Solutions to Homework 7

Problem 1. Cox, Section 5.3, Exercise 10a:
Let F be a field of characteristic $p \geq 2$, and let L/F be a finite extension.

Prove that L/F is purely inseparable if and only if for every $\alpha \in L$,
the minimal polynomial of α over F is of the form $x^{p^e} - a$ for some $e \geq 0$ and some $a \in F$.

Proof. (a) ($\Rightarrow$): Given $\alpha \in L$, let $f \in F[x]$ be the minimal polynomial of α over F. By Proposition 5.3.16, there exist $e \geq 0$ and a separable, irreducible $g \in F[x]$ such that $f(x) = g(x^{p^e})$.
Let $a = \alpha^{p^e}$. Then $g(a) = f(\alpha) = 0$. Since g is monic and irreducible, it is the minimal polynomial of a over L. Thus, a is separable over F, since its minimal polynomial g is separable. Because L/F is purely inseparable, we must have $a \in F$. Because g is monic and irreducible over F, it follows that $g(x) = x - a$, and hence $f(x) = x^{p^e} - a$.

($\Leftarrow$): Given $\alpha \in L \smallsetminus F$, let $f \in F[x]$ be the minimal polynomial of α over F. By assumption, there exist $a \in F$ and $e \geq 0$ such that $f(x) = x^{p^e} - a$.
If $e = 0$, then $f(x) = x - a$. Therefore, because $f(\alpha) = 0$, we have $\alpha = a \in F$, contradicting the fact that $\alpha \in L \smallsetminus F$. Thus, $e \geq 1$, and hence $p | p^e$. Therefore, $f'(x) = p^e x^{p^e - 1} = 0$. It follows that $(f, f') = f \neq 1$, and hence by Proposition 5.3.2, f is not separable. Thus, α is not separable over F, as desired. QED

Problem 2. (not from Cox):
Let $L/M/K$ be finite extensions of characteristic p fields. If L/K is purely inseparable, prove that both M/K and L/M are purely inseparable.

Proof. Given $\alpha \in M \smallsetminus K$, we have $\alpha \in L \smallsetminus K$, whence α is not separable over K, since L/K is purely inseparable. We have therefore shown that M/K is purely inseparable.
Given $\beta \in L \smallsetminus M$, we must show that β is not separable over M. By Problem 1 above (i.e., Cox 5.3, Exercise 10a), the minimal polynomial of β over K is of the form $f(x) = x^{p^e} - a$ for some $a \in K$ and $e \geq 0$. Thus, $f(x) = (x - \beta)^{p^e}$. The minimal polynomial $g \in M[x]$ of β over M must be a factor of $f(x)$ in $M[x]$, and hence $g(x) = (x - \beta)^m$ for some integer $1 \leq m \leq p^e$. If $m = 1$, then $g = x - \beta$, whence $\beta \in M$, a contradiction. Therefore, $m \geq 2$, and hence g has a repeated root (namely β), so g is not separable. Thus, β is not separable over M. Since this is true for all $\beta \in L \smallsetminus M$, we have proven that L/M is purely inseparable. QED

Problem 3. Cox, Section 5.3, Exercise 10b:
Let F be a field of characteristic $p \geq 2$, and let L/F be a finite extension. If L/F is purely inseparable, prove that $[L : F]$ is a power of p.

Proof. Since $[L : F] < \infty$, there exist $\alpha_1, \ldots, \alpha_n \in L$ algebraic over F such that $L = F(\alpha_1, \ldots, \alpha_n)$. Define $K_j = F(\alpha_1, \cdots, \alpha_j)$ for each $j = 0, \ldots, n$. Then $K_n / K_{n-1} / \cdots / K_1 / K_0$ is a tower of extensions of fields, with $K_n = L$ and $K_0 = F$. Moreover, for each $j = 1, \ldots, n$, we have $K_j = K_{j-1}(\alpha_j)$.
By the previous problem [plus an induction argument, technically], observe that K_j / K_{j-1} is purely inseparable for each $j = 1, \ldots, n$.
For each such j, let f_j be the minimal polynomial of $\alpha_j \in K_j$ over K_{j-1}. By part (a) and the fact that K_j / K_{j-1} is purely inseparable, we have $\deg(f_j) = p^{e_j}$ for some integer $e_j \geq 0$. Thus,

$$[K_j : K_{j-1}] = [K_{j-1}(\alpha_j) : K_{j-1}] = \deg(f_j) = p^{e_j} \quad \text{for every } j = 1, \ldots, n.$$

