

2.

Después de una parafada ...

Base: $\{1, x, \dots, x^5\}$

$$\varphi_1: x \longrightarrow x$$

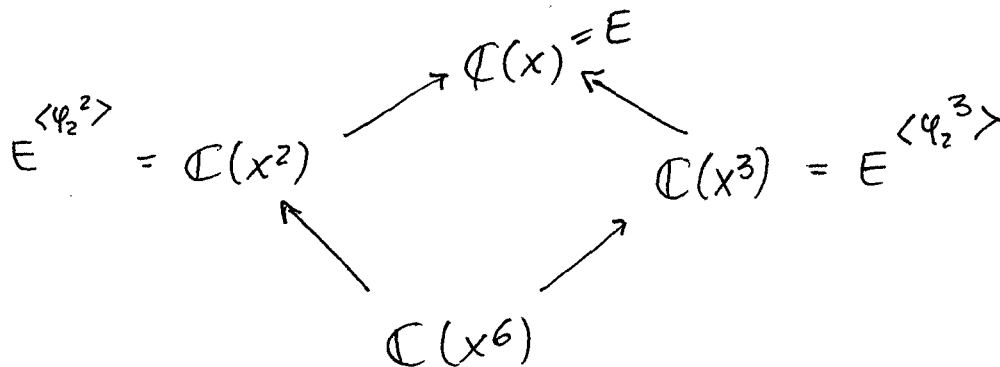
$$\varphi_2: x \longrightarrow x \xi$$

$$\varphi_3: x \longrightarrow x \xi^2$$

$$\vdots$$

$$\varphi_6: x \longrightarrow x \xi^5$$

$$\varphi_2: x \xrightarrow{1} x \xi \xrightarrow{2} x \xi^2 \xrightarrow{3} x \xi^3 \xrightarrow{4} \dots \xrightarrow{6} x \quad \text{orden 6 cíclico}$$



5.

$$\text{Gal}(\mathbb{C} / \text{Gal}(\mathbb{C}(t) / \mathbb{C}(t^3))) \cong C_3$$

$$\mathbb{F}_3(t) / \mathbb{F}_3(t^3)$$

$$\mathbb{F}_3(t)[y] \quad (y^3 - t^3) = (y - t)^3$$

$$\text{Irr}(t, \mathbb{F}_3(t^3)) \mid y^3 - t^3 \in \mathbb{F}_3(t^3)[y]$$

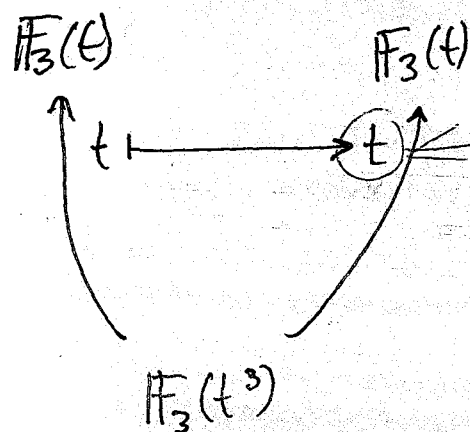
$$\mathbb{F}_3(t^3)[y]$$

$$\text{Calculamos } \text{Gal}(\mathbb{F}_3(t) / \mathbb{F}_3(t^3))$$

$$\mathbb{F}_3(t^3) \hookrightarrow \mathbb{F}_3(t)$$

Obs: $\text{Frob}: \mathbb{F}_3(t) \rightarrow \mathbb{F}_3(t)$
 $\alpha \mapsto \alpha^3$ homomorfismo

pero no es biyectivo (no es automorfismo)



no hay más raíces
 solo hay 1 automorfismo

$$\text{Gal}(\mathbb{F}_3(t^3) / \mathbb{F}_3(t)) = \{\text{id}\}$$

$$c) H = \left\{ \begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} \mid d \in \mathbb{F}_p^\times, c \in \mathbb{F}_p \right\} \leq GL(2, p)$$

$$Gal(E/\mathbb{Q}) \cong H$$

$$\begin{array}{ccc} \mathbb{Q}(\alpha, \xi) & \longrightarrow & \mathbb{Q}(\alpha, \xi) \\ \uparrow & & \uparrow \\ \mathbb{Q}(\xi) & \xrightarrow{\varphi_i} & \mathbb{Q}(\xi) \\ \uparrow & & \uparrow \\ & \mathbb{Q} & \end{array}$$

$$\xi \xrightarrow{\varphi_i} \xi^i \quad i = 1, \dots, p-1$$

por cada uno que ~~fijamos~~ fijemos aquí hay ~~no de~~ estos:

$$\begin{array}{ccc} \alpha & \longmapsto & \alpha \\ \alpha & \longmapsto & \alpha \xi \\ & \vdots & \\ \alpha & \longmapsto & \alpha \xi^{p-1} \end{array}$$

