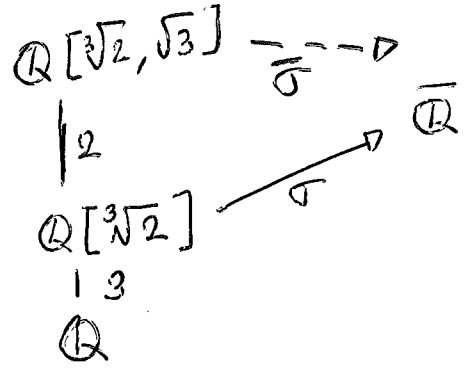
INMERSIONES y extensiones



σ: $\sqrt[3]{2} \mapsto \sqrt[3]{2}$ ①
ó $\sqrt[3]{2} \mapsto \sqrt[3]{2}\,\zeta_3$ ②
ó $\sqrt[3]{2} \mapsto \sqrt[3]{2}\,\zeta_3^2$ ③

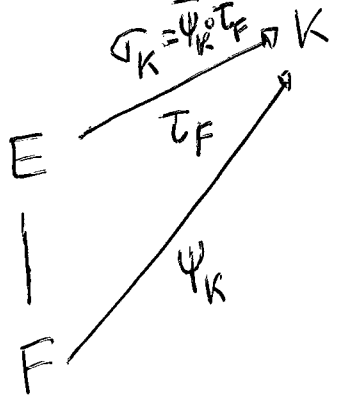
$\bar{\sigma}$: $\begcases \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \sqrt{3} \mapsto \sqrt{3} \endcases$ ó $\begcases \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \sqrt{3} \mapsto -\sqrt{3} \endcases$ ①

$\begcases \sqrt[3]{2} \mapsto \sqrt[3]{2}\,\zeta_3 \\ \sqrt{3} \mapsto \sqrt{3} \endcases$ ó $\begcases \sqrt[3]{2} \mapsto \sqrt[3]{2}\,\zeta_3 \\ \sqrt{3} \mapsto -\sqrt{3} \endcases$ ②

$\begcases \sqrt[3]{2} \mapsto \sqrt[3]{2}\,\zeta_3^2 \\ \sqrt{3} \mapsto \sqrt{3} \endcases$ ó $\begcases \sqrt[3]{2} \mapsto \sqrt[3]{2}\,\zeta_3^2 \\ \sqrt{3} \mapsto -\sqrt{3} \endcases$ ③

TEOREMA Sea $E/F/K$ algebraica.

Entonces hay una biyección entre $\mathrm{Hom}(E/K, \bar{K}/K)$ y $\mathrm{Hom}(F/K, \bar{K}/K) \times \mathrm{Hom}(E/F, \bar{K}/F)$



En particular si E/K es finita, entonces

$$\#\,\mathrm{Hom}(E/K, \bar{K}/K) = \#\,\mathrm{Hom}(F/K, \bar{K}/K) \cdot \#\,\mathrm{Hom}(E/F, \bar{K}/F)$$

La biyección está dada por:

$$\phi : \mathrm{Hom}(F/K, \bar{K}/K) \times \mathrm{Hom}(E/F, \bar{K}/F) \to \mathrm{Hom}(E/K, \bar{K}/K)$$
$$(\psi_K, \tau_F) \mapsto \sigma_K = \bar{\psi}_K \circ \tau_F$$

donde $\bar{\psi}_K \in \mathrm{Hom}(\bar{K}/K, \bar{K}/K) = \mathrm{Gal}(\bar{K}/K)$ es cualquier extensión fijada de $\psi_K : F \to \bar{K}$

Demostración

Dada $\psi_K : F \xrightarrow[K]{} \bar{K}$, sea $\bar{\psi}_K : \bar{K} \xrightarrow[K]{} \bar{K}$ la extensión (q. sabemos q existe por ser $\bar{K}/K$ algebraica) que fijé. En particular notemos que $\bar{\psi}_K$ es automorfismo por ser endomorfismo y $\bar{K}/K$ alg.

y dada $\tau_F : E \xrightarrow[F]{} \bar{K}$, tenemos

$$E \xrightarrow[F]{\tau_F} \bar{K} \xrightarrow[K]{\bar{\psi}_K} \bar{K}$$

$$\sigma_K = \bar{\psi}_K \circ \tau_F \in \mathrm{Hom}(E/K, \bar{K}/K)$$

Probemos que ϕ definida por $\phi(\psi_K, \tau_F) = \bar{\psi}_K \circ \tau_F$ es biyectiva:

