22.4

$$\begin{aligned} f(x)+g(x) &= (0+3)x^4+(2+0)x^3+(4+0)x^2+(3+2)x+(2+4) \\ &= 3x^4+2x^3+4x^2+0x+1 \\ &= 3x^4+2x^3+4x^2+1 \end{aligned}$$

and

$$\begin{aligned} f(x)g(x) &= (2\cdot 4)+(2\cdot 2+3\cdot 4)x+(2\cdot 0+3\cdot 2+4\cdot 4)x^2+\dots \\ &= 3+x+2x^2+x^3+4x^5+2x^6+x^7 \end{aligned}$$

22.6

There are 5 choices for each coefficient meaning there are $5^3 = 125$ polynomials of deg ≤ 2 in $\mathbb{Z}_5[x]$.

22.10

$$\begin{aligned} \phi\big[(x^3+2)(4x^2+3)(x^7+3x^2+1)\big] &\equiv (5^3+2)(4(5)^2+3)(5^7+3(5)^2+1) \\ &\equiv (5\cdot 4+2)(4^2+3)(5\cdot(125)^2+3\cdot 4+1) \\ &\equiv (6+2)(2+3)(5\cdot(6)^2+5+1) \\ &\equiv (1)(5)(5+5+1) \\ &\equiv (1)(5)(4) \\ &\equiv 6 \pmod 7 \end{aligned}$$

22.16

$$3^231 \equiv 3^3\cdot\left(3^4\right)^{57} \equiv 2\cdot 1^{57} \equiv 2 \pmod 5.$$

$$3\cdot 3^{117} \equiv 3^2\cdot\left(3^4\right)^{54} \equiv 3^2\cdot 1^{54} \equiv 4 \pmod 5.$$

$$2\cdot 3^{53} \equiv 2\cdot 3\cdot\left(3^4\right)^{13} \equiv 2\cdot 3\cdot 1^{13} \equiv 1 \pmod 5.$$

Therefore

$$\phi_3\left(x^{231}+3x^{117}-2x^{53}+1\right) = 2+4-1+1 = 1.$$

22.22

$2x+1$ is a unit since

$$(2x+1)^2 = 4x^2+4x+1 = 1.$$

22.24

Proof. Take $f(x) = a_n x^n + \ldots + a_0$ and $g(x) = b_n x^n + \ldots + b_0$ in $D[x]$ with $a_0, b_0 \neq 0$. Since the product will have a constant term of $a_0 b_0$, and D is an integral domain, $a_0 b_0 \neq 0$ and therefore there are no zero divisors. Since D is already a commutative ring with unity, so is $D[x]$ and hence $D[x]$ is an integral domain. ■

22.25

Part A

The unity 1 is degree zero, and so any units have to be polynomials whose product is of degree 0. However, this means that any polynomial of degree ≥ 1 cannot be a unit since its product with another polynomial will have a degree ≥ 1 (if the other isn't 0, but that will never give unity). Therefore the only units are going to be the constant polynomials which are the units of D.

Part B

The units of $\mathbb{Z}$ are -1 and 1 and since $\mathbb{Z}$ is an integral domain, the units of $\mathbb{Z}[x]$ are -1 and 1 as well.

Part C

Every element of $\mathbb{Z}_7$ is a unit and since $\mathbb{Z}$ is an integral domain, the units of $\mathbb{Z}[x]$ are $1, 2, 3, 4, 5$ and 6.

22.27

Part A

Proof. Let $f(x) = \sum_{i=0}^{\infty} a_i x^i$ and $g(x) = \sum_{j=0}^{\infty} b_j x^j$ be polynomials in $F[x]$. Then

$$\begin{aligned}
D(f(x) + g(x)) &= D\left(\sum_{i=0}^{\infty} (a_i + b_i) x^i\right) \\
&= \sum_{i=1}^{\infty} i \cdot (a_i + b_i) x^{i-1} \\
&= \sum_{i=1}^{\infty} i \cdot a_i x^{i-1} + \sum_{j=1}^{\infty} j \cdot b_j x^{j-1} \\
&= D\left(\sum_{i=0}^{\infty} a_i x^i\right) + D\left(\sum_{j=0}^{\infty} b_j x^j\right) \\
&= D(f(x)) + D(g(x))
\end{aligned}$$

Therefore D is an additive group homomorphism into itself. It is not necessarily a ring homomorphism however. Consider in $\mathbb{R}[x]$ the polynomials x^2 and x^3. Then

$$D(x^2 \cdot x^3) = D(x^5) = 5x^4 \neq 6x^3 = D(x^2)D(x^3).$$

Since $\mathbb{R}$ is a field of characteristic 0, this is a counter example to the general statement.

