

Cuerpos de descomposición (feat. Último Teorema de Fermat)

18/9/20

Def:

Dado $f \in K[x]$ no constante, decimos que E es un cuerpo de descomposición (cdd) para f sobre K si cumple a la vez:

- ① f se factoriza linealmente en E .
- ② E está generado como K -álgebra por las raíces de f en E (es decir, si $f = \prod_{i=1}^n (x - \alpha_i)$ con $\alpha_i \in E$, entonces se tiene $E = K(\alpha_1, \dots, \alpha_n) = K[\alpha_1, \dots, \alpha_n]$).

Ejemplos:

① $f(x) = x^2 + bx + c \in \mathbb{Q}[x]$, $\alpha = \sqrt{b^2 - 4c}$
 $\Rightarrow \mathbb{Q}(\alpha)$ es cdd para f sobre $\mathbb{Q}$.

② $f = x^{15} - 2$ sobre $K = \mathbb{Q}(\sqrt[15]{2})$.
¿Cuál es su cdd sobre K y cuál es el grado de esa extensión?

Buscamos su cdd sobre $\mathbb{Q}$. Las raíces de f son:
 $\sqrt[15]{2}, \xi_{15} \sqrt[15]{2}, \dots, \xi_{15}^{14} \sqrt[15]{2}$, donde $\sqrt[15]{2}$ es alguna raíz (podemos suponer que es real) y ξ_{15} es una raíz 15-ava primitiva de la unidad en $\mathbb{C}$.

$$\Rightarrow \text{Desc}(f | \mathbb{Q}) = \mathbb{Q}(\sqrt[15]{2}, \xi_{15} \sqrt[15]{2}, \dots, \xi_{15}^{14} \sqrt[15]{2})$$

Veamos que de hecho:

$$\mathbb{Q}(\sqrt[15]{2}, \zeta_{15} \cdot \sqrt[15]{2}, \dots, \zeta_{15}^{14} \cdot \sqrt[15]{2}) = \mathbb{Q}(\sqrt[15]{2}, \zeta_{15}).$$

$$\Leftrightarrow \zeta_{15}^n \cdot \sqrt[15]{2} \in \mathbb{Q}(\sqrt[15]{2}, \zeta_{15}), \quad \forall 0 \leq n \leq 14.$$

$$\Rightarrow \sqrt[15]{2} \in \mathbb{Q}(\sqrt[15]{2}, \zeta_{15} \cdot \sqrt[15]{2}, \dots, \zeta_{15}^{14} \cdot \sqrt[15]{2}) \text{ y}$$

$$\zeta_{15} = \frac{\zeta_{15} \cdot \sqrt[15]{2}}{\sqrt[15]{2}} \in \mathbb{Q}(\sqrt[15]{2}, \zeta_{15} \cdot \sqrt[15]{2}, \dots, \zeta_{15}^{14} \cdot \sqrt[15]{2})$$

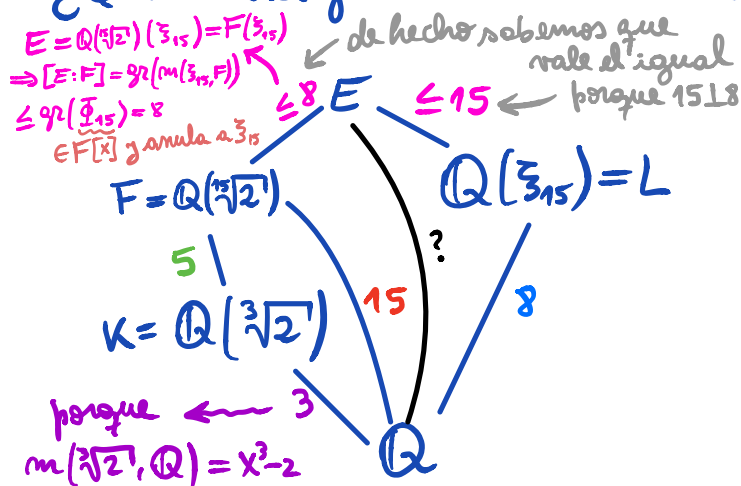
$\in \mathbb{Q}(\sqrt[15]{2}, \zeta_{15} \cdot \sqrt[15]{2}, \dots, \zeta_{15}^{14} \cdot \sqrt[15]{2})$

Este también es el cuerpo de descomposición de f sobre K .

