3.5 Caracterizaciones de las Extn. de Galois

3.5.1. Teorema Para una extn. de campos $K \supset k$ son equivalentes

(1) $K \supset k$ es extn. de Galois

(2) $K \supset k$ es finita, normal y separable

(3) $K \supset k$ es campo de descomposición de un polinomio que es producto de pol. separables de $k[X]$.

Para la demostración necesitamos un par de resultados preliminares

3.5.2. Lema Sea $K \supset k$ una extn. de campos y $Z = \{a_1, a_2, \dots, a_n\}$ con $|Z| = n$ y sea

$$f := (X - a_1)(X - a_2) \cdots (X - a_n) = X - s_1 X^{n-1} + \cdots + (-1)^n s_n \in K[X]$$

Entonces $\varphi(a_i) = a_i \quad \forall\, i = 1, 2, \dots, n$ y todo $\varphi \in \mathrm{Aut}(K)$ con $\varphi(Z) \subseteq Z$

Dem. φ permuta los elementos de Z.

Con ϕ la extensión de φ a $K[X]$ entonces

$$\phi(f) = \prod_{i=1}^{n} (X - \varphi(a_i)) = \prod_{i=1}^{n} (X - a_i) = f$$

$$\Rightarrow \varphi(a_i) = a_i \quad \forall i \qquad \square$$

3.5.3 Lema Sea $K \supset k$ extn. de Galois, $a \in K$ y $Z := \{\varphi(a) \mid \varphi \in \mathrm{Aut}(K, k)\}$. Entonces

$$f := \prod_{b \in Z} (X - b)$$ es el pol. mínimo de a / k

Dem. $\varphi(Z) = Z \quad \forall\, \varphi \in \mathrm{Aut}(K, k)$ por constr. y porque $\mathrm{Aut}(K, k)$ es un grupo.

3.5.2.

$\Longrightarrow$ · $f \in k[X]$ ya que $k = \mathrm{Fix}(K, \mathrm{Aut}(K:k))$

· f es mónico y $f(a)=0$ por construcción

falta ver que $f \in k[X]$ es irred.

Sea $f = g \cdot h$ factorización en $k[X]$, $g(a)=0$

Para todo $b \in Z$ $\exists\, \varphi \in \mathrm{Aut}(K:k)$ con $\varphi(a) = b$

$\Longrightarrow$ $g(b) = g(\varphi(a)) \underset{\substack{\uparrow \\ \varphi|_k = id}}{=} \varphi\, g(a) = 0$

$\Longrightarrow$ $f \mid g$ $\Longrightarrow$ $h \in k^*$

$\square$

Dem de Tma 3.5.1

1) $\Rightarrow$ 2) Por 3.2.4 $K \overset{Gal}{\supset} k$ es finita.

Por 3.5.3 el pol. mínimo $/k$ de cada $a \in K$ es producto de factores lineales (mónicos) en $K[X]$ que son diferentes 1:1

$\Longrightarrow$ $K \supset k$ es separable y normal.

2) $\Rightarrow$ 3) Por ser $K \supset k$ normal y finita K es el campo de desc. de algún $f \in k[X]$ (3.3.2). Tenemos que verificar que cada factor irreducible de f sea separable:

Sea $g \underset{k[X]}{|} f$ irred y $a \in K$ con $g(a) = 0$ entonces g es (salvo un escalar $b \in k^*$) el pol. mínimo de a $/k$ $\xRightarrow{K \supset k \text{ sep.}}$ g sep.

3) $\Rightarrow$ 1) Sea $K \supset k$ campo de desc. de $f \in k[X]$ como en (3) y $G = Aut(K; k)$.

Claramente, $[K : k] < \infty \Rightarrow$

$\infty > [K : Fix(K, G)] \overset{3.2.8}{\geq} |G|$ i.e. G es finito.

Vamos a demostrar que $k = Fix(K, G)$

Por inducción sobre

$$r := |\underbrace{\{a \in K \setminus k \mid f(a) = 0\}}_{= Z'}|$$

$\underline{r=0}$ $\Rightarrow$ $K = k \overset{\text{triv}}{\Longrightarrow} \mathrm{Fix}(K, G) = k.$

$\underline{r \geq 1}$ Sea $a \in Z'$. El polinomio mínimo g de a/k es un divisor de f en $k[X]$

Con $k' := k(a)$ tenemos $K \supset k'$ el campo de desc. de $f \in k'(a)[X]$ con la misma propiedad de (3), pero visto así f tiene a lo más $r-1$ ceros en $K \setminus k'$

$\overset{\text{hip. ind}}{\Longrightarrow}$ $K \supset k'$ es extn. de galois.

