Álgebra Moderna III: 2 de octubre

Clase pasada: Polígonos regulares de 17 lados

Hoy: Grupo de Galois de extensiones ciclotómicas

Ej: $n=5$ $\zeta_5 = e^{2\pi i/5}$ raíz de

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

$\alpha = 2\cos 2\pi/5 = \zeta_5 + \zeta_5^{-1}$ & grado 2 $\begin{cases} \mathbb{Q}(\zeta_5) \\ | \\ \mathbb{Q}(\alpha) \end{cases}$ grado 2 $\begin{cases} \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q} \end{cases}$

$\Phi_5(x)$ es el polinomio mínimo de ζ_5.

Pregunta: Sea $\alpha \in \mathbb{C}$.

¿Es posible saber si α es constructible a través de su polinomio minimal?

↳ $\alpha = a + bi$ es constructible

<u>sii</u> a & b son constructibles.

Sea $a \in \mathbb{R}$,

¿Es posible saber si a es constructible analizando su polinomio minimal?

Ejemplo: $f(x) = x^4 - x^3 - 5x^2 + 1$ tiene 4 raíces reales. Sea α una de ellas

$$\left.\begin{array}{c} \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q} \end{array}\right\} \text{grado } 4, \quad f \text{ irreducible}/\mathbb{Q}.$$

Sin embargo α <u>no</u> es constructible (!?)

En el ejemplo anterior $\mathbb{Q}(\alpha)$ no es el campo de descomposición de $f(x)$.

→ En el caso $\Phi_5(x)$ & $\mathbb{Q}(\gamma_5)$

sí ←

Más aún, $\alpha = \gamma + \gamma^{-1}$

podemos construir

$$\begin{array}{c} \mathbb{Q}(\gamma_5) \\ | \quad \} \text{gr } 2 \\ \mathbb{Q}(\alpha) \\ | \quad \} \text{gr } 2 \\ \mathbb{Q} \end{array}$$

Esta fue/es la clave para concluir que γ_5 es constructible.

↳ analicemos más de cerca esta construcción.

$[\mathbb{Q}(\gamma_5) : \mathbb{Q}] = 4$ sea

$\mathcal{B} = \{1, \gamma, \gamma^2, \gamma^3\}$ una base.

afirmación: $y \longmapsto y^2$ induce un

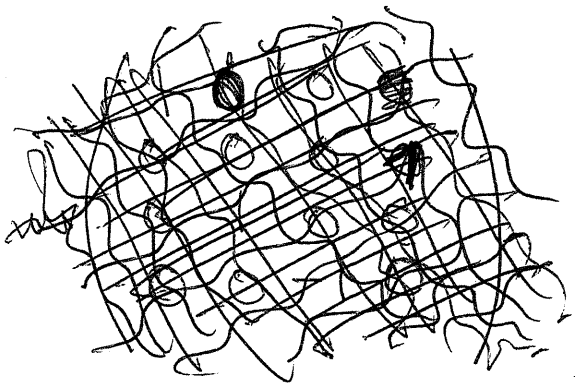
automorfismo de campo.

de $\mathbb{Q}(y) \longrightarrow \mathbb{Q}(y)$

$$T_2 = \begin{cases} 1 \longmapsto 1 \\ y \longmapsto y^2 \\ y^2 \longmapsto y^4 = -1-y-y^2-y^3 \\ y^3 \longmapsto y^6 = y \end{cases}$$

con respecto a la base $\mathcal{Y}$, T_2 se puede representar como

$$T_2 = \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$



OBSERVAR: $T_2^2 = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & -1 & 1 & 0 \end{pmatrix}$

$T_2^3 \longrightarrow \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \end{pmatrix}$

$; T_2 \neq Id$

$$T_2^4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Afirmación: $\gamma \longmapsto \gamma^3$ induce un

automorfismo de campo $\mathbb{Q}(\gamma) \longrightarrow \mathbb{Q}(\gamma)$

$$\mathbb{Q}(\gamma) \longrightarrow \mathbb{Q}(\gamma)$$

$$T_3 = \begin{cases} 1 \longmapsto 1 \\ \gamma \longmapsto \gamma^3 \\ \gamma^2 \longmapsto \gamma^6 = \gamma \\ \gamma^3 \longmapsto \gamma^9 = -(1+\gamma+\gamma^2+\gamma^3) \end{cases}$$

representación matricial de T_3:

$$T_3 = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \end{pmatrix} = T_2^3$$

inducida por $\gamma \longmapsto \gamma^4$

$$T_3^2 = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & -1 & 1 & 0 \end{pmatrix} = T_2^2 = T_4$$

$$\hookrightarrow T_4^2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$T_3^3 = \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix} = T_2$$

El conjunto $G = \{Id, T_2, T_3, T_4\}$

¡es un grupo!

