Exercise 1. $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ are isomorphic as vector spaces but not fields.

By DF §13.1 Corollary 7, since $\sqrt{2}$ is the root of x^2-2 and i is the root of x^2+1 (both irreducible polynomials over $\mathbb{Q}$), their two respective field extensions are

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\},$$
$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}.$$

As vector spaces: Define $\phi : \mathbb{Q}(i) \to \mathbb{Q}(\sqrt{2})$ by

$$\phi(a + bi) = a + b\sqrt{2}.$$

This is clearly bijective, and we will show that it also respects addition and scalar multiplication. For addition we have

$$\begin{aligned}\phi(a_1 + b_1 i + a_2 + b_2 i) &= \phi((a_1 + a_2) + (b_1 + b_2)i) \\ &= a_1 + a_2 + (b_1 + b_2)\sqrt{2} \\ &= \phi(a_1 + b_1 i) + \phi(a_2 + b_2 i).\end{aligned}$$

For scalar multiplication, let $\lambda \in \mathbb{Q}$ be an arbitrary scalar (both extensions have $\mathbb{Q}$ as their base field, then

$$\phi(\lambda(a + bi)) = \phi(\lambda a + \lambda bi) = \lambda a + \lambda b\sqrt{2} = \lambda\phi(a + bi).$$

Thus $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ are isomorphic as vector spaces.

As fields: Suppose there is a field isomorphism $\varphi : \mathbb{Q}(i) \to \mathbb{Q}(\sqrt{2})$. Then $\varphi(i) = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$. Then since φ is a homomorphism, it maps -1 to

$$\varphi(-1) = \varphi(i^2) = \varphi(i)\varphi(i) = a^2 + 2ab\sqrt{2} + 2b^2.$$

However, since field isomorphisms also map 1 to 1, we have

$$\varphi(-1) = -\varphi(1) = -1.$$

This means $(a^2 + 2b^2) + 2ab\sqrt{2} = -1$. This is impossible, though, as $a^2 + 2b^2$ is always nonnegative and $2ab\sqrt{2}$ is either 0 or irrational. Thus by contradiction, $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ are not isomorphic as fields.

Exercise 2. A finite field is always a simple extension of its prime subfield.

Let K be some finite field with prime subfield F. By DF §9.5 Proposition 18, $K^\times$ is cyclic, so there is some $\alpha \in K^\times$ that generates all of $K^\times$. Consider the extension $F(\alpha)$. It is by definition the smallest field containing both F and α. Since K contains both F and α, we must have $F(\alpha) \subset K$.

Conversely, since α generates $K^\times$, every element of $K^\times$ is also in $F(\alpha)$. Since fields also always contain 0, we have $K \subset F(\alpha)$. Since we have shown both inclusions, we have $K = F(\alpha)$, so K is a simple extension of F.

Exercise 3. Construct a field of 9 elements and give its addition and multiplication tables. Discuss how your work is consistent with what we know about the structure of the additive group and multiplicative group of units of a finite field.

Consider the polynomial $f(x) = x^2 + 1$ over $\mathbb{F}_3$. It is irreducible over $\mathbb{F}_3$ because it is cubic and has no roots of $\mathbb{F}_3$, so the field $K \doteq \mathbb{F}_3[x]/(f(x))$ is a field extension of degree 2 over $\mathbb{F}_3$. Thus K is a field with $3^2 = 9$ elements. Below is the addition table for this field, where addition is peformed modulo $x^2 + 1$.

	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
1	1	2	0	x+1	x+2	x	2x+1	2x+2	2x
2	2	0	1	x+2	x	x+1	2x+2	2x	2x+1
x	x	x+1	x+2	2x	2x+1	2x+2	0	1	2
x+1	x+1	x+2	x	2x+1	2x+2	2x	1	2	0
x+2	x+2	x	x+1	2x+2	2x	2x+1	2	0	1
2x	2x	2x+1	2x+2	0	1	2	x	x+1	x+2
2x+1	2x+1	2x+2	2x	1	2	0	x+1	x+2	x
2x+2	2x+2	2x	2x+1	2	0	1	x+2	x	x+1

Below is the multiplication table for this field, where multiplication is performed modulo $x^2 + 1$. The values are calculated using the identity $x^2 \equiv 2 \mod (x^2 + 1)$.

