1.1

- Note that the polynomial $f(x) = (x-7)^3 - 2$ satisfies $f(7+\sqrt[3]{2}) = 0$ since
$$f(7+\sqrt[3]{2}) = (7+\sqrt[3]{2}-7)^3 - 2 = 2-2 = 0.$$
- Note that the polynomial $f(x) = (x^2-8)^2 - 60$ satisfies $f(\sqrt{3}+\sqrt{5}) = 0$ since
$$f(\sqrt{3}+\sqrt{5}) = (5+3+2\sqrt{15}-8)^2 - 60 = 60-60 = 0$$

1.8 (a) $\{1, 5, 7, 11\}$

(b) $\{1, 3, 5, 7\}$

(c) We claim that the set $\Phi(n) = \{k \in [n] : \gcd(n,k) = 1\}$ is the set of units of $\mathbb{Z}/n\mathbb{Z}$. Note that if $\gcd(a,n) = 1$ then there exists $x, y \in \mathbb{Z}$ such that $ax+ny = 1$. Therefore $1 = ax+ny \equiv ax \mod n$. Thus $x \mod n$ is the inverse of a. However consider for contradiction that $\Phi(n)$ does not contain all of the units. Thus there exists $u \in \mathbb{Z}/n\mathbb{Z}$ which $u \notin \Phi(n)$ and there exists $w \in \mathbb{Z}/n\mathbb{Z}$ such that $uw \equiv 1 \mod n$. Thus by the definition of modular arithmatic there exists $m \in \mathbb{Z}$ then $uw + my = 1$. Thus by definition of the gcd, $\gcd(u,n) = 1$. Thus $u \in \Phi(n)$. This is a contradiction. Thus $\Phi(n)$ contains all of the units of $\mathbb{Z}/n\mathbb{Z}$.

2.2 Proving that $F[[x]]$ is a ring

- Addition is an abelian group.
  - Commutativity: Suppose $a, b \in F[[x]]$ where $a = \sum_{i=0} a_i x^i, b = \sum_{i=0} b_i x^i$. Then
  $$a+b = \sum_{i=0} a_i x^i + \sum_{i=0} b_i x^i = \sum_{i=0} (a_i+b_i) x^i = \sum_{i=0} (b_i+a_i) x^i = \sum_{i=0} b_i x^i + \sum_{i=0} a_i x^i = b+a$$
  - Identity: Suppose $a \in F[[x]]$. Then
  $$0+a = a+0 = \sum_{i=0} a_i x^i + \sum_{i=0} 0 x^i = \sum_{i=0} (a_i+0) x^i = \sum_{i=0} a_i x^i = a.$$
  Thus 0 is the additive identity for $F[[x]]$.
  - Associativity: Suppose $a, b, c \in F[[x]]$. Then
  $$\begin{aligned}(a+b)+c &= \sum_{i=0} (a_i+b_i) x^i + \sum_{i=0} c_i x^i \\ &= \sum_{i=0} (a_i+b_i+c_i) x^i \\ &= \sum_{i=0} a_i x^i + (b_i+c_i) x^i \\ &= \sum_{i=0} a_i x^i + \sum_{i=0} (b_i+c_i) x^i \\ &= a+(b+c)\end{aligned}$$

- Additive inverses: Suppose $a \in F[[x]]$. Then by definition $a = \sum_{i=0} a_i x^i$. Since F is a field then the sequence $(-a_0, -a_1, \cdots) \subseteq F$. Therefore we can construct $b = \sum_{i=0} -a_i x^i$. Thus $a + b = \sum_{i=0}(a_i - a_i)x^i = \sum_{i=0} 0x^i = 0$. Thus b is the inverse of a.

- Multiplication is commutative: Suppose $a, b \in F[[x]]$ Then

$$\begin{aligned}(ab)_n &= \sum_{i+j=n} a_i b_j \\ &= \sum_{j+i=n} b_j a_i \text{ commutativity of } F \\ &= \sum_{l+k=n} b_l a_k \text{ let } l = j, k = i \\ &= (ba)_n\end{aligned}$$

  Since the nth coefficient is the same, then the power series is identical.

