LOS TEOREMAS DE STEINITZ EN LA TEORÍA DE CAMPOS

LUIS MIGUEL VILLEGAS SILVA

RESUMEN. En este trabajo presentamos la demostración de dos teoremas de E. Steinitz. A saber, la existencia de la cerradura algebraica de campos y que dos campos de la misma característica y cardinalidad innumerable son isomorfos. La intención es presentar una prueba detallada, en lo que a teoría de modelos y de conjuntos respecta, de estos resultados importantes.

1. INTRODUCCIÓN

Un resultado bien conocido en teoría de campos afirma que todo campo K tiene una extensión K' que es algebraicamente cerrada. Esto es, cualquier polinómio con coeficientes en K' tiene sus raíces en K'. La demostración original debida a E. Steinitz recurre al teorema de recursión transfinita. Posteriormente, E. Artin [Ar88] desarrolló una demostración «más algebraica» de este resultado, para aliviar en la medida de lo posible, la ignorancia conjuntista de la inmensa mayoría de los algebristas de aquel entonces. Sin embargo, la demostración original es ciertamente más elegante y sencilla. No obstante, la demostración original debida a Steinitz es poco amigable y no totalmente formal. Existe una presentación posterior debida a Van der Waerden [Wa66] pero que tampoco incluye los detalles importantes de teoría de conjuntos.

En este artículo presento los detalles necesarios mencionados explicados claramente, en particular el uso del teorema de recursión. Más aun, en la prueba de la isomorfía de dos campos de la misma característica y cardinalidad se evita el uso del teorema de categoricidad de Morley, figura recurrente en la prueba de este teorema en los textos de teoría de modelos. Suponemos conocidos por el lector diversos resultados puramente algebraicos de la teoría de campos, pero damos una referencia para revisar la demostración en caso de necesidad. También suponemos conocimientos básicos sobre aritmética cardinal, teorema de recursión y teoría de modelos. Los resultados aquí presentados son conocidos.

2. TEORÍA DE MODELOS

Trabajeremos en el lenguaje formal $\mathscr{L} = \{+, \cdot, 0, 1\}$, donde $+, \cdot$ son funciones (operaciones) binarias y 0,1 símbolos de constante, cuya interpretación es la que es de esperarse.

Definición 2.1. Sea φ un $\mathscr{L}$-enunciado,

(a)

$$Mod^{\mathscr{L}}(\varphi) = \{\mathfrak{A} : \mathfrak{A} \models \varphi, \mathfrak{A} \text{ es una } \mathscr{L}\text{-estructura}\}.$$

Sea $\mathfrak{K}$ una clase de $\mathscr{L}$-estructuras.

(b) $\mathfrak{K}$ es *elemental o finito axiomatizable* si existe un $\mathscr{L}$-enunciado φ tal que $\mathfrak{K} = Mod^{\mathscr{L}}(\varphi)$.

(c) $\mathfrak{K}$ es *Δ-elemental* si existe un conjunto de $\mathscr{L}$-enunciados Φ tal que $\mathfrak{K} = Mod^{\mathscr{L}}(\Phi)$; en este caso decimos que $\mathfrak{K}$ es axiomatizable por Φ.

2010 *Mathematics Subject Classification.* 03C35, 03C60, 03C98, 03E75.

Key words and phrases. Cerradura algebraica, categoricidad, teorema de recursión transfinita, teorema de Morley.

Teorema 2.2. *Sea $\mathfrak{K}$ una clase de $\mathscr{L}$-estructuras.*

(a) $\mathfrak{K}$ es elemental si y sólo si, tanto $\mathfrak{K}$ como su clase complementaria

$$\mathfrak{K}^* \equiv \{\mathfrak{A} : \mathfrak{A} \text{ es una } \mathscr{L}\text{-estructura }, \mathfrak{A} \notin \mathfrak{K}\}$$

son Δ-elementales.

(b) Si $\mathfrak{K} = Mod^{\mathscr{L}}(\Phi)$, entonces $\mathfrak{K}$ es elemental si y sólo si existe un subconjunto finito Φ' de Φ con $\mathfrak{K} = Mod^{\mathscr{L}}(\Phi')$.

Demostración. (a) ($\Rightarrow$) Sea $\mathfrak{K}$ elemental, digamos $\mathfrak{K} = Mod^L(\varphi)$. Entonces $\mathfrak{K}^* = Mod^L(\neg\varphi)$.

($\Leftarrow$) Sean $\mathfrak{K}$ y $\mathfrak{K}^*$ clases Δ-elementales, digamos $\mathfrak{K} = Mod^L(\Phi)$ y $\mathfrak{K}^* = Mod^L(\Phi^*)$, donde Φ, Φ^* son conjuntos de $\mathscr{L}$-enunciados. Si $\mathfrak{K}$ no fuese elemental, existiría, para cada $\Phi' \subseteq \Phi$ una $\mathscr{L}$-estructura $\mathfrak{A}$ con $\mathfrak{A} \models \Phi'$ pero $\mathfrak{A} \not\models \Phi$. Lo último significa que $\mathfrak{A} \notin \mathfrak{K}$, por lo que $\mathfrak{A} \in \mathfrak{K}^*$ y por consiguiente, $\mathfrak{A} \models \Phi^*$. En consecuencia, $\Phi \cup \Phi^*$ es finito satisfacible y posee (por el teorema de compacidad) un modelo $\mathfrak{A}$. Puesto que $\mathfrak{K} \cap \mathfrak{K}^* = \emptyset$, esto no es posible. Por lo tanto, $\mathfrak{K}$ debe ser elemental.

(b) Sea $\mathfrak{K}$ elemental, digamos $\mathfrak{K} = Mod^{\mathscr{L}}(\varphi)$. Ya que también $\mathfrak{K} = Mod^{\mathscr{L}}(\Phi)$, se sigue que $\Phi \models \varphi$. Por el teorema de compacidad, sabemos que existe un subconjunto finito $\Phi' \subseteq \Phi$ con $\Phi' \models \varphi$. Así que $Mod^{\mathscr{L}}(\Phi') \subseteq Mod^{\mathscr{L}}(\varphi)$. Dado que $\Phi' \subseteq \Phi$, se cumple $Mod^{\mathscr{L}}(\Phi) \subseteq Mod^{\mathscr{L}}(\Phi')$. En resumen, $Mod^{\mathscr{L}}(\Phi') = Mod^{\mathscr{L}}(\Phi) = \mathfrak{K}$, como se afirmó. ❐

Definición 2.3. Sea κ un cardinal. Para cada $\alpha < \kappa$ sea $\mathfrak{A}_\alpha$ una $\mathscr{L}$-estructura, tal que $\mathfrak{A}_\alpha \subseteq \mathfrak{A}_\beta$ siempre que $\alpha < \beta$. Tal sucesión de modelos $(\mathfrak{A}_\alpha : \alpha < \kappa)$ se llama *una cadena* de $\mathscr{L}$-estructuras.

