Solutions to Homework 5

Problem 1. Cox, Section 4.4, Exercise 1:
Recall that $\overline{\mathbb{Q}}$ is the field of algebraic numbers, i.e., $\{\alpha \in \mathbb{C} | \alpha \text{ is algebraic over } \mathbb{Q}\}$.

(a) For each integer $n \geq 2$, prove that $\overline{\mathbb{Q}}$ has a subfield L such that $[L : \mathbb{Q}] = n$.
[**Suggestion**: Use Example 4.2.4.]

(b) Use part (a) to prove that $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

Proof. (a): Given $n \geq 2$, following Example 4.2.4, let $f = x^n + 2x + 2 \in \mathbb{Q}[x]$.
Then by Eisenstein's Criterion with $p = 2$, we have that f is irreducible over $\mathbb{Q}$.
Let $\alpha \in \overline{\mathbb{Q}}$ be a root of f, and define $L = \mathbb{Q}(\alpha)$, so that $\overline{\mathbb{Q}}/L/\mathbb{Q}$.
Since f is irreducible over $\mathbb{Q}$, we have $[L : \mathbb{Q}] = \deg(f) = n$. QED (a)

(b): Suppose towards a contradiction that $[\overline{\mathbb{Q}} : \mathbb{Q}] < \infty$.
Let $n = [\overline{\mathbb{Q}} : \mathbb{Q}]$, which (by this supposition) is a positive integer.
By part (a), there exists a field L with $\overline{\mathbb{Q}}/L/\mathbb{Q}$ such that $[L : \mathbb{Q}] = n + 1$.
Then by the Tower Theorem,

$$n = [\overline{\mathbb{Q}} : \mathbb{Q}] = [\overline{\mathbb{Q}} : L][L : \mathbb{Q}] = [\overline{\mathbb{Q}} : L](n + 1) \geq n + 1 > n,$$

which is a contradiction. QED

Problem 2. Cox, Section 4.4, Exercise 3:
We say $\alpha \in \mathbb{C}$ is an *algebraic integer* if α is a root of a monic polynomial in $\mathbb{Z}[x]$ (i.e., monic and with *integer* coefficients).

(a) Prove that $\alpha \in \mathbb{C}$ is an algebraic integer if and only if α is algebraic over $\mathbb{Q}$ and its minimal polynomial $f \in \mathbb{Q}[x]$ has integer coefficients.

(b) Prove that $\omega/2$ is *not* an algebraic integer, where $\omega = \zeta_3$ is a root of $x^2 + x + 1$.

Proof. (a), ($\Rightarrow$): By hypothesis, there exists monic $g \in \mathbb{Z}[x]$ with $g(\alpha) = 0$.
Then α is algebraic over $\mathbb{Q}$, so it has a minimal polynomial $f \in \mathbb{Q}[x]$.
By properties of minimal polynomials, we have $f|g$, and hence there is some $h \in \mathbb{Q}[x]$ such that $fh = g$.
Since $g \in \mathbb{Z}[x]$, then By Gauss's Lemma, there exists $q \in \mathbb{Q}^\times$ such that $qf, q^{-1}h \in \mathbb{Z}[x]$
Let $b \in \mathbb{Q}^\times$ be the lead coefficient of h. Then since $fh = g$ and f and g are both monic, we must have $b = 1$, so that h is also monic.
Thus, the lead coefficient of $q^{-1}h \in \mathbb{Z}[x]$ is q^{-1}, so $q^{-1} \in \mathbb{Z}$. [In fact, $q = q^{-1} = \pm 1$, although we do not need that fact here.]
Therefore, $f = q^{-1} \cdot (qf) \in \mathbb{Z}[x]$. QED ($\Rightarrow$)

(a), ($\Leftarrow$): By assumption, $f \in \mathbb{Z}[x]$ is the minimal polynomial of α over $\mathbb{Q}$.
In particular, $f \in \mathbb{Z}[x]$ is monic, and $f(\alpha) = 0$. QED ($\Leftarrow$)