- Multiplication is associative: Suppose $a, b, c \in F[[x]]$. Then

$$\begin{aligned}(ab)c &= \left(\sum_{i=0}^{\infty} \sum_{k+j=i} a_k b_j x^i\right)\left(\sum_{l=0}^{\infty} c_l x^l\right) \\ &= \sum_{i=0}^{\infty} \sum_{i=j+k+l} a_j b_k c_l x^i \\ &= \left(\sum_{j=0}^{\infty} a_j x^j\right)\left(\sum_{n=0^{\infty}} \sum_{k+l=n} b_k c_l x^n\right) \\ &= a(bc)\end{aligned}$$

- Distributive rule: Suppose $a, b, c \in F[[x]]$. Then

$$\begin{aligned}c(a+b) &= \left(\sum_{i=0}^{\infty} c_i x^i\right)\left(\sum_{i=0} a_i + \sum_{i=0} b_i\right) \\ &= \sum_{i=0} \sum_{j+k=i} c_j(a_k + b_k)x^i \\ &= \sum_{i=0} \sum_{j+k=i} c_j a_k x^i + \sum_{i=0} \sum_{j+k=i} c_j b_k x^i \\ &= ca + cb\end{aligned}$$

The units of $F[[x]]$ have to be pairs of power series of the form $A = \sum_{i=0}^{\infty} a_i x^i$ and $B = \sum_{i=0}^{\infty} b_i x^i$ satisfying $AB = 1$. Therefore b_0 must be $\frac{1}{a_0}$, giving us a requirement that the original power series A must have a non-zero constant term, and that for $n > 0, \sum_{i+j=n} a_i b_j = 0$. Note that we can use the second condition to define b_n recursively via $b_n = \frac{-1}{a_0} \sum_{i=0}^{n-1} a_{n-i} b_i$. This gives us that the sum

$$\sum_{i+j=n} a_i b_j = a_0 b_n + \sum_{i=0}^{n-1} a_{n-i} b_i = -\sum_{i=0}^{n-1} a_{n-i} b_i + \sum_{i=0}^{n-1} a_{n-i} b_i = 0$$

Satisfying the requirements that all of the non-constant mononomial terms have a coefficient of 0. Therefore the only requirement on a given power series to be invertible is that there must be a non-zero constant term.

3.2 Suppose $I \subset \mathbb{Z}[i]$ and consider $x \in I$. By definition of $\mathbb{Z}[i]$ there exists $a, b \in \mathbb{Z}$ such that $x = a + bi$ where at least one of the a, b is non-zero. Therefore the element $a - bi \in \mathbb{Z}[i]$ since $-b \in \mathbb{Z}$. Thus by the definition of an ideal $(a - bi)(a + bi) \in I$. Therefore $a^2 - b^2 \in I$. Since $a, b \in \mathbb{Z}$ then I contains an integer.

3.6 Let the automorphism be denoted $\psi : R[x, y] \to R[x, y]$, given by $\psi(p(x, y)) = p(x + f(y), y)$

- Injectivity: Suppose $p, q \in R[x, y], \psi(p) = \psi(q)$. We want to show that $p = q$. Note that we can set $z = x + f(y)$. From our original supposition we have that $p(z, y) = q(z, y)$. Therefore trivially $p(x, y) = q(x, y)$
- Surjectivity: Suppose $p \in R[x, y]$. We want to show there exists $p' \in R[x, y]$ such that $\psi(p') = p$. We claim that $p' = p(x - f(y), y)$. Observe that $\psi(p') = p((x - f(y)) + f(y), y) = p(x, y)$.
- Homomorphism requirements: Suppose $p, q, r \in R[x, y], g = pq, w = g + r$ then

$$\psi(pq + r) = \psi(w(x, y)) = w(x + f(y), y) = g(x + f(y), y) + r(y)$$

$$= p(x + f(y), y)q(x + f(y), y) + r(x + f(y), y) = \psi(p)\psi(q) + \psi(r)$$

.

Additionally, since ψ is a substitution map on the variables x,y, then it does not affect constants, thus $\psi(1) = 1$.

3.12 We must show that $I + J = i + j : i \in I, j \in J$ is an ideal in the ring R

- Suppose $a, b \in I + J$. Then there exists $a_i, b_i \in I, a_j, b_j \in J$ such that $a = a_i + a_j, b = b_i + b_j$. Therefore $a + b = a_i + a_j + b_i + b_j = (a_i + b_i) + (a_j + b_j)$. Since I, J are closed under addition then $a_i + b_i \in I, a_j + b_j \in J$. Since $a + b$ is the sum of an element from I and an element from J then it's an element of $I + J$.
- Suppose $c \in R, a \in I + J$. Then there exists $a_i \in I, a_j \in J$ such that $a_i + a_j = a$. Thus $ca = c(a_i + a_j)ca_i + ca_i$. Since ideals "absorb" multiplication then $ca_i \in I, ca_j \in J$. Thus by the definition of $I + J, ca \in I + J$.

Therefore $I + J$ is an ideal of R.