■

Part B

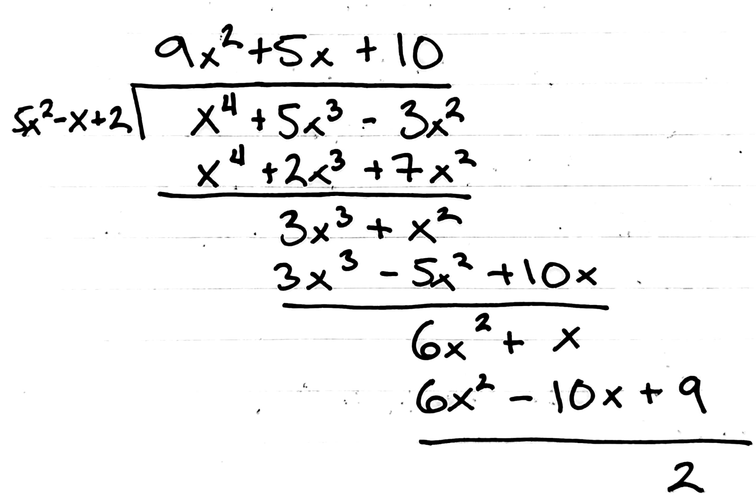
The kernel of D is F itself since F is characteristic 0 meaning the only time an element in $F[x]$ is sent to 0 is when its a constant.

Part C

The image of D is still $F[x]$. For any term in a polynomial $f(x)$ in $F[x]$ such as $a_i x^i$, the term $\frac{a_i}{i+1}x^{i+1}$ will be mapped to it under D (a.k.a polynomials have anti derivatives).

23.4

Doing the long division gives



Therefore $q(x) = 9x^2 + 5x + 10$ and $r(x) = 2$.

23.10

Note that -1 is a zero, meaning the linear factor $x + 1$ is in its factorization. The division algorithm using $x+1$ as the divisor gives x^2+x+1 which by inspection factors into $(x-2)(x-4)$. Therefore the factorization is

$$(x + 1)(x - 2)(x - 4).$$

23.14

Using $p = 2$ it follows that the polynomial satisfies the Einstein criterion meaning it is irreducible over $\mathbb{Q}$. The quadratic formula gives the zeros

$$\frac{-8 \pm \sqrt{64+8}}{2} = -4 \pm 6\sqrt{2}$$

which are both real and therefore it is not irreducible over $\mathbb{R}$. The fundamental theorem of algebra implies every polynomial in $\mathbb{C}$ is not irreducible.

23.16

If f factors in $\mathbb{Q}$, then it has a zero in $\mathbb{Q}$. Since $a_0 = -8 \neq 0$, it must therefore have a zero in $\mathbb{Z}$ that divides -8. This means the possible candidates are $x = \pm 1, \pm 2, \pm 4, \pm 8$. However, none of the candidates are zero's, meaning there isn't a zero in $\mathbb{Z}$ and hence it must be irreducible in $\mathbb{Q}$.

23.20

Choosing $p = 3$ gives

$$1x^{10} + 0x^3 + 0x - 0.$$

Therefore it satisfies the Einstein criterion.

23.30

An irreducible polynomial will need to have a non zero constant term, otherwise 0 would be a zero of the polynomial. Since $f(x)$ is zero iff $2f(x)$ is zero, this means that the set of irreducible polynomials with leading coefficient 1 give rise to the other irreducible polynomials, their doubles. The only cases (coefficients are expressed as ordered tuples for space) of this then are

$$\begin{gathered}
(1,0,2,1),(2,0,1,2)\\
(1,0,2,2),(2,0,1,1)\\
(1,1,0,2),(2,2,0,1)\\
(1,2,0,1),(2,1,0,2)\\
(1,1,1,2),(2,2,2,1)\\
(1,1,2,1),(2,2,1,2)\\
(1,2,1,1),(2,1,2,2)\\
(1,2,2,2),(2,1,1,1)
\end{gathered}$$

