Example/Remark: Let \( f(x) \in K[x] \) be an irreducible polynomial. We know that \( f \) has multiple roots \( \iff (f, f') = 1 \iff f \nmid f' \), as \( f \) is irreducible \( \iff f' = 0 \). So, if \( \text{Char } K = 0 \) then every irreducible polynomial has only simple roots. If \( \text{Char } K = p > 0 \), then there may exist \( f(x) \) irreducible such that \( f'(x) = 0 \).

Indeed, assume that \( K^p \neq K \) (i.e. \( K \) is not perfect), and take \( a \in K^p \setminus K \). Then \( x^p - a \) is irreducible and has multiple roots. To see that \( x^p - a \) is irreducible, then there would exist \( g \) irreducible in \( K[x] \) such that \( \deg g < \deg f = p \) and \( g \mid f \). Note that \( g' \neq 0 \) as \( g \) leading term of the polynomial is not a power of \( p \). If \( g = x^i + \cdots + \beta_1 x + \beta_0 \) where \( i < p \), then \( g' = i x^{i-1} + \cdots + \beta_1 \neq 0 \) so \( g \) has no multiple roots. Note that this is true for every irreducible factor of \( f \). However, \( f \) itself has multiple roots, and hence \( f = (x - b)^p \) (since different irreducible polynomials do not share roots???) where \( b^p = a \in K^p \), a contradiction.

Definition: An irreducible polynomial is called separable if it has no multiple roots. (i.e. \( \gcd(f, f') = 1 \)). This is the case \( \iff f \) has precisely as many roots as its degree. The example show that in characteristic zero, every polynomial is separable but in \( \text{Char } p > 0 \), there exist irreducible polynomials \( f \) that have a unique root.

Remark: Let \( \alpha \) be a root of an irreducible polynomial \( f \in K[x] \). Then there is an embedding

\[
K(\alpha) \to \bar{K}
\]

that fixes \( K \). For each root of \( f \), we get such an embedding, and distinct roots give distinct embeddings. So, the number of embeddings is the number of distinct roots.

Proposition: Let \( K \subseteq F \subseteq E \) be a sequence of algebraic field extensions, and let \( \sigma, \tau : F \to \bar{F} \) be embeddings over \( K \). Set \( S_\sigma = \{ \pi : E \to \bar{F} \mid \pi|_F = \sigma \} \) and \( S_\tau = \{ \pi : E \to \bar{F} \mid \pi|_F = \tau \} \). Then the sets \( S_\sigma \) and \( S_\tau \) have the same cardinality.

Proof: Since \( \bar{F} \) is algebraic over \( \sigma(F) \), there exists a \( \lambda : \bar{F} \to \bar{F} \) so that \( \lambda|_{\sigma(F)} = \tau \sigma^{-1} \) by the lifting theorem we did a while ago. So, for every \( \chi \in S_\sigma \), consider the composition \( \lambda \chi : E \to \bar{F} \). Then for \( a \in A \), note that

\[
\lambda \chi(a) = \lambda \sigma(a) = (\tau \sigma^{-1})(\sigma(a)) = \tau(a)
\]

so that \( \lambda \chi \in S_\tau \). Switching \( \sigma \) and \( \tau \) and using the map \( \lambda^{-1} \) we get a similar correspondence in which the composition is the identity on both sets. Therefore \( |S_\sigma| = |S_\tau| \).

Definition: The cardinality of the set of extensions of any embedding \( \sigma : F \to \bar{F} \) is called the separability degree of \( E/F \) and is denoted \( [E : F]_s \). This is well defined in view of the above proposition.

Theorem: Let \( K \subseteq F \subseteq E \) be algebraic. Then \( [E : K]_s = [E : F]_s [F : K]_s \).

Proof: Let \( \{ \sigma_i : F \to \bar{E} \} \) be the set of all embeddings of \( F \) into \( \bar{E}(= \bar{F}) \) fixing \( K \). For each \( i \in I \), choose, by the proposition, \( [E : F]_s \) extensions \( \tau_{ij} : E \to \bar{E} \) such that \( \tau_{ij}|_F = \sigma_i \). In this way, we get \( [E : F]_s [F : K]_s \) distinct embeddings of \( E/K \). We have the picture:
Since for every embedding $\tau : E \to \bar{E}$ over $K$, we have that $\tau|_F = \sigma_i$ for some $i$, we have obtained all embeddings of $E \to \bar{E}$ over $K$.

Lemma: If $F = K(\alpha)$ is and algebraic extension, then $[F : K]_s = \text{number of distinct roots of } \text{Irr}(\alpha, F) \leq [F : K]$. For the proof, this is the initial example that we computed.

