El teorema fundamental del álgebra

Vía álgebra lineal

José Cuevas Barrientos

Pontificia Universidad Católica de Chile

5 de julio de 2021

Introducción

Introducción

Historia

Historia

El teorema fundamental del álgebra (TFA) fue demostrado originalmente por D'Alambert, pero fue descartada por carecer de formalidad; para su tesis doctoral Gauss ofrece una demostración alternativa que fue mejor recibida, en su vida publicó cuatro demostraciones y fue uno de los matemáticos que estableció la importancia de los números complejos.
Hoy en día la demostración usual ocupa el concepto de "número de giro" topológico que puede ser evitado mediante el uso de cálculo multivariable (en concreto la demostración utiliza el teorema de Fubini, una generalización del teorema fundamental del cálculo y el teorema de Schwarz).

Historia


Demostraciones del TFA
Dominio de ideales principales
Teorema de Kronecker
Extensiones algebraicas
Cuerpos formalmente reales
Teoría y extensiones de Galois
k-monomorfismos
Teoría de grupos
Teoremas de Sylow
Funciones complejas analíticas
Teorema de Green
Teorema de Liouville
Teorema de Cauchy-Goursat
Integrales paramétricas
Teorema de Fubini-Tonelli
Teorema de Schwarz
Wolfram, cuanto vale
ésta integral?
$\int_{-\pi/2}^{\pi/2} \cos^2 u \, \mathrm{d}u$

Para nuestra fortuna, en 2003 se publicó un artículo por Derksen que establece una equivalencia entre el TFA y la existencia de autovalores de matrices complejas y que sólo utiliza una inducción truquera.

Para la demostración de Derksen utilizaremos el hecho de que el TFA es equivalente a que toda matriz posea autovalores. Ésta equivalencia derivada de que dado el polinomio mónico

$$p(x) := a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$$

se cumple que la matriz

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}$$

le tiene como polinomio característico.
Luego el problema se reduce en demostrar que las matriz complejas poseen autovalores.

Introducción

Receta para el TFA

Receta

Vamos a necesitar:

1. Alguna propiedad que relacione la completitud de $\mathbb{R}$.

Vamos a necesitar:

1. Alguna propiedad que relacione la completitud de $\mathbb{R}$.

Teorema de polinomios reales

Todo polinomio real de grado impar posee raíces reales.

Receta

Vamos a necesitar:

1. Alguna propiedad que relacione la completitud de $\mathbb{R}$.

Teorema de polinomios reales

Todo polinomio real de grado impar posee raíces reales.

2. El hecho de que $\mathbb{C}$ es cerrado por raíces cuadradas.

Vamos a necesitar:

1. Alguna propiedad que relacione la completitud de $\mathbb{R}$.

Teorema de polinomios reales

Todo polinomio real de grado impar posee raíces reales.

2. El hecho de que $\mathbb{C}$ es cerrado por raíces cuadradas.
3. Y un elemento sorpresa...

$P(k, d, r)$

Se dice que se cumple la propiedad $P(k, d, r)$ si para todo conjunto $\{A_1, \ldots, A_r\}$ de matrices cuadradas u operadores lineales sobre k^n con $d \nmid n$ cuya **composición o producto conmuta** posee un autovector en común.

Receta

Vamos a necesitar:

1. Alguna propiedad que relacione la completitud de $\mathbb{R}$.

Teorema de polinomios reales

Todo polinomio real de grado impar posee raíces reales.

2. El hecho de que $\mathbb{C}$ es cerrado por raíces cuadradas.
3. Y un elemento sorpresa...

$P(k, d, r)$

Se dice que se cumple la propiedad $P(k, d, r)$ si para todo conjunto $\{A_1, \dots, A_r\}$ de matrices cuadradas u operadores lineales sobre k^n con $d \nmid n$ cuya **composición o producto conmuta** posee un autovector en común.

Ejemplo: $P(\mathbb{R}, 2, 1)$ significa que toda matriz de orden impar posee un autovector.

Estrategia

Para poder probar que toda matriz compleja posee autovalores mediante nuestra propiedad mágica veamos que $P(\mathbb{C}, 2^n, 1)$ significa que toda matriz compleja de orden $m \times m$ con $2^n \nmid m$ posee autovalores.
Así que probaremos, por inducción, que $P(\mathbb{C}, 2^n, 1)$ siempre se cumple para todo n.

La demostración

Lema

Si se cumple $P(k,d,1)$ entonces se cumple $P(k,d,r)$ para todo $r>0$.

Demostración.

