9.3 #1 Assume \( R \) is int. dom. with field of fractions \( F \),
monic \( p(x) \in R[x] \), \( p(x) = a(x)b(x) \) with \( a(x), b(x) \in R[x] \),
nonconstant. We show that if \( R \) is U.F.D. then \( a(x), b(x) \in R[x] \).

Applying Gauss' Lemma gives \( \alpha(x) \in R[F \setminus \{0\}] \) such that
\[ \alpha(x) \in R[x] \text{ and } \frac{1}{\alpha(x)} \in R[F \setminus \{0\}] \text{.} \]
But \( b(x) \) has lead coeff. \( = 1 \),
so \( \frac{1}{\alpha(x)} \) has lead coeff. \( \frac{1}{\alpha(x)} \),
so \( \frac{1}{\alpha(x)} \in R \). (Similarly \( \alpha(x) \in R \))

Thus \( \alpha(x) = \frac{1}{\alpha(x)} \in R[x] \) since \( \frac{1}{\alpha(x)} \in R \) and \( \alpha(x) \in R[x] \).

Now consider \( R = R[x] / (x^2 + x + 1) \) and note that in \( R[x] \) we have
monic \( x^2 + 2 \sqrt{2} x + 2 = (x + \sqrt{2})(x + \sqrt{2}) \),
but \( a(x) = x + \sqrt{2} \notin R[x] \).
(Indeed \( x = 4 \cdot 2 = (2 \sqrt{2})(2 \sqrt{2}) \).

#2 \( f(x), g(x) \in R[x] \) and \( p(x) = f(x)g(x) \in Z[x] \).
By Gauss' Lemma, \( \exists \alpha, \beta = 0 \) s.t. \( \alpha f(x) \in Z[x] \) and \( \frac{1}{\alpha} g(x) \in Z[x] \).
Then the \( j \)th coeff. in \( f(x) \)
multiplied \( k \)th coeff. in \( g(x) \) equals the \( j \)th coeff. in \( \frac{1}{\alpha} g(x) \), but both are integers, so the product is an integer.

#3 \( R = \mathbb{F}_p(\sqrt{2}) \) is a group under addition since \( \mathbb{F}_p \) and
\( \sqrt{2} \) are. It is closed under mult since
\( (a + x^2 p(x))(b + x^2 q(x)) = ab + x^2(a p(x) + b q(x)) \).
Thus it is a subring of \( F[x] \).

Now \( x^2 \) and \( x^3 \) are irreducible in \( R \) since
nonzero constants in \( R \) are units and thus a nontrivial factorization of either would require
two nonconstant polynomials whose degrees add up to 2 or 3. This calls for a polynomial
of degree one, but there are none in \( R \).

So \( (x^2)^3 = x^6 = (x^3)^2 \) gives two irreducible factorizations of \( x^6 \),
and \( R \) is not a U.F.D.
\#4 \( R = \mathbb{Z} + x\mathbb{Q}[x] \),

a) \( R \) is an integral domain since it is contained in the int. dom. \( \mathbb{Q}[x] \).

A unit of \( R \) must be a unit of \( \mathbb{Q}[x] \), hence is a constant.

That is, if \( p(x)q(x) = 1 \), then clearly \( p(x) \) and \( q(x) \) have degree 0, and if they are in \( R \), they must be integers whose product is 1. This leaves \( \pm 1 \) as the only units.

b) If \( p \) is an integer prime, we see that it is irreducible in \( R \), as it can only be factored into constants, which must be in \( \mathbb{Z} \).

If \( f(x) \) is irreducible with constant term \( \pm 1 \), then it is irreducible in \( \mathbb{Q}[x] \), hence can only be factored using constants. But a constant in the factorization must divide the constant \( \pm 1 \), so is a unit. So \( f(x) \) is irreducible in \( R \).

Conversely, suppose \( g(x) \) is irreducible in \( R \). If \( g(x) \) is constant, it is in \( \mathbb{Z} \) and must be a prime in \( \mathbb{Z} \), since a factorization in \( \mathbb{Z} \) would be a factorization in \( R \).

If \( g(x) \) is not constant and has non-zero constant term \( a \), we can factor \( g(x) = (a)(\frac{1}{a}g(x)) \).

\( \frac{1}{a}g(x) \in \mathbb{Q}[x] \) and \( a \) is not a unit because it is not constant. Therefore, since we are assuming \( g(x) \) is irreducible, \( a \) must be a unit \( \pm 1 \), and \( g(x) \) is irreducible with constant term \( \pm 1 \). We also note that if \( g(x) \) has 0 constant term, \( \mathbb{Q}(\frac{x}{x}) \) is not irreducible as it is \( (\mathbb{Q}(\frac{x}{x}), (\frac{x}{x})) \) or \( (\mathbb{Q}(\frac{x}{x})) \).

\[ R/(p) \cong \mathbb{F}_p^2 \text{, a field, so \( p \) is maximal} \Rightarrow \text{\( p \) prime} \Rightarrow \text{\( p \) prime. If \( f(x) \) is irreducible with \( f(0) = 0 \), then \( \mathbb{Z}[x]/(f(x)) \) is a field.}

The composition \( \mathbb{Z} + x\mathbb{Q}[x] \rightarrow \mathbb{Q}[x] \rightarrow \mathbb{Q}[x]/(f(x)) \) has kernel \( (f(x)) \) in \( R \), as one can check. So by the Fundamental Isomorphism Theorem, \( \mathbb{Z} + x\mathbb{Q}[x]/(f(x)) \cong \mathbb{Q}[x]/(f(x)) \) and we know \( f(x) \) is irreducible in \( \mathbb{Q}[x] \), hence \( f(x) \) is prime in \( \mathbb{Q}[x] \), so \( \mathbb{Q}[x]/(f(x)) \) is an int. dom.

