4.5 Exercise Solutions

Solution 4.1.
Let $P(x) = ax^3 + bx^2 + cx + d$.

Given:

$$P(0) = d = 1$$

So, $d = 1$.

$$P(1) = a + b + c + d = 0$$

Substitute $d = 1$*:*

$$a + b + c + 1 = 0 \Rightarrow a + b + c = -1$$

$$P(-1) = -a + b - c + d = -2$$

Substitute $d = 1$*:*

$$-a + b - c + 1 = -2 \Rightarrow -a + b - c = -3$$

$$P(2) = 8a + 4b + 2c + d = 4$$

Substitute $d = 1$*:*

$$8a + 4b + 2c + 1 = 4 \Rightarrow 8a + 4b + 2c = 3$$

Now solve the system of equations:

From $a + b + c = -1$ *and* $-a + b - c = -3$*: Add these equations:*

$$2b = -4 \Rightarrow b = -2$$

Substitute $b = -2$ *into* $a + b + c = -1$*:*

$$a - 2 + c = -1 \Rightarrow a + c = 1$$

Substitute $b = -2$ *into* $8a + 4b + 2c = 3$*:*

$$8a - 8 + 2c = 3 \Rightarrow 8a + 2c = 11$$

Now solve $a + c = 1$ *and* $8a + 2c = 11$*:*

Multiply $a + c = 1$ *by 2:*

$$2a + 2c = 2$$

Subtract from $8a + 2c = 11$*:*

$$6a = 9 \Rightarrow a = \frac{3}{2}$$

Substitute $a = \frac{3}{2}$ *into* $a + c = 1$*:*

$$\frac{3}{2} + c = 1 \Rightarrow c = -\frac{1}{2}$$

So, $a = \frac{3}{2}$, $b = -2$, $c = -\frac{1}{2}$, $d = 1$.

Therefore, the polynomial $P(x)$ *is:*

$$P(x) = \frac{3}{2}x^3 - 2x^2 - \frac{1}{2}x + 1$$

Solution 4.2.

1. *For* $A = 3X^5 + 4X^2 + 1$ *and* $B = X^2 + 2X + 3$*:*

$$\begin{aligned} Q &= 3X^3, \\ R &= -6X^2 + 1. \end{aligned}$$

2. *For* $A = 3X^5 + 2X^4 - X^2 + 1$ *and* $B = X^3 + X + 2$*:*

$$\begin{aligned} Q &= 3X^2 - X, \\ R &= 2X^2 + X + 1. \end{aligned}$$

3. *For* $A = X^4 - X^3 + X - 2$ *and* $B = X^2 - 2X + 4$*:*

$$\begin{aligned} Q &= X^2, \\ R &= -X^3 + 3X - 10. \end{aligned}$$

Solution 4.3.

1. *Suppose $P \mid Q$ and $Q \mid R$. Then there exist polynomials $A(X), B(X), C(X) \in A[X]$ such that $Q = PA$ and $R = QB$. Substituting $Q = PA$ into $R = QB$, we get $R = P(AB)$, which implies $P \mid R$.*
2. *If $P \mid Q$ and $P \mid R$, then there exist polynomials $A(X), B(X) \in A[X]$ such that $Q = PA$ and $R = PB$. Therefore, $Q + R = PA + PB = P(A + B)$, which shows that $P \mid (Q + R)$.*
3. *Assume $P \mid Q$ and $Q \neq 0$. Then $Q = PA$ for some polynomial $A(X)$, implying* $\deg(Q) = \deg(PA) = \deg(P) + \deg(A)$. *Since* $\deg(Q) \geq \deg(P)$, *we conclude* $\deg(P) \leq \deg(Q)$.
4. *Given $P \mid Q$ and $R \mid S$, there exist polynomials $A(X), B(X), C(X), D(X) \in A[X]$ such that $Q = PA$ and $S = RC$. Therefore, $QS = (PA)(RC) = (PR)(AC)$, which means $PR \mid QS$.*
5. *If $P \mid Q$, then there exists a polynomial $A(X) \in A[X]$ such that $Q = PA$. Thus, $Q^n = (PA)^n = P^n A^n$, which shows $P^n \mid Q^n$ for all $n \geq 1$.*

Solution 4.4.

