Exercise 1 (DF 13.5: 2)**.** Find all irreducible polynomials of degrees 1, 2, and 4 over $\mathbb{F}_2$ and prove that their product is $x^{16} - x$.

The degree 1 irreducible polynomials are clearly x and $x + 1$.

Any polynomial of higher degree must have a 1 as its coefficient, as otherwise it would have 0 as a root and then be reducible. We can then check the two remaining possibilities for degree 2, of which only $x^2 + x + 1$ is irreducible.

We note that any polynomial with an odd number of x^i (plus the coefficient 1) has 1 as a root in $\mathbb{F}_2$, so these polynomials are divisible by $x + 1$. If a reducible degree 4 polynomial has no linear divisors, it must be the product of two irreducible quadratics. Since we have only one irreducible quadratic over $\mathbb{F}_2$, we can manually calculate its square and remove that from the list of possible polynomials. This leaves us with three irreducible quartics: x^4+x^3+1, $x^4 + x + 1$, and $x^4 + x^3 + x^2 + x + 1$.

Lemma 1. *$\mathbb{F}_{p^k} \subset \mathbb{F}_{p^l}$ if and only if k divides l.*

Proof. If $\mathbb{F}_{p^k} \subset \mathbb{F}_{p^l}$, then since degrees multiply in towers, k divides l. Conversely, suppose k divides l, then $l = km$ for some nonnegative integer m. Let $\alpha \in \mathbb{F}_{p^k}$, then $\alpha^{p^k} = \alpha$. Then $\alpha^{p^l} = \alpha^{p^{km}} = \alpha^{p^k \cdots p^k} = \alpha$, so $\alpha \in \mathbb{F}_{p^l}$. □

Lemma 2. *Two subfields of the same finite field are equal if they have the same size.*

Proof. Given $\mathbb{F}_{p^n}$, by Lemma 1 we know that its only subfields are all those $\mathbb{F}_{p^k}$ such that k divides n. This means there is at most 1 subfield of $\mathbb{F}_{p^n}$ of each size. So if two subfields of $\mathbb{F}_{p^n}$ have the same size, they are the same. □

Lemma 3. *The polynomial $x^{p^n} - x$ over $\mathbb{F}_p$ is the product of the distinct monic irreducible polynomials over $\mathbb{F}_p$ whose degrees divide n.*

Proof. Let $p(x)$ be the product of all the monic irreducible polynomials over $\mathbb{F}_p$ whose degrees divide n, and let R denote the set of roots of $p(x)$. We will first show that $R = \mathbb{F}_{p^n}$.

Let $\alpha \in R$, then it is the root of some monic irreducible $f(x) \in \mathbb{F}_p[x]$ whose degree divides n. Since $\mathbb{F}_p(\alpha) \cong \mathbb{F}_p[x]/(f(x))$, it is a subfield of $\mathbb{F}_{p^n}$ with size $p^{\deg f}$, so by Lemma 2, $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^{\deg f}}$. And by Lemma 1, $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^{\deg f}} \subset \mathbb{F}_{p^n}$. Thus $\alpha \in \mathbb{F}_{p^n}$, so $R \subset \mathbb{F}_{p^n}$.

Conversely, suppose $\beta \in \mathbb{F}_{p^n}$, then β corresponds to some minimal polynomial $m_\beta(x)$ over $\mathbb{F}_p$. Since degrees multiply in towers, $[\mathbb{F}_p(\beta) : \mathbb{F}_p]$ divides n, so $\deg(m_\beta)$ divides n, so $\beta \in R$. This shows $\mathbb{F}_{p^n} \subset R$, so we have equality.

Now $R = \mathbb{F}_{p^n}$ is the roots of $x^{p^n} - x$. Additionally, since the irreducible polynomials that make up $p(x)$ are over a finite field, they are all separable by Proposition 37 in Dummit and Foote. They also can't share any common roots, as this would contradict the uniqueness of the minimal polynomial. Thus

$$p(x) = \prod_{\alpha \in \mathbb{F}_{p^n}} (x - \alpha) = x^{p^n} - x.$$

It follows from this lemma that since $16 = 2^4$, the product of the monic irreducible polynomials of degrees 1, 2, and 4 is $x^{16} - x$. □

Exercise 2 (DF 13.5: 6)**.** Prove that $x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (x - \alpha)$. Conclude that $\prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = (-1)^{p^n}$ so the product of the nonzero elements of a finite field is $+1$ if $p = 2$ and -1 if p is odd. For p odd and $n = 1$ derive Wilson's Theorem: $(p-1)! \equiv -1 \mod p$.