Proposition: For every finite extension $K \subset F$ there is an inequality $[F : K]_s \leq [F : K]$. 
Proof: $F$ is finitely generated by algebraic elements, so $F = K(\alpha_1, \ldots, \alpha_n)$. Then we have a chain of field extensions

$$K \subseteq K(\alpha_1) = K_1 \subseteq K(\alpha_1, \alpha_2) = K_2 \subseteq \cdots \subseteq K(\alpha_1, \ldots, \alpha_n) = K_n = F$$

So we have $[K_{i+1} : K_i]_s \leq [K_{i+1} : K]$ and multiplying these inequalities we get $[F : K]_s \leq [F : K]$.

Definition: An element $\alpha \in F$ is called separable over $K$ if its irreducible polynomial over $K$ is separable. An algebraic extension $F/K$ is called separable if every element $\alpha \in F$ is separable over $K$.

Remark: Let $K \subseteq F \subseteq E$, and let $\alpha \in E$. Suppose that $\alpha$ is separable over $K$. Then $\alpha$ is separable over $F$. Indeed, we know that $\text{Irr}(\alpha, K)$ has distinct roots. However, $\text{Irr}(\alpha, F) | \text{Irr}(\alpha, K)$ so $\text{Irr}(\alpha, F)$ has distinct roots.

Theorem: If $F/K$ is an algebraic extension, then it is separable if and onyl if $[F : K]_s = [F : K]$.
Proof: Induct on $[E : F]$. If $[E : F] = 1$ then $E = F$ hence $E/F$ is separable. If $[E : F] > 1$, pick $\alpha \in E \setminus F$, and consider the diagram

$$E$$
$$\downarrow$$
$$F(\alpha)$$
$$\downarrow^{>1}$$
$$F$$

As $\alpha$ is separable over $F$ and since $\alpha \in E \setminus F$, we have that $[F(\alpha) : F]_s = [F(\alpha) : F] > 1$. By induction, we have that $[E : F(\alpha)]_s = [E : F(\alpha)]$. Therefore, using the multiplicative law for separable extensions, we have that $[E : F]$ is separable. For the reverse direction, note that $[E : F]_s = [E : F]$ means that $[F(\alpha) : F]_s = [F(\alpha) : F]$ for all $\alpha \in E$ and hence $\alpha$ is separable for all $\alpha \in E$.

Corollary: Let $E = F(\alpha_1, \cdots, \alpha_n)$ be an algebraic extension. Then $E/F$ is separable $\iff$ each $\alpha_i$ is separable over $F$. 

2
Proof: The forward direction is trivial. For the reverse, consider the chain of fields:

\[ F \subseteq F(\alpha_1) = F_1 \subseteq F(\alpha_1, \alpha_2) = F_2 \subseteq \cdots \subseteq F(\alpha_1, \ldots, \alpha_n) = F_n = E \]

Then consider also \( F_i/F_{i-1} \). As \( \alpha_i \) is separable over \( F \), \( \alpha_i \) is separable over \( F_{i-1} \). Therefore, we have that \( [F_i : F_{i-1}]_s = [F_i : F_{i-1}] \). Therefore, by multiplicativity of the separability degree, we get that \( [E : F]_s = [E : F] \).

**Theorem:** Let \( E/F \) be an algebraic field extension. If \( \text{Char} \ F = 0 \) then \( E/F \) is separable.

**Proof:** Let \( \alpha \in E \) and \( f(x) = \text{Irr}(\alpha, F) \). Then \( \gcd(f, f') = 1 \) and hence \( f(x) \) has distinct roots, so \( \alpha \) is separable.

**Definition:** A field \( F \) is called **perfect** if every algebraic extension of \( F \) is separable (hence if \( \text{Char} \ F = 0 \) then \( F \) is perfect).

**Theorem:** Let \( F \) be a field of characteristic \( p \) \( > 0 \). Then \( F \) is perfect \( \iff F = F^p = \{ \alpha^p \mid \alpha \in F \} \) (i.e. every element of \( F \) has a \( p \)th root). Note also that \( F^p \) is a subfield of \( F \) in this case.

**Proof:** " \( \Rightarrow \) ": Let \( \alpha \in F \). Consider \( f(x) = x^p - \alpha \in F[x] \). Let \( E \) be a splitting field for \( f \) and let \( \alpha \) be a root of \( f(x) \) in \( E \). So \( \alpha^p = \alpha \), so we wish to show that \( \alpha \in F \). In \( E[x], f(x) = x^p - \alpha^p = (x - \alpha)^p \). Let \( h(x) = \text{Irr}(\alpha, F) \). Then \( h(x) \mid f(x) \). So, in \( E[x] \), we have that \( h(x) \mid (x - \alpha)^p \). But \( E/F \) is separable, so \( \alpha \) is separable over \( F \), hence \( h(x) \) has no multiple roots. Therefore \( h(x) = (x - \alpha) \). Therefore \( \alpha \in F \) and we have that \( \alpha \) is a \( p \)th power of \( \alpha \).

