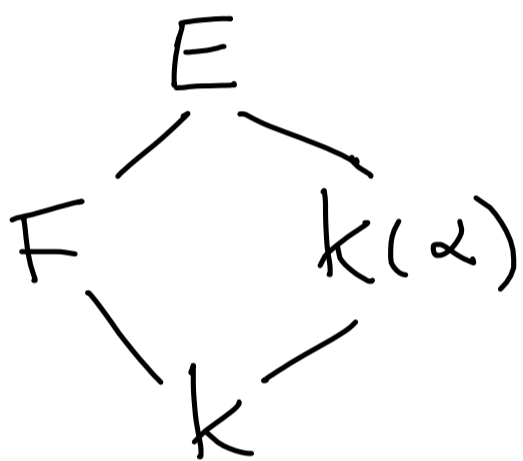


Ej. Sea K cuerpo, $f \in K[x]$ irreducible, E es cdd sobre K , y sea $K \subseteq F \subseteq E$, con F un cuerpo, tal que F/K es normal. Supongamos que $f = f_1 \cdot f_2$, con $f_1, f_2 \in F[x]$ irreducibles. Probar que $g_r(f_1) = g_r(f_2)$ con $g_r(f_1), g_r(f_2) \geq 1$.

E
 $|$
 F
 $|$
 K

Sean α y β raíces de f_1 y f_2 respectivamente ($\alpha, \beta \in E$)



Sea $\sigma: K(\alpha) \xrightarrow{K} K(\beta)$

$\alpha \mapsto \beta$

Tenemos que σ se

extiende a $\bar{\sigma}: E \xrightarrow{K} E$ y podemos tomar

$\bar{\sigma}|_F: F \xrightarrow{K} F$, pues F/K es normal

Ahora.
$$\bar{\sigma}_F(f_1)(\beta) = \bar{\sigma}_F(f_1)(\sigma(\alpha)) = \bar{\sigma}_F(f_1(\alpha)) = \bar{\sigma}_F(0) = 0$$

O sea, $\bar{\sigma}_F(f_1) \in F[x]$ fue anula a β .

Luego: $f_2 \mid \bar{\sigma}_F(f_1)$, pues $f_2 = m_{\beta, F}$

En particular $g_r(f_2) \leq g_r(\bar{\sigma}_F(f_1)) = g_r(f_1)$

y listo, por simetría

Prop 1) E/k separable y finita, entonces:

a) $[E:k] = \cancel{\text{Hom}}(E/k, \bar{k})$

b) $\alpha \in E \Rightarrow m_{\alpha, k} = \prod_{\sigma: k[\alpha] \rightarrow \bar{k}} (x - \sigma(\alpha))$

$= \prod_{\sigma: E \rightarrow \bar{k}} (x - \sigma(\alpha))$
 (entre los σ 's que dan distinto)

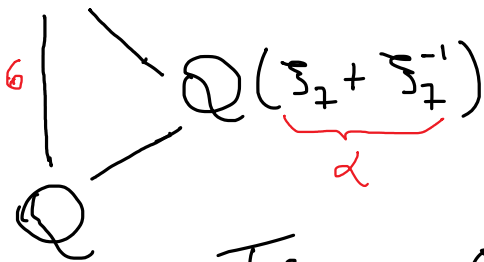
$[E:k(\alpha)]$

c) $(m_{\alpha, k}) = \prod_{\sigma: E \rightarrow \bar{k}} (x - \sigma(\alpha))$

ej.

$\mathbb{Q}(\zeta_7) = E$

$\text{Hom}(E/\mathbb{Q}, \bar{\mathbb{Q}}) = \{\sigma_1, \dots, \sigma_6\}$,



con $\sigma_i: \zeta_7 \mapsto \zeta_7^i$

Tenemos

$\sigma_1(\alpha) = \alpha$
 $\sigma_2(\alpha) = \zeta_7^2 + \zeta_7^{-2}$
 $\sigma_3(\alpha) = \zeta_7^3 + \zeta_7^{-3}$
 $\sigma_4(\alpha) = \zeta_7^4 + \zeta_7^{-4}$
 $\sigma_5(\alpha) = \zeta_7^5 + \zeta_7^{-5}$
 $\sigma_6(\alpha) = \zeta_7^6 + \zeta_7^{-6}$

Luego

$m_{\alpha, \mathbb{Q}} = (x - (\zeta_7 + \zeta_7^{-1})) (x - (\zeta_7^2 + \zeta_7^{-2})) \times$
 $(x - (\zeta_7^3 + \zeta_7^{-3}))$

$$= x^3 - (-1)x^2 + (\dots)x + (\dots)$$

Ej: calcular $M_{\beta, \mathbb{Q}}$, con $\beta = \sqrt[3]{2} + \sqrt[3]{2}^2 + \sqrt[3]{2}^4$

Obs: Sea E/k separable y finita, con $\text{Hom}(E/k, \bar{k}/k) = \{\sigma_1, \dots, \sigma_n\}$. Si $\alpha \in E$ es tal que $\sigma_i(\alpha) \neq \sigma_j(\alpha) \forall i \neq j$, entonces:

$$E = k(\alpha).$$

Ej: $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) = \mathbb{Q}(\sqrt[3]{2} + \sqrt{3})$

$\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) = \mathbb{Q}(d_1\sqrt{p_1} + \dots + d_n\sqrt{p_n})$
con $d_i \neq 0, \forall i$

Recordo^(*) k cuerpo, $a \in k - k^p$, con p primo, entonces $x^p - a \in k[x]$ es irreducible.

