - \frac{1}{6}\right) - a_2 \\ &= \frac{\sqrt{12}}{12} - a_2\end{aligned}$$

So $\langle v_2 - a_2e_1 - b_2e_0, e_1\rangle = 0$ iff $a_2 = \frac{\sqrt{12}}{12}$. Note that $a_2e_1 = x - \frac{1}{2}$. Thus $f_2 = v_2 - a_2e_1 - b_2e_0 = x^2 - x + \frac{1}{6}$ is perpendicular to both e_0 and e_1. We want to normalize f_2 to get e_2. So we compute its norm:

$$\begin{aligned} ||f_2||^2 &= \langle f_2, f_2\rangle \\ &= \int_0^1 (x^2 - x + \frac{1}{6})^2 dx \\ &= \frac{1}{180} \end{aligned}$$

Thus, $||f_2|| = \frac{1}{\sqrt{180}}$, so $e_2 = \frac{f_2(x)}{||f_2(x)||}$ is

$$e_2 = \sqrt{180}(x^2 - x + \frac{1}{6}) = \sqrt{5}(1 - 6x + 6x^2)$$

So the orthonormal basis we obtain via the Gram-Schmidt method is:

$$\boxed{e_0 = 1, \qquad e_1 = \sqrt{3}(2x - 1), \qquad \text{and } e_2 = \sqrt{5}(1 - 6x + 6x^2).}$$

□

Exercise 6.B.7. Find a polynomial $q \in \mathcal{P}_2(\mathbb{R})$ such that

$$p(\frac{1}{2}) = \int_0^1 p(x)q(x)\,dx$$

For every $p \in \mathcal{P}_2(\mathbb{R})$

Proof. We will use the orthonormal basis we found in Exercise 6.B.5. It was $e_0 = 1, e_1 = \sqrt{3}(2x - 1)$ and $e_2 = \sqrt{5}(6x^2 - 6x + 1)$. Any polynomials $p(x)$ and $q(x)$ can be expressed as linear combinations of e_0, e_1 and e_2. Suppose $p(x), q(x)$ are written

$$p(x) = a_0e_0 + a_1e_1 + a_2e_2 \text{ and } q(x) = b_0e_0 + b_1e_1 + b_2e_2$$

Since $\int_0^1 p(x)q(x)\,dx$ is the inner product of $p(x)$ and $q(x)$, we want to find a $q(x)$ s.t. $\langle p(x), q(x)\rangle = p(1/2)$ for each polynomial $p(x)$. Since e_0, e_1, e_2 are an orthonormal basis,

$$\begin{aligned} \langle p(x), q(x)\rangle &= \langle a_0e_0 + a_1e_1 + a_2e_2, b_0e_0 + b_1e_1 + b_2e_2\rangle \\ &= a_0b_0 + a_1b_1 + a_2b_2 \end{aligned}$$

On the other hand, if $p(x) = a_0e_0 + a_1e_1 + a_2e_2$ then $p(1/2) = a_0 - \frac{\sqrt{5}}{2}a_2$. (We use that $e_0(1/2) = 1$, $e_1(1/2) = 0$ and $e_2(1/2) = \sqrt{5}(-\frac{1}{2})$.)

Thus, let $q(x) = b_0e_0 + b_1e_1 + b_2e_2$ for $b_0 = 1$, $b_1 = 0$ and $b_2 = -\frac{\sqrt{5}}{2}$. So

$$\boxed{q(x) = -15x^2 + 15x - \frac{3}{2}}$$

Then $\langle p(x), q(x)\rangle = a_0 - \frac{\sqrt{5}}{2}a_2$. That is, $p(\frac{1}{2}) = \int_0^1 p(x)q(x)dx$ for each $p(x) \in \mathcal{P}_2(\mathbb{R})$. □