Therefore there are 16 irreducible cubics in $\mathbb{Z}_3[x]$

23.34

Proof. Let p be prime and consider $x^p + a$ where $a \in \mathbb{Z}_p$. Since $-a$ is less than p and not divided by p, then by Fermat's Little Theorem,

$$(-a)^{p-1} \equiv 1 \pmod{p} \implies (-a)^p + a \equiv 0 \pmod{p}.$$

Therefore $x = -a$ is a zero of $x^p + a$ meaning it is not irreducible. ■

23.36

Proof. By the division algorithm,

$$f(x) = g(x)(x - \alpha) + c$$

for some constant $c \in F$. Applying the evaluation homomorphism at α gives

$$\phi_\alpha(f(x)) = g(\alpha)(\alpha - \alpha) + c = g(\alpha) \cdot 0 + c = c.$$

Therefore the remainder is $f(\alpha)$. ■

23.37

Part A

Proof. Note that $\overline{\sigma_m}$ is linear and multiplicative over elements of $\mathbb{Z}$. Let $f(x) = \sum_{i=0}^{\infty} a_i x^i$ and $g(x) = \sum_{j=0}^{\infty} b_j x^j$ be elements of $\mathbb{Z}[x]$. Checking if $\overline{\sigma_m}$ is an additive group homomorphism gives

$$\begin{aligned}
\overline{\sigma_m}(f(x) + g(x)) &= \overline{\sigma_m}\left(\sum_{i=0}^{\infty} a_i x^i + \sum_{j=0}^{\infty} b_j x^j\right) \\
&= \overline{\sigma_m}\left(\sum_{i=0}^{\infty} (a_i + b_i) x^i\right) \\
&= \sum_{i=0}^{\infty} \overline{\sigma_m}(a_i + b_i) x^i \\
&= \sum_{i=0}^{\infty} \overline{\sigma_m}(a_i) x^i + \overline{\sigma_m}(b_i) x^i \\
&= \overline{\sigma_m}(f(x)) + \overline{\sigma_m}(g(x))
\end{aligned}$$

Checking if $\overline{\sigma_m}$ is multiplicative gives

$$\begin{aligned}
\overline{\sigma_m}(f(x)g(x)) &= \overline{\sigma_m}\left(\sum_{i=0}^{\infty}\left(\sum_{j=0}^{i} a_j b_{i-j}\right)x^i\right) \\
&= \sum_{i=0}^{\infty}\left(\sum_{j=0}^{i} \overline{\sigma_m}(a_j b_{i-j})\right)x^i \\
&= \sum_{i=0}^{\infty}\left(\sum_{j=0}^{i} \overline{\sigma_m}(a_j)\overline{\sigma_m}(b_{i-j})\right)x^i \\
&= \overline{\sigma_m}(f(x))\overline{\sigma_m}(g(x)).
\end{aligned}$$

Therefore $\overline{\sigma_m}$ is a ring homomorphism from $\mathbb{Z}[x]$ to $\mathbb{Z}_m[x]$ ■

Part B

Proof. Assume towards contradiction that that some $f(x)$ factors into two polynomials of degree $r, s < \deg f$ and $\overline{\sigma_m}(f(x))$ has degree n but is irreducible. Since $\overline{\sigma_m}$ is a ring homomorphism and $f(x) = g(x)h(x)$ with $\deg h, \deg g < n$, it follows

$$\overline{\sigma_m}(f(x)) = \overline{\sigma_m}(g(x)h(x)) = \overline{\sigma_m}(g(x))\overline{\sigma_m}(h(x)).$$

However, this gives a factorization of $\overline{\sigma_m}(f(x))$ into polynomials with degree smaller than n, a contradiction. ■

Part C

Taking $m = 5$ gives $\overline{\sigma_5}(x^3 + 17x + 36) = x^3 + 2x + 1$. Inspection shows that $x = 0, 1, -1, 2, -2$ aren't zeroes and therefore the polynomial is irreducible in $\mathbb{Z}[x]$ by the previous part. Since it is irreducible in $\mathbb{Z}[x]$, it is irreducible in $\mathbb{Q}[x]$.