10.2.1(a)

Let $E = \mathbb{Q}(u)$ where $u = e^{2\pi i/5}$. $E$ is the splitting field of $f(x) = x^5 - 1$ (check this!), so $E$ is Galois over $\mathbb{Q}$. The minimal polynomial of $u$ is the fifth cyclotomic polynomial,

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

(you have proven in the past that this is irreducible). Thus, $[E : \mathbb{Q}] = 4$. Since $E$ is Galois, $|\text{gal}(E : \mathbb{Q})| = 4$. The roots of $\phi_5(x)$ are $u, u^2, u^3, \text{and } u^4$. By Theorem 1 in 10.2, the automorphisms of $E$ are $\sigma_i$, where $\sigma_i(u) = u^i$ for $i = 1, 2, 3, 4$. Notice that

$$\sigma_2(u) = u^2$$
$$\sigma_2^2(u) = \sigma_2(u^2) = u^4$$
$$\sigma_2^3(u) = u^8 = u^3$$
$$\sigma_2^4(u) = u^{16} = u$$

so the order of $\sigma_2$ is 4. Thus, $\text{gal}(E : \mathbb{Q})$ is the cyclic group of order 4, $C_4$, generated by $\sigma_2$.

To determine the subgroup lattice of intermediate subfields, we will use the Galois correspondence. We start with the subgroup lattice of $C_4$. It has exactly one subgroup of orders 1, 2, and 4:

$$1 = \langle \sigma_1 \rangle < \langle \sigma_2 \rangle < \langle \sigma_2^2 \rangle < \langle \sigma_4 \rangle = \langle \sigma_2 \rangle$$

The intermediate fields will correspond to the fixed fields of these subgroups. The fixed field of $\langle \sigma_2 \rangle$ is $\mathbb{Q}$. The fixed field of $\langle \sigma_2 \rangle$ is $\mathbb{Q}(u)$. It remains to determine the fixed field of $\sigma_4$. First, notice that $\sigma_4^2 = \sigma_4$. Every element of $E = \mathbb{Q}(u)$ is of the form $a + bu + cu^2 + du^3$ for $a, b, c, d \in \mathbb{Q}$. Suppose that an element is fixed by $\sigma_4$. That is,

$$u + bu + cu^2 + du^3 = \sigma_4(u + bu + cu^2 + du^3) = a + bu^4 + cu^8 + du^{12} = a + bu^4 + cu^3 + du^2$$

Since $u$ is a root of $\phi_5(x)$, we have $u^4 = -(u^3 + u^2 + u + 1)$ so that the above is equal to

$$a - b(u^3 + u^2 + u + 1) + cu^3 + du^2 = (a - b) - bu + (d - b)u^2 + (c - b)u^3$$

Since $\{1, u, u^2, u^3\}$ is a basis for $E$ over $\mathbb{Q}$, we must have that

$$a - b = a, \quad b = -b \quad c = d - b \quad d = c - b$$

Thus, $b = 0$ and $c = d$, so the elements of $E$ fixed by $\sigma_4$ are of the form $a + cu^2 + cu^3$. The subfield $K$ consisting of all such elements is clearly generated by $u^2 + u^3$. That is, $K = \mathbb{Q}(u^2 + u^3)$. Finally, notice that

$$u^2 + u^3 = e^{4\pi i/5} + e^{6\pi i/5} = e^{4\pi i/5} - e^{\pi i/5} = -e^{\pi i/5} - e^{\pi i/5}$$
$$= -2 \cos(\pi/5)$$

Thus, $K = \mathbb{Q}(\cos(\pi/5))$, and so the lattice of intermediate subfields is

$$\mathbb{Q}(u) \supset \mathbb{Q}(\cos(\pi/5)) \supset \mathbb{Q}$$

$\square$

10.2.1(b)

Let $E = \mathbb{Q}(u)$ where $u = e^{2\pi i/7}$. The minimal polynomial of $u$ is the 7th cyclotomic polynomial, which has degree 6 and whose roots are the primitive 7th roots of unity. Thus, $E$ is a Galois extension (splitting field of $\Phi_7(x)$). As in part (a), the Galois group will turn out to be cyclic, now of order 6, generated by $\sigma_3$ given by $\sigma_3(u) = u^3$. (Check all of this!)
Notice that $C_6$ is isomorphic to $C_2 \times C_3$, where the $C_2$ is generated by $\sigma_3^2$ and the $C_3$ is generated by $\sigma_3^2$. This determines the subgroup lattice:

(link to image on website)

Now we proceed to calculating the lattice of intermediate fields. As usual, the fixed field of the identity subgroup is $E$, and the fixed field of the entire Galois group, $C_6$, is $\mathbb{Q}$ (since $E$ is Galois over $\mathbb{Q}$). Use the same method as in part (a) to show that $\sigma_3^2$ fixes $\cos(2\pi/7)$. As before, $|E : \mathbb{Q}| = 2$. Find a quadratic polynomial with coefficients in $\mathbb{Q}(\cos(2\pi/7))$ of which $u$ is a root, and use this to conclude that $|E : \mathbb{Q}(\cos(2\pi/7))| = 2$, and thus

$$< \sigma_3^2 >^0 = \mathbb{Q}(\cos(2\pi/7))$$

Finally, we need to find the fixed field of $\sigma_3^2$. An arbitrary element of $E$ looks like

$$a + bu + cu^2 + du^3 + eu^4 + fu^5$$

with the coefficients in $\mathbb{Q}$. Suppose such an element was fixed by $\sigma_3^2$:

$$a + bu + cu^2 + du^3 + eu^4 + fu^5 = \sigma_3^2(a + bu + cu^2 + du^3 + eu^4 + fu^5)$$

$$= a + bu^9 + cu^{18} + du^{27} + eu^{36} + fu^{45} = a + bu^2 + cu^4 + du^6 + eu + fu^3$$

Since $u^6 = -(u^5 + u^4 + u^3 + u^2 + u + 1)$, we have that the above is equal to

$$= a + bu^2 + cu^4 - d(u^5 + u^4 + u^3 + u^2 + u + 1) + eu + fu^3 = (a-d) + (e-d)u - (b-d)u^2 + (f-d)u^3 + (c-d)u^4 - du^5$$

Thus, we have the following equations

$$a = a - d, b = e - d, c = b - d, d = f - d, e = c - d, f = -d$$

so that

$$d = 0, b = c = e, f = 0$$

Thus, the fixed field of $\sigma_3^2$ is $\{a + b(u + u^2 + u^4)|a, b \in \mathbb{Q}\}$. Clearly, a primitive element for this field extension is $u + u^2 + u^4$. Thus,

$$< \sigma_3^2 >^0 = \mathbb{Q}(u + u^2 + u^4)$$

(since $u + u^2 + u^4$ generates a quadratic extension, we should be able to write it in terms of square roots of rational numbers. Here's how you could do this: find the quadratic minimal polynomial of $u + u^2 + u^4$. Then use the quadratic formula to find its roots and identify $u + u^2 + u^4$ with the correct one of the two. (Link to image of intermediate field lattice on website)

□

10.2.1(e)

Let $E = \mathbb{Q}(\sqrt{2}, i)$. The polynomial $f(x) = x^4 - 2$ has roots $\pm \sqrt{2}, \pm i \sqrt{2}$. Thus, $E$ is the splitting field for this polynomial. Since we are in characteristic zero, $E$ is separable over $\mathbb{Q}$, and thus $E$ is Galois over $\mathbb{Q}$. Notice that $f(x)$ is Eisenstein for $p = 2$, hence irreducible. Thus, $|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 4$. And since $i$ is a root of $x^2 + 1$, $|E : \mathbb{Q}(\sqrt{2})|$ is at most 2. It is exactly 2 since $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ and $i \notin \mathbb{R}$. Thus,

$$|E : \mathbb{Q}| = |E : \mathbb{Q}(\sqrt{2})| \cdot |\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2 \cdot 4 = 8$$

