Exercise 1 (DF 13.2: 8)**.** Let F be a field of characteristic $\neq 2$. Let D_1 and D_2 be elements of F, neither of which is a square in F. Prove that $F(\sqrt{D_1}, \sqrt{D_2})$ is of degree 4 over F if $D_1 D_2$ is not a square in F and is of degree 2 over F otherwise.

Since neither D_1 nor D_2 are squares in F, the extensions $F(\sqrt{D_1})$ and $F(\sqrt{D_2})$ are both quadratic extensions, so we know that their composite satisfies

$$\left[F(\sqrt{D_1}, \sqrt{D_2}) : F\right] \leq \left[F(\sqrt{D_1}) : F\right] \left[F(\sqrt{D_2}) : F\right] = 2 \cdot 2 = 4.$$

This gives us the following tower.

$$\begin{tikzcd}
 & F(\sqrt{D_1}, \sqrt{D_2}) \arrow[dd, dashed, no head, "\leq 4"] & \\
F(\sqrt{D_1}) \arrow[ur, no head] & & F(\sqrt{D_2}) \arrow[ul, no head] \\
 & F \arrow[ul, no head, "2"] \arrow[ur, no head, "2"'] &
\end{tikzcd}$$

Then since degrees multiply in towers, we know that the degree of $F(\sqrt{D_1}, \sqrt{D_2})$ over F must be divisible by 2, i.e. it must be either 2 or 4.

Case 1 - $D_1 D_2$ is a square in F: If $\sqrt{D_1 D_2} \in F$, then

$$\sqrt{D_1} = \sqrt{D_1 D_2}/\sqrt{D_2} \in F(\sqrt{D_2})$$
$$\sqrt{D_2} = \sqrt{D_1 D_2}/\sqrt{D_1} \in F(\sqrt{D_1}),$$

so $F(\sqrt{D_1}, \sqrt{D_2}) = F(\sqrt{1}) = F(\sqrt{2})$, i.e. the degree of $F(\sqrt{D_1}, \sqrt{D_2})$ over both intermediate extensions in the tower is 1. This forces the degree of $F(\sqrt{D_1}, \sqrt{D_2})$ over F to be 2.

Case 2 - $D_1 D_2$ is not a square in F: If $\sqrt{D_1 D_2}$ is not in F, then the polynomial $x^2 - D_1 D_2$, which has roots $\pm\sqrt{D_1 D_2}$, is irreducible over $F(\sqrt{D_1})$ and $F(\sqrt{D_2})$. This means the degree of $F(\sqrt{D_1}, \sqrt{D_2})$ over both intermediate extensions in the tower is 2, which forces the degree of $F(\sqrt{D_1}, \sqrt{D_2})$ over F to be 4.

Exercise 2 (DF 13.2: 14)**.** Prove that if $[F(\alpha) : F]$ is odd then $F(\alpha) = F(\alpha^2)$.

The polynomial $x^2 - \alpha^2$ over $F(\alpha^2)$ has α as a root, so α has degree at most 2 over $F(\alpha^2)$. Then

$$[F(\alpha, \alpha^2) : F(\alpha^2)] = [F(\alpha) : F(\alpha^2)] \leq 2.$$

But $[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F]$ is odd, which, since anything multiplied by 2 is even, forces $[F(\alpha) : F(\alpha^2)]$ to be 1, so $F(\alpha) = F(\alpha^2)$.

Exercise 3 (DF 13.2: 17)**.** Let $f(x)$ be an irreducible polynomial of degree n over a field F. Let $g(x)$ be any polynomial in $F[x]$. Prove that every irreducible factor of the composite polynomial $f(g(x))$ has degree divisible by n.

If either $f(x)$ or $g(x)$ is 0, then so is $f(g(x))$, so it is already irreducible and with degree 0, which every integer n divides. Thus we consider the case when both $f(x)$ and $g(x)$ are nonzero.

Suppose $h(x)$ is an irreducible factor of $f(g(x))$. If h has some root α, then $f(g(\alpha)) = 0$, so $g(\alpha)$ is a root of f. This means the extension $F(g(\alpha))$ over F has degree n. Additionally, since $g(\alpha)$ is a function of α, we know that $F(g(\alpha)) \subset F(\alpha)$. These two facts allow us to express $\deg(h)$ as

$$\deg(h) = [F(\alpha) : F] = [F(\alpha) : F(g(\alpha))][F(g(\alpha)) : F] = [F(\alpha) : F(g(\alpha))]n.$$

Thus the degree of h is divisible by n.

Exercise 4 (DF 13.4: 1)**.** Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 - 2$.

