Chapter 4: Polynomials

Linear Algebra Done Right, by Sheldon Axler

Problem 1

Verify all the assertions in 4.5 except the last one.

Proof. Suppose $w, z \in \mathbb{C}$, and let $a, b, c, d \in \mathbb{R}$ be such that $w = a + bi$ and $z = c + di$.

- Notice $z + \overline{z} = (c + di) + (c - di) = 2c = 2\Re(z)$.
- We have $z - \overline{z} = (c + di) - (c - di) = 2di = 2\Im(z)i$.
- Notice $z\,\overline{z} = (c + di)(c - di) = c^2 + d^2 = \left(\sqrt{c^2 + d^2}\right)^2 = |z|^2$.
- We have $\overline{w + z} = \overline{(a + c) + (b + d)i} = (a - bi) + (c - di) = \overline{w} + \overline{z}$. Also, $\overline{wz} = \overline{(ac - bd) + (ad + bc)i} = (ac - bd) - (ad + bc)i$ and $\overline{w}\,\overline{z} = (a - bi)(c - di) = (ac - bd) - (ad + bc)i$, so that $\overline{wz} = \overline{w}\,\overline{z}$.
- Notice $\overline{\overline{z}} = \overline{c - di} = c + di = z$.
- We have $\left|\Re(z)\right| = |c| = \sqrt{c^2} \leq \sqrt{c^2 + d^2} = |z|$, and similarly $\left|\Im(z)\right| = |d| = \sqrt{d^2} \leq \sqrt{c^2 + d^2} = |z|$.
- Notice $|\overline{z}| = |c - di| = \sqrt{c^2 + (-d)^2} = \sqrt{c^2 + d^2} = |z|$.
- We have

$$\begin{aligned}
|wz| &= \left|(ac - bd) + (ad + bc)i\right| \\
&= \sqrt{(ac - bd)^2 + (ad + bc)^2} \\
&= \sqrt{a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2} \\
&= \sqrt{(a^2 + b^2)(c^2 + d^2)} \\
&= \sqrt{a^2 + b^2}\sqrt{c^2 + d^2} \\
&= |w|\,|z|\,,
\end{aligned}$$

  as desired. $\square$

Problem 3

Is the set

$$\{0\} \cup \{p \in \mathcal{P}(\mathbb{F}) \mid \deg p \text{ is even}\}$$

a subspace of $\mathcal{P}(\mathbb{F})$?

Proof. Let $E = \{0\} \cup \{p \in \mathcal{P}(\mathbb{F}) \mid \deg p \text{ is even}\}$. Then E is not a subspace of $\mathcal{P}(\mathbb{F})$. To see this, notice $p(x) = x^2 \in E$ and $q(x) = -x^2 + x \in E$ (since $\deg(-x^2+x) = 2$), but $p+q = x \notin E$, so that E is not closed under addition. $\square$

Problem 5

Suppose m is a nonnegative integer, $z_1, \ldots, z_{m+1}$ are distinct elements of $\mathbb{F}$, and $w_1, \ldots, w_{m+1} \in \mathbb{F}$. Prove that there exists a unique polynomial $p \in \mathcal{P}_m(\mathbb{F})$ such that

$$p(z_j) = w_j$$

for $j = 1, \ldots, m+1$.

Proof. Define

$$\begin{aligned} T : \mathcal{P}_m(\mathbb{F}) &\to \mathbb{F}^{m+1} \\ p &\mapsto (p(z_1), \ldots, p(z_{m+1})). \end{aligned}$$

It suffices to show that T is an isomorphism, since injectivity implies uniqueness of such a $p \in \mathcal{P}_m(\mathbb{F})$, and surjectivity implies its existence. So we first show that T is a linear map. Suppose $p, q \in \mathcal{P}_m(\mathbb{F})$. Then

$$\begin{aligned} T(p+q) &= \big((p+q)(z_1), \ldots, (p+q)(z_{m+1})\big) \\ &= \big(p(z_1) + q(z_1), \ldots, p(z_{m+1}) + q(z_{m+1})\big) \\ &= \big(p(z_1), \ldots, p(z_{m+1})\big) + \big(q(z_1), \ldots, q(z_{m+1})\big) \\ &= Tp + Tq, \end{aligned}$$

so that T is additive. Next suppose $\lambda \in \mathbb{F}$. Then

$$\begin{aligned} T(\lambda p) &= \big((\lambda p)(z_1), \ldots, (\lambda p)(z_{m+1})\big) \\ &= \big(\lambda p(z_1), \ldots, \lambda p(z_{m+1})\big) \\ &= \lambda \big(p(z_1), \ldots, p(z_{m+1})\big) \\ &= \lambda(Tp), \end{aligned}$$

so that T is also homogenous. Hence T is a linear map. To see that T is an isomorphism, it's enough to show T is injective. So suppose $Tp = 0$ for some $p \in \mathcal{P}_m(\mathbb{F})$. Then

$$Tp = \big(p(z_1), \ldots, p(z_{m+1})\big) = (0, \ldots, 0),$$

and hence p has $m+1$ zeros. Since it has degree at most m, p must therefore be the zero polynomial, completing the proof. $\square$

Problem 7

Prove that every polynomial of odd degree with real coefficients has a real zero.

