Solutions to Homework 6

Problem 1. Cox, Section 5.2, Exercise 1:
Prove that $\mathbb{Q}(\sqrt[4]{2})$ is not the splitting field (over $\mathbb{Q}$) of any polynomial in $\mathbb{Q}[x]$.

Proof. Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$, which has a root $\alpha = \sqrt[4]{2}$ in $K = \mathbb{Q}(\sqrt[4]{2})$. Note that f is irreducible over $\mathbb{Q}$, by Eisenstein's Criterion with $p = 2$.
However, $K \subseteq \mathbb{R}$, so K does *not* contain the root $\beta = i\sqrt[4]{2}$ of f. Since f is irreducible over $\mathbb{Q}$, then $K/\mathbb{Q}$ is *not* a normal extension.
If K were the splitting field of some $g \in \mathbb{Q}[x]$, then by Theorem 5.2.4, $K/\mathbb{Q}$ would be a normal extension. This is a contradiction, so K is not a splitting field over $\mathbb{Q}$. QED

Problem 2. Cox, Section 5.2, Exercise 3:
For each of the following field extensions, determine whether or not it is normal. (And, of course, prove your answers.)

(a) $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, where $n \geq 1$ and $\zeta_n = e^{2\pi i/n}$, a primitive n-th root of unity.
(b) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})/\mathbb{Q}$
(c) $F(\alpha)/F$, where $F = \mathbb{F}_3(t)$ and α is a root of $x^3 - t \in F[x]$.

Solutions/Proofs. (a): Yes, normal. Let $f(x) = x^n - 1 \in \mathbb{Q}[x]$, and let ζ_n denote a primitive n-th root of unity. Then the roots of f are $\{\zeta_n^j : 0 \leq j \leq n-1\}$, all of which lie in $\mathbb{Q}(\zeta_n)$. Therefore, $\mathbb{Q}(\zeta_n)$ is the splitting field of f over $\mathbb{Q}$. Hence, by Theorem 5.2.4, the extension is normal. QED

(b): No, not normal. We have $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \subseteq \mathbb{R}$. However, $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ contains a root $\sqrt[3]{2}$ of $x^3 - 2 \in \mathbb{Q}[x]$, which is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion with $p = 2$. If the extension were normal, then $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ would also contain the root $\zeta_3\sqrt[3]{2} \notin \mathbb{R}$. This is a contradiction, so the extension is not normal. QED

(c): Yes, normal. Working in the ring $F(\alpha)[x]$, we have $(x - \alpha)^3 = x^3 - \alpha^3 = x^3 - t$. Thus, the polynomial $x^3 - t \in F[x]$ factors completely as $(x - \alpha)^3$ over $F(\alpha)$. Therefore, $F(\alpha)$ is the splitting field of $x^3 - t$ over F, and hence (by Theorem 5.2.4 again) the extension is normal. QED

Problem 3. Cox, Section 5.2, Exercise 4:
Give an example of a normal extension of fields that is not finite. (And, of course, prove your answer.)

Solution/Proof. Let $L = \overline{\mathbb{Q}}$, which we know from another exercise [HW 5, Problem 1; i.e., Cox 4.4, Exercise 1] is an infinite extension of $\mathbb{Q}$. Then every irreducible $f \in \mathbb{Q}[x]$ (and in particular, every such f that has a root in L, i.e., every such f) splits completely over L. By definition, $L/\mathbb{Q}$ is normal. QED

Problem 4. Cox, Section 5.3, Exercise 1:
Prove equations (5.6). That is, for any $g, h \in F[x]$ and any $a, b \in F$, prove that:

(a) $(ag + bh)' = ag' + bh'$
(b) $(gh)' = g'h + gh'$

Here, of course, f' denotes the **formal derivative** of $f \in F[x]$.

Proof. Given $g, h \in F[x]$, write $g = \sum_{j \geq 0} A_j x^j$ and $h = \sum_{j \geq 0} B_j x^j$, where both are actually finite sums.

(a) We compute $ag + bh = a\sum_{j \geq 0} A_j x^j + b\sum_{j \geq 0} B_j x^j = \sum_{j \geq 0}(aA_j + bB_j)x^j$, so

$$(ag + bh)' = \sum_{j \geq 0} j(aA_j + bB_j)x^{j-1} = a\sum_{j \geq 0} jA_j x^{j-1} + b\sum_{j \geq 0} jB_j x^{j-1} = ag' + bh' \quad \text{QED}$$

(b) First, consider the case that $g = A_n x^n$ for some $n \geq 0$. Then $gh = \sum_{j\geq 0} A_n B_j x^{j+n}$, and hence

$$(gh)' = \sum_{j\geq 0}(j+n)A_nB_jx^{j+n-1} = \sum_{j\geq 0} nA_nB_jx^{j+n-1} + \sum_{j\geq 0} jA_nB_jx^{j+n-1}$$
$$= nA_nx^{n-1}\sum_{j\geq 0} nA_nB_jx^j + A_nx^n \sum_{j\geq 1} jB_jx^{j-1} = g'h + gh'.$$

