4.2.5 and **4.2.7** Find the gcd of the given polynomials, over the given field. Write the gcd as a linear combination of the given polynomials.
(b) $f(x) = x^3 - 2x^2 + 3x + 1$ and and $g(x) = x^3 + 2x + 1$ over $\mathbb{Z}_5$.
(d) $f(x) = x^5 + x^4 + 2x^2 + 4x + 4$ and $g(x) = x^3 + x^2 + 4x$ over $\mathbb{Z}_5$.

(b) The Euclidean algorithm gives me $(3x^2 + 2x + 2)f + (2x + 4x + 4)g = 1$, so the gcd is 1.
(d) Here, I get $(4x + 4)f + (x^3 + x^2 + x + 2)g = 1$, so the gcd is again 1.

4.2.9 Let $a \in \mathbb{R}$, and let $f(x) \in \mathbb{R}[x]$, with derivative $f'(x)$. Show that the remainder when $f(x)$ is divided by $(x - a)^2$ is $f'(a)(x - a) + f(a)$.

The division/remainder theorem tells us that there are unique q and r such that $f(x) = (x-a)^2q(x)+r(x)$, where $\deg r < 2$. That means we can write $r(x) = Ax+B$ and it only remains to solve for the coefficients A and B. We'll do that by computing $f(a)$ and $f'(a)$.
Plugging in to the above equation, we have $f(a) = r(a)$, and we know $r(a) = Aa+B$, so putting these together gives $Aa + B = f(a)$. Taking a derivative of f gives $f'(x) = 2(x - a)q(x) + (x - a)^2q'(x) + r'(x)$, so we have $f'(a) = r'(a)$, and $r'(x)$ is the constant function A, so putting these together gives $f'(a) = A$. But then solving for B we have $B = f(a) - Aa = f(a) - af'(a)$, so finally $r(x) = Ax + B = f'(a)x + f(a) - af'(a) = f'(a)(x - a) + f(a)$, as desired.

4.2.13 Find all monic irreducible polynomials of degree ≤ 3 over $\mathbb{Z}_3$. Using your list, write each of the following polynomials as a product of irreducible polynomials.

The point of this problem was just to get you practice manipulating/factoring/unfactoring polynomials. An example of a method to do this is to list all the monic linear polynomials for yourself: $x, x+1, x+2$. Then form all nine products of these with each other to find the reducible quadratics. (The others are irreducible.) Then find all products of quadratics with linears to get all reducible cubics. I won't reproduce this process here.
List of quadratic irreducibles: x^2+1, x^2+x+2, x^2+2x+2. List of cubic irreducibles: $x^3 + 2x + 1, x^3 + 2x + 2, x^3 + x^2 + 2, x^3 + x^2 + x + 2, x^3 + x^2 + 2x + 1, x^3 + 2x^2 + 1, x^3 + 2x^2 + x + 1, x^3 + 2x^2 + 2x + 2$.

Here are the factorizations...
(a) $x^2 - 2x + 1 = (x-1)^2 = (x+2)^2$.
(b) $x^4 + 2x^2 + 2x + 2$. First look for a root (there are only 3 to try). We can check that 2 is a root, so $x - 2$ factors out. Long division gives the quotient $x^3 + 2x^2 + 2$, which is $(x^2 + x + 2)(x + 1)$. Final answer $(x^2 + x + 2)(x + 1)^2$.
(c) $2x^3 - 2x + 1 = 2(x^3 + 2x + 2)$.
(d) $x^4 + 1$ doesn't have a root, so if it factors, it factors into quadratics. We try products of the irreducible quadratics and find $(x^2 + 2x + 2)(x^2 + x + 2)$.
(e) $x^9 - x = x(x^8 - 1) = x(x^4 + 1)(x^2 + 1)(x + 1)(x + 2)$ and then finish it off with the factorization of $x^4 + 1$ from above.