① inyectiva: $\bar{\psi}_K \circ \tau_F = \overline{\psi'_K} \circ \tau'_F \Rightarrow \psi_K = \psi'_K$ y $\tau_F = \tau'_F$:

$\forall \beta \in F$, $\bar{\psi}_K \circ \tau_F(\beta) = \overline{\psi'_K} \circ \tau'_F(\beta)$

$\Rightarrow \bar{\psi}_K(\beta) = \overline{\psi'_K}(\beta)$ pues $\beta \in F$ y $\tau_F|_F = id_F$

$\Rightarrow \psi_K(\beta) = \psi'_K(\beta)$ pues $\beta \in F$ y $\bar{\psi}_K, \overline{\psi'_K}$ extienden a ψ_K, ψ'_K.

$\Rightarrow \psi_K = \psi'_K$. Luego la extensión que fijé de ψ_K es la que fijé para $\psi'_K \Rightarrow \bar{\psi}_K = \overline{\psi'_K} \in Gal(\bar{K}/K)$

y $\bar{\psi}_K \circ \tau_F = \bar{\psi}_K \circ \tau'_F \underset{\bar{\psi}_K \text{ invertible}}{\Longrightarrow} \tau_F = \tau'_F$

② sobreyectiva: Sea $\sigma_K \in \mathrm{Hom}(E/K, \bar{K}/K)$. Qpq $\exists\, \psi_K \in \mathrm{Hom}(F/K, \bar{K}/K)$ y $\tau_F \in \mathrm{Hom}(E/F, \bar{K}/F)$ tq $\sigma_K = \bar{\psi}_K \circ \tau_F$ (para la ext fijada)

Consideremos $\sigma_K|_F \in \mathrm{Hom}(F/K, \bar{K}/K)$. Luego $\exists\, \psi_K \in \mathrm{Hom}(F/K, \bar{K}/K)$

tal que $\sigma_K|_F = \psi_K$.

Sea $\bar{\psi}_K$ la extensión fijada de ψ_K a $Gal(\bar{K}/K)$ y consideremos

$\bar{\psi}_K^{-1} \circ \sigma_K \in Hom(E/K, \bar{K}/K)$.

$\bar{\psi}_K^{-1} \circ \sigma_K$ resulta ser una F-inmersión pues $\forall \beta \in F$, se tiene

$$\bar{\psi}_K^{-1} \circ \sigma_K(\beta) = \bar{\psi}_K^{-1} \circ \psi_K(\beta) = \bar{\psi}_K^{-1} \circ \bar{\psi}_K(\beta) = \beta.$$
$$\beta \in F \qquad\qquad \beta \in F$$

o sea $\exists\, \tau_F \in Hom(E/F, \bar{K}/F)$ tq $\bar{\psi}_K^{-1} \circ \sigma_K = \tau_F$

y así $\sigma_K = \bar{\psi}_K \circ \tau_F$. ∎

Ejemplo:

$E = \mathbb{Q}[\sqrt[3]{2}, \zeta_3]$: Tenemos $Hom(F/\mathbb{Q}, \bar{\mathbb{Q}}/\mathbb{Q}) = \{\psi_1, \psi_2, \psi_3\}$

$|$ donde $\psi_1(\sqrt[3]{2}) = \sqrt[3]{2}$

$F = \mathbb{Q}(\sqrt[3]{2})$ $\psi_2(\sqrt[3]{2}) = \sqrt[3]{2}\,\zeta$

$|$ $\psi_3(\sqrt[3]{2}) = \sqrt[3]{2}\,\zeta^2$

$\mathbb{Q}$

y $Hom(E/F, \bar{\mathbb{Q}}/F) = \{\tau_1, \tau_2\}$ con $\tau_1(\zeta_3) = \zeta_3$ y $\tau_2(\zeta_3) = \zeta_3^2$

Fijo extensiones de ψ_1, ψ_2, ψ_3 a $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$.