Exercise 6.B.8 Find a polynomial $q \in \mathcal{P}_2(\mathbb{R})$ such that

$$\int_0^1 p(x)(\cos \pi x)\,dx = \int_0^1 p(x)q(x)\,dx.$$

for every $p \in \mathcal{P}_2(\mathbb{R})$

Proof. We will use the orthonormal basis we found in Exercise 6.B.5. It was $e_0 = 1, e_1 = \sqrt{3}(2x-1)$ and $e_2 = \sqrt{5}(6x^2-6x+1)$. Any polynomials $p(x)$ and $q(x)$ can be expressed as linear combinations of e_0, e_1 and e_2. Suppose $p(x), q(x)$ are written

$$p(x) = a_0e_0 + a_1e_1 + a_2e_2 \text{ and } q(x) = b_0e_0 + b_1e_1 + b_2e_2$$

Since $\int_0^1 p(x)q(x)\,dx$ is the inner product of $p(x)$ and $q(x)$, we want to find a $q(x)$ s.t. $\langle p(x), q(x)\rangle = \int_0^1 p(x)\cos(\pi x)\,dx$ for each polynomial $p(x)$. Since e_0, e_1, e_2 are an orthonormal basis,

$$\begin{aligned}\langle p(x), q(x)\rangle &= \langle a_0e_0 + a_1e_1 + a_2e_2, b_0e_0 + b_1e_1 + b_2e_2\rangle \\ &= a_0b_0 + a_1b_1 + a_2b_2\end{aligned}$$

On the other hand, if $p(x) = a_0e_0 + a_1e_1 + a_2e_2$ then $\int_0^1 p(x)\cos(\pi x)\,dx = \frac{-4\sqrt{3}}{\pi^2}a_1$. (We use that $\int_0^1 e_0(x)\cos(\pi x)\,dx = 0$, $\int_0^1 e_1(x)\cos(\pi x)\,dx = \frac{-4\sqrt{3}}{\pi^2}$ and $\int_0^1 e_2(x)\cos(\pi x)\,dx = 0$.)

Thus, let $q(x) = b_0e_0 + b_1e_1 + b_2e_2$ for $b_0 = 0$, $b_1 = \frac{-4\sqrt{3}}{\pi^2}$ and $b_2 = 0$. So

$$\boxed{q(x) = \frac{-24x+12}{\pi^2}}$$

Then $\langle p(x), q(x)\rangle = \frac{-4\sqrt{3}}{\pi^2}a_1$. That is, $\int_0^1 p(x)(\cos\pi x)\,dx = \int_0^1 p(x)q(x)\,dx$ for each $p(x) \in \mathcal{P}_2(\mathbb{R})$. □

Question 1. Let V be a finite-dimensional vector space over $\mathbb{C}$, and let $T \in \mathcal{L}(V)$. Let U, W be nonzero subspaces s.t. $V = U \oplus W$. Assume U, W are invariant under T, so we can restrict the operator $T : V \to V$ to an operator $T|_U : U \to U$ and similarly we can restrict T to an operator $T|_W : W \to W$.

a) Prove that if $\lambda \in \mathbb{C}$ is an eigenvalue of T, then either λ is an eigenvalue of $T|_U$ or λ is an eigenvalue of $T|_W$ (or both).

   Let $f(x)$ be the minimal polynomial of $T|_U$ and let $g(x)$ be the minimal polynomial of $T|_W$.

b) Prove that $f(T)g(T) = 0$ in $\mathcal{L}(V)$.

c) Prove that if $f(x), g(x)$ have no shared roots, then $f(x)g(x)$ is the minimal polynomial of T.

d) Prove that if $f(x), g(x)$ have a shared rood $\lambda \in \mathbb{C}$ then $f(x)g(x)$ is not the minimal polynomial of T.

Proof. a) Suppose λ is an eigenvalue of T. Then there is some $v \in V$ s.t. $Tv = \lambda v$ (and $v \neq 0$). Since $V = U \oplus W$, we can write $v = u + w$ for some $u \in U$ and $w \in W$. Thus $Tv = Tu + Tw$, so $Tv = \lambda v$ implies that

$$Tu + Tw = \lambda u + \lambda w$$

Since U and W are invariant under T, $Tu \in U$ and $Tw \in W$. We also have that $\lambda u \in U$ and $\lambda w \in W$. Since V is the direct sum of U and W, there is only one way to write any vector as a sum of an element of U and an element of W. Therefore we must have that $Tu = \lambda u$ and $Tw = \lambda w$.

