Homework #13 Solutions

p 377, #6 Let $m = \deg f(x)$, $n = \deg g(x)$ and let b be a root of $g(x)$ in some extension of $F(a)$. We start by observing that, since $f(x)$ and $g(x)$ are irreducible over F, we have

$$\begin{aligned}[F(a,b):F] &= [F(a,b):F(a)][F(a):F] = [F(a,b):F(a)]m \\ [F(a,b):F] &= [F(b,a):F(b)][F(b):F] = [F(b,a):F(b)]n\end{aligned}$$

so that $[F(a,b):F]$ is divisible by both m and n. Since m and n are relatively prime, this implies that $[F(a,b):F]$ is actually divisible by mn.

Since $g(b) = 0$ and $g(x) \in F(a)[x]$, the minimal polynomial $\widehat{g}(x)$ of b over $F(a)$ divides $g(x)$. This means that $[F(a,b):F(a)] = \deg \widehat{g}(x) \leq \deg g(x) = n$. Our computations above then show that $[F(a,b):F] = [F(a,b):F(a)]m \leq nm$. Since mn divides $[F(a,b):F]$, it must actually be the case that $[F(a,b):F] = mn$. Comparing this with $[F(a,b):F] = [F(a,b):F(a)]m$, we immediately conclude that $\deg \widehat{g}(x) = [F(a,b):F(a)] = n = \deg g(x)$. Since $\widehat{g}(x)$ divides $g(x)$ we find that $g(x)$ and $\widehat{g}(x)$ must differ only by a constant in $F(a)$. Since $\widehat{g}(x)$ is irreducible over $F(a)$, the same must therefore be true for $g(x)$.

p 378, #8 According to Example 21.6 of the text, $\mathbb{Q}(\sqrt{3}+\sqrt{5})$ has degree 4 over $\mathbb{Q}$. Since $\mathbb{Q}(\sqrt{15})$ has degree 2 over $\mathbb{Q}$, we must have $[\mathbb{Q}(\sqrt{3}+\sqrt{5}):\mathbb{Q}(\sqrt{15})] = 2$ from which it follows that $\{1, \sqrt{3}+\sqrt{5}\}$ is a basis for $\mathbb{Q}(\sqrt{3}+\sqrt{5})$ over $\mathbb{Q}(\sqrt{15})$.

Since $\sqrt{2} = \sqrt[4]{2}^2 \in \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{2})$, we conclude that $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{2})$. Moreover, since $x^3 - 2, x^4 - 2$ are irreducible over $\mathbb{Q}$ of relatively prime degree, exercise 6 implies that $x^4 - 2$ is irreducible over $\mathbb{Q}(\sqrt[3]{2})$. Thus $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{2}):\mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{2}):\mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 4 \cdot 3 = 12$ and $\{1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}\}$ is a basis for $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{2})$ over $\mathbb{Q}(\sqrt[3]{2})$. Since $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ is a basis for $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$, we know that we can obtain a basis for $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{2})$ over $\mathbb{Q}$ by multiplying the previous two bases together. Therefore, a basis for our extension over $\mathbb{Q}$ is

$$\{1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}, \sqrt[3]{2}, \sqrt[3]{2}\sqrt[4]{2}, \sqrt[3]{2}\sqrt[4]{4}, \sqrt[3]{2}\sqrt[4]{8}, \sqrt[3]{4}, \sqrt[3]{4}\sqrt[4]{2}, \sqrt[3]{4}\sqrt[4]{4}, \sqrt[3]{4}\sqrt[4]{8}\}.$$

p 378, #16 Let $\alpha = \sqrt[3]{2} + \sqrt[3]{4}$. Then $\alpha^3 = 6 + 6\sqrt[3]{2} + 6\sqrt[3]{4} = 6 + 6\alpha$ so that α is a root of $f(x) = x^3 - 6x - 6 \in \mathbb{Q}[x]$. Since this polynomial is monic and irreducible (by Eisenstein's criterion with the prime 2), it must be the minimal polynomial for α.

p 378, #20 It was proven in class that if $a_1, \ldots, a_n$ are algebraic over F then $E = F(a_1, \ldots, a_n)$ has finite degree over F. Therefore we only prove the converse. Let $[E:F] = n < \infty$. Then there exist $a_1, \ldots, a_n \in E$ that form a basis for E over F. Since E is of finite degree over F we know that each a_i is algebraic over F, and because the a_i's form a basis for E over F we clearly have $E = F(a_1, \ldots, a_n)$.

