Theorem: $f$ is separable $\iff f$ and $f'$ are relatively prime.

"Proof":

$$f = (x-2)^2 (x+1) \quad \text{(not separable)}$$

$$f' = (x-2)^2 \frac{d}{dx} (x+1) + \frac{d}{dx} (x-2)^2 (x+1)$$

$$= (x-2)^2 (1) + 2(x-2)(1)(x+1)$$

Note: The derivative is taken with respect to $x$.
Theorem 1: If $\mathbb{F} = \mathbb{F}_p^n$, finite field $\Rightarrow$ $F$ is the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$

Proof:

\[
f = x^{p^n} - x
\]

\[
f' = x^{p^n} \cdot x^{p^n-1} - 1
\]

\[
= 0 \cdot x^{p^n-1} - 1 \quad \text{char}(\mathbb{Z}_p) = p
\]

\[
= -1
\]

So $f$ and $f'$ are relatively prime $\Rightarrow f$ separable

$R =$ set of all roots of $x^{p^n} - x$ in splitting field $F$

$|R| = p^n$ (if separable & degree $p^n$)

$R$ is a field (all by itself)

Closure?
\( r_1, r_2 \in \mathbb{R} \)  

Know \( r_1^{p^n} - r_1 = 0 \) \( \rightarrow r_1^{p^n} = r_1 \)

\( r_2^{p^n} - r_2 = 0 \) \( \rightarrow r_2^{p^n} = r_2 \)

Is \( r_1r_2 \in \mathbb{R} \)?  \( (r_1r_2)^{p^n} = r_1^{p^n}r_2^{p^n} = r_1r_2 \) \( \rightarrow \) \( r_1r_2 \) root of \( x^{p^n} - x \)

Is \( r_1 + r_2 \in \mathbb{R} \)?  \( (r_1 + r_2)^{p^n} = r_1^{p^n} + r_2^{p^n} = r_1 + r_2 \) \( \rightarrow \) \( r_1 + r_2 \) root of \( x^{p^n} - x \)

\( \text{Freshman's Dream} \)

So \( R \) is a field with all the roots of \( x^{p^n} - x \) and must be the smallest field with all the roots.

So \( R \) is a splitting field of \( x^{p^n} - x \) of order \( p^n \).

Grab any other field of order \( p^n \), it too will be a splitting field of \( x^{p^n} - x \), and splitting fields are unique.

"The field of order \( p^n \)."
Subfields

Fact: \( F \) field of order \( p^n \), \( K \) subfield

\[ \iff 1K1 = p^m \text{, with } m \mid n. \]

Example: \( 1F1 = p^6 \)

Subfields have order \( p^1, p^2, p^3, p^6 \) (not \( p^4, p^5 \))

\[ \implies 1F1 = p^n, K \text{ subfield} \]

\[ \text{char}(F) = p \implies \text{char}(K) = p \quad (\text{both contain } \mathbb{Z}_p) \]

\[ \implies 1K1 = p^m \text{ for some } m \quad (\text{OR, } K \text{ subfield of } F \text{ additively closed by Lagrange's Theorem}) \]

Then

\[ [F: \mathbb{Z}_p] = [F:K][K: \mathbb{Z}_p] \]

\[ n = [F:K] m \implies m \mid n \]
Assume $F = \mathbb{F}_p^n$, $m | n$, create a subfield of order $\mathbb{F}_p^m$.

Algebra

\[ p^n - 1 = p^m - 1 = (p^s)^m - 1 \]
\[ = (p^s - 1) \left( (p^s)^{m-1} + (p^s)^{m-2} + \ldots + (p^s) + 1 \right) \]
\[ = (p^s)^m - (p^s)^{m-1} - \ldots - (p^s) - p^s - 1 \]

\[ x^{p^n} - x = x \left( x^{p^m-1} - 1 \right) \]
\[ = x \left( x^{p^m-1} - 1 \right) \]
\[ = x \left( x^{p^m-1} - 1 \right) \]

Switch $s \neq m$

\[ f = (p^m)^{s-1} + (p^m)^{s-2} + \ldots + p^m + 1 \]
\[ = x \left( x^{p^{m-1}} - 1 \right) \left( x^{p^{m-1} \cdot 2} + x^{p^{m-1} \cdot 3} + \cdots + x^{p^{m-1}} + 1 \right) \]

So \( x(x^{p^{m-1}} - 1) = x^{p^m} - x \) is a factor of \( x^{p^m} - x \) 

So the roots of \( x^{p^m} - x \) are roots of \( x^{p^m} - x \) 

(when \( m/n \) =) splitting field of \( x^{p^m} - x \) is a subfield of \( F \) with order \( p^m \)

\underline{Calculus geometric series}

\[ \frac{x^{k-1}}{x-1} = x^{k-1} + x^{k-2} + \cdots + x + 1 \]

\[
\frac{1}{1-r} = \frac{a}{1-r}
\]