1. *If F has characteristic p and $a \in F$,consider the polynomial $f(x) = x^p - a \in F[x]$. Prove that either $f(x)$ is irreducible over F or $f(x)$ splits in F.*

   Let E be the splitting field of $f(x)$ over F, so that there is some $b \in E$ such that $f(b) = 0$. Thus $b^p = a$, and since F has characteristic p, we may rewrite $f(x) = x^p - a = x^p - b^p = (x-b)^p$. We may thus consider two possibilities:

   Case I: $b \in F$**.** Then $f(x) = (x-b)^p$ is a factorization of $f(x)$ into linear factors in $F[x]$, so $f(x)$ splits in F.

   Case II: $b \notin F$**.** Then every nontrivial factorization of $f(x)$ in $F[x]$ must be of the form $f(x) = (x-b)^m(x-b)^{p-m}$ for $0 < m < p$ (wlog, we can actually establish $0 < m \leq \frac{p}{2}$); thus since every coefficient of these factors must be in F, in particular $(x-b)^m = x^m + mbx^{m-1} + \cdots$ requires $mb \in F$. Since F has characteristic $p > m$, $m^{-1}mb = b \in F$, contradicting our premise, so no nontrivial factorizations exist.

2. *Let $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Find a polynomial $f(x) \in \mathbb{Q}[x]$ such that $F \cong \mathbb{Q}[x]/\langle f(x)\rangle$, and find a basis for F considered as a vector field over $\mathbb{Q}$.*

   We need $f(x)$ to be irreducible so that F is a field; we then will require that for α such that $f(\alpha) = 0$, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. There are actually infinitely many such α (refer to the Primitive Element Theorem), but one easy one is to choose $\alpha = \sqrt{2} + \sqrt{3}$. Then we want an irreducible polynomial in $\mathbb{Q}[x]$ with $\sqrt{2}+\sqrt{3}$ as a zero. We could note that this value actually has three "irrational conjugates": $\sqrt{2} - \sqrt{3}$, $-\sqrt{2} + \sqrt{3}$, and $-\sqrt{2} - \sqrt{3}$, and if $\sqrt{2} + \sqrt{3}$ is a zero of a polynomial in $\mathbb{Q}$, so must these other three, yielding a minimal polynomial

   $$(x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3}) = x^4 - 10x^2 + 1$$

   Incidentally, note that this is a way to show that $\sqrt{2}+\sqrt{3} = \sqrt{5 + 2\sqrt{6}}$, since the above is a quadratic equation in x^2.

3. *Let K be an extension of field F. If $\gamma \in K$ and $a, b \in F$ with a nonzero, prove that $F(a\gamma + b) = F(\gamma)$ (note: this is set-equality, not simply isomorphism).*

   Note that $\gamma = [(a\gamma + b) - b] \cdot a^{-1}$, which must be an element of $F(a\gamma + b)$, since $F(a\gamma + b)$ is a field containing $a\gamma + b$, a, and b (and a is nonzero, so a^{-1} exists). Since $\gamma \in F(a\gamma + b)$, it must be the case that $F(\gamma) \subseteq F(a\gamma + b)$.

   Similarly, it is obvious that $a\gamma + b \in F(\gamma)$, so that $F(a\gamma + b) \subseteq F(\gamma)$. The pair of nonstrict subset inclusions guarantees set equality.

4. *Let $\alpha \in \mathbb{R}$. Prove that $\mathbb{Q}(\alpha) \cong \mathbb{Q}(x)$ if and only if α is transcendental, i.e., if α is not the root of any polynomial with rational coefficients.*

   If α is not the root of any nonzero polynomial $f(x)$, then consider the homomorphism $\varphi : \mathbb{Q}(x) \to \mathbb{Q}(\alpha)$ induced by letting $\varphi(1) = 1$ and $\varphi(x) = \alpha$. Every element of $\mathbb{Q}(x)$ can be written as a ratio $\frac{f(x)}{x^k}$ for some $f(x) \in \mathbb{Q}[x]$, and tghen $\varphi\left(\frac{f(x)}{x^k}\right) = \frac{f(a)}{\alpha^k}$, which is nonzero when $f(x)$ is a nonzero polynomial. Thus, $\ker\varphi = \{0\}$, so this mapping is injective. It will also be surjective, since $\mathbb{Q}(x)$ is a field containing $\mathbb{Q}$ and x, and $\varphi(\mathbb{Q}(x))$ is thus a field containing $\mathbb{Q}$ and α. This homomorphism φ is thus an isomorphism.

   Conversely, suppose α is the root of a nonzero polynomial $f(x) \in \mathbb{Q}[x]$. We want to show that no isomorphism exists between the two fields, so we shall consider an arbitrary surjective homomorphism φ from $Q(x) \to Q(\alpha)$ and strive to show it is not injective. It must be the case that $\varphi(1) = 1$, and by surjectivity there is some $g(x) \in \mathbb{Q}(x)$ such that $\varphi(g(x)) = \alpha$. Now, let us consider $\varphi(f(g(x))$; since f

is a polynomial and φ a homomorphism, this will equal $f(\varphi(g(x))) = f(\alpha) = 0$. So $f(g(x)) \in \ker \varphi$, but since this is a nonzero polynomial, φ is non-injective.

5. *Prove that there is no irreducible polynomial in $\mathbb{Q}[x]$ which is zero at both $x = \sqrt{5}$ and $x = \sqrt{7}$.*

   Suppose $f(x)$ is an irreducible polynomial with zeroes at both $x = \sqrt{5}$ and $x = \sqrt{7}$. Then $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{7})$ will both be isomorphic to $\mathbb{Q}[x]/\langle f(x)\rangle$ and will thus be isomorphic to each other (in a manner which fixes $\mathbb{Q}$ itself). Thus, since $(0 + \sqrt{7})^2 = 7$, there would need to be an element of $\mathbb{Q}(\sqrt{5})$ whose square is also 7, i.e. $(a + b\sqrt{5})^2 = 7$ for rational a and b. But this would require that $a^2 + 5b^2 = 7$ and $2ab = 0$, which can be easily seen to have no solution in rational numbers.

   Alternatively: we can easily show that $x^2 - 5$ is the minimal polynomial of $\sqrt{5}$ over $\mathbb{Q}$, so any polynomial in $\mathbb{Q}[x]$ with $\sqrt{5}$ as a root must be divisible by $x^2 - 5$; if it is not an associate of $x^2 - 5$ itself, then it is not irreducible. Since $\sqrt{7}$ is not a root of $x^2 - 5$, there is clearly no irreducible with the desired properties.