

02/22/2021

$E \ni \alpha \rightarrow \text{Irr}(x: \alpha/k) = f(x)$  monic, irred in  $k[x]$ ,  
 $f(x) \neq 0$ .

If  $\text{char}(k) = 0$ , then  $f(x)$  is separable; i.e.  $f(x)$  has no multiple root.

∴ If  $f(x)$  has a multiple root, may assume  $\alpha$  is a multiple root. i.e.  $(x-\alpha)^2 \mid f(x)$  in  $k^a[x]$

Have  $\frac{d}{dx}: k[x] \rightarrow k[x]$   $\hookrightarrow f'(x) := \frac{d}{dx}(f)$   $k^a$ : an alg-closure of  $k$   
 $x^i \mapsto ix^{i-1} \quad \forall i \in \mathbb{N}$   
End  $k$ -linear  $(k[x], k[x])$   $\Rightarrow \equiv 0 \pmod{(x-\alpha)}$  in  $k^a[x]$

$g \rightarrow g'$   
 $(g \cdot h)' = g'h + gh'$   $\forall g, h \in k[x]$  (Exer.)  $k[x](k[x]f(x) + k[x]f'(x)) \not\subseteq k[x]$   
a principal ideal

$$\Rightarrow \underline{k[x]f(x) + k[x]f'(x)} \not\subseteq k[x]$$

$\Rightarrow \underline{f'(x) = 0}!$  Note  $f'(x) \neq 0$  if  $\text{char}(k) = 0$ .  $k[x]g(x)$  and  $g(x) = 0$   
non-constant  $\Rightarrow f(x) = 0$   
 $f'(x) = 0$

Furthermore, Have shown: Assume  $p = \text{char}(k) > 0$ .

If  $f(x) \in k[x]$  nonconst irred. has a multiple root

then  $f'(x) = 0!$

$$f(x) = \sum_{i \text{ finite}} a_i x^i$$

$$f'(x) = 0 \Leftrightarrow ia_i = 0 \quad \forall i$$

$$\Rightarrow \text{if } a_i \neq 0, \text{ then } i \equiv 0 \pmod{p}$$

$$\Rightarrow \exists \underbrace{g(x) \in k[x]}_{\text{non-const irreducible}} \text{ s.t. } f(x) = g(x)^p$$

Repeat this argument.

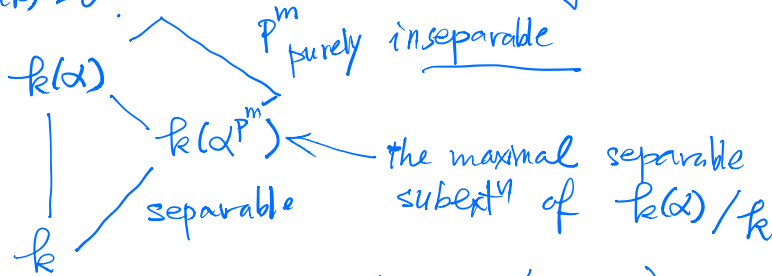
$\Rightarrow p = \text{char}(k) > 0$ ,  $f(x) \in k[x]$  nonconst. irred

then  $\exists m \in \mathbb{N}$  and  $g(x) \in k[x]$  nonconst irred separable

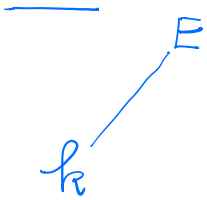
s.t.  $f(x) = g(x^{p^m})$

$\deg(f(x)) = p^m \cdot \deg(g(x))$

$p = \text{char}(k) > 0$



$\text{Irr}(x; \alpha / k(\alpha^{p^m})) = x^{p^m} - \alpha^{p^m}$



Q.1)  $\exists \alpha \in E$  s.t.  $E = k(\alpha)$ ?

2)  $\alpha, \beta \in E$

$\exists \gamma \in k(\alpha, \beta)$  s.t.  $k(\alpha, \beta) = k(\gamma)$ ?

Fact (Artin) 1) Given  $E/k$  finite ext<sup>n</sup>,  $\exists \alpha \in E$  s.t.  $E = k(\alpha)$

iff there exists only a finite number of subext<sup>n</sup>s of  $E/k$

— Fact: Please find a proof.

2) If  $\alpha, \beta \in E$ ,  $[E:k] < \infty$ ,  $\beta$  separable over  $k$  then  $\exists \gamma \in k(\alpha, \beta)$  s.t.  $k(\alpha, \beta) = k(\gamma)$

$\Rightarrow$  If  $\alpha, \beta_1, \dots, \beta_m \in E$ ,  $\beta_i$  separable over  $k$  then  $\exists \gamma \in k(\alpha, \beta_1, \dots, \beta_m) = k(\gamma)$

Proof of 2)  $E$   
 $k$  finite ext<sup>n</sup> of fields

Case 1  $k$  is finite. (Will see: the assertion is obvious)

Case 2  $k$  is infinite.  $\text{Irr}(x; \alpha/k) = f(x) = (x-\alpha) \cdots (x-\alpha_n)$

$\alpha \in E, E \supset \beta$  separable  $\text{Irr}(x; \beta/k) = g(x)$

Consider elements of the form  $(x-\beta_1) \cdots (x-\beta_m)$   $m = [E:k]$

$$\alpha_i + t \beta_j \quad t \in k$$

$\circ \circ$   $k$  is infinite  $\Rightarrow \exists t_1 \in k$  s.t.  $\alpha_i + t_1 \beta_j \neq \alpha_{i'} + t_1 \beta_{j'}$   
 $\circ \circ$   $\beta_i, \beta_{i'}$  are mutually distinct if  $(i, j) \neq (i', j')$ .

