Purely inseparable extensions

Recall separability

F a field, $f \in F[t]$ irreducible. f is said to be **separable** if it has distinct roots in a (so all) splitting fields.

e.g. $F = \mathbb{F}_p(t)$, $f = x^p - t \in F[x]$. Then in a splitting field of f over F, $f = (x - t^{1/p})^p$.

Let K/F and $\alpha \in K$. α is separable $/F$ if $m_F(\alpha)$ is separable $/F$.

If K/F is algebraic, we say K/F is separable if all of its elements are separable $/F$.

Now, recall some facts about the derivative

Lemma. Let $f \in F[t]$ with a root $\alpha \in K$, some K/F. Then α is a repeated root of f iff $f'(\alpha) = 0$.

Pf. Factor f in K as $(t-\alpha)^e g(t)$, where $t - \alpha \nmid g$, i.e. $g(\alpha) \neq 0$. $f'(t) = e(t-\alpha)^{e-1} g(t) + (t-\alpha)^e g'(t)$, so $f'(\alpha) = e(\alpha-\alpha)^{e-1} g(\alpha)$. $g(\alpha) \neq 0$, so $f'(\alpha) = 0 \iff e(\alpha-\alpha)^{e-1} = 0 \iff e \geq 2$. $\square$

Cor. $f \in F[t]$ has a multiple root in an extension iff

$(f, f') \neq (1)$ in $F[t]$.

Pf. ($\Rightarrow$) Let $f(\alpha) = f'(\alpha) = 0$. Then $m_F(\alpha) \mid \gcd(f, f')$.

($\Leftarrow$) If f is constant there is nothing to do, so suppose not.

Then $0 \subsetneq (f, f') \subsetneq (1)$ so there is a nonconstant

polynomial $g \in F[t]$ s.t. $g \mid \gcd(f, f')$.

g has a root α in an extension, so $f(\alpha) = f'(\alpha)$ thus

f has a multiple root by the lemma.

Recall also HW 19

a) $f \in F[t]$, char $F = 0$. Then $f' = 0 \Rightarrow f \in F$.

b) " ", char $F = p \neq 0$. Then $f' = 0 \Rightarrow \exists g \in F[t]$ s.t. $g(t^p) = f(t)$.

Furthermore, in (b), f irreducible $\Rightarrow g$ irreducible, as if

$g(t) = g_1(t) g_2(t)$ then $f(t) = g_1(t^p) g_2(t^p)$.

Def. Let α be algebraic over F. Then α is purely inseparable if $m_F(\alpha)$ has one root in a splitting field.

e.g. $x^p - t$ in $\mathbb{F}_p(t)[x]$ as before.

Thm. Let α algebraic $/F$, char $F = p$. TFAE.

i) α is purely inseparable over F

ii) $m_F(\alpha) = t^{p^e} - a$ for some $e \geq 0$ and $a \in F$.

iii) $\exists e \geq 0$ s.t. $\alpha^{p^e} \in F$.

Pf. i) $\Rightarrow$ ii). Let $f(t) = m_F(\alpha) \in F[t]$. If $\deg(f) = 1$ we are done. Else, α is a repeated root so $(f, f') \subset (1)$. But $(f) \subseteq (f, f')$ is maximal, so $f' \in (f)$, i.e. $f \mid f'$. As $\deg(f) \geq \deg(f') + 1$, we have that $f' = 0$. Hence, $f(t) = f_1(t^p)$, some irreducible $f_1 \in F[t]$, which is purely insep.

Repeat this argument until $f_e(t)$ is linear, hence of the form $t - a$, $a \in F$. Then $f(t) = f_e(t^{p^e}) = t^{p^e} - a$ as desired.

Rmk. $f_k(t) = m_F(\alpha^{p^k})$.

ii) $\Rightarrow$ iii). α is a root of $m_F(\alpha) = t^{p^e} - a$.

iii) $\Rightarrow$ i). Let $\alpha^{p^e} = a \in F$. Then $m_F(\alpha) \mid t^{p^e} - a$.

