Cerraduras algebraicas y campos algebraicamente cerrados

Facultad de Ciencias UNAM

Introducción

En las secciones 2.9 y 2.10 demostramos la existencia y unicidad de una extensión de campos que contiene a todas las raíces de un polinomio dado[1]. En el proceso vimos que esta extensión es finita[2] y por lo tanto, algebraica.

En esta sección demostramos la existencia y unicidad de una extensión algebraica que contiene a todas las raíces de *todos* los polinomios sobre un campo.

[1] Por supuesto, nos referimos al campo de descomposición del polinomio dado.

[2] Recuerda que es $F(\alpha_1, \ldots, \alpha_n)$ donde $\alpha_1, \ldots, \alpha_n$ son las raíces del polinomio.

Cerraduras algebraicas

Definición

Supongamos que E/F es una extensión de campos. Decimos que E es una **cerradura algebraica de** F si

1. E es algebraico sobre F y
2. todo $f(x) \in F[x]$ se descompone en E/F.

Notemos que la condición (2) es equivalente a que E contenga todas las raíces de todos los polinomios con coeficientes en F.

Como esta notación, lo mencionado en el objetivo de la sección (mencionado en la introducción) se puede decir de la siguiente manera: Dado un campo F, existe una única cerradura algebraica de F.

Para lograr nuestro objetivo, resulta útil la siguiente definición.

Campos algebraicamente cerrados

Definición

Supongamos que K es un campo. Decimos que K es **algebraicamente cerrado** si todo polinomio con coeficientes en K tiene una raíz en K.

Por ejemplo, ya sabes (pero demostramos) que $\mathbb{C}$ es algebraicamente cerrado.

En la siguiente proposición, veremos que la condición que define a los campos algebraicamente cerrados es mas mucho fuerte de lo que parece.

Un campo algebraicamente cerrado contiene *todas* las raíces de *todos* sus polinomios

Proposición 1

Supongamos que K es un campo algebraicamente cerrado. Si $f(x) \in K[x]$, entonces $f(x) \in K[x]$ se descompone en K/K.

Demostración. Supongamos que $f(x) \in K[x]$. Como K es algebraicamente cerrado, existe $\alpha_1 \in K$ que es raíz de $f(x)$. En particular, $(x - \alpha_1)$ divide a $f(x)$ en $K[x]$ y por lo tanto existe $g_1(x) \in K[x]$ tal que

$$f(x) = (x - \alpha_1)g_1(x). \tag{1}$$

De nuevo, como $g_1(x) \in K[x]$ y K es algebraicamente cerrado, entonces existe $\alpha_2 \in K$ que es raíz de $g_1(x)$. En particular, existe $g_2(x)$ en $K[x]$ tal que

$$g_1(x) = (x - \alpha_2)g_2(x). \tag{2}$$

Sustituyendo (2) en (1) obtenemos

$$f(x) = (x - \alpha_1)(x - \alpha_2)g_2(x).$$

Continuando de esta manera obtenemos lo deseado. □

K es una cerradura de $K \iff K$ es cerrado

Corolario 2

Si K es un campo, entonces K es una cerradura algebraica de K si y solo si K es algebraicamente cerrado.

Demostración.

$\Longrightarrow$) Supongamos que K es una cerradura algebraica de K. Entonces (por definición de cerradura algebraica) todo polinomio con coeficientes en K se descompone en K/K. En particular, todo polinomio con coeficientes en K tiene una raíz en K.

$\Longleftarrow$) Supongamos que K es algebraicamente cerrado. Para ver que K es una cerradura algebraica de K necesitamos ver que

1. K es algebraico sobre K y
2. todo $f(x) \in K[x]$ se descompone en K/K.

El primer inciso es trivial y el segundo es consecuencia inmediata de la proposición anterior.

□

E cerradura algebraica $\Longrightarrow$ E algebraicamente cerrado

Proposición 3

Supongamos que F es un campo. Si E es una cerradura algebraica de F, entonces E es algebraicamente cerrado.

Demostración. Supongamos que E es una cerradura algebraica de F. Queremos ver que todo polinomio con coeficientes en E tiene una raíz en E.

Para esto, supongamos que $f(x) \in E[x]$. Sea α una raíz de $f(x)$ y consideremos el campo $E(\alpha)$. Evidentemente, $E(\alpha)$ es una extensión finita de E y por lo tanto también es algebraica (c.f. proposición 2.6.5).

Mas aun, como E es algebraica sobre F (por definición de cerradura algebraica) y (ii) la propiedad "es algebraico sobre" es transitiva (c.f. proposición 2.7.11), entonces $E(\alpha)$ es algebraico sobre F. En particular, como $\alpha \in E(\alpha)$, entonces existe un polinomio $g(x) \in E[x]$ tal que $g(\alpha) = 0$.