Convertimos $A = \bigcup_{\alpha<\kappa} A_\alpha$ en una $\mathscr{L}$-estructura $\mathfrak{A}$ como sigue.

$$R_i^{\mathfrak{A}} \equiv \bigcup_{\alpha<\kappa} R_i^{\mathfrak{A}_\alpha};$$
$$f_j^{\mathfrak{A}} \equiv \bigcup_{\alpha<\kappa} f_j^{\mathfrak{A}_\alpha};$$
$$c_k^{\mathfrak{A}} \equiv c_k^{\mathfrak{A}_\alpha}.$$

De la relación $\mathfrak{A}_\alpha \subseteq \mathfrak{A}_\beta$ se deduce fácilmente que realmente tenemos definida una $\mathscr{L}$-estructura sobre $\bigcup_{\alpha<\kappa} A_\alpha$. Esta estructura se denota con

$$\bigcup_{\alpha<\kappa} \mathfrak{A}_\alpha$$

y la llamamos la *unión de las* $\mathfrak{A}_\alpha$. De la construcción se desprende el siguiente resultado.

Lema 2.4. *Para $\alpha < \kappa$ se cumple $\mathfrak{A}_\alpha \subseteq \bigcup_{\beta<\kappa} \mathfrak{A}_\beta$.*

Teorema 2.5. *Sea φ un Π_2-enunciado de $\mathscr{L}$, es decir, un enunciado de la forma*

$$\varphi = \forall x_1, \ldots, x_m \exists y_1, \ldots y_n \psi(x_1, \ldots, x_m, y_1, \ldots, y_n),$$

donde ψ es una $\mathscr{L}$-fórmula sin cuantificadores. Si $\mathfrak{A}_\alpha \models \varphi$ para toda $\alpha < \kappa$, es cierto que $\bigcup_{\alpha<\kappa} \mathfrak{A}_\alpha \models \varphi$.

Demostración. Sean $A \equiv \bigcup_{\alpha<\kappa} A_\alpha$ el universo de $\bigcup_{\alpha<\kappa} \mathfrak{A}_\alpha$, y $a_1, \ldots, a_m \in A$ arbitrarios. Entonces existe una $\alpha < \kappa$ con $a_1, \ldots a_m \in A_\alpha$. Puesto que $\mathfrak{A}_\alpha \models \varphi$, existen $b_1, \ldots, b_n \in A_\alpha$ con

$$\mathfrak{A}_\alpha \models \psi[a_1, \ldots, a_m, b_1, \ldots b_n].$$

Ya que $\mathfrak{A}_\alpha \subseteq \bigcup_{\beta<\kappa}\mathfrak{A}_\beta$ y ψ está libre de cuantificadores, se deduce

$$\bigcup_{\beta<\kappa}\mathfrak{A}_\beta \models \psi[a_1,\ldots,a_m,b_1,\ldots,b_n],$$

dando paso a $\bigcup_{\beta<\kappa}\mathfrak{A}_\beta \models \exists y_1\ldots y_n\ \psi(x_1,\ldots,x_m,y_1,\ldots,y_n)\ [a_1,\ldots,a_m]$. En vista de que los $a_1,\ldots,a_m$ se eligieron arbitrariamente, se sigue

$$\bigcup_{\beta<\kappa}\mathfrak{A}_\beta \models \forall x_1\cdots x_m\exists y_1\cdots y_n\psi(x_1,\ldots,x_m,y_1,\ldots,y_n),$$

lo que se quería demostrar. ❐

Una consecuencia inmediata del teorema 2.5 se expone a continuación.

Corolario 2.6. *Si $\mathfrak{K}$ es axiomatizable mediante una teoría Φ, que consiste en Π_2-enunciados, entonces $\mathfrak{K}$ es cerrada respecto a uniones de cadenas, es decir, si κ es un cardinal y $(\mathfrak{A}_\alpha : \alpha<\kappa)$ es una cadena de modelos en $\mathfrak{K}$, también $\bigcup_{\alpha<\kappa}\mathfrak{A}_\alpha$ pertenece a $\mathfrak{K}$.*

De hecho, también la conversa es cierta, si $\mathfrak{K}$ es cerrada respecto a uniones de cadenas, $\mathfrak{K}$ es axiomatizable mediante un conjunto que consta sólo de Π_2-enunciados. La demostración se puede encontrar en [FeVill13, Teorema IV.5.7, pp. 316].

3. Existencia de la cerradura algebraica

Ahora probaremos la existencia de la cerradura algebraica de todo campo. Para ello presentamos primero la teoría de campos.

La $\mathscr{L}$-teoría Φ_{Camp} (la teoría de campos) consiste en los siguientes enunciados.

(i) $\forall v_0\forall v_1(v_0+v_1=v_1+v_0$ (conmutatividad de la suma).
(ii) $\forall v_0v_1v_2(v_0+(v_1+v_2)=(v_0+v_1)+v_2)$ (ley asociativa de la suma).
(iii) $\forall v_0(v_0+0=v_0)$ (0 es el elemento neutro para la suma).
(iv) $\forall v_0\exists v_1(v_0+v_1=0)$ (existencia de un elemento inverso).
(v) $\forall v_0\forall v_1(v_0\cdot v_1=v_1\cdot v_0)$ (ley conmutativa de la multiplicación).
(vi) $\forall v_0\forall v_1\forall v_2(v_0\cdot(v_1\cdot v_2)=(v_0\cdot v_1)\cdot v_2)$ (ley asociativa de la multiplicación).
(vii) $\forall v_0(v_0\cdot 1=v_0)$ (1 es elemento neutro de la multiplicación).
(viii) $\forall v_0\exists v_1(\neg v_0=0\rightarrow v_0\cdot v_1=1)$ (existencia de un inverso multiplicativo).
(ix) $\forall v_0\forall v_1\forall v_2(v_0\cdot(v_1+v_2)=v_0\cdot v_1+v_0\cdot v_2)$ (ley distributiva).
(x) $\neg 0=1$.