Let  $\gamma = \alpha + t_1 \beta$

Consider  $f(\gamma - t_1 x) =: h(x) \in k(\gamma)[x]$

Clearly:  $h(\beta) = 0$ .

and  $h(\beta_j) \neq 0$  for  $j=2, \dots, m$   
 by the choice of  $t_1$

Want:  $k(\gamma)[x]h(x) + k(\gamma)[x]g(x) = k(\gamma)[x] \cdot (x-\beta)$

The only common root is  $\beta$

$$E^a[x] \cdot \frac{\text{l.h.s}}{k(\gamma)[x]} = E^a[x] \cdot (x-\beta)$$

$\uparrow$  a poly. generated by  $\text{gcd}(h(x), g(x))$

$$\dim_{E^a} \left( \frac{E^a[X]}{E^a[X] \cdot (\text{l.h.s})} \right) = \dim_{k(\gamma)} \left( \frac{k(\gamma)[X]}{\text{l.h.s}} \right)$$

$\parallel$   $\parallel$   
 $\perp$   $\perp$

$$\Rightarrow \beta \in k(\gamma) \Rightarrow \alpha \in k(\gamma)$$

QED.

Basic about finite fields

$k$ : a finite field  $\rightsquigarrow \text{char}(k) = p > 0$

$$k \cong \mathbb{F}_p \quad [k : \mathbb{F}_p] = n \in \mathbb{N}_{\geq 1} \Rightarrow \text{card}(k) = p^n$$

$$\text{card}(k^\times) = p^n - 1$$

$$\Rightarrow \alpha^{p^n - 1} = 1 \quad \forall \alpha \in k^\times$$

$$\Rightarrow \alpha^{p^n} - \alpha = 0 \quad \forall \alpha \in k$$

$\Rightarrow k =$  a splitting field of  $x^{p^n} - x$

def  $\bar{k}$  (all roots of  $x^{p^n} - x$   
in an alg. closure of  $k$ )

$\Rightarrow k$  is separable over  $\mathbb{F}_p$

(o.g.  $\text{Irr}(\alpha/\mathbb{F}_p, X)$  divides  $\underbrace{x^{p^n} - x}_{\substack{\uparrow \\ \text{separable}}}$ )

The finite group  $k^\times$  is cyclic

$$\cong \mathbb{Z}/(p^n - 1)\mathbb{Z}$$

(o.g.  $\forall d \mid p^n - 1$ ,  
the polynomial  $x^d - 1$   
has at most  $d$  roots in  $k$ )

$\Rightarrow \forall$  finite ext<sup>m</sup> field  $F/k$   $[k: \mathbb{F}_p] = n$   
 $[F:k] = m$   
 $\Rightarrow [F: \mathbb{F}_p] = m \cdot n$

i.e.  $\text{Card}(E) = p^{mn}$

and  $F^{\times} \cong \mathbb{Z}/(p^{mn} - 1)\mathbb{Z}$

$\Rightarrow \exists \gamma \in F^{\times}$  s.t.  $F^{\times} = \langle \gamma \rangle$

$\Rightarrow k(\gamma) = F$   
trivially

Normal ext<sup>n</sup>



algebraic ext<sup>n</sup>

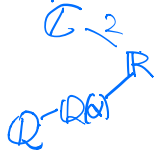
Def An algebraic ext<sup>n</sup> of fields  $E/k$  is normal

if  $\forall \alpha \in E \quad \forall \sigma \in \text{Hom}_{k, \text{ring}}(E, \overline{k})$

$\sigma(\alpha) \in E$

$\overline{k} = \text{an alg. closure of } k$

Example Let  $\alpha \in \mathbb{R}$  be a cubic root of 2 (or 3)



Is  $\mathbb{Q}(\alpha)/\mathbb{Q}$  normal?

NO!  $\beta = \alpha \cdot e^{2\pi i/3}$  is a root of  $x^3 - 2$

$\exists \sigma: \mathbb{Q}(\alpha) \rightarrow \mathbb{C}$   
 $\alpha \mapsto \beta = \alpha \cdot e^{2\pi i/3}$

Exer: A finite algebraic ext<sup>n</sup>  $E/k$  is normal

iff  $\exists$  a polynomial  $f(x) \in k[x]$

st.  $E/k =$  a splitting field of  $f(x)/k$

(if: "obvious".)

Def: An algebraic ext<sup>n</sup> of fields  $E/k$  is Galois if  $E/k$  is normal and separable.

Prop: Let  $E$  be a field

and  $G \leq \text{Aut}_{\text{ring}}(E)$  be a finite subgroup of field autom of  $E$

Then

$E$  is finite Galois over  $E^G = \{y \in E \mid \sigma(y) = y \forall \sigma \in G\}$

Given  $E$

1)  $G \rightsquigarrow E^G$

2)  $\begin{array}{c} E \\ \downarrow \\ F \end{array} \quad \begin{array}{c} E/F: \text{ finite} \\ \text{Galois} \end{array} \rightsquigarrow \text{Gal}(E/F) = \left\{ \sigma \in \text{Aut}_{\text{ring}, F} E \right\}$   
is a finite group of field automorphisms of  $E$