En efecto, $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[15]{2}, \zeta_{15})$ porque $\sqrt[3]{2} = (\sqrt[15]{2})^5$.

$$\mathbb{Q}(\sqrt[3]{2})(\sqrt[15]{2}, \zeta_{15}) = \mathbb{Q}(\sqrt[15]{2}, \zeta_{15}) = E.$$

¿Cuál es el grado de E sobre K ?



$$[F:Q] = 15 \text{ porque}$$

$$m(\sqrt[15]{2}, Q) = x^{15} - 2$$

$$(\text{Eisenstein}) = \Phi_{15}$$

$$[L:Q] = \deg(m(\zeta_{15}, Q))$$

$$= \varphi(15) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$$

·) Por multiplicatividad de grados en Torres debe ser $[F:\mathbb{Q}] = 5$.

$$\begin{aligned} \cdot) [E:\mathbb{Q}] &= [E:L] \cdot \underbrace{[L:\mathbb{Q}]}_{=8} \Rightarrow 8 \mid [E:\mathbb{Q}] \\ \cdot) [E:\mathbb{Q}] &= [E:F] \cdot \underbrace{[F:\mathbb{Q}]}_{=15} \Rightarrow 15 \mid [E:\mathbb{Q}] \end{aligned} \quad \left. \vphantom{\begin{aligned} \cdot) [E:\mathbb{Q}] &= [E:L] \cdot \underbrace{[L:\mathbb{Q}]}_{=8} \\ \cdot) [E:\mathbb{Q}] &= [E:F] \cdot \underbrace{[F:\mathbb{Q}]}_{=15} \end{aligned}} \right\} \begin{aligned} &\Rightarrow 120 = 15 \cdot 8 \mid [E:\mathbb{Q}] \\ &15 \perp 8 \end{aligned}$$

Pero como $[E:F] \leq 8$, se tiene $[E:\mathbb{Q}] = \underbrace{[E:F]}_{\leq 8} \cdot \underbrace{[F:\mathbb{Q}]}_{=15} \leq 120$
 $\Rightarrow [E:\mathbb{Q}] = 120$.

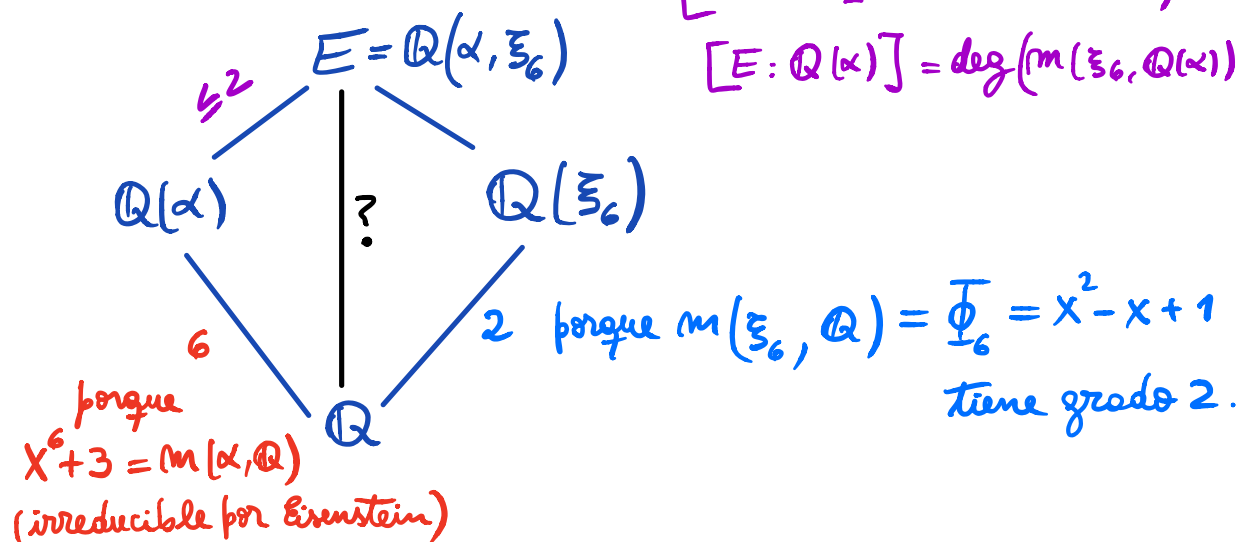
③ $f = x^6 + 3$, ¿cuál es su cdd sobre $\mathbb{Q}$ y cuál es el grado de esa extensión?

