Separable extensions and finite fields

<u>Recall</u>: A field F of char $p>0$ is perfect if the Frobenius map $\phi: F \to F$, $x \mapsto x^p$ is an isomorphism.

A pathological case we hope to avoid: $\mathbb{F}_p(t^{1/p})$ over $\mathbb{F}_p(t)$; $t^{1/p}$ has minimal polynomial $x^p - t = (x - t^{1/p})^p$.

<u>Definition</u>. If F is a field and $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$ is a polynomial,

$\rightsquigarrow$ define $D(f) := a_1 + a_2 x + \cdots + n a_n x^{n-1}$, called its <u>formal derivative</u> (形式导数)

If $f(x) = c \cdot (x-\alpha_1)^{e_1} \cdots (x-\alpha_r)^{e_r} \in F[x]$ with α_i pairwise distinct,

say α_i is a zero of $f(x)$ with multiplicity e_i.

<u>Theorem</u>. $f(x) \in F[x]$ with $\deg(f) \geq 1$ has no repeated roots in its splitting field K if and only if $(f(x), D(f)(x)) = (1)$.

Proof: "$\Leftarrow$" $f(x) \cdot p(x) + D(f)(x) \cdot g(x) = 1$ in $F[x] \subseteq K[x]$

But if $(x-\alpha)^2 \mid f(x)$ for $\alpha \in K \Rightarrow x - \alpha \mid D(f)(x) \Rightarrow x-\alpha \mid 1$ (in $K[x]$). This is absurd!

So $f(x)$ has no repeated roots in K.

"$\Rightarrow$" Say $(d(x)) = (f(x), D(f)(x))$

$\Rightarrow$ in $K[x]$, $d(x) \mid f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ with α_i distinct

$$\left.\begin{array}{l} \text{Yet } D(f)(\alpha_i) = \prod_{j\neq i}(\alpha_i - \alpha_j) \neq 0 \\ d(x) \mid D(f)(x) \end{array}\right\} \Rightarrow (x-\alpha_i) \nmid d(x) \Rightarrow d(x) = 1$$

<u>Definition/Corollary</u>. If $f(x)$ is an irreducible polynomial in $F[x]$, we have a dichotomy

- $f(x)$ has repeated roots in its splitting field $\Leftrightarrow D(f)(x) = 0$ $\rightsquigarrow$ call f <u>inseparable</u> (不可分多项式)
- $f(x)$ has only simple roots $\rightsquigarrow$ call f <u>separable</u>

Proof: $f(x)$ has repeated roots $\Leftrightarrow (f(x), D(f)(x)) \neq (1)$

$$\overset{\text{But } f(x) \text{ is irreducible}}{\Longleftrightarrow} f(x) \mid D(f)(x) \overset{\deg D(f) < \deg f}{\Longleftrightarrow} D(f)(x) = 0 \quad \square$$

<u>Corollary</u> If $\operatorname{char} F = 0$, all irreducible polynomials are separable

$$(\text{b/c } f(x) \neq 0,\ \deg(f) \geq 1 \Rightarrow D(f)(x) \neq 0)$$

<u>Corollary</u>. If $\operatorname{char} F = p > 0$, if $f(x)$ is inseparable, then

$$f(x) = g(x^p) \text{ for some } g \in F[x] \text{ irreducible}$$

Moreover, this can only happen when F is imperfect.

Proof. $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ irreducible and $D(f)(x) = a_1 + a_2 x + \cdots + n a_n x^{n-1} = 0$

This implies $i a_i = 0 \overset{\text{if } p \nmid i}{\Longrightarrow} a_i = 0$

So $f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots = g(x^p)$ for $g(x) = a_0 + a_p x + a_{2p} x^2 + \cdots$ irreducible

If F is perfect, then every $a_{ip} = b_i^p$ for some $b_i \in F$

$\rightsquigarrow f(x) = b_0^p + b_1^p x^p + b_2^p x^{2p} + \cdots = (b_0 + b_1 x + b_2 x^2 + \cdots)^p$ is not irreducible $\divideontimes$ $\square$