Φ_{camp} axiomatiza la clase de los modelos de los campos y se llama la teoría de los campos.

Definición 3.1. Un campo $\mathfrak{K}$ es algebraicamente cerrado si todo polinomio $p(x)=a_0+a_1x+\ldots+a_nx^n$ con coeficientes en $\mathfrak{K}$ se factoriza en factores lineales.

Una definición equivalente es que $\mathfrak{K}$ es algebraicamente cerrado si cualquier polinomio no constante $p(x)$ con coeficientes en $\mathfrak{K}$ tiene al menos una raíz en $\mathfrak{K}$ y por tanto un factor lineal. En efecto, si esta condición se satisface y si un polinomio arbitrario $p(x)$ se factoriza en factores irreducibles, estos sólo pueden ser lineales.

Definición 3.2. Si $\mathfrak{K}$ es un campo,

$$\mathfrak{K}[x]=\{a_0+a_1x+a_2x^2+\ldots+a_nx^n : a_0,a_1,\ldots,a_n\in\mathfrak{K}\}.$$

Teorema 3.3. *Sean $\mathfrak{K}$ un campo, $p(x)$ un polinomio mónico irreducible in $\mathfrak{K}[x]$ de grado d, $K = \mathfrak{K}[x]/(p)$ y $\beta = x+(p) \in K$. Se cumplen ls siguientes afirmaciones.*

(1) K es un campo y $K' = \{a+(p) : a \in \mathfrak{K}\}$ es un subcampo de K isomorfo a $\mathfrak{K}$. Así, si identificamos a K' con $\mathfrak{K}$ mediante $a \mapsto a+(p)$, $\mathfrak{K}$ es un subcampo de K.
(2) β es una raíz de p en K.
(3) Si $q(x) \in \mathfrak{K}[x]$ y β es raíz de q en K, entonces $p|q$ en $\mathfrak{K}[x]$.
(4) p es el único polinomio mónico irreducible en $\mathfrak{K}[x]$ que tiene a β como raíz.
(5) El conjunto finito $\{1, \beta, \beta^2, \ldots, \beta^{d-1}\}$ es una base para K como espacio vectorial sobre $\mathfrak{K}$, por lo que la dimensión de K es d.

Demostración. Véase [Ro15, Proposition A-3.84]. ❐

Definición 3.4. Si K es un campo que contiene a $\mathfrak{K}$ como subcampo, K se conoce como una extensión de $\mathfrak{K}$ y denotamos una extensión mediante

$$K/\mathfrak{K}.$$

Una extensión $K/\mathfrak{K}$ es una extensión finita, si K es un espacio vectorial de dimensión finita sobre $\mathfrak{K}$. La dimensión de K se denota como $[K : \mathfrak{K}]$ y se llama el grado de $K/\mathfrak{K}$.

Definición 3.5. Sea $K/\mathfrak{K}$ una extensión. Un elemento $\alpha \in K$ es algebraico sobe $\mathfrak{K}$ si existe un polinomio distinto de cero $p(x) \in \mathfrak{K}[x]$ que tiene a α como raíz; en otro caso, α es trascendente sobre $\mathfrak{K}$. Una extensión $K/\mathfrak{K}$ es algebraica cuando todo $\alpha \in K$ es algebraico sobre $\mathfrak{K}$.

Proposición 3.6. *Si $K/\mathfrak{K}$ es una extensión finita, entonces es una extensión algebraica.*

Demostración. Véase [Ro15, Proposition A-2.86]. ❐

Definición 3.7. Si $K/\mathfrak{K}$ es una extensión y $\alpha \in K$, el campo

$$\mathfrak{K}(\alpha)$$

es la intersección de los subcampos de K que contienen a $\mathfrak{K}$ y a α; $\mathfrak{K}(\alpha)$ se conoce como el subcampo de K que se obtiene al adjuntar α a $\mathfrak{K}$, en lugar de llamarlo el subcampo de K generado por $\mathfrak{K}$ y α.

En general, si A es un subconjunto de K (puede ser infinito), $\mathfrak{K}(A)$ es el subcampo de K generado por $\mathfrak{K}$ y A en K. Si $A = \{z_1, \ldots, z_n\}$, $\mathfrak{K}(A) = \mathfrak{K}(z_1, \ldots, z_n)$.

Teorema 3.8. *Si $K/\mathfrak{K}$ es una extensión y $\alpha \in K$ es algebraico sobre $\mathfrak{K}$, existe un único polinomio mónico e irreducible $p(x) \in \mathfrak{K}[x]$ que tiene a α como raíz. Más aún, $\mathfrak{K}[x]/(p) \cong \mathfrak{K}(\alpha)$. En efecto, existe un isomorfismo*

$$\varphi : \mathfrak{K}[x]/(p) \longrightarrow \mathfrak{K}(\alpha),$$

donde $\varphi(x+(p)) = \alpha$ y $\varphi(c+(p)) = c$ para cada $c \in \mathfrak{K}$.

Demostración. Véase [Ro15, Theorem A-3.87]. ❐

Teorema 3.9. *Sean $L \subseteq E \subseteq K$ campos tales que E es una extensión finita de L y K es una extensión finita de E. Entonces, K es una extensión finita de L y*

$$[K : L] = [K : E][E : L].$$

Demostración. Véase [Ro15, Theorem A-3.88]. ❐

Lema 3.10. *(1) Suponga que $L \subseteq K \subseteq E$ son campos tales que E/K y K/L son algebraicos, entonces E/L también es algebraico.*

(2) Suponga que la cadena

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq K_{n+1} \subseteq \cdots$$

es creciente y conformada por campos. Si K_{n+1}/K_n es algebraico para toda $n \in \mathbb{N}$, entonces $K = \bigcup_{n\in\mathbb{N}} K_n$ es un campo algebraico sobre K_0.

(3) Sea $K = \mathfrak{K}(A)$, esto es, K se obtiene de $\mathfrak{K}$ adjuntando los elementos del conjunto (puede ser infinito) A. Si cada $a \in A$ es algebraico sobre $\mathfrak{K}$, así lo es la extensión $K/\mathfrak{K}$.

