Álgebra III - 2do C. 2020 - Clase 2 - 4/9/2020

1.3 La ecuación de grado 4

$$f = X^4 + aX^3 + bX^2 + cX + d \text{ con raíces } x_1\,,\ x_2\ ,\ x_3 \text{ y } x_4$$

Sea

$$t_1(x_1, x_2, x_3, x_4) := x_1 + i\,x_2 - x_3 - i\,x_4$$

y sus $4! = 24$ permutaciones para $\sigma \in S_4$ permutación de las raíces.
Se tiene que

$$g(X) \ = \ \prod_{k=1}^{24}(X - t_k) = (X^4 - t_1^4)(X^4 - t_5^4)(X^4 - t_9^4)\cdots(X^4 - t_{21}^4)$$

está compuesto por 6 factores de grado 4, que se pueden ir reduciendo...

Pero tanto Vandermonde como Lagrange se dieron cuenta de algo más simple: si en vez del t_1 de arriba se toma

$$t_1(x_1, x_2, x_3, x_4) := x_1 - x_2 + x_3 - x_4$$

las 24 permutaciones de las raíces dan solamente 6 valores distintos que se repiten 4 veces cada uno y son:

$$\pm t_1, \pm t_3 \text{ con } t_3 := x_1 + x_2 - x_3 - x_4 \quad \text{y} \quad \pm\, t_5 \text{ con } t_3 := x_1 - x_2 - x_3 + x_4$$

O sea para ese nuevo t_1 se puede tomar simplemente

$$\begin{aligned} g(X) &= (X - t_1)(X + t_1)(X - t_3)(X + t_3)(X - t_5)(X + t_5) \\ &= (X^2 - t_1^2)(X^2 - t_3^2)(X^2 - t_5^2) \end{aligned}$$

que es nuevamente un polinomio cuyos coeficientes

$$-(t_1^2 + t_3^2 + t_5^2),\ s_2(t_1^2, t_3^2, t_5^2) \quad \text{y} \ -t_1^2 t_3^2 t_5^2$$

son simétricos en las raíces $x_1, \ldots, x_4$, y por lo tanto expresiones en los coeficientes de f.

Esto implica que t_1^2, t_3^2 y t_5^2 son raíces de una cúbica cuyos coeficientes se pueden calcular, y teniendo t_1^2, t_3^2 y t_5^2 se recuperan los posibles valores de t_1, t_3 y t_5 sacando raíz cuadrada. Finalmente

$$x_1 = \frac{1}{4}\big((x_1 + x_2 + x_3 + x_4) + t_1 + t_3 + t_5\big), \quad \text{etc.}$$

(Solo hay que asignar correctamente los signos al final para quedarse con las 4 raíces.)

1.4 La ecuación de grado 5 (o más)

Para la ecuación de grado 5 se llega a un polinomio g con 24 factores de grado 5 de la forma $x^5 - t^5$, pero que no se logran reducir de ninguna manera como ocurrió en la ecuación de grado 4 (o de grado 3)...

Comentario final sobre esta primera sección:
Estos métodos que estuvimos describiendo por un lado asumen la existencia de las raíces "en algún lado"y por otro lado tratan a esas raíces desconocidas como objetos (variables) independientes, que no tienen relación entre sí. Cuando sabemos que eso no ocurre siempre: por ejemplo en las ecuaciones $X^n - 1$ las raíces cumplen un montón de relaciones, se tiene que hay una raíz x tal que todas las raíces son de la forma x^k, $0 \leq k \leq n-1$...

1.5 Teorema Fundamental del Álgebra

Sabemos que

- X^2+aX+b con $a, b \in \mathbb{C}$ tiene sus dos raíces en $\mathbb{C}$ (contadas con multiplicidad)
- $X^n - a$ con $a \in \mathbb{C}$ tiene sus n raíces en $\mathbb{C}$ (todas distintas si $a \neq 0$)

Estos son casos particulares que Teorema Fundamental del Álgebra, que dice que $\mathbb{C}$ es *algebraicamente cerrado*:

Teorema 1.5.1 (Teorema fundamental de álgebra (TFA))
Sea $f \in \mathbb{C}[X]$ un polinomio de grado $n \geq 1$. Entonces