1. ***Part 1:***

   Claim: *If $P \mid Q$ and $Q \mid P$, then P and Q are associated.*

   Proof:

   If $P \mid Q$, then there exists $A \in A[X]$ such that $Q = P \cdot A$.

   If $Q \mid P$, then there exists $B \in B[X]$ such that $P = Q \cdot B$.

   Combining these, $Q = P{\cdot}A$ and substituting in $P = Q{\cdot}B$, we get $P = P{\cdot}A{\cdot}B$.

   Since $P \neq 0$, dividing by P gives $1 = A \cdot B$, implying A and B are units.

   Therefore, P and Q are associated.

2. ***Part 2:***

   Claim: *If P is associated to R and Q is associated to S, then $P \mid Q \iff R \mid S$.*

   Proof:

Assume $P = u \cdot R$ and $Q = v \cdot S$ for units $u, v \in A[X]$.

$P \mid Q$ implies $Q = P \cdot A$, so $Q = u \cdot R \cdot A$.

$R \mid S$ implies $S = R \cdot B$, so $Q = v \cdot S = v \cdot R \cdot B$.

Therefore, $P \mid Q \iff R \mid S$ because $u \cdot R \cdot A = v \cdot R \cdot B$ implies $u = v$ (since $R \neq 0$).

Solution 4.5.

1. *Let $P(X) = X^3 - X^2 - X - 2$ and $Q(X) = X^5 - 2X^4 + X^2 - X - 2$. Apply the Euclidean algorithm:*

$$Q(X) = P(X) \cdot X^2 + (-2X^4 + 3X^2 - 2),$$
$$P(X) = (-2X^4 + 3X^2 - 2) \cdot \left(-\frac{1}{2}X + \frac{3}{2}\right) + \left(\frac{5}{2}X^2 - \frac{3}{2}X - 2\right).$$

Continuing this process, we find:

$$\gcd(P(X), Q(X)) = \frac{5}{2}X^2 - \frac{3}{2}X - 2.$$

Therefore, the gcd of $X^3 - X^2 - X - 2$ and $X^5 - 2X^4 + X^2 - X - 2$ is $\frac{5}{2}X^2 - \frac{3}{2}X - 2$.

2. *Let $R(X) = X^4 + X^3 - 2X + 1$ and $S(X) = X^3 + X + 1$. Apply the Euclidean algorithm:*

$$R(X) = S(X) \cdot X + (X^2 - 2X),$$
$$S(X) = (X^2 - 2X) \cdot X + (X + 1),$$
$$X^2 - 2X = (X + 1) \cdot (X - 2).$$

Thus,

$$\gcd(R(X), S(X)) = X + 1.$$

Therefore, the gcd of $X^4 + X^3 - 2X + 1$ and $X^3 + X + 1$ is $X + 1$.

Solution 4.6.

1. *Reducible polynomials in $\mathbb{K}[X]$ have degree greater than or equal to 2. Let $p(X)$ be a polynomial in $\mathbb{K}[X]$. Consider the cases when the degree of $p(X)$ is less than 2:*

- *If the degree is* 0*, then* $p(X)$ *is a constant polynomial. Constant polynomials are not considered reducible in the sense of factorization into non-constant polynomials.*
- *If the degree is* 1*, then* $p(X)$ *is of the form* $aX + b$*, where* $a \neq 0$*. Polynomials of degree* 1 *cannot be factored into smaller degree polynomials in* $\mathbb{K}[X]$*; hence, they are irreducible.*

Therefore, polynomials that are reducible must have a degree greater than or equal to 2*.*

2. *All polynomials of degree* 1 *are irreducible. A polynomial of degree* 1 *is of the form* $p(X) = aX + b$*, where* $a \neq 0$*. Such polynomials cannot be factored into polynomials of smaller degree in* $\mathbb{K}[X]$*, and hence they are irreducible.*