The polynomial $x^4 - 2$ has roots

$$\sqrt[4]{2},\ \sqrt[4]{2}\,\zeta_4,\ \sqrt[4]{2}\,\zeta_4^2,\ \sqrt[4]{2}\,\zeta_4^3,$$

so its splitting field is clearly $\mathbb{Q}(\sqrt[4]{2}, \zeta_4)$. But $\zeta_4 = i$, so the splitting field is actually $\mathbb{Q}(\sqrt[4]{2}, i)$.

By Eisenstein's criterion for $p = 2$, $x^4 - 2$ is irreducible over $\mathbb{Q}$, so

$$[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4.$$

The polynomial $x^2 + 1$ (which has i as a root) is also irreducible over $\mathbb{Q}$ since it has no roots in $\mathbb{Q}$, so

$$[\mathbb{Q}(i) : \mathbb{Q}] = 2.$$

Thus $[Q(\sqrt[4]{2}, i) : \mathbb{Q}] \leq 8$ and is divisible by 2 and 4, so the only possibilities for it are 4 and 8. If it is 4, then

$$4 = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] \cdot 4,$$

which implies that $\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2})$. But they are clearly distinct fields, so $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$.

Exercise 5 (DF 13.4: 3)**.** Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 + x^2 + 1$.

We can reduce the given polynomial into

$$x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1).$$

A rational number c/d, if its a root for either of these factors, must satisfy $c, d \mid 1$. Since 1 and -1 are not roots of either factor, they are then both irreducible over $\mathbb{Q}$. By the quadratic formula, the roots of the factors are

$$\frac{-1 \pm i\sqrt{3}}{2}, \frac{1 \pm i\sqrt{3}}{2}.$$

The splitting field for this polynomial is then clearly $\mathbb{Q}(i\sqrt{3})$.

Since $i\sqrt{3}$ is a root of $x^2 + 3$, and since this is irreducible over $\mathbb{Q}$ by Eisenstein's criterion for $p = 3$, the degree of this extension over $\mathbb{Q}$ is $[\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 2$.

Exercise 6 (DF 13.4: 4)**.** Determine the splitting field and its degree over $\mathbb{Q}$ for $x^6 - 4$.

We can factor $x^6 - 4$ into

$$x^6 - 4 = (x^3 + 2)(x^3 - 2).$$

Both of these factors are irreducible over $\mathbb{Q}$ by Eisenstein's criterion for $p = 2$, but we can still manually calculate their roots as

$$\begin{aligned} x^3 + 2 :& \quad \sqrt[3]{-2}, \sqrt[3]{-2}\,\zeta_3, \sqrt[3]{-2}\,\zeta_3^2 \\ x^3 - 2 :& \quad \sqrt[3]{2}, \sqrt[3]{2}\,\zeta_3, \ \zeta_3^2. \end{aligned}$$

Since $\zeta_3 = (-1 + i\sqrt{3})/2$, this means the splitting field of $x^6 - 4$ over $\mathbb{Q}$ needs to include $\sqrt[3]{-2}$, $\sqrt[3]{2}$, and $i\sqrt{3}$. We can actually prune this list slightly: since $\left(-\sqrt[3]{2}\right)^3 = -2$, we know $\sqrt[3]{-2} = -\sqrt[3]{2}$, so the splitting field is actually just

$$\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}).$$

Now $\sqrt[3]{2}$ is a root of $x^3 - 2$ and $i\sqrt{3}$ is a root of $x^2 + 3$, which are both irreducible by Eisenstein's criterion for $p = 2$ and $p = 3$, respectively. Thus $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 2$, giving us the following tower.

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) \arrow[dd, dash, dashed] & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[ur, dash] & & \mathbb{Q}(i\sqrt{3}) \arrow[ul, dash] \\
 & \mathbb{Q} \arrow[ul, dash, "3"] \arrow[ur, dash, "2"'] &
\end{tikzcd}$$

Since 2 and 3 are relatively prime, this means that the splitting field, which is the composite of the two intermediate field extensions in the tower, has degree 6 over $\mathbb{Q}$.

Exercise 7 (DF 13.4: 5)**.** Let K be a finite extension of F. Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[x]$ that has a root in K splits completely in $K[x]$ (use theorems 8 and 27).

Forward: Suppose K is the splitting field for some $f(x) \in F[x]$. Now let $g(x)$ be any irreducible polynomial in $F[x]$ with a root $\alpha_i \in K$. We know there exists *some* splitting field of $g(x)$, so we can write it as

$$g(x) = \prod_{i=1}^{n}(x - \alpha_i),$$

where α_1 is for sure an element of K. We must show that all the other α_i are also in K, and then $g(x)$ will split in $K[x]$. We will show that α_2 is in K, then appeal to induction for the rest of the α_i.