4.2.15 Show that for any real number $a \neq 0$, the polynomial $x^n - a$ has no multiple roots in $\mathbb{R}$.

There are many ways to do this! Let's use the problem we did above, 4.2.9, to say that the remainder when $f(x)$ is divided by $(x-b)^2$ is $f'(b)(x-b) + f(b)$. We'll show that this remainder is NOT zero for our function $f(x) = x^n - a$, which means that b is NOT a root of multiplicity two or more.
For our function, $f(b) = b^n - a$, and $f'(x) = nx^{n-1}$, so $f'(b) = nb^{n-1}$. That means the remainder is $nb^{n-1}(x-b) + b^n - a$. Sorting this to look more like a polynomial, we have remainder $(nb^{n-1})x + (nb^n + b^n - a)$, and we need to show that this is not the zero function. The only way for the coefficient of x to be zero is if $b = 0$. However if $b = 0$, the linear term of this remainder function is $-a$, which we are told is not zero. So we are done.

4.2.20 Find a polynomial $q(x)$ such that (b) $(a + bx)q(x) \equiv 1 \pmod{x^2 - 2}$ over $\mathbb{Q}$; (d) $(x^2 + 2x + 1)q(x) \equiv 1 \pmod{x^3 + x^2 + 1}$ over $\mathbb{Z}_3$.

(b) Putting $f(x) = bx + a$ and $g(x) = x^2 - 2$, we can find the linear combination of these that gives 1. The Euclidean algorithm gives $(\frac{b}{a}x - 1)f + (\frac{-b^2}{a})g = \frac{2b^2 - a^2}{a}$, and dividing out to get one, we find that the coefficient of f is $q(x) = \frac{bx - a}{2b^2 - a^2}$. Now something a bit more interesting: let's check that this works. When you multiply $f(x)q(x)$, you get $\frac{b^2x^2 - a^2}{2b^2 - a^2}$, and since we're working mod $x^2 - 2$, we know that $x^2 \equiv 2$, so this simplifies to one!
(d) The Euclidean algorithm will tell you that $x^2 + 2x + 1$ is its own inverse in $\mathbb{Z}_3[x]/\langle x^3 + x^2 + 1\rangle$.

4.2.10 Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with rational coefficients such that a_n and a_0 are nonzero. Show that $p(x)$ is irreducible over $\mathbb{Q}$ iff its "reversal" $q(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$ is.

First, the hypothesis that a_n and a_0 are nonzero means that both p and q have degree exactly n. Note that $x^n \cdot q(1/x) = p(x)$ (as you can check by just writing out the terms). Now suppose that q is reducible, so that it factors as $q(x) = a(x)b(x)$ where $\deg(a) = k \geq 1$ and $\deg(b) = n - k$. Then $q(1/x) = a(1/x)b(1/x)$. Now if a has degree k, then $x^k \cdot a(1/x)$ is a polynomial (i.e., has no x terms in the denominator). So we have $p(x) = x^n \cdot q(1/x) = (x^k \cdot a(1/x))(x^{n-k} \cdot b(1/x))$, and this is a factorization of p into two polynomials. So we've seen that if q is reducible then p is reducible. But we can run the exact same argument in the other direction by writing $q(x) = x^n \cdot p(1/x)$, and that completes the proof.

4.3.6 Let F be a field, let $p(x) \in F[x]$ be an irreducible polynomial, and let $E = \{[a] \in F[x]/\langle p(x)\rangle : a \in F\}$. Show that E is a subfield of $F[x]/\langle p\rangle$. Then show that $\phi : F \to E$ defined by $\phi(a) = [a]$ for all $a \in F$ is a field isomorphism.

What are the elements of $F[x]/\langle p\rangle$? They are equivalence classes of polynomials whose lowest-degree representatives are PRECISELY the polynomials in $F[x]$ of degree strictly less than $\deg p$. Now we can regard $a \in F[x]$ as either zero or a polynomial of degree zero (a nonzero constant). So since p is irreducible, its degree is at least one, and therefore these are all valid, distinct elements of the quotient ring $F[x]/\langle p\rangle$. So E is a subset of that ring, and it is identified with F by the natural map ϕ. But in fact it's a subfield, because its elements are in bijective correspondence with the elements of the field F and multiplication and addition are well-defined in the usual way (see Prop 4.3.4).