Finalmente, como (i) E es una cerradura algebraica de F y (ii) las cerraduras algebraicas contienen todas las raíces de todos los polinomios con coeficientes en el campo base, entonces $\alpha \in E$. $\square$

Observación

Nuestro objetivo ahora es demostrar que todo campo tiene una cerradura algebraica. Específicamente, para todo campo F queremos construir una extensión K/F tal que

1. K es una extensión algebraica de F.
2. K contiene todas las raíces de todos los polinomios con coeficientes en F.

Dado un polinomio $f(x) \in F[x]$, ya sabemos que el campo de descomposición K_f de $f(x)$ sobre F satisface

1. K_f es una extensión algebraica de F. (Recuerda que si $\alpha_1, \ldots, \alpha_n$ son las raíces de $f(x)$ en K_f, entonces $K_f \cong F(\alpha_1, \ldots, \alpha_n)$ y toda extensión finita es algebraica.)
2. K_f contiene todas las raíces de $f(x)$.

Una idea para encontrar K podría ser considerar el campo generado por todos los K_f. Pero ¿"generado" *donde*? Recuerda que la idea de campo generado depende de que haya un campo que contenga a los generadores, y en principio no conocemos ningún campo que contenga a todos K_f.

Veamos que para una cantidad finita de polinomios, la idea anterior funciona.

Dados $f(x), g(x) \in F[x]$ queremos construir una extensión $K_{f,g}$ tal que

1. $K_{f,g}$ es una extensión algebraica de F
2. K contiene todas las raíces de $f(x)$ y $g(x)$.

Es fácil verificar que el campo de descomposición del producto $f(x)g(x)$ sobre F cumple lo deseado.

Obviamente, en general tenemos la siguiente proposición.

Proposición 4

Supongamos que F es un campo y que $f_1(x), f_2(x), \ldots, f_n(x) \in F[x]$. Si F' es el campo de descomposición de $f_1(x)f_2(x)\cdots f_n(x)$ sobre F, entonces

1. F' es una extensión algebraica (finita) de F y
2. F' contiene a todas las raíces de $f_i(x)$ para toda $i = 1, \ldots, n$.

En particular, para cualquier cantidad finita de polinomios existe una extensión finita en donde viven las raíces de estos polinomios.

Comentario

Usando el lema de Zorn y la idea de la proposición anterior se puede encontrar una extensión algebraica de F. Sin embargo, este camino es tedioso y por eso damos una demostración alternativa que de hecho, tiene varias similitudes con la demostración del teorema de existencia de raíces en una extensión.

En el camino que tomaremos primero demostraremos que todo campo esta contenido en un campo algebraicamente cerrado. Luego, el hecho de que todo campo tiene una cerradura algebraica sera corolario de este resultado.

Antes de demostrar que todo campo esta contenido en un campo algebraicamente cerrado, introducimos un concepto que usaremos en su demostración: el concepto de anillo de polinomios en una cantidad arbitraria de variables

Polinomios sobre una cantidad arbitraria de variables

Supongamos que R es un anillo y que $\{x_i\}_{i\in I}$ es un conjunto arbitrario de variables indeterminadas. Un **polinomio en** $\{x_i\}_{i\in I}$ **con coeficientes en** R es una suma finita de elementos de la forma

$$ax_{i_1}^{d_1}\cdots x_{i_n}^{d_n}$$

donde $a \in R$, $n \in \mathbb{Z}_{\geq 0}$, y $x_{i_1}, \ldots, x_{i_n} \in \{x_i\}_{i\in I}$.

Al conjunto de todos los polinomios en $\{x_i\}_{i\in I}$ con coeficientes en R lo denotamos por $R\left[\{x_i\}_{i\in I}\right]$ y lo llamamos **el anillo de polinomios en** $\{x_i\}_{i\in I}$ **sobre** R.

Para operar a dos elementos de $R\left[\{x_i\}_{i\in I}\right]$, nota que en tu operación solo aparece una cantidad finita de variables y opera a los polinomios de la misma manera que lo harías en el anillo de polinomios sobre estas variables. Si no queda claro como operar, considera la siguiente igualdad

$$R\left[\{x_i\}_{i\in I}\right] = \bigcup_{x_1,\ldots,x_n\in\{x_i\}_{i\in I}} R[x_1,\ldots,x_n].$$

Para todo campo existe una extensión en donde cada uno de sus polinomios tiene una raíz

Lema 5

Si F es un campo, entonces existe una extensión de campos K/F tal que para toda $f(x) \in F[x]$ existe una raíz de $f(x)$ en K.

