Álgebra III - 2do C. 2020 - Clase 7 - 22/9/2020

6 Inmersiones y torres

Ejemplo

$$\begin{array}{c} \mathbb{Q}(\sqrt[3]{2},\sqrt{3}) \\ |_2 \\ \mathbb{Q}(\sqrt[3]{2}) \\ |_3 \\ \mathbb{Q} \end{array}$$

$\mathrm{Hom}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}, \overline{\mathbb{Q}}/\mathbb{Q}) = \{\psi_1, \psi_2, \psi_3\}$ donde $\sqrt[3]{2} \underset{\psi_1}{\mapsto}$, $\sqrt[3]{2} \underset{\psi_2}{\mapsto}$, $\sqrt[3]{2} \underset{\psi_3}{\mapsto}$

¿Cómo se extiende cada una de esas $\mathbb{Q}$-inmersiones a $\mathbb{Q}(\sqrt[3]{2},\sqrt{3})$? ¿De cuántas maneras posibles? ¿Cuáles son todas las $\mathbb{Q}$-inmersiones de $\mathbb{Q}(\sqrt[3]{2},\sqrt{3})$ a $\overline{\mathbb{Q}}$?

Teorema 6.0.1 (Inmersiones y torres)
Sea $E/F/K$ algebraica. Entonces
existe una biyección Φ entre los conjuntos

$$\mathrm{Hom}(E/K, \overline{K}/K) \quad y \quad \mathrm{Hom}(F/K, \overline{K}/K) \times \mathrm{Hom}(E/F, \overline{K}/F),$$

dada de la manera siguiente:
Para cada $\psi_K : F \underset{K}{\hookrightarrow} \overline{K}$, se fija una extensión $\overline{\psi}_K \in \mathrm{Gal}(\overline{K}/K)$
(recuerdo, es un morfismo tal que $\overline{\psi}_K|_F = \psi_K$),
que existe pues ψ_K se extiende a todo $\overline{K}$, y resulta por lo tanto ser un K-endo que es un K-auto, por ser $\overline{K}/K$ algebraica.
(Nota: la notación ψ_K es para recordar que es la identidad sobre K)
Entonces

$$\begin{array}{rccc} \Phi: & \mathrm{Hom}(F/K, \overline{K}/K) \times \mathrm{Hom}(E/F, \overline{K}/F) & \to & \mathrm{Hom}(E/K, \overline{K}/K) \\ & (\psi_K, \tau_F) & \mapsto & \sigma_K := \overline{\psi}_K \circ \tau_F \end{array} .$$

En particular, si E/K *es finita, entonces*

$$\#\operatorname{Hom}(E/K, \overline{K}/K) \;=\; \#\operatorname{Hom}(F/K, \overline{K}/K) \cdot \#\operatorname{Hom}(E/F, \overline{K}/F).$$

Prueba.–
Verificamos primero para nuestra tranquilidad que σ_K definida como

$$E \underset{F}{\overset{\tau_F}{\hookrightarrow}} \overline{K} \underset{K}{\overset{\overline{\psi}_K}{\hookrightarrow}} \overline{K}$$

está efectivamente en $\operatorname{Hom}(E/K, \overline{K}/K)$.

Probemos entonces que Φ es biyectica.

Inyectiva: Sup. que $\overline{\psi}_K \circ \tau_F = \overline{\psi'}_K \circ \tau'_F$. Qpq $\psi_K = \psi'_K$ y $\tau_F = \tau'_F$:

Sea $\beta \in F$, entonces $\tau_F(\beta) = \tau'_F(\beta) = \beta$ y por lo tanto,

$$\begin{aligned} \overline{\psi}_K \circ \tau_F(\beta) &= \overline{\psi'}_K \circ \tau'_F(\beta) \\ \Rightarrow \quad \overline{\psi}_K(\beta) &= \overline{\psi'}_K(\beta) \\ \Rightarrow \quad \psi_K(\beta) &= \psi'_K(\beta) \end{aligned}$$

pues $\beta \in F$ y $\overline{\psi}_K|_F = \psi_K$, $\overline{\psi'}_K|_F = \psi'_K$.

O sea $\psi_K = \psi'_K$. Falta probar que $\tau_F = \tau'_F$.

