02/22/2021

$E \ni \alpha$ / k $\quad [E:k]<\infty$ $\leadsto \mathrm{Irr}(x;\alpha/k) = f(x)$ monic, irred in $k[x]$, $f(\alpha)=0$.

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

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

k^a: an alg. closure of k

Have $\frac{d}{dx}: k[x] \longrightarrow k[x]$, $x^i \longmapsto i x^{i-1}$ $\forall i \in \mathbb{N}$

$\frac{d}{dx} \in \mathrm{End}_{k\text{-linear}}(k[x], k[x])$

$\leadsto f'(x) := \frac{d}{dx}(f) \in k[x]$, $\equiv 0 \pmod{(x-\alpha)}$ in $k^a[x]$.

$g \mapsto g'$

$(g\cdot h)' = g'h + gh'$ $\forall g,h \in k[x]$ (Exer.)

$k^a[x](\underbrace{k[x]f(x) + k[x]f'(x)}_{\text{a principal ideal}}) \subsetneqq k^a[x]$

$\Rightarrow \underbrace{k[x]f(x) + k[x]f'(x)}_{= k[x]\,g(x)} \subsetneqq k[x]$

$g(x)$: non-constant and $g(\alpha)=0$ $\because f(\alpha)=0$, $f'(\alpha)=0$

$\Rightarrow \underline{f'(x)=0}$!

Note $f'(x) \neq 0$ if $\mathrm{char}(k)=0$.

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

If $f(x) \in k[x]$ noncont. irred. has a multiple root then $f'(x)=0$!

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

$f'(x)=0 \iff i a_i = 0 \quad \forall i$

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

$\Rightarrow \exists\, g(x) \in k[x]$ s.t. $f(x) = g(x^p)$

$g(x)$: non-const irreducible

Repeat this argument.

$\Longrightarrow$ $p = \mathrm{char}(k) > 0$, $f(x) \in k[x]$ noncont. irred

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

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

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

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

$$\begin{tikzcd}
k(\alpha) \arrow[dr, dash, "p^m \text{ purely inseparable}"] \arrow[dd, dash] & \\
& k(\alpha^{p^m}) \arrow[dl, dash, "\text{separable}"] \\
k &
\end{tikzcd}$$

the maximal separable subext^n of $k(\alpha)/k$

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

$$\begin{tikzcd}
& E \\
k \arrow[ur, dash] &
\end{tikzcd}$$

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^n, $\exists\, \alpha \in E$ s.t. $E = k(\alpha)$

iff there exists only a finite number of subext^{n}s

of E/k — Fact: Please find a proof.

2) If $\alpha, \beta \in E$, $[E:k] < \infty$, β separable over k

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

$\Longrightarrow$ If $\alpha, \beta_1, \dots, \beta_m \in E$, β_i separable over k $\forall i$

then $\exists\, \gamma \in k(\alpha, \beta_1 \cdots \beta_m) = k(\gamma)$

Proof of 2) $\quad \begin{array}{c} E \\ | \\ k \end{array}$ finite ext^n of fields

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

Case 2 $\quad k$ is infinite. $\quad Irr(x; \alpha/k) = f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$

$\alpha \in E$, $E \ni \beta$ separable $\quad Irr(x; \beta/k) = g(x)$

$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \| $

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

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

$\because$ k is infinite $\underset{\substack{\because\ \beta_1, \dots, \beta_m \\ \text{are mutually} \\ \text{distinct}}}{\Longrightarrow}$ $\exists\, t_1 \in k$ s.t. $\alpha_i + t_1\beta_j$

$\neq \alpha_{i'} + t_1 \beta_{j'}$

if $(i,j) \neq (i',j')$.

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

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

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

and $\quad h(\beta_j) \neq 0$ for $j = 2, \dots, m$

by the choice of t_1

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

The only common root is β

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

a poly. generated by $\gcd(h(x), g(x))$

$$\dim_{E^a}\Bigg(\underbrace{E^a[X] \big/ E^a[X]\cdot(\text{l.h.s})}_{=1}\Bigg) = \dim_{k(\gamma)}\Bigg(\underbrace{k(\gamma)[X] \big/ \text{l.h.s}}_{=1}\Bigg)$$

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

QED.

Basic about finite fields

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

$k \supseteq \mathbb{F}_p \qquad [k : \mathbb{F}_p] = n \in \mathbb{N}_{\geq 1} \Rightarrow \mathrm{Card}(k) = p^n$

$\mathrm{Card}(k^\times) = p^n - 1$

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

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

$\Longrightarrow \quad k = $ a splitting field of $X^{p^n} - X$

$\overset{\text{def}}{=} k(\text{all roots of } X^{p^n}-X \text{ in an alg. closure of } k)$

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

$\left(\because \mathrm{Irr}(\alpha/\mathbb{F}_p, X) \text{ divides } \underbrace{X^{p^n}-X}_{\text{separable}}\right)$

The finite group $k^\times$ is cyclic $\left(\because \forall d \mid p^n-1, \text{ the polynomial } X^d - 1 \text{ has at most } d \text{ roots in } k\right)$

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

$\Longrightarrow$ $\forall$ finite ext^n field $/k$ $\quad [k : \mathbb{F}_p] = n$

$$\begin{array}{c} F \\ | \\ k \end{array} \qquad [F : k] = m$$

$$\Rightarrow [F : \mathbb{F}_p] = m \cdot n$$

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

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

$\Longrightarrow \exists\, \gamma \in F^\times$ s.t. $F^\times = \gamma^{\mathbb{Z}}$

$\underset{\text{trivially}}{\Rightarrow} \quad k(\gamma) = F$

Normal ext^n:

$$\begin{array}{c} E \\ | \\ k \end{array} \text{ algebraic ext}^n.$$

Def^n An algebraic ext^n of fields E/k is normal if $\forall \underset{E}{\alpha}$ $\forall \sigma \in \mathrm{Hom}_{k,\text{ring}}(E, k^a)$

$\sigma(\alpha) \in E$

k^a = an alg. closure of k

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

$$\begin{array}{c} \mathbb{C} \\ |\,2 \\ \mathbb{R} \\ | \\ \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q} \end{array}$$

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

NO! $\beta = \alpha \cdot e^{2\pi\sqrt{-1}/3}$ is a root of $x^3 - 2$

$$\exists\, \sigma : \mathbb{Q}(\alpha) \longrightarrow \mathbb{C}$$
$$\alpha \longmapsto \beta = \alpha \cdot e^{2\pi\sqrt{-1}/3}$$

Exer: A finite algebraic ext^n E/k is normal iff $\exists$ a polynomial $f(x) \in k[x]$ s.t. E/k = a splitting field of $f(x)/k$.

(if: "obvious".)

Def: An algebraic ext^n of fields E/k is Galois if E/k is normal and separable.

Prop. Let E be a field and $G \leq \mathrm{Aut}_{ring}(E)$ 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) E E/F: finite Galois $\rightsquigarrow$ $\mathrm{Gal}(E/F) = \{ \sigma \in \mathrm{Aut}_{ring, F} E \}$
$|$
F

is a finite group of field automorphisms of E