$\Rightarrow \exists\, G' \overset{\text{fin.}}{<} \mathrm{Aut}(K)$ t.q.

$$k' = \mathrm{Fix}(K; G') \quad \wedge \quad G' = \mathrm{Aut}(K; k') \leq G$$

Sea ahora $x \in \mathrm{Fix}(K; G) \subset \mathrm{Fix}(K; G') = k(a)$

Con $n := \deg(g) \wedge g$ pol. min de a/k existen $c_0, \dots, c_{n-1} \in k$ con

$$x = c_{n-1} a^{n-1} + \dots + c_1 a + c_0$$

Sean $a = a_1, a_2, \dots, a_n$ los ceros de g en K entonces por 2.2.7 existe para $\forall i = 1, 2, \dots, n$ un $\varphi_i \in G = \mathrm{Aut}(K, k)$ con $\varphi_i(a) = a_i$

$$\Rightarrow \quad x \underset{\substack{\uparrow \\ x \in \mathrm{Fix}(K, G)}}{=} \varphi_i(x) = c_{n-1} a_i^{n-1} + \dots + c_1 a_i + c_0 \quad \forall i$$

$$\Rightarrow \quad h := c_{n-1} X^{n-1} + \dots + c_1 X + (c_0 - x) \in K[X]$$

tiene los n ceros diferentes $a_1, a_2, \dots, a_n$, pero $\deg(h) \leq n-1$

$$\Rightarrow \quad h = 0 \quad \Rightarrow \quad x = c_0 \in k \qquad \square$$

3.5.4. Cor Si k es un campo con $\mathrm{char}(k) = 0$, entonces $K \supset k$ es una extn. de Galois si y solamente si K es el campo de desc. de algun polinomio $f \in k[X]$.

3.5.5 Cor. Sea $K \supset k$ una extn. de campo.
Si $K = k(a_1, a_2, \ldots, a_n)$ para ciertos $a_i \in K$ que son separables sobre k, entonces vale

(1) $K \supset k$ es finita y separable.

(2) Existe una extensión de campos $L \supset K$ t.q. $L \supset k$ es Galois.

Dem.: · $K \supset k$ es finita por 1.6.2.

Si $f_i \in k[X]$ es el pol. mínimo de a_i / k, f_i es sep. por hip.

$\Rightarrow f := \prod_{i=1}^{n} f_i$ cumple la propiedad (3) del Tma. 3.5.1.

L campo de desc. de f/k $\overset{3.5.1.}{\Longrightarrow}$ $L \overset{\text{Gal}}{\supset} k$ $\overset{3.5.1.}{\Longrightarrow}$ L/k sep.

$\Rightarrow K \supset k$ sep.

3.5.6 Ejemplos

a) El grupo de Galois de $f = X^4 - X^2 - 1 \in \mathbb{Q}[X]$.

Rec. K campo de desc. de $f / \mathbb{Q}$

$\Rightarrow Gal(f, \mathbb{Q}) \equiv Aut(K, \mathbb{Q}) = Aut(K)$

y $K \supseteq \mathbb{Q}$ es extn. de Gal por 3.54

(char($\mathbb{Q}$) = 0),

(a1) $f \in \mathbb{Q}[X]$ es irreducible

f mónico $\Rightarrow$ primitivo, y no tiene ceros en $\mathbb{Z}$

$\Rightarrow$ no tiene ceros en $\mathbb{Q}$!

sup. que f es producto de dos pol. de grado 2

entonces por II. 4.5.5 suficiente considerar

$f = (X^2 + aX + 1)(X^2 + bX - 1)$ (con $a, b \in \mathbb{Z}$)

$= X^4 + \underbrace{(a+b)}_{=0} X^3 + \underbrace{ab}_{=1} X^2 + \underbrace{(b-a)}_{=0} X - 1$ ↯

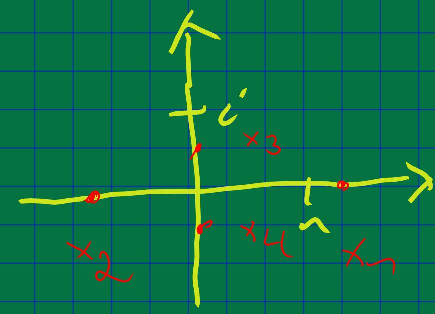
(a2) Ceros de f

Con $y = x^2$ se reduce a una eqn. cuadrática

$\rightsquigarrow$ soluciones

$$x_1 = \frac{\sqrt{1+\sqrt{5}}}{\sqrt{2}}, \quad x_2 = -x_1$$

$$x_3 = \frac{\sqrt{1-\sqrt{5}}}{\sqrt{2}} \quad \rightsquigarrow$$



(a3) <u>Cálculo de $[K:\mathbb{Q}]$</u>

Obviamente $K = \mathbb{Q}[x_1, x_3]$

$x_1 \in \mathbb{R}$, $x_3 \notin \mathbb{R} \Rightarrow \mathbb{Q}[x_1] \neq K$

f irred, $\deg(f) = 4 \Rightarrow [\mathbb{Q}[x_1] : \mathbb{Q}] = 4$

$$x_3^2 = \frac{1-\sqrt{5}}{2} = 1 - x_1^2 \in \mathbb{Q}[x_1] \Rightarrow [K : \mathbb{Q}[x_1]] = 2$$