	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
2	0	2	1	2x	2x+2	2x+1	x	x+2	x+1
x	0	x	2x	2	x+2	2x+2	1	x+1	2x+1
x+1	0	x+1	2x+2	x+2	2x	1	2x+1	2	x
x+2	0	x+2	2x+1	2x+2	1	x	x+1	2x	2
2x	0	2x	x	1	2x+1	x+1	2	2x+2	x+2
2x+1	0	2x+1	x+2	x+1	2	2x	2x+2	x	1
2x+2	0	2x+2	x+1	2x+1	x	2	x+2	1	2x

Since both tables are symmetric, we see that $(K, +)$ and $(K, \cdot)$ are both abelian. Also, each element can be multiplied by another element to yield 1, i.e. each element has an inverse. Since 0 only appears in the multiplication table in the first row and first column, there are no zero-divisors in K. Also, by calculating $(x + 1)^d$ for $1 \leq d \leq 9$, we see that $(K^\times, \cdot)$ is cyclic.

In the addition table, we note that for any element $y \in K$, the sum $y + y + y$ is always 0, meaning that the character of K is 3, as expected since $\mathbb{F}_3$ is the prime subfield of K.

Exercise 4. Let $F \leq E \leq K$ be fields and suppose that $E = F(a_1, \ldots, a_k)$ for $\{a_i\}_{i=1}^k$ a subset of the roots of $f(x) \in F[x]$. Prove that K is a splitting field of f over F if and only if K is a splitting field of f over E.

Forward: Suppose K is the splitting field of $f(x)$ over F, then K is the smallest field containing both F and all the roots a_i of $f(x)$. Since $E = F(a_1, \ldots, a_k)$ is a subfield of K, this means that extending E with roots of $f(x)$ will yield either a proper subfield of K or K itself. Since by assumption none of these proper subfields contain all the roots of $f(x)$, the splitting field of $f(x)$ over E must be K.

Backward: Suppose K is the splitting field of $f(x)$ over E, then K is the smallest field containing both E and all the roots of $f(x)$. But since E is the smallest field containing F and the roots $a_1, \ldots, a_k$ of $f(x)$, this means that K is the smallest field containing F and all the roots of $f(x)$, which is the definition of the splitting field of $f(x)$ over F.

Exercise 5. Let p be a prime and suppose $f(x) \in \mathbb{F}_p[x]$ is a cubic polynomial. Let K be a splitting field for f over $\mathbb{F}_p$. Discuss the possibilities for the order of K and how each might arise.

By DF §13.4 Proposition 26, the degree of K over $\mathbb{F}_p$ is at most 3!. If the degree of K is d over $\mathbb{F}_p$, then there is a basis of d elements for K as an $\mathbb{F}_p$-vector space. Then by simply counting the number of possible coefficient choices for this basis (each coefficient could have p different values), the order of K is p^d.

By DF §13.4 Proposition 26, the degree of K over $\mathbb{F}_p$ is at most 3!, so this significantly limits the possible orders of K. Note that it is not possible for $[K : \mathbb{F}_p]$ to be 4 or 5. If it were 4, then K would be generated by the roots of two irreducible polynomials, but this cannot be the case since $f(x)$ is only cubic. Since 5 is prime, K having degree 5 over $\mathbb{F}_p$ would mean that it was generated by the root of an irreducible quintic, which again cannot be the case since $f(x)$ is only cubic. The other degrees are possible, and we describe below how each can arise.

- Order p: $|K| = p$ if it is a degree 1 extension over $\mathbb{F}_p$, i.e. $f(x)$ splits already in $\mathbb{F}_p$.
- Order p^2: $|K| = p^2$ if it is a degree 2 extension over $\mathbb{F}_p$. This occurs if $f(x)$ reduces into an irreducible quadratic times a linear term over $\mathbb{F}_p$. Then extending with one of the roots of the quadratic makes $f(x)$ split, so the extension is degree 2.
- Order p^3: $|K| = p^3$ if it is a degree 3 extension over $\mathbb{F}_p$. This occurs if $f(x)$ is irreducible over $\mathbb{F}_p$ and an extension by one of the roots contains both other roots.
- Order p^6: $|K| = p^6$ if it is a degree 6 extension over $\mathbb{F}_p$. This occurs if $f(x)$ is irreducible over $\mathbb{F}_p$ and then if extending by any of the roots of $f(x)$ doesn't make $f(x)$ split. In that case, $f(x)$ is an irreducible quadratic times a linear, so we extend by one of the roots of the quadratic to make $f(x)$ split. The degree of the splitting field is then $3 \cdot 2 = 6$.