- *f tiene al menos una raíz en $\mathbb{C}$: existe $x \in \mathbb{C}$ tal que $f(x) = 0$,*

o equivalentemente,

- *f tiene sus n raíces en $\mathbb{C}$ (contadas con multiplicidad).*

Han visto ya una demostración de este teorema si hicieron Analisis Complejo, ya que es una consecuencia del Teorema de Liouville (Cauchy 1844) que dice que toda función holomorfa y acotada en $\mathbb{C}$ es constante. Hay también una demostración muy bella y elemental que solo usa herramientas del Álgebra Lineal (y alguna de analisis). En este curso verán otra demostración que es consecuencia de la teoría de cuerpos. Históricamente hubo demostraciones, casi siempre con algún problema, de Girard (1629), Euler (1719) y Laplace (1791), D'Alembert (1796) y Gauss (1797/99, 1816, 1849). Aquí quiero presentar la hermosa versión (combinada) de Euler y Laplace, cuyos ingredientes son

- Un polinomo $f \in \mathbb{R}[X]$ de grado impar tiene al menos una raíz real (teorema de Bolzano),
- Un polinomio $f \in \mathbb{C}[X]$ de grado 2 tiene dos raíces en $\mathbb{C}$,
- El Teorema fundamental de los polinomios simétricos elementales.

Prueba del TFA.–

(1) Sin pérdida de generalidad se puede suponer $f \in \mathbb{R}[X]$ pues si f no lo está, podemos considerar

$$f \cdot \overline{f} = (\sum_i a_i X^i)(\sum_i \overline{a_i} X^i) = \sum_k (\sum_{i+j=k} a_i \overline{a_j}) X^k \ \in \mathbb{R}[X]$$

(Verificar que este polinomio está efectivamente en $\mathbb{R}[X]$.)

Y si $x \in \mathbb{C}$ es raíz de $f \cdot \overline{f}$, o bien es raíz de f o bien es raíz de $\overline{f}$, en cuyo caso $\overline{x} \in \mathbb{C}$ es raíz de f.

(2) Sea entonces $f \in \mathbb{R}[X]$. Qpq que f tiene (al menos) una raíz en $\mathbb{C}$.
Dado $\mathrm{gr}(f) = n = 2^k q$ con q impar, la demostración es por inducción en $k \geq 0$.

– Caso $k = 0$: $\mathrm{gr}(f)$ impar $\Rightarrow$ f tiene una raíz real ($\Rightarrow$ compleja) por el teo de Bolzano.

– Caso $k > 0$: Sea $f = (X - x_1) \cdots (X - x_n)$. Quiero probar que alguno de los x_i pertenece a $\mathbb{C}$.

Dado $c \in \mathbb{R}$, defino $z_{ij} := x_i + x_j + c\, x_i x_j$ para todo $1 \leq i < j \leq n$, y consideramos el polinomio

$$g = \prod_{i,j} (X - z_{ij}) \ \in \mathbb{R}[x_1, \ldots, x_n][X].$$

Este polinomio tiene grado

$$\binom{n}{2} = \frac{n(n-1}{2} = \frac{2^k q(2^k q - 1)}{2} = 2^{k-1} q(2^k q - 1) = 2^{k-1} m \ \text{ con } m \text{ impar}.$$

Si probamos que $g \in \mathbb{R}[X]$ podremos entonces aplicarle la hipótesis inductiva.

Afirmación: $g \in \mathbb{R}[X]$:

Puede pensarlo por su cuenta o mirar lo que sigue.

Sea $\sigma \in S_n$ una permutación de las raices $x_1, \ldots, x_n$ desconocidas de f. Entonces

$$\begin{aligned}\sigma(g(X)) &= \prod (X - \sigma(z_{ij}) = \prod (X - (\sigma(x_i) + \sigma(x_j) + c\,\sigma(x_i)\sigma(x_j) \\ &= \prod \big(X - (x_{i'} + x_{j'} + c\,x_{i'}x_{j'})\big) = g(X)\end{aligned}$$

pues en definitiva σ manda bijectivamente $\{z_{i,j}, i < j\}$ en $\{z_{i,j}, i < j\}$.

Así los coeficientes de $g \in \mathbb{R}[x_1, \ldots, x_n][X]$ son polinomios simétricos en $\mathbb{R}[x_1, \ldots, x_n]$, las raíces de f, y por lo tanto son polinomios en $\mathbb{R}[s_1(\mathbf{x}), \ldots, s_n(\mathbf{x})]$, los coeficientes (reales) de f (aquí $\mathbf{x} = (x_1, \ldots, x_n)$).

