Example: $x^p - t$ in $K[x]$ where $K = \mathbb{F}_p(t)$, is an example of an irreducible, non separable polynomial.

Definition: For any field K and $f(x) \in K[x]$ given by

$f(x) = \sum_{i=0}^{d} a_i x^i$. Define the derivative of f by

$f'(x) = \sum_{i=1}^{d} i a_i x^{i-1}$.

Proposition: For $f, g \in K[x]$,

(i) $(f(x) + g(x))' = f'(x) + g'(x)$

(ii) $(f(x) g(x))' = f'(x) g(x) + f(x) g'(x)$

(iii) $((f \circ g)(x))' = f'(g(x)) \, g'(x)$.

Suppose $f(x) \in K[x]$ is irreducible and not separable. Let L be a splitting field. $f(x) = (x-\alpha)^2 g(x) \in L[x]$ for some α

$f'(x) = 2(x-\alpha) g(x) + (x-\alpha)^2 g'(x) \Rightarrow f'(\alpha) = 0$.

But $f'(x) \in K[x]$ and $f'(\alpha) = 0$, so $f'(x) \in \langle f(x) \rangle$.

However, $\deg(f'(x)) < \deg(f(x))$

and $f'(x) = f(x) g(x) \Rightarrow \deg(f'(x)) > \deg(f(x))$ (absurd)

or $f'(x) = 0$.

If $f(x) = \sum_{i=1}^{d} a_i x^i$, then $f'(x) = \sum_{i=0}^{d} i a_i x^{i-1} = 0$ if and only if $i a_i = 0$. Assuming $d > 1$, then not all a_i are zero so, some $i = 0 \Rightarrow \mathrm{char}(K) \neq 0$. In particular, $\mathrm{char}(K) = p$, and $i a_i = 0$ $\forall i$, so $a_i = 0$ $\forall i$ not divisible by p. So,

$f(x) = \sum_{i=0}^{n} a_{p^i} x^{p^i} = \sum_{i=0}^{n} a_{p^i} (x^p)^i = g(x^p)$ for some polynomial $g(x) \in K[x]$. So $f(x)$ is irreducible and inseparable implies

$f(x) = g(x^p)$ for some $g(x) \in K[x]$,

Note: Any irreducible polynomial (in characteristic p) can be written as $g(x^{p^e})$ for $e \geq 0$ and g is separable.

If $f(x) = g(x^{p^e})$, the roots of f are p^eth roots of a separable polynomial.

If $\text{char}(K) = 0$, irreducible $\Leftrightarrow$ separable.

Note: Let $\text{char}(K) = p$ and suppose $K = K^p = \{a^p : a \in K\}$

if $f(x) = g(x^p) = \sum_{i=0}^{d} a_i x^{p^i} = \sum_{i=0}^{d} b_i^p x^{p^i}$ for $a_i = b_i^p$, $b_i \in K$

$= \left(\sum_{i=0}^{d} b_i x^i\right)^p \Rightarrow f$ is reducible, so $\text{char}(K) = p$ and $K = K^p$ implies irreducible $\Leftrightarrow$ separable.

Definition: K is called perfect if $\text{char}(K) = 0$ or $\text{char}(K) = p$ and $K = K^p$.

<u>Stronger</u>: K is perfect if every irreducible polynomial is separable.

Note: All finite fields are perfect.

Proof: If K is a finite field of $\text{char}(K) = p$, $\varphi(x) = x^p$ is additive $\varphi(x+y) = \varphi(x) + \varphi(y)$ and

$\varphi(a) = \varphi(b) = 0 = \varphi(a) - \varphi(b) = \varphi(a-b) = (a-b)^p \Rightarrow a = b$.

So φ is one-to-one, and hence onto as well.

Theorem: If F/K is an extension, TFAE

(a) F is algebraic and Galois over K

(b) F is separable and splitting field

(c) F is a splitting field over K of a set of separable polynomials.

Proof: omitted.

Definition: An extension F/K is normal if every irreducible polynomial $f(x) \in K[x]$ which has a root in F factors as a product of linear factors

$$f(x) = \alpha(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

Theorem: An algebraic extension is Galois if and only if it is normal and separable.

Note: If F/K is a finite separable extension, it has a basis $b_1, \dots, b_n \in K$ and those have some (separable) minimal polynomials $f_1, \dots, f_n$. The splitting field of these is a finite, separable splitting field, so its Galois extension of K containing F. This is called the Galois closure over K

Example: The Galois closure of $\mathbb{Q}(\sqrt[4]{2})$ is $\mathbb{Q}(i, \sqrt[4]{2})$ over $\mathbb{Q}$

Galois Group of Polynomials

Definition: The Galois group of $f(x) \in K[x]$ is $\mathrm{Aut}_K(F)$ for a splitting field F of f over K.

Example: If $\deg(f) = 2$ and f is irreducible, then the Galois group of f is $\mathbb{Z}_2$, unless $\mathrm{char}(K) = 2$ in which the Galois group could be trivial if $f(x) = x^2 - t$, for example.

Example: If $\deg(f) = 3$, then the splitting field has degree at most $3!$

Observation: If $\deg(f) = n$, then the action of $\mathrm{Aut}_K(F)$ on the roots of f (F a splitting field) gives an embedding $\mathrm{Aut}_K(F) \hookrightarrow S_n$. Also, if f is separable, this subgroup of S_n is transitive.

Example: Let $f(x) = ax^3 + bx^2 + cx + d$ irreducible, separable, then the Galois group is a transitive subgroup of S_3, so it is S_3 or A_3. Can we tell which one?

Definition: Let $\mathrm{char}(K) \neq 2$. If $f(x) \in K[x]$ has distinct roots $\alpha_1, \dots, \alpha_n$ (in some splitting field F), let

$$\Delta_f = \prod_{i<j} (\alpha_i - \alpha_j) \quad \text{and} \quad D_f = \Delta_f^2$$

D_f is called the discriminant of f.

Observations:

(i) $\Delta_f \in F$

(ii) $D_f \in K$

Indeed, if $\sigma \in \mathrm{Gal}(F/K)$, σ permutes the roots, so

$\sigma(\Delta_f) = \prod_{i<j} (\alpha_{\sigma(i)} - \alpha_{\sigma(j)}) = \mathrm{sgn}(\sigma)\,\Delta_f$

$\sigma(D_f) = \sigma(\Delta_f)^2 = (\mathrm{sgn}(\sigma)\Delta_f)^2 = \Delta_f^2 = D_f$

So $D_f \in K$.

So $K(\Delta_f)$ is an extension of K of degree 1 or 2.

In the case of cubic, $[K(\Delta_f) : K] = 2 \Rightarrow [F : K] = 6$