Por ejemplo $\bar{\psi}_1$ satisface $\bar{\psi}_1(\sqrt[3]{2}) = \sqrt[3]{2}$, $\bar{\psi}_1(\zeta_3) = \zeta_3^2$

$\bar{\psi}_2$ satisface $\bar{\psi}_2(\sqrt[3]{2}) = \sqrt[3]{2}\,\zeta_3$, $\bar{\psi}_2(\zeta_3) = \zeta_3$

$\bar{\psi}_3$ satisface $\bar{\psi}_3(\sqrt[3]{2}) = \sqrt[3]{2}\,\zeta_3^2$, $\bar{\psi}_3(\zeta_3) = \zeta_3^2$

Entonces $\sigma_{11} = \bar{\psi}_1 \circ \tau_1$: $\sigma_{11}(\sqrt[3]{2}) = \sqrt[3]{2}$ y $\sigma_{11}(\zeta_3) = \zeta_3^2$

$\sigma_{12} = \bar{\psi}_1 \circ \tau_2$: $\sigma_{12}(\sqrt[3]{2}) = \sqrt[3]{2}$, $\sigma_{12}(\zeta_3) = \zeta_3$

$\sigma_{21} = \bar{\psi}_2 \circ \tau_1$: $\sigma_{21}(\sqrt[3]{2}) = \sqrt[3]{2}\zeta_3$, $\sigma_{21}(\zeta_3) = \zeta_3$

$\sigma_{22} = \bar{\psi}_2 \circ \tau_2$: $\sigma_{22}(\sqrt[3]{2}) = \sqrt[3]{2}\zeta_3$, $\sigma_{22}(\zeta_3) = \zeta_3^2$

$\sigma_{31} = \bar{\psi}_3 \circ \tau_1$: $\sigma_{31}(\sqrt[3]{2}) = \sqrt[3]{2}\zeta_3^2$, $\sigma_{31}(\zeta_3) = \zeta_3^2$

$\sigma_{32} = \bar{\psi}_3 \circ \tau_2$: $\sigma_{32}(\sqrt[3]{2}) = \sqrt[3]{2}\zeta_3^2$, $\sigma_{32}(\zeta_3) = \zeta_3$

Consecuencias

① Sea $\alpha \in \overline{K}$.

$$\#\,\mathrm{Hom}(K[\alpha]/K, \overline{K}/K) \leq [K[\alpha]:K] = \text{gr}(f(\alpha,K))$$

(Vale $=$ si $f(\alpha,K)$ tiene raíces simples)

② Sea E/K finita

$$\#\,\mathrm{Hom}(E/K, \overline{K}/K) \leq [E:K]$$

Demostración

① Ya sabemos que $\exists\ \sigma: K(\alpha) \xrightarrow[K]{} \overline{K}$ por cada raíz de $f(\alpha,K)$, y es un si y solo si. Puede ocurrir sin embargo que $f(\alpha,K)$ tenga raíces múltiples! Por lo hecho

$$\#\,\mathrm{Hom}(K[\alpha]/K, \overline{K}/K) \leq \text{gr}(f(\alpha,K)) = [K[\alpha]:K]$$

② Por inducción en $n = [E:K]$

- $[E:K] = 1$ $\quad E = K$ y $\mathrm{Hom}(E/K, \overline{K}/K) = \mathrm{id}$
- $[E:K] > 1$. Sea $\alpha \in E - K$ y $f(\alpha,K) \in K[X]$

$$\begin{array}{c} E \\ | \\ K[\alpha] \\ | \\ K \end{array}$$

Tenemos $[E:K] = [E:K[\alpha]]\,[K[\alpha]:K]$

Por otro lado

① $\#\,\mathrm{Hom}(E/K, \overline{K}/K) = \#\,\mathrm{Hom}(E/K[\alpha], \overline{K}/K[\alpha]) \cdot \#\,\mathrm{Hom}(K[\alpha]/K, \overline{K}/K)$

② $\#\,\mathrm{Hom}(K[\alpha]/K, \overline{K}/K) \leq [K[\alpha]:K]$ por el caso anterior y $\#\,\mathrm{Hom}(E/K[\alpha], \overline{K}/K[\alpha]) \leq [E:K[\alpha]]$ por HI pues $[E:K[\alpha]] < [E:K]$

Así $\#\,\mathrm{Hom}(E/K, \overline{K}/K) \leq [E:K]$ ∎

Notamos la conexión entre $\#\,\mathrm{Hom}(\Omega/k, \overline{k}/k)$ y $[\Omega : k]$ y el hecho que los minimales tienen que tener todas sus raíces simples para que valga la $=$.

Existen casos de polinomios irreducibles (minimales) con raíces múltiples!? Ej. típico

en $\mathbb{F}_p(t)[X]$ donde t es trascendente / $\mathbb{F}_p$

El polinomio $X^p - t$ es irreducible ⊛

pero en característica p, $X^p - t = (X - \sqrt[p]{t})^p$; una sola raíz.

