§6: Inseperable extensions

Definition 6.0

Let $f(X) = (X-\alpha)^m g(X) \in k[X]$ and assume that $X-\alpha \nmid g(X)$. We say that α is a multiple root of if $m > 1$. Otherwise we say that α is a simple root.

Proposition 6.1.

Let α be algebraic over k; $\alpha \in k^a$ and let:

$$f(X) = Irr(\alpha, k, X)$$

If $\operatorname{char} k = 0$. Then all roots of f have multiplicity 1.

Otherwise if $\operatorname{char} k = p$; then there exists an integer $\mu \geq 0$ s/t every root of f has multiplicity p^μ. We have:

$$[k(\alpha) : k] = p^\mu [k(\alpha) : k]_s$$

and α^{p^μ} is seperable over k.

Proof: First we will show that for all k; if α

has multiplicity m; then all roots of f has multiplicity m.

Let $\alpha_1, \dots, \alpha_n$ be the distinct roots of $w/\ \alpha_1 = \alpha$. We let $E = k(\alpha_1, \dots, \alpha_n)$ and:

$$\sigma_i : E \longmapsto k^a$$

be an embedding of E in k^a over k extending the isomorphism:

$$k(\alpha_i) \longmapsto k(\alpha)$$
$$\alpha_i \longmapsto \alpha$$

If $f(X) = \prod_{i=1}^{n} (X - \alpha_i)^{m_i}$; we have:

$$\sigma f(X) = \prod_{j=1}^{\hat{}} (X - \sigma(\alpha_j))^{m_j} = (X - \alpha_1)^{m_i} \prod_{j \neq i} (X - \sigma(\alpha_j))^{m_j} = f(X).$$

$$= (X - \alpha_1)^{m_1} \prod_{j \neq 1} (X - \alpha_j)^{m_j}$$

So if $g_1(X) = \prod_{j \neq i} (X - \sigma(\alpha_j))^{m_j}$; $g_2(X) = \prod_{j \neq 1} (X - \alpha_j)^{m_j}$ and

assume that $m_i \neq m_1$ so WLOG $m_i < m_1$:

$$0 = (X-\alpha_1)^{m_i}\left(g_1(X) - (X-\alpha_1)^{m_1-m_i} g_2(X)\right)$$

$$\Rightarrow g_1(X) - (X-\alpha_1)^{m_1-m_i} g_2(X) = 0$$

Since E is normal, σ_i is an automorphism, so

$\sigma_i(\alpha_j) \neq \alpha_1 \ \forall\, j \neq i$. So $g_1(\alpha_1) \neq 0$ but

$$0 = g_1(\alpha_1) - (\alpha_1 - \alpha_1)^{m_1-m_i} g_2(\alpha_1) \to 0$$

$\not\Rightarrow$

So $m_i = m_1$. Since i was arbitrary all roots of f have all the same multiplicity.

Now we will look at two cases:

- $\mathrm{char}\, k = 0$:

Then notice $f'(x) \neq 0$ and $\deg f' < \deg f$.

Therefore $f'(x) \notin (f(x))$ so $f'(\alpha) \neq 0$ so

α is a simple root and so all roots of f

have multiplicity 1.

- $\operatorname{char} k = p > 0$

Assume that α is a multiple root of f.

So $f'(\alpha) = 0 \Rightarrow f'(x) \in (f(x))$ and $\deg f' < \deg f$

so:

$$f'(x) = 0.$$

Now let

$$f(x) = (x-\alpha)^m g(x) \text{ where } x - \alpha \nmid g(x).$$

Then we see that:

$$f'(X) = m(X-\alpha)^{m-1} g(X) + (X-\alpha)^m g'(X)$$

$$= 0$$

$$\therefore (X-\alpha)^{m-1}\left(m g(X) + (X-\alpha) g'(X)\right) = 0$$

$$\Rightarrow \quad m g(X) + (X-\alpha) g'(X) = 0.$$

So

$$m g(\alpha) = 0 \quad \text{but } g(\alpha) \neq 0 \text{ so.}$$

$p \mid m$, assume that $m = p^\mu r$ w/ $p \nmid r$.