4.1 Since the substitution homomorphism is surjective from $\mathbb{Z}[x]$ to $\mathbb{Z}$ then we can apply the correspondence theorem. This gives us a bijective correspondence between ideals in $\mathbb{Z}[x]$ containing $x - 1$ and ideals in $\mathbb{Z}$. Note that the ideals in $\mathbb{Z}$ are exactly (n) where $n \in \mathbb{Z}$. Since constants are unaffected by substitution then this says that all of the ideals which contain $(x - 1)$ are exactly the ideals of the form $(n, x - 1)$.

5.6 (a) Let $\phi : R[x] \to R[\alpha]$ be the substitution homomorphism $\phi(x) = \alpha$, $\pi : R[x] \to R[x]/(ax-1)$ be the projection map, and $\psi : R[x]/(ax-1) \to R[\alpha]$ be the isomorphism guaranteed by the first isomorphism theorem. We know by the first isomorphism theorem that $R[x]/(ax-1) \cong R[\alpha]$. Therefore we must show that all elements in $R[x]/(ax-1)$ are equal to cx^k, where $c \in R$. Given a polynomial in $R[x]$, $p(x) = b_0 + b_1 x + \cdots + b_n x^n$, one can remove the constant term b_0 by adding $b_0(ax-1)$. Note that our new polynomial is equivalent in $R[x]/(ax-1)$. Therefore we can continue the process via adding $(b_1 + b_0 ax)(ax-1)$, which will elimate the x. This process can be continued til we end up with a polynomial of the form bx^n where $b \in R$. Since ψ is a bijection between $R[x]/(ax-1)$ and $R[\alpha]$ then we have that all elements in $R[\alpha]$ are of the form $b\alpha^n$.

(b) Note that if $b \in \ker \psi$ then there exists $p(x) \in R[x]$ such that $b = (ax-1)p(x)$. Since $p(x) \in R[x]$ then it takes the form $p(x) = c_0 + c_1 x + \cdots + c_n x^n$. Therefore we have the equation $b = (ax-1)(c_0 + c_1 x + \cdots + c_n x^n)$, which must satisfy $-c_0 = b, c_0 a = c_1, c_1 a = c_2, \cdots, c_{n-1} a = c_n, 0 = c_n a$. Thus going up the equations we end with $0 = a^n b$.

(c)
- ($\Rightarrow$) Suppose R' is the zero ring. Then trivially all elements are in the kernel. Thus there exists an n for every element $b \in R$ where $a^n b = 0$. This implies that all elements are either zero divisors or $a^n = 0$. If every element is a zero divisor then R is the zero ring, making a trivially nilpotent. Otherwise $a^n = 0$, thus making a nilpotent.
- ($\Leftarrow$) Suppose a is nilpotent. We want to show that R' is the zero ring. Then by definition there exists $n \in \mathbb{N}$ such that $a^n = 0$. Thus all elements $b \in R$ satisfy $a^n b = 0$. Thus all elements from R are in the kernel of γ. Thus R' is the zero ring.

6.1 Let $\varphi : \mathbb{R}[x] \to \mathbb{C} \times \mathbb{C}$ be the homomorphism given by $\varphi(x) = (1, i), \varphi(r) = (r, r), r \in \mathbb{R}$.

- We claim that $im\varphi = \mathbb{R} \times \mathbb{C}$. Observe that no matter the polynomial, the first coordinate must be a real number because both $\varphi(x), \varphi(r)$ have a real number in the first coordinate, and we are taking linear combinations of x and $r \in \mathbb{R}$. Furthermore the second coordinate spans $\mathbb{C}$ since $ax + b \in \mathbb{R}[x]$

$$\varphi(ax+b) = \varphi(a)\varphi(x) + \varphi(b) = (a,a)(1,i) + (b,b) = (a+b, a+bi)$$

  Clearly the second coordinate spans all of $\mathbb{C}$.
- We claim that $\ker \varphi = (x^4 - 1)$. Note that $\varphi(x^4) = \varphi(x)^4 = (1,i)^4 = (1^4, i^4) = (1,1)$, therefore $\varphi(x^4) = \varphi(1)$. Thus $\varphi(x^4 - 1) = 0$. Note that if there exists a smaller polynomial which generates the kernel then it must divide $x^4 - 1$. Note that $\varphi(x^2+1) = (2,0)$ and $\varphi(x^2-1) = (0,-2)$, thus the divisors are non-zero. Therefore $x^4 - 1$ is the smallest polynomial in the kernel. Therefore $\ker \varphi = (x^4 - 1)$.