Demostración. Véase [Ro15, Lemma B-2.38]. ❒

Lema 3.11. *Sea V un espacio vectorial infinito sobre el campo K de dimensión finita. Entonces $|V| \leq |K| + \aleph_0$.*

Demostración. Que V tenga dimensión finita significa que tiene una base $B = \{v_1, \ldots, v_n\}$ para alguna $n \in \mathbb{N}$. Esta base genera a V y los elementos de B son linealmente independientes. Así, cualquier elemento $z \in V$ se puede representar en forma única como,

$$z = k_1 v_1 + \cdots + k_n v_n,$$

donde $k_1, \ldots, k_n \in K$. En consecuencia, podemos establecer una inyección $f : V \longrightarrow \overbrace{K \times \cdots \times K}^{n \text{ veces}}$, mediante $f(z) = (k_1, \ldots, k_n)$, según se estableció arriba.

Si K es infinito, sabemos que $K^n = \overbrace{K \times \cdots \times K}^{n \text{ veces}}$ tiene cardinalidad igual a la de K mismo. Si K es finito, entonces $|K^n| = |K|^n$. En cualquier caso, se cumple $|V| \leq |K| + \aleph_0$, pues si K es finito, V también lo es; mientras qe si K es infinito, V tiene su mismo tamaño y el sumando $\aleph_0$ no desempeña ningún papel. ❒

Recuerde que si A es un conjunto infinito, la cardinalidad del conjunto de subconjuntos finitos de A es igual a la de A mismo. Esto se expresa como

$$|[A]^{<\omega}| = |A|.$$

Lema 3.12. *Si K es un campo de cardinalidad finita o infinita, entonces*

$$|K[x]| = \begin{cases} |K|, & \text{cuando } K \text{ es infinito} \\ \aleph_0, & \text{en otro caso} \end{cases}$$

Demostración. Por definición, $K[x]$ consiste en polinomios en la variable x, es decir, expresiones de la forma $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, para $n \in \mathbb{N}$. Propiamente, el polinomio $p(x)$ está determinado por la $n+1$-ada $(a_0, \ldots, a_n) \in K^{n+1}$.

Tenemos dos casos.

Caso I. K es finito.

$$\begin{aligned} |K[x]| &= \left| \bigcup_{n\in\mathbb{N}} K^n \right| \\ &= \sum_{n\in\mathbb{N}} |K^n| = \sum_{n\in\mathbb{N}} |K|^n = |K|^0 + |K|^1 + |K|^2 + \cdots + |K|^m + \cdots \end{aligned}$$

Note que del lado derecho aparecen potencias finitas de un número natural, y estas potencias crecen. No obstante, para cada potencia l podemos encontrar un natural k que la excede, y para cada natural n existe una potencia m que lo excede. Así que la suma del lado derecho es igual a $\sum_{n\in\mathbb{N}} n$.

Por otro lado, como $n < \aleph_0$, tenemos

$$\sum_{n\in\mathbb{N}} n \leq \sum_{n\in\mathbb{N}} \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0,$$

mientras que $\aleph_0 = \omega = \bigcup_{n\in\omega} n = \bigcup_{n\in\mathbb{N}} n$, por lo que $\aleph_0 \leq \sum_{n\in\mathbb{N}} n$. Estas dos desigualdades propician que $\sum_{n\in\mathbb{N}} n = \aleph_0$. Por consiguiente,

$$|K[x]| = \aleph_0.$$

Caso II. K es infinito. Cada elemento $a \in K$ da lugar a un polinomio constante, el polinomio $p(x) = a$, así que, $|K[x]| \geq |K|$. Por otro lado, como vimos antes, cada elemento de $K[x]$ está asociado a una única n-ada $(k_1, \ldots, k_n)$ de elementos de K. Por tanto,

$$|K[x]| \leq \left|\bigcup_{n\in\mathbb{N}} K^n\right| = \sum_{n\in\mathbb{N}} |K^n| = \sum_{n\in\mathbb{N}} |K| = \aleph_0 \cdot |K| = |K|.$$

(Recuerde que $|K^n| = |K|$ para cualquier $n \in \mathbb{N}$ cuando $|K|$ es infinita.) ❐

Ahora podemos enunciar nuestro teorema principal.

Teorema 3.13. *Sea $\mathfrak{K}$ un campo. Entonces existe una* cerradura algebraica *de $\mathfrak{K}$, es decir, un campo $\overline{\mathfrak{K}}$ que contiene a $\mathfrak{K}$ como subcampo, tal que*

(a) $\overline{\mathfrak{K}}$ es algebraicamente cerrado, es decir, todo polinomio no constante en $\overline{\mathfrak{K}}[x]$ tiene una raíz en $\overline{\mathfrak{K}}$.

(b) $\overline{\mathfrak{K}}$ es algebraico *sobre $\mathfrak{K}$, es decir, cada elemento de $\overline{\mathfrak{K}}$ es algebraico sobre $\mathfrak{K}$, por tanto, es el cero de un polinomio no trivial con coeficientes en $\mathfrak{K}$. Se cumple además $|\overline{\mathfrak{K}}| = |\mathfrak{K}| + \aleph_0$.*

Antes de presentar la prueba formal es importante entender la idea de la misma, la cual es ciertamente simple. De hecho, las pruebas «puramente algebraicas» sólo logran oscurecer innecesariamente esta idea.

Tenemos un campo $\mathfrak{K}$ y queremos construir un campo K que contenga a $\mathfrak{K}$ y que sea algebraicamente cerrado. En particular, cualquier polinomio con coeficientes en $\mathfrak{K}$ se puede descomponer en factores lineales sobre K. Si $\mathfrak{K}$ ya tiene esta característica, hacemos $K = \mathfrak{K}$. En otro caso, lo primero que hacemos será añadir las raices de todos los posibles polinomios con coeficientes en $\mathfrak{K}$. Por supuesto, habrá que hacerlo en forma controlada, asegurando que al final obtengamos un campo. Pero aún cuando tengamos éxito en esto, habremos añadido puntos nuevos (el menos las raíces), lo que da lugar a nuevos polinomios, pues tendremos nuevos posibles coeficientes. Así que habremos de repetir el procedimiento recién descrito una y otra vez. Como veremos, esta repetición no es tan larga como pudiera pensarse y se hace «sólo» una cantidad numerable de veces. El teorema de recursión hace su aparición precisamente para elegir uno a uno los polinomios, añadir sus raíces y generar campos. Si el campo original es numerable, la recursión se lleva a cabo sobre ω. De ser $\mathfrak{K}$ innumerable, aparecen etapas límite y sucesor, lo que complica ligeramente la construción.