p 378, #22 We have the following inclusion diagram:

$$\begin{array}{c} F(a) \\ | \\ F(f(a)) \\ | \\ F \end{array}$$

Since a is a root of $f(x) - f(a) \in F(f(a))[x]$, $F(a)$ is algebraic over $F(f(a))$. Since $f(a)$ is algebraic over F, $F(f(a))$ is algebraic over F. It follows that $F(a)$ is algebraic over F and hence that a is algebraic over F.

p 388, #6 Since the two given polynomials have degree two and are irreducible over $\mathbb{Z}_3$, both rings are fields with nine elements and are therefore isomorphic to GF(9), and hence to each other.

p 388, #8 The finite fields that contain $\mathrm{GF}(p^5)$ are those of the form $\mathrm{GF}(p^{5k})$, where $k \in \mathbb{Z}^+$. In order for $\mathrm{GF}(p^5)$ to be a proper subfield we need $k \geq 2$ and in order for $\mathrm{GF}(p^5)$ to be the largest subfield we need 5 to be the largest proper divisor of $5k$. This is the case only when $k = 2, 3, 5$ and so the subfields in question are $\mathrm{GF}(p^{10})$, $\mathrm{GF}(p^{15})$, and $\mathrm{GF}(p^{25})$.

p 388, #20 Since $g(x)$ divides $x^{p^n} - x$ and every element in $\mathrm{GF}(p^n)$ is a root of the latter, we see that $\mathrm{GF}(p^n)$ contains every root of $g(x)$. Let a be any such root in GF. Then we have

$$\begin{aligned} n &= [\mathrm{GF}(p^n) : \mathrm{GF}(p)] \\ &= [\mathrm{GF}(p^n) : \mathrm{GF}(p)(a)]\,[\mathrm{GF}(p)(a) : \mathrm{GF}(p)] \\ &= [\mathrm{GF}(p^n) : \mathrm{GF}(p)(a)]\deg g(x) \end{aligned}$$

since the irreducibility of $g(x)$ over $\mathrm{GF}(p)$ implies $[\mathrm{GF}(p)(a) : \mathrm{GF}(p)] = \deg g(x)$. This is what we were asked to show.

p 388, #22 For *any* prime p we have

$$\begin{tikzcd}
\mathrm{GF}(p^{18}) \arrow[d, dash] \arrow[dr, dash] & & \\
\mathrm{GF}(p^9) \arrow[dr, dash] & \mathrm{GF}(p^6) \arrow[d, dash] \arrow[dr, dash] & \\
& \mathrm{GF}(p^3) \arrow[dr, dash] & \mathrm{GF}(p^2) \arrow[d, dash] \\
& & \mathrm{GF}(p)
\end{tikzcd}$$

and

$$\begin{tikzcd}
& \mathrm{GF}(p^{30}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathrm{GF}(p^{15}) \arrow[d, dash] \arrow[dr, dash] & \mathrm{GF}(p^{10}) \arrow[dl, dash] \arrow[dr, dash] & \mathrm{GF}(p^6) \arrow[dl, dash] \arrow[d, dash] \\
\mathrm{GF}(p^2) \arrow[dr, dash] & \mathrm{GF}(p^3) \arrow[d, dash] & \mathrm{GF}(p^5) \arrow[dl, dash] \\
& \mathrm{GF}(p) &
\end{tikzcd}$$

p 389, #24 Let E be a splitting field for $p(x)$ over $\mathbb{Z}_p$. Since E is obtained from $\mathbb{Z}_p$ by adjoining finitely many algebraic elements (i.e. the roots of $p(x)$), we know that E is a finite extension of $\mathbb{Z}_p$. Therefore, E is isomorphic to $GF(p^n)$ for some n. Since every element of $GF(p^n)$ is a root of the polynomial $x^{p^n} - x$, the same is true of the elements of E. Since E contains the roots of $p(x)$, the roots of $p(x)$ must also be roots of $x^{p^n} - x$. As none of the roots of $p(x)$ are repeated, this implies that $p(x)$ divides $x^{p^n} - x$.