By the Tower Theorem, then,

$$[L : F] = [K_n : K_{n-1}] \cdot \cdots \cdot [K_2 : K_1][K_1 : K_0] = p^{e_n} \cdot \cdots \cdot p^{e_2} \cdot p^{e_1} = p^{e_1 + e_2 + \cdots + e_n}$$ QED

Problem 4. Cox, Section 5.3, Exercise 13:
Let F be a field of characteristic $p \geq 2$, and let L/F be a finite extension with $p \nmid [L : F]$. Prove that L/F is separable.

Proof. Given $\alpha \in L$, let $f \in F[x]$ be the minimal polynomial of α over F. We must show that f is separable.
We know that $\deg(f) = [F(\alpha) : F]$. By the Tower Theorem applied to $L/F(\alpha)/F$, we have

$$[L : F] = [L : F(\alpha)][F(\alpha) : F].$$

Since $p \nmid [L : F]$, it follows that $p \nmid [F(\alpha) : F]$, and hence $p \nmid \deg(f)$.
Thus, $f = a_n x^n + \cdots + a_0$ with $p \nmid n$ and $a_n \neq 0$. Therefore, $na_n \neq 0$ in F, from which it follows that $f' = na_n x^{n-1} + \cdots + a_1 \in F[x]$ is not identically zero. By Exercise 5.3.7(a), i.e. Homework 6, Problem 7(a) [or by Proposition 5.3.16 plus a little work], it follows that f is separable. QED

Problem 5. Cox, Section 5.3, Exercise 14: Let $L/K/F$ be algebraic extensions. Suppose that L/F is separable. Prove that both L/K and K/F are separable.

Proof. First consider K/F. Given $\alpha \in K$, then $\alpha \in L$, and hence α is separable over F by hypothesis. By definition, then, K/F is separable.

Now consider L/K. Given $\alpha \in L$, we have that α is separable over F by hypothesis. Let $f \in F[x]$ be the minimal polynomial of α over F, and let $g \in K[x]$ be the minimal polynomial of α over K. Let M be a splitting field of f containing L.
Then because α is separable over F, the polynomial f has no repeated roots in M. In addition, g divides f in $K[x]$, and therefore g also splits completely over M with no repeated roots. Thus, g is separable over K, and hence its root α is also separable over K. By definition, then, L/K is separable. QED

Problem 6. Cox, Section 5.3, Exercise 16:
Let F be a field of characteristic $p \geq 2$, let $a \in F$, and let $f = x^p - x + a \in F[x]$.

(a) Prove that f is separable.

(b) Let α be a root of f in some extension L of F. Prove that $\alpha + 1$ is also a root of f.

(c) Use part (b) to prove that f splits completely over $F(\alpha)$.

(d) Use Theorem 5.3.15(a) to prove that $F(\alpha)/F$ is normal and separable.

Proof. (a) We have $f' = -1$, and hence $\gcd(f, f') = \gcd(f, -1) = 1$. Therefore, by Proposition 5.3.2, f is separable. QED (a)

(b) We compute

$$f(\alpha + 1) = (\alpha + 1)^p - (\alpha + 1) + a = \alpha^p + 1 - \alpha - 1 + a = \alpha^p - \alpha + a = f(\alpha) = 0,$$

where the second equality is by the fact that $(s + t)^p = s^p + t^p$ in characteristic p. QED (b)

(c) Applying part (b) repeatedly, we see that for each $j = 0, 1, \ldots, p - 1$, the element $\alpha + j \in L$ is a root of f. For any distinct $i \neq j$ in $\{0, 1, \ldots, p-1\}$, we have $i \neq j$ in F (since $p \nmid i - j$ as integers), and hence $\alpha + i \neq \alpha + j$. Since $\deg(f) = p$, and since these p elements $\alpha + j$ are all disinct, it follows that f splits completely over L as $f(x) = \prod_{j=0}^{p-1}(x - \alpha - j)$. QED (c)

(d) By part (c), $F(\alpha)$ is the splitting field of f over F, and hence $F(\alpha)/F$ is a normal extension by Proposition 5.2.1. In addition, since f is separable by part (a), it follows from Theorem 5.3.15 [either part (a) or (b) of that Theorem] that $F(\alpha)/F$ is separable. QED (d)

Problem 7. Cox, Section 5.4, Exercise 2:
Let F be a finite field, and let L/F be a finite extension.