Demostración. **Afirmación 1.** Si $\mathfrak{L}$ es un campo y $p \in \mathfrak{L}[x]$ es un polinomio no constante, existe una extensión algebraica $\mathfrak{L}^p$ de $\mathfrak{L}$ en la que p tiene una raíz. Se cumple $|\mathfrak{L}^p| \leq |\mathfrak{L}| + \aleph_0$.

Prueba de 1. Se sigue de los resultados previos, pues $\mathfrak{L}^p = \mathfrak{L}/(p)$ contiene una raíz α de $p(x)$. Además, este campo es isomorfo a $\mathfrak{L}(\alpha)$.

Por último, como $\mathfrak{L}(\alpha)$ es un $\mathfrak{K}$-espacio vectorial de dimensión finita, se obtiene que $|\mathfrak{L}(\alpha)| \leq |\mathfrak{K}| + \aleph_0$. ✓ (1)

Ahora construimos una extensión $\mathfrak{L}'$ para cada campo $\mathfrak{L}$ mediante cadenas de modelos, en el que cada polinomio no constante tiene al menos una raíz. En este paso usamos recursión transfinita.

Afirmación 2. Sea $\mathfrak{L}$ un campo. Existe una extensión $\mathfrak{L}'$ de $\mathfrak{L}$ tal que:

(a) todo polinomio no constante $p \in \mathfrak{L}[x]$ tiene una raíz en $\mathfrak{L}'$;
(b) $\mathfrak{L}'$ es una extensión algebraica de $\mathfrak{L}$;
(c) $|\mathfrak{L}'| \leq |\mathfrak{L}| + \aleph_0$.

Prueba de 2. Sean $\kappa = |\mathfrak{L}[x]| = |[\mathfrak{L}]^{<\omega}| (= |\mathfrak{L}| + \aleph_0)$ y $(p_\alpha : \alpha < \kappa)$ una enumeración de todos los polinomios no constantes con coeficientes en $\mathfrak{L}$. Definimos una cadena $(\mathfrak{L}_\alpha : \alpha < \kappa)$ de campos de la siguiente manera.

$$\begin{aligned} \mathfrak{L}_0 &\equiv \mathfrak{L}; \\ \mathfrak{L}_{\alpha+1} &\equiv \mathfrak{L}_\alpha^{p_\alpha}; \\ \mathfrak{L}_\delta &\equiv \bigcup_{\alpha<\delta} \mathfrak{L}_\alpha, \quad \text{cuando } \delta \text{ es límite.} \end{aligned}$$

Observe los siguientes hechos. El paso sucesor $\mathfrak{L}_\alpha$ a $\mathfrak{L}_{\alpha+1}$ arroja una extensión algebraica sobre $\mathfrak{L}_\alpha$ y $\mathfrak{L}_\alpha^{p_\alpha}$ existe porque p_α es un polinomio con coeficientes en $\mathfrak{L} = \mathfrak{L}_0 \subseteq \mathfrak{L}_\alpha$.

Cuando δ es un ordinal límte, debemos cerciorarnos de que $\mathfrak{L}_\delta$ es un campo, que es una extensión algebraica de $\mathfrak{L}_0$ y que tiene la cardinalidad adecuada. Nuestra hipótesis de inducción es que los campos $\mathfrak{L}_\beta$, para $\beta < \delta$, cumplen lo requerido. Un ordinal límite $\gamma > 0$ puede tomar exactamente una de las siguientes formas: $\gamma = \beta + \omega$, donde β es el ordinal líte más grande menor que γ (β puede ser 0), o γ es límite de ordinales límite.

Caso I. $\delta = \beta + \omega$, donde β es un ordinal menor que δ. Sabemos que $\mathfrak{L}_\beta$ es una extensión algebraica de $\mathfrak{L}_0$, y $|\mathfrak{L}_\beta| \leq |\mathfrak{L}_0| + \aleph_0$. Obtenemos $\mathfrak{L}_\delta$ como la unión de las extensiones

$$\mathfrak{L}_\beta \subseteq \mathfrak{L}_{\beta+1} \subseteq \mathfrak{L}_{\beta+2} \subseteq \cdots \subseteq \mathfrak{L}_{\beta_n} \subseteq \cdots$$

Dado que $\mathfrak{L}_\delta$ es unión de campos, es un campo, según el corolario 2.6, porque los axiomas de la teoría de campos son Π_2-enunciados.

Más aún, de acuerdo al lema 3.10(ii), $\mathfrak{L}_\delta$ es una extensión algebraica de $\mathfrak{L}_\beta$, que a su vez es una extensión algebraica de $\mathfrak{L}_0$. Por lo tanto, $\mathfrak{L}_\delta$ es una extensión algebraica de $\mathfrak{L}_0$ de acuerdo con el lema 3.10(i).

Caso II. δ es un ordinal límite de ordinales límite. Nuestra hipótesis de inducción asegura que cualquier campo $\mathfrak{L}_\gamma$ con $\gamma < \delta$ es algebraico sobre $\mathfrak{L}_0$ y tiene el tamaño adecuado. Sabemos que

$$\mathfrak{L}_\delta = \bigcup_{\beta<\delta} \mathfrak{L}_\beta$$

y sin perder generalidad alguna, podemos suponer que

$$\mathfrak{L}_\delta = \bigcup_{\substack{\gamma<\delta \\ \gamma \text{ ordinal límite}}} \mathfrak{L}_\gamma$$

Como antes, inferimos que $\mathfrak{L}_\delta$ es un campo. Dado que cada $\mathfrak{L}_\gamma$ es algebraico sobre $\mathfrak{L}_0$, cada elemento de $\mathfrak{L}_\gamma$ es algebraico sobre $\mathfrak{L}_0$. Sea

$$A = \bigcup_{\substack{\gamma<\delta \\ \gamma \text{ ordinal límite}}} A_\gamma,$$

donde A_γ son los elementos de $\mathfrak{L}_\gamma$, para cada $\gamma < \delta$, γ un ordinal límite.

Se sigue que $\mathfrak{L}_\delta = \mathfrak{L}(A)$, que es una extensión algebraica según el lema 3.10(iii).