Probaremos el paso inductivo $P(k,d,r+1)$ por inducción fuerte sobre la dimensión n del espacio. El caso base ($n=1$) es trivial.
Sean $\{A_1,\dots,A_r,A_{r+1}\}$ matrices conmutativas en k^{n+1} con $d\nmid n+1$.
Por $P(k,d,1)$ se cumple que A_{r+1} posee un autovalor $\lambda\in k$, y así definimos $B:=A_{r+1}-\lambda I$ que claramente conmuta con el resto de A_is y se definen:

$$U:=\ker(B),\quad W:=\operatorname{Img}(B).$$

Probaremos que U,W son invariantes para todos los operadores: Si $\vec{u}\in U$, entonces

$$A_i(B(\vec{u}))=A_i(\vec{0})=\vec{0}=B(A_i(\vec{u})),$$

de modo que $A_i(\vec{u})\in U$. $\square$

Demostración.

Si $\vec{w} \in W$, entonces por definición existe $\vec{v} \in k^{n+1}$ tal que $B(\vec{v}) = \vec{w}$, luego

$$A_i(\vec{w}) = A_i(B(\vec{v})) = B(A_i(\vec{v})) \in W.$$

Si $U = k^{n+1}$ entonces todos son autovectores de A_{r+1}.
Si $U \neq k^{n+1}$ entonces como $\dim U + \dim W = n + 1$ se cumple que al menos uno de ellos posee dimensión no divisible por d. Supongamos que U lo es, como $\dim U < n + 1$ por inducción $\{A_1, \ldots, A_{r+1}\}$ poseen un autovector común en U. $\square$

Una observación

Veamos que si A es una matríz de $\mathrm{Mat}_m(\mathbb{R})$ con m impar, entonces

$$p_A(x) = x^m + \cdots$$

luego, por TPR se cumple que $p_A(x)$ posee una raíz λ, i.e., un autovalor de A.
Es decir, se cumple $P(\mathbb{R}, 2, 1)$ y nuestro lema asegura que se cumple $P(\mathbb{R}, 2, r)$.

Si $A, B \in \mathrm{Mat}_n(\mathbb{C})$ entonces

$$AB = \underbrace{\frac{AB + B^*A^*}{2}}_{=:L_1(B)} + i \cdot \underbrace{\frac{AB - B^*A^*}{2i}}_{=:L_2(B)}$$

donde $L_1(B)^* = L_1(B)$ y $L_2(B)^* = L_2(B)$.
Así que si B fuese autoadjunta se cumpliría que $L_1(B)$ y $L_2(B)$ también.

Lema

Se cumple $P(\mathbb{C}, 2, 1)$.

Demostración.

Sea n impar, $A \in \mathrm{Mat}_n(\mathbb{C})$ cualquiera y V el espacio de matrices auto-adjuntas de $\mathrm{Mat}_n(\mathbb{C})$ tomado como $\mathbb{R}$-espacio vectorial. Como vimos, L_1, L_2 (definidos como antes) son operadores lineales sobre V. Veamos que conmutan:

$$\begin{aligned} L_1(L_2(B)) = L_1\left(\frac{AB - BA^*}{2i}\right) &= \frac{1}{4i}[A(AB - BA^*) + (AB - BA^*)A^*] \\ &= \frac{1}{4i}[AAB + ABA^* - (ABA^* + BA^*A^*)] \\ &= \frac{1}{4i}[A(AB + BA^*) - (AB + BA^*)A^*] = L_2(L_1(B)). \end{aligned}$$

$\square$

Demostración.

Nótese que $\dim_{\mathbb{R}} V = n^2$ que es impar. Luego, como se cumple $P(\mathbb{R}, 2, 2)$, entonces L_1, L_2 poseen un autovector en común B, de modo que $L_1(B) = \alpha B$ y $L_2(B) = \beta B$ y se cumple que

$$AB = L_1(B) + iL_2(B) = (\alpha + i\beta)B.$$

de modo que A posee un autovalor complejo $\alpha + i\beta$. $\square$

Teorema

Para todo n se cumple $P(\mathbb{C}, 2^n, 1)$.

Demostración.

Lo haremos por inducción fuerte sobre n, donde en el lema anterior probamos el caso base.
Sea $A \in \mathrm{Mat}_m(\mathbb{C})$ con $2^n \mid m$ y $2^{n+1} \nmid m$. Sea V el conjunto formado por matrices anti-simétricas (i.e., $B \in V$ cumple $B^t = -B$) resulta ser un $\mathbb{C}$-espacio vectorial, cuya dimensión es $\dfrac{m(m-1)}{2}$ de modo que $2^n \nmid \dim V$. Si definimos L_1, L_2 por

$$L_1(B) := AB - BA^t, \quad L_2(B) := ABA^t$$

éstos cumplen ser operadores lineales que conmutan. $\square$

Demostración.

