Extensiones cíclicas:

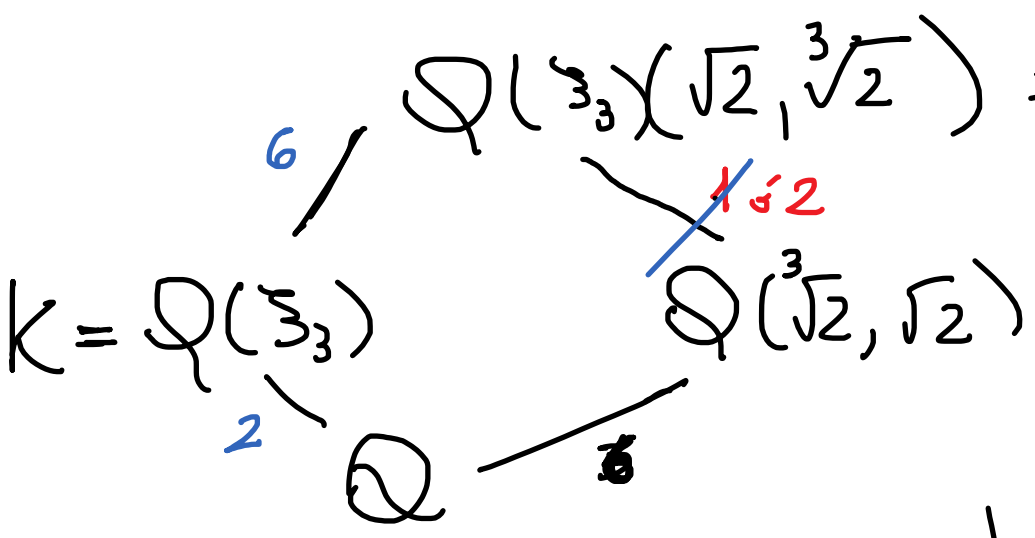
Teo $\mathrm{car}\,k = 0$, $\xi_m \in k$, N/k Galois:

1) N/k cíclica de orden $m \Rightarrow N = k(\theta)$, con $\theta^m \in k$

2) $N = k(\theta)$, con $\theta^m \in k \Rightarrow N/k$ es cíclica de orden $d \mid m$

Ej. $k = \mathbb{Q}(\xi_3)$, N cdd de $(x^2-2)(x^3-2)$.

Entonces N/k es cíclica



y luego $N = k(\sqrt[6]{2})$,

Pues $N \subseteq k(\sqrt[6]{2})$

y ambos tienen grado 6 sobre k

(pues $x^6 - 2 \in \mathbb{Z}[\sqrt{3}i]$ y 2 es primo en ese anillo y usa Eisenstein)

Obs Para 1) usamos $\theta = \alpha + \xi_m \sigma(\alpha) + \cdots + \xi_m^{m-1} \sigma^{m-1}(\alpha)$,

con $\mathrm{Gal}(N/k) = \langle \sigma \rangle$ y $\theta \neq 0$

¿Cómo saber ese α?

Tenemos que $\sigma: N \to N$ es una transf lineal de K-esp vectoriales.

Si $\lambda \in K$ es un autovalor y $\alpha \in N$ es un autovector asociado: $\sigma(\alpha) = \lambda\alpha$

$$\Rightarrow \sigma^m(\alpha) = \lambda^m \alpha$$

$$\Rightarrow \alpha = \lambda^m . \alpha$$

$$\sigma^m = I \Rightarrow \lambda^m = 1 \Rightarrow \lambda \in G_m$$

$\alpha \neq 0$

Sea $A := \{\text{autovalores de } \sigma\} \subseteq G_m$

Más aún, A es un subgrupo de G_m

Pues: • $\lambda, \mu \in A \Rightarrow \sigma(\alpha) = \lambda\alpha$, $\sigma(\beta) = \mu\beta$

$$\Rightarrow \sigma(\alpha\beta) = \lambda\mu\alpha\beta$$

$$\Rightarrow \lambda\mu \in A$$

• $\lambda \in A \Rightarrow \sigma(\alpha) = \lambda\alpha$

$$\Rightarrow \sigma(\alpha^{-1}) = \sigma(\alpha)^{-1} = \lambda^{-1}.\alpha^{-1}$$