We have $t^{p^e} - a = (t - \alpha)^{p^e}$. Thus $m_F(\alpha)$ has

a unique root, so α is purely insep/F. $\square$

Rmk. This shows that any irreducible factor of $t^{p^e} - a$ is of the form $t^{p^d} - a$, $d \le e$. Indeed, if $f \mid t^{p^e} - a$ was irred, then $f^k = t^{p^e} - a$ some k, and $t^{p^e} - a = (t - \alpha)^{p^e}$ so $f = (t - \alpha)^l$. Then $lk = p^e$ so $l = p^d$.

Rmk. Normally $t^n - a$ would have n distinct roots $\{\zeta^i a^{1/n} \mid 1 \le i \le n\}$

for ζ a primitive n^{th} root of unity.

But if $char(F) = p$, the only p^eth root of unity is 1.

Indeed, $t^{p^e} - 1 = (t-1)^{p^e}$.

Def. K/F is purely inseparable if all $\alpha \in K$ are purely inseparable $/F$.

Prop. Let $K/E/F$ char p. K/F is purely inseparable iff K/E and E/F are purely inseparable.

Pf. ($\Rightarrow$) All $\alpha \in K$ have a power $\alpha^{p^e} \in F$. $F \subseteq E$ so $\alpha^{p^e} \in E$, so K/E purely insep.

Let $\alpha \in E$. $E \subseteq K$ so $\alpha \in K$, so $\exists e \ge 0$ s.t. $\alpha^{p^e} \in F$. Thus E/F purely insep.

($\Leftarrow$) Let K/E and E/F be purely inseparable.

Let $\alpha \in K$. $\exists\, e \geq 0$ s.t. $\alpha^{p^e} \in E$

$\exists\, d \geq 0$ s.t. $(\alpha^{p^e})^{p^d} \in F$

$$\begin{gathered} (\alpha^{p^e})^{p^d} \\ \parallel \\ \alpha^{p^e p^d} \\ \parallel \\ \alpha^{p^{e+d}} \end{gathered}$$

$\square$

Prop. K/F is purely insep. iff it is generated by purely insep elements.

Pf. ($\Rightarrow$) ✓

($\Leftarrow$) Let $K = F(S)$, S consisting of purely inseparable elements, and $\alpha \in K$. Then we may write

$\alpha = f(\beta_1, \ldots, \beta_n)$, $\beta_i \in S$, $f \in F[t_1, \ldots, t_n]$.

Write $f(t) = \sum_{I \in \mathbb{N}^n} a_I t^I$ for $a_I \in F$ and

$t^I := \prod_{j=1}^{n} t_j^{I(j)}$ where $I = (I(1), \ldots, I(n))$.

Each β_i is insep $/F$, so $\exists\, e_i \geq 0$ s.t. $\beta_i^{p^{e_i}} \in F$.

Let e be the max of the e_i. Then $\forall i$, $\beta_i^{p^e} \in F$.

Hence, $\alpha^{p^e} = f(\beta_1, \ldots, \beta_n)^{p^e}$

$$= \left(\sum_I a_I \beta_i\right)^{p^e}$$

$$= \sum_I a_I^{p^e} \beta_i^{p^e} \in F \qquad \square$$

Prop. Let K/F be purely insep and finite. Then $[K:F]$ is a power of $p = \mathrm{char}(F)$.

Pf. By induction, it suffices to consider $K = F(\alpha)$, and $m_F(\alpha) = t^{p^e} - a$. $\square$

Prop. Let K/F algebraic. Then K/F_{sep} is purely inseparable.

Pf. Let $\alpha \in K$, $f(t) = m_F(\alpha)$. If α is separable we are done, else $f(t)$ has a repeated root so $f(t) = f_1(t^p)$, where f_1 is irreducible. Repeat this to get $f_2, \ldots, f_e$ until f_e is separable. $f(t) = f_e(t^{p^e})$, so α^{p^e} is a root of f_e, a separable polynomial. Thus, $\alpha^{p^e} \in F_{sep}$. $\square$

Def. K/F alg. $[K:F]_i := [K:F_{sep}]$, $[K:F]_s := [F_{sep}:F]$.