(a) Prove that L is also a finite field.

(b) By Proposition A.5.3, since L is a finite field, its multiplicative group (i.e., $L^\times = L \smallsetminus \{0\}$ under the operation of $\cdot$) is a cyclic group. Let $\alpha \in L^\times$ be a generator of this cyclic group. Prove that $L = F(\alpha)$.

(c) Let $m = |L| - 1 = |L^\times|$ and $f(x) = x^m - 1 \in F[x]$. Prove that for all $0 \le i \le m-1$, we have $f(\alpha^i) = 0$. Then conclude that

$$x^m - 1 = (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{m-1}).$$

(d) Use part (c) to prove that α is separable over F. [Thus, $L = F(\alpha)$, and L/F is separable.]

Proof. (a) Let $q = |F| < \infty$ and let $n = [L : F] < \infty$. Then there is an F-basis $\{\alpha_1, \ldots, \alpha_n\}$ for L as a vector space over F. Thus, $L = \{c_1\alpha_1 + \cdots + c_n\alpha_n \,|\, c_i \in F\}$ has the same cardinality as $F^n = \{(c_1, \ldots, c_n) | c_i \in F\}$, i.e., $|L| = |F^n| = q^n < \infty$. QED (a)

(b) Since $\alpha \in L$, we have $F(\alpha) \subseteq L$. Conversely, given $\beta \in L$, then either $\beta = 0 \in F$, or else $\beta \in L^\times$. In the latter case, by hypothesis there exists an integer $j \in \mathbb{Z}$ such that $\beta = \alpha^j \in F$. QED (b)

(c) Since $L^\times$ has order m, then by Lagrange's Theorem we have $\beta^m = 1$ for all $\beta \in L^\times$. Therefore, for any $i \in \mathbb{Z}$, we have $f(\alpha^i) = (\alpha^i)^m - 1 = 1 - 1 = 0$.
By part (b), since α is a generator for the group $L^\times$ of order m, the powers $1, \alpha, \alpha^2, \ldots \alpha^{m-1}$ are all distinct. Thus, these are m distinct roots of the degree m polynomial f, and hence they are all the roots. Since f is monic, it follows that

$$x^m - 1 = (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{m-1}).$$ QED (c)

(d) Let $g \in F$ be the minimal polynomial of α over F. Then $g | f$ in $F[x]$, where $f = x^m - 1$ as in part (c). As noted in (c), the roots $1, \alpha, \alpha^2, \ldots \alpha^{m-1}$ of f are all distinct, and hence the roots of g, which form a subset of the roots of f, are also all distinct. That is, α is separable over F. QED (d)

Problem 8. Cox, Section 5.4, Exercise 4, variant:
As in Example 5.4.4, let k be a field of characteristic $p \ge 2$, let $F = k(t, u)$, and let L/F be the splitting field of $f(x) = (x^p - t)(x^p - u) \in F[x]$, where $\alpha^p = t$ and $\beta^p = u$.
[That is, $\alpha = \sqrt[p]{t}$ and $\beta = \sqrt[p]{u}$.]

(a) Prove that $L = F(\alpha, \beta)$.

(b) Let $E = F(\alpha)$. Prove that $g(x) = x^p - t$ has no roots in F, and that $h(x) = x^p - u$ has no roots in E.

(c) Use part (b) to prove that $[L : F] = p^2$.

(d) Prove that for all $\gamma \in L \smallsetminus F$, we have $[F(\gamma) : F] = p$.

(e) Prove that L/F is purely inseparable.

[Note that parts (c) and (d) together show that L/F is an example of a finite extension that does *not* have a primitive element.]

Proof. (a) Let $K = F(\alpha, \beta)$, so that $L/K/F$. Because $\operatorname{char} L = \operatorname{char} K = \operatorname{char} F = \operatorname{char} k = p$, we have

$$f(x) = (x^p - \alpha^p)(x^p - \beta^p) = (x-\alpha)^p(x-\beta)^p$$

in $K[x]$ and in $L[x]$. Thus, the only roots of f in its splitting field L are α and β, whence $K = F(\alpha, \beta)$ is a splitting field of f over F. Therefore, the splitting field L is in fact $L = F(\alpha, \beta)$. QED (a)

(b) Suppose $g(a) = 0$ for some $a \in F$, and write $a = b/c$ for $b, c \in k[t, u]$. Then $b^p = tc^p$, contradicting unique factorization in $k[t, u]$. Thus, g has no roots in F.