The splitting field of $x^{p^n} - x$ (which has p^n distinct roots) is $\mathbb{F}_{p^n}$, and since every finite field contains 0,

$$\begin{aligned} x^{p^n} - x &= \prod_{\alpha \in \mathbb{F}_{p^n}} (x - \alpha) \\ x(x^{p^n-1} - 1) &= x \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (x - \alpha) \\ x^{p^n-1} - 1 &= \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (x - \alpha). \end{aligned}$$

Evaluating at 0 gives

$$-1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (-\alpha).$$

Note that since 2 is the smallest prime, $p^n - 1 > 0$, so evaluating this at 0 is well-defined. Then raising both sides to the power p^n and using the identity $\alpha^{p^n} = \alpha$ (since α is a root of $x^{p^n} - x$) gives

$$(-1)^{p^n} = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (-1)^{p^n} \alpha.$$

Note that $p^n - 1$ copies of $(-1)^{p^n}$ appear in the product on the right. So if p is odd, then p^n is odd, then the product is $\prod \alpha = -1 = (-1)^{p^n}$. And if p is even, then p^n is even, then the product is $\prod \alpha = 1 = (-1)^{p^n}$.

Letting $n = 1$ and p be odd, we have $\mathbb{F}_p \cong \mathbb{Z}_p$, so modulo p,

$$(p-1)! \equiv \prod_{\alpha \in \mathbb{F}_p^\times} \alpha \equiv -1.$$

Exercise 3 (DF 13.5: 7)**.** Suppose K is a field of characteristic p which is not a perfect field: $K \neq K^p$. Prove there exist irreducible inseparable polynomials over K. Conclude that there exist inseparable finite extensions of K.

Since K is not perfect, there is some $\alpha \in K$ such that α is not the p-th power of any element of K. Then the polynomial $f(x) = x^p - \alpha$, since $\text{char}(F) = p$ has formal derivative $px^{p-1} = 0$. Since the derivative is the zero polynomial, any root of $f(x)$ is also a root of the derivative and is thus a multiple root. This shows that $f(x)$ is inseparable, so now we must show that it is irreducible.

If $p = 2$, then $f(x)$ having no roots of K is enough to show that is is irreducible. Suppose instead that p is odd and β is a root of $f(x)$ in the splitting field of $f(x)$. Then $\beta^p = \alpha$, so by the Freshman's Dream over fields with characteristic p,

$$x^p - \alpha = x^p - \beta^p = x^p + (-\beta)^p = (x - \beta)^p.$$

Thus $f(x)$ has only one distinct root, and it has multiplicity p. Then since K does not contain a root of $f(x)$, $f(x)$ is irreducible over K.

Denote one of the roots of $f(x)$ by $\sqrt[p]{\alpha}$. Since $f(x)$ is irreducible and monic, it is the irreducible polynomial of $\sqrt[p]{\alpha}$. Then by the uniqueness of minimal polynomials, $\sqrt[p]{\alpha}$ is not a root of any separable polynomial, so $K(\sqrt[p]{\alpha})$ is inseparable over K. Additionally, since $\sqrt[p]{\alpha}$ is a root of $f(x)$, it's algebraic over K, so $K(\sqrt[p]{\alpha})$ is a finite extension of K. We have thus found an inseparable finite extension of K.

Exercise 4 (DF 13.6: 2)**.** Let ζ_n be a primitive n-th root of unity and let d divide n. Prove that ζ_n^d is a primitive (n/d)-th root of unity.

Given $\mu_n = \langle \zeta_n \rangle$, we want to show $\mu_{n/d} = \langle \zeta_n^d \rangle$. We can do this by showing that ζ_n^d generates n/d distinct elements, all of which are (n/d)-th roots of unity.

Let $\zeta_n^{dm} \in \langle \zeta_n^d \rangle$, then

$$(\zeta_n^{dm})^{(n/d)} = \zeta_n^{nm} = 1^m = 1,$$

so ζ_n^d generates (n/d)-th roots of unity, i.e. $\langle \zeta_n^d \rangle \subset \mu_{n/d}$. It in fact generates all (n/d) of them: if $1 \leq k < n$, then

$$(\zeta_n^d)^{k/d} = \zeta_n^k,$$

which is not 1 since ζ_n is itself primitive. Thus $\left|\langle \zeta_n^d \rangle\right| = n/d$, so $\langle \zeta_n^d \rangle = \mu_{n/d}$. This means ζ_n^d is a primitive (n/d)-th root of unity.

