TUTORIA ANA 3/12/19

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

$\boxed{2.}$

Después de una parrafada ...

$\varphi_1 : x \longrightarrow x$

$\varphi_2 : x \longrightarrow x\xi$

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

$\vdots$

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

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

cíclico

$$\begin{tikzcd}
 & \mathbb{C}(x) = E & \\
E^{\langle \varphi_2^2 \rangle} = \mathbb{C}(x^2) \arrow[ur] & & \mathbb{C}(x^3) = E^{\langle \varphi_2^3 \rangle} \arrow[ul] \\
 & \mathbb{C}(x^6) \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

$\boxed{5.}$ $\cancel{Gal(\mathbb{C}}$ $Gal(\mathbb{C}(t)/\mathbb{C}(t^3)) \cong C_3$

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

$$\begin{array}{c} \mathbb{F}_3(t)[y] \quad (y^3-t^3) = (y-t)^3 \\ \cup \\ \mathbb{F}_3(t^3)[y] \end{array}$$

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

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

<u>Obs</u>: $Frob: \mathbb{F}_3(t) \longrightarrow \mathbb{F}_3(t)$, $\alpha \longmapsto \alpha^3$ homomorfismo

pero no es biyectivo (<u>no es automorfismo</u>)

$$\begin{tikzcd} \mathbb{F}_3(t) & & \mathbb{F}_3(t) \\ t \arrow[rr, mapsto] & & t \\ & \mathbb{F}_3(t^3) \arrow[uul, bend left] \arrow[uur, bend right] & \end{tikzcd}$$

no hay más raices

sólo hay 1 automorfismo

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

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

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

$$\begin{tikzcd}
\mathbb{Q}(\alpha,\xi) \arrow[r] & \mathbb{Q}(\alpha,\xi) \\
\mathbb{Q}(\xi) \arrow[u] \arrow[r, "\varphi_i"] & \mathbb{Q}(\xi) \arrow[u] \\
\mathbb{Q} \arrow[u, bend left] \arrow[ur]
\end{tikzcd}$$

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

por cada uno que ~~fijemo~~ fijemos aqu[í]

hay ~~no de~~ estos: $\alpha \longmapsto \alpha$

$\alpha \longmapsto \alpha\xi$

$\vdots$

$\alpha \longmapsto \alpha\xi^{p-1}$

$$\begin{tikzcd}
\mathbb{Q}(\alpha,\xi) \arrow[r] & \mathbb{Q}(\alpha,\xi) \\
\mathbb{Q}(\xi) \arrow[u] \arrow[r, "\varphi_i"] & \mathbb{Q}(\xi) \arrow[u] \\
\mathbb{Q} \arrow[u, bend left] \arrow[ur]
\end{tikzcd}$$

$\alpha \longmapsto \alpha$

$\alpha \longmapsto \alpha\xi$

$\alpha \longmapsto \alpha\xi^2$

$\vdots$

$\alpha \longmapsto \alpha\xi^{p-1}$

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

$$\phi : H \longrightarrow G = Gal(\mathbb{Q}(\alpha,\xi)/\mathbb{Q})$$

$$\begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} \longmapsto \varphi_{d,c}$$

¿ Es $\phi$ hom. de grupos?

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

$$\phi\left(\begin{pmatrix} 1 & 0 \\ c+dc' & d' \end{pmatrix}\right) = \varphi_{dd', c+dc'} \qquad \varphi_{dc} \circ \varphi_{d'c'}$$

??

$\cancel{\varphi_{dd', c+dc'}(\xi)} =$

20. $f$ irred. sobre $\mathbb{Q}$ $\qquad$ $G$ abeliano

$u \in \mathbb{C} \setminus \mathbb{Q}$ una raíz de $f$

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

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

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

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

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

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

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

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

$$\begin{tikzcd} & E = \mathbb{Q}(\alpha, \xi) & \\ \mathbb{Q}(\alpha) \arrow[ur] & & \mathbb{Q}(\xi) \arrow[ul] \\ & \mathbb{Q} \arrow[ul, "p"] \arrow[ur, "p-1"'] & \end{tikzcd}$$

