1. (a) There are 8 symmetries of the square:

- Identity (I)
- Rotation by $90^\circ$
- Rotation by $180^\circ$
- Rotation by $270^\circ$
- Flip along main diagonal
- Flip along main diagonal followed by Rotation by $90^\circ$
- Flip along main diagonal followed by Rotation by $180^\circ$
Flip along main diagonal followed by Rotation by 270°
As we can see from this description, there are two generators for the group of symmetries; Rotation by 90° (R) and a verticle flip (F). We can write the presentation as

$$\langle R, F | R^4 = I, F^2 = I, RFRF = I \rangle,$$

which is isomorphic to $D_{2(4)}$.

(b) There are 4 symmetries to the rectangle:

- **Identity (I)**
- **Rotation of 180°**
- **Vertical Flip**
- **Vertical Flip followed by Rotation of 180°** which is also a horizontal flip.

There are only two groups of order four and we know this is the Klein-4 group, because each non-identity symmetry $S$ has the property that $S^2 = I$.

(c) There are many possibilities, all you need is an object that has only one line of symmetry. For example, the boomerang has symmetry only at the corner (ignoring the designs and only considering the shape)

or Rorschach tests (inkblot tests) that are designed to have symmetry across the fold in the paper.
There are also many possibilities for irregular shapes without any non-identity symmetry, for example

2. For a regular polygon, the set of rotational symmetries will send each vertex to every other vertex, so it acts transitively.

Since the set of symmetries of a polygon is orthogonal, then all angles must be preserved. We know that every vertex is sent to every other vertex, since our group acts transitively, therefore each angle must be the same. Therefore, every polygon that has a transitively acting permutation group, must be a regular polygon.

3. We are essentially going to generalize the case for the square, but this will require some new notation. First, let $R$ be the counter-clockwise rotation of the \( n \)-gon of \( \frac{2\pi}{n} \) radians in the plane and $F$ be the flip over an axis of symmetry of your choosing. We know that there are \( 2n \) symmetries found by the \( n \) rotations in the plane (including the identity) and the \( n \) rotations after a flip. Also, $F^2 = I$ and $R^n = I$, so it remains to show that $RFRF = I$.

First, fix the axis of symmetry of the regular polygon used as $F$. Starting from the right of this axis (or on it if the axis cuts through a vertex), label the vertices in order $1, 2, \ldots, n-1, n$. Using this same ordering from the fixed axis of symmetry, we will track the positions of our vertices. We begin with

\[
1, 2, \ldots, n-1, n
\]

then after the first flip we get

\[
\begin{cases}
1, n, n-1, \ldots, 3, 2 & \text{if 1 is on the axis of symmetry} \\
n, n-1, \ldots, 2, 1 & \text{if it is not.}
\end{cases}
\]

Following it by a rotation results in

\[
\begin{cases}
n, n-1, \ldots, 3, 2, 1 & \text{if 1 was on the axis of symmetry} \\
n-1, \ldots, 2, 1, n & \text{if it was not.}
\end{cases}
\]

We then flip again and each case results in

\[
n, 1, 2, \ldots, n-1.
\]
Finally, we take one last rotation to get the vertices in their original positions of 

\[1, 2, \ldots, n-1, n.\]

Thus, \(\Sigma(P_n) = \langle R, F| R^n = I, F^2 = I, RFRF = I \rangle \cong D_{2n}.\)

4. The group of symmetries of the circle \(\Sigma(F)\) can be represented as \(\{e^{i\theta} | 0 \leq \theta < 2\pi\}\) the points on the unit circle. The operation is multiplication of these elements or can be viewed as simply angle addition, since the rotations the disk by any angle \(0 \leq \theta < 2\pi\) is a symmetry of the disk. Of course, there are infinitely many numbers in the interval \([0, 2\pi)\).

5. We prove that the intersection of any family of subrings of \(R\) is likewise a subring of \(R\). Let \(a, b \in \cap_\alpha R_\alpha\). Since \(a\) and \(b\) are in each \(R_\alpha\) and each ring is closed under addition and multiplication, the sum \(a + b\) and product \(ab\) must likewise be in \(\cap_\alpha R_\alpha\). The intersection of rings automatically inherits commutativity, distributivity, and associativity from each ring in the intersection having these properties. Since \(a\) is in \(\cap_\alpha R_\alpha\), \(a\) is in each ring \(R_\alpha\), and so \(-a\) must be in each \(R_\alpha\), and thus \(-a\) is in \(\cap_\alpha R_\alpha\). Lastly, since the additive and multiplicative identities are in each \(R_\alpha\), they are in \(\cap_\alpha R_\alpha\). Thus the intersection of any family of rings satisfies all the properties of a subring and is itself a subring.

6. First, we must show that the identity

\[\binom{n-1}{i} + \binom{n-1}{i-1} = \binom{n}{i}\]

is true. Consider the left hand side

\[\binom{n-1}{i} + \binom{n-1}{i-1} = \frac{(n-1)!}{i!(n-i-1)!} + \frac{(n-1)!}{(i-1)!(n-1-(i-1))!}\]

\[= \frac{(n-1)!(n-i)}{i!(n-i-1)!(n-i)} + \frac{(n-1)!i}{(i-1)!(n-1-i)!}\]

\[= \frac{(n-1)!(n-i) + (n-1)!i}{i!(n-i)!}\]

\[= \frac{(n-1)!(n-i+i)}{i!(n-i)!} = \frac{n!}{i!(n-i)!} = \binom{n}{i}\]

We will prove the binomial theorem holds in any ring by induction, that is if \(n \geq 1\)

\[(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}\]

For the inductive step, we have

\[(a + b)^1 = \sum_{i=0}^{1} a^i b^{1-i} = a^0 b^1 + a^1 b^0\]

Now assume the theorem holds for \(n-1\), that is

\[(a + b)^{n-1} = \sum_{i=0}^{n-1} \binom{n-1}{i} a^i b^{n-1-i}\]
Then
\[(a + b) (a + b)^{n−1} = (a + b)^n = \sum_{i=0}^{n−1} \binom{n−1}{i} a^{i+1} b^{n−1−i} + \sum_{i=0}^{n−1} \binom{n−1}{i} a^i b^{n−i}\]

Changing indices, we have
\[\sum_{i=1}^{n−1} \binom{n−1}{i−1} a^i b^{n−i} + \sum_{i=1}^{n−1} \binom{n−1}{i} a^i b^{n−i} + b^n + a^n\]

Using the identity
\[\binom{n−1}{i} + \binom{n−1}{i−1} = \binom{n}{i}\]

we have
\[\sum_{i=1}^{n−1} \binom{n−1}{i−1} a^i b^{n−i} + \sum_{i=1}^{n−1} \binom{n−1}{i} a^i b^{n−i} + b^n + a^n = \sum_{i=1}^{n−1} \binom{n}{i} a^i b^{n−i}\]

7. We will prove that if \(p\) is a prime, then \(p\) divides \(\binom{p}{i}\) for \(i \neq 0\) and \(i \neq p\). By definition,
\[\binom{p}{i} = \frac{p!}{(p−i)!i!}\]

Since \(i\) is less than \(p\) and not equal to 0, \(i!\) does not divide \(p\) and so \(p\) must divide \(\binom{p}{i}\).

8. We now show that
\[\left[f(x) + g(x)\right]' = f'(x) + g'(x)\]

and
\[\left[f(x) g(x)\right]' = f(x) g'(x) + f'(x) g(x)\]

Let
\[f(x) = f_0 + f_1 x + \ldots + f_n x^n\]

and
\[g(x) = g_0 + g_1 x + \ldots + g_m x^m\]

Then \(f'(x) = f_1 + 2 f_2 x + \ldots + n f_n x^{n−1}\) and \(g'(x) = g_1 + 2 g_2 x + \ldots + n g_n x^{n−1}\) and (WLOG, we assume \(m \geq n\)), we have
\[\left[f(x) + g(x)\right]' = \left[(f_0 + g_0) + (f_1 + g_1) x + \ldots + (f_n + g_n) x^n + \ldots + g_m x^m\right]'\]
\[= (f_1 + g_1) + 2 (f_2 + g_2) x + \ldots + n (f_n + g_n) x^{n−1} + \ldots + m g_m x^{m−1} = f'(x) + g'(x).\]

For the second identity, we first find
\[\left[f(x) g(x)\right]'\]
\[= (f_0 g_0 + (f_0 g_1 + f_1 g_0)x + \ldots + (f_0 g_n + f_n g_0) x^n + \ldots + (f_n g_m) x^{m+n})'\]
\[= (f_0 g_1 + f_1 g_0) + \ldots + n(f_0 g_0 + f_1 g_{n−1} + \ldots + f_{n−1} g_1 + f_n g_0) x^{n−1} + \ldots + (m+n) (f_n g_m) x^{m+n−1}\]
On the other hand, we have
\[ f'(x)g(x) + f(x)g'(x) = (f_1 + 2f_2x + \ldots + n f_nx^{n-1}) (g_0 + g_1x + \ldots + g_mx^m) + \\
(f_0 + f_1x + \ldots + f_nx^n) (g_1 + 2g_2x + \ldots + m g_mx^{m-1}) \\
= (f_0 g_1 + f_1 g_0) + \ldots + n(f_0 g_n + f_1 g_{n-1} + \ldots + f_{n-1} g_1 + f_n g_0) x^{n-1} + \ldots + (m+n) (f_n g_m) x^{m+n-1} \\
\]
This proves the product rule for polynomial rings.

9. If \( R \) is a ring and \( S \) is a set, the set \( R^S \) consisting of all functions \( S \to R \) equipped with the operations of pointwise addition and pointwise multiplication is a ring. To prove this statement, we first show prove that the map \( z(s) = 0 \) for all \( s \in S \) acts as the identity in \( R^S \). If \( m(s) \in R^S \), then \( m(s) + z(s) = z(s) + m(s) = m(s) \) for all \( s \in S \). Now given \( m(s) \in R^S \) with \( m : s \to r \) (where \( r \in R \)), let \( m'(s) \) denote the map \( m : s \to -r \). Then we have
\[ m(s) + m'(s) = m(s) + m(s) = r - r = 0 = z(s) \]
Since addition is a pointwise operation in a ring, it inherits associativity, commutativity, and distributivity properties from the ring \( R \). For multiplication, let \( y(s) = 1 \). As with addition, this map is clearly the identity:
\[ m(s) y(s) = y(s) m(s) = m(s) 1 = m(s) \text{ for all } s \in S. \]
Thus \( R^S \) satisfies all the properties of a ring and the theorem is proved.