(b): Since ω is a root of $x^2 + x + 1$, it follows that $\omega/2$ is a root of $4x^2 + 2x + 1$.
Hence, $\omega/2$ is a root of the monic polynomial $f(x) = x^2 + \frac{1}{2}x + \frac{1}{4} \in \mathbb{Q}[x]$.
The discriminant of f is $\left(\frac{1}{2}\right)^2 - 4(1)\left(\frac{1}{4}\right) = -\frac{3}{4} < 0$, so f has no roots in $\mathbb{R}$, and hence no roots in $\mathbb{Q}$.
Since $\deg(f) = 2$, a Math 350 result says that f is irreducible over $\mathbb{Q}$.
Thus, being monic and irreducible, f is the minimal polynomial of $\omega/2$ over $\mathbb{Q}$.
But $f \notin \mathbb{Z}[x]$, so by part (a), $\omega/2$ is not an algebraic integer. QED

Problem 3. Cox, Section 4.4, Exercise 6:

Let F be a field, and let $M = \{\alpha \in F(x) | \alpha \text{ is algebraic over } F\}$. Prove that $M = F$.

Proof. Note: since $F[x]$ denotes a subset of M, I'll use $F[t]$ for the ring of polynomials whose roots are algebraic over F.

($\supseteq$): Given $\alpha \in F$, then α is algebraic over F (since it is a root of $t - \alpha \in F[t]$), so $\alpha \in M$.

($\subseteq$): Given $h \in M$, then by definition $h \in F(x)$ is a quotient f/g of polynomials $f, g \in F[x]$. Since $F[x]$ is a UFD, we may cancel any common irreducible factors of f and g and hence assume without loss that f and g have no common factors. That is, $f, g \in F[x]$ are relatively prime polynomials.
Since h is algebraic over F (because $h \in M$), we may define $k(t) \in F[t]$ to be the minimal polynomial of h over F. That is, $k(t)$ is irreducible over F, and $k(h) = 0$. Write $k(t) = a_n t^n + \cdots + a_0$ with $a_0, a_1, \ldots, a_n \in F$. If $a_0 = 0$, then $t|k$, and since k is irreducible, we have $k(t) = t$, whence $h = 0 \in F$. Thus, we may assume for the rest of the proof that $a_0 \neq 0$. In addition, k is monic, so $a_n = 1 \neq 0$.
Since $k(h) = 0$, we have

$$a_n \left(\frac{f}{g}\right)^n + \cdots + a_1 \frac{f}{g} + a_0 = 0, \quad \text{and hence} \quad a_n f^n + a_{n-1} f^{n-1} g + \cdots + a_1 f g^{n-1} + a_0 g^n = 0.$$

That last equation is an equation in the ring $F[x]$.
Working modulo the ideal $\langle g \rangle \subseteq F[x]$, that equation yields $a_n f^n \in \langle g \rangle$. Since $a_n = 1$, we have $f^n \in \langle g \rangle$, so there exists $b(x) \in F[x]$ such that $f^n = bg$. If g has an irreducible factor $p(x)$, then $p|f^n$, so $p|f$ since p is irreducible. Since $p|f$ and $p|g$, we have contradicted our assumption that $(f, g) = 1$; hence, no such p exists, and therefore $g \in F$ is constant.
On the other hand, working modulo the ideal $\langle f \rangle \subseteq F[x]$, the same equation yields $a_0 g^n \in \langle f \rangle$. Since $a_0 \in F^\times$, we may multiply by $a_0^{-1} \in F$ to get $g^n \in \langle f \rangle$. By the same reasoning as in the previous paragraph, it follows that $f \in F$ is constant.
Thus, $h = f/g$ is constant, i.e., $h \in F$. QED

Problem 4. Cox, Section 5.1, Exercise 1:
Prove that the splitting field of $x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\omega, \sqrt[3]{2})$.