Luego, por hipótesis inductiva, para cada $c \in \mathbb{R}$, $g = g_c$ tiene una raíz en $\mathbb{C}$. O sea dado $c \in \mathbb{R}$, existe $z_{i,j}(c) \in \mathbb{C}$. Más precisamente, dado $c \in \mathbb{R}$ existen $i(c), j(c)$ tales que

$$x_{i(c)} + x_{j(c)} + c\,x_{i(c)}x_{j(c)} \ \in \mathbb{C}.$$

Pero hay infinitos $c \in \mathbb{R}$ y finitos x_i. Por el principio de los casilleros (¿lo conoce no? el maravilloso principio de los casilleros de Dirichlet), deben existir $c \neq c' \in \mathbb{R}$ tales que $i(c) = i(c') =: i$ y $j(c) = j(c') =: j$. ¿Se entiende? Escribirlo bien por favor....

Así:

$$\left\{ \begin{array}{c} x_i + x_j + c\,x_i x_j \in \mathbb{C} \\ x_i + x_j + c'\,x_i x_j \in \mathbb{C} \end{array} \right. \quad \Rightarrow \quad \left\{ \begin{array}{c} x_i + x_j \in \mathbb{C} \\ x_i x_j \in \mathbb{C} \end{array} \right.$$

(Escribir bien este razonamiento.) Y por lo tanto x_i, x_j son soluciones de una cuadrática con coeficientes en $\mathbb{C}$, lo que implica que $x_i, x_j \in \mathbb{C}$.

■

2 Cuerpos

2.1 Hechos generales

Ya todes saben... Un conjunto K es un *cuerpo* si viene provisto con dos operaciones (internas) suma $+$ y producto $\cdot$ de manera que

- $(K, +)$ es un grupo abeliano con elemento neutro $0 = 0_K$,
- $(K^\times, \cdot)$ es un grupo abeliano con elemento neutro $1 = 1_K \neq 0_K$ (donde $K^\times = K \setminus \{0_K\}$),
- vale la distributividad del producto $\cdot$ sobre la suma $+$:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad \forall\, a, b, c \in K.$$

Ejemplos Todos los que se les ocurran, escriban....

Comentarios (para demostrar cuando hace falta)

- En todo lo que sigue, K va a ser un cuerpo, para no complicarnos.
- Un cuerpo tiene al menos 2 elementos distintos: 0 y 1.
- K cuerpo $\Rightarrow$ K dominio íntegro ¿Qué era un dominio íntegro?
- A anillo conmutativo e I ideal de A. Entonces

$$A/I \text{ cuerpo} \quad \Leftrightarrow \quad I \text{ ideal maximal}$$

(donde I maximal si cada vez que $I \subset J$ con J ideal, $J \neq A$, entonces $I = J$.)

2.2 Característica de un cuerpo $(\mathrm{car}(K))$

$$\mathrm{car}(K) := \begin{cases} \min\{n \in \mathbb{N} :\ n \cdot 1 := \underbrace{1 + \cdots + 1}_{n} = 0_K\} & \text{si existe tal } n \in \mathbb{N} \\ 0 \quad \text{si no existe tal } n \in \mathbb{N} \end{cases}$$

Esta misma definición se puede dar para un anillo A, donde puede dar cualquier número, pero en el caso de un cuerpo K la característica no puede dar cualquier cosa.

Proposición 2.2.1 *La característica de un cuerpo K siempre da 0 o un número primo p.*

Prueba.–

Sea $\Phi : \mathbb{Z} \to K$ el homomorfismo de anillos definido por $1_{\mathbb{Z}} \mapsto 1_K$.

Homomorfismo de anillos: función $\Phi : A \to B$ que satisface $\forall\, a, a' \in A$

$$\begin{cases} \Phi(a + a') = \Phi(a) + \Phi(a') \\ \Phi(aa') = \Phi(a)\Phi(a') \\ \Phi(1_A) = 1_B \end{cases}$$

O sea $\Phi(0) = 0$, $\Phi(m) = \underbrace{1 + \cdots + 1}_{m}$, y $\Phi(-m) = \underbrace{(-1) + \cdots + (-1)}_{m}$, $\forall\, m \in \mathbb{N}$.

Sabemos que el núcleo de Φ, $\mathrm{Nu}(\Phi) = \ker(\Phi) := \{m \in \mathbb{Z} : \Phi(m) = 0_K\}$, es un ideal de $\mathbb{Z}$, y por lo tanto sólo puede ser el ideal $\{0\}$ o un $n\mathbb{Z}$ para algún $n \in \mathbb{N}$ (y no puede ser $n = 1$ pues Φ no es nulo como endomorfismo si manda 1 en 1).