10. (a) We inherit the associativity of multiplication from the ring. Also, since our ring has unity (1), which is a unit, so we have a multiplicative identity. Suppose \( a \in U(R) \) then \( a \) is a unit of \( R \), which means there exists \( b \) so that \( ab = 1 \). Thus \( b \) is also a unit, so we have multiplicative inverses. The remaining thing to show is that this set is closed under multiplication. Suppose \( a, b \in U(R) \), so that \( a^{-1}, b^{-1} \) are the multiplicative inverses, respectively. Then \( ab \) is a unit since \( (ab)(b^{-1}a^{-1}) = 1 \). Thus \( U(R) \) is a group under multiplication.

(b) \( \Rightarrow \) If \( R \) is a field, then each element of \( R - \{ 0 \} \) has a multiplicative inverse. The set \( R \) is closed under multiplication, is commutative and has multiplicative identity since \( R \) is a commutative ring with unity.

\( \Leftarrow \) If \( R - \{ 0 \} \) is a group under multiplication, then we know that since \( R \) is a commutative ring with unity that we need to show each element has a multiplicative inverse. Since every non-zero element is an element of the multiplicative group \( R - \{ 0 \} \), it does have a multiplicative inverse. Thus \( R \) is a field.

11. \( \Leftarrow \) If \( \gcd(a, n) = 1 \) then there exists an \( x, y \in \mathbb{Z} \) so that \( ax + ny = 1 \) by Bezout’s Identity. Thus in \( \mathbb{Z}_n \) we have that \( ax \equiv 1 \). Thus, \( a \) is a unit in \( \mathbb{Z}_n \).

\( \Rightarrow \) Suppose \( a \) is a unit in \( \mathbb{Z}_n \). Then there exists \( b \in \mathbb{Z} \) so that \( ab \equiv 1 \). In other words, \( ab - nc = 1 \). If \( \gcd(a, n) = d \), then \( \frac{a}{d}b - \frac{n}{d}c = \frac{1}{d} \). However, \( \frac{a}{d}, \frac{n}{d}, c \in \mathbb{Z} \) which would imply that \( \frac{1}{d} \in \mathbb{Z} \), so \( d = 1 \).

12. Let
\[ f(x) = f_0 + f_1x + \ldots + f_nx^n \]
and
\[ g(x) = g_0 + g_1x + \ldots + g_mx^m. \]
14. If \( R \) is a domain, then the leading coefficient of \( f(x)g(x) \) is the product of the leading coefficients of \( f(x) \) and \( g(x) \). The value of the leading coefficient of \( f(x)g(x) \) is nonzero since both the leading coefficients of \( f(x) \) and \( g(x) \) are nonzero and the product is in a domain. Using this fact and basic exponent addition, we have

\[
\partial(fg) = \partial(f) + \partial(g).
\]

(b) We now prove that if \( R \) is a domain, then likewise \( R[x] \) is also a domain. By (a), we know that given two nonzero polynomials \( f(x) \) and \( g(x) \), the degree of their product is equal to the sum of their degrees. Since \( f(x)g(x) \) has a nonzero leading coefficient, \( R[x] \) cannot have any zero-divisors and thus must be a domain.

(c) If \( R = \mathbb{Z}_4[x] \), then \((2x + 1)^2 = 4x^2 + 4x + 1 = 1\) Thus the formula \( \partial(fg) = \partial(f) + \partial(g) \) fails to hold if \( R \) is not a domain.

(d) Consider the factorization of \((2x^2 + 3x)(2x + 3)\) in \( R = \mathbb{Z}_4 \) In this ring, we have

\[
(2x^2 + 3x)(2x + 3) = 4x^3 + 12x^2 + 9x = x
\]

This is an example of a factorization of \( x = f(x)g(x) \) in which neither \( f(x) \) nor \( g(x) \) is constant.

13. (a) If \( f(x) \) and \( g(x) \) are nonzero polynomials in \( R[x] \) where \( R \) is a domain, then the leading coefficient of \( f(x)g(x) \) is the product of the leading coefficients of \( f(x) \) and \( g(x) \). The value of the leading coefficient of \( f(x)g(x) \) is nonzero since both the leading coefficients of \( f(x) \) and \( g(x) \) are nonzero and the product is in a domain. Using this fact and basic exponent addition, we have

\[
\partial(fg) = \partial(f) + \partial(g).
\]

(b) We now prove that if \( R \) is a domain, then likewise \( R[x] \) is also a domain. By (a), we know that given two nonzero polynomials \( f(x) \) and \( g(x) \), the degree of their product is equal to the sum of their degrees. Since \( f(x)g(x) \) has a nonzero leading coefficient, \( R[x] \) cannot have any zero-divisors and thus must be a domain.

(c) If \( R = \mathbb{Z}_4[x] \), then \((2x + 1)^2 = 4x^2 + 4x + 1 = 1\) Thus the formula \( \partial(fg) = \partial(f) + \partial(g) \) fails to hold if \( R \) is not a domain.

(d) Consider the factorization of \((2x^2 + 3x)(2x + 3)\) in \( R = \mathbb{Z}_4 \) In this ring, we have

\[
(2x^2 + 3x)(2x + 3) = 4x^3 + 12x^2 + 9x = x
\]

This is an example of a factorization of \( x = f(x)g(x) \) in which neither \( f(x) \) nor \( g(x) \) is constant.

14. If \( R \) is a domain then \( R[x] \) is a domain by Exercise 13b. Thus by induction on \( n \) if \( R[x_1, \ldots, x_{n-1}] \) is a domain, then \( R[x_1, \ldots, x_{n-1}][n] = R[x_1, \ldots, x_n] \) is a domain.

15. Let \( R \) be a domain and let \( f, g \in R \) be nonzero elements in \( R \) satisfying

\[
f = u g \quad g = v f
\]

where \( u, v \in R \). Then \( f = uvf \) and by the uniqueness of the multiplicative identity, \( uv = 1 \). Thus \( u \) and \( v \) are both units.

16. (a) We will prove that if \( F \) is a field, then the units in \( F[x] \) are the nonzero constants. By exercise 13, we know that if we have two nonzero polynomials in a domain and one has degree greater than one, than their product likewise has degree greater than one and thus the product cannot be equal to one. Thus all the units in \( F[x] \) must be nonzero constants.

(b) By (a), the only unit in \( \mathbb{Z}_2[x] \) is the nonzero constant \( 1 \). It is an infinite ring because it contains \( 1, x, x^2, x^3, \ldots \).

(c) The polynomial \((2x + 1)\) is nonconstant in \( \mathbb{Z}_4[x] \) and \((2x + 1)^2 = 1\), so \((2x + 1)\) is a unit.

17. (a) If \( \text{deg}(f) < \text{deg}(g) \) then let \( q(x) = 0 \) and \( r(x) = f(x) \). Now, suppose \( \text{deg}(g) \leq \text{deg}(f) \), so we will induct on the degree of \( f(x) \) for a fixed \( g(x) \in R[x] \). Let

\[
f(x) = f_0 + f_1 x + \ldots + f_n x^n
\]

and

\[
g(x) = g_0 + g_1 x + \ldots + g_m x^m.
\]
Suppose that $\deg(g) = \deg(f)$. We define $q(x) = f_ng_m^{-1}$. Then 
\[
 f(x) - q(x)g(x) = \begin{cases} 
 0 & \text{where } \deg(r) < \deg(f) = \deg(g) \\
 r(x) & \text{since we have cancelled the leading terms.}
\end{cases}
\]
Assume we know this statemt is true for all $f$ where $\deg(f) \leq k$ for some $k \geq \deg(g)$.
Suppose $\deg(f) = k+1$. Let $q_1(x) = f_{k+1}g_m^{-1}x^{m-(k+1)}$. The polynomial $f(x) - q_1(x)g(x) = f_1(x)$ has degree strictly less than $\deg(f)$ since the leading term has been cancelled. By our strong induction hypothesis, there exists two polynomials $q_2(x)$ and $r(x)$ so that $f_1(x) = q_2(x)g(x) + r(x)$ with $r(x) = 0$ or $\deg(r) < \deg(g)$. Thus 
\[
 f(x) - q_1(x)g(x) = q_2(x)g(x) + r(x)
\]
or if we let $q(x) = q_1(x) + q_2(x)$ then 
\[
 f(x) = q(x)g(x) + r(x)
\]
with $r(x) = 0$ or $\deg(r) < \deg(g)$.

(b) Suppose $f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$. If $q_1(x) \neq q_2(x)$ there exists some $b$ so that $q_1b \neq q_2b$, where $q_i = q_{a_i}x + \ldots + q_{ik}x^k$ for some $k$. If we continue with the expression for $f(x)$ and $g(x)$ that we established above, we have that $f_{b+m} = q_{1b}g_m = q_{2b}g_m$ since $\deg(r) < \deg(g) = m$ it cannot sum into any coefficient of $f$ greater than or equal to $m$. Since $R$ is a domain, we have right cancellation, so $q_{1b} = q_{2b}$ and thus $q_1(x) = q_2(x)$. Now, $f(x) - q_1(x)g(x) = r_1(x)$ and $f(x) - q_2(x)g(x) = r_2(x)$, so $r_1(x) = r_2(x)$. Therefore, if $R$ is a domain, the factorization is unique.

18. \(\Rightarrow\) From the definition of a field, the resulting operations follow.
\[\Leftarrow\] If we have a set $X$ that is closed under subtraction then it contains 0 since $a - a = 0$ and is also a group under addition (one of the characterizations of groups). Since the addition is commutative in $R$, it will also be in $X$. We are given the multiplicative identity, closure of multiplication and inverses and distributivity will follow from that of the ring. Therefore, $X$ is a subfield of $R$.

