Homework 2 Key

12.3.1) (a) First notice that $1+\sqrt{2}$ is a root of the polynomial x^2-2x-1, so $(x^2-2x-1) \subseteq \ker\varphi$. To see the reverse inclusion, suppose that $f(x) \in \ker\varphi$. Since this polynomial is monic, we can find polynomials $q(x), r(x) \in \mathbb{Z}[x]$ with $\deg r(x) < \deg(x^2-2x-1) = 2$ such that

$$f(x) = q(x)(x^2-2x-1) + r(x).$$

Plugging in $1+\sqrt{2}$, we see that $r(1+\sqrt{2}) = 0$. Since $r \in \mathbb{Z}[x]$ must be linear or constant and since $1+\sqrt{2}$ is irrational, we get that r is the constant polynomial 0. Thus $f(x) = q(x)(x^2-2x-1)$, so by definition, $f \in (x^2-2x-1)$. We conclude that $\ker\varphi$ is a principal ideal generated by x^2-2x-1.

(b) First notice that $\frac{1}{2}+\sqrt{2}$ is a root of the polynomial $4x^2-4x-7$, so $(4x^2-4x-7) \subseteq \ker\varphi$. Now let $f \in \ker\varphi$. Since $\mathbb{Q}[x]$ is a Euclidean domain, viewing f as a polynomial with rational coefficients, we can find $q(x), r(x) \in \mathbb{Q}[x]$ such that r has degree 0 or 1, and

$$f(x) = q(x)(4x^2-4x-7) + r(x).$$

Plugging in $\frac{1}{2}+\sqrt{2}$, we see that $r(\frac{1}{2}+\sqrt{2}) = 0$, and by the same reasoning as above, r is identically 0. Then $f(x) = q(x)(4x^2-4x-7)$. Since $4x^2-4x-7$ is a primitive polynomial that divides f in $\mathbb{Q}[x]$, $q(x)$ is actually in $\mathbb{Z}[x]$. We conclude that $\ker\varphi$ is a principal ideal generated by $4x^2-4x-7$.

12.3.2) $\Longrightarrow$ Assume two integer polynomials f, g are relatively prime elements of $\mathbb{Q}[x]$. Then there are $a, b \in \mathbb{Q}[x]$ such that $af + bg = 1$. Multiply by some integer N to clear the denominators of the coefficients of a and b to get $(Na)f + (Nb)g = N$. Then $Na, Nb \in \mathbb{Z}[x]$, so $N \in (f, g)$.

$\Longleftarrow$ Assume that f, g are integer polynomials such that the ideal $(f, g) \subseteq \mathbb{Z}[x]$ contains an integer N. Then $N = af + bg$ for some integer polynomials a, b. Dividing by N, we get $\frac{a}{N}f + \frac{b}{N}g = 1$, where $\frac{a}{N}, \frac{b}{N} \in \mathbb{Q}[x]$. Thus f, g are relatively prime elements of $\mathbb{Q}[x]$.

12.3.4) Assume $xy - zw = fg$ for some $f, g \in \mathbb{C}[x, y, z, w]$. Then without loss of generality, f must have x-degree 1 and g has x-degree 0, so $f = ax + b$ for $a, b \in \mathbb{C}[y, z, w]$ and $g \in \mathbb{C}[y, z, w]$. We then get

$$xy - zw = agx + bg,$$

so $ag = y$ and $bg = -zw$, forcing one of a, g to have y-degree 1 and the other to have y-degree 0. If g has y-degree 1, then bg has y-degree at least 1, a contradiction, so g has y-degree 0. Similarly, g has z-degree and w-degree 0, so g is a nonzero constant in $\mathbb{C}$, and thus is a unit. We conclude that $xy - zw$ is irreducible in $\mathbb{C}[x, y, z, w]$.

12.3.5) (a) It is clear that if $f(x,y) \in \mathbb{C}[x,y]$, then $p(t) = f(t^2, t^3) = \psi(f)$ is a polynomial with $\frac{dp}{dt}(0) = 0$, as the coefficient of t in p is 0.