Otra forma de probar esto es mostrar que cualquier elemento de $\mathfrak{L}_\delta$ es algebraico sobre $\mathfrak{L}_0$, de la siguiente manera. Sea $x \in \mathfrak{L}_\delta$. Entonces $x \in \mathfrak{L}_\gamma$ para algún ordinal límite $\gamma < \delta$, el menor posible. Por esta elección y la defincición de $\mathfrak{L}_\gamma$, se deduce que $x \in \mathfrak{L}_{\beta+n}$ para $\beta < \gamma$ un ordinal límite el mayor posible y algún $n \in \mathbb{N}$. Por construcción de $\mathfrak{L}_{\beta+n}$ e hipótesis de inducción, x es algebraico sobre $\mathfrak{L}_0$.

En cualquier caso $|\mathfrak{L}_\delta| \leq |\mathfrak{L}_0| + \aleph_0$, pues $\delta < |\mathfrak{L}_0| + \aleph_0$.

Entonces tenemos una cadena creciente de subcampos $(\mathfrak{L}_\alpha : \alpha < \kappa)$ cada uno de los cuales es algebraico sobre $\mathfrak{L}$. Sea

$$\mathfrak{L}' \equiv \bigcup_{\alpha<\kappa} \mathfrak{L}_\alpha$$

y obtenemos un campo que satisface la afirmación 2, pues $\mathfrak{L}'$ es, como antes, un campo que extiende a $\mathfrak{L}$. Si $p(x)$ es un polinomio en $\mathfrak{L}[x]$, debe ser igual a p_α para algún $\alpha < \kappa$, por lo que en la construcción de $\mathfrak{L}'$ debió añadirse una raíz del mismo. También por un razonamiento similar a los anteriores, $|\mathfrak{L}'| \leq |\mathfrak{L}| + \aleph_0$. $\boxed{\checkmark}$ (2)

Lo que tenemos en este punto es un campo $\mathfrak{K}'$ que tiene raíces para cualquier polinomio $p(x)$ con coeficientes en $\mathfrak{K}$. Pero es claro que si agrandamo $\mathfrak{K}$, debieron aparcer elementos que dan lugar a coeficientes de nuevos polinomios. Para estos polinomios recién nacidos no podemos asegurar que $\mathfrak{K}'$ tenga raíces.

Si iteramos $\aleph_0$-veces la construcción de la afirmación 2 encontramos el campo requerido. Definimos

$$\begin{aligned} \mathfrak{K}_0 &\equiv \mathfrak{K} \\ \mathfrak{K}_{n+1} &\equiv \mathfrak{K}_n'; \\ \overline{\mathfrak{K}} &\equiv \bigcup_{n<\omega} \mathfrak{K}_n. \end{aligned}$$

Como antes, se corrobora que $\overline{\mathfrak{K}}$ es un campo, y que $\overline{\mathfrak{K}}$ es algebraico sobre $\mathfrak{K}$.

El campo $\overline{\mathfrak{K}}$ es algebraicamente cerrado, pues los coeficientes de un polinomio arbitrario no constante $p \in \overline{\mathfrak{K}}[x]$ están en algún $\mathfrak{K}_n$, y por construcción tiene un cero en $\mathfrak{K}_{n+1} = \mathfrak{K}_n'$ (y por consiguiente en $\overline{\mathfrak{K}}$). La cardinalidad de $|\overline{\mathfrak{K}}|$ se calcula como sigue. Por un lado, en vista de la afirmación 2(c)

$$|\mathfrak{K}_n| \leq |\mathfrak{K}| + \aleph_0,$$

de donde concluimos

$$|\overline{\mathfrak{K}}| \leq \aleph_0 \cdot (|\mathfrak{K}| + \aleph_0) = |\mathfrak{K}| + \aleph_0.$$

Por otro lado, $|\mathfrak{K}| \leq |\overline{\mathfrak{K}}|$ pues $\mathfrak{K} \subseteq \overline{\mathfrak{K}}$. Además $\aleph_0 \leq |\overline{\mathfrak{K}}|$, ya que un campo finito no puede ser algebraicamente cerrado. Por lo tanto,

$$|\overline{\mathfrak{K}}| = |\mathfrak{K}| + \aleph_0$$

y concluimos la demostración del teorema. ❒

Teorema 3.14. *Cualesquier dos cerraduras algebraicas de un campo $\mathfrak{K}$ son isomorfas.*

Demostración. Véase [Ro15, Theorem B-2.44]. ❐

Por consiguiente, la cerradura algebraica de un campo es única (salvo isomorfismos).

En este punto presentamos otra aplicación de las cadenas de modelos para probar que la clase de los campos algebraicamente cerrados no es finito axiomatizable.

Definición 3.15. Si $K/\mathfrak{K}$ es un campo extensión y $\alpha \in K$ es algebraico sobre $\mathfrak{K}$, entonces el único polinomio $p(x) \in \mathfrak{K}[x]$ mónico e irreducible que tiene a α como raíz se conoce como el polinomio mínimo de α sobre $\mathfrak{K}$ y se denota $irr(\alpha, \mathfrak{K}) = p(x)$; su grado es igual a $[K : \mathfrak{K}]$.

Lema 3.16. *Para cada $n < \omega$ existe una extensión $\mathbb{Q}^n$ de $\mathbb{Q}$ tal que,*
(a) Todo polinomio $p \in \mathbb{Q}^n[x]$ de grado $\leq n$ tiene un cero en $\mathbb{Q}^n$.
(b) $\mathbb{Q}^n$ no es algebraicamente cerrado.

Demostración. Sea $\overline{\mathbb{Q}}$ la cerradura algebraica de $\mathbb{Q}$. Según el teorema 3.13, $\overline{\mathbb{Q}}$ es numerable, así que lo enumeramos como $(a_k : k < \omega)$. Para $n < \omega$ construimos una cadena $(\mathbb{Q}_i^n : i < \omega)$ de subcampos de $\overline{\mathbb{Q}}$ como se describe a continuación. Sea $\mathbb{Q}_0^n \equiv \mathbb{Q}$, y supongamos que $\mathbb{Q}_i^n$ ya está definido. Si existe un k tal que $a_k \notin \mathbb{Q}_i^n$ que sea la raíz de un polinomio de grado $\leq n$ en $\mathbb{Q}_i^n[x]$, escogemos la menor de tales k y definimos $\mathbb{Q}_{i+1}^n \equiv \mathbb{Q}_i^n(a_k)$. De no existir tal k, hacemos $\mathbb{Q}_{i+1}^n \equiv \mathbb{Q}_i^n$. Establecemos entonces $\mathbb{Q}^n \equiv \bigcup_{i<\omega} \mathbb{Q}_i^n$. Si $p(x) = \sum_{j\leq m} b_j x^j$ es un polinomio de grado $\leq n$ con coeficientes en $\mathbb{Q}^n$, existe $i < \omega$ con $b_0, \ldots, b_m \in \mathbb{Q}_i^n$. Ya que $\overline{\mathbb{Q}}$ es algebraicamente cerrado, existe $j < \omega$, tal que a_j es un cero de p. De la construcción del campo se sigue fácilmente que $a_{j+1} \in \mathbb{Q}_{i+j}^n$. Así que p tiene un cero en $\mathbb{Q}^n$. Queda demostrado (a). Para probar (b) necesitamos los siguientes hechos algebraicos, que se deducen de los resultados previos.