$$\Rightarrow [K:\mathbb{Q}] = 4 \cdot 2 = 8$$

(a4) $\underline{\mathrm{Gal}(f,\mathbb{Q})} = \mathrm{Aut}(K,\mathbb{Q})$, $K \overset{\mathrm{Gal}}{\supseteq} \mathbb{Q}$

$\overset{\mathrm{Gal.}}{\Longrightarrow} |\mathrm{Aut}(K,\mathbb{Q})| = [K:\mathbb{Q}] = 8$

$\mathrm{Aut}(K,\mathbb{Q}) \overset{3.14}{<} \mathcal{S}_4$, $|\mathcal{S}_4| = 24 = 2^3 \cdot 3$

$\Longrightarrow$ $\mathrm{Aut}(K,\mathbb{Q})$ es el 2-grupo de Sylow de $\mathcal{S}_4$

$\Longrightarrow$ $\mathrm{Gal}(f,\mathbb{Q}) = \mathrm{Aut}(K,8) \cong D_4$ el grupo diédrico del cuadrado

Ojo $\underline{\text{no}}$ es abeliano

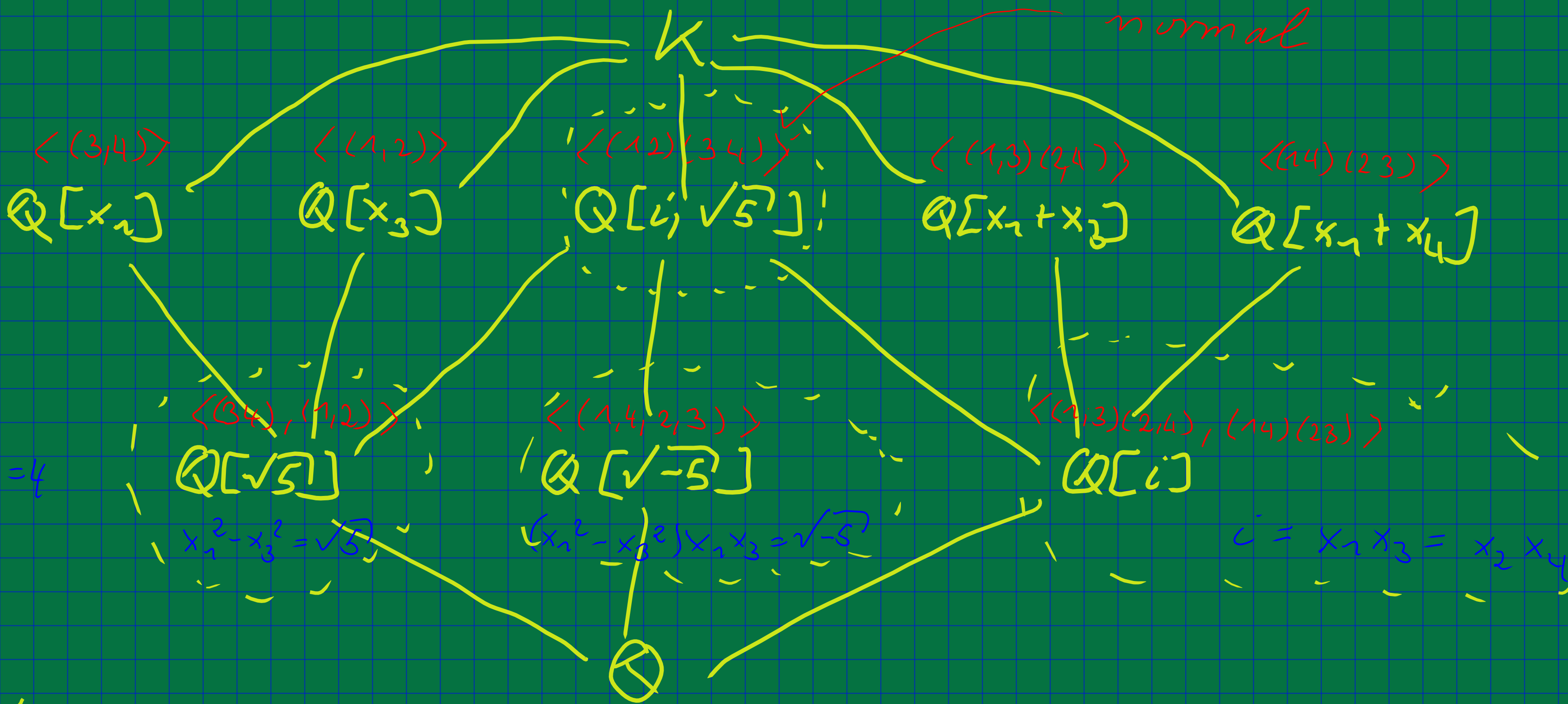
$\Longrightarrow$

(a5) Ejercicio $\mathrm{Gal}(f,\mathbb{Q}) = \mathrm{Sym}\left(\begin{array}{ccc} x_1 & - & x_4 \\ | & & | \\ x_3 & - & x_2 \end{array}\right)$

(a6) Con el teorema principal de Teoría de Galois se obtiene el siguiente diagrama para todos los campos intermedios de $K \supset \mathbb{Q}$:

$|\mathrm{Fix}(K,L)| = 2$
$[K:L] = 2$
$[L:\mathbb{Q}] = 4$

$|\mathrm{Fix}(K,L)| = 4$
$[K:L] = 4$
$[L:\mathbb{Q}] = 2$



L son Gal $/\mathbb{Q}$

(b) Grupo de Galois de $f = X^5 - 4X + 2 \in \mathbb{Q}[X]$

- f es irred en $\mathbb{Q}[X]$ (Eisenstein con $p = 2$)

$\Longrightarrow G := \mathrm{Gal}(f; \mathbb{Q}) \leq S_5$