Proof. Let $f = x^3 - 2 \in \mathbb{Q}[x]$, and let $K = \mathbb{Q}(\omega, \sqrt[3]{2})$.
For each $j = 0, 1, 2$, let $\alpha_j = \omega^j \sqrt[3]{2} \in K$.
Then $\alpha_j^3 = 2$ for each j, and $\alpha_0, \alpha_1, \alpha_2$ are all distinct since $1, \omega, \omega^2$ are all distinct.
Thus, the three roots of $f(x) = x^3 - 2$ must be precisely α_j for $j = 0, 1, 2$. Since f is monic, it follows that $f = (x - \alpha_0)(x - \alpha_1)(x - \alpha_2)$ splits completely over K.

Let $L = \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2)$, which is the splitting field of f. We must show that $L = K$.

We have $L \subseteq K$ since $\alpha_j \in K$ for each j.

We have $K \subseteq L$ since $\sqrt[3]{2} = \alpha_0 \in L$, and $\omega = \alpha_1/\alpha_0 \in L$. QED

Problem 5. Cox, Section 5.1, Exercise 3:
Let L/F be an extension of fields with $[L : F] = 2$. Prove that L is a splitting field of some $f \in F[x]$.

Proof. We have $F \subset L$ but $F \neq L$ (since if $L = F$, then $[L : F] = 1$). Thus, there exists $\alpha \in L$ with $\alpha \notin F$.
Let $K = F(\alpha)$, so that $L/K/F$. Since $\alpha \in K$ but $\alpha \notin F$, we have $[K : F] > 1$.
By the Tower Theorem, $2 = [L : F] = [L : K][K : F] > [L : K]$, since $[K : F] > 1$.
The previous sentence says that $1 \leq [L : K] < 2$, and hence $[L : K] = 1$ Therefore $L = K = F(\alpha)$.
Since $[F(\alpha) : F] = 2$, the minimal polynomial $f \in F[x]$ of α over f has $\deg(f) = 2$. Since f has (at least one) root $\alpha \in L = F(\alpha)$, there exists $h \in F[x]$ with $f(x) = (x - \alpha)h(x)$.
Then h must be monic of degree 1, so we may write $h(x) = x - \beta \in L[x]$.
Thus, $f(x) = (x - \alpha)(x - \beta)$ in $L[x]$. Hence, the splitting field of f is $F(\alpha, \beta) = L$. QED

Problem 6. Cox, Section 5.1, Exercise 4, variant:

Consider the following three subfields of $\mathbb{C}$:
$K_1 = \mathbb{Q}(\omega)$, $K_2 = \mathbb{Q}(\sqrt{-3})$, and K_3 is the splitting field of $x^6 - 1 \in \mathbb{Q}[x]$ over $\mathbb{Q}$.
Prove that $K_1 = K_2 = K_3$.

Proof. We have $\omega = (-1 + \sqrt{-3})/2 \in K_2$, so $K_1 \subseteq K_2$.
Since $\omega^2 = (-1 - \sqrt{-3})/2$, se also have $\sqrt{-3} = \omega - \omega^2$, so $K_2 \subseteq K_1$.
The roots of $f = x^6 - 1$ are ζ_6^j for $j = 0, 1, 2, 3, 4, 5$. Thus, $K_3 = \mathbb{Q}(\zeta_6)$.
Note that $\omega = \zeta_3 = \zeta_6^2 \in K_3$, and hence $K_1 \subseteq K_3$.