To prove that h has no roots in E, first observe that $R = k[\alpha, u]$ is simply a polynomial ring in two variables with coefficients in k, and hence R is a UFD. Similarly to the above, then, suppose $h(a) = 0$ for

some $a \in E$, and write $a = b/c$ for $b, c \in R = k[\alpha, u]$. Then $b^p = uc^p$, contradicting unique factorization in R. Thus, h has no roots in E. QED (b)

(c) By part (b) together with Proposition 4.2.6, g is irreducible over F and that h is irreducible over E. Since $\alpha \in E = F(\alpha)$ is a root of g, then $[E : F] = \deg(g) = p$. Since $\beta \in L = E(\beta)$ is a root of h, then $[L : E] = \deg(h) = p$. Therefore, by the Tower Theorem, $[L : F] = [L : E][E : F] = p^2$. QED (c)

(d) By the proof of the Tower Theorem, the p^2-element set $\{\alpha^i \beta^j \,|\, 0 \leq i, j \leq p-1\}$ is an F-basis for $L = F(\alpha, \beta)$ over F. Given $\gamma \in L$, then, there exist $a_{ij} \in F$ (for each $0 \leq i, j \leq p-1$) such that $\gamma = \sum_{i,j} a_{ij} \alpha^i \beta^j$.
Therefore $\gamma^p = c$ where $c = \sum_{i,j} a_{ij}^p t^i u^j \in F$. Define $q_\gamma(x) = x^p - c \in F[x]$.
Then $q_\gamma(x) = x^p - \gamma^p = (x - \gamma)^p$ has only one root γ, which is not in F. Hence, by Proposition 4.2.6, q_γ is irreducible over F, and therefore $[F(\gamma) : F] = \deg(q_\gamma) = p$. QED (d)

(e) By our proof of part (d), for every $\gamma \in L \smallsetminus F$, the minimal polynomial is $q_\gamma(x) = x^p - \gamma^p \in F[x]$, which factors as $(x - \gamma)^p$. Since this minimal polynomial has repeated roots, it follows that γ is not separable over F. By definition, then, L/F is purely inseparable. QED (e)

Problem 9. Cox, Section 5.4, Exercise 5:
With notation as in Problem 8 above (Cox 5.4 Exercise 4), for each $\lambda \in F$, define $K_\lambda = F(\alpha + \lambda\beta)$. Clearly we have $L/K_\lambda/F$. Suppose that there exist $\lambda \neq \mu \in F$ such that $K_\lambda = K_\mu$.

(a) Prove that $\alpha, \beta \in K_\lambda$.

(b) Conclude that $K_\lambda = L$, and explain why this, together with the results of Problem 8, yields a contradiction.

[It follows that the fields K_λ are all distinct. Since F is infinite, this means that there are infinitely many different fields between L and F, even though L/F is a finite extension.]

Proof. (a) We have $\alpha + \lambda\beta \in K_\lambda$ and $\alpha + \mu\beta \in K_\mu = K_\lambda$. Therefore, since $\lambda - \mu \in F \smallsetminus \{0\}$, we have

$$\beta = \frac{1}{\lambda - \mu}\big((\alpha + \lambda\beta) - (\alpha + \mu\beta)\big) \in K_\lambda,$$

and hence also $\alpha = (\alpha + \lambda\beta) - \lambda\beta \in K_\lambda$. QED (a)

(b) We have $L = F(\alpha, \beta) \subseteq K_\lambda \subseteq L$, and hence $K_\lambda = L$, where the first equality is by Problem 8(a), and the first inclusion is by part (a) of this problem.
To prove the requested contradiction, define $\gamma = \alpha + \lambda\beta \in L$, so that $L = K_\lambda = F(\gamma)$. If $\gamma \in F$, then $L = F$, and hence $[L : F] = 1 \neq p^2$, contradicting Problem 8(c). Otherwise, we have $\gamma \in L \smallsetminus F$, and hence Problem 8(d) yields $[L : F] = [F(\gamma) : F] = p \neq p^2$, again contradicting Problem 8(c). QED (b)