primos

Continuación 13

$$\varphi_{dd', c+dc'}(\xi) = \xi^{dd'}$$

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

$$\varphi_{dc} \circ \varphi_{d'c'}(\xi) = \varphi_{dc}(\xi^{d'}) = \xi^{d'd}$$

$$\varphi_{dc} \circ \varphi_{d'c'}(\alpha) = \varphi_{dc}(\alpha\,\xi^{c'}) = \varphi_{d,c}(\alpha) \cdot \varphi_{d,c}(\xi^{c'}) =$$

$$= \alpha\,\xi^{c} \cdot \xi^{c'd} = \alpha\,\xi^{c+c'd}$$

$\boxed{18.}$ $(x^2-p)(x^2-q)$

$$\begin{tikzcd} E \arrow[rr] & & E \\ \mathbb{Q}(\sqrt{p}) \arrow[u] \arrow[rr] & & \mathbb{Q}(\sqrt{p}) \arrow[u] \\ & \mathbb{Q} \arrow[ul, bend left] \arrow[ur, bend right] & \end{tikzcd}$$

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

Como la ext. es de grado 4 : $\mathrm{Gal}(E/\mathbb{Q}) \to C_4$, $\mathrm{Gal}(E/\mathbb{Q}) \to \boxed{C_2 \times C_2}$

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

$\boxed{13.}$ d) $x^5-2$

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

$E = \mathbb{Q}(\sqrt[5]{2}\,\xi^i,\ i=0\dots4) \qquad \sqrt[5]{2} \in E$

$\qquad = \qquad\qquad\qquad\qquad \sqrt[5]{2}\,\xi \in E$

$\mathbb{Q}(\sqrt[5]{2}, \xi)$

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

12. $E/K$ Galois $\quad G = Gal(E/K)$

$G \simeq C_n$

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

b) TFTG

c) $E/K$ normal

T^ma^ Artin $\quad [E:E^G] = |G|$

$$\underbrace{K \subset E^G}_{\text{¿qué pasa con este trozo? } (*)} \qquad \underbrace{E^G \subset E}_{\text{Teorema}}$$

¿qué pasa con este trozo?
(*)

Teorema (Corolario 1 del Tma de Artin)

$\Rightarrow E/E^G$ es Galois

> $E/K$ finita $G = Gal(E/K)$.
> Son equivalentes:
> 1) $K = E^G$
> 2) $E/K$ Galois
> 3) $E$ es el cuerpo de descomposición de un pol. separable sobre $K$.

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

$$E^G \subset \underbrace{E^H \subset E}_{= d}$$

(*) ~~Sup. $E^K$~~

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

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

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

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

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

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

$\boxed{1.}$ Al tener orden primo tiene la unidad

$\boxed{2.}$ Normal porque es el cuerpo de descomp. de $x^6-T^6$

Separable porque → es perfecto

→ tiene característica cero al tener una copia de los enteros

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

Miramos donde van las raíces:

| | orden |
|---|---|
| $\varphi_0 : T \longrightarrow T\xi^0 = T$ | $1$ |
| $\varphi_1 : T \longrightarrow T\xi^1$ | $6 \longrightarrow C_6$ cíclico |
| $\vdots$ | $\vdots$ |
| $\varphi_5 : T \longrightarrow T\xi^5$ | |

Retículo

$$\begin{tikzcd}
& \mathrm{Gal}(E/K)=\langle\varphi_1\rangle \arrow[dl, dash, "2"'] \arrow[dr, dash, "3"] \arrow[rrr, leftrightarrow] & & & K \arrow[dl, "2"'] \arrow[dr, "3"] & \\
\langle\varphi_2\rangle \arrow[dr, dash, "3"'] \arrow[rrr, leftrightarrow] & & \langle\varphi_3\rangle \arrow[dl, dash, "2"] \arrow[rrr, leftrightarrow] & E^{\langle\varphi_2\rangle} \arrow[dr, "3"] & & E^{\langle\varphi_3\rangle} \arrow[dl, "2"'] \\
& \langle\varphi_0\rangle \arrow[rrr, leftrightarrow] & & & E &
\end{tikzcd}$$

$\boxed{\{id\}}$

$\boxed{5.}$

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 $x^3 - t^3 = (x-t)^3$

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

$\boxed{6.}$ $f(x) = (x^3-2)(x^2-3) \in \mathbb{Q}[x]$

$x^2 - 3 \longrightarrow \pm\sqrt{3}$

$x^3 - 2 \longrightarrow \sqrt[3]{2}\,\xi^i \quad i = 0, 1, 2$

?