Demostración. Supongamos que F es un campo y para cada polinomio mónico no constante $p(x) \in F[x]$ sea x_p una variable indeterminada. Denotemos por $F[\dots, x_p, \dots]$ a los polinomios con coeficientes en F y variables en $\{x_p \mid p(x) \in F[x] \text{ es mónico no constante } \}$. Específicamente, sea

$$F[\dots, x_p, \dots] := F\left[\left\{x_p \mid p(x) \in F[x] \text{ es mónico no constante } \right\}\right].$$

Naturalmente, a los elementos de $F[\dots, x_p, \dots]$ los denotamos por

$$g(\dots, x_f, \dots).$$

Mas aun, para cada cada polinomio mónico no constante $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ denotamos

$$f(x_f) \coloneqq (x_f)^n + a_{n-1}(x_f)^{n-1} + \cdots + a_1 x_f + a_0 \in F[\ldots, x_p, \ldots].$$

Considera el ideal $I \subset F[\ldots, x_f, \ldots]$ generado por estos elementos. Específicamente,

$$I \coloneqq \left(\left\{ f(x_f) \mid f(x) \in F[x] \text{ es mónico no constante } \right\} \right).$$

Recuerda que si R es un anillo conmutativo arbitrario y A es un subconjunto de R, entonces (A) es precisamente el conjunto de las sumas finitas de elementos de la forma ra con $r \in R$ y $a \in A$. Por lo tanto,

$$I = \Big\{ g_1(\ldots, x_p, \ldots) f_1(x_{f_1}) + \cdots + g_n(\ldots, x_p, \ldots) f_n(x_{f_n}) \;\Big|\; n \in \mathbb{Z}_{\geq 1},\ \ g_i(\ldots, x_p, \ldots) \in F[\ldots, x_p, \ldots],\ \text{y}\ f_i(x) \in F[x] \text{ es mónico no constante} \Big\}.$$

Veamos que I es un ideal propio de $F[\dots, x_p, \dots]$.

Para esto, supongamos lo contrario. En particular $1 \in I$ y por lo tanto, existen

- $n \in \mathbb{Z}_{\geq 1}$,
- $g_1(\dots, x_p, \dots), \ \dots \ , g_n(\dots, x_p, \dots) \in F[\dots, x_p, \dots]$, y
- $f_1(x), \dots, f_n(x) \in F[x]$ mónicos no constantes

tales que

$$g_1(\dots, x_p, \dots) f_1(x_{f_1}) + \cdots + g_n(\dots, x_p, \dots) f_n(x_{f_n}) = 1. \tag{3}$$

Ahora bien, por la proposición 4, sabemos que existe una extensión F'/F que para cada $i \in \{1, \dots, n\}$ contiene una raíz α_i de $f_i(x)$. Evaluando $x_{f_1} = \alpha_i$ en (3) obtenemos[3]

$$g_1(\dots, x_p, \dots) \cancelto{0}{f_1(\alpha_1)} + \cdots + g_n(\dots, x_p, \dots) \cancelto{0}{f_n(\alpha_n)} = 1$$

Es decir, $0 = 1$. Una contradicción.

Por lo tanto, I es un ideal propio de $F[\dots, x_p, \dots]$.

[3] No hay ningún problema con evaluar elementos de F' en (3) porque (3) es una ecuación en $F[\dots, x_p, \dots]$ y como este campo esta contenido en $F'[\dots, x_p, \dots]$, entonces (3) también es una ecuación en $F'[\dots, x_p, \dots]$.

Recordemos que en la proposición 1.11.2 demostramos (usando el lema de Zorn) que todo ideal propio de un anillo con 1 esta contenido en un ideal maximal. En particular, el ideal I esta contenido en un ideal maximal $\mathcal{M}$ de $F[\dots, x_p, \dots]$.

Como $\mathcal{M}$ es maximal, el cociente

$$K \coloneqq F[\dots, x_p, \dots]/\mathcal{M}$$

es un campo. Además, K contiene una copia isomorfa de F (el homomorfismo $a \mapsto a + \mathcal{M}$ es inyectivo porque su kernel es trivial: $\mathcal{M}$ no contiene ningún polinomio constante por definición). Por eso, de ahora en adelante tratamos a F como subconjunto de K.

Mas aun, para todo $g(\dots, x_p, \dots) \in F[\dots, x_p, \dots]$ denotemos

$$\overline{g(\dots, x_p, \dots)} \coloneqq g(\dots, x_p, \dots) + \mathcal{M}.$$

Es decir, $\overline{g(\dots, x_p, \dots)}$ es la clase de equivalencia de $g(\dots, x_p, \dots)$ en K.

Finalmente, veamos que para toda $f(x) \in F[x]$ existe una raíz de $f(x)$ en K.

