Ej. Sea K cuerpo, $f \in K[x]$ irreducible, E su 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 $gr(f_1) = gr(f_2)$ con $gr(f_1), gr(f_2) \geq 1$.

$$\begin{array}{c} E \\ | \\ F \\ | \\ K \end{array}$$

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

$$\begin{tikzcd} & E \arrow[dl, dash] \arrow[dr, dash] & \\ F \arrow[dr, dash] & & K(\alpha) \arrow[dl, dash] \\ & K & \end{tikzcd}$$

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

$\alpha \longmapsto \beta$

Tenemos que σ se extiende a $\overline{\sigma} : E \xrightarrow[K]{} E$ y puedo tomar $\overline{\sigma}|_F : F \xrightarrow[K]{} F$, pues F/K es normal

Ahora: $\overline{\sigma}|_F(f_1)(\beta) = \overline{\sigma}|_F(f_1)(\sigma(\alpha)) = \overline{\sigma}|_F(f_1(\alpha))$
$= \overline{\sigma}|_F(0) = 0$

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

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

En particular $gr(f_2) \leq gr(\overline{\sigma}|_F(f_1)) = gr(f_1)$

y listo, por simetría ∎

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

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

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

$$= \prod_{\sigma : E \to_k \bar{k}} (x - \sigma(\alpha))$$

(sobre los σ's que dan distinto)

c) $(m_{\alpha,k})^{[E:k(\alpha)]} = \prod_{\sigma : E \to_k \bar{k}} (x - \sigma(\alpha))$

Ej.

$$\begin{tikzcd}
\mathbb{Q}(\zeta_7) = E \arrow[dd, dash, "6"'] \arrow[dr, dash] & \\
& \mathbb{Q}(\underbrace{\zeta_7 + \zeta_7^{-1}}_{\alpha}) \arrow[dl, dash] \\
\mathbb{Q} &
\end{tikzcd}$$

$\operatorname{Hom}(E/\mathbb{Q}, \bar{\mathbb{Q}}/\mathbb{Q}) = \{\sigma_1, \dots, \sigma_6\}$, 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
$$m_{\alpha,\mathbb{Q}} = \left(x - (\zeta_7 + \zeta_7^{-1})\right)\left(x - (\zeta_7^2 + \zeta_7^{-2})\right) \times$$
$$\left(x - (\zeta_7^3 + \zeta_7^{-3})\right)$$

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

Ej: Calcular $m_{\beta,\mathbb{Q}}$, con $\beta = \xi_7 + \xi_7^2 + \xi_7^4$

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

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

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

• $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) = \mathbb{Q}(\lambda_1\sqrt{p_1} + \dots + \lambda_n\sqrt{p_n})$, con $\lambda_i \neq 0$, $\forall i$

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

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

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

Tenemos $f(x^p) = (x^p - \alpha_1) \cdots (x^p - \alpha_n)$

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

Si no lo fuera, por el ej (*), $\alpha_1 \in k(\alpha_1)^p$, digamos $\alpha_1 = \beta_1^p$, con $\beta_1 \in k(\alpha_1)$.

Ahora: $f(0) = \pm \alpha_1 \cdot \cdot \cdot \alpha_n = \pm \prod_{\sigma : k[\alpha_1] \xrightarrow{k} \overline{k}} \sigma(\alpha_1)$

$$= \pm \prod_{\sigma : k[\alpha_1] \xrightarrow{k} \overline{k}} \sigma(\beta_1^p) = \pm \left(\prod_{\sigma : k[\alpha_1] \xrightarrow{k} \overline{k}} \sigma(\beta_1) \right)^p =$$

$\beta_1 \in k(\alpha_1)$

$$= \pm \left(\prod_{\sigma : k[\beta_1] \xrightarrow{k} \overline{k}} \sigma(\beta_1) \right)^p = \pm \Big(\underbrace{\pm m_{\beta_1, k}(0)}_{\in K \ (p \neq 2)} \Big)^p \quad \text{Abs}$$

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

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

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

Del mismo modo: $x^p - \alpha_2 \mid \dfrac{f(x^p)}{(x^p - \alpha_1)} = \tilde{g} \cdot \tilde{h}$, 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

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

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

con $\{G, H\}$ una partición de $\{1, \ldots, n\}$

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

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

$\boxed{\equiv}$

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, car$(K) = p$,

$$K^{p^{-\infty}} := \{x \in \overline{K} : \sigma(x) = x, \ \forall \sigma \in \mathrm{Gal}(\overline{K}/K)\}$$

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

Dem $\supseteq$) $\alpha^{p^n} \in K$, y sea $\sigma \in Gal(\overline{K}/K)$,

entonces; bvf α es la única raíz de

$m_{\alpha,K}$. Pero: $m_{\alpha,K} \mid X^{p^n} - \alpha^{p^n} = (X-\alpha)^{p^n}$

$\blacksquare$

$\subseteq$) Después