1. (a) Since $x^3 + 2x^2 + x + 1$ has no roots in $\mathbb{Z}_3$ and its degree is 3, it is irreducible. Therefore, $\mathbb{Z}_3[x]/(x^3 + 2x^2 + x + 1)$ is a field.

(b) Since 2 is a root of $2x^3 - 4x^2 + 2x + 1$ in $\mathbb{Z}_5$, $2x^3 - 4x^2 + 2x + 1$ is reducible. Therefore, this is not a field.

(c) $x^4 + x^2 + 1$ has no roots in $\mathbb{Z}_2$, so it cannot have a linear factor. It could have two quadratic irreducible factors. In $\mathbb{Z}_2[x]$, the only irreducible quadratic polynomial is $x^2 + x + 1$. Now $(x^2 + x + 1)(x^2 + x + 1) = x^4 + x^2 + 1$, so $x^4 + x^2 + 1$ is reducible. Therefore, $\mathbb{Z}_2[x]/(x^4 + x^2 + 1)$ is not a field.

2. (a) Since $d$ is not a perfect square, exercise 32 in Section 3.1 (which you did) shows that $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{C}$. In particular, it is a field, and since $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$, it is also a subfield of $\mathbb{R}$.

(b) This will be easy in a few days. For now, define $\phi : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}[x]/(x^2 - 2)$ by $\phi(a + b\sqrt{2}) = [a + bx]$. Then $\phi((a + b\sqrt{2}) + (c + d\sqrt{2})) = \phi(a + c) + (b + d)\sqrt{2}) = [(a + c) + (b + d)x] = [a + bx] + [c + dx] = \phi(a + bx) + \phi(c + dx)$. Also, $\phi((a + b\sqrt{2})(c + d\sqrt{2})) = \phi(ac + 2bd) + (ad + bc)\sqrt{2}) = [ac + 2bd] + (ad + bc)x] = [a + bx][c + dx] = \phi(a + bx)\phi(c + dx)$. Thus $\phi$ is operation-preserving. Furthermore, $\phi$ is surjective by Corollary 5.5: every equivalence class can be represented in the form $[a + bx] = \phi(a + b\sqrt{2})$. Finally, if $\phi(a + bx) = \phi(c + dx)$, then $[a + bx] = [c + dx]$. Again employing Corollary 5.5, we see that $a = c$ and $b = d$, so $a + b\sqrt{2} = c + d\sqrt{2}$.

3. Here, every equivalence class can be represented in the form $[b]$, where $b \in F$. Thus $F[x]/(x - a) \cong F$ by the proof of Theorem 5.7. (Specifically, that $F$ is isomorphic to the subring $F^*$.) Notice that we do get a root of the irreducible polynomial $x - a$ — namely, $a$!

5. (a) This follows by the same reasoning as in 2(a).

(b) This follows by the same reasoning as in 2(b). Frankly, I'm not now sure why I put both exercises on this assignment.

7. The proof is by induction on $n$. The theorem is certainly true if $n = 1$ since a linear polynomial already has its lone root in $F$. Assume now that $f(x)$ has degree $n > 1$ and that the theorem holds for all polynomials of degree $n - 1$. Let $c_0$ be the leading coefficient of $f(x)$.

By corollary 5.12, there is an extension field $K$ of $F$ such that $K$ contains a root $c_1$ of $f(x)$. Thus, in $K[x]$, $f(x) = c_0(x - c_1)g(x)$, where $\deg(g(x)) = n - 1$ and $g(x)$ is monic. By the induction hypothesis, there exist a field $E$ and constants $c_2, \ldots, c_n \in E$ such that $g(x) = (x - c_2) \cdots (x - c_n)$. Thus $f(x) = c_0(x - c_1) \cdots (x - c_n)$.

9. Keep in mind that we are working over $\mathbb{Z}_2$, where $-1 = 1$. I will make frequent use of this idea without necessarily mentioning it, so stay on your toes!

(a) Since $x^3 + x + 1$ does not have a root in $\mathbb{Z}_2$ and its degree is 3, it is irreducible. Thus $\mathbb{Z}_2[x]/(x^3 + x + 1)$ is a field.

(b) One of the roots is $[x]$. We must find the other two. I will demonstrate two methods:

i. Method 1: The elements of $\mathbb{Z}_2[x]/(x^3 + x + 1)$ are $0, 1, [x], [x] + 1, [x^2], [x^2] + 1, [x^2] + [x]$, and $[x^2] + [x] + 1 = [x^3 + 3x^2 + 2x + 1] + 1 = [x^3 + x^2 + x + 1] = [x^3 + x^2 + 1] = [x^2 + x] \neq 0$; so $[x + 1]$ is not a root.

$[x^2]^3 + [x^2] + 1 = [x^6] + [x^2 + 1] = [x^3]^2 + [x^2 + 1] = [x^2 + 1]^2 + [x^2 + 1] = [x^2 + 1]^2 + [x^2 + 1] = 0$. Thus, $[x^2]$ is another root. Notice also that $[x^3] = [x^2 + 1]$.

$[x^2 + 1]^3 + [x^2 + 1] = [x^6 + 3x^4 + 3x^2 + 1 + x^2 + 1] = [x^2 + 1 + x + x^3] = [x^2 + 1 + x^2 + x] = [x + 1] \neq 0$, so $[x^2 + 1]$ is not a root.