So:

$$f(X) = \prod_i (X-\alpha_i)^{p^\mu r} = \prod_i \left(X^{p^\mu} - \alpha_i^{p^\mu}\right)^r$$

Yet

$$m(X) = \prod_i \left(X - \alpha_i^{p^\mu}\right)^r \in k[X]$$

Assume that $m(X) = p(X)q(X)$ w/ $p, q \in k[X]$.

Then

$$f(X) = m(X^{p^n}) = p(X^{p^n}) q(X^{p^n}).$$

Which contradicts the fact that $f(X)$ is irreducible.

So $m(X)$ is irred but $\mathrm{Irr}(\alpha^{p^n}, k, X) \mid m(X)$, so

$$m(X) = \mathrm{Irr}(\alpha^{p^n}, k, X)$$

Likewise to above we see that either $r = 1$ or $p \mid r$, the second case is impossible since $p \nmid r$.

So:

$$f(X) = \prod_i (X^{p^n} - \alpha^{p^n}) = \prod_i (X - \alpha)^{p^n}$$

Note that:

$$X^{p^n} - \alpha^{p^n} = \mathrm{Irr}(\alpha, k(\alpha^{p^n}), X).$$

This is true if $p(X) \in k(\alpha^{p^n})[X]$ w/ $p(X) \mid X^{p^n} - \alpha^{p^n}$

then since $X^{p^\mu} - \alpha^{p^\mu} = (X-\alpha)^{p^\mu} \in k^u[X]$.

$$\Rightarrow p(X) = (X-\alpha)^{p^\omega} = X^{p^\omega} - \alpha^{p^\omega} \quad \text{w/ } \omega \leq \mu.$$

But since $\alpha^{p^\omega} \in k(\alpha^{p^\mu}) \Rightarrow \omega \geq \mu$.

$$[k(\alpha) : k(\alpha^{p^\mu})] = p^\mu.$$

Furthermore since $m(X) = Irr(\alpha^{p^\mu}, k, X)$ has no multiple roots:

$$n = [k(\alpha^{p^\mu}) : k]_s = [k(\alpha^{p^\mu}) : k].$$

$$\Rightarrow [k(\alpha) : k] = [k(\alpha) : k(\alpha^{p^\mu})][k(\alpha^{p^\mu}) : k]$$
$$= p^\mu [k(\alpha^{p^\mu}) : k]_s$$
$$= p^\mu n$$
$$= p^\mu [k(\alpha) : k]_s$$

Pf

Corollary 6.2.

For any finite extension E of k, $[E:k]_s \mid [E:k]$. The quotient is 1 if $\mathrm{char}\, k = 0$ and a power of p if $p > 0$.

Proof: Let $E = k(\alpha_1, \dots, \alpha_n)$, and apply 6.1 on the tower:

$$k(\alpha_1) \subseteq k(\alpha_1, \alpha_2) \subseteq \dots \subseteq k(\alpha_1, \dots, \alpha_n) = E$$

∎

Definition 6.1

If $E|k$ is finite, we call:

$$[E:k]_i = \frac{[E:k]}{[E:k]_s}$$

the inseparable degree

We will now assume that k is a field of characteristic $p > 0$.

Definition 6.2.

An element α algebraic over k is

said to be purely inseperable over k if there exists an integer $n \geq 0$ s/t α^{p^n} lies in k.

