Section 5.1, Problem 4. Show that, under congruence modulo $x^3 + 2x + 1$ in $\mathbb{Z}_3[x]$, that there are exactly 27 congruence classes.

By Corollary 5.5, there is exactly one congruence class for each possible remainder when a polynomial in $\mathbb{Z}_3[x]$ is divided by $x^3 + 2x + 1$. By the Division Algorithm, the possible remainders are 0 and all polynomials of degree 2 or less. Therefore, all polynomials of the form $ax^2 + bx + c$ where $a, b, c \in \mathbb{Z}_3$. Since there are three choices for $a, b$ and $c$, we have $3 \cdot 3 \cdot 3 = 27$ congruence classes in $\mathbb{Z}_3[x]$ modulo $x^3 + 2x + 1$.

Section 5.1, Problem 11. If $p(x)$ is not irreducible in $F[x]$ (and of positive degree), prove that there exists $f(x), g(x) \in F[x]$ such that $f(x) \not\equiv 0_F(\text{mod } p(x))$ and $g(x) \not\equiv 0_F(\text{mod } p(x))$ but $f(x)g(x) \equiv 0_F(\text{mod } p(x))$.

Proof. Since $p(x)$ is not irreducible and of positive degree, then by Theorem 4.10, $p(x) = f(x)g(x)$ for polynomials $f(x), g(x) \in F[x]$ of strictly lower degree than $p(x)$. Since $p(x) \not\equiv 0_F$, we have $f(x) \not\equiv 0_F, g(x) \not\equiv 0_F$ since $F[x]$ is an integral domain by Theorem 4.2. Hence, by Corollary 5.5, $f(x) \not\equiv 0_F(\text{mod } p(x))$ and $g(x) \not\equiv 0_F(\text{mod } p(x))$, but $f(x)g(x) = p(x) \equiv 0_F(\text{mod } p(x))$. Q.E.D.

Section 5.2, Problem 6. Determine the addition and multiplication of congruence classes in $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$.

As stated in the text, each congruence class of $R = \mathbb{Q}[x]/\langle x^2 - 2 \rangle$ is of the form $[ax + b]$ for some $a, b \in \mathbb{Q}$. Therefore, let $[ax + b], [cx + d] \in R$ where $a, b, c, d \in \mathbb{Q}$. Then

$$[ax + b] + [cx + d] = [(a + c)x + (b + d)]$$

and

$$[ax + b][cx + d] = [acx^2 + (ad + bc)x + bd] = [ac(2) + (ad + bc)x + bd] = [(ad + bc)x + (bd + 2ac)].$$

Section 5.2, Problem 14. In each part explain why $[f(x)]$ is a unit in $F[x]/\langle p(x) \rangle$ and find its inverse.

(a) $[f(x)] = [2x - 3] \in \mathbb{Q}[x]/\langle x^2 - 2 \rangle$.

Note that $(x^2 - 2, 2x - 3) = 1$, so by Theorem 5.9, $[f(x)]$ is a unit in $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$. Since

$$4(x^2 - 2) + (-2x - 3)(2x - 3) = 1$$

we get $[2x - 3]^{-1} = [-2x - 3]$.

(b) $[f(x)] = [x^2 + x + 1] \in \mathbb{Z}_3[x]/\langle x^2 + 1 \rangle$.  


Note that \((x^2 + x + 1, x^2 + x^2 + 1) = 1\), so by Theorem 5.9, \([f(x)]\) is a unit in \(\mathbb{Z}_3[x]/(x^2 + 1)\). Since

\[(x + 1)(x^2 + 1) + (2x)(x^2 + x + 1) = 1\]

we get \([x^2 + x + 1]^{-1} = [2x]\).

\[(c)\] \([f(x)] = [x^2 + x + 1] \in \mathbb{Z}_2[x]/(x^3 + x + 1)\).

Note that \((x^3 + x + 1, x^2 + x + 1) = 1\), so by Theorem 5.9, \([f(x)]\) is a unit in \(\mathbb{Z}_2[x]/(x^3 + x + 1)\). Since

\[(x + 1)(x^3 + x + 1) + x^2(x^2 + x + 1) = 1\]

we get \([x^2 + x + 1]^{-1} = [x^2]\).

Section 5.3, Problem 1. Determine whether the given congruence-class ring is a field.

\[(a)\] \(\mathbb{Z}_3[x]/(x^3 + 2x^2 + x + 1)\).

By Theorem 5.10, we just need to determine whether \(f(x) = x^3 + 2x^2 + x + 1\) is irreducible or not. By Corollary 4.18, we just need to determine if \(f(x)\) has any roots in \(\mathbb{Z}_3\). But \(f(0) = 1, f(1) = 5 = 2,\) and \(f(2) = 19 = 1\), so \(f(x)\) is irreducible and \(\mathbb{Z}_3[x]/(x^3 + 2x^2 + x + 1)\) is a field.

\[(b)\] \(\mathbb{Z}_5[x]/(2x^3 - 4x^2 + 2x + 1)\).

By Theorem 5.10, we just need to determine whether \(f(x) = 2x^3 - 4x^2 + 2x + 1\) is irreducible or not. By Corollary 4.18, we just need to determine if \(f(x)\) has any roots in \(\mathbb{Z}_5\). But \(f(0) = 1, f(1) = 1,\) but \(f(2) = 5 = 0\). Since \(f(x)\) has a root of \(2, (x - 2) = x + 3\) is a factor of \(f(x)\) and hence \(\mathbb{Z}_5[x]/(2x^3 - 4x^2 + 2x + 1)\) is NOT a field.

\[(a)\] \(\mathbb{Z}_2[x]/(x^4 + x^2 + 1)\).

By Theorem 5.10, we just need to determine whether \(f(x) = x^4 + x^2 + 1\) is irreducible or not. But \(f(x) = (x^4 + x^2 + 1) = (x^2 + x + 1)^2\), so \(f(x)\) is reducible. Therefore, \(\mathbb{Z}_2[x]/(x^4 + x^2 + 1)\) is NOT a field.