• $1 \in A$, pues $\sigma(1) = 1.1$

Luego: $A = G_d$, con $d \mid m$

Ahora $\sigma^m = Id$, o sea $x^m - 1$ anula a σ

$\Rightarrow m_\sigma \mid x^m - 1$. Entonces m_σ tiene raíces simples

Pol mínimo de alg. lineal $\Rightarrow m_\sigma = \prod_{r \in Gd} (x - r)$

$\Rightarrow m_\sigma \equiv x^d - 1$

$\Rightarrow \sigma^d = I \Rightarrow o \mid = m$

Luego $A = G_m$. En particular $\xi_m \in A$, y

tomamos θ un autovector asociado. O sea $\sigma(\theta) = \xi_m \theta$

$\Rightarrow \sigma(\theta^m) = \sigma(\theta)^m = (\xi_m \theta)^m = \theta^m$

Luego $\theta^m \in K$

Además: $\sigma^i(\theta) = \xi_m^i \theta$, con $0 \le i \le m-1$,

y como son todos distintos, $N = K(\theta)$.

ξ_m es primitiva

Ej $f = x^3 + ax + b \in \mathbb{Q}[x]$ irreducible,

$a \neq 0$, $K = \mathbb{Q}(\xi_3)$, N cdd de f sobre K

Probar que si $L = K(\sqrt{\Delta})$, entonces

N/L es cíclica, y hallar $\theta \in N$ tq $N = K(\theta)$

de orden 3 y $\theta^3 \in L$

Si $f = (x-\alpha)(x-\beta)(x-\gamma)$.

$N = k(\alpha,\beta,\gamma)$

$L = k(\sqrt{\Delta})$ — $k(\alpha)$

$|G| = 2$ — 3

k

(Ejercicio 1). $[N:L] = 3$, y en particular es cíclica.

(Ejercicio 2) $B = \{1, \alpha, \beta\}$ es base de N como L-esp vect (cuentas!; se usa que $a \neq 0$)

Tenemos $\sigma : \alpha \mapsto \beta$, $\beta \mapsto \gamma$, entonces

$$[\sigma]_B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}$$, pues $\alpha+\beta+\gamma = 0$

Tenemos que $1, z_3, z_3^2$ son autovalores y resulta que $(0, 1, -z_3)$ es autovector asociado a z_3

Luego, defino $\theta = \alpha - z_3\beta$ y es que

i.e. $\theta^3 \in L$ y $N = L(\theta)$

Resolubilidad. Car $k = 0$

1) E/k es radical si $\exists\ k = k_0 \subset \cdots \subset k_m = E$

tq $k_i = k_{i-1}(\alpha_i)$, con $\alpha_i^{m_i} \in k_{i-1}$

2) E/k es resoluble, si $\exists\ F/k$ radical tq $E \subseteq F$

(por radicales)

Teo: E/k Galois:

E/k resoluble por radicales $\iff$ $\mathrm{Gal}(E/k)$ es resoluble (*)

(se entró internet)

$=: G$

(*) O sea, existen:

$G_0 = G_1 \subseteq \cdots \subseteq G_m = G$ tq $\begin{cases} G_i \triangleleft G_{i+1} \\ G_{i+1}/G_i \simeq \mathbb{Z}/p_i\mathbb{Z} \end{cases}$

(por radicales, pero no lo escribo más!)

Def f resoluble si $\mathrm{Gal}(k(f)/k)$ resoluble

Prop. • $\deg(f) \leq 4 \Rightarrow f$ resoluble (S_n resoluble si $n \leq 4$)

• $\deg(f) \geq 5$ $\not\Rightarrow$ " (S_n no resoluble si $n \geq 5$)

Ej 1) (los locos) $x^5 - 6x + 3$: No resoluble.

Usando que un p-ciclo y una transposición generan S_p

Ej 2) Sea $f \in \mathbb{Q}[x]$ irreducible, $gr(f) = 5$ y $\Delta(f) < 0$.

Probar que f NO es resoluble

- f tiene 0, 2 ó 4 raíces en $\mathbb{C} - \mathbb{R}$.