By Theorem 8, there is an isomorphism

$$\begin{aligned} \phi : F(\alpha_1) &\to F(\alpha_2) \\ \alpha_1 &\mapsto \alpha_2. \end{aligned}$$

We can now use this isomorphism ϕ and the fields $F(\alpha_1)$ and $F(\alpha_2)$ as the inputs to Theorem 27. Consider the polynomials $h(x) = (x - \alpha_1)f(x) \in F(\alpha_1)[x]$ and $\phi(h(x)) = (x - \alpha_2)f(x) \in F(\alpha_2)[x]$. They clearly have splitting fields $K(\alpha_1) = K$ and $K(\alpha_2)$, respectively. Then by theorem 27, $K \cong K(\alpha_2)$, which can only be true if $\alpha_2 \in K$. After passing to induction, we get that all the α_i are in K, so $g(x)$ splits in K.

Backward: Since K is a finite extension of F,

$$K = F(\alpha_1, \ldots, \alpha_n),$$

for some fixed n and distinct $\alpha_i \in K$ algebraic over F. By assumption, all the minimal polynomials $m_{\alpha_i,F}(x)$, since they are irreducible over F with a root in K, split in $K[x]$. Their product

$$f(x) = \prod_{i=1}^{n} m_{\alpha_i,F}(x) \in F[x]$$

then also splits in $K[x]$. Since the α_i are roots of $f(x)$, any field in which $f(x)$ splits must contain the α_i. Thus $K = F(\alpha_1, \ldots, \alpha_n)$ is the smallest field in which $f(x)$ splits, i.e. the splitting field of $f(x)$.

Exercise 8. Prove that $[K : F] = 1 \iff K = F$.

Backward: if $K = F$, then K has a basis $\{1\}$ as an F-vector space, so $[K : F] = 1$.

Forward: If $[K : F] = 1$, then K has a basis $\{\tilde{k}\}$ as an F-vector space. So for all nonzero $k \in K$,

$$k = f_k \tilde{k}$$

for some nonzero $f_k \in F$. In particular, this holds for $k = 1$, so we have

$$\begin{aligned} 1 &= f_1 \tilde{k} \\ f_1^{-1} &= \tilde{k}. \end{aligned}$$

Now since F is closed under nonzero inverses, this means $\tilde{k} \in F$. Then for all $k \in K$, $k = f_k \tilde{k}$ is the product of two elements of F, so $k \in F$. This shows $K \subset F$. Since K is an extension of F, we also have $F \subset K$, so $K = F$.

Exercise 9. Find the degree of $\sqrt[5]{2}$ over $\mathbb{Q}$. Then prove for each $a \in \mathbb{Q}(\sqrt[5]{2}) - \mathbb{Q}$, we have $\mathbb{Q}(a) = \mathbb{Q}(\sqrt[5]{2})$.

$\sqrt[5]{2}$ is a root of $x^5 - 2$, which is irreducible over $\mathbb{Q}$ by Eisenstein's criterion for $p = 2$, so the degree of $\sqrt[5]{2}$ over $\mathbb{Q}$ is 5.

Let $a \in \mathbb{Q}(a) - \mathbb{Q}$. Since a is an element of $\mathbb{Q}(\sqrt[5]{2})$, we have $\mathbb{Q}(a) \subset \mathbb{Q}(\sqrt[5]{2})$. We then have the following tower.

$$\begin{tikzcd} \mathbb{Q}(\sqrt[5]{2}) \arrow[d, dash] \arrow[dd, bend right, dash, "5"'] \\ \mathbb{Q}(a) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

Since degrees multiply in towers and 5 is prime, the other two extensions in this tower must be of degree 1 and 5. Now $[\mathbb{Q}(a) : \mathbb{Q}]$ cannot be 1, since $a \notin \mathbb{Q}$ forces $\mathbb{Q}(a)$ to be distinct from $\mathbb{Q}$. Thus $\mathbb{Q}(a)$ has degree 5 over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt[5]{2})$ has degree 1 over $\mathbb{Q}(a)$, meaning that $\mathbb{Q}(\sqrt[5]{2}) = \mathbb{Q}(a)$.

Exercise 10. Prove that a finite field cannot be algebraically closed.

Suppose F is a finite field with elements $a_1, \ldots, a_m$ for some arbitrary m. We can construct the polynomial

$$p(x) = (x - a_1) \cdots (x - a_m) + 1,$$

where 1 represents whichever of the a_i is the multiplicative identity of F. Since in the last homework we proved that any finite field has p^n elements, where p is a prime, and since 1 is not a prime, we know that any finite field has at least 2 elements, i.e. the multiplicative and additive identities are distinct.

Thus $p(a_i) = 1 \neq 0$ for all a_i, meaning that $p(x)$ has no roots in F, so F is not algebraically closed.