Exercise 5 (DF 13.6: 4)**.** Prove that if $n = p^k m$, where p is prime and m is relatively prime to p, then there are precisely m distinct n-th roots of unity over a field of characteristic p.

The n-th roots of unity are the roots of

$$x^n - 1 = x^{p^k m} - 1 = (x^m)^{p^k} - (1)^{p^k} = (x^m - 1)^{p^k},$$

where the final equality follows from the Freshman's Dream since we're working in a field of characteristic p. Note that since m and p are relatively prime, p^k is the most we can factor out. Then the roots of $x^n - 1$ are precisely the roots of $x^m - 1$.

We now show that $x^m - 1$ has m distinct roots. Its derivative is mx^{m-1}, which is nonzero for nonzero x since our field has characteristic p and m and p are relatively prime (the derivative has the root 0, but this is not a root of $x^m - 1$). Thus no root of $x^m - 1$ can be a root of its derivative, so it has no multiple roots. Thus $x^m - 1$ (and, by extension, $x^n - 1$) has m distinct roots, so there are m distinct n-th roots of unity in our field.

Exercise 6 (DF 14.1: 1)**.**

a. Show that if $K = F(\alpha_1, \ldots, \alpha_n)$, then an automorphism $\sigma \in \mathrm{Aut}_F(K)$ is uniquely determined by $\sigma(\alpha_i)$. In particular, show that an automorphism fixes K if and only if it fixes a set of generators for K.

b. Let $G \leq \mathrm{Gal}_F(K)$ be a subgroup of the Galois group of the extension K of F and suppose $\sigma_1, \ldots, \sigma_k$ generate G. Show that the subfield E over F is fixed by G if and only if it is fixed by the generators $\sigma_1, \ldots, \sigma_k$.

a. Let $k \in K = F(\alpha_1, \ldots, \alpha_n)$, then k has the form

$$k = \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)},$$

where $f, g \in F[\alpha_1, \ldots, \alpha_n]$ and $g \neq 0$. Since σ is a homomorphism that fixes F,

$$\sigma(a\alpha_i^k + b\alpha_i^l) = a\sigma(\alpha_i)^k + b\sigma(a_i)^l$$

for $a, b \in F$. Thus $\sigma(k)$ reduces to an expression in terms of just the $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$.

We then clearly have that if σ fixes each α_i, then σ fixes all of K. Conversely, if any of the α_i are *not* fixed by σ, then $\sigma(k) \neq k$, so K being fixed by σ implies σ fixing each α_i.

b. If G fixes E/F, then since $\sigma_i \in G$ for all i, each generator must fix E/F.

Conversely, suppose each σ_i fixes E/F. Let $\sigma \in G$ be arbitrary, then $\sigma = \sigma_{m_1}, \ldots, \sigma_{m_n}$ for some n. Then for $e \in E$,

$$\sigma(e) = (\sigma_{m_1}, \ldots, \sigma_{m_n})(e) = e.$$

Since σ was arbitrary, this shows that G fixes E/F.

Exercise 7 (A)**.** Let F be a field and $f(x) \in F[x]$ have positive degree. Let $f'(x)$ be its formal derivative. Prove the following:

a. If $\text{char}(F) = 0$, then $f'(x) \neq 0$.

b. If $\text{char}(F) = p \neq 0$, then $f'(x) = 0$ if and only if f is a polynomial in x^p.

In both parts, we suppose $f(x)$ has the form $f(x) = \sum_{i=0}^{n} a_i x^i$ for $a_i \in F$. Its formal derivative is then $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$.

a. Suppose $\text{char}(F) = 0$, then $a_i i \neq 0$ for all i, so $f'(x) \neq 0$.

b. Suppose $\text{char}(F) = p \neq 0$, then any element of F multiplied by a constant is 0 if and only if that constant is a multiple of p. Using the definition of the formal derivative, we can then construct a chain of if and only if statements:

$$\begin{aligned} f'(x) = 0 &\iff ia_i = 0 \text{ for all } i \\ &\iff i = pm_i \text{ for all } i, \text{ where } m_i \in \mathbb{N}_0 \\ &\iff f'(x) = \sum_{i=1}^{n} pm_i a_i x^{pm_i - 1} \\ &\iff f(x) = \sum_{i=0}^{n} a_i (x^p)^{m_i}. \end{aligned}$$

Thus $f'(x) = 0$ if and only if $f(x)$ is a polynomial in x^p.