Second, we consider the general case that $g = \sum_{j\geq 0} A_j x^j$. Then $gh = \sum_{j\geq 0} A_j x^j h$. Therefore, applying part (a), we have

$$(gh)' = \sum_{j\geq 0}\left(A_jx^jh\right)' = \sum_{j\geq 0}\left(jA_jx^{j-1}h + A_jx^jh'\right) = \sum_{j\geq 0} jA_jx^{j-1}h + \sum_{j\geq 0} A_jx^jh' = g'h + gh',$$

where the second equality is by the first case above of this part (b). QED

Problem 5. Cox, Section 5.3, Exercise 2:
Let F be a field of characteristic $p \geq 2$. Recall (from Lemma 5.3.10) that for all $\alpha, \beta \in F$, we have $(\alpha+\beta)^p = \alpha^p + \beta^p$. Use this to prove the following identities for all $\alpha, \beta \in F$:

(a) $(\alpha-\beta)^p = \alpha^p - \beta^p$

(b) $(\alpha+\beta)^{p^e} = \alpha^{p^e} + \beta^{p^e}$, for any integer $e \geq 1$.

Proof. (a) We claim that in F, we have $(-1)^p = -1$. If p is odd, this is clearly true. If $p = 2$, then $2 = 0$, so that $-1 = 1$, and hence $(-1)^2 = 1 = -1$, proving our claim.

Writing $\alpha - \beta = \alpha + (-\beta)$, we have $(\alpha-\beta)^p = \alpha^p + (-\beta)^p = \alpha^p + (-1)^p\beta^p = \alpha^p - \beta^p$,
where the final equality is by our claim. QED

(b) We proceed by induction on $e \geq 1$. The case $e = 1$ is given to us. Assuming the identity holds for $e-1$, then

$$(\alpha+\beta)^{p^e} = \left((\alpha+\beta)^p\right)^{p^{e-1}} = \left(\alpha^p+\beta^p\right)^{p^{e-1}} = \left(\alpha^p\right)^{p^{e-1}} + \left(\beta^p\right)^{p^{e-1}} = \alpha^{p^e} + \beta^{p^e}.$$ QED

Problem 6. Cox, Section 5.3, Exercise 3:
Let F be a field of characteristic $p \geq 2$, let $n \geq 1$, and define L to be the splitting field of $x^n - 1$ over F. The n-th roots of unity are defined to be the roots of $x^n - 1$ in L.

(a) If $p \nmid n$, prove that there are n distinct n-th roots of unity in L.

(b) Prove that there is only one p-th root of unity, namely $1 \in F$.

Proof. (a) Let $f = x^n - 1$. Then $f' = nx^{n-1}$. Since $p \nmid n$, we have $n \neq 0$ as an element of F, so f' is a nonzero element of $F[x]$ that factors as a nonzero constant times a power of x. Since $x \nmid f$ (since $f(0) = -1 \neq 0$), we have $(f, f') = 1$. By Proposition 5.3.2, f is separable. That is, the n roots of f in L (i.e., the n-th roots of unity) are all distinct. QED

(b) For $n = p$, we have $f = x^p - 1 = (x-1)^p$, so the only root of f is $1 \in F$. (Repeated p times.) QED

Problem 7. Cox, Section 5.3, Exercise 7:
Let F be a field of characteristic $p \geq 2$, and let $f \in F[x]$ be irreducible. In this problem you'll prove Proposition 5.3.16.

(a) Suppose f' is **not** the zero polynomial. Prove that f is separable.
[Cox suggests using the argument in the proof of Lemma 5.3.5.]

(b) Suppose f' **is** the zero polynomial.
Prove that there is a polynomial $g_1 \in F[x]$ such that $f(x) = g_1(x^p)$.

(c) In the situation of part (b), prove that the polynomial g_1 is irreducible.

(d) Prove Proposition 5.3.16: For any $f \in F[x]$ irreducible, there is an integer $e \geq 0$ and a separable, irreducible $g \in F[x]$ such that $f(x) = g\big(e^{p^e}\big)$.
[**Suggestion**: Cox says to "apply parts (a)–(c) repeatedly".]

Proof. (a) Since $f' \in F[x]$ is not zero and $F[x]$ is a UFD, f' has a factorization into irreducibles. If $q \in F[x]$ is an irreducible dividing f', then $\deg(q) \leq \deg(f') < \deg(f)$. Therefore, the two irreducibles q and f are not constant multiples of one another, so $q \nmid f$. This is true for all irreducible factors q of f', and hence $(f', f) = 1$. Thus, by Proposition 5.3.2, f is separable. QED

(b) Write $f = a_n x^n + \cdots + a_0$, so that $f' = n a_n x^{n-1} + \cdots + a_1$. Since $f' = 0$, we have $j a_j = 0$ in F for all $j = 0, \ldots, n$. However, $j = 0$ in F if and only if $p|j$ in $\mathbb{Z}$. Thus, we have $a_j = 0$ for all j with $p \nmid j$. That is, we have $f = a_{pm} x^{pm} + a_{p(m-1)} x^{p(m-1)} + \cdots + a_p x^p + a_0$.
Let $g_1(x) = a_{pm} x^m + a_{p(m-1)} x^{m-1} + \cdots + a_p x + a_0$. Then $g_1 \in F[x]$, and $f(x) = g_1(x^p)$, as desired. QED

