MODEL ANSWERS TO THE SEVENTH HOMEWORK

1. §22: 4. We have

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

and

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

6. A general polynomial of degree at most 2 looks like $ax^2 + bx + c \in \mathbb{Z}_5[x]$. There are five possibilities for a, five possibilities for b and five possibilities for c. Therefore the total number of polynomials of degree at most 2 is $5^3 = 125$.

14. Probably the easiest way is simply trial and error:

$$\begin{aligned} \phi_0(x^5 + 3x^3 + x^2 + 2x) &= 0^5 + 3 \cdot 0^3 + 0^2 + 2 \cdot 0 = 0 \\ \phi_1(x^5 + 3x^3 + x^2 + 2x) &= 1^5 + 3 \cdot 1^3 + 1^2 + 2 \cdot 1 = 2 \\ \phi_2(x^5 + 3x^3 + x^2 + 2x) &= 2^5 + 3 \cdot 2^3 + 2^2 + 2 \cdot 2 = 2 \\ \phi_3(x^5 + 3x^3 + x^2 + 2x) &= 3^5 + 3 \cdot 3^3 + 3^2 + 2 \cdot 3 = 4 \\ \phi_4(x^5 + 3x^3 + x^2 + 2x) &= 4^5 + 3 \cdot 4^3 + 4^2 + 2 \cdot 4 = 0. \end{aligned}$$

Therefore 0 and 4 are the zeroes of $x^5 + 3x^3 + x^2 + 2x$.

One can also attack this problem by using a little bit of theory. For a start notice that when we evaluate the polynomial $x^5 - x = x^5 + 4x$ at any point of $\mathbb{Z}_5$ then we get zero, by Fermat. So we might as well evaluate

$$x^5 + 3x^3 + x^2 + 2x - (x^5 - x) = 3x^3 + x^2 + 3x$$

as we will get the same values. On the other hand, we can pull out a factor x from this polynomial to get

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

So if α is a zero of $x^5 + 3x^3 + x^2 + 2x$ either $\alpha = 0$ or $\alpha \neq 0$ is a zero of $x^2 + 2x + 1$. But $x^2 + 2x + 1 = (x + 1)^2$ and visibly this is zero if and only if $x + 1 = 0$, that is, $x = 4$.

20.

$$\begin{aligned} f(x,y) &= (3x^3+2x)y^3+(x^2-6x+1)y^2+(x^4-2x)y+(x^4-3x^2+2) \\ &= 3x^3y^3+2xy^3+x^2y^2-6xy^2+y^2+x^4y-2xy+x^4-3x^2+2 \\ &= (y+1)x^4+(3y^3)x^3+(y^2-3)x^2+(2y^3-6y^2-2y)x+(y^2+2). \end{aligned}$$

23. T: (a), (b), (c), (d), (g), (h), (i),
F: (e), (f), (j).
27. (a) Suppose that

$$f(x) = \sum a_i x^i \qquad \text{and} \qquad g(x) = \sum b_i x^i.$$

Then

$$\begin{aligned} D(f(x)+g(x)) &= D\left(\sum (a_i+b_i)x^i\right) \\ &= \sum i \cdot (a_i+b_i)x^{i-1} \\ &= \sum i \cdot a_i x^{i-1} + \sum i \cdot b_i x^{i-1} \\ &= D(f) + D(g). \end{aligned}$$

Therefore D is a group homomorphism.
It is not a ring homomorphism. In fact D satisfies Leibniz's rule. If $f(x) = g(x) = x$ then

$$\begin{aligned} D(f(x)g(x)) &= D(x^2) \\ &= 2 \cdot x \\ &\neq 2 \cdot 1 \\ &= D(x) + D(x). \end{aligned}$$

(b) The kernel of D is all constant polynomials, all polynomials of degree zero, plus zero.
(c) D is onto, so the image of $F[x]$ is $F[x]$. Suppose that

$$g(x) = \sum a_i x^i \in F[x].$$

As the characteristic of F is zero, $i \cdot 1 \neq 0$ and if we put

$$f(x) = \sum \frac{a_i}{i \cdot 1} x^i \in F[x]$$

then

$$D(f(x)) = \sum i \cdot 1 \frac{a_i}{i \cdot 1} x^i = \sum a_i x^i = g(x).$$

§23: 2. We have $q(x) = 5x^4 + 5x^2 + 6x$ and $r(x) = x + 2$ so that

$$(x^6+3x^5+4x^2-3x+2) = (5x^4+5x^2+6x)(3x^2+2x-3)+(x+2).$$

10. To find the linear factors of $x^3+2x^2+2x+1 \in \mathbb{Z}_7[x]$, the first thing to do is find the zeroes. One way to proceed is brute computation.