Si $\mathfrak{L} = \mathfrak{K}(a)$, donde a es algebraico sobre $\mathfrak{K}$, entonces $[\mathfrak{L} : \mathfrak{K}]$ es el grado del polinomio irreducible de a (véase [We06, Proposition 2.4.6]). En el caso $\mathfrak{K}_1 \subseteq \mathfrak{K}_2 \subseteq \mathfrak{K}_3$, ocurre

$$[\mathfrak{K}_3 : \mathfrak{K}_1] = [\mathfrak{K}_3 : \mathfrak{K}_2][\mathfrak{K}_2 : \mathfrak{K}_1].$$

De aquí se sigue que si $\mathfrak{L} = \mathfrak{K}(a_1, \ldots, a_m)$, donde $a_1, \ldots, a_m$ son elementos algebraicos sobre $\mathfrak{K}$, entonces $[\mathfrak{L} : \mathfrak{K}]$ es divisible por el grado del polinomio irreducible de a_1, pues

$$[\mathfrak{L} : \mathfrak{K}] = [\mathfrak{K}(a_1, \ldots, a_m) : \mathfrak{K}(a_1, \ldots, a_{m-1})] \cdots [\mathfrak{K}(a_1) : \mathfrak{K}].$$

Para demostrar (b), supongamos que $\mathbb{Q}^n$ es algebraicamente cerrado. Entonces $\mathbb{Q}^n = \overline{\mathbb{Q}}$. Fijemos un primo racional arbitrario $q > n$. Sea a un elemento arbitrario de $\overline{\mathbb{Q}}$, cuyo polinomio irreducible sobre $\mathbb{Q}$ tiene grado q (por ejemplo, si $a = 2$, puede ser $p(x) = x^q - 2$). Puesto que $a \in \overline{\mathbb{Q}} = \mathbb{Q}^n$, existe un menor $i < \omega$ con $a \in \mathbb{Q}_i^n$. Ya que para $j < \omega$, $\mathbb{Q}_{j+1}^n$ se obtiene de $\mathbb{Q}_j^n$ mediante la adición de un cero de un polinomio de grado $\leq n$, deducimos que $[\mathbb{Q}_{j+1}^n : \mathbb{Q}_j^n] \leq n < q$. En vista de que

$$[\mathbb{Q}_i^n : \mathbb{Q}] = [\mathbb{Q}_i^n : \mathbb{Q}_{i-1}^n] \cdots [\mathbb{Q}_1^n : \mathbb{Q}_0^n],$$

se sigue que q no está entre los factores del lado derecho, por lo que no puede dividir al producto. Así, $\neg(q | [\mathbb{Q}_i^n : \mathbb{Q}])$. Dado que $[\mathbb{Q}_i^n : \mathbb{Q}] < \omega$ y $a \in \mathbb{Q}_i^n$, existen una cantidad finita de elementos $b_1, \ldots, b_m \in \mathbb{Q}_1^n$ que son algebraicos sobre $\mathbb{Q}$, tales que $\mathbb{Q}_i^n = \mathbb{Q}(a, b_1, \ldots, b_m)$. Acabamos de mostrar que en este caso $[\mathbb{Q}_i^n : \mathbb{Q}]$ es divisible entre el grado del polinomio irreducible de a, es decir $q | [\mathbb{Q}_i^n : \mathbb{Q}]$. Esta contradicción muestra que $\mathbb{Q}^n$ no puede ser algebraicamente cerrado. ❐

Para nuestro siguiente teorema sobre campos algebraicamente cerrados, necesitamos introducir la teoría de los campos algebraicamente cerrados. Primero definimos los siguientes $\mathscr{L}$-términos:

Definición 3.17. (a) Sea $i < \omega$. Definimos por recursión sobre $n < \omega$ el $\mathscr{L}$-término v_i^n mediante $v_i^0 = 1$ y $v_i^{n+1} = v_i^n \cdot v_i$.

(b) Definimos por recursión sobre $n < \omega$, $n \geq 1$, los $\mathscr{L}$-enunciados ψ_n mediante

$$\psi_n \equiv \forall v_0 \cdots v_n \exists v_{n+1} (\neg v_n = 0 \to \sum_{i<n+1} v_i \cdot v_{n+1}^i = 0).$$

(el enunciado ψ_n afirma que todo polinomio de grado n tiene una raíz).

La $\mathscr{L}$-teoría $\boldsymbol{\Phi}_{cac} \equiv \boldsymbol{\Phi}_{camp} \cup \{\psi_n : 1 \leq n \wedge n < \omega\}$ axiomatiza la clase de modelos de los campos algebraicamente cerrados y se llama la teoría de los campos algebraicamente cerrados.

Teorema 3.18. *La clase de los campos algebraicamente cerrados no es elemental.*

Demostración. Supongamos que la clase de los campos algebraicamente cerrados es finito axiomatizable. Entonces por 2.2 existe un subconjunto finito $\boldsymbol{\Phi}'$ de $\boldsymbol{\Phi}_{cac}$, que axiomatiza esta clase. Existe $n < \omega$ tal que $\psi_m \notin \boldsymbol{\Phi}'$ para toda $m > n$. De acuerdo al teorema 3.13, $\mathbb{Q}^n$ es un modelo de $\boldsymbol{\Phi}'$ pero no es modelo de $\boldsymbol{\Phi}_{cac}$, lo que contradice la suposición de que $\boldsymbol{\Phi}'$ axiomatiza la clase de los campos algebraicamente cerrados. ❐

Ahora nos ocupa mostrar la validez de otro teorema de Steinitz. A saber, dados dos campos innumerables del mismo tamaño y misma carcaterística, necesariamente existe un isomorfismo entre ellos.