↳ isomorfo a $\mathbb{Z}/4\mathbb{Z}$.

Nota: $G = Aut\begin{pmatrix} \mathbb{Q}(\gamma) \\ | \\ \mathbb{Q} \end{pmatrix}$ (¿?)

Definición: Sea $F \subset L$ una extensión finita de campos. Al conjunto

$$Gal(F|L) = \left\{ \tau : L \to L \;\middle|\; \begin{array}{l} \tau \text{ es un isomorfismo} \\ \tau|_F = Id. \end{array} \right\}$$

le llamaremos el grupo de Galois de la extensión $F \subset L$.

OBSERVAR: $G_1 = \{Id, T_4\} \leq Gal(\mathbb{Q}(\gamma_5) \setminus \mathbb{Q})$

$\mathbb{Z}/2\mathbb{Z} \leq \mathbb{Z}/4\mathbb{Z}$

más aún:

$$T_4(\alpha) = T_4(\gamma) + T_4(\gamma)^{-1}$$

$$= \gamma_5^4 + \gamma_5^{-4}$$

$$= \gamma_5^{-1} + \gamma_5 = \alpha$$

Esto implica: $T_4 : \mathbb{Q}(\gamma) \longrightarrow \mathbb{Q}(\gamma)$

&

$T_4 | \mathbb{Q}(\alpha) = Id.$

i.e. $G_1 = \{Id, T_4\} = Gal(\mathbb{Q}(\gamma) \setminus \mathbb{Q}(\alpha))$

Notación: $\mathbb{Z}/4\mathbb{Z} = \{1, 2, 3, 0\} = \{1, 2, -2, -1\} = Gal$

$\mathbb{Z}/2\mathbb{Z} = \{1, -1\} = G_1$

$\{e\} = \{1\}$

Recapitulando

$$\begin{cases} \mathbb{Q}(\gamma_5) \\ \quad | \\ \mathbb{Q}(\alpha) \\ \quad | \\ \mathbb{Q} \end{cases} \quad \text{Gal}(\mathbb{Q}(\gamma_5)\setminus\mathbb{Q}) = G_1 = \mathbb{Z}/2\mathbb{Z}$$

$\ell(\,) = \mathbb{Z}/4\mathbb{Z}$

más aún

$$\text{Gal}(\mathbb{Q}(\alpha)\setminus\mathbb{Q}) \cong \text{Gal}/G_1$$

EJERCICIO

Teorema (mejorado) γ_5 es construible con regla y compás.

Demostración: sabemos $\text{Gal}(\mathbb{Q}(\gamma_5)\setminus\mathbb{Q}) = \text{Gal}$ es isomorfo a $\mathbb{Z}/4\mathbb{Z}$. Sea $G_1 \leq \text{Gal}$ generado por $\tau \in \text{Gal}$ de órden 2.

Escribamos

$$\begin{array}{c} \mathbb{Q}(\gamma_5) \\ | \\ \mathbb{Q}(\alpha) = E \\ | \\ \mathbb{Q} \end{array}$$

$E \subseteq \mathbb{Q}(\gamma_5)$ subcampo tal que

$$Gal(\mathbb{Q}(\gamma_5) \setminus E) = G_1$$

$$\Rightarrow \quad Gal(E \setminus \mathbb{Q}) \cong {}^{Gal}/_{G_1} \cong \mathbb{Z}/2\mathbb{Z}$$

$\Rightarrow$ $E \setminus \mathbb{Q}$ es una extensión cuadrática.

$$\Rightarrow \quad \gamma_5 \in \begin{array}{c} \mathbb{Q}(\gamma_5) \\ | \\ E \\ | \\ \mathbb{Q} \end{array}$$

~~todas~~

Torre de extensiones cuadráticas

□

~~No~~ γ_7 NO es constructible.

$$Gal(\mathbb{Q}(\gamma_7) \setminus \mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z} = Gal$$

$\Rightarrow$

$\mathbb{Q}(\gamma_7)$
|
E } $Gal(\mathbb{Q}(\gamma_7) \setminus E) = G_1 = \langle \tau \rangle$
|
$\mathbb{Q}$ } $Gal(E \setminus \mathbb{Q}) \cong Gal/G_1 \cong \mathbb{Z}/3\mathbb{Z}$

$\tau \in Gal$ orden 2.

Si todos los subcampos de $\mathbb{Q}(\gamma_7)$ se originan ~~como~~ por subgrupos de Gal entonces tenemos el argumento completo (procediendo por contradicción)