Notemos que basta probar que para toda $f(x) \in F[x]$ mónico no constante existe una raíz de $f(x)$. Como para toda $p(x) \in F[x]$ y toda $a \in F$ las raíces de $a \cdot p(x)$ y $p(x)$ coinciden, basta probar el resultado para polinomios mónicos no constantes.

Por lo tanto supongamos que $f(x) = x^n + a_{n-1}x^{n-1} \cdots + a_1 x a_0$. Evaluando $\overline{x_f}$ en $f(x)$ obtenemos[4]

$$\begin{aligned} f(\overline{x_f}) &= (\overline{x_f})^n + a_{n-1}(\overline{x_f})^{n-1} \cdots + a_1\overline{x_f} + a_0 \\ &= \overline{(x_f)^n + a_{n-1}(x_f)^{n-1} + \cdots + a_1 x_f + a_0} \\ &= \overline{f(x_f)} \\ &= f(x_f) + \mathcal{M} \\ &= 0 + \mathcal{M} && (\text{pues } f(x_f) \in \mathcal{M}) \\ &= 0_K. \end{aligned}$$

Por lo tanto, para toda $f(x) \in F[x]$ existe una raíz de $f(x)$ en K. □

[4]De nuevo, no hay problema con evaluar $\overline{x_f} \in K$ en $f(x)$ porque como estamos considerando $F \subset K$, entonces $f(x) \in F[x] \subset K[x]$.

Todo campo esta contenido en un campo algebraicamente cerrado

Teorema 6

Si F es un campo, entonces existe un campo algebraicamente cerrado K que contiene a F.

Demostración. Supongamos que F es un campo. Por el lema anterior, existe una extensión de campos K_1/F tal que para toda $f(x) \in F[x]$ existe una raíz de $f(x)$ en K_1.

Análogamente, como K_1 es un campo, por el lema anterior, existe una extensión de campos K_2/F tal que para toda $f(x) \in K_1[x]$ existe una raíz de $f(x)$ en K_2.

Continuando de esta manera obtenemos una sucesión de campos

$$K_0 \coloneqq F \subset K_1 \subset K_2 \subset \cdots \subset K_j \subset K_{j+1} \subset \cdots$$

tal que para toda $j \in \mathbb{Z}_{\geq 0}$ y todo $f(x) \in F_j[x]$ existe una raíz de $f(x)$ en K_{j+1}. Naturalmente, definimos

$$K \coloneqq \bigcup_{j \geq 0} K_j.$$

Veamos que K es algebraicamente cerrado (dejamos al lector verificar que en efecto es un campo)[5].

Queremos ver que para todo $f(x) \in K[x]$ existe una raíz de $f(x)$ en K. Por eso, supongamos que $f(x) \in K[x]$. Por definición de K, cada uno de sus coeficientes pertenece a algún K_j. Sea N el máximo de estas j. Entonces $f(x) \in K_N[x]$ y por lo mencionado anteriormente, existe una raíz de $f(x)$ en $K_{N+1} \subset K$. □

[5] Es consecuencia inmediata de que es una unión de campos anidados.

Todo campo tiene una cerradura algebraica

Proposición 7

Si F es un campo, entonces existe una extensión E/F que es una cerradura algebraica de F.

Demostración. Supongamos que F es un campo. Por el teorema anterior existe un campo algebraicamente cerrado K que contiene a F. Definimos

$$E \coloneqq \{a \in K \mid a \text{ es algebraico sobre } F\}.$$

Dejamos al lector la tarea de verificar que E es un subcampo de K. Además, (por definición) E es algebraico sobre F. Resta probar que todo $f(x) \in F[x]$ se descompone en E/F. Por eso, supongamos que $f(x) \in F[x]$. Como $f(x)$ también pertenece a $K[x]$ y K es algebraicamente cerrado, entonces (por la proposición 1) $f(x) \in F[x]$ se descompone en K/F, digamos

$$f(x) = c \cdot (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \tag{4}$$

con $c \in F$ y $\alpha_1, \ldots, \alpha_n \in K$. Sin embargo, cada α_i es raíz de $f(x) \in F[x]$ y por lo tanto, cada α_i es algebraico sobre F o equivalentemente (por definición de E), $\alpha_i \in E$ para toda i. En particular, $(x - \alpha_i) \in E[x]$ y por lo tanto (4) demuestra que $f(x)$ se descompone en E/F. $\square$

Unicidad de la cerradura algebraica

Proposición 8

Supongamos que F es un campo. Si E/F y E'/F son cerraduras algebraicas de F, entonces $E \cong E'$.

La demostración requiere una aplicación muy trucuelenta del lema de Zorn, y por eso la omitimos. Al lector interesado, lo referimos a la siguiente respuesta en Stack Exchange.

https://math.stackexchange.com/a/2585337