Since $v \neq 0$, either u or w is non-zero. Suppose that $u \neq 0$. Then $Tu = \lambda u$ implies $T|_U u = \lambda u$. So λ is an eigenvalue for $T|_U$. Otherwise, if $u = 0$ we must have $w \neq 0$. Then $Tw = \lambda w$ implies $T|_W w = \lambda w$, so λ is an eigenvalue for $T|_W$. Therefore λ is an eigenvalue for either $T|_U$ or $T|_W$ (or both.)

b) Let $f(x)$ be the minimal polynomial of $T|_U$ and let $g(x)$ be the minimal polynomial of $T|_W$. We need to show that for any $v \in V$, $f(T)g(T)v = 0$.

Since $f(x)$ is the minimal polynomial of $T|_U$ we know that $f(T|_U)(u) = 0$ for any $u \in U$. Moreover since $T(u) = T|_U(u)$ for any $u \in U$, this can be written simply as $f(T)(u) = 0$ for any $u \in U$. Similarly, since $g(x)$ is the minimal polynomial for $T|_W$, we have $g(T)(w) = g(T|_W)(w) = 0$ for any $w \in W$.

Since $V = U \oplus W$, any $v \in V$ can be written as $v = u + w$ for $u \in U$ and $w \in W$. Therefore

$$\begin{aligned} f(T)g(T)(v) &= f(T)g(T)](u+w) \\ &= f(T)[g(T)(u+w)] \\ &= f(T)[g(T)(u)] + f(T)[g(T)(w)] \\ &= g(T)[f(T)(u)] + f(T)[g(T)(w)] \quad \text{(since } f(T) \text{ and } g(T) \text{ commute)} \\ &= 0 + 0 = 0, \end{aligned}$$

as desired.

c) In this proof, we will frequently use the general theorem that if $p(x)$ is the minimal polynomial of a linear operator T, and if $f(T) = 0$ for some other polynomial $f(x)$, then $p(x)$ divides $f(x)$.

Let $h(x) = f(x)g(x)$. Let $p(x)$ be the minimal polynomial of T. Since $h(T) = 0$, we have that $p(x)$ divides $h(x)$. In particular, the degree of $h(x)$ is at least the degree of $p(x)$.

Note that if $u \in U$, $f(T|_U)g(T|_U)(u) = f(T)g(T)(u) = 0$, and the same holds for $w \in W$. Thus $h(T|_U) = 0$ and $h(T|_W) = 0$. Since $f(x)$ is the minimal polynomial of $T|_U$, we have that $f(x)$ divides $h(x)$. Likewise, $g(x)$ divides $h(x)$, as well.

Since V is a vector space over $\mathbb{C}$, we can write $f(x), g(x)$ and $p(x)$ in terms of linear factors:

$$f(x) = \prod_{i=1}^{k} (x - \lambda_i)$$

where $\lambda_1, \ldots, \lambda_k$ are the eigenvalues for $T|_U$.

$$g(x) = \prod_{i=k+1}^{n} (x - \lambda_i)$$

where $\lambda_{k+1}, \ldots, \lambda_n$ are the eigenvalues for $T|_W$.

$$p(x) = \prod_{i=1}^{m} (x - \beta_i)$$

where $\beta_1, \ldots, \beta_m$ are the eigenvalues for T. Since the degree of $h(x)$ is at least the degree of $p(x)$, $m \leq n$.