<u>Corollary</u>. If $\operatorname{char} F = p > 0$, irreducible polynomial $f(x) \in F[x]$ is of the form $f(x) = g(x^{p^e})$

with $g(x) \in F[x]$ irreducible and separable, $e \geq 0$

and $f(x)$ in its splitting field has $\deg g$ distinct zeros

$$(\text{b/c } g(x) = \prod_i (x - \alpha_i) \Rightarrow f(x) = \prod_i (x^{p^e} - \alpha_i) = \prod_i (x - \alpha_i^{1/p^e})^{p^e}\ )$$

<u>Definition</u> Let K/F be an algebraic extension

$\alpha \in K$ is called <u>separable</u>/<u>inseparable</u> (可分元/不可分元) if $m_{\alpha,F}(x)$ is

Say that K/F is <u>separable</u> if every element $\alpha \in K$ is separable over F,

otherwise, say K/F is <u>inseparable</u>.

Things to remember: inseparable $\Leftrightarrow$ involves some sort of p^{th} root.

Easy property: Given a tower of extensions $K/E/F$ and $\alpha \in K$.

$$\alpha \text{ is separable}/F \Rightarrow \alpha \text{ is separable}/E \quad (\text{b/c } m_{\alpha,E}(x) \mid m_{\alpha,F}(x).)$$

<u>Theorem</u>. (1) If α is separable over F, then $F(\alpha)$ is a separable extension of F

(2) If K/E and E/F are separable, then K/F is separable

(<u>An exercise to generalize this theorem</u>: If K/F is a finite extension, then

$K^s := \{\alpha \in K \text{ separable over } F\}$ is the maximal intermediate field that is separable over F

Define $[K:F]_{sep} := [K^s : F]$ and $[K:F]_{insep} := [K:K^s]$

Then for a tower of finite extensions $K/E/F$, we have

$[K:F]_{sep} = [K:E]_{sep} \cdot [E:F]_{sep}$ and $[K:F]_{insep} = [K:E]_{insep} \cdot [E:F]_{insep}$.)

<u>Some tools to prove the theorem</u> (modifying this tool + proof gives the proof of the exercise.)

If K/F is a finite extension, and M/F is any normal extension that contains F (e.g. a normal closure)

M — K — F

Consider all possible homomorphisms $\varphi : K \longrightarrow M$ s.t. $\varphi|_F = id$ (← automatically injective)

Denote this set by $\text{Hom}_F(K, M)$

E.g. $M = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ or $\mathbb{C}$

$K = \mathbb{Q}(\sqrt[3]{2})$

$F = \mathbb{Q}$

$K \longrightarrow M$

$\varphi_0 = \text{identity}$

$\varphi_1 : \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3$

$\varphi_2 : \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3^2$

b/c $K \simeq \mathbb{Q}[x]/(x^3-2)$

$x \longmapsto \{\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2\}$ three possible zeros

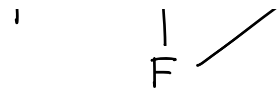
<u>Note</u>: In this example, $\#\text{Hom}_F(K, M) = [K:F]$

<u>Lemma</u>. If $K = F(\alpha)$ with $m_{\alpha,F}(x) = g(x^{p^e})$ for some $g \in F[x]$ irreducible + separable (when char $F = 0$ set $p^e = 1$)

then $\#\text{Hom}_F(F(\alpha), M) = \deg g(x) \leq [F(\alpha):F]$

(with equality iff α is separable.)

Proof: $K = F(\alpha) \overset{\varphi}{\dashrightarrow} M$ Such φ is determined by where α goes.



and $\varphi(\alpha)$ must be a zero of $m_{\alpha,F}(x)$ in M

↑ there are precisely deg g of them. □

Remark: $\# \mathrm{Hom}_F(F(\alpha), M)$ does NOT depend on M, as long as it is normal$/F$

The composite of $\varphi(F(\alpha))$ over all $\varphi \in \mathrm{Hom}_F(F(\alpha),M)$ is the normal closure of $F(\alpha)$ in M over F.