Proposit° 6.1.1. Let E be an algebraic extension of k. TFAE:

P. Ins 1: $[E:k]_s = 1$.

P. Ins 2: Every element α of E is purely insep. over k.

P. Ins 3: $\forall \alpha \in E$:

$$\mathrm{Irr}(\alpha, k, X) = X^{p^n} - a \quad \text{for some } n \geq 0 \text{ \& } a \in k$$

P. Ins 4: There exists generators $\{\alpha_i\}_{i \in I}$ of E over k s/t α_i is purely inseperable over k.

Proof:

1) $\Rightarrow$ 2)

Let $\alpha \in E$ we have the tower:

$E \supseteq k(\alpha) \supseteq k$ w/

$$1 = [E:k]_s = [E:k(\alpha)]_s \, [k(\alpha):k]_s$$

($[E:k(\alpha)]_s \to 1$, $[k(\alpha):k]_s \to 1$)

Furthermore recall:

$$[k(\alpha):k]_s = \#\text{ distinct roots of } f(X)$$

where $f(X) = Irr(\alpha, k, X)$.

$\therefore$

$f(X) = (X-\alpha)^m$. but recall $\exists\, n>0$ s.t. $m = p^n$ (by prop 6.1)

$$f(X) = (X-\alpha)^{p^n} = X^{p^n} - \alpha^{p^n} \in k[X]$$

$\therefore \alpha^{p^n} \in k$.

2) $\Rightarrow$ 3)

Let n be the smallest integer s.t. $a = \alpha^{p^n} \in k$.

$$\Rightarrow (X-\alpha)^{p^n} = X^{p^n} - \alpha^{p^n} = X^{p^n} - a \in k[X]$$

So $\mathrm{Irr}(\alpha, k, X) = f(X) \mid (X-\alpha)^{p^n}$

But this means that $f(X)$ only has one distinct root. So by Prop 6.1:

$$f(X) = (X-\alpha)^{p^\mu} \quad \text{for some } 0 \le \mu \le n.$$
$$= X - \alpha^{p^\mu}$$

Since $\alpha^{p^\mu} \in k$ and $\mu \le n$ by the definition of n:

$$f(X) = (X-\alpha)^{p^n} = X^{p^n} - a.$$

3) $\Rightarrow$ 4)

Since all elements of $\alpha \in E$ have their irreducible pol of the type:

$$X^{p^n} - a = 0 \Rightarrow \alpha^{p^n} = a \in k \text{ for some } n.$$

So all elements of E are purely inseparable over k. We can take E to be the set of generators of itself.

4) $\Rightarrow$ 1)

Let $\sigma : E \longmapsto E^a$; be an embedding over k.

Let $\{\alpha_i\}_{i \in I}$ be the set of generators of E over k s.t each α_i is purely inseparable over k.

So $\forall i$; let n_i be s.t.:

$$\alpha_i^{p^{n_i}} \in k.$$

So:

$$\alpha_i^{p^{n_i}} = \sigma(\alpha_i^{p^{n_i}}) = \sigma(\alpha_i)^{p^{n_i}}$$

$$\Rightarrow \sigma(\alpha_i)^{p^{n_i}} = \alpha_i^{p^{n_i}} = 0 .$$

$$\Rightarrow (\sigma(\alpha_i) - \alpha_i)^{p^{n_i}} = 0 .$$

$$\Rightarrow \sigma(\alpha_i) = \alpha_i$$

So $\forall \alpha \in E \Rightarrow \alpha = \sum_{i \in I} x_i \alpha_i \quad ; x_i \in k .$

$$\Rightarrow \sigma(\alpha) = \sum_i \sigma(x_i)\sigma(\alpha_i) = \sum_i x_i \alpha_i = \alpha$$

So σ is the identity. Since it was chosen to be an arbitrary embedding, any embedding of E over k is the identity.

$$[\bar{E} : k]_s = 1$$

By def of $[E : k]_s$.

∎

Definition 6.3.

Any extension satisfying one (hence all) of the above properties will be called purely inseparable.

Prop 6.5

Purely inseparable extensions form a "distinguished" class of extensions.

Proof: • If $E \supseteq F \supseteq k$:

$$[E : k]_s = [E : F]_s [F : k]_s.$$

$$\therefore [E : k]_s = 1 \iff [E : F]_s = [F : k]_s = 1.$$

- If $E, F \subseteq L$, $E \setminus k$ is purely inseperable

Let $\{\alpha_i\}_{i \in I}$ be the set of generators of E over k s.t. they are all purely inseperable.