It remains to show that $K_3 \subseteq K_1$.
Observe that $(\omega_3^2)^2 = \omega_3^4 = \omega$, and hence the roots of $y^2 = \omega$ are $\pm\omega^2$.
Since $\omega^2 = (\zeta_6^2)^2 = \zeta_6^4$, it follows that $-\omega^2 = -\zeta_6^4 = (\zeta_6)^3(\zeta_6)^4 = \zeta_6^7 = \zeta_6$.
Thus $\zeta_6 \in \mathbb{Q}(\omega_3) = K_1$, and hence $K_3 \subseteq K_1$. QED

Problem 7. Cox, Section 5.1, Exercise 6:
Let $f \in \mathbb{Q}[x]$ be the minimal polynomial of $\alpha = \sqrt{2 + \sqrt{2}}$ over $\mathbb{Q}$.

(a) Prove that $f = x^4 - 4x^2 + 2$, and hence that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

(b) Prove that $\mathbb{Q}(\alpha)$ is the splitting field of f over $\mathbb{Q}$.

Proof. (a): $f \in \mathbb{Z}[x]$ satisfies Eisenstein's Criterion for the prime $p = 2$, since it is monic, all the other coefficients are divisible by 2, and the constant term 2 is not divisible by 2^2. Thus, by Eisenstein, f is irreducible. QED

— — — — — — —

(b): Applying the quadratic formula to $t^2 - 4t + 2$ shows its roots are $2 \pm \sqrt{2}$, and hence the four roots of f are $\pm\sqrt{2 \pm \sqrt{2}}$. Thus, setting $\beta = \sqrt{2 - \sqrt{2}}$, the four roots of f are $\pm\alpha$ and $\pm\beta$. Hence, the splitting field of f over $\mathbb{Q}$ is $\mathbb{Q}(\alpha, \beta)$, which clearly contains $\mathbb{Q}(\alpha)$. We must show $\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\alpha)$. It suffices to show that $\beta \in \mathbb{Q}(\alpha)$.
Observe that $\alpha\beta = \sqrt{(2 + \sqrt{2})(2 - \sqrt{2})} = \sqrt{4 - 2} = \sqrt{2}$. In addition, $\alpha^2 = 2 + \sqrt{2}$, so that $\sqrt{2} = \alpha^2 - 2$. Thus, we have

$$\beta = \frac{\sqrt{2}}{\alpha} = \frac{\alpha^2 - 2}{\alpha} \in \mathbb{Q}(\alpha),$$

as desired. QED

Problem 8. Cox, Section 5.1, Exercise 7:
Let $f = x^3 - x + 1 \in \mathbb{F}_3[x]$.

(a) Prove that f is irreducible over $\mathbb{F}_3$.

(b) Let L be the splitting field of f over $\mathbb{F}_3$. Prove that $[L : F] = 3$.

(c) Prove that $|L| = 27$.

Proof. (a): Since $\deg(f) = 3$, it suffices to prove that f has no roots in $\mathbb{F}_3 = \{0, 1, 2\}$. We compute:

$$f(0) = 1 \neq 0, \quad f(1) = 1 - 1 + 1 = 1 \neq 0, \quad f(2) = 2 - 2 + 1 = 1 \neq 0,$$

proving that f has no roots in $\mathbb{F}_3$ and hence is irreducible over $\mathbb{F}_3$. QED (a)

— — — — — — —

(b): Define $L = \mathbb{F}_3(\alpha)$ where α is a root of f. Note that $\operatorname{char} L = \operatorname{char} \mathbb{F}_3 = 3$.
[Note: technically, $L = \mathbb{F}_3[x]/\langle f \rangle$ and $\alpha = x + \langle f \rangle$.]
Define $\beta = \alpha + 1 \in K$ and $\gamma = \alpha + 2 \in K$. We compute

$$\alpha + \beta + \gamma = \alpha + (\alpha + 1) + (\alpha + 2) = 3\alpha + 3 = 0,$$
$$\alpha\beta + \alpha\gamma + \beta\gamma = \alpha(\alpha + 1) + \alpha(\alpha + 2) + (\alpha + 1)(\alpha + 2) = 3\alpha^2 + 6\alpha + 2 = -1, \text{ and}$$
$$\alpha\beta\gamma = \alpha(\alpha + 1)(\alpha + 2) = \alpha^3 + 3\alpha^2 + 2\alpha = (\alpha^3 - \alpha + 1) - 1 = -1.$$