19. We have already shown that the intersection of a family of rings is still a ring. If these rings are commutative, then so will their intersection. So, it remains to show that we will have multiplicative inverses. Suppose $a \in \cap \alpha F_\alpha$ then $a \in F_\alpha$ for all $\alpha$. Since each $F_\alpha$ is a field there exists $a^{-1} \in F_\alpha$ so that $a(a^{-1}) = 1$. So $a^{-1} \in F_\alpha$ for all $\alpha$ and thus $a^{-1} \in \cap \alpha F_\alpha$. Therefore, the intersection of subfields is a subfield.

20. (a) Since $\mathbb{Z}_p$ is a domain by [1, Theorem 7], we have shown in Exercise 14 that $\mathbb{Z}_p[x]$ is a domain. The domain is infinite, if you consider the sequence of elements $x, x^2, x^3, \ldots$ From [1, Theorem 8], we know that $\mathbb{Z}_p$ is a field. In order to show it is a subfield, consider the constant terms of $\mathbb{Z}_p[x]$. It is clearly a ring as remarked in [1, p. 12 after Definition]. Notice that it is closed under multiplication, because multiplication of degree zero elements with sum to be of degree 0. Thus, it is enough to show that each non-zero element has a multiplicative inverse. Suppose $a \neq 0, a \in \mathbb{Z}_p[x]$ and $\deg(a) = 0$, then $a \in \mathbb{Z}_p$ so it has a multiplicative inverse $b$. Then $b \in \mathbb{Z}_p$ with $\deg(b) = 0$, where $ab = 1 \in \mathbb{Z}_p[x]$.

(b) The field of fractions $\mathbb{Z}_p(x)$ is an infinite field, since it contains $\mathbb{Z}_p[x]$, it contains $\mathbb{Z}_p$ as a subfield.

21. Suppose $R[x]$ is a field. Then there exists a polynomial $q(x) = q_0 + q_1x + \ldots + q_nx^n$ so that 
\[
 x(q(x)) = 1.
\]
However, by Exercise 12 we know that the constant terms of $xq(x)$ is simply $0(q_0) = 0 \neq 1$ since $R$ is a ring.
22. \( \Leftarrow \) This statement is shown in \([1, \text{Theorem 8}]\).

\( \Rightarrow \) If \( \mathbb{Z}_n \) is a field, then all non-zero elements are units. Thus the elements \( 1, \ldots, n-1 \) are units. By Exercise 11, the elements \( 1, \ldots, n-1 \) must be coprime to \( n \). Thus \( n \) has no elements less than it that divide it. Therefore, \( n \) is prime.

23. If \( R \) is a field, then we will prove that the map \( \phi : R \to \text{Frac}(R) \) given by \( a \mapsto \frac{a}{1} \) is an isomorphism.

We will then prove that if \( R \) is a domain and the map \( a \mapsto \frac{a}{1} \) is an isomorphism, then \( R \) is a field.

First, consider the map \( \phi : R \to \text{Frac}(R) \) given by \( a \mapsto \frac{a}{1} \). Then \( \phi(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \phi(a) + \phi(b) \). Likewise, we have

\[
\phi(ab) = \frac{ab}{1} = \frac{a b}{1} = \phi(a)\phi(b).
\]

Thus the map \( \phi \) is a homomorphism and it remains to show that it is a bijection. We know that \( \text{Frac}(R) = R \) since \( \text{Frac}(R) \) is the smallest field containing the subring \( R \), which in this case happens to be a field. We first show that \( \phi \) is onto. Let \( s = \frac{a}{b} \in \text{Frac}(R) \) be an arbitrary element in the field of fractions. Then, since \( R \) is a field, we know \( b^{-1} \in R \), and so is \( ab^{-1} \). If we take \( \phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \frac{a}{b} = \frac{a}{b} \). Thus \( \phi \) is onto. We now analyze the kernel of \( \phi \) and assume that \( \phi(s) = 0 \) for \( s \in R \). But this implies \( \phi(s) = \frac{s}{1} = 0 \) which means \( s = 0 \). Since \( \ker(\phi) = \{0\} \), we know that \( \phi \) is injective, and so it must be an isomorphism as well.

For the second step, we now show that if \( R \) is a domain and the map \( \phi : R \to \text{Frac}(R) \) given by \( a \mapsto \frac{a}{1} \) is an isomorphism, then \( R \) must be a field. First, choose any nonzero element \( a \in R \). Since \( \phi(a) = \alpha \in \text{Frac}(R) \), which is a field, there exists a \( \beta \in \text{Frac}(R) \) such that \( \alpha\beta = 1 \). Because \( \phi \) is bijective, there exists \( b \in R \) such that \( \phi(b) = \beta \). Then we have

\[
\phi(ab) = \phi(a)\phi(b) = \alpha \beta = 1.
\]

Because \( \phi \) is injective, we must have \( ab = 1 \), and thus every nonzero \( a \in R \) has a multiplicative inverse, and \( R \) is a field.

24. If \( \phi : R \to S \) is an isomorphism between domains, then we will show there exists an isomorphism between \( \text{Frac}(R) \) and \( \text{Frac}(S) \), namely \( \frac{a}{b} \mapsto \frac{\phi(a)}{\phi(b)} \). Let \( \psi(\frac{a}{b}) \to \frac{\phi(a)}{\phi(b)} \) and let \( \frac{a}{b} \) and \( \frac{c}{d} \) be elements of \( \text{Frac}(R) \). Then

\[
\psi\left(\frac{a}{b} + \frac{c}{d}\right) = \psi\left(\frac{ad + bc}{bd}\right) = \frac{\phi(ad + bc)}{\phi(bd)} = \frac{\phi(a) + \phi(c)}{\phi(b)} = \frac{\phi(a)}{\phi(b)} + \frac{\phi(c)}{\phi(d)}.
\]

Also,

\[
\psi\left(\frac{a}{b} \cdot \frac{c}{d}\right) = \frac{\phi(a)\phi(c)}{\phi(b)\phi(d)} = \frac{\phi(a)}{\phi(b)} \cdot \frac{\phi(c)}{\phi(d)} = \frac{\phi(a)}{\phi(b)} \cdot \frac{\phi(c)}{\phi(d)}.
\]

Now consider \( \frac{c}{d} \in \text{Frac}(S) \) and since \( \phi \) is an isomorphism, there exists \( a, b \in R \) such that \( \phi(a) = c \) and \( \phi(b) = d \). Then \( \psi(\frac{a}{b}) = \frac{c}{d} \) so \( \psi \) is onto. Lastly, if \( \frac{A}{B} = \frac{C}{D} \) and \( \frac{A}{B}, \frac{C}{D} \in \text{Frac}(S) \) with \( \phi(a) = A \ldots \phi(d) = D \), then

\[
\frac{A}{B} = \frac{C}{D} \Rightarrow \frac{\phi(a)}{\phi(b)} = \frac{\phi(c)}{\phi(d)} \Rightarrow \phi(ad) = \phi(bc).
\]
Since \( \phi \) is injective, we have
\[
\begin{align*}
    ad &= bc \\
    \frac{a}{b} &= \frac{c}{d}.
\end{align*}
\]
Thus \( \psi \) is an isomorphism between the fields of fractions.

25. Let \( R \) be a subring of a field \( F \) and \( K \) the intersection of all subfields of \( F \) containing \( R \) as a subring. Then \( K \) is isomorphic to \( \text{Frac}(R) \). To prove this, we show that the field of fractions of \( R \) is contained in the intersection of subfields of \( F \) containing \( R \) as a subring and vice-versa. Since \( R \) is contained in \( \text{Frac}(R) \), which is a field, we know that \( \text{Frac}(R) \subset \cap K_{\alpha} \) where \( K_{\alpha} \) are the subfields of \( F \) containing \( R \) as a subring. Now to show that \( \text{Frac}(R) \subset \cap K_{\alpha} \), consider the element \( \frac{a}{b} = ab^{-1} \in \text{Frac}(R) \). Since \( R \subset K_{\alpha} \), we must have \( a, b \in K_{\alpha} \forall \alpha \). Since each \( K_{\alpha} \) is field, we also know that \( b^{-1} \) must be in \( K_{\alpha} \) for all \( \alpha \). Thus
\[
ab^{-1} \in K_{\alpha}, \forall \alpha
\]
\[
\frac{a}{b} \in \cap K_{\alpha}.
\]
This means that \( \text{Frac}(R) \subset \cap K_{\alpha} \) and since both sets are subsets of each other, they must be equal.

26. (a) If \( \phi : R \to S \) is an isomorphism then \( \phi^{-1} : S \to R \) is also an isomorphism. Because \( \phi \) is a bijection, its inverse image is likewise a bijection, as it going to be both onto and one-to-one, which can be easily shown. Now, let \( \phi(a) = c \) and \( \phi(b) = d \). Then to evaluate \( \phi^{-1}(c + d) \) and \( \phi^{-1}(cd) \), we know that \( \phi(a + b) = c + d \), so \( \phi^{-1}(c + d) = a + b = \phi^{-1}(c) + \phi^{-1}(d) \). Similarly for multiplication, \( \phi(ab) = cd \), so \( \phi^{-1}(cd) = ab = \phi^{-1}(c)\phi^{-1}(d) \). This completes the proof that \( \phi^{-1} \) is an isomorphism.

(b) Now if \( \phi : R \to S \) is an isomorphism and \( \psi : S \to T \) is an isomorphism, then \( \psi \circ \phi : R \to T \) is also an isomorphism. First, \( \psi \circ \phi \) is clearly a bijection, since the bijection of a bijection is still going to be one-to-one and onto. Also, since \( \psi(\phi(a + b)) = \psi(\phi(a) + \phi(b)) = \psi(a) + \psi(b) \), where \( \phi(a) = A, \phi(b) = B, \psi(A) = \alpha, \) and \( \psi(B) = \beta \), we clearly that \( \psi \circ \phi \) is an additive homomorphism and it is likewise easily shown that it is a multiplicative homomorphism as well, as \( \psi(\phi(ab)) = \psi(AB) = \alpha \beta = \psi(\phi(a))\psi(\phi(b)) \). Thus it is an isomorphism.

27. If \( a \) is a unit in \( R \) and \( \phi : R \to S \) is a ring map, then \( \phi(a) \) is a unit in \( S \). Since \( a \) is a unit, we know there exists a \( b \in R \) such that \( ab = 1 \). Then
\[
\phi(ab) = \phi(a)\phi(b) = \phi(1) = 1
\]
Thus by definition \( \phi(a) \) is a unit in \( S \).