The isomorphism then shows that \( f(x) \) is prime in \( R \) so \( f(x) \) is prime.
(c) We have seen that all of the irreducibles in \( \mathbb{R} \) have a non-zero constant term, so any product of irreducibles has a non-zero constant term and cannot equal \( x \). Since \( x \) cannot be factored into irreducibles, \( \mathbb{R} \) is not a UFD.

(d) \( \mathbb{R} = \mathbb{Z} + \mathbb{Q} x + \mathbb{Q} x^2 + \ldots \)

So as a group, \( \mathbb{R}(x) = \mathbb{Z} + \mathbb{Q} x \)

with the rule \((a + b x)(c + d x) = ac + ad + bc x\).

This is not an integral domain since \((x)(x) = 0\),
so \(x\) is not prime by the criteria on \( \mathbb{R}(x) \).

9.4 #1 a) \(x^2 + x + 1\) has no root in \( \mathbb{F}_2\), so no linear factor

In \( \mathbb{F}_2 \), \(x\) is irreducible since it is degree 2.

b) \(x^3 + x + 1 = (x-1)(x^2 + x - 1)\) in \( \mathbb{F}_3 [x]\).

c) \(x^4 + 1 = x^4 - 4 = (x^2 - 2)(x^2 + 2)\) in \( \mathbb{F}_5 [x]\).

d) \(x^4 + 10 x^2 + 1\) has no linear factors, by the rational root theorem. If it had a factorization into quadratics, then reducing mod 5, we see that the terms must reduce to \((x^2 - 2)\) and \((x^2 + 2)\). In particular, the constant terms are not congruent to \(\pm 1\) mod 5.

But their product must be 1, so they must equal \(\pm 1\).

This is a contradiction, and the poly. is irreducible.

#2 a) Irred by Eisenstein using \(p = 2\).

b) Irred by Eisenstein using \(p = 3\).

c) After substitution, irreducible by Eisenstein using \(p = 2\).

d) Irred by Eisenstein for \(p\).

#3 Call this polynomial \(f(x)\) and note that \(f(i) = -1\) for \(i = \pm 1\).

If \(f(x) = p(x)q(x)\), let \(q(x)\) be the one of smaller degree.

So deg \((p(x)) \leq \frac{n}{2}\). Then \(-1 = f(i) = p(i)q(i)\) so \(q(i) = \pm 1\).

There are then at least \(\frac{n}{2}\) values of \(i\) for which \(q(x)\) has

the same value \(\pm 1\) so \(q(x) \pm 1\) is constant \(\Rightarrow\) \(q(x)\) constant \(\Rightarrow\)

\(f\) irreducible. (A clever proof is to consider \((p(x)-1)(q(x)-1)\)
5. \(1, x + 1, x^2 + x + 1, x^3 + x + 1, x^3 + x^2 + 1\)
   are irreducible in \(\mathbb{F}_2[x]\) because they have no roots.

11. Viewed in \(\mathbb{Q}[i\sqrt{3}][x]\), \(x^2 + (y^2 - 1)\) is irreducible by Eisenstein using the prime \(y - 1\) in \(\mathbb{Q}[i\sqrt{3}]\).

19. d. \(x^p - a = x^p - a^p = (x - a)^p\) in \(\mathbb{F}_p[x]\).

20. \((3x + 1)(4x + 5) = 12x^2 + 25x + 15 \equiv 7x\) in \(\mathbb{Z}/6\mathbb{Z}\).

a) \(x\) is irreducible over \(\mathbb{Z}/2\mathbb{Z}\) and \(\mathbb{Z}/3\mathbb{Z}\) since they are fields so \(x\) would have to be factored using polynomials of lower degree in \(\mathbb{Z}/2\mathbb{Z}[x]\) and \(\mathbb{Z}/3\mathbb{Z}[x]\) in which the non-zero constants are units.

b) The factorizations in \(\mathbb{Z}/2\mathbb{Z}[x]\) and \(\mathbb{Z}/3\mathbb{Z}[x]\) are unique (up to units) so any factorization in \(\mathbb{Z}/6\mathbb{Z}[x]\) must reduce to
   1. \(x\) or \(x+1\) in \(\mathbb{Z}/2\mathbb{Z}[x]\) and to
   1. \(x\) or \(x+1\) or \(-1-x\) or \(-x-1\) in \(\mathbb{Z}/3\mathbb{Z}[x]\).

Combining these by CRT we get in \(\mathbb{Z}/6\mathbb{Z}[x]\),

\[x = b \cdot x = (4x+3)(3x+1) = (-1)(-x) = (2x+3)(3x+2)\]

C) \((3, x) = (2x+3)\) Check it!

D) Similar to above

E) \(x\) is the product of \(k\) linear factors.