Exercise 6. Find the degree of the splitting field of $x^6 + 1$ over:

a. $\mathbb{Q}$.

b. $\mathbb{F}_2$.

a. We can manually check that since $\zeta_{12} = e^{\pi i/6}$, the polynomial $x^6 + 1$ has roots $\pm\zeta_{12}, \pm\zeta_{12}^3$, and $\pm\zeta_{12}^5$. Since there are only 6 roots maximum, though, we have found all of them. Thus the splitting field of $x^6 + 1$ over $\mathbb{Q}$ is just $\mathbb{Q}(\zeta_{12})$. By Corollary 42 in DF §13.6, $\mathbb{Q}(\zeta_{12})$ has degree $\phi(12)$ over $\mathbb{Q}$. Using the table of cyclotomic polynomials on page 553 of DF, we calculate $\phi(12)$ to be

$$\phi(12) = \deg \Phi_{12}(x) = \deg\left(x^4 - x^2 + 1\right) = 4,$$

so the degree of the splitting field of $x^6 + 1$ over $\mathbb{Q}$ is 4.

b. Since $\text{char}(\mathbb{F}_2) = 2$, by the Freshman's Dream we can write $x^6 + 1$ over $\mathbb{F}_2$ as

$$x^6 + 1 = (x^3)^2 + 1^2 = (x^3 + 1)^2.$$

Now $x^3 + 1$ has 1 as a root over $\mathbb{F}_2$, so we can divide out by $x - 1 = x + 1$ to get

$$x^6 + 1 = (x + 1)^2\left(x^2 + x + 1\right)^2.$$

The quadratic expression in this factorization is irreducible since it has no roots in $\mathbb{F}_2$, so we've fully factored $x^6 + 1$ into a product of irreducibles. Now $x+1$ has root $1 \in \mathbb{F}_2$, so we only need to append the roots of x^2+x+1 to $\mathbb{F}_2$ to get the splitting field.

By DF §13.4 Proposition 26, the splitting field of a quadratic is at most degree $2! = 2$ over the base field. Now it cannot be a degree 1 extension, because then it would be equal to $\mathbb{F}_2$, and we already know that our quadratic has no roots in $\mathbb{F}_2$. Thus the degree of the splitting field of $x^2 + x + 1$ (and hence also of $x^6 + 1$) over $\mathbb{F}_2$ is 2.

Exercise 7. If K is a field and $\text{char}(K) \mid n$, then there are no primitive n-th roots of unity in K.

Suppse $p \doteq \text{char}(F)$ divides n, then $n = pm$ for some nonnegative integer m. The n-th roots of unity are the roots of $x^n - 1$, but the Freshman's Dream means that over F this becomes

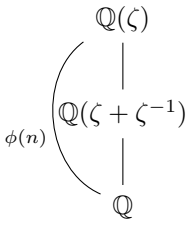
$$x^n - 1 = x^{pm} - 1 = (x^m)^p - 1^p = (x^m - 1)^p.$$

Thus in F, every n-th root of unity is also an m-th root of unity. Since 0 does not divide any number besides itself, the only other possibility for p is being prime, i.e. $p \geq 2$. Since $n = pm$, this means m is strictly less than n, so there are strictly fewer than n n-th roots of unity in F.

Now if F contained a primitive n-th root of unity, then it would contain all n of them. Since it does not contain all n of them, it cannot contain any primitive ones.

Exercise 8. If $n > 2$ and ζ is a primitive n-th root of unity over $\mathbb{Q}$, then $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \phi(n)/2$.