Sea α raíz de f en $\mathbb{C}$, y sea ξ_6 raíz sexta primitiva de la unidad.

Entonces, $\text{Desc}(f|\mathbb{Q}) = \mathbb{Q}(\alpha, \xi_6)$ (cuenta análoga a la de antes).

Veamos el grado:

$$\begin{aligned} [E:\mathbb{Q}(\alpha)] &\leq 2. \text{ Más aún,} \\ [E:\mathbb{Q}(\alpha)] &= \deg(m(\xi_6, \mathbb{Q}(\alpha))) \end{aligned}$$



Observación importante:

$$[\mathbb{Q}(\xi_6) : \mathbb{Q}] = 2 \implies \exists d \in \mathbb{Z} \text{ libre de cuadrados tal}$$

clase
parada

$$\text{que } \mathbb{Q}(\xi_6) = \mathbb{Q}(\sqrt{d})$$

(Más aún en este caso sabemos que $d < 0$).

$$\text{Sabemos que } m(\xi_6, \mathbb{Q}) = x^2 - x + 1$$

$\implies$ hacemos un cambio de variables $(x \mapsto x + \frac{1}{2})$:

$$(x + \frac{1}{2})^2 - (x + \frac{1}{2}) + 1 = x^2 + \frac{3}{4} \quad \text{"completar cuadrados"}.$$

$$\implies \mathbb{Q}(\xi_6) = \mathbb{Q}(\sqrt{-\frac{3}{4}}) = \mathbb{Q}(\sqrt{-3}).$$

Pregunta: $\phi(m(\sqrt{-3}, \mathbb{Q}(\alpha)))$?

Sabemos que $\alpha^6 = -3$ (pues $m(\alpha, \mathbb{Q}) = x^6 + 3$)

$$\iff (\alpha^3)^2 = -3$$

$$\implies \pm \alpha^3 = \sqrt{-3}$$

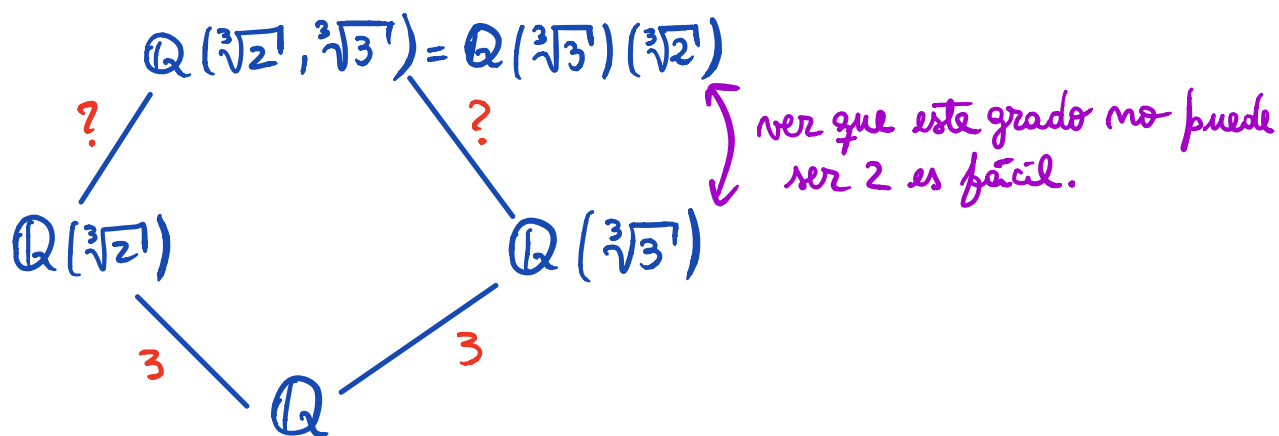
$$\therefore \sqrt{-3} \in \mathbb{Q}(\alpha) \implies [\mathbb{Q}(\alpha)(\sqrt{-3}) : \mathbb{Q}(\alpha)] = 1$$

Concluimos así que $\mathbb{Q}(\alpha) = \text{Desc}(f \mid \mathbb{Q})$ y $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$.