Corollary. K/F finite extension and M a normal extension of F containing K,

Then $\# \mathrm{Hom}_F(K,M) \leq [K:F]$ $\quad (*)$

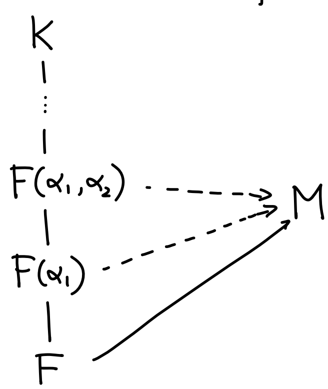
Moreover, TFAE (1) $K = F(\alpha_1, \cdots, \alpha_n)$ with each α_i separable$/F$

(2) The equality in $(*)$ holds

(3) K/F is separable, i.e. $\forall \alpha \in K$ is separable$/F$

($\Rightarrow$ Thm (1) as a special case.)

Proof:



By Lemma, $\# \mathrm{Hom}_F(F(\alpha_1), M) \leq [F(\alpha_1):F]$

For each embedding $F(\alpha_1) \hookrightarrow M$,

$\# \mathrm{Hom}_{F(\alpha_1)}(F(\alpha_1,\alpha_2), M) \leq [F(\alpha_1,\alpha_2):F(\alpha_1)]$

$\Rightarrow \# \mathrm{Hom}_F(F(\alpha_1,\alpha_2), M) \leq [F(\alpha_1,\alpha_2):F]$

Induction $\Rightarrow (*)$

(3) $\Rightarrow$ (1) is trivial (1) $\Rightarrow$ (2) by the above argument + equality condition in the previous lemma.

(2) $\Rightarrow$ (3) If α is not separable, then $\# \mathrm{Hom}_F(F(\alpha), M) < [F(\alpha):F]$

for each embedding $F(\alpha) \hookrightarrow M \rightsquigarrow \# \mathrm{Hom}_{F(\alpha)}(K,M) \leq [F(\alpha):F]$ by $(*)$

$\Rightarrow \# \mathrm{Hom}_F(K,M) < [K:F]$, contradiction!

Proof of Theorem (2): K/E separable, E/F separable $\Rightarrow K/F$ separable

* (Reduction to finite case) Take $\alpha \in K$, its minimal polynomial $m_{\alpha,E}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in E[x]$.

Consider $K' = F(a_{n-1}, \cdots, a_0, \alpha)$ instead. Take M a normal extension of F containing K'

$$E' = F(a_{n-1}, \cdots, a_0)$$
$$|$$
$$F$$

Then $\#\mathrm{Hom}_F(E', M) = [E' : F]$

For each given embedding $E' \hookrightarrow M$, $\#\mathrm{Hom}_{E'}(K', M) = [K' : E']$

$\Rightarrow \#\mathrm{Hom}_F(K', M) = [K' : F]$

So K' is separable over F and thus α is separable over F. □

<u>Theorem</u> (Primitive element theorem) A finite separable extension is generated by one element.

<u>Stronger</u>: If $K = F(\alpha, \beta)$ with α, β algebraic$/F$ and β separable$/F$ then $K = F(\gamma)$ for some $\gamma \in K$.

<u>Cor</u>. Primitive element theorem holds for fields F in char $p>0$ with $\lambda(F) \leq 1$, i.e. $[F : \sigma(F)] \leq p$.

<u>Typical non-monogenic extension</u> $\mathbb{F}_p(x^{1/p}, y^{1/p}) = K$

$$|$$
$$\mathbb{F}_p(x,y) = F$$

(for any $\alpha \in K$, $\alpha^p \in F$, so $[\mathbb{F}_p(x,y)(\alpha) : \mathbb{F}_p(x,y)] \leq p$.)

Proof: Basic idea: most $\theta = \alpha + c \cdot \beta$ should work. Just need to avoid the "bad ones"

Case of finite fields $\rightsquigarrow$ later. Now assume $\#F = +\infty$

- Let $f(x)$ and $g(x)$ be minimal polynomials of α and β over F

Let E be splitting field of $f(x)g(x)$ and $\alpha = \alpha_1, \cdots, \alpha_r$, $\beta = \beta_1, \cdots, \beta_s$ the distinct zeros of $f(x)$ and $g(x)$.