4.3.8 Prove that $\mathbb{R}[x]/\langle x^2 + 2\rangle$ is isomorphic to $\mathbb{C}$.

We build the map by hand. Let $E = \mathbb{R}[x]/\langle x^2 + 2\rangle$. Its elements are precisely the (equivalence classes of) linear polynomials: $E = \{ax + b : a, b \in \mathbb{R}\}$. To describe $\phi : E \to \mathbb{C}$, we only need to say where real numbers are sent by ϕ and where the special element x is sent; then if we extend this as a field homomorphism, we will know where all elements $ax + b$ are sent. A natural choice is to fix all real elements: $\phi(a) = a$ for all $a \in \mathbb{R}$. Then we want to send x to some root of the SAME polynomial. Now in $\mathbb{C}$ the roots of $x^2 + 2$ are $\pm\sqrt{2} \cdot i$. I can choose either one as the image of x, so I will choose $\phi(x) = \sqrt{2} \cdot i$. Then ϕ is completely defined by this: $\phi(ax + b) = a\sqrt{2}i + b$. This is a homomorphism by construction and is clearly injective; to see that it is surjective, note that $c + di$, an arbitrary element of $\mathbb{C}$, is $\phi\big((d/\sqrt{2})x + c\big)$.

4.3.9 Prove that $\mathbb{R}[x]/\langle x^2+x+1\rangle$ is isomorphic to $\mathbb{C}$.

This is essentially identical to the last problem! We similarly define the isomorphism to fix real numbers and to send x to (either of) the roots of the polynomial. The quadratic formula tells us that the solutions are $\frac{-1\pm\sqrt{1-4}}{2} = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$. Let us abbreviate $\tau := -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and choose $\phi(x) = \tau$, so that $\phi(ax+b) = a\tau + b = (\frac{\sqrt{3}}{2}a)i + (b - \frac{a}{2})$. Clearly this runs over all of $\mathbb{C}$ and distinct values of (a,b) map to distinct complex numbers; it is once again a homomorphism by construction.

4.3.14 Show that the polynomial x^2-3 has a root in $\mathbb{Q}(\sqrt{3})$ but not $\mathbb{Q}(\sqrt{2})$. Explain why this implies that those fields are not isomorphic.

As we have seen many times (e.g., page 180 in the book), as a set $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} : a,b \in \mathbb{Q}\}$. So to show that the field has no root of x^2-3, we show that $(a+b\sqrt{2})^2 - 3 = 0$ has no solutions for $a,b \in \mathbb{Q}$. Simplifying, we have $(a^2+2b^2-3)+(2ab)\sqrt{2} = 0$. Now we know that $c + d\sqrt{2} = 0$ is only possible if $c = d = 0$ (because it simplifies to $\sqrt{2} = -d/c$, which is impossible, unless $c = 0$ and that forces $d = 0$ as well). So $2ab = 0$ and $a^2 + 2b^2 - 3 = 0$. The first equation implies that $a = 0$ or $b = 0$. If $b = 0$, we deduce that $a^2 = 3$, which is impossible for rational a. But if $a = 0$, we have $2b^2 = 3$, which is impossible for rational b. (We are using the fact that $\sqrt{3}$ and $\sqrt{3/2}$ are irrational, which we proved earlier in the semester.) So we have shown that $x^2 - 3$ has no root in $\mathbb{Q}(\sqrt{2})$.

Why does this mean there's no isomorphism of fields $\phi : \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{2})$? Well, suppose there were such an isomorphism. Now we know that there is an element $a \in \mathbb{Q}(\sqrt{3})$ that satisifies $x^2 - 3 = 0$ (namely $a = \sqrt{3}$). Thus we can plug in and we have $a^2 - 3 = 0$. Now apply ϕ to both sides. $\phi(0) = 0$ because an additive homomorphism must fix the additive identity. As a multiplicative homomorphism, $\phi(1) = 1$, and thus $\phi(3) = 3$. Using the homomorphism property repeatedly we find $\phi(a^2 - 3) = \phi(a^2) - \phi(3) = [\phi(a)]^2 - 3 = 0$, so a root of that equation must be mapped by ϕ to a root of the same equation! But the target field has no such root, so our map has nowhere valid to send $a = \sqrt{3}$. Thus no such isomorphism exists.