Since ζ and ζ^{-1} are both in $\mathbb{Q}(\zeta)$, then $\zeta + \zeta^{-1}$ is also in $\mathbb{Q}(\zeta)$, so $\mathbb{Q}(\zeta + \zeta^{-1})$ is a subfield of $\mathbb{Q}(\zeta)$. This gives us the following tower.



Then since degrees multiply in towers,

$$[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \frac{\phi(n)}{[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})]},$$

so we must show that the degree of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}(\zeta + \zeta^{-1})$ is 2 when $n > 2$. We first show that $\zeta, \zeta^{-1} \notin \mathbb{Q}(\zeta + \zeta^{-1})$ when $n > 2$.

An n-th primitive root of unity can be written $\zeta = e^{2\pi i/n}$, so its inverse is $\zeta^{-1} = e^{-2\pi i/n}$. Writing them in their complex forms and using the identities $\sin(-t) = -\sin(t)$ and $\cos(-t) = \cos(t)$ gives

$$\begin{aligned}
\zeta &= \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right), \\
\zeta + \zeta^{-1} &= \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right) + \cos\left(-\frac{2\pi}{n}\right) + i\sin\left(-\frac{2\pi}{n}\right) \\
&= 2\cos\left(\frac{2\pi}{n}\right).
\end{aligned}$$

Thus for all n, the sum $\zeta + \zeta^{-1}$ is a real number. When $n > 2$, the quantity $2\pi/n$ is neither 0 nor any other multiple of π, so $\sin(2\pi/n)$ is nonzero, so $\zeta \in \mathbb{C} - \mathbb{R}$. Similarly, ζ^{-1} is also a complex number. Then for $n > 2$, ζ is not an element of the extension $\mathbb{Q}(\zeta + \zeta^{-1})$, so it is a proper subfield of $\mathbb{Q}(\zeta)$.

Now consider the polynomial

$$f(x) \doteq x^2 - (\zeta + \zeta^{-1})x + 1 \quad \in \quad \mathbb{Q}(\zeta + \zeta^{-1})[x].$$

We can manually check that it has roots ζ, ζ^{-1}. Since it is degree 2, it has at most 2 roots, so these are the only ones. Since we just showed that neither ζ nor ζ^{-1} are contained in $\mathbb{Q}(\zeta + \zeta^{-1})$, this polynomial is irreducible. Thus $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = \deg f = 2$, which shows that $[\mathbb{Q}(\zeta + \zeta^{-1}) : Q] = \phi(n)/2$.

Exercise 9. If n is odd and K is a field with $\text{char}(K) \neq 2$ containing a primitive n-th root of unity, then K contains a primitive $2n$-th root of unity.

The $2n$-th roots of unity are the roots of $x^{2n} - 1$, which can be factored into

$$x^{2n} - 1 = (x^n + 1)(x^n - 1).$$

(By Exercise 7, we know that $\text{char}(K)$ does not divide n, and by assumption, we know $\text{char}(K) \neq 2$. Thus no matter what the character of K is, there is no alternative way to factor this polynomial by using the Freshman's Dream.)

Since the n-th roots of unity satisfy the second of these polynomials, they are all certainly $2n$-th roots of unity themselves. We also know that since K contains a primitive n-th root of unity, say ζ_n, we know that $\zeta_n, \dots, \zeta_n^n$ are all distinct roots of unity in K by the definition of a primitive root of unity. Thus K has at least half of the $2n$-th roots of unity.

Then since n is odd, for any k satisfying $1 \leq k \leq n$, we have

$$(-\zeta_n^k)^n = (-1)^n(\zeta_n^n)^k = -1,$$

so $-\zeta_n, \dots, -\zeta_n^n$ are the roots of $x^n + 1$ and thus $2n$-th roots of unity in K. Since each ζ_n is distinct, all the negatives are also necessarily distinct. Thus K contains all $2n$ of the $2n$-th roots of unity.

All that's left is to show that this collection can be generated by a single element. Note that the collection of these $2n$-th roots of unity is a group under multiplication, as it inherits associativity from K, the multiplicative identity is $\zeta_n^n = 1$, and each element is its own inverse. In particular, this is a finite subgroup of $K^\times$. Then by DF §9.5 Proposition 18, the collection of $2n$-th roots of unity in K is cyclic. Thus there is a primitive $2n$-th root of unity in K.