28. (a) If \( R \) is a ring, we want to prove that \( \phi : R[x] \to R \) where \( \phi : f(x) \mapsto c_0 \), the constant term of \( f(x) \) is a ring map. Let \( f(x) = f_0 + f_1 x + \ldots + f_n x^n \) and \( g(x) = g_0 + g_1 x + \ldots + g_m x^m \). Then \( \phi(fg) = \phi(f)\phi(g) \). For addition, we have \( \phi(f + g) = \phi(f) + \phi(g) \). Thus \( \phi \) is a ring homomorphism.

(b) The \( \ker(\phi) \) is the ideal generated by \( x \).

29. (a) If \( \sigma : R \to S \) is a ring map, we will prove that \( \sigma^* : R[x] \to S[x] \), defined by \( \sum r_i x^i \mapsto \sum \sigma(r_i) x^i \) is also a ring map. Letting \( f(x) \) and \( g(x) \) be two polynomials in \( R[x] \) with
\[
\begin{align*}
f(x) &= f_0 + \ldots + f_n x^n \\
g(x) &= g_0 + \ldots + g_m x^m
\end{align*}
\]
We then have
\[ \sigma^*(f + g) = \sum \sigma(f_i + g_i) x^i = \sum \sigma(f_i) x^i + \sum \sigma(g_i) x^i = \sigma^*(f) + \sigma^*(g) \]
This is true since \( \sigma \) itself is a ring map. Likewise, we have
\[ \sigma^*(fg) = \sum_{i+j=0}^{m+n} (f_i g_j) x^{i+j} = \sum_{i+j=0}^{m+n} \sigma(f_i) \sigma(g_j) x^{i+j} = \sum_{i=0}^{n} \sigma(f_i) x^i \sum_{j=0}^{m} \sigma(g_j) x^j = \sigma^*(f) \sigma^*(g) \]

(b) If \( \tau : S \to T \) is a ring map, we will show that \((\tau \sigma)^* : R[x] \to T[x]\) is equal to \(\tau^* \sigma^*\). By definition, we have
\[ (\tau \sigma)^*(f) : \sum f_i x^i \mapsto \sum \tau \sigma(f_i) x^i. \]
Then, again by definition, we have
\[ \tau^*(\sigma^*(f)) = \sum (\tau \sigma)(f_i) x^i = (\tau \sigma)^*(f) \]
(c) Lastly, we show that if \( \sigma \) is an isomorphism, then \( \sigma^* \) is an isomorphism as well. We first show that \( \sigma^* \) is one-to-one. Assume \( \sigma^*(f) = \sigma^*(g) \). Then
\[ \sum \sigma(f_i) x^i = \sum \sigma(g_i) x^i \]
Since \( \sigma \) is an isomorphism (and hence one-to-one), we must have \( f_i = g_i \) for each \( i \). Thus \( \sigma^* \) is one-to-one. Next, to show that that \( \sigma^* \) is onto, we choose an arbitrary polynomial in \( S[x] \), say \( s(x) = s_0 + s_1 x^1 + \ldots + s_n x^n \). Since \( \sigma \) is onto, there exists \( r_i \) such that \( \sigma(r_i) = s_i \) for each \( i \). Selecting these \( r_i \) and creating a polynomial \( r(x) \) from them, we find that
\[ \sigma^*(r(x)) = \sum \sigma(r_i) x^i = \sum s_i x^i = s(x) \]

30. (a) The intersection of any family of ideals in \( R \) is an ideal in \( R \). Consider the intersection of ideals \( I_\alpha \) and let \( a, b \in \cap I_\alpha \). Since \( (a - b) \in I_\alpha \) for each \( \alpha \) and since for any \( c \in R \), we have \( ca \in I_\alpha \) for each \( \alpha \), \( I \) satisfies the properties of an ideal and is thus an ideal. Let \( U = \cap X_\alpha \) where \( X_\alpha \) is an ideal containing \( X \). Then clearly \( U \) is the smallest ideal containing \( X \) since any smaller ideal, say \( Y \), containing \( X \) would reduce \( U \) as \( Y \subset U \implies Y = U \).

(b) The ideal generated by \( X \) is the smallest ideal containing \( X \) in the sense that any other ideal \( J \) containing \( X \) must contain \( (X) \). As discussed above, since \( (X) \) is the intersection of all ideals containing \( X \) it must be the smallest ideal containing \( X \) and if \( X \subset J \), then \( J = X_\alpha \) for some \( \alpha \) and then \( \cap X_\alpha \subset J \Rightarrow (X) \subset J \).

31. (a) If \( a \in R \), we will prove that \( \{ra : r \in R\} \) is the ideal generated by \( a \). Since the ideal generated by \( a \) must contain all elements of the form \( ra : r \in R \), the ideal generated by \( a \) must at least contain these elements. In fact, these elements are sufficient to create an ideal since the condition \( a, b \in I \Rightarrow (a - b) \in I \) is satisfied as \( r_1 a - r_2 a = (r_1 - r_2)a \) and \( (r_1 - r_2) \in R \) since \( R \) is a ring. Of course, \( 0 \in (a) \) as \( 0 \in R \) and \( 0a = 0 \).

(b) If \( a_1, \ldots, a_n \) are elements in a ring \( R \), the set of linear combinations,
\[ I = \{ r_1 a_1 + \ldots + r_n a_n : r_i \in R, i = 1, \ldots, n \} \]
is equal to the ideal generated by \( \{a_1, \ldots, a_n\} \). We can prove this statement by first observing that the ideal generated by \( \{a_1, \ldots, a_n\} \) must contain all elements of the form \( r_i a_i, r_i \in R \), based off of the second property of an ideal. By the first property of an ideal, it must contain the difference of elements in the ideals, which given the previous observation, means that the ideal generated by \( \{a_1, \ldots, a_n\} \) must contain all linear combinations of \( \{a_1, \ldots, a_n\} \).
Let $u$ be a unit in a ring $R$.

(a) We first prove that if an ideal $I$ contains $u$, then $I = R$. Since $u$ is a unit, there exists a $y \in R$ such that $uy = 1$. Then since $u \in I$, we must have $uy = 1 \in I$. But if $1 \in I$, then so must any $r \in R$ because $r \cdot 1 \in I$. Thus $I = R$.

(b) We next prove that if $r \in R$, then $(ur) = (r)$. Since $(ur) = \{aur : a \in R\}$ and since there exists $y \in R$ such that $yu = 1$, we must have $yur = r \in (ur)$ and thus all the elements of $(ur)$ must be in $(r)$. Likewise, all the elements of $(r)$ must be contained in $(ur)$ as $ur \in (r)$ by definition and so $(r) \subseteq (ur)$. Thus $(ur) = (r)$.

(c) Lastly, we show that if $R$ is a domain and $r, s \in R$ then $(r) = (s)$ if and only if $s = ur$ for some unit $u$ in $R$. We have already shown that if $s = ur$ for some unit $u \in R$, then $(r) = (s) = (ur)$. We now show the forward direction, that is $(r) = (s)$ implies $s = ur$ for some unit $u \in R$. Since $(r) = (s)$, there must be some $k \in R$ such that $r = ks$. Likewise, there must be some $j \in R$ such that $s = jr$. However, Exercise 15 shows that $j$ and $k$ must be units, and thus this theorem is proved.

We prove that a ring $R$ is a field if and only if it has only one proper ideal, namely, $\{0\}$. First assume $R$ is a field and has an ideal that contains a nonzero element, say $k$. Then by definition it must contain $1$ since $\frac{1}{k} \in R$ and once this ideal contains $1$, it must contain every element of $R$ and thereby be nonproper. Now if a ring has only one proper ideal, namely, $\{0\}$, we will show that $R$ must be a field. This is true because the ideal generated by any nonzero element $k$ of $R$ must be a nonproper ideal and so $(k) = R$. This implies that there is some $u \in R$ such that $uk = 1$ and that means that $k$ must be a unit. Thus every nonzero element of $R$ is a unit, and we have a field.

The set $I$ of all $f(x) \in \mathbb{Z}[x]$ having even constant term is an ideal in $\mathbb{Z}[x]$; it consists of all the linear combinations of $x$ and $2$; that is $I = (x, 2)$. This is true since multiplying an element of this set by any other element of $\mathbb{Z}[x]$ is still going to result in an element of the set $(x, 2)$ since an even constant multiplied by any integer is still going to be even. Likewise, subtraction of these elements is still going to remain in the set since subtraction of even constants remains even.

We want to show that there does not exist an element $k$ of $\mathbb{Z}[x]$ such that $(k) = (x, 2)$. If this element $k$ is constant, then it fails to generate $x$ since $\mathbb{Z}$ is a domain and any nonunit constant cannot multiply with a polynomial to obtain $x$. Thus this element $k$ must have degree greater than $0$, but $2 \notin (k)$ since the ring $\mathbb{Z}[x]$ is a domain and the product of polynomials in a domain must have degree equal to the sum of the degrees of the polynomials in the product. Thus $(2, x)$ cannot be a principal ideal.

We prove that if $F$ is a field and $S$ is a ring, then a ring map $\phi : F \to S$ must be an injection and $\text{im}(\phi)$ is a subfield of $S$ isomorphic to $F$. We do this by showing that $\ker(\phi) = 0$. Suppose that for $a \in F$ and $a \neq 0$, we have $\phi(a) = 0$. Since $F$ is a field, there exists $a^{-1} \in F$ such that $aa^{-1} = 1$. Then $1 = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) = 0 \cdot \phi(a^{-1}) = 0$.

This is a contradiction, and so $\phi$ must be an injection. Since $\phi$ is automatically a surjection to the $\text{im}(\phi)$, $\phi$ satisfies all the properties of an isomorphism and so $\text{im}(\phi)$ is isomorphic to $F$.