  - Si tiene 0: $\Delta(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2 > 0$,

    pues es el cuadrado de un número real: Abs

  - Si tiene 4, digamos $\alpha, \bar{\alpha}, \beta, \bar{\beta}$, y sea $\Gamma \in \mathbb{R}$ la otra raíz.

$$\Rightarrow \Delta(f) = \underbrace{((\alpha - \bar{\alpha})(\beta - \bar{\beta}))^2}_{ib \; i\tilde{b}} \cdot \underbrace{((\alpha - \bar{\beta})(\bar{\alpha} - \beta))^2}_{\in \mathbb{R}} \cdot$$

$$\underbrace{((\alpha - \beta)(\bar{\alpha} - \bar{\beta}))^2}_{\in \mathbb{R}} \cdot \underbrace{((\alpha - \Gamma)(\bar{\alpha} - \Gamma))^2}_{\in \mathbb{R}} \cdot$$

$$\underbrace{((\beta - \Gamma)(\bar{\beta} - \Gamma))^2}_{\in \mathbb{R}} > 0 \quad : \text{Abs}$$

Luego: f tiene exactamente 2 raíces en $\mathbb{C} - \mathbb{R}$ y sigo como en el ejemplo 1)

Ej 3) $f \in \mathbb{Q}[x]$ irreducible, $gr(f) = 13$, $\Delta(f) < 0$.

Probar que f NO es resoluble

Sug: Ej 7, Práctica 6

Prop $f = x^5 + ax + b \in \mathbb{Q}[x]$ irreducible son equivalentes:

i) $\Delta(f) \in \mathbb{Q}^2$ y f es reducible

ii) $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q}) \cong D_5$

Dem i) $\Rightarrow$ ii) Llamo $G := \mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})$

- $5 \mid |G|$, pues f es irreducible
- $G \subseteq A_5$, pues $\Delta(f) \in \mathbb{Q}^2$. Pero $G \neq A_5$, pues f es reducible. Entonces $|G| \mid 60$ y $|G| \neq 60$.
- G no tiene 3-ciclos (ejercicio! De nuevo, uso ej 7 de la P.6 Hacerlo pues es fácil y lindo). Entonces $3 \nmid |G|$
- f no tiene TODAS sus raíces en $\mathbb{R}$, pues $f' = 5x^4 + a$, pues no tiene 4 raíces en $\mathbb{R}$.
- σ = "la conjugación compleja" siempre está en G, y en este caso, por el último punto, no es trivial en G. O sea, tiene orden 2. Luego $2 \mid |G|$

Luego hay 2 posibilidades: $|G| = 10$ ó $|G| = 20$

- Si $|G| = 20$, consideramos la acción:

$$A_5 \curvearrowright A_5/G : \sigma \cdot \overline{\pi} := \overline{\sigma\pi}$$

→ No es un grupo! G no tiene por qué ser normal en A_5 (en seguida diré que SEGURO no lo es). Es el conjunto de los co-closes.

Esta acción induce un morfismo de grupos:

$$A_5 \xrightarrow{\varphi} S_n, \text{ donde } n = \left|A_5/G\right| = 3$$

Pero no es el morfismo trivial, pues la acción no es trivial, ya que $\exists\, \sigma \in A_5 \setminus G$, $\overline{\sigma} \neq \overline{1}$.

Entonces hay un núcleo $\ker(\varphi) \subsetneq A_5$

De hecho: $\ker(\varphi) \lhd A_5$

DATO! A_5 es simple (no tiene subgrupos normales no triviales)

(Por eso G seguro no es normal en A_5)

$$\Rightarrow \ker(\varphi) = \{1\} \Rightarrow \underbrace{|A_5|}_{60} = \underbrace{|S_3|}_{6} \quad \text{Abs}$$

Pq lo tanto $|G| = 10$

OTRO DATO! Si $|G| = 10 \Rightarrow G \simeq D_5$ ó $\mathbb{Z}/10\mathbb{Z}$.

Basta descartar $\mathbb{Z}/10\mathbb{Z}$. Para esto podemos ver que G no es abeliano:

Sabemos que G tiene un 5-ciclo ($5 \mid |G|$) y un elemento de orden 2 ($2 \mid |G|$).

Pero G no tiene transposiciones! (Ejercicio! Cuando probaron que no tiene 3-ciclos también serán, por el mismo argumento, que no tiene 2-ciclos)

Entonces podemos suponer que tenemos en G:

$$\sigma = (1\,2)(3\,4)$$

$$\tau = (1\,2\,x\,y\,z).$$

Basta verificar que para las 6 posibilidades para $x\,y\,z$, se tiene $\sigma\tau \neq \tau\sigma$ (Esto pueden creerlo y ya No les aporta nada hacer la cuenta).

$$\therefore G \simeq D_5$$

ii) $\Rightarrow$ i) Ejercicio! (corto y fácil. Escriban $D_5 = \langle \rho, \sigma \rangle$ y ya con esto)