Solution Outlines for Chapter 16

 # 1: Let $f(x) = 4x^3 + 2x^2 + x + 3$ and $g(x) = 3x^4 + 3x^3 + 3x^2 + x + 4$, where $f(x), g(x) \in \mathbb{Z}_5[x]$. Compute $f(x) + g(x)$ and $f(x) \cdot g(x)$.

$f(x) + g(x) = 3x^4 + (4+3)x^3 + (2+3)x^2 + (1+1)x + (3+4) = 3x^4 + 2x^3 + x^2 + 2x + 2$

 # 2: In $\mathbb{Z}_3[x]$, show that the distinct polynomials $x^4 + x$ and $x^2 + x$ determine the same function from $\mathbb{Z}_3$ to $\mathbb{Z}_3$.

Let $f(x) = x^4 + x$ and $g(x) = x^2 + x$. Observe: $f(0) = 0 = g(0)$, $f(1) = 2 = g(1)$, and $f(2) = 2^4 + 2 = 18 = 0 = 6 = 2^2 + 2 = g(2)$.

 # 4: If R is a commutative ring, show that the characteristic of $R[x]$ is the same as the characteristic of R.

Let R be a commutative ring with characteristic k. Then $kr = 0$ for all $r \in R$. Now, let $f(x) \in R[x]$. Then $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ for some $a_i \in R$, and some $n \in \mathbb{Z}_{>0}$. Then $kf(x) = (ka_n)x^n + (ka_{n-1})x^{n-1} + \cdots + (ka_1)x + ka_0 = 0 + 0 + \cdots + 0 = 0$. Hence the characteristic of $R[x]$ is at most k. However, since for all $r \in R$, $r \in R[x]$, the characteristic of $R[x]$ must be at least k. Thus the characteristic is exactly k.

 # 6: List all the polynomials of degree 2 in $\mathbb{Z}_2[x]$. Which of these are equal as functions from $\mathbb{Z}_2$ to $\mathbb{Z}_2$?

If $f(x)$ is to have degree 2 in $\mathbb{Z}_2[x]$ then its leading term must be x^2. The linear and constant terms can have coefficient 0 or 1, so there are 4 total options. The options are x^2, $x^2 + 1$, $x^2 + x$, and $x^2 + x + 1$.

Now, to determine which are equal as functions, I simply need to observe the behavior of each polynomial on the elements of $\mathbb{Z}_2$. If they send the elements to the same place, then they are equal as functions. For x^2: $0 \mapsto 0$, $1 \mapsto 1$. For $x^2 + 1$: $0 \mapsto 1$, $1 \mapsto 0$. For $x^2 + x$: $0 \mapsto 0$, $1 \mapsto 0$. For $x^2 + x + 1$: $0 \mapsto 1$, $1 \mapsto 1$. Since none of these send both 0 and 1 to the same place, they are all distinct as functions.

 # 10: Let R be a commutative ring. Show that $R[x]$ has a subring isomorphic to R.

Let R be a commutative ring and consider $R[x]$. Define $\phi : R \to R[x]$ by $r \mapsto r$. Clearly ϕ is one-to-one and a homomorphism. Now, $\phi(R)$ is a subring of $R[x]$ since it is the image of a homomorphism. Then $\phi(R)$ is a subring of $R[x]$ isomorphic to R.

 # 11: If $\phi : R \to S$ is a ring homomorphism, define $\bar{\phi} : R[x] \to S[x]$ by $(a_n x^n + \cdots + a_1 x + a_0) \to \phi(a_n)x^n + \cdots + \phi(a_0)$. Show that $\bar{\phi}$ is a ring homomorphism.

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots b_1 x + b_0$ with $f(x), g(x) \in R[x]$. Let $s = max\{n, m\}$. Now, $\bar{\phi}(f(x) + g(x)) = \bar{\phi}((a_s + b_s)x^s + (a_{s-1} + b_{s-1})x^{s-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0)) = \phi(a_s + b_s)x^s + \cdots + \phi(a_1 + b_1)x + \phi(a_0 + b_0)$ where a_i and b_i are in R. But ϕ is a ring homomorphism from R to S so (i) it splits over addition and (ii) it yields coefficients in S. So $\bar{\phi}(f(x) + g(x)) = (\phi(a_n)x^n + \cdots + \phi(a_1)x + \phi(a_0) + (\phi(b_m)x^m + \cdots + \phi(b_1)x + \phi(b_0)) = \bar{\phi}(f(x)) + \bar{\phi}(g(x))$. Similarly, you can show that $\bar{\phi}$ preserves multiplication. Hence it is a ring homomorphism.

 # 15: Show that the polynomial $2x + 1$ in $\mathbb{Z}_4[x]$ has a multiplicative inverse in $\mathbb{Z}_4[x]$.

Observe that $(2x + 1)(2x + 1) = 4x^2 + 4x + 1 = 1$ so $2x + 1$ is its own inverse.

 # 16: Are there any nonconstant polynomials in $\mathbb{Z}[x]$ that have multiplicative inverses? Explain your answers.

No. Note, we argued this intuitively. Here's a more formal argument. Suppose that $f(x) = \sum_{i=0}^{n} a_i x^i$ has a multiplicative inverse $g(x) = \sum_{i=0}^{m} b_i x^i$. Then $f(x)g(x) = \sum_{i=0}^{n+m} c_i x^i = 1$. This implies that $c_0 = 1$ and $c_k = 0$ for all $k \neq 0$. In particular, $c_1 = a_0 b_1 + a_1 b_0 = 0$. But $a_0 = b_0^{-1}$ from $c_0 = 1$. So $c_1 = b_0^{-1} b_1 + a_1 b_0 = 0$ This implies that $b_1 = 0 = a_1$. But induction, it is clear that $a_i = b_i = 0$ for all $i \neq 0$. Hence, $f(x)$ and $g(x)$ are constant, which is a contradiction.