(c) Suppose g_1 factors as $g_1 = h_1 h_2$ with $h_1, h_2 \in F[x]$. Then $f(x) = g_1(x^p) = h_1(x^p) h_2(x^p)$ also factors. Since f is irreducible, it must be that either $h_1(x^p)$ or $h_2(x^p)$ is constant. That is, either h_1 or h_2 is constant. Thus, g_1 is irreducible. QED

(d) Let $S = \{j \geq 0 : \exists g_j \in F[x] \text{ s.t. } f(x) = g_j(x^{p^j})\}$. Note that any g_j with $f(x) = g_j(x^{p^j})$ must be nonconstant, since f is nonconstant. Thus,

$$\deg(f) = \deg(g_j(x^{p^j})) = p^j \deg(g_j) \geq p^j,$$

so that S is bounded above. [By $\log_p(\deg(f))$, but that detail is unimportant.] In addition, we have $0 \in S$, since $f(x) = g_0(x^1)$ with $g_0 = f$. Thus, S is a nonempty finite set of integers and hence has a largest element $e \in S$. By definition of S, there is some $g = g_e \in F[x]$ such that $f(x) = g(x^{p^e})$.
Suppose, towards contradiction, that $g' = 0$. Then by part (b) applied to g, there is some $g_{e+1} \in F[x]$ such that $g(x) = g_{e+1}(x^p)$, and hence $f(x) = g_{e+1}(x^{p^{e+1}})$. Therefore, $e + 1 \in S$, contradicting the maximality of e.
Thus, g' is *not* identically zero. Therefore, by part (a), g is separable. Finally, g is irreducible over F by the same argument as in part (c). [Or by an induction using part (c), if you prefer.] QED

Problem 8. Cox, Section 5.3, Exercise 9:
Let F be a field of characteristic $p \geq 2$, let $a \in F$, and define $f(x) = x^p - a$. Suppose that f has no roots in F (and hence is irreducible over F, by Proposition 4.2.6). Let α be a root of f in some extension L/F.

(a) Prove that $F(\alpha)$ is the splitting field of f over F and that $[F(\alpha) : F] = p$.
[Cox suggests using the argument in Example 5.3.11.]

(b) Let $\beta \in F(\alpha)$ with $\beta \notin F$. Use Lemma 5.3.10 to prove that $\beta^p \in F$.

(c) For β as in part (b), use parts (a) and (b) to prove that the minimal polynomial of β over F is $x^p - \beta^p$.

(d) Conclude by proving that the extension $F(\alpha)/F$ is purely inseparable.

Proof. (a) As noted in the statement of the problem, f is irreducible over F by Proposition 4.2.6. By Lemma 5.3.10, we have
$(x - \alpha)^p = x^p - \alpha^p = x^p - a = f(x)$,
so the only root of f is α. Therefore, $F(\alpha)$ is indeed the splitting field of f over F. Since f is irreducible over F of degree p with root α, it follows that $[F(\alpha) : F] = p$. QED

(b) Given $\beta \in F(\alpha)$, by part (a) and Lemma 4.3.4(b), there exist $c_0, \ldots, c_{p-1} \in F$ such that $\beta = c_0 + c_1 \alpha + \cdots + c_{p-1} \alpha^{p-1}$. Therefore, by Lemma 5.3.10, we have

$\beta^p = c_0^p + c_1^p \alpha^p + c_2^p \alpha^{2p} + \cdots + c_{p-1}\alpha^{p(p-1)} = c_0^p + c_1^p a + c_2^p a^2 + \cdots + c_{p-1} a^{p-1} \in F.$ QED

(c) Given $\beta \in F(\alpha)$ with $\beta \notin F$, part (b) shows that $b = \beta^p \in F$, so that $g(x) = x^p - b \in F[x]$ has β as a root. It suffices to show that g is irreducible.
We have $F(\alpha)/F(\beta)/F$, so that by the Tower Theorem, $[F(\alpha) : F(\beta)][F(\beta) : F] = [F(\alpha) : F] = p$.
In addition, $[F(\beta) : F] > 1$ since $\beta \notin F$. Therefore, since p is prime, we must have $[F(\beta) : F] = p$, and hence the minimal polynomial of β over F has degree p. Since g is monic of degree p with $g(\beta) = 0$, it follows that $g(x) = x^p - \beta^p \in F[x]$ is indeed the minimal polynomial of β over F. QED

(d) By part (c), every $\beta \in F(\alpha)$ with $\beta \notin F$ has minimal polynomial $g(x) = x^p - \beta^p \in F[x]$ over F.
Then g factors as $(x - \beta)^p$ over $F(\alpha)$, which has a repeated root. [Alternatively, the formal derivative is $g' = 0$, so $\gcd(g, g') = g \neq 1$.] Hence, β is not separable over F. QED