Since $f(x)$ divides $p(x)$, every term $(x - \lambda_i)$ for $i = 1, \ldots, k$ of $f(x)$ is a term of $p(x)$, as well. Thus, we can renumber the β_i s.t. $\beta_i = \lambda_i$ for $i = 1, \ldots, k$. Likewise, since $g(x)$ divides $p(x)$, every term $(x - \lambda_i)$ for $i = k+1, \ldots, n$ of $g(x)$ corresponds to a term $(x - \beta_{j_i}$ in $p(x)$. Since $T|_U$ and $T|_W$ have no common eigenvalues, no λ_i for $i = k+1, \ldots, n$ corresponds any of $\beta_1, \ldots, \beta_k$. Thus, we can renumber $\beta_{k+1}, \ldots, \beta_m$ s.t. $\lambda_i = \beta_i$ for $i = k+1, \ldots, n$. In particular, $m \geq n$.

Therefore, $m = n$, so the degree of $h(x)$ equals the degree of $p(x)$. Since $f(x), g(x)$ are minimal polynomials, they are monic. Thus $h(x) = f(x)g(x)$ is a monic polynomial. Since $h(x)$ and $p(x)$ are both monic and have the same degree, they are equal.

d) Prove that if $f(x), g(x)$ have a shared root $\lambda \in \mathbb{C}$ then $f(x)g(x)$ is not the minimal polynomial of T.

Suppose $f(x), g(x)$ have a shared root $\lambda \in \mathbb{C}$. Again, let

$$f(x) = \prod_{i=1}^{k} (x - \lambda_i)$$

where $\lambda_1, \ldots, \lambda_k$ are the eigenvalues for $T|_U$.

$$g(x) = \prod_{i=k+1}^{n} (x - \lambda_i)$$

where $\lambda_{k+1}, \ldots, \lambda_n$ are the eigenvalues for $T|_W$.

Up to renumbering, we can assume that $\lambda_1 = \lambda_n$. Then consider the polynomial

$$h(x) = \prod_{i=1}^{n-1} (x - \lambda_i)$$

where we multiply $f(x)$ and $g(x)$ but get rid of the last factor $(x - \lambda_n)$. Then $f(x)$ and $g(x)$ both still divide $h(x)$. So, there are polynomials $a(x)$ and $b(x)$ s.t. $h(x) = a(x)f(x) = b(x)g(x)$.

We claim that $h(T) = 0$. First, suppose $u \in U$. Then $h(T)(u) = a(T)f(T)(u)$. Since f is the minimal polynomial of $T|_U$, $f(T)(u) = 0$. Thus $a(T)(f(T)(u)) = 0$, so $h(T)(u) = 0$. Likewise, since $g(x)$ is the minimal polynomial of $T|_W$, $g(T)(w) = 0$ for any $w \in W$. Thus $h(T)(w) = 0$. Let $v \in V$. We can write $v = u + w$ for $u \in U$ and $w \in W$. Then

$$\begin{aligned} h(T)(v) &= h(T)(u + w) \\ &= h(T)(u) + h(T)(w) \\ &= 0 \end{aligned}$$

Therefore, $h(T) = 0$. Since the degree of $h(T)$ is one less than the degree of $f(x)g(x)$, and $h(T) = 0$, $f(x)g(x)$ cannot be the minimal polynomial of T. □

Question 2. Let V be an inner product space over $\mathbb{R}$, and suppose that $T \in \mathcal{L}(V)$ satisfies $\|Tv\| = \|v\|$ for all $v \in V$. Prove that T has at most two eigenvalues.

Proof. For any eigenvalue λ of T, we can find an eigenvector v of T corresponding to λ. So we have

$$\|Tv\| = |\lambda| \cdot \|v\| = \|v\|$$

Since $v \neq 0$, we must have $|\lambda| = 1$. But V is an inner product space over $\mathbb{R}$, and the only real numbers with absolute value 1 are 1 and -1. Therefore the only possible eigenvalues are $\lambda = 1$ and $\lambda = -1$; in particular, T can have at most 2 eigenvalues. □