4.3.15 Prove that the field of all matrices over $\mathbb{Q}$ of the form $\left[\begin{smallmatrix} a & b \\ 2b & a \end{smallmatrix}\right]$ is isomorphic to $\mathbb{Q}(\sqrt{2})$.

Let M stand for this collection of matrices and we will build a map $\phi : \mathbb{Q}(\sqrt{2}) \to M$ that is a field isomorphism. It must send the multiplicative identity to the multiplicative identity, so $\phi(1) = I = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$. But then for an integer p, we have $\phi(p) = pI = \left[\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right]$. Likewise $\phi(q) = \left[\begin{smallmatrix} q & 0 \\ 0 & q \end{smallmatrix}\right]$, so $\phi(1/q) = \left[\begin{smallmatrix} q & 0 \\ 0 & q \end{smallmatrix}\right]^{-1} = \left[\begin{smallmatrix} 1/q & 0 \\ 0 & 1/q \end{smallmatrix}\right]$, and therefore $\phi(p/q) = \left[\begin{smallmatrix} p/q & 0 \\ 0 & p/q \end{smallmatrix}\right]$. So we know where all rational numbers are mapped, and only need to decide on an image for $\sqrt{2}$ and then extend by the homomorphism property. To find a suitable image, we note that $\sqrt{2}$ satisfies $x^2 = 2$, so we need a solution to $A^2 = 2I$ in M. If $A = \left[\begin{smallmatrix} a & b \\ 2b & a \end{smallmatrix}\right]$, we square it to obtain $A^2 = \left[\begin{smallmatrix} a^2+2b^2 & 2ab \\ 4ab & a^2+2b^2 \end{smallmatrix}\right]$, which IS of the right form to be in M. When does this equal $2I$? Only when $a = 0, b = 1$. So the solution is $A = \left[\begin{smallmatrix} 0 & 1 \\ 2 & 0 \end{smallmatrix}\right]$, and we complete the definition of ϕ by sending $\sqrt{2}$ to this A. Then for an arbitrary element we have $\phi(c+d\sqrt{2}) = \left[\begin{smallmatrix} c & d \\ 2d & c \end{smallmatrix}\right]$, which clearly puts M in bijective correspondence with $\mathbb{Q})(\sqrt{2})$ and is once again a homomorphism by construction.

4.3.21 (bdf) Find multiplicative inverses for: (b) $[a + bx]$ in $\mathbb{Q}[x]/\langle x^2 - 2\rangle$; (d) $[x^2 - 2x + 1]$ in $\mathbb{Z}_3[x]/\langle x^3 + x^2 + 2x + 1\rangle$; (f) $[x + 4]$ in $\mathbb{Z}_5[x]/\langle x^3 + x + 1\rangle$.

(b) We did this in the last assignment! (Problem 4.2.20, just phrased a bit differently but the exact same question.) Answer: $\frac{bx-a}{2b^2-a^2}$.

(d) Euclidean algorithm gives $(x^2 + 1)f + (2x)g = 1$, so the inverse of f mod g is $x^2 + 1$.

(f) Euclidean algorithm gives $(3x^2 + 3x + 1)f + 2g = 1$, so the inverse of f mod g is $3x^2 + 3x + 1$.

4.2.24 (EC) Let F be a finite field. Show that $F[x]$ has irreducible polynomials of arbitrarily high degree.

Suppose, for the sake of contradiction, that there is some highest degree D of an irreducible polynomial over F. We are supposing the field is finite; say $F = n$. Then there are at most n^{D+1} polynomials of degree $\leq D$, because these are all possible ways to fill in the coefficients of $a_D x^D + \cdots + a_0$, including zeros. Thus, the hypothesis that D is the largest degree ensures that there are only finitely many irreducible polynomials in all, and we may enumerate them $f_1, f_2, \ldots, f_N$. Now we mimic the proof (attributed to Euclid) of the infinitude of primes. Define a new polynomial by $F(x) = (f_1(x) \cdots f_N(x)) + 1$. The degree of F is greater than D because it is the sum of the degrees of the f_i, and that means it is not on the list of all irreducible polynomials, so it must be reducible. But we can see that no f_i is a factor of F, because dividing F by any f_i gives remainder 1. But every polynomial factors into a product of irreducible polynomials, so this is a contradiction.