$p \cdot (p-1)$ en total

$$\begin{array}{ccc} \mathbb{Q}(\alpha, \xi) & \longrightarrow & \mathbb{Q}(\alpha, \xi) \\ \uparrow & & \uparrow \\ \mathbb{Q}(\xi) & \xrightarrow{\varphi_i} & \mathbb{Q}(\xi) \\ \uparrow & & \uparrow \\ & \mathbb{Q} & \end{array}$$

$\alpha \mapsto \alpha$
 $\alpha \mapsto \alpha \xi$
 $\alpha \mapsto \alpha \xi^2$
 \vdots
 $\alpha \mapsto \alpha \xi^{p-1}$

$$\begin{aligned} \phi : H &\longrightarrow G = Gal(\mathbb{Q}(\alpha, \xi)/\mathbb{Q}) \\ \begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} &\longmapsto \varphi_{d,c} \end{aligned}$$

¿Es ϕ hom. de grupos?

$$\phi \left(\begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c' & d' \end{pmatrix} \right) \stackrel{?}{=} \phi \left(\begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} \right) \circ \phi \left(\begin{pmatrix} 1 & 0 \\ c' & d' \end{pmatrix} \right)$$

$$\phi \left(\begin{pmatrix} 1 & 0 \\ c+dc' & d' \end{pmatrix} \right)$$

$$\varphi_{dd', c+dc'}$$

$$\varphi_{dc} \circ \varphi_{d'c'}$$

??

$$\varphi_{dd', c+dc'} =$$

20. | f irred. sobre \mathbb{Q} G abeliano
 $u \in \mathbb{C} \setminus \mathbb{R}$ una raíz de f

$$\mathbb{Q} \longrightarrow \frac{\mathbb{Q}[x]}{\langle f(x) \rangle} = \mathbb{Q}(u) = E$$

Cosas clave: • G abeliano \Rightarrow todas las subextensiones son normales

• $\mathbb{Q}(u)$ es \mathbb{Q} añadiendo una raíz de un pol. irred.

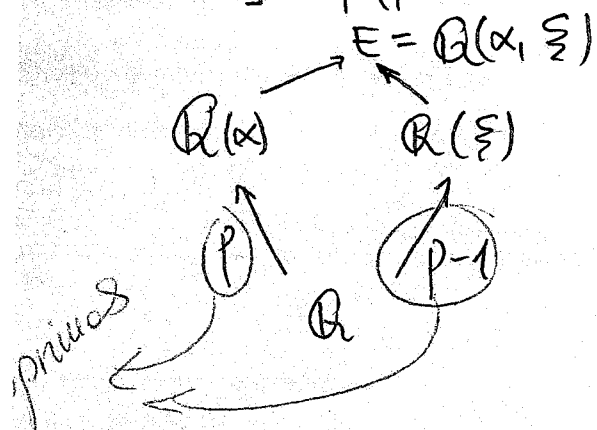
$\text{gr}(f)$ es primo \iff no hay extensiones intermedias entre \mathbb{Q} y $\mathbb{Q}(u)$

Esto es así porque: $\mathbb{Q} \xrightarrow[\text{grado de } f]{} \frac{\mathbb{Q}[x]}{\langle f(x) \rangle}$