Question 3. Fix an integer $n \geq 1$, and let $V = \mathbb{C}^n$ with the standard inner product. We let $R : V \to V$ be the operator defined by

$$R(a_1, \dots, a_n) = (a_2, \dots, a_n, a_1)$$

a) Set $p(x) = x^n - 1$. Prove that $p(R) = 0$. Convince yourself that $p(x) = x^n - 1$ is in fact the minimal polynomial of R.
b) Since $p(x)$ has n distinct roots, we know that R is diagonalizable. Diagonalize R by finding a basis of eigenvectors $v_1, \dots, v_n$ for $\mathbb{C}^n$ satisfying

$$R(v_i) = \omega^i v_i \text{ and } ||v_i|| = 1$$

c) Prove that if $\mu \in \mathbb{C}$ satisfies $\mu^n = 1$ but $\mu \neq 1$, then $1 + \mu + \mu^2 + \cdots + \mu^{n-1} = 0$.
d) Prove your basis $v_1, \dots, v_n$ is orthonormal.
e) If $v = (a_1, \dots, a_n)$ is written as $v = b_1 v_1 + \cdots + b_n v_n$, give a formula for the coefficient b_i in terms of the coordinates $a_1, \dots, a_n$.
f) If $v = (a_1, \dots, a_n)$ is written as $v = b_1 v_1 + \cdots + b_n v_n$, give a formula for the coordinate a_i in terms of the coefficients $b_1, \dots, b_n$.
g) If $v = (a_1, \dots, a_n)$ is written as $v = b_1 v_1 + \cdots + b_n v_n$, prove that the coordinates $a_1, \dots, a_n$ and the coefficients $b_1, \dots, b_n$ satisfy the relation

$$|a_1|^2 + \cdots + |a_n|^2 = |b_1|^2 + \cdots + |b_n|^2$$

Proof. (a) For any element $a = (a_1, \dots, a_n) \in \mathbb{C}^n$, we just need to prove that $R^n a = a$. Since $Ra = R(a_1, \dots, a_n) = (a_2, \dots, a_n, a_1)$, we have

$$R^2 a = R(a_2, \dots, a_n, a_1) = R(a_3, \dots, a_n, a_1, a_2).$$

Repeating this n times, we conclude that

$$R^{n-1} a = (a_n, a_1, \dots, a_{n-1})$$

$$R^n a = R(R^{n-1} a) = R(a_n, a_1, \dots, a_{n-1}) = (a_1, \dots, a_n) = a.$$

Therefore we have $(R^n - I)a = 0$. Therefore $p(R) = 0$, as desired.

(b) We just need to show that if $f(x)$ is a nonzero polynomial of degree $< n$, then $f(R) \neq 0$. Write this polynomial as $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$ for some coefficients $c_0, c_1, c_2, \dots, c_{n-1} \in \mathbb{C}$. [Note that we have not bothered to assume that $f(x)$ is monic; it's a bit easier that way, notationally.]

Consider the vector $v = (0, \dots, 0, 1)$. We will show that $f(R)$ is not the zero operator by showing that $f(R)v$ is not the zero vector. From the computations above, we know that

$$Rv = (0, \dots, 0, 1, 0), \qquad R^2 v = (0, \dots, 1, 0, 0), \dots \qquad R^{n-1} v = (1, 0, \dots, 0).$$

Therefore $f(R)v$ is equal to

$$\begin{aligned}
\left(c_0 + c_1 R + c_2 R^2 + \cdots + c_{n-1} R^{n-1}\right) v &= c_0 v + c_1 Rv + c_2 R^2 v + \cdots + c_{n-1} R^{n-1} v \\
&= \quad (0, \dots, 0, 0, c_0) \\
&\quad + (0, \dots, 0, c_1, 0) \\
&\quad + (0, \dots, c_2, 0, 0) \\
&\quad + \cdots \\
&\quad + (c_{n-1}, \dots, 0, 0, 0) \\
&= (c_{n-1}, \dots, c_3, c_2, c_1, c_0)
\end{aligned}$$

Since $f(x)$ is a nonzero polynomial, at least one of the coefficients c_i must be nonzero, so this vector $f(R)v = (c_{n-1}, \ldots, c_3, c_2, c_1, c_0)$ must be nonzero. This proves that n is the smallest possible degree of a polynomial with $f(R) = 0$; since $p(x)$ has degree n, this shows that $p(x) = x^n - 1$ is the minimal polynomial of R.