" \( \Leftarrow \) ": Let \( E/F \) be an algebraic extension. Let \( \alpha \in E \) and suppose \( \alpha \) is not separable over \( F \). Let \( f(x) = \text{Irr}(\alpha, F) \). Then \( f(x) \) has multiple roots and by a previous result, we have that \( f(x) = g(x^p) \) for some \( g \in F[x] \), say \( g(x) = a_0 x^p + \cdots + a_1 x + a_0 \in F[x] \). For each \( i \), let \( a_i = b_i^p \), since \( F = F^p \). Then we have that \( f(x) = g(x^p) = b_n^p (x^n)^p + \cdots + b_1 x^p + b_0^p = (b_n x^n + \cdots + b_1 x + b_0)^p \), a contradiction to the fact that \( f(x) \) was irreducible. Therefore, \( \alpha \) is separable.

**Corollary:** Every finite field is perfect.

**Proof:** Let \( F \) be a finite field, \( \text{Char} F = p \). Consider the Frobenius endomorphism

\[ \phi : F \to F \]

\[ a \to a^p \]

Note that \( \ker \phi = \{0\} \), so as \( F \) is finite, \( \phi \) is surjective as well, so \( F = F^p \). Therefore, \( F \) is perfect.

**Example:** Let \( t \) be an indeterminant over \( \mathbb{Z}_p \). Let \( F = \mathbb{Z}_p(t) \). Then \( F \neq F^p \) as \( t \) is not a \( p \)th power. Therefore, \( F \) is not perfect. An inseparable element would be \( \alpha \) where \( \alpha \) is a root of \( f(x) = x^p - t \).

**Major Proposition on Separability:** Let \( K \) be a field of \( \text{Char} \ K, \alpha \in K \).

1. \( \alpha \) is separable over \( K \iff K(\alpha) = K(\alpha^p) \).
2. If \( \alpha \) is inseparable over \( K \), then \( [K(\alpha) : K(\alpha^p)] = p \) and \( \text{Irr}(\alpha, K(\alpha^p)) = x^p - \alpha^p \).
3. \([K(\alpha) : K]_s = [K(\alpha^p) : K]_s \) for all \( n \geq 1 \).
4. \( \alpha^{p^n} \) is separable over \( K \) for all large \( n \).
5. \([K(\alpha) : K] = p^n [K(\alpha) : K]_s \) where \( n \) is the largest nonnegative integer such that \( \alpha^{p^n} \) is separable.
Proof:

1. $\Rightarrow$: Suppose $\alpha$ is separable over $K$. So $\alpha$ is separable over $K(\alpha^p)$. Let $f(x) = \text{Irr}(\alpha, K(\alpha^p))$. Then $f(x) | x^p - \alpha^p \in K(\alpha^p)[x]$. Therefore, in $K(\alpha)[x]$, $f(x) | (x - \alpha)^p$. As $f(x)$ has no multiple roots $f(x) = x - \alpha$. Therefore $\alpha \in K(\alpha^p)$ and hence $K(\alpha) = K(\alpha^p)$.

$\Leftarrow$: Suppose $K(\alpha) = K(\alpha^p)$. Let $h(x) = \text{Irr}(\alpha, K)$. Suppose $h(x)$ has multiple roots. Then $h(x) = g(x^p)$ for some $g(x) \in K[x]$. But $h(\alpha) = g(\alpha^p) = 0$. Thus, $[\alpha^p : K] \leq \deg g(x) < \deg h$. On the other hand, $[K(\alpha^p) : K] = [\alpha : K] = \deg h$, a contradiction. Thus $h(x)$ does not have multiple roots.

2. Let $f(x) = \text{Irr}(\alpha, K(\alpha^p))$. We know $f(x) | x^p - \alpha^p = (x - \alpha)^p$. Therefore, we have that $f(x) = (x - \alpha)^m$ for some $1 \leq m \leq p$. Note that $m > 1$ as $\alpha$ is inseparable. So, expanding $f(x)$ gives $f(x) = x^m + (m\alpha)x^{m-1} + \cdots$, so $m\alpha \in K(\alpha^p) \Rightarrow \alpha \in K(\alpha^p)$ unless $m = p$, so we must have that $m = p$, again, since $\alpha$ is inseparable. Therefore, $\text{Irr}(\alpha, K(\alpha^p)) = x^p - \alpha^p$ and hence $[K(\alpha) : K(\alpha^p)] = p$.