Let $I = (n)$ be the principal ideal in $\mathbb{Z}$ generated by $n$. We will prove that the quotient ring $\mathbb{Z}/I$ is equal to $\mathbb{Z}_n$. We begin by noting that the elements of the quotient ring $\mathbb{Z}/I$ are the cosets of the form $I, 1 + I, \ldots, (n - 1) + I$. These elements are the same as the elements in $\mathbb{Z}_n$, namely $[a] = a + I$ and addition and multiplication are precisely the same in both rings. Since both sets contain the same elements and have the same operations, the two rings are equal.
37. We next prove that if \( R \) is a ring and \( I = (x) \) is the principal ideal in \( R[x] \) generated by \( x \), then \( R[x]/I \cong R \). We know that \( I = (x) \) is the set of polynomials in \( R[x] \) that has a zero-constant term. The elements of \( R[x]/I \) are of the form \( c + I \) where \( c \in R \). Let \( \phi \) map \( f(x) + I \) to \( c \), where \( c \) is the constant term of \( f(x) \). That is \( \phi : \frac{R[x]}{I} \rightarrow R \) by \( \phi(f(x) + I) = c \). We first show that this map is well-defined. Let \( f(x) + I = g(x) + I \), so that \( \phi(f(x) + I) = c \) and \( \phi(g(x) + I) = d \), where \( c \) and \( d \) are the constant terms of \( f(x) \) and \( g(x) \) respectively. Since \( f(x) + I = g(x) + I \) and \( I \) is the principal ideal generated by \( (x) \), when we evaluate at \( x = 0 \), we have \( c + I = d + I \), which means that we must have \( c = d \).

We next claim this map is an isomorphism. First, since 
\[
\phi((f(x) + I) + (g(x) + I)) = \phi((f(x) + g(x)) + I) = c + d = \phi(f(x) + I) + \phi(g(x) + I)
\]
Also 
\[
\phi((f(x) + I)(g(x) + I)) = \phi(cd + (c_0d_1 + c_1d_0)x + \ldots + I) = \phi(cd + I) = cd = \phi(c + I)\phi(d + I)
\]
Thus \( \phi \) is a homomorphism. Now assuming \( c = d \) for two functions \( f(x) \) and \( g(x) \), it is obvious that \( c + I = d + I \) and is thus one-to-one. Likewise, since for any \( c \in R \) with polynomial \( f(x) \) having constant term \( c \), we know that \( \phi(f(x) + I) = c \), so clearly \( \phi \) is onto. Thus we have shown that \( \phi \) satisfies all the properties of an isomorphism and \( R[x]/I \cong R \).

38. We now go about proving the Correspondence Theorem for Rings, that is if \( I \) is a proper ideal in a ring \( R \), then there is a bijection from the family of all intermediate ideals \( J \), where \( I \subset J \subset R \), to the family of all ideals in \( R/I \), given by
\[
J \mapsto \pi(J) = J/I = \{a + I : a \in J\},
\]
where \( \pi : R \rightarrow R/I \) is the natural map. Moreover, if \( J \subset J' \) are intermediate ideals, then \( \pi(J) \subset \pi(J') \). Clearly the map \( \pi \) is a homomorphism, as it is the natural homomorphism between \( R \) and \( R/I \). We now check to see that it is a bijection. First, assume \( a + I = b + I \) where \( a, b \in J \). Since \( a, b \in J \), we know that \( a - b \in I \) and so \( \pi(a - b) = I = (a - b) + I \leftrightarrow a + I = b + I \). So \( \pi \) is injective. Next, we check that \( \pi \) is a surjection. Because \( J/I = \{a + I : a \in J\} \), any element in \( J/I \), say \( k + I \) where \( k \in J \), we instantly have the fact that \( \pi(k) = k + I \). So \( \pi \) is indeed onto and this completes the proof that \( \pi \) is a bijection.

For the second part of the theorem, we need to show that if \( J \subset J' \), then \( \pi(J) \subset \pi(J') \). We know that \( \pi(J) = \{a + I : a \in J\} \) and \( \pi(J') = \{b + I : b \in J'\} \). Choose any element of \( \pi(J) \), say \( a + I \) where \( a \in J \). Since \( a \in J \), it is also in \( J' \), and so the element \( a + I \) must be in \( \pi(J') \). This proves that \( \pi(J) \subset \pi(J') \).

39. Let \( I \) be an ideal in a ring \( R \), let \( J \) be an ideal in a ring \( S \), and let \( \phi : R \rightarrow S \) be a ring isomorphism with \( \phi(I) = J \). We will prove that the function \( \bar{\phi} : r + I \mapsto \phi(r) + J \) is a well-defined isomorphism \( R/I \rightarrow S/J \). Assume \( r + I = t + I \), where \( r, t \in R \). Then \( \bar{\phi}(r + I) = \phi(r) + J \) and \( \bar{\phi}(t + I) = \phi(t) + J \).
Since \( \phi(r) - \phi(t) = \phi(r - t) \in J \) (as \( r - t \in I \), we must have \( \phi(r) + J = \phi(t) + J \). Thus the map is well-defined. It is a homomorphism since
\[
\bar{\phi}((r + I) + (t + I)) = \bar{\phi}(r + t + I) = \phi(r + t) + J = \phi(r) + J + \phi(t) + J = \bar{\phi}(r + I) + \bar{\phi}(t + I)
\]
Similarly,
\[
\bar{\phi}((r + I)(t + I)) = \bar{\phi}(rt + I) = \phi(rt) + J = (\phi(r) + J)(\phi(t) + J) = \bar{\phi}(r + I)\bar{\phi}(t + I)
\]
Now we check that \( \bar{\phi} \) is a bijection. Assume \( \phi(r) + J = \phi(t) + J \). Then \( \phi(r - t) \in J \), so because \( \phi \) is an isomorphism, we know that \( (r - t) \in I \) and thus \( r + I = t + I \). To show it is a surjection, take any element in \( S/J \), say \( k + J \), where \( k \in S \). Because \( \phi \) is a ring isomorphism, we know there exists \( a \in R \) such that \( \phi(a) = k \). Applying our new map \( \bar{\phi} \) on this coset, we find

\[
\bar{\phi}(a + I) = \phi(a) + J = k + J
\]

This proves that \( \bar{\phi} \) is in fact an well-defined isomorphism.

40. We will show that there exists domains \( R \) containing a pair of elements having no gcd. Consider a field \( F \) and let \( R \) be the subring of \( F[x] \) consisting of no linear terms. Then the elements \( x^5 \) and \( x^6 \) have as common monic factors \( 1, x^2 \), and \( x^3 \). However, none of these factors are divisible by the other two (\( x^3 \) is not divisible by \( x^2 \) since \( x \) is not in \( R[x] \)), and so the conditions for the gcd are not satisfied and the theorem is proved.

41. (a) We prove that the gcd of integers \( a_1, a_2, \ldots, a_n \), defined as the positive integer \( d \) which is the common divisor of all the \( a_i \) that is divisible by all common divisors, exists and is a linear combination of \( a_1, a_2, \ldots, a_n \). Let \( d \) denote the positive generator of the ideal generated by \( a_1, \ldots, a_n \). By exercise 31, \( d \) can be written as a linear combination

\[
d = c_1 a_1 + \ldots + c_n a_n
\]

where the \( c_i \in \mathbb{Z} \). Each \( a_i \) must clearly be in the ideal generated by \( (d) \), which implies that \( b_i d = a_i, \) or in other words, \( d|a_i \). This shows that \( d \) is a divisor of \( a_i \) for all \( i \). Now suppose there exists a \( b \) such that \( b|a_i, \forall i \). Then \( b|(c_1 a_1 + \ldots + c_n a_n) \) which means \( b|d \), and so \( d \) is indeed the greatest common divisor.

(b) Define the gcd of polynomials \( f_1, \ldots, f_n \in F[x] \), where \( F \) is a field to be a monic polynomial \( d \) which is a common divisor of each \( f_i \) and that is divisible by every common divisor. We generalize Corollary 16 that the gcd \( d \) of \( f_1, \ldots, f_n \) exists and that \( d \) is a linear combination of \( f_1, \ldots, f_n \). First, we know that by Theorem 14, for \( n = 2 \), the gcd is well-defined and is a linear combination of \( f_1 \) and \( f_2 \). Using induction, assume the gcd is well-defined and is a linear combination for \( f_1, \ldots, f_{n-1} \), so \( f = \text{gcd}(f_1, \ldots, f_{n-1}) = c_1 f_1 + \ldots + c_{n-1} f_{n-1} \). Then the gcd of \( f \) and \( f_n \), call it \( d \), is a linear combination of \( f \) and \( f_n \), which implies that \( d \) is a linear combination of \( f_1, \ldots, f_n \). Clearly \( d|f_i, \forall i \). Assume there exists some \( b \) such that \( b|f_i, \forall i \). Then

\[
b|(c_1 f_1 + \ldots + c_n f_n)
\]

and so \( b|d \) and \( d \) is therefore the gcd.

42. If \( a_1, \ldots, a_n \) are distinct elements in a field \( F \), the for all \( i \), the polynomials \( x - a_{i+1} \) and \( (x - a_1)(x - a_2 \ldots (x - a_i) \) are relatively prime. By Corollary 21, the only monomial that divides \( (x - a_{i+1}) \) is \( (x - a_1). \) The only monomials dividing \( f(x) = (x - a_1)(x - a_2) \ldots (x - a_i) \) are the monomials \( (x - a_1), \ldots, (x - a_i) \). Since \( a_{i+1} \neq a_i, \forall i, (x - a_{i+1}) \) and \( f(x) \) must be relatively prime.

43. Since \( \mathbb{Z} \) is an integral domain, we know that \( \partial(x f(x)) \geq 1 \), so \( x f(x) \neq 2 \forall f(x) \in \mathbb{Z}[x] \). Likewise, since \( 2(a_0 + a_1 x + \ldots + a_n x^n) = 2a_0 + 2a_1 x + \ldots + 2a_n x^n \neq x \), we must have \( 2 \) and \( x \) being relatively prime. Now let

\[
f(x) = f_0 + f_1 x + \ldots + f_n x^n
\]
\[
g(x) = g_0 + g_1 x + \ldots + g_n x^n.
\]

Consider the sum

\[
xf(x) + 2g(x)
\]
\[ f(x) = f_0x + f_1x + \ldots + f_nx^{n+1} + 2g_0 + 2g_1x + \ldots + 2g_nx^n \]
\[ = 2g_0 + (f_0 + 2g_1)x + \ldots + (f_{n-1} + 2g_n)x^n + f_nx^{n+1}. \]

Setting this equation equal to 1, we quickly find there are no solutions in \( \mathbb{Z} \), as this would require \( g_0 = \frac{1}{2} \).