Take $c \in F$ so that $\alpha_i + c\beta_1 \neq \alpha_k + c\beta_j$ as long as $j \neq 1$

(away from some finitely many choices of c)

Set $\theta := \alpha_1 + c\beta_1$

$F(\theta) \subseteq F(\alpha, \beta)$. Want to solve α, β over $F(\theta)$

The common zero of $f(\theta - cx)$ and $g(x)$ is when $\theta - c\beta_j = \alpha_i$

i.e. when $\alpha_1 + c\beta_1 = \alpha_i + c\beta_j$ only when $x = \beta_1$

i.e. in $F(\theta)[x]$, $(f(\theta - cx), g(x)) = (x-\beta_1)$

$\Rightarrow \beta_1 \in F(\theta)$ and hence $\alpha \in F(\theta)$ $\square$

Finite fields:

Theorem. (1) If F is a finite field, then $\mathrm{char}\, F = p > 0$ for a prime p and $\# F = p^n$ for $n = [F : \mathbb{F}_p]$

(2) For each p^n, there's a unique field F of p^n elements (up to isomorphisms)

It's the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$.

Proof: (1) is clear.

(2) If F is a finite field of p^n elements,

$F^\times$ is finite and a cyclic group of order $p^n - 1$

$\Rightarrow \forall a \in F^\times$, $a^{p^n-1} - 1 = 0$

So all elements in F are zeros of $x^{p^n} - x = 0$, and they are exactly the p^n zeros.

$\Rightarrow F$ is the splitting field of $x^{p^n} - x$

Conversely, if F is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$,

note: $D(x^{p^n} - x) = p^n \cdot x^{p^n-1} - 1 = -1$ in F $\Rightarrow (x^{p^n} - x, D(x^{p^n} - x)) = (1)$

So $x^{p^n} - x$ has only simple zeros in $F \Rightarrow$ it has p^n zeros.

Claim: These p^n zeros form a subfield of F (and thus must be equal to F)

$\forall \alpha, \beta \neq 0$ satisfies $\alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta$

$\Rightarrow \alpha + \beta, \alpha - \beta, \alpha\beta, \alpha/\beta$ are all zeros of $x^{p^n} - x$. $\square$

Lemma. (1) $\mathbb{F}_{p^m}$ can be viewed as a subfield of $\mathbb{F}_{p^n}$ iff $m \mid n$. (As a subset, $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ is unique) as $\mathbb{F}_{p^m}/\mathbb{F}_p$ is a splitting field.

(2) $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ for some α with $\deg m_{\alpha, \mathbb{F}_p}(x) = n$.

Proof: (1) $\mathbb{F}_{p^n}$ $\Rightarrow m \mid n$

$\mathbb{F}_{p^n} \supseteq \mathbb{F}_{p^m} \supseteq \mathbb{F}_p$, with $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ and $[\mathbb{F}_{p^m} : \mathbb{F}_p] = m$.

Conversely, if $m \mid n$, $\mathbb{F}_{p^m}$ is a splitting field of $x^{p^m} - x$

But $\mathbb{F}_{p^n}$ splits $x^{p^n} - x = (x^{p^m} - x) \cdot \dfrac{x^{p^n - 1} - 1}{x^{p^m - 1} - 1}$

$\Rightarrow \exists\ \mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$

(In fact, $\mathbb{F}_{p^m} = \{ a \in \mathbb{F}_{p^n} \mid a^{p^m} = a \}$.)

(2) Take any $\alpha \in \mathbb{F}_{p^n} \setminus \bigcup_{m \mid n,\, m \neq n} \mathbb{F}_{p^m}$

The number of such elements is: if $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$

$$p^n \left(1 - \frac{1}{p^{p_1}}\right) \cdots \left(1 - \frac{1}{p^{p_r}}\right) > 0$$

$\Rightarrow [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = n$. So $m_{\alpha, \mathbb{F}_p}(x)$ has degree n.