Luego por hipótesis inductiva se cumple que admiten un autovector común B.

$$L_1(B) = \lambda B, \quad L_2(B) = \mu B = A(BA^t) = A(AB - L_1(B))$$

despejando

$$(A^2 - \lambda A - \mu I)B = 0.$$

Pero como $\mathbb{C}$ admite raíces a todo polinomio cuadrático, entonces existen $\alpha, \beta \in \mathbb{C}$ tales que

$$x^2 - \lambda x + \mu = (x - \alpha)(x - \beta),$$

Si $\vec{v}$ es una columna no nula de B, entonces se obtiene que

$$(A - \alpha I)(A - \beta I)\vec{v} = 0$$

con lo que o $\vec{v}$ es autovector de A, o $(A - \beta I)\vec{v}$ lo es. $\square$

Prólogo

Prólogo

Importancia del teorema

Como saben, no existe $x \in \mathbb{R}$ tal que $x^2 = -1$...

Como saben, no existe $x \in \mathbb{R}$ tal que $x^2 = -1$... ¡Así que inventamos un número mágico i tal que $i^2 = -1$ xDDdddDdDDDd!

Construcción de $\mathbb{C}$ (según la educación media)

Como saben, no existe $x \in \mathbb{R}$ tal que $x^2 = -1$... ¡Así que inventamos un número mágico i tal que $i^2 = -1$ xDDdddDdDDDd!
Luego si definimos $\mathbb{C} := \{a + ib : a, b \in \mathbb{R}\}$ entonces $\mathbb{C}$ resulta ser un cuerpo?!

Construcción de $\mathbb{C}$ (según la educación media)

Como saben, no existe $x \in \mathbb{R}$ tal que $x^2 = -1$... ¡Así que inventamos un número mágico i tal que $i^2 = -1$ xDDdddDdDDDd!
Luego si definimos $\mathbb{C} := \{a + ib : a, b \in \mathbb{R}\}$ entonces $\mathbb{C}$ resulta ser un cuerpo?!

Como saben, no existe $x \in \mathbb{R}$ tal que $x^2 = -1$... ¡Así que inventamos un número mágico i tal que $i^2 = -1$ xDDdddDdDDDd!
Luego si definimos $\mathbb{C} := \{a + ib : a, b \in \mathbb{R}\}$ entonces $\mathbb{C}$ resulta ser un cuerpo?!

¿Y por qué no hacer lo mismo con otros problemas sin solución? ¿Por qué no definir α tal que $\sin \alpha = 2$, o β tal que $\log \beta = 0$?

Teorema de Kronecker

Si k es un cuerpo y $p(x) \in k[x]$ no constante y sin raíces, entonces existe un cuerpo K tal que $k \subseteq K$ y $p(x)$ posee raíces en K.

Teorema de Kronecker

Si k es un cuerpo y $p(x) \in k[x]$ no constante y sin raíces, entonces existe un cuerpo K tal que $k \subseteq K$ y $p(x)$ posee raíces en K.

Conclusión: La importancia del TFA se atribuye a que nos dice que $\mathbb{C}$ no posee extensiones algebraícas, lo que significa que $\mathbb{C}$ posee "todos los números que podríamos necesitar".
Ésta es también la razón de que Gauss critíque el nombre de "números imaginarios" pues son tan reales como los reales.

El camino más corto entre dos verdades del análisis real pasa por el análisis complejo.

–Jacques Hadamard

Generalizaciones...

- ¿Existen otros cuerpos K/k tales que $K = k(i)$ y K es la clausura algebraíca de k?

- ¿Existen otros cuerpos K/k tales que $K = k(i)$ y K es la clausura algebraíca de k?
  ¡Sí! De hecho, $\mathbb{R}_a$ (números reales algebraícos) cumple con todos las propiedades que usamos de $\mathbb{R}$, así que nuestra demostración también se aplica para ver que $\mathbb{C}_a$ (complejos algebraícos) es algebraícamente cerrado.

- ¿Existen otros cuerpos K/k tales que $K = k(i)$ y K es la clausura algebraíca de k?
  ¡Sí! De hecho, $\mathbb{R}_a$ (números reales algebraícos) cumple con todos las propiedades que usamos de $\mathbb{R}$, así que nuestra demostración también se aplica para ver que $\mathbb{C}_a$ (complejos algebraícos) es algebraícamente cerrado.
- ¿Pero existen cuerpos que **no** se parezcan a $\mathbb{R}$ y a $\mathbb{C}$?

Generalizaciones...

- ¿Existen otros cuerpos K/k tales que $K = k(i)$ y K es la clausura algebraíca de k?
  ¡Sí! De hecho, $\mathbb{R}_a$ (números reales algebraícos) cumple con todos las propiedades que usamos de $\mathbb{R}$, así que nuestra demostración también se aplica para ver que $\mathbb{C}_a$ (complejos algebraícos) es algebraícamente cerrado.
- ¿Pero existen cuerpos que **no** se parezcan a $\mathbb{R}$ y a $\mathbb{C}$?
  ¡No, véase teorema de Artin-Schreier!

Bibliografía

1. Derksen, H. The Fundamental Theorem of Algebra and Linear Algebra. *The American Mathematical Monthly* (2003).
2. Fine, B. y Rosenberger, G. *The Fundamental Theorem of Algebra.* (Springer-Verlag New York, 1997).