Since $E$ is Galois over $\mathbb{Q}$, the order of $\text{gal}(E : \mathbb{Q})$ must be 8. Every automorphism of $E$ over $\mathbb{Q}$ must send each of $\sqrt{2}$ and $i$ to the roots of their respective minimal polynomials. Thus, there are 8 possibilities:

$$\sigma_1: \{ \sqrt{2} \to \sqrt{2}, i \to i \} \quad \sigma_2: \{ \sqrt{2} \to -\sqrt{2}, i \to -i \} \quad \sigma_3: \{ \sqrt{2} \to -\sqrt{2}, i \to i \} \quad \sigma_4: \{ \sqrt{2} \to -\sqrt{2}, i \to -i \}$$

$$\sigma_5: \{ \sqrt{2} \to i \sqrt{2}, i \to i \} \quad \sigma_6: \{ \sqrt{2} \to i \sqrt{2}, i \to -i \} \quad \sigma_7: \{ \sqrt{2} \to -i \sqrt{2}, i \to i \} \quad \sigma_8: \{ \sqrt{2} \to -i \sqrt{2}, i \to -i \}$$
To determine the lattice of intermediate subfields, we start by determining the subgroup lattice of \( D_4 \). Since we know that there must be 8 automorphisms and also that there are only 8 possible automorphisms, all of the functions listed above must be automorphisms of \( E \). Now that we know the elements of \( \text{gal}(E : \mathbb{Q}) \), we need to figure out which group of order 8 it is. After playing around for a while, we see that the group is not abelian (for example, \( \sigma_2 \) and \( \sigma_5 \) don’t commute) and that
\[
\sigma_5 \sigma_2 = \sigma_6 \\
\sigma_2 \sigma_5^{-1} = \sigma_2 \sigma_7 = \sigma_6
\]
so that \( \sigma_5 \sigma_2 = \sigma_2 \sigma_5^{-1} \). Also, \( |\sigma_2| = 2 \) and \( |\sigma_5| = 4 \), and \( \sigma_2 \) and \( \sigma_5 \) generate the Galois group. Thus, \( \text{gal}(E : \mathbb{Q}) \) is isomorphic to \( D_4 \), with \( r = \sigma_5 \) and \( s = \sigma_2 \).

**NOTE 1:** You should check all of these things yourself. While none of it is hard, it is important to get some practice with it. This also applies to the calculations below. Subgroup lattices are messy to calculate, so even though we give the subgroup lattice for \( D_4 \) below, you should work it out for yourself.

**NOTE 2:** Here is another way that you could recognize which group of order 8 it is. Find two elements that do not commute. Thus, it must be \( D_4 \) or \( Q_8 \). \( Q_8 \) has 6 elements of order 4, but our group has only 2 elements of order 4 (\( \sigma_5 \) and \( \sigma_7 \)). Thus, our group is \( D_4 \). Since our next step will be to figure out the subgroup structure, it is still useful to identify an element with \( r \) and an element with \( s \) such that the appropriate relations are satisfied.

To determine the lattice of intermediate subfields, we start by determining the subgroup lattice of \( D_4 \). The way to figure this out is to start by listing the subgroups which are generated by one element. First, write all of the elements of the Galois group as products of \( \sigma_2 \) and \( \sigma_5 \) so that we can continue to keep the structure of \( D_4 \) in mind (write \( \sigma_5 \) as \( r \) and \( \sigma_2 \) as \( s \) if it helps). We have
\[
\sigma_3 = \sigma_2^2, \sigma_4 = \sigma_2 \sigma_5^2, \sigma_6 = \sigma_2 \sigma_5, \sigma_7 = \sigma_5^3, \sigma_8 = \sigma_2 \sigma_5
\]
Now, the subgroups generated by one element are
\[
< \sigma_1 > = 1, < \sigma_5 > = < \sigma_5^2 >, < \sigma_2^2 >, < \sigma_2 >, < \sigma_2 \sigma_5^2 >, < \sigma_2 \sigma_5 >, < \sigma_2 \sigma_5^3 >, < \sigma_2 \sigma_5 >
\]
Try adding another generator to each of these subgroups. If we end up in the situation that we can use the relations to get both \( \sigma_2 \) and \( \sigma_5 \) in our subgroup, then it must be all of \( D_4 \). Working through all of the possibilities is a bit tedious, but if you do (and you should!), you will see that the remaining subgroups are
\[
< \sigma_2^2, \sigma_2 \sigma_5^2 >, < \sigma_2 \sigma_5 >, < \sigma_2, \sigma_5 >
\]
(\( \sigma_5 \) should now figure out the order of all of the subgroups we have listed). So there are 10 subgroups total. Let’s put them into a lattice (remember, vertical lines mean inclusions).