 # 17: Let p be a prime. Are there any non constant polynomials in $\mathbb{Z}_p[x]$ that have multiplicative inverses? Explain your answer.

No, there are not any. Consider $f(x)g(x) = (a_n x^n + \cdots a_1 x + a_0)(b_m x^m + \cdots + b_1 x + b_0) = a_n b^m x^{n+m} + \cdots + a_0 b_0$ and $a_n b_m \neq 0$. For this to have a multiplicative inverse, each non-constant term in $f(x)g(x)$ must be 0, but $a_n b_m$ non-zero shows this is not so.

 # 19: (Degree Rule) Let D be an integral domain and $f(x), g(x) \in D[x]$. Prove that deg $(f(x)g(x))$ = deg $f(x)$ + deg $g(x)$. Show, by example, that for a commutative ring R it is possible that deg $f(x)g(x) <$ deg $f(x)$ + deg $g(x)$, where $f(x)$ and $g(x)$ are nonzero elements in $R[x]$.

Let D be an integral domain and $f(x), g(x) \in D[x]$. Suppose that $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$ so that $deg(f(x)) = n$ and $deg(g(x)) = m$. We know that $f(x)g(x) = \sum_{i=0}^{n+m} c_{n+m} x^{n+m}$ where $c_{n+m} = a_0 b^{n+m} + a_1 b^{n+m-1} + \cdots + a_{n+m-1} b^1 + a_{n+m} b^0$. Since the a_i and b_j are in an integral domain, $a_i b_j \neq 0$ when $a_i \neq 0$ and $b_j \neq 0$. In particular, we know that a_n and b_m are non-zero so $a_n b_m \neq 0$. Now, all other terms in the sum of c_{n+m} are zero because either a_i has $i > n$ or b_j has $j > m$. Thus $c_{n+m} = a_n b_m$. Thus, c_{n+m} is not zero and the $deg(f(x)g(x)) = n + m$.

 # 20: Prove that the ideal $< x >$ in $\mathbb{Q}[x]$ is maximal.

First, let's look at $\mathbb{Q}[x]/ < x >$. This quotient ring contains cosets that look like $a+ < x >$ where $a \in \mathbb{Q}$. Thus, using the map $\mathbb{Q}[x]/ < x > \to \mathbb{Q}$ defined by $a+ < x >= a$ is an isomorphism. Thus $\mathbb{Q}[x]/ < x > \approx \mathbb{Q}$. Now, $\mathbb{Q}$ is a field so $< x >$ is maximal.

 # 28: Let $f(x) \in \mathbb{R}[x]$. Suppose that $f(a) = 0$ but $f'(a) \neq 0$ where $f'(x)$ is the derivative of $f(x)$. Show that a is a zero of $f(x)$ of multiplicity 1.

Clearly, $f(x)$ has a as a zero with multiplicity of at least 1. Suppose that it has multiplicity $k > 1$. Then $f(x) = (x-a)^k g(x)$ for some $g(x)$. So $f'(x) = k(x-a)^{k-1}g(x) + (x-a)^k g'(x) = (x-a)^{k-1}(kg(x) + (x-a)g'(x))$. Now, $k > 1$ implies that $k - 1 \geq 1$. So $f'(a) = 0$, which is a contradiction.

 # 50: Let R be a ring and x be an indeterminate. Prove that the rings $R[x]$ and $R[x^2]$ are ring-isomorphic.

Let R be a ring and x be an indeterminate. Consider the rings $R[x]$ and $R[x^2]$. To show that they are isomorphic, let $\phi : R[x] \to R[x^2]$ be defined by $f(x) \mapsto f(x^2)$. We see that addition is preserved since $\phi(f(x) + g(x)) = \phi((f+g)(x)) = (f+g)(x^2) = f(x^2) + g(x^2) = \phi(f(x)) + \phi(g(x))$. Similarly, it is clear that multiplication is preserved. This is one-to-one since $ker\phi = \{f(x) | f(x^2) = 0\} = \{0\}$, and onto is also straightforward to show.

 # 56: For any field F recall that $F(x)$ denotes the field of quotients of the ring $F[x]$. Prove that there is no element in $F(x)$ whose square is x.

Suppose that there is an element in $F(x)$ whose square is x. Then $\left(\frac{f(x)}{g(x)}\right)^2 = x$. WLOG, assume that $f(x)$ and $g(x)$ have no common factors (so that the quotient is already in reduced form). Then $\left(\frac{f(x)}{g(x)}\right)^2 = \frac{(f(x))^2}{(g(x))^2} = x$. So $(f(x))^2 = x(g(x))^2$. Hence, $(f(0))^2 = 0$ so $f(0) = 0$. This means that $x | f(x)$. So $f(x) = xh(x)$ for some $h(x)$. Plugging this in, we have that $(xh(x))^2 = x(g(x))^2$ so $x(h(x))^2 = (g(x))^2$. Using the same argument as before, $g(0) = 0$ and $x | g(x)$. Therefore $f(x)$ and $g(x)$ have x as a common factor, which is a contradiction.