$$\begin{aligned}
\phi_0(x^3+2x^2+2x+1) &= 0^3+2\cdot 0^2+2\cdot 0+1 = 1\\
\phi_1(x^3+2x^2+2x+1) &= 1^3+2\cdot 1^2+2\cdot 1+1 = 6\\
\phi_2(x^3+2x^2+2x+1) &= 2^3+2\cdot 2^2+2\cdot 2+1 = 0\\
\phi_3(x^3+2x^2+2x+1) &= 3^3+3\cdot 3^2+2\cdot 3+1 = 3\\
\phi_4(x^3+2x^2+2x+1) &= 4^3+2\cdot 4^2+2\cdot 4+1 = 0\\
\phi_5(x^3+2x^2+2x+1) &= 5^3+2\cdot 5^2+2\cdot 5+1 = 4\\
\phi_6(x^3+2x^2+2x+1) &= 6^3+2\cdot 6^2+2\cdot 6+1 = 0.
\end{aligned}$$

Thus

$$x^3+2x^2+2x+1 = (x-2)(x-4)(x-6) = (x+5)(x+3)(x+1) \in \mathbb{Z}_7[x].$$

Or we could observe that since 2 is a zero, we must be able to divide x^3+2x^2+2x+1 by $x-2 = x+5$. If we run the division algorithm we get

$$x^3+2x^2+2x+1 = (x+5)(x^2+4x+3).$$

We now look for zeroes of x^2+4x+3. We know that 0 and 1 are not zeroes.

$$\begin{aligned}
\phi_2(x^2+4x+3) &= 2^2+4\cdot 2+3 = 1\\
\phi_3(x^2+4x+3) &= 3^2+4\cdot 3+3 = 3\\
\phi_4(x^2+4x+3) &= 4^2+4\cdot 4+3 = 0.
\end{aligned}$$

Thus 4 is a zero of x^2+4x+3. It follows that we can divide x^2+4x+3 by $x-4 = x+3$. If we run the division algorithm we get

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

Thus

$$x^3+2x^2+2x+1 = (x+5)(x+3)(x+1) \in \mathbb{Z}_7[x],$$

as before.

14. There are many ways to show that $f(x) = x^2+8x-2$ is irreducible over $\mathbb{Q}$. First of all by Gauss, it suffices to show that it is irreducible over $\mathbb{Z}$.

If it is not irreducible it factors as

$$x^2+8x-2 = (ax+b)(cxd+d) \in \mathbb{Z}[x].$$

As the coefficient of x^2 is 1, we have $ac = 1$, so that $a = c = 1$ or $a = c = -1$. We may assume that $a = c = 1$. Thus

$$x^2+8x-2 = (x+b)(xd+d) \in \mathbb{Z}[x].$$

The product of b and d is two, $bd = 2$. Thus $b = \pm 1$ and $d = \pm 2$, up to switching b and d. The sum of b and d is 8, $b + d = 8$. On the other hand, the maximum of the sum of ± 1 and ± 2 is $1 + 2 = 3$, nowhere near 8. Thus $x^2 + 8x - 2$ is irreducible over $\mathbb{Z}$ and so it is irreducible over $\mathbb{Q}$.
We could also apply Eisenstein with $p = 2$.
The discriminant of $x^2 + 8x - 2$ is $8^2 - 4 \cdot -2 = 8 \cdot 9 = 72 > 0$. Thus $x^2 + 8x - 2$ has two real roots, α_1 and α_2, by the quadratic formula. Thus

$$x^2 + 8x - 2 = (x - \alpha_1)(x - \alpha_2) \in \mathbb{R}[x],$$

is reducible over $\mathbb{R}$. In particular it is certainly reducible over $\mathbb{C}$.
21. Yes. Take $p = 5$. Then p divides -25, 10 and 30 but p^2 does not divide -30.
25. T: (a), (b), (c), (e), (f), (g), (h), (i),
F: (d), (j) [depending on whether you allow the polynomial to be zero].
28. A polynomial of degree 3 is irreducible if and only if it has no zeroes. So we just want to list the polynomials of degree 3 with no zeroes. The general polynomial of degree three looks like

$$ax^3 + bx^2 + cx + d \in \mathbb{Z}_2[x].$$

Since this has degree 3, $a \neq 0$ and so we may assume that $a = 1$, so that we have a polynomial of the form