Pero como $\psi_K = \psi'_K$, su extensión fijada es la misma:

$$\overline{\psi}_K = \overline{\psi'}_K \quad \in \; \operatorname{Gal}(\overline{K}/K)$$

y la podemos invertir:

$$\overline{\psi}_K \circ \tau_F = \overline{\psi'}_K \circ \tau'_F \implies \overline{\psi}_K \circ \tau_F = \overline{\psi}_K \circ \tau'_F \underset{\overline{\psi}_K \text{ inversible}}{\Longrightarrow} \tau_F = \tau'_F.$$

Sobreyectiva: Sea $\sigma_K \in \operatorname{Hom}(E/K, \overline{K}/K)$. Qpq existen $\psi_K \in \operatorname{Hom}(F/K, \overline{K}/K)$ y $\tau_F \in \operatorname{Hom}(E/F, \overline{K}/F)$ tal que $\sigma_K = \overline{\psi}_K \circ \tau_F$.

Considero esta inmersión σ_K restringida a F: $\sigma_K|_F \in \operatorname{Hom}(F/K, \overline{K}/K)$, y por lo tanto existe $\psi_K \in \operatorname{Hom}(F/K, \overline{K}/K)$ tal que $\sigma_K|_F = \psi_K$.

Recordemos que la extensión $\overline{\psi}_K \in \mathrm{Gal}(\overline{K}/K)$ es inversible, y por lo tanto $\overline{\psi}_K^{-1} \circ \sigma_K \in \mathrm{Hom}(E/K, \overline{K}/K)$ satisface, para $\beta \in F$:

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

Es decir $\overline{\psi}_K^{-1} \circ \sigma_K \in \mathrm{Hom}(E/F, \overline{K}/F)$ pues es la identidad sobre F y por lo tanto existe $\tau_F \in \mathrm{Hom}(E/F, \overline{K}/F)$ tal que $\overline{\psi}_K^{-1} \circ \sigma_K = \tau_F$. Concluimos que

$$\sigma_K = \overline{\psi}_K \circ \tau_F.$$

■

Ejemplo Sea ω una raíz primitiva de orden 3 de la unidad.

$$\begin{array}{c} E = \mathbb{Q}(\sqrt[3]{2}, \omega) \\ \big|_2 \\ F = \mathbb{Q}(\sqrt[3]{2}) \\ \big|_3 \\ \mathbb{Q} \end{array}$$

Tenemos

$$\mathrm{Hom}(F/\mathbb{Q}, \overline{\mathbb{Q}}/\mathbb{Q}) = \{\psi_1, \psi_2, \psi_3\} \text{ donde } \sqrt[3]{2} \underset{\psi_1}{\mapsto} \sqrt[3]{2} \ , \ \sqrt[3]{2} \underset{\psi_2}{\mapsto} \sqrt[3]{2}\omega \ , \ \sqrt[3]{2} \underset{\psi_3}{\mapsto} \sqrt[3]{2}\omega^2,$$

y

$$\mathrm{Hom}(E/F, \overline{\mathbb{Q}}/F) = \{\tau_1, \tau_2\} \text{ donde } \omega \underset{\tau_1}{\mapsto} \omega \quad \text{y} \quad \omega \underset{\tau_2}{\mapsto} \omega^2 \ .$$

Fijo extensiones de ψ_1, ψ_2, ψ_3 a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, por ejemplo porque se me dio la gana fijé:

$$\begin{array}{lllll} \overline{\psi}_1 & \text{tq} & \overline{\psi}_1(\sqrt[3]{2}) = \sqrt[3]{2} & \text{y} & \overline{\psi}_1(\omega) = \omega^2, \\ \overline{\psi}_2 & \text{tq} & \overline{\psi}_2(\sqrt[3]{2}) = \sqrt[3]{2}\omega & \text{y} & \overline{\psi}_2(\omega) = \omega, \\ \overline{\psi}_3 & \text{tq} & \overline{\psi}_2(\sqrt[3]{2}) = \sqrt[3]{2}\omega^2 & \text{y} & \overline{\psi}_3(\omega) = \omega^2. \end{array}$$

Entonces $\mathrm{Hom}(E/\mathbb{Q}, \overline{\mathbb{Q}}/\mathbb{Q})$ está compuesto por