\( (D_4 \) lattice image, link on website)\]

Now we need to determine the fixed fields of each of these subgroups. We will work out some examples below and you should check the rest. Recall that \( H^0 \) denotes the fixed field of \( H \). Throughout, we will use the fact that if \( H \) is a subgroup of \( \text{gal}(E : \mathbb{Q}) \), the order of \( H \) is the degree of the extension \( [E : H^0] \) (NOT \( [H^0 : \mathbb{Q}] \)).

Clearly, \( D_4^0 = \mathbb{Q} \) and \( < \sigma_1 >^0 = E \). Let’s start with the subgroups of order 4. The fixed field of \( < \sigma_5 > \) should have \( [E : < \sigma_5 >^0] = 4 \), so \( < \sigma_5 >^0 : \mathbb{Q} = 2 \). \( \sigma_5 \) fixes \( i \), and \( [\mathbb{Q}(i) : \mathbb{Q}] = 2 \), so \( < \sigma_5 >^0 = \mathbb{Q}(i) \).

Similarly, the fixed field of \( < \sigma_2^2, \sigma_2 > \) should have degree 2 over \( \mathbb{Q} \). \( \sigma_2 \) fixes \( \sqrt{2} \) and sends \( i \) to \( -i \), but \( \sigma_5 \) sends \( \sqrt{2} \) to \( i \sqrt{2} \) and fixes \( i \). So neither \( i \) nor \( \sqrt{2} \) is fixed by both \( \sigma_2 \sigma_5 \) and \( \sigma_2 \). What is fixed by both of these elements? After testing various elements, we see that both of them fix \( \sqrt{2} \). Since \( [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \), we have
\[
< \sigma_2^2, \sigma_2 >^0 = \mathbb{Q}(\sqrt{2})
\]

Now let’s consider \( < \sigma_2^2, \sigma_2 \sigma_5^3 > \), the last of the order 4 subgroups. This one is a little trickier. We are still looking for a degree 2 extension over \( \mathbb{Q} \). None of \( \sqrt{2}, i, \) or \( \sqrt{2} \) are fixed by both \( \sigma_2^2 \) and \( \sigma_2 \sigma_5^3 (= \sigma_6) \).
What other elements of $E$ have degree 2 over $\mathbb{Q}$? The simplest element that we haven’t considered yet is $i\sqrt{2}$. Indeed, using the fact that $\sigma_5^2 = \sigma_3$, 
\[
\sigma_3^2(i\sqrt{2}) = \sigma_3(i\sqrt{2}^2) = \sigma_3(i)(\sqrt{2}^2) = i(-\sqrt{2})^2 = i\sqrt{2}
\]
and 
\[
\sigma_2\sigma_5^3(i\sqrt{2}) = \sigma_6(i\sqrt{2}^2) = -i(i\sqrt{2})^2 = i\sqrt{2}
\]
so that 
\[
<\sigma_5^2, \sigma_2\sigma_5^3> = \mathbb{Q}(i\sqrt{2})
\]

Now we move on to the order 2 subgroups, which should have fixed fields of degree 4 over $\mathbb{Q}$ (and over which $E$ has degree 2). $\sigma_5$ fixes $i$, and so does $\sigma_3^2$, but $<\sigma_5^2> = \mathbb{Q}(\sqrt{2})$ needs to have degree 4 over $\mathbb{Q}$. However, we saw earlier that $\sigma_5^2$ also fixes $\sqrt{2}$. Thus, 
\[
<\sigma_5^2> = \mathbb{Q}(i, \sqrt{2})
\]
which is an extension of degree 4 over $\mathbb{Q}$.