13. | $f(x) = x^p - 2$ sobre \mathbb{Q} , p primo

a) $E = \mathbb{Q}(\alpha, \xi)$ $\alpha = \sqrt[p]{2}$, $\xi = e^{2\pi i/p}$

b) $[E:\mathbb{Q}] = p(p-1)$



Continuación 13

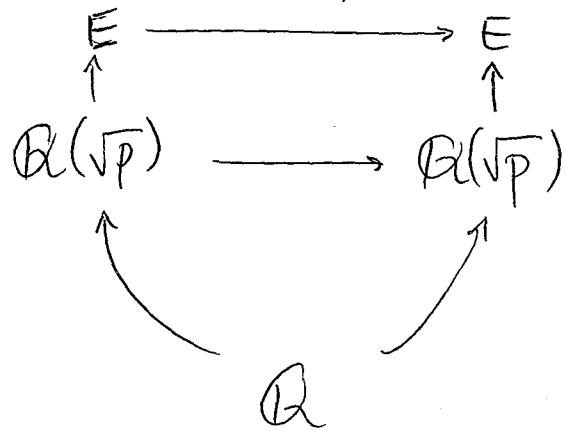
$$\varphi_{dd', c+dc'}\left(\frac{\Sigma}{\gamma}\right) = \frac{\Sigma}{\gamma}^{dd'}$$

$$\varphi_{dd', c+dc'}(\alpha) = \alpha \frac{\Sigma}{\gamma}^{c+dc'}$$

$$\varphi_{dc} \circ \varphi_{d'c'}(\Sigma) = \varphi_{dc}\left(\frac{\Sigma}{\gamma}^{d'}\right) = \frac{\Sigma}{\gamma}^{d'd}$$

$$\begin{aligned}\varphi_{dc} \circ \varphi_{d'c'}(\alpha) &= \varphi_{dc}\left(\alpha \frac{\Sigma}{\gamma}^{c'}\right) = \varphi_{d,c}(\alpha) \cdot \varphi_{d',c'}\left(\frac{\Sigma}{\gamma}\right) = \\ &= \alpha \frac{\Sigma}{\gamma}^c \cdot \frac{\Sigma}{\gamma}^{c'd} = \alpha \frac{\Sigma}{\gamma}^{c+c'd}\end{aligned}$$

18. $(x^2 - p)(x^2 - q)$



$\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$ p q. $\sqrt{q} \neq a+b\sqrt{p}$

Como la ext. es de grado 4: $\text{Gal}(E/\mathbb{Q})$

C_4

$C_2 \times C_2$

porque hay
mínimo dos
ext. intermedias
(hay 3 de hecho
 $\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{q}$

13. d) $x^5 - 2$

$\sqrt[5]{2} \zeta^i \quad i=0, \dots, 4 \quad \zeta = e^{2\pi i/5}$

$E = \mathbb{Q}(\sqrt[5]{2} \zeta^i, i=0 \dots 4)$
 \parallel
 $\mathbb{Q}(\sqrt[5]{2}, \zeta)$

$\sqrt[5]{2} \in E$
 $\sqrt[5]{2} \zeta \in E$

$\left\{ \begin{array}{l} (\sqrt[5]{2})^{-1} \in E \\ (\sqrt[5]{2})^{-1} \cdot \sqrt[5]{2} \zeta = \zeta \in E \end{array} \right.$

[12.] E/K Galois $G = \text{Gal}(E/K)$

$$G \simeq C_n$$

a) $d|n \Rightarrow \exists! L$ con $[E:L] = d$ porque G es cíclico

b) TFTG

c) E/K normal

Tma Artin $[E:E^G] = |G|$

$$K \subset E^G \subset E$$

¿qué pasa con este trozo?
(*)

Teorema (Corolario 1 del Tma de Artin)

E/E^G es Galois

Para cada $H \leq G$ $|H| = d$

$$E^G \subset E^H \subset E$$

||
d

E/K finita $G = \text{Gal}(E/K)$.

Son equivalentes:

1) $K = E^G$

2) E/K Galois

3) E es el cuerpo de descomposición de un pol. separable sobre K .

(*) ~~Sup. $E^G \neq K$~~
~~Sup. $E^G \neq K$, $\alpha \in E^G$ sobre K~~

Sup. $E^G \neq K$, $\alpha \in E^G$ sobre K

$p(x) = \text{Irr}(\alpha, K)$ todas las raíces de este polinomio están en

Sup. que $\beta \in E$ es otra raíz de $p(x)$, $\beta \neq \alpha$. \Rightarrow

$\Rightarrow \exists \gamma \in G = \text{Gal}(E/K)$ tal que $\gamma(\alpha) = \beta \Rightarrow \alpha \notin E^G$
contradicción

$\Rightarrow \alpha$ es inseparable $\Rightarrow \text{Irr}(\alpha, K)$ tiene todas sus raíces iguales

1

Al tener orden primo tiene la unidad

2.