(c) Let $w_i = (\omega^i, \omega^{2i}, \ldots, \omega^{ni})$ for $i = 1, \ldots, n$. So, $w_1 = (\omega, \omega^2, \ldots, \omega^{n-1}, 1)$, $w_2 = (\omega^2, \omega^4, \ldots, \omega^{2n-2}, 1)$ and so on until $w_n = (1, 1, \ldots, 1)$. We claim that these are eigenvectors s.t. w_i has eigenvalue ω^i. We can compute what R does to these vectors:

$$R(\omega^i, \omega^{2i}, \ldots, \omega^{ni}) = (\omega^{2i}, \omega^{3i}, \ldots, \omega^{ni}, \omega^i)$$

Since $\omega^i \cdot \omega^{ki} = \omega^{(k+1)i}$, we see that $R(w_i) = \omega^i \cdot w_i$ as desired. (Note that $\omega^{ni} = (\omega^n)^i = 1^i = 1$, so in the last coordinate we have $\omega^i \cdot \omega^{ni} = \omega^i$.) Since $1, \omega, \ldots, \omega^{n-1}$ are distinct eigenvalues, $w_1, \ldots, w_n$ are linearly independent. As there are n of them, they must form a basis for $\mathbb{C}^n$.

Since $|\omega| = 1$, we have that $|\omega^i| = 1^i = 1$ for all i. Thus for all i,

$$||w_i||^2 = |\omega^i| + |\omega^{2i}| + \cdots + |\omega^{ni}| = 1 + 1 + 1 + \cdots + 1 = n.$$

This shows that each of our eigenvectors w_i has length $||w_i|| = \sqrt{n}$. To get an eigenbasis $v_1, \ldots, v_n$ with length 1, we set $v_i = \frac{1}{\sqrt{n}} w_i$. In conclusion, $v_1, \ldots, v_n$ forms a basis for $\mathbb{C}^n$ s.t. $||v_i|| = 1$ for all i, and R is diagonal with respect to this basis. □

(d) If $\mu \neq 1$, then $1 - \mu$ is nonzero. If we multiply the sum $1 + \mu + \mu^2 + \cdots + \mu^{n-1}$ by $1 - \mu$, we get a telescoping sum:

$$\begin{aligned}(1-\mu)(1 + \mu + \mu^2 + \cdots + \mu^{n-1}) &= 1 - \mu + \mu - \mu^2 + \mu^2 - \cdots + \mu^{n-1} - \mu^n \\ &= 1 \qquad\qquad\qquad\qquad\qquad\quad - \mu^n\end{aligned}$$

But our assumption was that $\mu^n = 1$, so $1 - \mu^n = 0$. Since $1 + \mu + \mu^2 + \cdots + \mu^{n-1}$ becomes 0 when multiplied by the nonzero constant $1 - \mu$, it must be that $1 + \mu + \mu^2 + \cdots + \mu^{n-1} = 0$. □

(e) We have already shown that $||v_i|| = 1$ for all i. Now we need to show that $\langle v_i, v_j \rangle = 0$ for all $i \neq j$. So suppose that $i \neq j$. Then

$$\langle v_i, v_j \rangle = \frac{1}{n}\left(\omega^i \cdot \overline{\omega}^j + \omega^{2i} \cdot \overline{\omega}^{2j} + \cdots + \omega^{ni} \cdot \overline{\omega}^{nj}\right)$$

Since ω is on the unit circle, we know that $|\omega| = 1$, or in other words $\omega \cdot \overline{\omega} = 1$. This shows that $\overline{\omega} = \omega^{-1}$, and so in general $\overline{\omega}^{kj} = \omega^{-kj}$. Thus,

$$\langle v_i, v_j \rangle = \frac{1}{n}\left(\omega^{i-j} + \omega^{2(i-j)} + \cdots + \omega^{n(i-j)}\right)$$