Now assume that $p(t)$ is a polynomial with $\frac{dp}{dt}(0) = 0$. Let $p(t) = p_0 + p_2t^2 + p_3t^3 + \cdots + p_kt^k$, where we have not written p_1t since $p_1 = \frac{dp}{dt}(0) = 0$. Construct

$$f = \sum a_{ij}x^iy^j \in \mathbb{C}[x,y]$$

as follows: Let $a_{00} = p_0$. For $2 \leq \ell \leq k$, let $a_{ij} = p_\ell$ precisely when $2i+3j = \ell$ for i,j nonnegative and i as small as possible. We cannot find such a pair i,j when $\ell = 1$, but we are not considering $\ell = 1$ here. For $\ell \geq 2$, we can see that this is always possible with a quick induction argument:

- When $\ell = 2$, let $i = 1, j = 0$, which is the best we can do.
- Assume for some fixed $\ell \geq 2$ that we have $\ell = 2i + 3j$ for nonnegative integers i,j. If $i = 0$, then $j \geq 1$ so that $\ell \geq 2$. Then $\ell = 3j$, so $\ell+1 = 3(j-1)+2\cdot 2 = 3j'+2i'$ for i',j' nonnegative. Otherwise, $i \geq 1$, so

$$\ell + 1 = 2(i-1) + 3(j+1) = 2i' + 3j'$$

where i', j' are nonnegative integers. Since such a pair exists, there must be a smallest such nonnegative i'. We conclude by induction that this is always possible for $\ell \geq 2$.

Next, let $a_{ij} = 0$ for all other i,j. Then

$$\psi(f) = \sum_{\ell=0}^{k} p_\ell t^\ell = p(t).$$

We conclude that the image of ψ is the set of polynomials $p(t)$ such that $\frac{dp}{dt}(0) = 0$.

(b) It is simple to check that $g(x,y) = x^3 - y^2 + xy \in \mathbb{C}[x,y]$ is in the kernel of φ. I claim that this generates the kernel: Let $f \in \ker\varphi$. Viewing f as a polynomial in y with coefficients in $\mathbb{C}[x]$, since the leading y-coefficient of g is a unit, we can find $q, r \in \mathbb{C}[x,y]$ with

$$f(x,y) = q(x,y)g(x,y) + r(x,y)$$

where $r(x,y) = h(x)y + c(x)$ for $h(x), c(x) \in \mathbb{C}[x]$. Applying φ, we see that $r(t^2 - t, t^3 - t^2) = 0$, so

$$t^2(t-1)h(t(t-1)) + c(t(t-1)) = 0.$$

Assume h has degree i and c has degree j. If either of i,j is ≥ 1, then the other must be as well so that the highest coefficients can cancel out. Then $t^2(t-1)h(t(t-1))$ has degree $2i+3$, and $c(t(t-1))$ has degree $2j$, so $2i+3 = 2j$, a contradiction since the left side is odd and the right side is even. Thus $i = j = 0$, so h, c are constants. Then in order for the above polynomial to be 0, we must have $h = c = 0$. Thus $f = qg$, so $f \in (g)$, and we conclude that $g(x, y)$ generates $\ker \varphi$.

Now, if $f(x, y) \in \mathbb{C}[x, y]$, then

$$(\varphi(f))(t) = f(t^2 - t, t^3 - t^2) =: p(t),$$

so we see that $p(0) = f(0, 0) = p(1)$. Now, assume $p(0) = p(1)$ for a polynomial $p(t) \in \mathbb{C}[t]$. Then $p(t) = t(t-1)q(t) + c$ for some constant c. In a way similar to part (a), we can construct a polynomial $f(x, y) \in \mathbb{C}[x, y]$ such that $\varphi(f) = f(t^2 - t, t^3 - t^2) = p(t)$. We conclude that the image of φ is the set of polynomials $p(t)$ such that $p(0) = p(1)$.

An intuitive explanation is that thinking of x, y as parametrizing a curve in $\mathbb{C}^2$, we have $(x(t), y(t)) = (t^2 - t, t^3 - t^2)$, so $y = tx$, so $\frac{y}{x} = t$. Then $x = t^2 - t = (\frac{y}{x})^2 - \frac{y}{x}$, and multiplying across by x^2, we get $x^3 - y^2 + xy = 0$.

12.4.1) (a) We immediately get $x^9-x = x(x-1)(x+1)(x^2+1)(x^4+1)$, and since x^4+1 has no roots in $\mathbb{F}_3$, if it factors it must factor into a product of quadratics. We can find that $x^4+1 = (x^2+x+2)(x^2+2x+2)$, so

$$x^9 - x = x(x-1)(x+1)(x^2+1)(x^2+x+2)(x^2+2x+2)$$

in $\mathbb{F}_3[x]$.

