Álgebra Moderna III: 19 septiembre

Clase pasada: Números constructibles $\mathcal{C}$

Hoy: ¿Qué extensión de campo genera $\mathcal{C}$?

Definición: $\mathcal{C}$ se dice el campo de números constructibles.

Teorema: $\alpha \in \mathbb{C}$. El número $\alpha \in \mathcal{C}$ sii

existen campos

$$\begin{array}{c} F_n \\ \Big| \scriptstyle{\deg 2} \\ F_{n-1} \\ \Big| \\ \vdots \\ \Big| \\ F_1 \\ \Big| \scriptstyle{\deg 2} \\ \mathbb{Q} \end{array}$$

tal que

$\alpha \in F_n$

y

$$[F_i : F_{i-1}] = 2$$

$\forall \ 1 \leq i \leq n$

<u>Demostración</u>: Supongamos $\Leftarrow$) que existen campos $\mathbb{Q} \subseteq F_1 \subseteq \cdots \subseteq F_{n-1} \subseteq F_n$ donde $[F_i : F_{i-1}] = 2$. Sabemos (Tarea2) que $F_i = F_{i-1}[\sqrt{\alpha_i}]$ con $\alpha_i \in F_{i-1}$.

Aplicamos inducción en i

1) $F_0 = \mathbb{Q} \subseteq \mathcal{C}$

2) supongamos $F_{i-1} \subseteq \mathcal{C}$

$\hookrightarrow$ entonces $\alpha_i \in F_{i-1}$ es constructible

(clase pasada) $\Rightarrow \sqrt{\alpha_i} \in \mathcal{C}$. Entonces $F_i = F_{i-1}[\sqrt{\alpha_i}] \subseteq \mathcal{C}$.

$\Rightarrow$ $F_n \subseteq \mathcal{C}$ y cualquier $\alpha \in F_n$ es constructible.

$\Rightarrow$) Supongamos ahora $\alpha \in \mathcal{C}$. Necesitamos crear una torre de campos (extensiones cuadráticas de $\mathbb{Q}$) tal que $\alpha \in F_n$, para algún campo F_n en dicha torre.

Idea: α se construye iterando las reglas P1, P2 y P3.

P2 y P3, en general, generan una extensión cuadrática de campo.

Veamos: Supongamos α $\in \mathbb{Q}[i]$ se genera usando la regla P1: intersección de dos líneas rectas l_1 l_2

$$\left.\begin{array}{l} l_1 = \{a_1 x + b_1 y = c_1\} \\ l_2 = \{a_2 x + b_2 y = c_2\} \end{array}\right\} \geq \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \in F_0 (2\times 2) = M_{2\times 2}(\mathbb{Q})$$

La parte real de α (y la imaginaria)

está dada por x en

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}^{-1} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$$

$\Rightarrow$ $x \in \mathbb{Q} = F_0$ y $y \in \mathbb{Q} = F_0$

$\Rightarrow$ $\alpha \in \mathbb{Q}[i]$.

Supongamos ahora $\alpha \in \mathbb{Q}[i]$ y es generado por la regla P2 : $l_1 \cap$ Círculo.

$$l_1 = \{ a_1 x + b_1 y = c_1 \} \quad a_1, b_1, c_1 \in \mathbb{Q}.$$

$$C = \{ x^2 + y^2 + a_2 x + b_2 y + c_2 = 0 \}$$

$$a_2, b_2, c_2 \in \mathbb{Q}.$$

si $a_1 \neq 0$, podemos asumir

$$\ell = \{ x + b_1 y = c_1 \}$$

$$\Rightarrow \quad \ell \cap C = \left\{ \begin{array}{c} x + b_1 y = c_1 \\ \cap \\ x^2 + y^2 + a_2 x + b_2 y + c_2 = 0 \end{array} \right\}$$

$\Rightarrow$ sustituyendo $x = c_1 - b_1 y$,

$$(-b_1 y + c_1)^2 + y^2 + a_2(c_1 - b_1 y) + b_2 y + c_2 = 0$$

$\Rightarrow \quad y \in F_1 = \mathbb{Q}[i][\sqrt{\alpha_1}]$ para algún $\alpha_1 \in \mathbb{Q}[i]$.

extensión cuadrática de campo.

P3 genera también una extensión cuadrática de campo (Tarea).

El teorema se sigue por inducción en el número de pasos (P1 P2 P3) necesarios para construir $\alpha \in \mathcal{C}$.

<u>COROLARIO</u>: si $\alpha \in \mathcal{C}$, entonces

$$[\mathbb{Q}(\alpha):\mathbb{Q}] = 2^m \quad \text{para algún } m \geq 0.$$

Por lo tanto el polinomio minimal/$\mathbb{Q}$ de cualquier número constructible tiene grado una potencia de 2.

El recíproco de este corolario es falso: si el polinomio minimal de alpha tiene grado una potencia de 2,

no implica que alpha es constructible. Veremos un ejemplo

de esto la siguiente clase (o la siguiente a la siguiente)