$$\begin{array}{lcllll} \sigma_{11} = \overline{\psi}_1 \circ \tau_1 & : & \sigma_{11}(\sqrt[3]{2}) = \sqrt[3]{2} & \text{y} & \sigma_{11}(\omega) = \omega^2, \\ \sigma_{12} = \overline{\psi}_1 \circ \tau_2 & : & \sigma_{12}(\sqrt[3]{2}) = \sqrt[3]{2} & \text{y} & \sigma_{12}(\omega) = \omega, \\ \sigma_{21} = \overline{\psi}_2 \circ \tau_1 & : & \sigma_{21}(\sqrt[3]{2}) = \sqrt[3]{2}\omega & \text{y} & \sigma_{21}(\omega) = \omega, \\ \sigma_{22} = \overline{\psi}_2 \circ \tau_2 & : & \sigma_{22}(\sqrt[3]{2}) = \sqrt[3]{2}\omega & \text{y} & \sigma_{22}(\omega) = \omega^2, \\ \sigma_{31} = \overline{\psi}_3 \circ \tau_1 & : & \sigma_{31}(\sqrt[3]{2}) = \sqrt[3]{2}\omega^2 & \text{y} & \sigma_{31}(\omega) = \omega^2, \\ \sigma_{32} = \overline{\psi}_3 \circ \tau_2 & : & \sigma_{32}(\sqrt[3]{2}) = \sqrt[3]{2}\omega^2 & \text{y} & \sigma_{32}(\omega) = \omega. \end{array}$$

Corolario 6.0.2 (Inmersiones y grado)

1. *Sea* $\alpha \in \overline{K}$ *. Entonces*

   $\mathrm{Hom}(K(\alpha)/K, \overline{K}/K) = \left\{\sigma : K(\alpha) \underset{K}{\hookrightarrow} \overline{K} \text{ definido por } \sigma(\alpha) = \beta \text{ con } f(\alpha, K)(\beta) = 0\right\}$,

   y por lo tanto,

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

   Más aún,

   $\#\mathrm{Hom}(K(\alpha)/K, \overline{K}/K) = [K(\alpha) : K] \iff f(\alpha, K)$ *tiene todas sus raíces simples,*

   y en ese caso, solo en ese caso*,*

   $$\prod_{\sigma \in \mathrm{Hom}(K(\alpha)/K, \overline{K}/K)} (X - \sigma(\alpha)) \ = \ f(\alpha, K).$$

   (En particular el polinomio de la izquierda pertenece a $K[X]$ *y es irreducible.)*

2. *Sea* E/K *extensión finita. Entonces*

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

Prueba.–

1. Discutirlo
2. Por inducción en $[E : K]$.

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

     $$[E : K] = [E : K(\alpha)]\,[K(\alpha) : K] = [E : K(\alpha)]\,\mathrm{gr}(f(\alpha, K))$$

     con $\mathrm{gr}(f(\alpha, K) > 1$. Por otro lado, por la proposición *Inmersiones y torres*, también sabemos que

     $$\#\mathrm{Hom}(E/K, \overline{K}/K) = \#\mathrm{Hom}(E/K(\alpha), \overline{K}/K(\alpha))\,\#\mathrm{Hom}(K(\alpha)/K, \overline{K}/K).$$

     Además, por HI, como $[E : K(\alpha)] < [E; K]$,

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

     y también sabemos por (1) que

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

     Batimos bien, mezclamos todo y listo...

∎

Tenemos entonces la conexión entre cantidad de inmersiones y grado, y observamos que para que valga la igualdad, los minimales tienen que tener todas sus raíces simples (sino va a haber menos inmersiones, que son la cantidad de raíces distintas, que grado, que es la cantidad de raíces con multiplicidad). Y lo terrible es que sí ¡existen polinomios irreducibles, minimales, que tienen raíces múltiples! Desafío a la intuición porque uno piensa que todo es como $\mathbb{Q}$...

Ejemplo típico *(de polinomio minimal con raíces múltiples)*
Sea $K = \mathbb{F}_p(t)$ donde t es trascendente sobre $\mathbb{F}_p$, y consideremos el polinomio

$$f = X^p - t \quad \in \mathbb{F}_p(t)[X].$$

Afirmación: El polinomio f es irreducible en $\mathbb{F}_p(t)[X]$:
f es irreducible en $\mathbb{F}_p[t][X]$ por Eisenstein porque t es primo (= irreducible) en $\mathbb{F}_p[t]$. Y por lo tanto f es irreducible en $K(t)[X]$ pues es no constante (todo polinomio no constante irreducible en n $A[X]$, con A dominio íntegro, es irreducible en $K[X]$ si K es el cuerpo de fracciones de A).

Además, como estamos en característica p,

$$X^p - t = (X - \sqrt[p]{t})^p \quad \in \overline{\mathbb{F}_p(t)}[X],$$

o sea el polinomio irreducible $X^p - t \in \mathbb{F}_p[X]$ tiene una única raíz $\sqrt[p]{t} \in \overline{\mathbb{F}_p(t)}$ con multiplicidad p.

Esto induce el concepto esencial de *separabilidad*.

