1.5 Lemma: if $\gcd(a, b) = 1$ then $\gcd(ab, a + b) = 1$. Note that if any number divides ab then it divides either a or b, otherwise contradicting that $\gcd(a, b) = 1$ if it is larger. Suppose $d \mid a, d \nmid b$. Then since $d \nmid b$ then $d \nmid a + b$. The alternate case is identical. Therefore $\gcd(ab, a + b)$.
Since $\gcd(ab, a+b) = 1$, then by applying Euler's theorem there exists $n \in \mathbb{N}$ such that $(a+b)^n \equiv 1 \mod ab(< a+b >$ forms a subgroup of $\mathbb{Z}/ab$, therefore it will cycles back to 1). Thus noting that $(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} \equiv a^n + b^n \mod ab$ since all cross terms are of the form $ka^r b^q$ where both $r, q \geq 1$. Thus all of the cross terms

2.2 $\gcd(x^5 + 2x^3 + x^2 + x + 1, x^6 + x^4 + x^3 + x^2 + x + 1) = x^2 + 1$

2.10 Note that the set of all units is all power series with non-zero constant term. Consider $f(x) = \sum_{i=0}^{\infty} a_i x^i$ with first non-zero term being a_n. Therefore since $\sum_{i=0}^{\infty} a_{i+n} x^i$ is a unit then we have that $f(x) = x^n \sum_{i=0}^{\infty} a_{i+n} x^i$. Since both the unit and the power of x is uniquely determined by the sequence, then the factorization is unique. Additionally since this takes exactly one step then factoring terminates. Thus the ring of power series is a UFD.

3.1 (a) Let $\phi : \mathbb{Z}[x] \to \mathbb{R}$ be the homomorphism given by $\phi(x) = 1 + \sqrt{2}$. Therefore the kernel contains

$$\begin{aligned} x &= 1 + \sqrt{2} \\ x - 1 &= \sqrt{2} \\ (x - 1)^2 &= 2 \\ (x - 1)^2 - 2 &= 0 \\ x^2 - 2x + 1 - 2 &= 0 \\ x^2 - 2x - 1 &= 0 \end{aligned}$$

Since this polynomial found has an irrational root by construction, and since it has another root which also must be irrational then our polynomial is irreducible. Therefore our kernel is principle.

(b) Let $\phi : \mathbb{Z}[x] \to \mathbb{R}$ be the homomorphism given by $\phi(x) = \frac{1}{2} + \sqrt{2}$. Therefore the kernel contains

$$\begin{aligned} x &= \frac{1}{2} + \sqrt{2} \\ 2x - 1 &= 2\sqrt{2} \\ (2x - 1)^2 &= 8 \\ (2x - 1)^2 - 8 &= 0 \\ 4x^2 - 4x - 7 &= 0 \end{aligned}$$

Since this polynomial found has an irrational root by construction, and since it has another root which also must be irrational then our polynomial is irreducible. Therefore our kernel is principle.

3.2 Let $f, g \in \mathbb{Z}[x]$

- $\Rightarrow$ Suppose the $\gcd_{\mathbb{Q}[x]}(f(x), g(x)) = 1$. Then there exists $a(x), b(x) \in \mathbb{Q}[x]$ such that $a(x)f(x) + b(x)g(x) = 1$. Since $a(x), b(x) \in \mathbb{Q}[x]$ then they take the form $a(x) = \sum_{i=0}^{n} \frac{a_i}{a'_i} x^i, b(x) = \sum_{i=0}^{m} \frac{b_i}{b'_i} x^i$. If we multiply $a(x)f(x) + b(x)g(x) = 1$ by $a'_1 \cdots a'_n b'_1 \cdots b'_m$ then we guarantee $a(x), b(x)$ to now be integer polynomials. Thus we have found a combination in $\mathbb{Z}[x]$ of f, g which is an integer. Thus $a'_1 \cdots a'_n b'_1 \cdots b'_m \in (f(x), g(x))$. combination
- $\Leftarrow$ Suppose that there are $a(x), b(x) \in \mathbb{Z}[x]$ such that $a(x)f(x) + b(x)g(x) = n, n \in \mathbb{Z}$. Note that $a(x)/n, b(x)/n \in \mathbb{Q}[x]$ therefore we have found polynomials satisfying the requirements for f, g to be coprime over $\mathbb{Q}[x]$

4.1 (a)
- $x^9 - 1 = (x-1)^9$ over $\mathbb{F}_3[x]$
- $x^9 - x = x(x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2)$ over $\mathbb{F}_3[x]$

(b) $x^{16} - x = x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$ over $\mathbb{F}_2[x]$