Homework #12 Solutions

Handout, #1 We induct on the degree of \( f(x) \). If \( \deg f(x) = 1 \) then \( f(x) \) has no multiple roots and we can take \( g(x) = f(x), \ n = 0 \). Now suppose that \( \deg f(x) > 1 \) and that the statement holds for all irreducible polynomials with degree strictly less that \( \deg f(x) \). If \( f(x) \) has no multiple roots then again we may take \( g(x) = f(x) \) and \( n = 0 \). If \( f(x) \) does have multiple roots then, since \( f(x) \) is irreducible, we know that there must exist \( g_0(x) \in F[x] \) so that \( f(x) = g_0(x^p) \). The polynomial \( g_0(x) \) certainly has degree less than that of \( f(x) \) and must also be irreducible (otherwise \( f(x) \) would be reducible). The induction hypothesis then implies that \( g_0(x) = g(x^{p^n}) \) for some \( n \geq 0 \) and an irreducible \( g(x) \in F[x] \) with no multiple roots. But then we have

\[
f(x) = g_0(x^p) = g((x^p)^p^n) = g(x^{p^n+1})
\]

which shows that the result holds for \( f(x) \) as well. It follows, by (strong) induction, that the statement holds for all irreducible \( f(x) \in F[x] \).

Handout, #2

a. Since \( g(x) \) has no multiple roots, it must be that

\[
g(x) = c(x - b_1) \cdots (x - b_m)
\]

for some nonzero \( c \in F \). Therefore

\[
f(x) = g(x^{p^n}) = c(x^{p^n} - b_1) \cdots (x^{p^n} - b_m).
\]

b. By part (a) we have

\[0 = f(a) = c(a^{p^n} - b_1) \cdots (a^{p^n} - b_m)\]

which implies \( a^{p^n} - b_i = 0 \), or \( a^{p^n} = b_i \), for some \( i \).

c. Part (b) shows that the assignment \( a \mapsto a^{p^n} \) defines a function from the set of roots of \( f(x) \) in \( E \) to the set of roots of \( g(x) \in K \). This function is one-to-one since if \( a \) and \( a' \) are both roots of \( f(x) \) with \( a^{p^n} = (a')^{p^n} \) then \( 0 = a^{p^n} - (a')^{p^n} = (a - a')^{p^n} \) (since the characteristic of \( E \) is \( p \)) so that \( a = a' \). It follows that \( f(x) \) has at most \( m \) roots. We claim that this function is also onto, which proves that \( f(x) \) has exactly \( m \) roots. To see this, fix a root \( b \) of \( g(x) \) and let \( a \) be a root of \( x^{p^n} - b \) in some extension of \( K \). Then \( a^{p^n} = b \) so that \( (a) = (a^{p^n}) = g(b) = 0 \). It follows that \( a \) must belong to \( E \) and since \( a^{p^n} = b \) this proves our map is surjective, and we’re finished.

Handout, #3 According to part (c) we can order the roots of \( f(x) \) so that \( (a_i)^{p^n} = b_i \) for all \( i \). Then, by part (a), we have

\[
f(x) = c(x^{p^n} - b_1) \cdots (x^{p^n} - b_m) = c(x^{p^n} - a_1^{p^n}) \cdots (x^{p^n} - a_m^{p^n}) = c(x - a_1)^{p^n} \cdots (x - a_m)^{p^n}
\]
where in the last line we have used the fact that the characteristic of $E[x]$ is the same as that of $E$, namely $p$.

p 378, #10 If $a$ is algebraic over $\mathbb{Q}$ then there is a nonzero polynomial $f(x) \in \mathbb{Q}[x]$ so that $f(a) = 0$. Let $g(x) = f(x^2) \in \mathbb{Q}[x]$. Then $g(x)$ is nonzero and $g(\sqrt{a}) = f((\sqrt{a})^2) = f(a) = 0$, so that $\sqrt{a}$ is algebraic over $\mathbb{Q}$ as well.

p 378, #18 Choose $\alpha \in E$ so that $\alpha \notin \mathbb{Q}$. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ must be greater than 1 and divide $[E : \mathbb{Q}] = 2$. Hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$. Since $2 = [E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$, this implies $[E : \mathbb{Q}(\alpha)] = 1$ so that $E = \mathbb{Q}(\alpha)$. Since $\alpha$ has degree 2 over $\mathbb{Q}$, there is an irreducible polynomial $x^2 + ax + b \in \mathbb{Q}[x]$ of which $\alpha$ is a root. Then, according to the quadratic formula

$$\alpha = \frac{-a \pm \sqrt{a^2 - 4b}}{2}.$$

Since $a, 2 \in \mathbb{Q}$, this implies $E = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{a^2 - 4b})$. Write $a^2 - 4b = r/s$ with $r, s \in \mathbb{Z}$, $s > 0$. Then $\sqrt{a^2 - 4b} = \sqrt{rs}/s = \sqrt{rs}/s$ so that now $E = \mathbb{Q}(\sqrt{a^2 - 4b}) = \mathbb{Q}(\sqrt{rs})$. Finally, write $rs = q^2d$ where $q, d \in \mathbb{Z}$ and $d > 0$ is not divisible by the square of any prime. Then $\sqrt{rs} = q\sqrt{d}$ and we have $E = \mathbb{Q}(\sqrt{rs}) = \mathbb{Q}(\sqrt{d})$, as desired.

p 379, #26 Since $x^3 - 1 = (x - 1)(x^2 + x + 1)$ we see that $a^3 - 1 = 0$. Therefore $a^3 = 1$ and $a^4 = a$. Taking square roots on both sides yields $a^2 = \sqrt{a}$. From this it follows that $\sqrt{a} \in \mathbb{Q}(a)$ so that $\mathbb{Q}(\sqrt{a}) \subseteq \mathbb{Q}(a)$. Since we obviously have $\mathbb{Q}(a) \subseteq \mathbb{Q}(\sqrt{a})$ we see that $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(a)$.

p 379, #28 Write $r = m/n$ with $m, n \in \mathbb{Z}$ and $n > 0$. Suppose that $a$ is a root of $f(x) \in \mathbb{Q}[x]$, $f(x) \neq 0$. Then $a^{1/n}$ is a root of $g(x) = f(x^n) \in \mathbb{Q}[x]$, so that $a^{1/n}$ is algebraic over $\mathbb{Q}$. From this it follows that $\mathbb{Q}(a^{1/n})$ is an algebraic extension of $\mathbb{Q}$. Since $a^r = (a^{1/n})^n \in \mathbb{Q}(a^{1/n})$, we see that $a^r$ is algebraic over $\mathbb{Q}$. 