$[x^2 + x]^3 + [x^2 + x] + 1 = [x^6 + 3x^5 + 3x^4 + x^3 + x^2 + x + 1] = [x^6 + x^5 + x^4 + x^3 + x^2 + x + 1] = ([x^5 + 1] + (x + 1)x^4 + x(x + 1) + x^2) = [1 + x + 1 + x] = 0$, so $[x^2 + x]$ is the other root.
ii. Method 2: Let \( \alpha = [x] \). Then in \( \mathbb{Z}_2[x]/(x^3 + x + 1) \), the polynomial \( x^3 + x + 1 \) (note that this is \( x \), not \([x]\)) factors as \( (x - \alpha)(x^2 + \alpha x + (\alpha^2 + 1)) \). (Check this: multiplying it out gives \( x^3 + x + \alpha^2 + \alpha = x^3 + x + 1 \) since \( \alpha^3 + \alpha + 1 = 0 \).) We now need to factor \( x^2 + \alpha x + \alpha^2 + 1 \), but we can’t use the quadratic formula: it has a 2 (i.e., 0) in the denominator! However, we can still factor in the usual way. We need factors of \( \alpha^2 + 1 \) that add up to \( \alpha \). Now from above, we see that \( \alpha^4 = \alpha^2 + 1 \), so we have the following factorizations of \( \alpha^2 + 1 \): \( \alpha \cdot \alpha^4, \alpha^2 \cdot \alpha^4 = \alpha^2 \cdot (\alpha^2 + \alpha) \), and \( \alpha^3 \cdot \alpha^3 = (\alpha + 1)(\alpha + 1) \). The middle one gives us what we want, so we have \( x^2 + \alpha x + \alpha^2 + 1 = (x - \alpha^2)(x - (\alpha^2 + \alpha)) \). Since \( \alpha^2 \) and \( \alpha^2 + \alpha \) both belong to our field (since \( \alpha \) does), all three roots belong to the field.

10. Oh, yes! This is why I wanted you do do both 2 and 5. We know that given any isomorphism between fields, the multiplicative identity of one field must map to the multiplicative identity of the other. Thus, if \( \phi \) is an isomorphism between \( \mathbb{Q}(\sqrt{2}) \) and \( \mathbb{Q}(\sqrt{3}) \), then \( \phi(1) = 1 \). This also gives \( \phi(2) = \phi(1 + 1) = \phi(1) + \phi(1) = 1 + 1 = 2 \). (In fact, we can show that \( \mathbb{Q} \) is fixed by such an isomorphism.) Now suppose that \( \phi(\sqrt{2}) = a + b\sqrt{3} \) for some \( a, b \in \mathbb{Q} \). Then \( 2 = \phi(2) = \phi(\sqrt{2})^2 = \phi(\sqrt{2})^2 = (a + b\sqrt{3})^2 = (a^2 + 3b^2) + 2ab\sqrt{3} \). We can now see that \( a^2 + 3b^2 = 2 \) and \( 2ab = 0 \) (so that \( a = 0 \) or \( b = 0 \)). Unfortunately, this has no rational solution: if \( a \) or \( b \) is zero, we get \( 3b^2 = 2 \) or \( a^2 = 2 \), neither of which is possible. Therefore, no such isomorphism can exist.

13. It is enough to show that every irreducible polynomial has a root in \( \mathbb{Z}_2[x]/(x^4 + x + 1) \). Certainly every polynomial of degree 1 has a root in this field since every such polynomial has a root in \( \mathbb{Z}_2 \). The only irreducible polynomial of degree 2 in \( \mathbb{Z}_2[x] \) is \( x^2 + x + 1 \). If \( \alpha \) is a root of \( x^4 + x + 1 \), then, after a little playing around, we find that \( \alpha^2 + \alpha \) is a root of \( x^2 + x + 1 \). Therefore every quadratic over this field has a root in this field, as well.

Finally, consider \( x^4 + ax^3 + bx^2 + cx + 1 \). We may assume that the constant term is 1 or else we can factor out an \( x \), and we can assume the polynomial is monic since the only other option for a leading coefficient is 0. Here are the polynomials:

<table>
<thead>
<tr>
<th>Polynomial</th>
<th>Why it has a root in the field</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x^4 + 1 )</td>
<td>( = (x + 1)^4 )</td>
</tr>
<tr>
<td>( x^4 + x + 1 )</td>
<td>( a ) is a root</td>
</tr>
<tr>
<td>( x^4 + x^2 + 1 )</td>
<td>( = (x^2 + x + 1)^2 ) (and this has a root)</td>
</tr>
<tr>
<td>( x^4 + x^3 + 1 )</td>
<td>*</td>
</tr>
<tr>
<td>( x^4 + x^2 + x + 1 )</td>
<td>( x = 1 ) is a root</td>
</tr>
<tr>
<td>( x^4 + x^3 + x^2 + 1 )</td>
<td>( x = 1 ) is a root</td>
</tr>
<tr>
<td>( x^4 + x^3 + x^2 + x + 1 )</td>
<td>*</td>
</tr>
</tbody>
</table>

* I’m out of time! Bonus points to whomever finds these first without using the web!