$5 \mid |G|$: x_1 cero de f en campo de desc. K de f

$\Rightarrow [\mathbb{Q}[x_1] : \mathbb{Q}] = 5$ y

$$\underset{\substack{\| \\ G = \mathrm{Fix}(K:\mathbb{Q})}}{[K : \mathbb{Q}]} = [\mathbb{Q}[x_1] : \mathbb{Q}] \cdot [K : \mathbb{Q}[x_1]]$$

$\Rightarrow G$ contiene un 5-ciclo porque los únicos elementos de orden 5 en S_5 son los 5-ciclos.

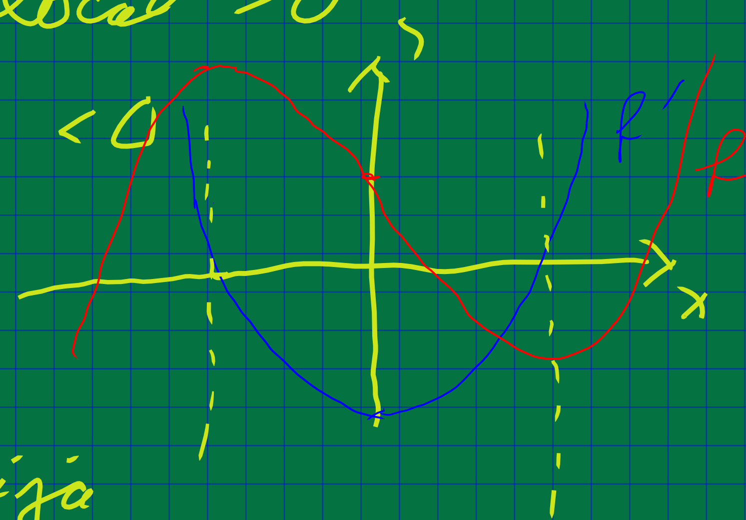
Podemos suponer que $\sigma = (1, 2, 3, 4, 5) \in G$.

- f tiene precisamente 3 ceros reales porque $f' = 5X^4 - 4$ tiene exactamente los ceros $\pm \sqrt[4]{5/4}$ reales

(los otros dos ceros son imaginarios)

$\Rightarrow$ f tiene un mínimo local >0

y un máximo local <0



En $\mathbb{C}$, $\bar{\ }$: $x \mapsto \bar{x}$

(conjugación compleja)

es un automorfismo que fija los ceros reales de f y que intercambia los dos ceros no reales de f, porque $f \in \mathbb{Q}[x] \subset \mathbb{R}[x]$.

$\Rightarrow$ G contiene una transposición (a,b).

Podemos suponer $1 \le a < b \le 5$

$\Rightarrow$ $\sigma^{(b-a)} = (a, b, \dots)$ también es un 5-ciclo

Despues de renombrar los ceros, podemos suponer

$\sigma = (1,2,3,4,5)$ y $\tau = (1,2)$ son elementos de G

$\Rightarrow \boxed{G = S_5}$

$(\sigma^k \tau \sigma^{k-1} = (k+1, k+2)$

$\Rightarrow (1,2), (2,3), (3,4), (4,5) \in G$ son un conjunto de Generadores de S_5