⊛ pues $X^p - t$ es irreducible en $\mathbb{F}_p[t, X]$ al tener grado 1 en t. Si fuera $X^p - t = g(X,t)\,h(X,t)$, ent. $\mathrm{gr}_t\, g$ ó $\mathrm{gr}_t\, h = 0 \Rightarrow$ sup. que es g, entonces $g(X,t) \in \mathbb{F}_p[X]$

$\Rightarrow X^p - t$ tiene un contenido en X, pero es primitivo en X, luego $g(X,t) \in \mathbb{F}_p^{\times}$.

SEPARABILIDAD

Definición (Polinomio separable)

Se dice que $f \in k[X]$ es un polinomio separable si $\mathrm{gr}(f) \geq 1$ y f tiene raíces simples en $\overline{k}$

Ejemplos:

① $f = (X-1)(X+\sqrt{2})(X-\sqrt{2}) \in \mathbb{Q}[X]$ es separable

pero $f = (X-1)^2$ no lo es.

Pero claro, este pol. no es irreducible...

② $f = X^p - t \in \mathbb{F}_p(t)[X]$ es irreducible y no es separable

Observación: Sea $f \in K[X]$, $\operatorname{gr} f \geq 1$

f separable $\Leftrightarrow (f : f') = 1$

Demostración

$(\Rightarrow)$ $(f : f') \neq 1 \Rightarrow \exists\, g \in K[X]$ con $\operatorname{gr} g \geq 1$ tq $g \mid f$ y $g \mid f'$

$\Rightarrow \exists\, \alpha \in \overline{K} /\ g(\alpha) = 0$ y por lo tanto $f(\alpha) = f'(\alpha) = 0$

Pero $f = (x-\alpha)\, h \Rightarrow f' = h + (x-\alpha) h'$

satisface $f'(\alpha) = 0 \Leftrightarrow h(\alpha) = 0 \Leftrightarrow x - \alpha \mid h \Leftrightarrow$

$f = (x-\alpha)^2 \tilde{h} \Rightarrow f$ no es separable

$(\Leftarrow)$ $(f : f') = 1 \Rightarrow \exists\, s, t \in K[X] :\ 1 = sf + tf'$

Luego, $\forall \alpha /\ f(\alpha) = 0$, se tiene $f'(\alpha) \neq 0$, o sea α es raíz simple de $f \Rightarrow f$ separable.

Por ejemplo:

$f = X^n - 1 \qquad f' = n X^{n-1} \qquad f'(\alpha) \neq 0$ si $n \neq 0$ en K

o sea $X^n - 1$ es separable en característica 0 o

en característica p con $p \mid n$

Pero $X^n - 1$ no es separable en característica p:

$p \mid n$: $X^n - 1 = (X^k)^p - 1 = (X^k - 1)^p$.

Observación: Sea $f \in K[X]$, $\operatorname{gr} f \geq 1$

- f separable $\Leftrightarrow \Delta(f) = c \prod (\alpha_i - \alpha_j)^2 \neq 0$ en K.

~~Corolario~~

Observación

Sea $f = \prod f_i$ descomposición en irreducibles de $f \in K(X)$

Entonces

f separable $\Leftrightarrow$ h_i todos $\neq$ y h_i separable $\forall i$.

Demostración ($\Rightarrow$) obvio. ($\Leftarrow$) Sup α es raíz múltiple de f. Entonces α no puede ser raíz de más de un $h_i \Rightarrow \exists\, i \neq j$ / $h_i(\alpha) = h_j(\alpha) = 0$

Todo se reduce a irreducibles

Pero $1 = (h_i : h_j) \Rightarrow$

$1 = (h_i : h_j)(\alpha) = 0$ Absurdo. ⊠

Proposición:

① Si $car(K) = 0$, todo pol. irreducible es separable

② Si $f \in K[X]$ es irreducible y $car(K) \nmid gr\, f$, entonces f es separable (caso $car(K) = p$)

Demostración

① $car(K) = 0 \Rightarrow (f : f') = 1$ para f irreducible pues

$g \mid f \Rightarrow g = 1$ o $gr\, g = gr\, f$ pero $f \nmid f'$ ($gr\, f' = gr\, f - 1$)

② Si $f = a_n X^n + \dots$ con $a_n \neq 0$ en K

y $f' = \mu a_\mu X^{\mu-1} + \dots$: si $p \nmid \mu$, entonces $f' \neq 0$, y mismo argumento que en ①.

Observación: En característica 0, dado $f \in K[X]$, $gr\, f \geq 1$

$\dfrac{f}{(f : f')}$ es un polinomio separable (libre de cuadrados) asociado a f

Demostración. idea: $g^2 \mid f \Rightarrow g \mid (f : f')$ ⊠

hacerlo en detalle