7 Extensiones separables

7.1 Separabilidad

Definición 7.1.1 (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

- $f = (X-1)(X+\sqrt{2})(X-\sqrt{2}) \in \mathbb{Q}[X]$ es separable pero $g = (X-1)^2$ no lo es. Pero claro, g no es irreducible...
- $f = X^p - t \in \mathbb{F}_p(t)[X]$ es irreducible y no es separable.

Observación 7.1.2 (Separabilidad y derivada)
Sea $f \in K[X]$, $\mathrm{gr}(f) \geq 1$. *Entonces*

$$f \text{ es separable} \iff \mathrm{mcd}(f, f') = 1.$$

Prueba.–

$(\Rightarrow)$

$$\begin{aligned} \mathrm{mcd}(f, f') \neq 1 &\implies \exists\, g \in K[X] \text{ con } \mathrm{gr}(g) \geq 1 \text{ tq } g \mid f \text{ y } g \mid f' \\ &\implies \exists\, \alpha \in \overline{K} \text{ tq } g(\alpha) = 0 \\ &\implies \exists\, \alpha \in \overline{K} \text{ tq } f(\alpha) = 0 \text{ y } f'(\alpha) = 0 \end{aligned}$$

Pero $f = (x - \alpha)h$ implica $f' = h + (x - \alpha)h'$, y por lo tanto

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

y esto implica $(X - \alpha)^2 \mid f$, o sea f no es separable.

$(\Leftarrow)$

$$\mathrm{mcd}(f, f') = 1 \implies \exists\, s, t \in K[X] \text{ tq } 1 = s\, f + t\, f'$$

O sea, si $f(\alpha) = 0$ entonces $f'(\alpha) \neq 0$: α es raíz simple de f y f es separable.

■

Ejemplo
$f = X^n - 1 \in K[X]$ es separable $\Leftrightarrow$ $\mathrm{car}(K) = 0$ o $\mathrm{car}(K) = p$ con $p \nmid n$:

Esto es pues $f' = nX^{n-1}$ que es no nulo y con única raíz 0 cuando $\mathrm{car}(K) = 0$ o $\mathrm{car}(K) = p$ con $p \nmid n$.
Y si $\mathrm{car}(K) = p \mid n$, $X^n - 1 = (X^k)^p - 1 = (X^k - 1)^p$, no es separable.

Observación 7.1.3 (Separabilidad y discriminante)
Sea $f \in K[X]$, $\mathrm{gr}(f) \geq 1$, *con* $f = (X - \alpha_1) \cdots (X - \alpha_n) \in \overline{K}[X]$. *Entonces*

$$f \text{ es separable} \iff \Delta(f) = c \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \neq 0.$$

Observación 7.1.4 (Separabilidad y factorización)
Sea $f = \prod g_i \in K[X]$ *la factorización de* f *como producto de irreducibles en* $K[X]$. *Entonces*

$$f \text{ es separable} \iff g_i \neq g_j \text{ para } i \neq j \text{ y } g_i \text{ separable } \forall\, i.$$

Prueba.–

■

Todo se reduce a polinomios irreducibles...

Proposición 7.1.5 (Polinomios separables y característica)

1. *Si* $f \in K[X]$ *es irreducible con* $\operatorname{car}(K) = 0$, *entonces* f *es separable.*
2. *Si* $f \in K[X]$ *es irreducible con* $\operatorname{car}(K) = p \nmid \operatorname{gr}(f)$, *entonces* f *es separable.*

Prueba.–

1. $\operatorname{car}(K) = 0$: para f irreducible, $\operatorname{mcd}(f, f') = 1$ pues $g \mid f \to g \sim 1$ o $g \sim f$, pero $f \nmid f'$ por cuestiones de grado...
2. $\operatorname{car}(K) = p$: si $f = a_n X^n + \cdots + a_0$ con $a_n \neq 0$ en K, entonces $f' = n a_{n-1} X^{n-1} + \cdots a_1 \neq 0$ si $p \nmid n$, y por lo tanto en ese caso $\operatorname{gr}(f') = \operatorname{gr}(f) - 1$ como en el caso de característica 0. Se sigue como en ese caso.

■

Observación 7.1.6 (Volver un polinomio separable en característica 0)
Sea $f \in K[X]$ *con* $\operatorname{car}(K) = 0$ *y* $\operatorname{gr}(f) \geq 1$. *Entonces*

$$\frac{f}{\operatorname{mcd}(f, f')}$$

es el polinomio separable asociado a f *(tiene todas las mismas raíces, pero simples).*

Prueba.–

■