Por otro lado $\Phi(\mathbb{Z}) = \mathrm{Im}(\Phi) \simeq \mathbb{Z}/\mathrm{Nu}(\Phi)$ (por el 1er teorema del isomorfismo)

- Si $\mathrm{Nu}(\mathbb{Z}) = \{0\}$, entonces $\mathbb{Z} \simeq \Phi(\mathbb{Z}) \subset K$: es el caso de característica 0.
  Más aun, como en este caso, via el isomorfismo, $\mathbb{Z} \subset K$, entonces el cuerpo $\mathbb{Q} \subset K$: $\mathbb{Q}$ es el *cuerpo primo* de K (menor cuerpo contenido en K).
- Si $\mathrm{Nu}(\mathbb{Z}) = n\mathbb{Z}$ para algún $n \geq 2$, entonces $\mathbb{Z}/n\mathbb{Z} \simeq \Phi(\mathbb{Z}) \subset K$ pero K es íntegro, y por lo tanto $\mathbb{Z}/n\mathbb{Z} \simeq \Phi(\mathbb{Z})$ es íntegro también, o sea $n = p$ para algún primo p: es el caso de característica p.
  Más aun, como en este caso, via el isomorfismo, $\mathbb{Z}/p\mathbb{Z} \subset K$, entonces el cuerpo $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} \subset K$: $\mathbb{F}_p$ es el *cuerpo primo* de K.

■

Observación ¡trivial pero fundamental!

K es un espacio vectorial sobre su cuerpo primo.

2.3 Extensiones de cuerpos

Recordemos que un homomorfismo de cuerpos es un homomorfismo de anillos, pero siempre va a tener una particularidad, ¡siempre es inyectivo! pues dado tal $\varphi : K \to E$, $\mathrm{Nu}(\varphi)$ es un ideal del cuerpo K ¿ cuyos únicos ideales son ?

Y como la función nula no es homomorfismo, la única que queda es $\mathrm{Nu}(\varphi) = \{0_K\}$. Así, φ es mono, $\varphi(K) \simeq K$, y $K \hookrightarrow E$, o identificando $K \simeq \varphi(K)$, notamos $K \subset E$.

Definición 2.3.1 (Extensión de cuerpo)
Sean K, E cuerpos. Se dice que E es una extensión *de K si existe un (mono)morfismo $\varphi : K \hookrightarrow E$. Lo notamos E/K.*

Observación 2.3.2 *Sea E/K una extensión de cuerpos. Entonces E es un K-espacio vectorial.*

Definición 2.3.3 (Grado de una extensión, extensión finita)
Sea E/K una extensión de cuerpos.

- *El* grado *de E sobre K es la dimensión de E como K-espacio vectorial y se nota $[E : K]$.*

$$[E : K] := \dim_K(E).$$

- *Se dice que E/K es (una extensión)* finita *cuando $[E : K] < \infty$ (e* infinita *sino).*

Ejemplos

- $[\mathbb{C} : \mathbb{R}] = ?$
- $[\mathbb{R} : \mathbb{Q}] = ?$

Observación 2.3.4

$$[E : K] = 1 \Leftrightarrow E = K$$

Miremos ahora que pasa con torres de extensiones $E/F/K$ (se entiende lo que es ¿no?). (Notar que esto es consistente pues si $K \hookrightarrow F$ via φ y $F \hookrightarrow E$ via ψ, entonces $K \hookrightarrow E$ via $\psi \circ \varphi$)

¿Cómo será el grado de una torre?

Proposición 2.3.5 (Torres y extensiones finitas)
Sea $E/F/K$ una torre de cuerpos. Entonces

$$E/K \text{ finita} \quad \Leftrightarrow \quad E/F \text{ y } F/K \text{ finitas},$$

y en ese caso $[E:K] = [E:F]\,[F:K]$.

Prueba.–

($\Rightarrow$) Sea $\mathcal{B}$ base de E/K, entonces $\mathcal{B}$ genera E sobre F, y por lo tanto si $[E:K] < \infty$, ent. $[E:F] < \infty$.

Por otro lado el subcuerpo F es un K-subespacio de E, y por lo tanto si $[E:K] < \infty$, ent. $[F:K] < \infty$.

($\Leftarrow$) Sean $\{v_1, \ldots, v_n\}$ base de F/K y $\{w_1, \ldots, w_m\}$ base de E/F, entonces ¿quién es base de E/K?

■

Consecuencia Sea $E/F/K$ con E/K finita. Entonces $[E:F] \,|\, [E:K]$ y $[F:K] \,|\, [E:K]$.