14. Let $\text{char}(K) = p$. Let $L$ be a finite extension of $K$, and suppose $[L : K]$ is prime to $p$. Show that $L$ is separable over $K$.

*Proof.* Let $E$ be an algebraic closure of $K$. Since $L$ is finite, it is algebraic, and so $L = K[\alpha_1, \dots, \alpha_n]$ for some $\alpha_1, \dots, \alpha_n \in E$. We will know that $L$ is separable if $K(\alpha_i)$ is separable for each $i$. Also, $[K(\alpha_i) : K]$ divides $[L : K]$ for each $i$, thus the degree of each $\alpha_i$ is also prime to $p$. So, it suffices to show that $K(\alpha)$ is separable over $K$ for any algebraic $\alpha \in E$ of degree prime to $p$.

Suppose $\alpha \in E$ satisfies this, and let $f(X)$ be the minimal polynomial of $\alpha$ over $K$. Assume for a contradiction that $f(X)$ is inseparable. Then $f(X)$ and its derivative $f'(X)$ share a root. But $f(X)$ is irreducible, and so it must divide $f'(X)$ over $K$. However, $f'(X)$ has degree strictly less than that of $f(X)$, and so we must have $f'(X) = 0$.

Now, say $f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1 X + a_0$. We know $m > 0$ because $f$ is irreducible and $p \nmid m$ because the degree of $f$ is prime to $p$. Then $f'(X) = mX^{m-1} + (m-1)a_{m-1}X^{m-2} + \cdots + a_1 = 0$, and so $p$ divides $m$, a contradiction. $\square$

15. Suppose $\text{char}(K) = p$. Let $a \in K$. If $a$ has no $p$-th root in $K$, show that $X^{p^n} - a$ is irreducible in $K[X]$ for all positive integers $n$.

*Proof.* Suppose $a$ has no $p$-th root in $K$. Let $E$ be an algebraic closure of $K$, and let $\alpha$ be a root of $f(X) = X^{p^n} - a = (X - \alpha)^{p^n}$ in $E$. Suppose $f(X) = g(X)h(X)$ with $g(X), h(X) \in K[X]$. We may assume $g(X)$ is monic, since otherwise we could multiply both factors by units to make it so. So $g(X) = (X - \alpha)^s$ for some $s \le p^n$, and $h(X) = (X - \alpha)^{p^n - s}$.

If $k$ is the highest power of $p$ dividing $s$, then we may write $s = p^k t$ where $p \nmid t$ and $k \le n$. Therefore,

$$g(X) = (X - \alpha)^{p^k t} = (X^{p^k} - \alpha^{p^k})^t = \sum_{m=0}^{t} \binom{t}{m} (\alpha^{p^k})^m X^{p^k m}$$

has coefficients in $K$. In particular, the coefficient of the term where $m = 1$ is in $K$. This coefficient is $t\alpha^{p^k}$. Dividing by $t$ gives us that $\alpha^{p^k} \in K$. If $k < n$, then $(\alpha^{p^k})^{p^{n-k-1}} = \alpha^{p^{n-1}} \in K$ is a $p$th root of $a$, a contradiction. So the only possibility is that $n = k$, and so $h(X)$ must be a unit. So, by definition, $f(X)$ is irreducible in $K[X]$. $\square$

16. Let $\text{char}(K) = p$. Let $\alpha$ be algebraic over $K$. Show that $\alpha$ is separable if and only if $K(\alpha) = K(\alpha^{p^n})$ for all positive integers $n$.

*Proof.* First, suppose $\alpha$ is separable, and consider $f(X) = X^{p^n} - \alpha^{p^n} \in K(\alpha^{p^n})[X]$. Since $\alpha$ is a root of this polynomial, the minimal polynomial $g(X)$ of $\alpha$ over $K(\alpha^{p^n})$ divides $f(X)$. If $g(X)$ is linear, then it must be $X - \alpha$ and so $\alpha \in K(\alpha^{p^n})$, as desired. Otherwise, $g(X)$ must contain multiple factors of $X - \alpha$. We know that $g(X)$ divides the minimal polynomial of $\alpha$ over $K$, and so in this case we know that $\alpha$ is a multiple root of its minimal polynomial over $K$, and so cannot be separable over $K$, a contradiction. So it must be that $g(X) = X - \alpha$, meaning $K(\alpha^{p^n}) = K(\alpha)$.