44. Let \( f(x) = \prod (x - a_i) \in F[x] \), where \( F \) is a field and \( a_i \in F \) for all \( i \). We claim that \( f(x) \) has no repeated roots if and only if \( (f(x), f'(x)) = 1 \), where \( f'(x) \) is the derivative of \( f(x) \). First suppose \( f(x) \) has one repeated root, so \( f(x) = (x - a_1)^2(x - a_2)\ldots(x - a_n) \). Taking the derivative and regrouping, we have \( f'(x) = 2(x-a_1)(x-a_2)\ldots(x-a_n)+\ldots+(x-a_1)^2(x-a_3)\ldots(x-a_n)+\ldots+(x-a_1)^2\ldots(x-a_{n-1}) \). Since \( (x-a_1) \) divides each of the terms in this sum, it divides the sum and shows that \( (f(x), f'(x)) \neq 1 \). For the converse, assume \( f(x) = (x - a_1)(x - a_2)\ldots(x - a_n) \) where the \( a_i \) are distinct. Taking the derivative and regrouping we have \( f'(x) = (x - a_2)\ldots(x - a_n)+\ldots+(x - a_1)\ldots(x - a_{n-1}) \). Each monomial \( (x - a_i) \) fails to divide this derivative since it divides every term in the sum except for one term, which will always leave a remainder. This means that that \( (f(x), f'(x)) = 1 \) since these monomials are precisely the divisors of \( f(x) \).

45. Using basic polynomial division and the Euclidean algorithm, we find the gcd of \( x^3 - 2x^2 + 1 \) and \( x^2 - x - 3 \) in \( \mathbb{Q} \). Dividing \( x^3 - 2x^2 + 1 \) by \( x^2 - x - 3 \), we obtain the quotient \( x - 1 \) with remainder \( 2x - 2 \). Next we divide \( x^2 - x - 3 \) by \( 2x - 2 \) to get the quotient \( \frac{1}{2}x \) with remainder \(-3\). This implies
\[
x^3 - 2x^2 + 1 = (x^2 - x - 3)(x - 1) + (2x - 2)
\]
\[
x^2 - x - 3 = (2x - 2)\left(\frac{1}{2}x\right) - 3
\]
\[
-3 = (1 - \frac{1}{2}x - \frac{1}{2} \cdot x^2)(x^2 - x - 3) - (\frac{1}{2}x)(x^3 - 2x^2 + 1)
\]
\[
1 = (-\frac{1}{3} + \frac{1}{6}x + \frac{1}{6} \cdot x^2)(x^2 - x - 3) + (\frac{1}{6}x)(x^3 - 2x^2 + 1)
\]

Thus the gcd of these two polynomials in \( \mathbb{Q} \) is 1.

46. In order to show that \( \mathbb{Z}_2[x]/(x^3 + x + 1) \) is a field, we first note that addition is given component wise, so is an abelian group isomorphic to the direct product of three \( \mathbb{Z}_2 \). The multiplication will still be commutative, as induced from \( \mathbb{Z}_2[x] \) with 1 as the unity. So, the task it really to show that each non-zero element has an inverse.

\[ 1^1 = 1 \]
\[ x(1 + x^2) = x + x^3 = x + x + 1 = 1 \]
\[ x^2(1 + x + x^2) = x^2 + x^3 + x^4 = x^2 + x + 1 + x(x + 1) = 2x^2 + 2x + 1 = 1 \]
\[ (1 + x)(x + x^2) = x + x^2 + x^2 + x^3 = x + x + 1 = 1 \]

Therefore, each element has a multiplicative inverse and \( \mathbb{Z}_2[x]/(x^3 + x + 1) \) is a field.
47. If \( R \) is a ring and \( a \in R \), let \( e_a : R[x] \to R \) be evaluation at \( a \). We prove that \( \ker e_a \) consists of all polynomials over \( R \) having \( a \) as a root, and so \( \ker e_a = (x - a) \), the principal ideal generated by \( x - a \). Consider \( f(x) = (x - r_1)(x - r_2) \ldots (x - r_n)g(x) \in R[x] \), where the \( r_i \) are roots in \( F \) and \( g(x) \) is an irreducible polynomial in \( F \). To have \( e_a(f(x)) = 0 \), we must have for some \( a = r_i \) for some \( i \) by Corollary 21. This immediately implies that the \( \ker e_a \) consists of all polynomials that have \( x - a \) as a factor, and this is equivalent to the principal ideal generated by \( (x - a) \).

48. Let \( F \) be a field and let \( f, g \in F[x] \). We will prove that if \( \partial(f) \leq \partial(g) = n \) and if \( f(a) = g(a) \) for \( n + 1 \) elements \( a \in F \), then \( f(x) = g(x) \). To prove this, we first let \( h(x) = g(x) - f(x) \) which must have \( \partial(h(x)) \leq n \). Since \( h(a) = g(a) - f(a) = 0 \), we see that \( (x - a) \) is a divisor of \( h(x) \) for all \( n + 1 \) elements \( a \in F \). But this implies that \( h(x) \) either is identically zero or has degree \( n + 1 \), which would be a contradiction to our previous statement. Thus \( h(x) \) must be everywhere 0, and this means that \( f(x) = g(x) \).

49. We prove that a polynomial \( p(x) \in F[x] \) of degree 2 or 3 is irreducible over \( F \) if and only if \( F \) contains no root of \( p(x) \). First, for the forward direction, assume \( p(x) \) is irreducible and of degree 2 or 3. Assume by way of contradiction that \( F \) contains a root of \( p(x) \), call it \( a \). Then by Corollary 21, the first degree polynomial \( x - a \) divides \( p(x) \) and this proves that \( p(x) \) is not irreducible. To prove the converse, assume that for a polynomial \( p(x) \) of degree 2 or 3, the field \( F \) contains no root of \( p(x) \). By Corollary 21 again, since \( F \) contains no roots of \( p(x) \), there can be no first degree polynomial divisors of \( p(x) \). Thus any polynomial dividing \( p(x) \) must have degree greater than 2, which implies that \( p(x) \) is irreducible if it is of degree 2. If \( p(x) \) is of degree 3 and has a divisor of degree 2, then the other factor is of degree 1, which is a contradiction. Thus \( p(x) \) is irreducible if it is of degree 2 or 3.

50. Let \( p(x) \in F[x] \) be an irreducible polynomial. If \( g(x) \in F[x] \) is not constant, then we will show that either \( (p(x), g(x)) = 1 \) or \( p(x) | g(x) \). Since the gcd of \( p(x) \) and \( g(x) \) must divide \( p(x) \), it must be constant or equal to \( p(x) \) since \( p(x) \) is irreducible. If it is constant, it must be equal to 1, since \( g(x) \) is a non-constant polynomial and the gcd must be monic. If the gcd is simply \( p(x) \), then clearly it divides \( g(x) \) since it divides both \( p(x) \) and \( g(x) \) by its very definition.

51. (a) Every nonzero polynomial \( f(x) \) in \( F[x] \) has a factorization of the form

\[
f(x) = ap_1(x) \ldots p_t(x),
\]

where \( a \) is a nonzero constant and the \( p_i(x) \) are (not necessarily distinct) monic irreducible polynomials. Either \( f(x) \) is irreducible or it is not. If it is, we are done. Assume it is reducible, so there is a factorization \( f(x) = p_1(x)p_2(x) \) where \( p_1(x) \) and \( p_2(x) \) are of lesser degree than \( f(x) \) and non-constants. Using induction, we can continue this argument until all the \( p_i(x) \) are irreducible, proving our assertion.

(b) We now show that the factors and multiplicities of \( f(x) \) are uniquely determined. Assume there are two factorizations of \( f(x) \), say

\[
f(x) = ap_1(x) \ldots p_t(x)
\]

and

\[
f(x) = bq_1(x) \ldots q_s(x).
\]

Then, since \( p_1(x) \) divides \( f(x) \), it must divide one of the \( q_i(x) \), and we can reorder the \( q_i(x) \) so that \( p_1(x) | q_1(x) \). Since \( q_1(x) \) is irreducible and monic, we must have \( p_1(x) = q_1(x) \). Continuing this argument, we induct and conclude that the factors and their multiplicities are indeed unique.
52. Let \( f(x) = \sum_{i=0}^{k_1} a_i x^{k_1i} \) and \( g(x) = \sum_{i=0}^{k_2} b_i x^{k_2i} \), where \( k_i \geq 0 \), \( a_i, b_i \) are nonzero constants, and the \( p_i(x) \) are distinct monic irreducible polynomials. We prove that
\[
\mu(x) = p_1(x)^{m_1} \cdots p_i(x)^{m_i} = \gcd(f, g)
\]
and
\[
\lambda(x) = p_1(x)^{M_1} \cdots p_i(x)^{M_i} = \text{lcm}(f, g),
\]
where \( m_i = \min\{k_i, n_i\} \) and \( M_i = \max\{k_i, n_i\} \). Clearly, \( \mu(x) \) divides \( f(x) \) and \( g(x) \), and likewise \( f(x) \) and \( g(x) \) both divide \( \lambda(x) \), and both \( \mu(x) \) and \( \lambda(x) \) are monic. We want to show that
\[
\gcd\left( \frac{f(x)}{\mu(x)}, \frac{g(x)}{\mu(x)} \right) = 1.
\]
We then have
\[
\frac{f(x)}{\mu(x)} = p_1^{k_1-m_1} \cdots p_i^{k_i-m_i} \quad \text{and} \quad \frac{g(x)}{\mu(x)} = p_1^{n_1-m_1} \cdots p_i^{n_i-m_i}.
\]
Since each polynomial is irreducible, they and some of their powers are the only possible divisors of \( \frac{f(x)}{\mu(x)} \) and \( \frac{g(x)}{\mu(x)} \). However, any \( p_i(x) \) in the product of \( \frac{f(x)}{\mu(x)} \) cannot be in the product of \( \frac{g(x)}{\mu(x)} \), since that would imply that \( m_i \neq \min\{k_i, n_i\} \), a contradiction to how we defined the \( m_i \).
This proves that \( \mu(x) \) is the gcd of \( f(x) \) and \( g(x) \). Likewise, for the lcm, we want to show that
\[
\text{lcm}\left( \frac{\lambda(x)}{f(x)}, \frac{\lambda(x)}{g(x)} \right) = 1.
\]
By a similar argument, any common divisor (other than 1) would contradict the fact \( M_i = \max\{k_i, n_i\} \), and thus \( \lambda(x) \) is in fact the lcm of \( f(x) \) and \( g(x) \).