Work out the next few subgroups yourself. We have 
\[
<\sigma_2> = \mathbb{Q}(\sqrt{2})
\]
and 
\[
<\sigma_2\sigma_5^3> = \mathbb{Q}(i\sqrt{2})
\]

The next one is tricky again. Let’s start with $<\sigma_2\sigma_5^3>$. Notice, $\sigma_2\sigma_5^3 = \sigma_6$. What does $\sigma_6$ fix? Notice that $\sigma_6$ takes $\sqrt{2}$ to $i\sqrt{2}$ and it takes $i\sqrt{2}$ to $\sqrt{2}$. Thus, it must fix their sum, $\sqrt{2} + i\sqrt{2}$. We need to check that this element generates a degree 4 extension over $\mathbb{Q}$. $\sqrt{2} + i\sqrt{2}$ is a root of $x^4 + 8$. Since $8 = 2^3$, the Eisenstein criterion doesn’t work, but we can see that it has no roots in $\mathbb{Q}$, and $x^4 + 8 = (x^2 + 2i\sqrt{2})(x^2 - 2i\sqrt{2})$. Since these polynomials are not in $\mathbb{Q}[x]$ and since factorization in $\mathbb{C}[x]$ is unique, this polynomial must be irreducible over $\mathbb{Q}$. Thus, $[\mathbb{Q}(\sqrt{2} + i\sqrt{2}) : \mathbb{Q}] = 4$ and so 
\[
<\sigma_2\sigma_5^3> = \mathbb{Q}(\sqrt{2} + i\sqrt{2})
\]

**NOTE:** That $\sigma_6$ fixes $\sqrt{2} + i\sqrt{2}$ is not something that you should realize a priori. In general, if you can’t figure out what gets fixed after a few minutes of playing around, here is what you could do. Notice that, by the multiplication theorem, a basis for $E$ over $\mathbb{Q}$ is $\{1, i, \sqrt{2}, \sqrt{2}i, i\sqrt{2}, i\sqrt{2}i\}$. Take an arbitrary linear combination of these elements, assume it is fixed by $\sigma_6$, and see what equations you get for the coefficients in the linear combination. The set of all elements that satisfy the equations gives you the fixed field of $\sigma_6$. Pick an element that might generate this extension (for us this was $\sqrt{2} + i\sqrt{2}$) and prove that it does in fact generate it (we did this by showing that the degree of $\mathbb{Q}(\sqrt{2} + i\sqrt{2})$ over $\mathbb{Q}$ was 4).

The only fixed field we have left to compute is $<\sigma_2\sigma_5>$. Use what we did for the last subgroup to figure out what $\sigma_2\sigma_5 = \sigma_3$ fixes. You’ll find that 
\[
<\sigma_2\sigma_5> = \mathbb{Q}(\sqrt{2} - i\sqrt{2})
\]

By the Galois correspondence, these must be all of the intermediate fields, and the lattice is given below.

(field lattice image, link on website)
10.2.2(b)
Suppose that $|gal(E : F)| = 2p$. By Theorem 5 in 8.2, the Galois group must either be $C_{2p}$ or $D_{p}$. To determine the possible intermediate field lattices, we need to figure out the subgroup lattices for each of these groups. $C_{2p}$ is straightforward; any cyclic group has exactly one subgroup of order $d$ for each $d$ that divides the order of the group. Let $\sigma$ be a generator of $C_{2p}$. Then the subgroups of $C_{2p}$ are $< \sigma >$, $< \sigma^2 >$, $< \sigma^p >$, and $< \sigma^{2p}> = 1$. The fixed field of $< \sigma >$ is $\mathbb{Q}$, the fixed field of $< \sigma^2 >$ will have degree $2$ over $\mathbb{Q}$, the fixed field of $< \sigma^p >$ will have degree $p$ over $\mathbb{Q}$, and the fixed field of $1$ will be all of $E$.

Now consider $D_{p}$. It is generated by an element $r$ of order $p$ and an element $s$ of order $2$ such that $rs = sr^{-1}$. Any element in $D_{p}$ is of the form $r^i s^j$ where $i = 0, ..., p - 1$ and $s = 0$ or $1$. Notice that

$$(r^i s)^2 = r^i s r^i s = sr^{-1} r^i s = s^2 = 1$$

so for any $i = 0, ..., p - 1$, $r^i s$ generates a subgroup of order $2$. Since the order of $r$ is $p$, for any $i = 1, ..., p - 1$, $r^i$ will also have order $p$ (since $i$ and $p$ are coprime) and thus $< r^i > = < r >$ for any $i = 1, ..., p$. Thus, there is only one subgroup of order $p$ (actually, we also know this from the Sylow theorems: any subgroup of index 2 is normal, and if a Sylow $p$-subgroup is normal, it is unique). Any subgroup of order $2$ must be generated by one element, and we have enumerated all of the subgroups generated by one element, so every subgroup of order $2$ must be of the form $r^i s$ for some $i = 0, ..., p - 1$. Thus, $D_{p}$ has $p$ subgroups of order $2$ and one subgroup of order $p$.