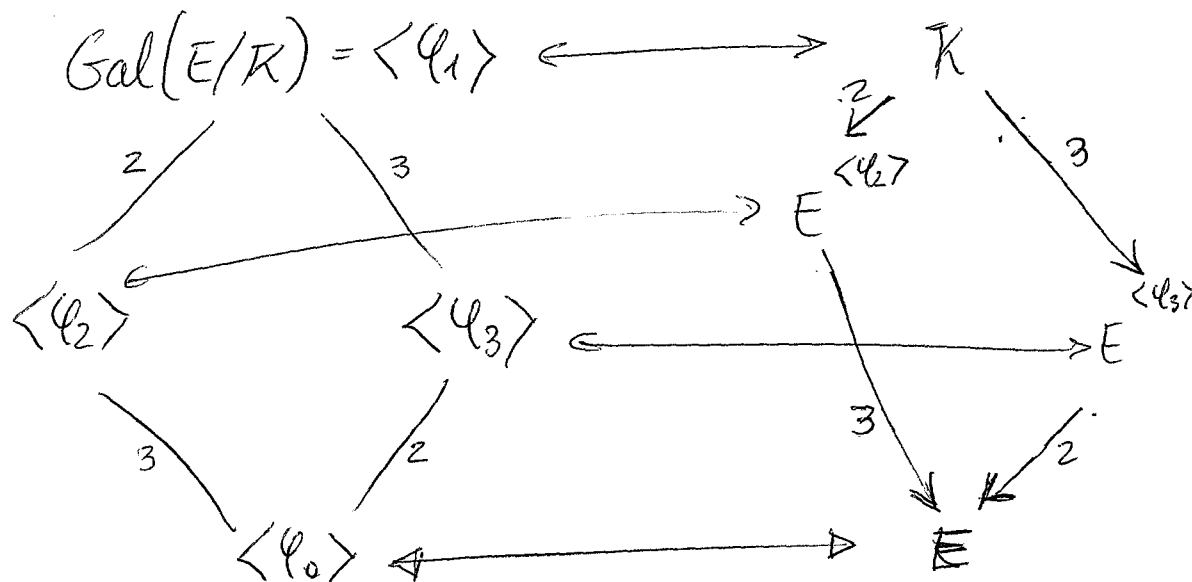
Normal porque es el cuerpo de descomp. de $x^6 - T^6$
 Separable porque \rightarrow es perfecto
 \rightarrow tiene característica cero
 al tener una copia de los enteros

$$|E:K| = 6 = |\text{Gal}(E/K)| \quad \left(\begin{array}{l} \text{donde } E = \mathbb{C}(T) \\ \text{donde } K = \mathbb{C}(T^6) \end{array} \right)$$

Miramos donde van las raíces:

	orden	
$\varphi_0: T \rightarrow T \cong^0 = T$	1	
$\varphi_1: T \rightarrow T \cong^1$	6	$\rightarrow C_6$
\vdots	\vdots	
$\varphi_5: T \rightarrow T \cong^5$		cíclico

Rekulo



5.

Ziel 5

a) $\mathbb{F}_3(t) / \mathbb{F}_3(t^3)$

Es normal porque $\mathbb{F}_3(t)$ es el cuerpo de desc. de $x^3 - t$
No es separable porque $x^3 - t^3 = (x - t)^3$

$\text{Gal}(\mathbb{F}_3(t) / \mathbb{F}_3(t^3)) = \{\text{id}\}$ porque σ_i mandaría raíces en raíces y $x^3 - t^3$ solo tiene 1.

6.

$$f(x) = \underbrace{(x^3 - 2)}_{\substack{\downarrow \\ \sqrt[3]{2}}} \underbrace{(x^2 - 3)}_{\substack{\hookrightarrow \pm\sqrt{3}}} \in \mathbb{Q}[x]$$

$$\sqrt[3]{2} \sum_{i=0}^2 \quad \quad \quad \hookrightarrow \pm\sqrt{3} \quad \quad \quad i = 0, 1, 2$$

