Prop: Seja $f \in k[X]$ tq. $\deg f > 0$ e f é irred. ASASE:

(a) f tem raiz múltipla;

(b) $\text{mdc}(f, f') \neq 1$

(c) $\text{char}(k) = p > 0$ e $\exists g \in k[X]$:

$$f(X) = g(X^p)$$

(d) todas as raízes de f são múltiplas.

Dem: (a) $\Rightarrow$ (b) $f = (X-\alpha)^2 q(X)$

em E/k $\Rightarrow$

$$f' = 2(X-\alpha)q(X) + (X-\alpha)^2 q'(X)$$

(b) $\Rightarrow$ (c) $\quad \gcd(f, f') \neq 1$

$\Rightarrow \quad f' = 0$

$\deg f' < \deg f$

$$f = \sum_i a_i X^i \quad \Rightarrow \quad f' = \sum_i i a_i X^{i-1}$$

$$\Rightarrow \begin{cases} \operatorname{char} k = p > 0 \\ f(X) = g(X^p) \end{cases}$$

(c) $\Rightarrow$ (d) nume ext. de decomp. de g:

$$g(X) = \prod_i (X - \alpha_i)$$

$$\Rightarrow g(X^p) = \prod_i (X^p - \alpha_i)$$

$\Rightarrow$ nume ext. de decomp. de f

$$f = g(x^p) = \prod_i (x^p - c_i^p)$$

$$= \prod_i (x - c_i)^p$$

□

Def: $f \in u[X]$ diz-se <u>separável</u> se nenhum dos seus <u>factores irredutíveis</u> tem <u>raízes múltiplas</u>.

<u>Exemplo</u>: $f = (X-1)^2(X+1)$ é separável.

<u>NB</u>: f não separável $\Rightarrow$ $\operatorname{char} u = p > 0$ e um dos factores irred. de f é pol. em X^p.

Def: Um corpo K diz-se perfeito se $\forall f \in K[X]$ f é separável.

Exemplos: 1. $\mathrm{char}(K) = 0 \implies$ K perfeito

2. $K = \mathbb{F}_p(T)$ não é perfeito.

Prop: Seja K corpo

(a) $\mathrm{char}\, K = 0 \Rightarrow K$ é perfeito

(b) se $\mathrm{char}\, K = p > 0$, então K é perfeito sse $K = K^p$ ($\forall \alpha \in K$ $\exists a \in K : a^p = \alpha$).

Dem (b) se K é perfeito então $X^p - a$ é separável. Temos

$$(X^p - a) = (X - a)^p$$

salvo extensão $\therefore a \in K \therefore K = K^p$

Reciprocamente: exercício.

□

NB: Se $\operatorname{char} K = p > 0$ e K é perfeito, então $\varphi : K \to K ; a \mapsto a^p$ é um automorfismo. Chama-se automorfismo de Frobenius.

Exemplo: se $\operatorname{char} K = p$ e K é finito então K é perfeito.

Automorfismos de Extensões de Decomposição de polinômios separáveis

Prop: Se E/k é uma extensão de decomposição de um polinômio separável $f \in k[X]$, então

$$|Aut_k(E)| = [E:k]$$

Dem: Seja $f = \prod f_i^{m_i}$ com f_i irred. separáveis. Logo E/k é extensão de $g = \prod_i f_i$. Como os f_i's são separáveis g tem $\deg g$ raízes distintas. Daqui segue

$$|\mathrm{Aut}_k(E)| = |\mathrm{Hom}_k(E|_k, E|_k)|$$

$$= [E:k] .$$

□

Example: $f = \frac{X^3-1}{X-1} = X^2+X+1$

$\in \mathbb{Q}[X]$, $\zeta \in e^{2\pi i/3} \in \mathbb{C}$

$$\Rightarrow |\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta))| = [\mathbb{Q}(\zeta):\mathbb{Q}]$$

$$= 2$$

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta)) = \{1_{\mathbb{Q}(\zeta)}, \sigma\}$$

$\sigma : z \mapsto \bar{z}$.

Subcorpos Fixados por Automorfismos

Def: E um corpo e $G < \mathrm{Aut}(E)$.

Define-se

$$E^G := \{ \alpha \in E \mid \forall_{\sigma \in G} \ \sigma(\alpha) = \alpha \}.$$

Então E^G é um subcorpo de E, denominado dos elementos G-invariantes.

Obtemos corresp.

$$\left\{ \begin{array}{c} \text{subgrupos de} \\ \mathrm{Aut}\, E \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{subcorpos de} \\ E \end{array} \right\}$$

$$G \longmapsto E^G$$

Em sentido inverso, temos tb correspondência

$$\{F \subset E \text{ subcorpos}\} \longrightarrow \{\text{subgrupos de } \mathrm{Aut}(E)\}$$

$$F \longmapsto \mathrm{Aut}(E/F)$$

NB: $H < H' \Rightarrow E^H \supset E^{H'}$

$F \subset F' \Rightarrow \mathrm{Aut}(E/F) \supset \mathrm{Aut}(E/F')$

Prop (E. Artin): Seja E um corpo e seja $G < \mathrm{Aut}\, E$ um subgrupo finito e seja $k = E^G$. Então

$$[E : k] \leq |G|.$$

Dem: Seja $G = \{\sigma_1, \ldots, \sigma_r\}$.