Más general: k cuerpo con $\text{car}(k) = p \neq 2$, primo. Dado $f \in k[x]$ mónico e irreducible, tq $f(0) \in k - k^p$, entonces $f(x^p) \in k[x]$ es irreducible.

Dem: Supongamos que $f = (x - \alpha_1) \dots (x - \alpha_n)$, con $\alpha_i \in E$, siendo E su cdd sobre k .

Tendríamos $f(x^p) = (x^p - \alpha_1) \dots (x^p - \alpha_n)$

Veamos que $x^p - \alpha_1 \in k(\alpha_1)[x]$ es irreducible.

Si no lo fuera, por el $q(*)$, $\alpha_1 \in k(\alpha_1)^p$, digamos

$$\alpha_1 = \beta_1^p, \text{ con } \beta_1 \in k(\alpha_1).$$

Ahora. $f(x) = \pm \alpha_1 \cdots \alpha_n = \pm \prod_{\sigma: k(\alpha_1) \rightarrow \bar{k}} \sigma(\alpha_1)$

$$= \pm \prod_{\sigma: k(\alpha_1) \rightarrow \bar{k}} \sigma(\beta_1^p) = \pm \left(\prod_{\sigma: k(\alpha_1) \rightarrow \bar{k}} \sigma(\beta_1) \right)^p =$$

$$\beta_1 \in k(\alpha_1) \quad \in K \quad (p \neq 2)$$

$$= \pm \left(\prod_{\sigma: k(\beta_1) \rightarrow \bar{k}} \sigma(\beta_1) \right)^p = \pm \left(\pm m_{\beta_1, k}(\alpha) \right)^p \quad \underline{\underline{Abs}}$$

Pues. $k(\alpha_1) = k(\beta_1)$ ($\alpha_1 = \beta_1^p$ y $\beta_1 \in k(\alpha_1)$)

Supongamos entonces que $f(x^p) = g \cdot h$, con $g, h \in k[x]$. Pero $x^p - \alpha_1 \mid f(x^p)$ en $k(\alpha_1)[x]$, y como es irreducible

$$x^p - \alpha_1 \mid g \quad \text{o} \quad x^p - \alpha_1 \mid h$$

$$\Rightarrow \frac{f(x^p)}{(x^p - \alpha_1)} = \frac{g \cdot h}{x^p - \alpha_1} = \tilde{g} \cdot \tilde{h} \text{ en } k(\alpha_1)[x]$$

Del mismo modo. $x^p - \alpha_1 \mid \frac{f(x^p)}{(x^p - \alpha_1)} = \tilde{g} \cdot \tilde{h}$,

y lo mismo en $k[\alpha_1][\alpha_2][x]$; Pero $x^p - \alpha_2$ es irreducible en $k(\alpha_1)(\alpha_2)[x]$ (pues se demuestra idéntico). Luego.

$$\frac{f(x^p)}{(x^p - \alpha_1)(x^p - \alpha_2)} = \tilde{g} \cdot \tilde{h}. \text{ Repetiendo esto.}$$

$$g = \prod_{i \in G} (x^p - \alpha_i) \quad \text{y} \quad h = \prod_{i \in H} (x^p - \alpha_i),$$

con $\{G, H\}$ una partición de $\{1, \dots, m\}$

Pero entonces esto daría una factorización de f , contradictoriamente. $f = f_1 \cdot f_2$, con

$$f_1 = \prod_{i \in G} (x - \alpha_i) \quad \text{y} \quad f_2 = \prod_{i \in H} (x - \alpha_i). \quad \underline{\underline{\text{Abs}}}$$

□

Ej. $x^3 - 3x - 3 \in \mathbb{Q}[x]$ irred
 $p = 7 \Rightarrow x^{21} - 3x^7 - 3$ es irred
 $(3 \notin \mathbb{Q}^7)$.

Def. Dado k , con $\text{car}(k) = p$,

$$K^{p^{-\infty}} := \{x \in \bar{k} \cdot \sigma(x) = x, \forall \sigma \in \text{Gal}(\bar{k}/k)\}$$

Prop. $K^{p^{-\infty}} = \{x \in \bar{K} : \exists n \text{ tq } x^{p^n} \in K\}$

Dem \supseteq) $\alpha^{p^m} \in K$, y sea $\sigma \in \text{Gal}(\bar{K}/K)$,

entonces; bvp α es la única raíz de $m_{\alpha, K}$. Pero: $m_{\alpha, K} \mid X^{p^m} - \alpha^{p^m} = (X - \alpha)^{p^m}$ ▣

\subseteq) Después