For the converse, assume $\alpha$ is inseparable over $K$, so that its minimal polynomial $f(X)$ over $K$ has multiple roots. As discussed in the proof of exercise 14, we must have that the derivative $f'(X) = 0$, and so $p$ divides the exponent of $X$ in every term of $f(X)$. Thus, $f(X)$ is actually polynomial in $K[X^p]$. If $\alpha^p$ is also a multiple root of $f(X)$, then by the same reasoning, $f(X)$ is a polynomial in $K[X^{p^2}]$. This phenomenon can occur only finitely many times, since otherwise we would eventually end up at some $K[X^{p^m}]$ where $p^m$ exceeds the degree of $f(X)$, a contradiction. So suppose $n$ is the largest integer such that $f(X) \in K[X^{p^n}]$. Then $\alpha^{p^n}$ is a root of $f(X)$ (which is its minimal polynomial over $K$), but is separable over $K$. Therefore, $K(\alpha^{p^n})$ is separable, and so cannot equal the inseparable extension $K(\alpha)$. $\square$

17. Prove that the following two properties are equivalent:

    (a) Every algebraic extension of $K$ is separable.

    (b) Either $\mathrm{char}(K) = 0$, or $\mathrm{char}(K) = p$ and every element of $K$ has a $p$-th root in $K$.

*Proof.* Suppose $\mathrm{char}(K) = 0$, and let $f(X)$ be irreducible over $K$. Assume, for a contradiction, that $f(X)$ is inseparable, so that $f'(X)$ shares a root with $f(X)$. Since $f(X)$ divides $f'(X)$, but $\deg f' < \deg f$, this means that $f'(X) = 0$. The only possibility is that $f(X) \in K$, and so is not irreducible in $K[X]$ since it is a unit, a contradiction.

Now, suppose $\mathrm{char}(K) = p$ and every element of $K$ has a $p$-th root in $K$. Assume, for a contradiction, that some element $\alpha$ is not separable over $K$, and let $f(X)$ be its minimal polynomial. Then $f(X) = a_n X^n + \cdots + a_1 X + a_0$. Each $a_i$ has a $p$th root $b_i$, and so

$$f(X) = a_n X^n + \cdots + a_1 X + a_0 = (b_n X^n + \cdots + b_1 X + b_0)^p$$

contradicting that $f(X)$ was irreducible.

For the converse, suppose that every algebraic extension of $K$ is separable but that $\mathrm{char}(K) \neq 0$, so that $\mathrm{char}(K) = p$. Let $a \in K$ and consider the polynomial $f(X) = X^p - a$. If $\alpha$ is a root of this in some algebraic closure, then the minimal polynomial of $\alpha$ over $K$ divides $f(X) = (X - \alpha)^p$, hence is of the form $(X - \alpha)^q$ for some $q \leq p$. If $q > 1$ then $\alpha$ is not separable, a contradiction. So $X - \alpha \in K[X]$, meaning $\alpha \in K$. So every element of $K$ has a $p$th root in $K$. $\square$

18. Show that every element of a finite field can be written as a sum of two squares in that field.

*Proof.* Let $K$ be the finite field of order $q = p^n$. The multiplicative group of $K$ is cyclic of order $q - 1$. If $p = 2$, then $q - 1$ is odd, and so every element of $K^\times$ is a square. Since $0 = 0^2$, this means every element of $K$ is a square. So assume $p \neq 2$.

In this case, $q - 1$ is even. The map $x \mapsto x^2$ is an endomorphism of $K^\times$. Identifying $K^\times$ with $\mathbf{Z}_{q-1}$, we see that the kernel is $\{0, \frac{q-1}{2}\}$ and so the image of this map has $\dfrac{\#\mathbf{Z}_{q-1}}{\#\,\mathrm{Ker}} = \dfrac{q-1}{2}$ elements. Since 0 is a square, there are exactly $\frac{q+1}{2}$ squares in $K$.

Let $x \in K$. There must be at least one element which is both a square and is also of the form $x - a^2$ for some $a \in K$, since there are more than $\frac{\#K}{2}$ squares and more than $\frac{\#K}{2}$ elements of the form $x - a^2$. Therefore, $x - a^2$ is a square for some $a \in K$, hence $a^2 + b^2 = x$ for some $b \in K$. $\square$

19. Let $E$ be an algebraic extension of $F$. Show that every subring of $E$ which contains $F$ is actually a field. Is this necessarily true if $E$ is not algebraic over $F$? Prove or give a counterexample.

*Proof.* Recall that if $\alpha$ is algebraic over $F$ with minimal polynomial $f(X)$, then $F[\alpha] = F/(f(X))$ is a field. Let $F \subseteq R \subseteq E$ for a subring $R$, and let $\alpha \in R$. $\alpha$ is algebraic, hence $\alpha^{-1} \in F[\alpha] \subseteq R$. So $R$ is a field.

This is false if $E$ is not algebraic. Take $F = \mathbf{Q}$ and $E = \mathbf{Q}(e)$. Since $\mathbf{Q}[e] \cong \mathbf{Q}[X]$, we know that $\mathbf{Q}(e) \cong \mathbf{Q}(X)$. Clearly, $\mathbf{Q}[X]$ is a subring of $\mathbf{Q}(X)$ that is not a field. $\square$