Sejam $\alpha_1, \ldots, \alpha_s \in E$ com $s > r$.

Objetivo: Mostrar que $\{\alpha_1, \ldots, \alpha_s\}$ é L.D. $/k$.

Consideremos o sistema

$$(*) \begin{cases} \sigma_1(\alpha_1) X_1 + \cdots + \sigma_1(\alpha_s) X_s = 0 \\ \vdots \\ \sigma_r(\alpha_1) X_1 + \cdots + \sigma_r(\alpha_s) X_s = 0 \end{cases} \quad \begin{matrix} r \text{ eqs.} \\ s \text{ var.} \end{matrix}$$

e seja $(c_1, \dots, c_s)$ um sol. não trivial com um # máximo de zeros. Podemos supor $c_1 \neq 0$ e $c_1 \in K$. Se $c_i \notin K$, então $\exists j : \sigma_j(c_i) \neq c_i$.

Aplicando σ_j ao sistema (*), obtemos

$$\begin{cases} \sigma_j(\sigma_1(a_1))\sigma_j(c_1) + \dots + \sigma_j(\sigma_1(a_s))\sigma_j(c_s) = 0 \\ \vdots \\ \sigma_j(\sigma_r(a_1))\sigma_j(c_1) + \dots \sigma_j(\sigma_r(a_s))\sigma_j(c_s) = 0 \end{cases} \quad (**)$$

mas $(\sigma_j \circ \sigma_1, \dots, \sigma_j \circ \sigma_r)$ é permutação de $(\sigma_1, \dots, \sigma_r)$

$\therefore (c_1, \sigma_j(c_2), \dots, \sigma_j(c_s))$ é solução de (**)

$\therefore \quad (0, c_2 - \sigma_j(c_2), \dots, c_i - \sigma_j(c_i), \dots)$

é uma solução não trivial de $(*)$ com mais zeros do que $(c_1, \dots, c_s)$ $\lightning$

$\therefore \quad c_i \in K$

$\therefore \{\alpha_1, \dots, \alpha_s\}$ é L.D. $/K$. $\square$

Cor: Seja $G \leq Aut(E)$ finito, então

$$G = Aut(E/E^G).$$

Dem: Temos

1. $[E : E^G] \leq |G|$ (E. Artin)
2. $G \leq Aut(E/E^G)$

3. $|\mathrm{Aut}(E/E^G)| \le [E:E^G]$

$\therefore [E:E^G] = |G| = |\mathrm{Aut}(E/E^G)|.$

□

Def: Uma extensão algébrica E/κ diz-se <u>separável</u> se $\forall \alpha \in E$ o pol. mínimo de α / κ é separável. Caso contrário, diz-se <u>não separável</u>.

Exemplo: Se κ é perfeito e E/κ é algébrica então E/κ é separável.

Se E/κ não é separável, então
- $\text{char}\,\kappa = p > 0$
- $\exists \alpha \in E$ com pol. min. de forma $g(x^p)$.

Exemplo: $\mathbb{F}_p(T) / \mathbb{F}_p(T^p)$ é

ext. alg. não separável.

Def: Uma extensão algébrica E/k diz-se normal se $\forall \alpha \in E$ o pol min. se α se decompõe em E.

Exemplo: $\mathbb{C}/\mathbb{R}$ é normal.

Exemplo: $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ não é normal.

NB: Seja E/k alg. e $f \in k[x]$ tq. f é irred., $\deg f = n$ e f tem raiz em E. Então

- E/k separável $\Rightarrow$ f não tem raízes mult.
- E/k normal $\Rightarrow$ f decompõe-se em E
- E/k separável + normal $\Rightarrow$ f tem exatamente n raízes em E.

Cor: Se E/k é normal e separável, então $\forall \alpha \in E$

$$[k[\alpha]:k] = \#\text{raízes (distintas) do pol. mínimo de } \alpha/k.$$

Exemplo: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ é separável mas não é normal. $f = X^3 - 2$ não se decompõe em $\mathbb{Q}(\sqrt[3]{2})$.

Def: Uma extensão finita E/k diz-se de Galois se

$$E^{\mathrm{Aut}(E/k)} = k.$$

Diz-se que $\mathrm{Gal}(E/k) := \mathrm{Aut}(E/k)$ é o grupo de Galois da extensão E/k.

Teorema: Seja E/k extensão. ASASE:

(a) E é corpo de decomp. de $f \in k[X]$ separável.

(b) $\exists G < \mathrm{Aut}(E/k)$ t.q. $|G| < \infty$ e $k = E^G$.

(c) E/k é normal, separável e finita.