3. $[K(\alpha) : K(\alpha^p)]_s = [K(\alpha^p)(\alpha) : K(\alpha^p)]_s$ is the number of distinct roots of $\text{Irr}(\alpha, K(\alpha^p)) = 1$ since the only root of $\text{Irr}(\alpha, K(\alpha^p))$ is $\alpha$. So, as $[\cdot, \cdot]_s$ is multiplicative, $[K(\alpha) : K]_s = [K(\alpha^p) : K]_s$ and by induction we see that $[K(\alpha) : K]_s = [K(\alpha^p) : K]_s$ for all $n \geq 1$.

4. Consider the chain of fields

$$K(\alpha) \subseteq K(\alpha^p) \subseteq K(\alpha^{p^2}) \subseteq \cdots \subseteq K$$

This is a descending chain of finite dimensional vector $K$ vector spaces (as $\alpha$ is algebraic over $K$, $[K(\alpha) : K] < \infty$). Therefore, for some $n$, we have that $K(\alpha^{p^n}) = K(\alpha^{p^{n+1}})$. Therefore, $\alpha^{p^n}$ is separable over $K$. Thus $K(\alpha^{p^n})/K$ is separable and hence $\alpha^{p^l}$ is separable for all $l \geq n$.

5. By the above propositions, we have the following tower of fields and their degrees

$$\begin{array}{c}
K(\alpha) \\
\text{p} \\
K(\alpha^p) \\
\text{p} \\
\vdots \\
\text{p} \\
K(\alpha^{p^n}) \\
\text{sep} \\
K
\end{array}$$

Therefore, we have that $[K(\alpha) : K] = p^n[K(\alpha^{p^n}) : K] = p^n[K(\alpha^{p^n}) : K]_s = p^n[K(\alpha) : K]_s$, as desired.
Theorem: Let $E = K(\alpha_1, \ldots, \alpha_n)$ be a finite extension. Then $[E : K] = p^m[E : K]_s$ for some $m \geq 0$.

Proof: Prove by induction on $n$. For the case $n = 1$, this is part 5 of the above major proposition. For $n > 1$, let $F = K(\alpha_1, \ldots, \alpha_{n-1})$. By induction, $[F : K] = p^l[F : K]_s$. As $E = F(\alpha_n)$, $[E : F] = p^k[E : F]_s$, and hence $[E : K] = p^{k+l}[E : K]_s$.

Corollary: If $[E : K] < \infty$ then $[E : K]_s \mid [E : K]$.

Definition: Let $E/K$ be a finite field extension. Then define the inseparable degree of $E/K$ by $[E : K]_i = [E : K]_s$. By the theorem, $[E : K]_i = 1$ or a power of the characteristic. As a remark, we also have that the inseparability degree is multiplicative since both the usual degree and the separable degree are multiplicative.

Definition: Let $K$ be a field of characteristic $p$ and $\alpha$ an algebraic element of $\bar{K}$. Then $\alpha$ is purely inseparable over $K$ if $\alpha^{p^n} \in K$ for some $n \geq 0$. An algebraic extension $E/K$ is called purely inseparable if each $\alpha \in E$ is purely inseparable.

Lemma: An element $\alpha \in \bar{K}$ is purely inseparable over $K \iff [K(\alpha) : K] = [K(\alpha) : K]_i \iff [K(\alpha) : K]_s = 1$.

Proof: Suppose that $\alpha$ is purely inseparable over $K$. Then $\alpha^{p^n} \in K$ for some $n$. Then $[K(\alpha) : K]_s = [K(\alpha^{p^n}) : K]_s = [K : K]_s = 1$, by part 3) of the proposition. Suppose that $[K(\alpha) : K]_s = 1$. By part 4), $\alpha^{p^n}$ is separable over $K$ for some $n \geq 0$. Then $[K(\alpha^{p^n}) : K] = [K(\alpha^{p^n}) : K]_s = [K(\alpha) : K]_s = 1$ and hence $\alpha^{p^n} \in K$.

Theorem: Let $E/K$ be a finite extension. Write $E = K(\alpha_1, \ldots, \alpha_n)$. Then TFAE:

1. $E/K$ is purely inseparable.
2. Each $\alpha_i$ is purely inseparable.
3. $[E : K]_s = 1$
4. $[E : K]_i = [E : K]$

Proof: Induction on $n$ (Exercise).