Translating this to the lattice of intermediate fields, this means that there will be $p$ subfields of degree $p$ over $\mathbb{Q}$ and one subfield of degree $2$ over $\mathbb{Q}$. □

10.2.3 Suppose $E = GF(p^n)$. Example 6 in 10.1 shows that $gal(E : \mathbb{F}_p)$ is cyclic of order $n$ and is generated by the Frobenius automorphism, $\sigma$, given by $\sigma(x) = x^p$. Since $|E| = p^n$ and $|\mathbb{F}_p| = p$, we have that $[E : \mathbb{F}_p] = n$. But by the Dedekind-Artin Theorem, $|gal(E : \mathbb{F}_p)| = [E : E_G]$. Thus, $[E : E_G] = n$. But we have that $E_G \supset \mathbb{F}_p$ so that

$$n = [E : \mathbb{F}_p] = [E : E_G] \cdot [E_G : \mathbb{F}_p] = n \cdot [E_G : \mathbb{F}_p]$$

which forces $[E_G : \mathbb{F}_p] = 1$. That is, $(G^o =) E_G = \mathbb{F}_p$. Thus, condition (a) of Lemma 4 is satisfied, so $GF(p^n)$ is a Galois extension.

We have that $gal(GF(p^{12}) : \mathbb{F}_p)$ is cyclic of order $12$, generated by the Frobenius automorphism, $\sigma$. It will have a subgroup of each order which divides $12$. Thus, the subgroups are

$$< \sigma >= C_{12}, < \sigma^2 >= C_6, < \sigma^3 >= C_4, < \sigma^4 >= C_3, < \sigma^6 >= C_2, < \sigma^9 >= \{1\}$$

The fixed fields of each of these are

$$< \sigma >^o = \mathbb{F}_p, < \sigma^2 >^o = GF(p^2), < \sigma^3 >^o = GF(p^3),$$

$$< \sigma^4 >^o = GF(p^4), < \sigma^6 >^o = GF(p^6), < \sigma^9 >^o = GF(p^{12})$$

and the lattice of intermediate fields is

(intermediate field lattice picture. link on website)

□

10.2.5(a)
Let $E = F(t)$. Let $G = < \sigma >$ where $\sigma(t) = -t$ is an $F$-automorphism of $E$. By the Dedekind-Artin Theorem, $|G| = [E : E_G]$. Since $\sigma^2(t) = t$, we have that $|G| = 2$. Thus, $[E : E_G] = 2$. What sorts of rational functions does $\sigma$ fix? It certainly fixes ones with no odd degree terms. Does it fix any others? Notice that $t$ is a root of $x^2 - t^2 \in F(t^2)[x]$. Thus, $[E : F(t^2)] \leq 2$. But since $t \notin F(t^2)$ (check this), we have that $[E : F(t^2)] = 2$ (thus, $x^2 - t^2$ is the minimal polynomial of $t$ over $F(t^2)$). Since $G$ fixes everything in $F(t^2)$, we have that $F(t^2) \subseteq E_G$. Since $[E : E_G] = 2$, we must have that $E_G = F(t^2)$.

□

10.2.5(b)
This one is not on the optional homework, but it is an interesting problem, and I meant to do it in section but I think I ran out of time. Let $G = <\sigma>$, where $\sigma(t) = 1 - t$ is an $F$-automorphism of $E = F(t)$. We would have to be very clever or very persistent to find all of the rational functions $\alpha(t)$ such that $\alpha(1 - t) = \alpha(t)$ directly. Let’s use some general theory instead. Notice that $\sigma^3(t) = \sigma(1 - t) = 1 - \sigma(t) = 1 - (1 - t) = t$, so that the order of $\sigma$ is 2. Thus, $|G| = 2$ and using the Dedekind-Artin theorem as above, we have that $[E : E_G] = 2$. Notice that $\sigma$ fixes the polynomial $t(1 - t)$. Thus, $F(t(1 - t)) \subseteq E_G$. Also, $t$ is a root of the polynomial $x^2 - x + t(1 - t) \in F(t(1 - t))[x]$. Check that $t \notin F(t(1 - t))$ so that $[E : F(t(1 - t))] = 2$ and so $x^2 - x + t(1 - t)$ is the minimal polynomial of $t$ over $E_G = F(t(1 - t))$. □