(d) E/k é Galois.

Dem: (a) $\Rightarrow$ (b), (c). Seja $G = \mathrm{Aut}(E/k)$.

exerc.

Temos: E é tb o corp. de decomp.

de $f \in E^G[X]$, logo

$$[E : E^G] = |\mathrm{Aut}(E|E^G)|$$

$$[E : k] = |\mathrm{Aut}(E|k)|$$

Como $\mathrm{Aut}(E|E^G) = \mathrm{Aut}(E|k)$

$= G$. $\therefore$ $E^G = k$.

(d) $\Rightarrow$ (b) $|\mathrm{Aut}(E|k)| \leq [E:k]$

e $k = E^{\mathrm{Aut}(E/k)}$.

(b) $\Rightarrow$ (c) Pela prop. E. Artin

$$[E : E^G] \leq |G|$$

$\therefore$ E/κ finita

Seja $f \in \kappa[X]$ irred. tq.
f tem raiz $\mu \in E$. Sejam $\mu_1, \dots, \mu_n$
a órbita de μ por G. Seja

$$g := (X - \mu_1) \cdots (X - \mu_n).$$

Temos $g \mid f$ e $g \in \kappa[X]$

pois $f(\mu_i) = 0 \ \forall i$ e $\sigma \cdot g = g \ \forall \sigma \in G$

$\therefore$ $g = f$ e f decompõe-se em
E e não raízes múltiplas.

(c) $\Rightarrow$ (G) exercício

□

NB: Da demonstração, vem

E/k Galois e $\mu \in E \Longrightarrow$

μ tem pol. mínimo

$$f = \prod_{i=1}^{n} (X - \mu_i)$$

onde $\{\mu_1, \dots, \mu_n\}$ é a órbita de μ por $G = Gal(E/k)$.

Notação: Os μ_i's dizem-se conjugados de μ.

Cor: E/k é Galois e $k \subset F \subset E$

é corpo intermédio, então E/F é Galois.

Teorema Fundamental da Teoria de Galois:

Seja E/k uma extensão de Galois e $G = Gal(E/k)$. Então as aplicações $H \longmapsto E^H$ e $F \mapsto Gal(E/F)$ são bijeções inversas

$$\{\text{subgrupos } H < G\} \hookrightarrow \{\text{corpos intermédios } k \subset F \subset E\}$$

Além disso, temos

(a) $H_1 > H_2 \iff E^{H_1} \subset E^{H_2}$

(b) $(H_1 : H_2) = [E^{H_2} : E^{H_1}]$

(c) $E^{\sigma H \sigma^{-1}} = \sigma(E^H)$; $Gal(E/\sigma E^H) = \sigma\, Gal(E/F)\sigma^{-1}$

(d) $H \lhd G \iff E^H/k$ é normal (logo Galois).

e tem-se $\boxed{Gal(E^H/k) = G/H}$

Dem: 1ª asserção:

$H < G \Rightarrow E/E^H$ Galois

$H < Aut(E/k)$ finito $\Rightarrow$

$H = Aut(E/E^H) =: Gal(E/E^H)$

Seja $k \subset F \subset E$. Então E/F é Galois

$\Rightarrow F = E^{Aut(E/F)}$

(b) temos

$[E : E^{H_i}] = |H_i|$

logo $H_2 \subset H_1 \Rightarrow$

$$|H_1| = [E : E^{H_1}] = [E : E^{H_2}][E^{H_2} : E^{H_1}]$$

$$= |H_2|\,[E^{H_2} : E^{H_1}]$$

$$\Rightarrow [E^{H_2} : E^{H_1}] = |H_1| / |H_2|$$

$$= (H_1 : H_2)$$

(c) $\alpha \in E^{\sigma H \sigma^{-1}} \iff \forall_{h \in H}\ \sigma h \sigma^{-1}(\alpha) = \alpha$

$$\iff \forall_{h \in H}\ h(\sigma\alpha) = \sigma^{-1}\alpha$$

$$\iff \sigma^{-1}\alpha \in E^H$$

$$\iff \alpha \in \sigma(E^H)$$

(d) $H \lhd G \iff \sigma H \sigma^{-1} = H \quad \forall_{\sigma \in G}$

$$\iff \sigma(E^H) = E^H \quad \forall_{\sigma \in G}$$

$$\iff E^H / \kappa \text{ é normal pq } \circ$$

pol. mínimo de $\alpha \in E$ tem raízes

$$\sigma(\alpha), \ \sigma \in G.$$

Falta provar $\mathrm{Gal}(E^H/K) = G/H$.

□

Def: Seja $f \in K[X]$ separável e seja E_f/K uma ext. decomp. Então E_f/K é de Galois.

Diz-se que $\mathrm{Gal}(E_f/K)$ é o grupo de Galois de f.

Exercício: Calcular o grupo de Galois de $x^4 - 2 \in \mathbb{Q}[x]$.

Sugestão: $f = x^4 - 2$ é irredutível.