Ejercicio 2.4:

Cuerpo de descomposición de $f = (x^3 - 2)(x^3 - 3)(x^2 - 2)$ sobre $\mathbb{Q}(\sqrt{-5})$
y sobre $\mathbb{F}_5$.

Para $\mathbb{Q}(\sqrt{-5})$:



Ver que no es 1 es lo mismo que ver que $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{3})$.

$$\Leftrightarrow \nexists a, b, c \in \mathbb{Q} / \sqrt[3]{2} = a + b\sqrt[3]{3} + c\sqrt[3]{3^2}$$

④ Ejemplos en cuerpos finitos:

Sean $f = x^5 - x - 2$, $g = x^5 + 4x - 3 \in \mathbb{F}_5[x]$.

i) Hallar sus cdd sobre $\mathbb{F}_5$.

ii) ¿Son isomorfos sus cdd sobre $\mathbb{F}_5$? En tal caso, ¿podemos dar un isomorfismo explícito?

i) f no tiene raíces en $\mathbb{F}_5$:

$$f(0) = \dots, f(1) = \dots, f(2) = \dots, f(3) = \dots, f(4) = \dots$$

$\Rightarrow$ no tiene raíces.

Sean $\alpha, \beta \in \overline{\mathbb{F}_5}$ raíces de f . (Truco útil en cuerpos de característica p).

Así:

$$\begin{aligned} f(\alpha) &= \alpha^5 - \alpha - 2 = 0 \\ f(\beta) &= \beta^5 - \beta - 2 = 0 \end{aligned}$$

$$\begin{aligned} &\alpha^5 - \beta^5 - (\alpha - \beta) = 0 \\ \text{cor}(\overline{\mathbb{F}_5}) \leftarrow &(\alpha - \beta)^5 - (\alpha - \beta) = 0 \implies \alpha - \beta \text{ es raíz de } \\ &X^5 - X, \text{ cuyas raíces} \\ &\text{son todo } \mathbb{F}_5. \end{aligned}$$

$$\implies \alpha - \beta \in \mathbb{F}_5$$

$\therefore$ Las raíces de f son $\alpha, \alpha+1, \alpha+2, \alpha+3$ y $\alpha+4$.

Entonces el c.d.d de f sobre $\mathbb{F}_5$ es $\mathbb{F}_5[\alpha]$.

¿Es f irreducible?

Recordemos que $\alpha \notin \mathbb{F}_5$.

Supongamos que $f = h_1 \cdot h_2$ con $h_1, h_2 \in \mathbb{F}_5[x]$, $\deg(h_1), \deg(h_2) \geq 1$, y miramos el segundo coeficiente de h_1 (o de h_2 , da lo mismo). Ese coeficiente es de la forma $a \cdot \alpha + b$ con $a, b \in \mathbb{F}_5$, pero esto es absurdo, porque $\alpha \notin \mathbb{F}_5$. $\in \mathbb{F}_5$ (pues es un coeficiente de $h_1 \in \mathbb{F}_5[x]$).

La misma cuenta funciona para g , o sea:

$$\text{Desc}(g|\mathbb{F}_5) = \mathbb{F}_5[\beta], \text{ con } \beta \text{ alguna raíz de } g \text{ en } \overline{\mathbb{F}_5}.$$

Como f, g son irreducibles:

$$[\mathbb{F}_5(\beta) : \mathbb{F}_5] = 5 = [\mathbb{F}_5(\alpha) : \mathbb{F}_5]$$

$$\textcircled{2} \quad \alpha \longmapsto a + b\beta + c\beta^2 + d\beta^3 + e\beta^4?$$

Sí, son isomorfos. (lo veremos más adelante en la materia).

Remarcable :

Tenemos dos polinomios sin raíces en común con el mismo cdd (y sin un isomorfismo obvio).