Then note they are also the set of generators of EF over F.

∎

Prop 6.6

Let E be an algebraic extension of k. If E_0 is the compositum of all subfields F of E s.t. $F \supseteq k$ and F is seperable over k.
Then E_0 is seperable over k; and E is purely inseperable over E_0.

Proof: E_0 is seperable over k since seperable

extensions form a "distinguished" class.
Furthermore note that all elements of E_0 are seperable over k; and for all $\alpha \in E$ s/t α is seperable over k, $k(\alpha)$ is a subfield of E that is seperable over k.
So $\alpha \in E_0$.

i.e. $E_0 = \{$all elements of E; seperable over $k\}$.

But note $\forall \alpha \in E$, $\exists\, n \geq 0$ s/t α^{p^n} is seperable over k.
So $\alpha^{p^n} \in E_0 \Rightarrow E$ is purely insep over E_0. ∎

Cor 6.7. If $E \backslash k$ is purely inseperable & seperable then $E = k$.

Proof: Let $\alpha \in E$, by Prop 6.1.1 :: for some $n \in \mathbb{N}$

$$\mathrm{Irr}(\alpha, k, X) = X^{p^n} - \alpha^{p^n} = (X-\alpha)^{p^n}$$

But since α is seperable $\mathrm{Irr}(\alpha, k, X)$ has

no multiple roots, so $p^n = 1 \Rightarrow n = 0$.

$\therefore \alpha = \alpha^{p^n} \in k \quad \forall \alpha \in E$.

So $E = k$.

∎

Cor 6.8. Let K be normal over k and K_0 be it's maximal seperable subextension.
Then K_0 is also normal over k.

Proof: Let

$$\sigma : K_0 \longmapsto K^a \text{ over } k$$

be an embedding and extend this to an embedding of K.

Since K is normal $\sigma K = K$. Now note that

σK_0 is still normal over k & $\sigma K_0 \subseteq \sigma K = K$.

So $\sigma k_0 \subseteq k_0$.

So $\sigma : k_0 \to k_0$ is an embedding and so it is an isomorphism

□

Corollary 6.9. Let E, F be two finite extensions of k. Assume that E/k is separable. F/k is purely inseparable.
Assume E, F are subfields of a common field. Then:

$$[EF : F] = [E : k] = [EF : k]_s$$
$$[EF : E] = [F : k] = [EF : k]_i$$

Proof:

- $[EF : F] = [EF : F]_s$ since $EF \setminus F$ is sep

$$= [EF : F]_s [F : k]_s$$
$$= [EF : k]_s.$$

$$= [EF : E]_s \, [E : k]_s$$

$$= [E : k]_s \quad \text{since } EF \setminus E \text{ is s.i.}$$

$$= [E : k]$$

- $[EF : E] = [EF : E]_i \quad$ since $EF \setminus E$ is s.i.

$$= \frac{[EF : k]_i}{[E : k]_i}$$

$$= [EF : k]_i \quad \text{since } E \setminus k \text{ is sep}$$

$$= [EF : F]_i \cdot [F : k]_i$$

$$= [F : k]_i \quad \text{since } EF \setminus F \text{ is sep}$$

$$= [F : k]$$

∎

Cor. 6.10

Let E^p denote the field of all elements x^p; $x \in E$.
Let E be a finite extension of k.

If $E^p k = E$ then E is seperable over k. If E is sep over k then $E^{p^n} k = E \ \forall n \geq 1$.

Def 6.4 $K \backslash k$ be normal; the group of automorphisms of K over k is called the Galois group of the extension $K \backslash k$.

Def 6.5.

A field k is called perfect if $k^p = k$. (Every field of char zero is also called perfect).

Cor 6.12. If k is perfect then every algebraic extension of k is seperable, and every alg. extension of k is perfect.