where the final equality above is because $\alpha^3 - \alpha + 1 = f(\alpha) = 0$. Thus,

$$(x-\alpha)(x-\beta)(x-\gamma) = x^3 - (\alpha+\beta+\gamma)x^2 + (\alpha\beta+\alpha\gamma+\beta\gamma)x - \alpha\beta\gamma = x^3 - x + 1 = f(x).$$

Thus, the splitting field of f is $\mathbb{F}_3(\alpha,\beta,\gamma) = \mathbb{F}_3(\alpha) = L$.
And since f is the minimal polynomial of α over $\mathbb{F}_3$ (being irreducible and monic with $f(\alpha) = 0$), we have $[L : \mathbb{F}_3] = \deg(f) = 3$. QED

———— ———— ———— ———— ———— ———— ————

(c): By part (b), we have $\dim_{\mathbb{F}_3}(L) = 3$. So L has an $\mathbb{F}_3$-basis $S = \{1, \alpha, \alpha^2\}$.
Thus, $L = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{F}_3\}$, since S spans L.
Because there are $3^3 = 27$ choices for (a, b, c), and because (by the linear independence of S) all 27 resulting linear combinations are distinct, it follows that $|L| = 27$. QED

Problem 9. Cox, Section 5.1, Exercise 11:
Let F be a field, let $f \in F[x]$ be irreducible over F of degree $n \geq 1$, and let L be the splitting field of f over F.

(a) Prove that $n | [L : F]$.

(b) Give an example with $n \geq 4$ to show that $n = [L : F]$ can occur.

[**Note**: In fact, for any $n \geq 1$, there are examples where $n = [L : F]$. Can you prove this?]

Proof. (a): By definition of splitting field, and because $\deg f \geq 1$, L contains a root α_1 of f. Then $L/F(\alpha)/F$, and because f is irreducible over F, we have $[F(\alpha) : F] = \deg f = n$.
Therefore, by the Tower Theorem, $[L : F] = [L : F(\alpha)][F(\alpha) : F] = n[L : F(\alpha)]$. We also know that $[L : F] \leq n! < \infty$ by Theorem 5.1.5, so that $[L : F(\alpha)]$ is also finite and hence an integer. Thus, $n | [L : F]$. QED (a)

———— ———— ———— ———— ———— ———— ————

(b): Let $F = \mathbb{Q}$, and let $f = x^4 - 4x^2 + 2$ as in Problem 7 above. As we saw in that problem, we have $L = \mathbb{Q}(\alpha)$ is the splitting field of f, where α is a root of f. We also saw that $[L : \mathbb{Q}] = 4 = \deg(f)$, as desired. QED (b)

———— ———— ———— ———— ———— ———— ————

Note: There are, of course, many other examples that would work for (b). For example, $\Phi_8 = x^4 + 1$ is irreducible over $\mathbb{Q}$ (although this takes a little extra work to prove), and its splitting field is $\mathbb{Q}(\zeta_8)$.
For general $n \geq 2$, this is a hard problem with only what we have learned so far. One way to do it would be the following:
Let $F = \mathbb{C}(t)$, and let $f(x) = x^n - t$. It takes some work to show that f is irreducible over F. (The proof would be similar in style to the proof of Eisenstein's Criterion.)
Define α to be a root of f, i.e., $\alpha = t^{1/n}$, and let $L = F(\alpha)$. Then it is not difficult to prove that L is the splitting field of f, since the roots of f are $\zeta_n^j \alpha$ for $j = 0, 1, \ldots, n-1$, all of which are in L since $\zeta_n \in \mathbb{C} \subseteq F$.