Proof. Suppose not. Then there exists some $p \in \mathcal{P}(\mathbb{R})$ of odd degree with no real zeros. By Theorem 4.17, p must be of the form

$$p(x) = c(x^2 + b_1 x + c_1) \cdots (x^2 + b_M x + c_M),$$

where $c, b_1, \ldots, b_M, c_1, \ldots, c_M \in \mathbb{R}$ and $M \in \mathbb{Z}^+$. But then p has even degree, a contradiction. Thus every polynomial of odd degree with real coefficients must indeed have a real zero. $\square$

Problem 9

Suppose $p \in \mathcal{P}(\mathbb{C})$. Define $q : \mathbb{C} \to \mathbb{C}$ by

$$q(z) = p(z)\,\overline{p(\overline{z})}\,.$$

Prove that q is a polynomial with real coefficients.

Proof. Suppose p has degree n. Then there exist $c, \lambda_1, \ldots, \lambda_n \in \mathbb{C}$ such that

$$p(z) = c(z - \lambda_1) \cdots (z - \lambda_n).$$

Thus we have

$$\begin{aligned}
q(z) &= c(z - \lambda_1) \cdots (z - \lambda_n)\,\overline{c\,(\overline{z} - \lambda_1) \cdots (\overline{z} - \lambda_n)} \\
&= c(z - \lambda_1) \cdots (z - \lambda_n)\,\overline{c}\left(z - \overline{\lambda_1}\right) \cdots \left(z - \overline{\lambda_n}\right) \\
&= c\overline{c}(z - \lambda_1)\left(z - \overline{\lambda_1}\right) \cdots (z - \lambda_n)\left(z - \overline{\lambda_n}\right) \\
&= |c|^2\left(z^2 - 2\Re(\lambda_1)z + |\lambda_1|^2\right) \cdots \left(z^2 - 2\Re(\lambda_n)z + |\lambda_n|^2\right),
\end{aligned}$$

so that $q(z)$ is the product of polynomials with real coefficients. Thus q is itself a polynomial with real coefficients, as was to be shown. $\square$

Problem 11

Suppose $p \in \mathcal{P}(\mathbb{F})$ with $p \neq 0$. Let $U = \{pq \mid q \in \mathcal{P}(\mathbb{F})\}$.

(a) Show that $\dim \mathcal{P}(\mathbb{F})/U = \deg p$

(b) Find a basis of $\mathcal{P}(\mathbb{F})/U$.

Proof. Suppose $\deg p = n$ for some $n \in \mathbb{Z}^+$.

(a) Consider the map

$$\begin{aligned}
T : \mathcal{P}(\mathbb{F}) &\to \mathcal{P}_{n-1}(\mathbb{F}) \\
f &\mapsto r(f),
\end{aligned}$$

where $r(f)$ is the unique remainder when f is divided by p. We will show that T is linear, $\operatorname{null} T = U$, and $\operatorname{range} T = \mathcal{P}_{n-1}(\mathbb{F})$, so that

$\mathcal{P}(\mathbb{F})/U \cong \mathcal{P}_{n-1}(\mathbb{F})$. Since $\mathcal{P}_{n-1}(\mathbb{F}) \cong \mathbb{F}^n$ and $\dim \mathbb{F}^n = n = \deg p$, this gives the desired result.

First we show T is a linear map. To see this, suppose $f, g \in \mathcal{P}(\mathbb{F})$. Then there exist unique $q_1, q_2 \in \mathcal{P}(\mathbb{F})$ such that $f = q_1 p + r(f)$ and $g = q_2 p + r(g)$. But then $f + g = (q_1 + q_2)p + r(f) + r(g)$, and hence $r(f+g) = r(f) + r(g)$. Thus

$$T(f+g) = r(f) + r(g) = T(f) + T(g),$$

and so T is additive. To see that T is also homogenous, suppose $\lambda \in \mathbb{F}$. Then $\lambda f = (\lambda q_1)p + \lambda r(f)$, and since both the quotient and remainder are unique, we must have $\lambda r(f) = r(\lambda f)$. Therefore

$$T(\lambda f) = \lambda r(f) = \lambda T f,$$

and so T is homogeneous. Thus T is a linear map, as claimed.

Next we show $\operatorname{null} T = U$. Suppose $f \in \operatorname{null} T$. Then $Tf = 0$, and hence $r(f) = 0$. That is, there exists $q_1 \in \mathcal{P}(\mathbb{F})$ such that $f = pq_1$, and thus $f \in U$. Conversely, if $g \in U$, then there exists $q_2 \in \mathcal{P}(\mathbb{F})$ such that $g = pq_2$. But then $r(g) = 0$, and hence $Tg = 0$ and $g \in \operatorname{null} T$.

Lastly we show $\operatorname{range} T = \mathcal{P}_{n-1}$. Of course $\operatorname{range} T \subseteq \mathcal{P}_{n-1}$. So suppose $r \in \mathcal{P}_{n-1}$. Then $r = 0p + r$ (where 0 denotes the zero polynomial), and hence $Tr = r$. Thus $\operatorname{range} T = \mathcal{P}_{n-1}(\mathbb{F})$.

(b) We claim $1 + U, x + U, \ldots, x^{n-1} + U$ is a basis of $\mathcal{P}(\mathbb{F})/U$. Notice none of these vectors is the zero vector since elements of U are of the form pq where $\deg p = n$, so when $q \neq 0$, we have $\deg(pq) \geq n$, and when $q = 0$, we have $pq = 0$. Since $1, x, \ldots, x^{n-1}$ all have degree $< n$, none can be in U. Clearly the list is linearly independent. Since it has the right length, it's indeed a basis. $\square$