53. (a) We prove that the zero ideal in a ring \( R \) is a prime ideal if and only if \( R \) is a domain. First, assume that the zero ideal in a ring is a prime ideal. Then if \( ab \in (0) \), then either \( a \in (0) \) or \( b \in (0) \). Since \( (0) = \{0\} \), this means that either \( a = 0 \) or \( b = 0 \), or in other words, there are no zero divisors, or that \( R \) is a domain. For the converse, assume that \( R \) is a domain and consider the zero ideal in this ring. Since there are no zero divisors, if \( ab = 0 \), we must have \( a = 0 \) or \( b = 0 \). This proves that the zero divisor is a prime ideal.

(b) Next, we show that the zero ideal in a ring \( R \) is maximal if and only if \( R \) is a field. By Theorem 26, we know that a proper ideal in a ring \( R \) is a maximal ideal if and only if \( R/I \) is a field. When \( I \) is the zero ideal, this theorem becomes the above statement since \( R/(0) \cong R \).

54. The ideal \( I \) in \( \mathbb{Z}[x] \) consisting of all polynomials having even constant term is a maximal ideal. This is the ideal generated by 2 and \( x \), so \( I = (2, x) \). We look at the quotient ring \( \mathbb{Z}[x]/(2, x) \) and prove that this is isomorphic to the field \( \mathbb{Z}_2 \). Every element of \( \mathbb{Z} \) not in \( I = (2, x) \) can be written as an element of the coset \( 1 + I \), as this coset contains all polynomials with an even constant term. Therefore, there are only two cosets in the quotient ring \( \mathbb{Z}/(2, x) \) which implies \( \mathbb{Z}/(2, x) \cong \mathbb{Z}_2 \), which is of course a field. By Theorem 26 then, \( I = (2, x) \) is a maximal ideal.

55. Let \( f(x), g(x) \in F[x] \). Then \( (f, g) \neq 1 \) if and only if there is a field \( E \) containing both \( F \) and a common root of \( f(x) \) and \( g(x) \). Let \( \mu = \gcd(f, g) \) and let \( q \) be an irreducible factor of \( \mu \). Then by Corollary 29, the quotient ring \( F[x]/(q(x)) \) is a field containing an isomorphic copy of \( F \) and a root of \( q(x) \). If \( \mu(x) \neq 1 \), then by Corollary 29, there is a field \( E' \) such that \( E' \cong F[x]/(q(x)) \) that contains \( F \) and a root of \( q(x) \), which is a common root of both \( f(x) \) and \( g(x) \) since it is an irreducible factor of their gcd. On the other hand, if \( \gcd(f, g) = 1 \), then since \( f \) and \( g \) can be written as a factorization of monic irreducible polynomials, \( f \) and \( g \) do not share any common roots in any field, and thus there is no field \( E \) containing both \( F \) and a common root of \( f \) and \( g \).

56. (a) We prove that if \( f(x) \in \mathbb{Z}_p[x] \), then \( (f(x))^p = f(x^p) \). Let \( f(x) = a_0 + a_1 x + \ldots + a_n x^n \). Then by Lemma 32, we have
\[
(f(x))^p = (a_0 + a_1 x + \ldots + a_n x^n)^p = a_0^p + \ldots + a_n^p x^{np} = a_0 + a_1 x^p + \ldots + a_n x^{np} = f(x^p)
\]
(In this process, we used Fermat’s Little Theorem.)
(b) The above theorem may not be true if \( \mathbb{Z}_p \) is replaced by any infinite field of characteristic \( p \). For example, if we consider the field of fractions \( \text{Frac}(\mathbb{Z}_p[x]) \), then its polynomial ring \( \text{Frac}(\mathbb{Z}_p[x])[y] \) does not satisfy the above property. For instance, \( f(y) = xy \) and \( f(y)^p = x^p y^p \), while \( f(y') = xy \) and \( x^p y^p \neq xy^p \).

57. The field of fractions of \( \mathbb{Z}_p[x] \) is an infinite field and has characteristic \( p \) as \( \mathbb{Z}_p \) is its prime subfield.

58. If \( F \) is a field, we will prove that the kernel of any evaluation map \( F[x] \to F \) is a maximal ideal.

For any \( f(x) = f_0 + f_1 x + \ldots + f_n x^n \), let \( \phi_\alpha(f(x)) = f_0 + f_1 \alpha + \ldots + f_n \alpha^n \). Then the kernel of \( \phi_\alpha \) is given by all polynomials where \( \alpha \) is a root, that is \( \ker(\phi_\alpha) = (x - \alpha) \). By Corollary 29, since \( (x - \alpha) \) is irreducible, we have that \( F[x]/\ker(\phi_\alpha) \) is a field, and then by Theorem 26, \( \ker(\phi_\alpha) \) must be maximal.

59. If \( F \) is a field of characteristic 0 and \( p(x) \in F[x] \) is irreducible, then \( p(x) \) has no repeated roots. We will prove this by proving the contrapositive of this statement. By exercise 44, we know that if \( p(x) \) has multiple roots, then \( (p(x), p'(x)) \neq 1 \). But if \( (p(x), p'(x)) \) does not equal 1, then clearly \( p(x) \) is not irreducible. This concludes the proof of the theorem.

60. In this exercise, we use Kronecker’s theorem to construct a field with four elements by adjoining a root of \( x^3 - x \) to \( \mathbb{Z}_2 \). We first factor \( x^3 - x \), which can be factored into irreducibles as \( x(x - 1)(x^2 + x + 1) \). By Corollary 29, \( \mathbb{Z}_2[x]/(x^2 + x + 1) \) is a field. The elements of this field are \( \{0, 1, x, 1 + x\} \). The additive subgroup of this field is isomorphic to the Klein-4 group \( V \), while the multiplicative subgroup of the nonzero elements is isomorphic to \( \mathbb{Z}_3 \).

61. We now construct a field with eight elements and provide the addition and multiplication tables by again using Kronecker’s Theorem, this time adjoining a suitable root of \( x^8 - x \) over \( \mathbb{Z}_2 \). First, factoring \( x^8 - x \) into irreducibles, we have \( x^8 - x = x(x - 1)(x^2 + x^2 + 1)(x^2 + x + 1) \) in \( \mathbb{Z}_2 \). Now again by Corollary 29, we know that \( \mathbb{Z}_2[x]/(x^2 + x + 1) \) is a field, with the following elements: \( \{0, 1, x, 1 + x, x^2, 1 + x^2, x + x^2, 1 + x + x^2\} \). The addition table is as follows:

\[
\begin{array}{cccccccc}
+ & 0 & 1 & x & 1+x & x^2 & 1+x^2 & x+x^2 & 1+x+x^2 \\
0  & 0 & 1 & x & 1+x & x^2 & 1+x^2 & x+x^2 & 1+x+x^2 \\
1  & 1 & 0 & 1+x & x & 1+x^2 & x^2 & 1+x^2 & x+x^2 \\
x  & x & 1+x & 0 & 1 & x & 1+x^2 & x^2 & 1+x^2 \\
1+x & 1+x & x & 1 & 0 & 1+x & x+x^2 & 1+x & x^2 \\
x^2 & x^2 & 1+x^2 & x+x^2 & 1+x^2 & 0 & 1 & x & 1+x \\
1+x^2 & 1+x^2 & x^2 & 1+x & x^2 & x+x^2 & 1 & 0 & 1+x \\
x+x^2 & x+x^2 & 1+x & x^2 & x & 1+x & 0 & 1 \\
1+x+x^2 & 1+x+x^2 & x^2 & 1+x^2 & x & 1 & 0 & \\
\end{array}
\]

The multiplication table is given below:

\[
\begin{array}{cccccccc}
* & 1 & x & 1+x & x^2 & 1+x^2 & x+x^2 & 1+x+x^2 \\
1 & 1 & x & 1+x & x^2 & 1+x^2 & x+x^2 & 1+x+x^2 \\
x & x & x^2 & 1+x & x^2 & 1+x^2 & x+x^2 & 1+x+x^2 \\
1+x & 1+x & x+x^2 & 1+x^2 & x & x+x^2 & 1+x+x^2 & 1+x \\
x^2 & x^2 & 1+x & x^2 & x & 1+x & x+x^2 & x \\
1+x^2 & 1+x^2 & x & 1+x & x^2 & x & 1+x & x+x^2 \\
x+x^2 & x+x^2 & x & 1 & 1+x^2 & x & x & x \\
1+x+x^2 & 1+x+x^2 & x & 1 & 1+x^2 & x & x & x \\
\end{array}
\]
62. It is impossible for a field with four elements to be isomorphic to a subfield field with eight elements. This is simply because the multiplicative subgroups would have to be isomorphic, but we know that they must isomorphic to $\mathbb{Z}_3$ and $\mathbb{Z}_7$, respectively, and there are no subgroups of $\mathbb{Z}_7$ isomorphic to $\mathbb{Z}_3$. Thus the original assertion is proven.

63. Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$. If $r/s$ is a rational root of $f(x)$, where $r/s$ is in lowest terms, i.e., $(r, s) = 1$, then $r | a_0$ and $s | a_n$. Since $r/s$ is a root, we know that $(sx - r)g(x) = f(x)$, where $g(x)$ is a polynomial of degree $n - 1$. By Theorem 39 (Gauss), we know that $g(x) \in \mathbb{Z}[x]$. Let $g(x) = g_0 + g_1 x + \ldots + g_n x^n$. Then $sg_n = a_n$, or $s | a_n$ and $-rg_0 = a_0$ or $r | a_0$.

64. We test whether the following polynomials factor in $\mathbb{Q}[x]$.

(a) The polynomial $3x^2 - 7x - 5$ does not factor in $\mathbb{Q}[x]$, since the map $\sigma : \mathbb{Z} \to \mathbb{Z}_2$ maps the polynomial to $x^2 - x - 1$, which has no roots in $\mathbb{Z}_2[x]$, and since the conditions for Theorem 34 are met, the polynomial $3x^2 - 7x - 5$ is irreducible in $\mathbb{Q}[x]$.