Using the Frobenius automorphism $(a+b)^p = a^p + b^p$ in a ring of characteristic p, we get

$$x^9 - 1 = (x^3)^3 + (-1)^3 = (x^3-1)^3 = (x-1)^9$$

in $\mathbb{F}_3[x]$.

(b) We immediately get $x^{16} - x = x(x-1)(1+x+\cdots+x^{14})$. Applying the sieve of Eratosthenes, we see

$$\begin{aligned}1+x+\cdots+x^{14} &= (x^2+x+1)(x^{12}+x^9+x^6+x^3+1)\\ &= (x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1),\end{aligned}$$

which are irreducible, so

$$x^{16} - x = x(x-1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

in $\mathbb{F}_2[x]$.

12.4.4)
- In $\mathbb{F}_2[x]$: This polynomial is x^5+x^3+x+1, which has 1 as a root, so can be written as $(x-1)(x^4+x^3+1)$, each of which are irreducible.
- In $\mathbb{F}_3[x]$: This polynomial is x^5+2x^4+2, which has -1 as a root, so can be written as $(x+1)(x^4+x^3+2x^2+x+2)$. The term on the right also has -1 as a root, so we can write this as $(x+1)^2(x^2+2x+2)$, and these terms are each irreducible.
- In $\mathbb{Q}[x]$: -1 is a root, so we can write this polynomial as $(x+1)(x^4+x^3+2x^2-2x+5)$. For the term on the right, reduce modulo 2 to get the polynomial x^4+x^3+1, which is irreducible in $\mathbb{F}_2[x]$. Since the original polynomial is monic, we conclude that it is irreducible in $\mathbb{Q}[x]$ as well, so we cannot factor this polynomial any further.

12.4.6)

- In $\mathbb{Q}[x]$: By Eistenstein's criterion with the prime $p = 5$, $x^5 + 5x + 5$ is irreucible in $\mathbb{Q}[x]$
- In $\mathbb{F}_2[x]$: This polynomial is $x^5 + x + 1$ in $\mathbb{F}_2[x]$. Since there are no roots in $\mathbb{F}_2$, any factorization must involve a quadratic and a cubic, and indeed we can find

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

12.4.13) (a) Let

$$p(x) := \prod_{i=1}^{n} \frac{x - a_i}{a_0 - a_i},$$

which has degree n. It is immediately clear that $p(a_i) = 0$ for $1 \leq i \leq n$ and $p(a_0) = 1$.

(b)
- Uniqueness: Assume f, g are each polynomials of degree $\leq d$ such that $f(a_i) = g(a_i) = b_i$ for $0 \leq i \leq d$. Then $f - g$ is a polynomial of degree $\leq d$ that is zero at the $d+1$ distinct points $a_0, \ldots, a_d$, so $f - g$ must be identically 0. Thus $f = g$.
- Existence: Let

$$g(x) := \sum_{i=0}^{d} b_i \prod_{j \neq i} \frac{x - a_j}{a_i - a_j},$$

which has degree at most d. We immediately see that $g(a_i) = b_i$ for $0 \leq i \leq d$.

12.4.16) Suppose for a contradiction that $x^{14} + 8x^{13} + 3 = fg$, where $f, g \in \mathbb{Q}[x]$ and

$$f = a_0 + \cdots + a_r x^r,$$
$$g = b_0 + \cdots + b_{14-r} x^{14-r}$$

for some $r = 1, \ldots, 13$. Reducing modulo 3, we get

$$x^{13}(x+2) = \overline{f}\overline{g}.$$

Since $\mathbb{F}_3[x]$ is a UFD, without loss of generality we have $\overline{f} = x^k$ and $\overline{g} = x^{13-k}(x+2)$ for some $k = 0, \ldots, 13$. If $k = 0$, then $\overline{g} = x^{14} + 2x^{13}$, so g has degree 14, contradicting that $\deg g \leq 13$. Thus $1 \leq k \leq 13$. Since $a_0 b_0 = 3$, we have either $a_0 = \pm 3$ and $b_0 = \pm 1$ or $a_0 = \pm 1$ and $b_0 = \pm 3$. Thus one of $\overline{f}, \overline{g}$ should have constant term ± 1, but each has constant term 0, a contradiction. Thus $x^{14} + 8x^{13} + 3$ is irreducible in $\mathbb{Q}[x]$.