$$x^3 + bx^2 + cx + d \in \mathbb{Z}_2[x].$$

$\alpha = 0$ is a zero if and only if $d = 0$. So we may assume that $d = 1$ and we have a polynomial of the form

$$x^3 + bx^2 + cx + 1 \in \mathbb{Z}_2[x].$$

$\alpha = 1$ is a zero if and only if $1 + b + c + 1 = 0$ so that $b + c = 0$. This happens if $b = c = 0$ or $b = c = 1$. So $\alpha = 1$ is not a zero if $b = 1$, $c = 0$ or $b = 0$, $c = 1$. Thus the irreducible polynomials in $\mathbb{Z}_2[x]$ of degree 3 are

$$x^3 + x^2 + 1 \qquad \text{and} \qquad x^3 + x + 1.$$

3. **Challenge Problems** §23: 37. (a) Let

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum a_i x^i \\ g(x) &= b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 = \sum b_i x^i, \end{aligned}$$

be two polynomials in $\mathbb{Z}[x]$.

Then

$$\begin{aligned}
\overline{\sigma}_m(f(x)+g(x)) &= \overline{\sigma}_m(\sum_i a_i x^i + \sum_i b_i x^i) \\
&= \overline{\sigma}_m(\sum_i (a_i + b_i) x^i) \\
&= \sum_i \sigma_m(a_i + b_i) x^i \\
&= \sum_i (\sigma_m(a_i) + \sigma_m(b_i)) x^i \\
&= \sum_i \sigma_m(a_i) x^i + \sum_i \sigma_m(b_i) x^i \\
&= \overline{\sigma}_m(\sum_i a_i x^i) + \overline{\sigma}_m(\sum_i b_i x^i) \\
&= \overline{\sigma}_m(f(x)) + \overline{\sigma}_m(g(x)).
\end{aligned}$$

Thus $\overline{\sigma}_m$ is a group homomorphism.
We now check it is a ring homomorphism.

$$\begin{aligned}
\overline{\sigma}_m(f(x)g(x)) &= \overline{\sigma}_m((\sum_i a_i x^i)(\sum_i b_i x^i)) \\
&= \overline{\sigma}_m(\sum_i (\sum_j a_j b_{i-j}) x^i) \\
&= \sum_i \sigma_m(\sum_j a_j b_{i-j}) x^i \\
&= \sum_i (\sum_j \sigma_m(a_i)\sigma_m(b_{i-j})) x^i \\
&= (\sum_i \sigma_m(a_i) x^i)(\sum_i \sigma_m(b_i) x^i) \\
&= \overline{\sigma}_m(\sum_i a_i x^i)\overline{\sigma}_m(\sum_i b_i x^i) \\
&= \overline{\sigma}_m(f(x))\overline{\sigma}_m(g(x)).
\end{aligned}$$

Therefore $\overline{\sigma}_m$ is a ring homomorphism.
(b) Suppose not, suppose that $f(x)$ is reducible. Then we may find $g(x)$ and $h(x)$ polynomials with rational coefficients such that

$$f(x) = g(x)h(x),$$

and both have degree less than n. By Gauss, we may assume that $g(x)$ and $h(x)$ have integer coefficients. Since $\overline{\sigma}_m$ is a ring homomorphism, we have

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

The LHS has degree n by assumption. Both $\overline{\sigma}_m(g(x))$ and $\overline{\sigma}_m(h(x))$ have degree less than n, a contradiction.
Thus $f(x)$ is irreducible over the rationals.
(c) Take $m = 5$. Then

$$\overline{\sigma}_5(x^3 + 17x + 36) = x^3 + 2x + 1 \in \mathbb{Z}_5[x].$$

We check that the RHS is irreducible. It suffices to check that it has no zeroes. We compute

$$\begin{aligned}
\phi_0(x^3 + 2x + 1) &= 0^3 + 2 \cdot 0 + 1 = 1 \\
\phi_1(x^3 + 2x + 1) &= 1^3 + 2 \cdot 1 + 1 = 4 \\
\phi_2(x^3 + 2x + 1) &= 2^3 + 2 \cdot 2 + 1 = 3 \\
\phi_3(x^3 + 2x + 1) &= 3^3 + 2 \cdot 3 + 1 = 4 \\
\phi_4(x^3 + 2x + 1) &= 4^3 + 2 \cdot 4 + 1 = 3.
\end{aligned}$$

Thus $x^3+2x+1 \in \mathbb{Z}_5[x]$ is irreducible and so $x^3+17x+36$ is irreducible over the rationals by (b).