10.3.2(a) Let $f(x) = x^5 - 4x - 2$. Let $E$ be the splitting field of $f(x)$. Since $f$ has (at most) five roots and any automorphism of $E$ must permute the roots, the Galois group of $E$ over $\mathbb{Q}$ must be a subgroup of $S_5$. We will show that, as a subgroup of $S_5$, $\text{gal}(E : \mathbb{Q})$ contains a 5-cycle and a transposition. By Lemma 2, a 5-cycle and a transposition generate $S_5$, so this will prove that $\text{gal}(E : \mathbb{Q}) \cong S_5$.

First, notice that $f(x)$ is Eisenstein for $p = 2$, hence irreducible. If $u$ is any one root of $f$ in $\mathbb{C}$, we have that $\mathbb{Q} \subseteq \mathbb{Q}(u) \subseteq E$, and since $f$ is irreducible, it is the minimal polynomial for $u$ over $\mathbb{Q}$. Thus, $[\mathbb{Q}(u) : \mathbb{Q}] = 5$, and by the multiplication theorem, this means that 5 divides $[E : \mathbb{Q}]$. Then 5 divides $|\text{gal}(E : \mathbb{Q})|$, so by Cauchy’s theorem, the Galois group contains an element of order 5. But the only elements of order 5 in $S_5$ are the 5-cycles, so, as a subgroup of $S_5$, the Galois group must contain a 5-cycle.

Now let us show that the Galois group also contains a transposition. We do this by showing that $f$ has exactly two complex roots. Indeed, we have that $f'(x) = 5x^4 - 4$, which has zeros at $x = \pm \sqrt[5]{4/5}$. The second derivative is $f''(x) = 20x^3$, which is negative at $x = -\sqrt[5]{4/5}$ and positive at $x = \sqrt[5]{4/5}$. Thus, by the second derivative test, $f(x)$ must have a maximum at $x = -\sqrt[5]{4/5}$ and a minimum at $x = \sqrt[5]{4/5}$ and no other local extrema. Check that $f$ is positive at $x = -\sqrt[5]{4/5}$ and negative at $x = -\sqrt[5]{4/5}$. Sketch the graph of $f$. The above shows that it crosses the $x$-axis exactly 3 times. Since $f$ has 5 distinct roots (since it is irreducible and we in characteristic zero), exactly two of its roots must be complex. Since $E$ is Galois over $\mathbb{Q}$, the automorphism $\tau$ of $\mathbb{C}$ given by complex conjugation restricts to an automorphism of $E$. $\tau$ must fix the real roots, and since no complex number is fixed under complex conjugation, $\tau$ must transpose the two complex roots. This corresponds to a transposition in the Galois group, thought of as a subgroup of $S_5$.

Thus, by Lemma 2, $\text{gal}(E : \mathbb{Q}) \cong S_5$. But $S_5$ is not solvable, and thus $f(x)$ is not solvable by radicals. □

10.3.3 Let $f(x) = x^7 - 14x + 2$. Let $E$ be the splitting field for $f(x)$ over $\mathbb{Q}$. $f(x)$ is Eisenstein for $p = 2$, hence irreducible, so 7 divides $[E : \mathbb{Q}]$, so the Galois group contains an element of order 7. Thought of as a subgroup of $S_7$, the Galois group must contain a 7-cycle, since the only elements of order 7 in $S_7$ are 7-cycles. Using the second derivative test, we can show that $f(x)$ has 3 real roots and four nonreal roots. UPDATE: Ignore this problem. It could be figured out using some hard work and a theorem that is slightly outside the scope of our class. Ask me about it if you’re interested.)

10.3.4 This one is just like the previous two problems. Use the fact that $f(x)$ is irreducible to show that $p$ divides the order of the Galois group, and hence the Galois group contains a $p$-cycle. Use the fact that
$f$ has exactly two nonreal roots to show that the Galois group contains a transposition. Use Lemma 2 to conclude that the Galois group must be $S_p$. □