(b) The polynomial $6x^3 - 3x - 18$ is irreducible in $\mathbb{Q}[x]$, since under the map $\sigma : \mathbb{Z}[x] \to \mathbb{Z}_11[x]$, the polynomial $6x^3 - 3x - 7$ has no roots in $\mathbb{Z}_11$.

(c) The polynomial $x^3 - 7x + 1$ does not factor in $\mathbb{Q}[x]$, since the map $\sigma : \mathbb{Z}[x] \to \mathbb{Z}_2[x]$ sends our polynomial to $x^3 - x - 1$, which has no roots in $\mathbb{Z}_2[x]$.

(d) Again, the polynomial $x^3 - 9x - 9$ is irreducible in $\mathbb{Q}[x]$ since under the map $\sigma : \mathbb{Z}[x] \to \mathbb{Z}_2[x]$, the polynomial $x^3 - x - 1$ has no roots in $\mathbb{Z}_2[x]$.

65. Let $F$ be a field. We prove that if $a_0 + a_1 x + \ldots + a_n x^n \in F[x]$ is irreducible, then so is $a_n + a_{n-1} x + \ldots + a_0 x^n$. Equivalently, if $a_n + a_{n-1} x + \ldots + a_0 x^n$ is reducible, then so is $a_0 + a_1 x + \ldots + a_n x^n$. Since $a_n + a_{n-1} x + \ldots + a_0 x^n$ is reducible, we set it equal to $f(x)g(x)$, where $f(x) = f_0 + f_1 x + \ldots + f_k x^k$ and $g(x) = g_0 + g_1 x + \ldots + g_{n-k} x^{n-k}$, and $0 < k < n$. Then, we must have $f_0 g_0 = a_n$, $f_0 g_1 + f_1 g_0 = a_{n-1}$, \ldots, $f_k g_{n-k} = a_0$, and in general,

$$a_j = \sum_{r+s=j-n} f_r g_s.$$

Now if we let $f^*(x) = a_k + a_{k-1} x + \ldots + a_0 x^k$ and $g^*(x) = g_{n-k} + g_{n-k-1} x + \ldots + g_0 x^{n-k}$, then the product $f^*(x)g^*(x) = a_0 + a_1 x + \ldots + a_n x^n$, which completes the proof that $a_0 + a_1 x + \ldots + a_n x^n$ is reducible.

66. If $c \in R$, where $R$ is a ring, then the map $f(x) \mapsto f(x + c)$ is an isomorphism of the ring $R[x]$ with itself. Let $\phi_c(x) = f(x + c)$. We first check the homomorphism property:

$$\phi_c(f(x) + g(x)) = \phi_c((f + g)(x)) = (f + g)(x + c) = f(x + c) + g(x + c)$$

$$\phi_c(f(x)g(x)) = \phi_c((fg)(x)) = (fg)(x + c) = f(x + c)g(x + c)$$

Next, we check to see that $\phi_c$ is surjective and injective. For surjectivity, let $f(x)$ be an arbitrary $n^{th}$ degree polynomial in $R[x]$. We want to show that there exists a polynomial $g(x)$ of degree $n$ such that $g(x + c) = f(x)$. Expanding $g(x + c)$ and matching coefficients with $f(x)$, we obtain $n + 1$ equations with $n + 1$ unknowns, and a solution to this system exists because the coefficient matrix is upper-triangular echelon with determinant 1.

Now we must show that $\phi_c$ is injective. Let $\phi_c(f(x) = \phi_c(g(x))$. Then $f(x + c) = g(x + c)$, and making the substitution $u = x + c$, we have

$$f_0 + f_1 u + \ldots + f_n u^n = g_0 + g_1 u + \ldots + g_n u^n.$$
This equation implies $f_0 = g_0, f_1 = g_1, \ldots, f_n = g_n$, and so $f(x) = g(x)$ as we initially wanted to show. Thus $\phi_\epsilon$ is indeed an isomorphism from $R[x]$ to itself.

Since $\phi_\epsilon$ is an isomorphism, if $p(x)$ is a reducible polynomial in $R[x]$, then $p(x+c)$ is likewise reducible, since $\phi_\epsilon(p(x)) = \phi_\epsilon(f(x)g(x)) = \phi_\epsilon(f(x))\phi_\epsilon(g(x)) = f(x+c)g(x+c)$ where $f(x), g(x)$ each are of degree less than the degree of $p(x)$ but both greater than 1. Likewise if $p(x+c)$ is reducible, then $p(x)$ is also reducible. This follows as before:

$$\phi_\epsilon^{-1}(p(x+c)) = \phi_\epsilon^{-1}(f(x)g(x)) = \phi_\epsilon^{-1}(f(x))\phi_\epsilon^{-1}(g(x)) = f(x-c)g(x-c).$$

67. We show that $f(x) = x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Q}[x]$. By exercise 63, we conclude that $f(x)$ has no rational roots. We next factor $f(x)$ as $f(x) = x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 - ax + c)$. We want to show that this there are no rationals satisfying this factorization of $f(x)$. Expanding this factorization and equating coefficients, we obtain the following system of equations:

$$-10 = c + b - a^2$$
$$a(c - b) = 0$$
$$bc = 1$$

From the second equation, either $a = 0$ or $b = c$ (since $\mathbb{Q}$ is in integral domain). If $a = 0$, then solving the other two equations (using the quadratic equation), we find that either $b$ or $c$ must be irrational. If, on the other hand, $c = b$, then $b = c = 1$ or $b = c = -1$. If $b = c = 1$, then we must have $a^2 = 12$, making $a$ irrational. If $b = c = -1$, then $a^2 = 8$, and again $a$ is irrational. Thus there are no rationals satisfying the factorization of $f(x)$ and $f(x)$ must indeed be irreducible.

68. Given numbers $u$ and $v$, there exists numbers (possibly complex) $y$ and $z$ such that

$$y + z = u$$
$$yz = v$$

We first choose a $y$ value by solving the quadratic $y^2 - uy + v = 0$, where $u$ and $v$ are given. Then

$$y = \frac{u + \sqrt{u^2 - 4v}}{2}.$$  We now set $z = u - y$. Multiplying this equation by $y$, we have $yz = uy - y^2$, and from how we originally defined $y$, we must have $yz = v$.

69. Since 3 is a root of $x^3 + x^2 - 36$, we quickly factor it into $(x - 3)(x^2 + 4x + 12)$. The factor on the right is irreducible since under the map $\sigma: \mathbb{Z} \rightarrow \mathbb{Z}_5[x]$, we obtain the polynomial $x^2 + 4x + 2$, which has no roots in $\mathbb{Z}_5[x]$. Thus the factorization given above is the complete factorization of $x^3 + x^2 - 36$ over $\mathbb{Q}[x]$.

70. Let $g(x) = x^3 + qx + r$ and define $R = r^2 + 4q^3/27$ Let $u$ be a root of $g(x)$ and let $u = y + z$, where

$$y^3 = \frac{1}{2} \left( -r + \sqrt{R} \right).$$  We prove that

$$z^3 = \frac{1}{2} \left( -r - \sqrt{R} \right).$$

Since $u$ is a root, we have

$$(y + z)^3 + qu + r = y^3 + z^3 + (3yz + q)u + r = 0$$
Setting \( yz = \frac{-q}{3} \), we obtain the system

\[
\begin{align*}
y^3 + z^3 + r &= 0 \\
y^3 z^3 &= \frac{-q^3}{27}
\end{align*}
\]

Solving the first equation using the second, we obtain the sextic \( y^6 + ry^3 - \frac{q^3}{27} \), which we quickly solve for \( y^3 \) as expected:

\[
y^3 = \frac{1}{2} \left( -r + \sqrt{R} \right).
\]

Then using the relation \( y^3 z^3 = \frac{-q^3}{27} \), we see that

\[
z^3 = \frac{-q^3}{27 y^3}
\]

\[
z^3 = \frac{1}{2} \left( -r - \sqrt{R} \right).
\]

71. We find the roots of the following polynomials.

(a) \( f(x) = x^3 - 3x + 1 \). Using exercise 70, we have one root of \( f(x) \) as

\[
u_1 = \sqrt[3]{\frac{1}{2} \left( -1 + \sqrt{-3} \right)} + \sqrt[3]{\frac{1}{2} \left( -1 - \sqrt{-3} \right)}.
\]

The other roots are given by

\[
u_2 = \omega \sqrt[3]{\frac{1}{2} \left( -1 + \sqrt{-3} \right)} + \omega^2 \sqrt[3]{\frac{1}{2} \left( -1 - \sqrt{-3} \right)}
\]

\[
u_3 = \omega^2 \sqrt[3]{\frac{1}{2} \left( -1 + \sqrt{-3} \right)} + \omega \sqrt[3]{\frac{1}{2} \left( -1 - \sqrt{-3} \right)}
\]

where \( \omega = e^{2\pi i/3} \).

(b) \( f(x) = x^3 - 9x + 28 \). We first observe that \( x = -4 \) is a root of this polynomial, and after dividing by \( x + 4 \), we have the reduced polynomial \( x^2 - 4x + 7 \), which has as its roots

\[
x = \frac{4 \pm \sqrt{12}}{2}
\]

(c) \( f(x) = x^3 - 24x^2 - 24x - 25 \). We notice that \( x = 25 \) is a root of this polynomial, so dividing by \( x - 25 \), we have the reduced polynomial \( x^2 + x + 1 \). This polynomial has roots

\[
x = \frac{-1 \pm \sqrt{-3}}{2}
\]

(d) \( f(x) = x^3 - 15x - 4 \). We see that \( x = 4 \) is a solution, so dividing out we have the quadratic \( x^2 + 4x + 1 \), which has roots

\[
x = \frac{-4 \pm \sqrt{12}}{2}
\]
(e) $x^3 - 6x + 4$. Since $x = 2$ is a factor, we look at the reduced polynomial $x^2 + 2x - 2$, which has roots

$$x = \frac{-2 \pm \sqrt{12}}{2}.$$

(f) $x^4 - 15x^2 - 20x - 6$. We first observe that $x = -3$ and $x = -1$ are both roots to this biquadratic equation. Once factored out, we have the quadratic $x^2 - 4x - 2$, which has roots

$$x = \frac{4 \pm \sqrt{24}}{2}.$$