Set $\mu = \omega^{i-j}$; note that the last term above is $\mu^n = \omega^{n(i-j)} = (\omega^n)^{i-j} = 1^{i-j} = 1$, so the sum inside the parentheses is

$$\mu + \mu^2 + \cdots + \mu^{n-1} + \mu^n = \mu + \mu^2 + \cdots + \mu^{n-1} + 1.$$

Since $i \neq j$ we know that $\mu \neq 1$, so part c) implies that the sum inside the parentheses is 0:

$$\langle v_i, v_j \rangle = \frac{1}{n}(1 + \mu + \mu^2 + \cdots + \mu^{n-1}) = \frac{1}{n} \cdot 0 = 0.$$

Therefore $\langle v_i, v_j \rangle = 0$ for all $i \neq j$, demonstrating that the vectors $v_1, \ldots, v_n$ form an orthonormal basis for $\mathbb{C}^n$. □

(f) If $v = b_1v_1 + \cdots + b_nv_n$, then $\langle v, v_i \rangle = b_i$ since $v_1, \ldots, v_n$ form an orthonormal basis for $\mathbb{C}^n$. Thus,

$$\begin{aligned} b_i &= \langle (a_1, a_2, \ldots, a_n), \frac{1}{\sqrt{n}}(\omega^i, \ldots, \omega^{ni}) \rangle \\ &= \frac{1}{\sqrt{n}}\big(a_1\omega^{-i} + a_2\omega^{-2i} + \cdots + a_n\omega^{-ni}\big) = \frac{1}{\sqrt{n}}\sum_{j=1}^{n}\omega^{-ij}a_j \end{aligned}$$

[TC: this is the analogue of the Fourier transform $\hat{f}(\theta) = \frac{1}{\sqrt{(2\pi)^n}}\int e^{-i\theta x}f(x)dx$.]

(g) If $v = b_1v_1 + \cdots + b_nv_n$, we can just compute

$$\begin{aligned} v = (a_1, \ldots, a_n) = &\frac{b_1}{\sqrt{n}}(\omega, \omega^2, \ldots, \omega^n) + \\ &+ \frac{b_2}{\sqrt{n}}(\omega^2, \omega^4, \ldots, \omega^{2n}) \\ &+ \vdots \\ &+ \frac{b_n}{\sqrt{n}}(1, 1, 1, \ldots, 1) \end{aligned}$$

So looking at the ith component we have:

$$a_i = \frac{1}{\sqrt{n}}\big(b_1\omega^i + b_2\omega^{2i} + \cdots + b_n\omega^{ni}\big) = \frac{1}{\sqrt{n}}\sum_{j=1}^{n}\omega^{ij}b_j$$

[TC: this is analogous to the inverse Fourier transform $f(x) = \frac{1}{\sqrt{(2\pi)^n}}\int e^{i\theta x}\hat{f}(\theta)d\theta$.]

□

(h) If we write $v = (a_1, \ldots, a_n)$ then the standard inner product on $\mathbb{C}^n$ satisfies $||v||^2 = |a_1|^2 + \cdots + |a_n|^2$.

On the other hand, if we write $v = b_1v_1 + \cdots + b_nv_n$, then

$$||v||^2 = \langle b_1v_1 + \cdots + b_nv_n, b_1v_1 + \cdots + b_nv_n \rangle.$$

Since $v_1, \ldots, v_n$ is an orthonormal basis, this is just

$$\langle b_1v_1 + \cdots + b_nv_n, b_1v_1 + \cdots + b_nv_n \rangle = |b_1|^2 + \cdots + |b_n|^2$$

Therefore we must have

$$|a_1|^2 + \cdots + |a_n|^2 = |b_1|^2 + \cdots + |b_n|^2,$$

because both sides are equal to $||v||^2$. □