Recall Thm 2-19

Thm 2.19 If $\varphi : F \to \tilde{F}$ an isom of fields $f \in F[x]$ with K a splitting field of f / F and $\tilde{K}$ a splitting field of φf over $\tilde{F}$

Then $[K : F] = [\tilde{K} : \tilde{F}]$ and φ extends to an isom $\sigma : K \to \tilde{K}$ and the number of such extensions is at most $[K : F]$

The proof fixed $\alpha \in F$ and extended φ to $\varphi' = F(\alpha) \to F(\tilde{\alpha})$ where $\tilde{\alpha}$ is a root of φm, with $m(x) = \min_{\alpha, K}$

The choices of $\tilde{\alpha}$ are the roots of φm which is at most $\deg m$. If m is separable then m has exactly $\deg m$ distinct roots and the same proof gives

Thm 2-19' If $f(x)$ is separable, then there are exactly $[K : F]$ extensions $\sigma : K \to \tilde{K}$ s.t $\sigma|_F = \varphi$.

In particular if $\varphi : F \to F$ identity isom. $f \in F[x]$, and K is a splitting field of f, f a separable poly. Then $\exists$ exactly $[K : F]$ isom $\sigma : K \to K$ s.t $\sigma|_F = id_F$

Rmk In the case of finite fields we'll see that any poly of the form $f(x) = g(x^p)$ is necessarily reducible which will show that over a finite field every irred poly is seperable as well.

Hence to find irred, inseparable poly we need to look at fields of char p which are not finite fields, as was the case in the example.

$$x^p - t \in \mathbb{Z}_p(t)[x]$$

Before looking at finite fields and char p we state an important theorem in char 0 which says that every finite (seperable) extension $K:F$ is a simple extension, ie $\exists\ \alpha \in K$ s.t $K = F(\alpha)$

Thm 2.29. Let F be a char 0 field and $K:F$ a finite extension. Then $\exists\ \alpha \in K$ s.t $K = F(\alpha)$.

Proof Since $[K:F]$ is finite we have that $K = F(\alpha_1 \ldots \alpha_n)$ for some $\alpha_i \in K$.

We use induction on n.

If $n=1$ there is nothing to prove

Note

It is enough to prove the thm for $n=2$

Since if $F(a,b) = F(c)$ for some $c \in K$ then

for $n>2$ by induction we have

$F(\alpha_1, \ldots, \alpha_{n-1}) = F(a)$ for some $a \in K$

and

$K = F(\alpha_1, \ldots \alpha_{n-1}, \alpha_n) = F(a, \alpha_n) = F(c)$

for some c.

So assume $K = F(a,b)$. We w.t.s $\exists c \in K$ s.t $K = F(c)$, for a lin. comb $c = a + zb$ with $z \in F$

Let f, g be minimal polys of a and b over F. Let $M:F$ be a field extension of F where f, g split into linear factors

Let $a = x_1, x_2 \ldots x_r$ be roots of f

$b = y_1, \ldots, y_s$ be roots of g.

Then since we are in char 0, g has distinct roots and hence $b \neq y_j$ for $j \neq 1$

If we define $z_{ij} := \dfrac{x_i - a}{b - y_j} \in M$ then z_{ij} is the

$j \neq 1,\ i \neq 1$

only element of M which solves $a + tb = x_i + ty_j$

Since F is infinite, we can choose a $z \in F$ different from all z_{ij}'s and hence

$a + zb \neq x_i + z y_j$ unless $i = j = 1$.

Put $c = a + bz$ then clearly $F(c) \subset F(a,b)$

w.t.s $F(a,b) \subset F(c)$

Define $h(x) := f(c - zx) \in F(c)[x]$

Then $h(b) = f(c - zb) = f(a) = 0$.

Since b is also a zero of $g(x)$, $(x-b) \mid g$
so $(x - b) \mid h$ and $(x-b) \mid g$

We will show that $\gcd(h, g) = x - b$
This in return shows that $x - b \in F(c)[x]$
(since $\gcd(h,g) \in F(c)[x]$ for $h, g \in F(c)[x]$)
but then $b \in F(c)$ hence
$a = c + zb \in F(c)$ thus
$F(a,b) \subset F(c)$

It remains to show $\gcd(h, g) = x - b$.
Since g splits over M into linear factors the gcd must be some product of linear factors of g.
But if $y_j \neq b$ another root of g

$h(y_j) = f(c - zy_j) \neq 0$ since with

our choice of z $c - zy_j \neq x_i$ for any root x_i of f.

$(c = a + bz \neq x_i + zy_j)$

Thus $X - y_j$ is not a factor of h

Thus $X - b$ is the gcd of h and g $\square$

Rmk This thm follows more easily once we have the Galois correspondence

In fact it is true that

Thm An alg extension $L:K$ is simple $\Leftrightarrow$ there are only finitely many intermediate fields

Using this one can show

Thm Suppose $L:K$ is finite and separable. Then $L:K$ is simple.