4. CATEGORICIDAD

A principios de siglo XX Steinitz [St10] demostró el siguiente resultado. Dos campos algebraicamente cerrados de la misma característica y con igual cardinalidad (infinita no numerable) son isomorfos. Este resultado se traduce en teoría de modelos en la afirmación de que la teoría de los campos algebraicamente cerrados de característica p o cero es κ-categórica para toda $\kappa > \aleph_0$. A continuación presentamos una demostración directa de este resultado utilizando métodos de teoría de modelos. Pero mucha atención; como se apreciará al final, podemos también dar una prueba que no requiere la teoría de modelos.

Definición 4.1. Una $\mathscr{L}$-teoría es *λ-categórica*, si tiene un único modelo (salvo isomorfismos) de cardinalidad λ.

La teoría que nos concierne es la teoría de los campos algebraicamente cerrados $\boldsymbol{T}_{cac}$. La formulamos en el lenguaje antes mencionado $\mathscr{L} = \{+, \cdot, 0, 1\}$. Para p un número primo, definimos el $\mathscr{L}$-enunciado

$$C_p \equiv \sum_{i<p} 1 = 0.$$

Con lo que la teoría de los campos algebraicamente cerrados de característica p se axiomatiza como

$$\boldsymbol{T}_{cac,p} \equiv \boldsymbol{T}_{cac} \cup \{C_p\}.$$

y la de los campos algebraicamente cerrados de característica cero mediante:

$$\boldsymbol{T}_{cac,0} \equiv \boldsymbol{T}_{cac} \cup \{\neg C_p : p \text{ es primo}\}.$$

Observe que $\boldsymbol{T}_{cac}$ tiene sólo modelos infinitos, pues si $\mathfrak{K}$ es un campo finito cuyo universo es $\{k_i : i < n\}$, entonces el polinómio $1 + \Pi_{i<n}(x - k_i)$ no tendría raíz en $\mathfrak{K}$.

Recuerde que una $\mathscr{L}$-teoría $\boldsymbol{T}$ es completa, si para todo $\mathscr{L}$-enunciado φ, se cumple que $\varphi \in \boldsymbol{T}$ o $\neg\varphi \in \boldsymbol{T}$.

Definición 4.2. Sea E/K una extensión. Un subconjunto $U \subseteq E$ es algebraicamente dependiente sobre K, cuando existe un subconjunto finito $\{u_1,\ldots,u_n\} \subseteq U$ y un polinómio distinto de cero $f(x_1,\ldots,x_n) \in K[x_1,\ldots,x_n]$ tales que $f(u_1,\ldots,u_n) = 0$. Un subconjunto $B \subseteq E$ es algebraicamente independiente, cuando no es algebraicamente dependiente.

Un campo extensión E/K es trascendente puro cuando $E = K$ o E contiene un subconjunto algebraicamente independiente B tal que $E = K(B)$.

Ya que subconjuntos algebraicamente dependientes son necesariamente no vacíos, el conjunto vacío $\emptyset$ es algebraicamente independiente. El conjunto unitario $\{u\} \subseteq E$ es algebraicamente dependiente si u es algebraico sobre K; esto es, u es raíz de un polinomio no constante sobre K. Si $\{u\}$ es algebraicamente independiente, entonces u es trascendente sobre K.

Recuerde que si V es un espacio vectorial y $X = \{v_1,\ldots,v_n\} \subseteq V$, X es linealmente dependiente si y sólo si algún v_i está en el subespacio generado por el resto de los elementos de X. La siguiente proposición establece un resultado análogo para dependencia algebraica.

Proposición 4.3. *Sea E/K una extensión. El subconjunto $U \subseteq E$ es algebraicamente dependiente sobre K si y sólo si existe $v \in U$ tal que v es algebraico sobre $K(U - \{v\})$.*

Demostración. Véase [Ro15, Proposition B-2.48]. ❐

Existe un fuerte paralelismo entre dependencia lineal en un espacio vectorial y dependencia algebraica en un campo. El análogo a una base en un espacio vectorial es una base de trascendencia en un campo; el símil de dimensión es el grado de trascendencia.

Sea E/K un campo extensión. Si $u \in E$ y $S \subseteq E$, entonces u es dependiente en S, que se denota $u \preccurlyeq S$, cuando u es algebraico sobre $k(S)$, el subcampo de E generado por K y S.

Teorema 4.4. *Sean E/K una extensión, $u \in E$ y $S \subseteq E$. Se cumplen las siguientes afirmaciones.*

(1) Si $u \in S$, entonces $u \preccurlyeq S$.
(2) Si $u \preccurlyeq S$, existe un subconjunto finito $S' \subseteq S$ con $u \preccurlyeq S'$.
(3) Sean $T \subseteq E$; si $u \preccurlyeq S$ y cada elemento de S es dependiente en T, entonces u es dependiente en T.
(4) Si u es dependiente en $S = \{v, s_1,\ldots,s_n\}$ pero no en $\{s_1,\ldots,s_n\}$, entonces v es dependiente en $\{u, s_1,\ldots,s_n\}$ pero no en $\{s_1,\ldots,s_n\}$.

Demostración. Véase [Ro15, Theorem B-2.49]. ❐

Se puede extender la notación $\preccurlyeq$ a espacios vectoriales. Si V es un espacio vectorial sobre un campo K y $S \subseteq V$, decimos que $v \in V$ depende en S, $v \preccurlyeq S$, si v es una combinación lineal de vectores en S. Así, un subconjunto S es linealmente dependiente, si $s \preccurlyeq S - \{s\}$ para algún $s \in S$.

Si E/K es una extensión, un subconjunto $S \subseteq E$ no vacío es algebraicamente independiente si y sólo si $s \not\preccurlyeq S - \{s\}$ para toda $s \in S$. Se sigue que todo subconjunto de un conjunto algebraicamente independiente es él mismo algebraicamente independiente.

Definición 4.5. Si E/K es una extensión, un subconjunto $S \subseteq E$ genera a E (en el sentido de la relación de dependencia; no cofundir con $K(S) = E$) si $x \preccurlyeq S$ para cada $x \in E$.

Una base de E es un subconjunto algebraicamente independiente que genera a E.

Lema 4.6. *Sea E/K una extensión. Si $T \subseteq E$ es algebraicamente independiente sobre K y $z \in E$ es trascendente sobre $K(T)$, entonces $T \cup \{z\}$ es algebraicamente independiente.*

Demostración. Véase [Ro15, Lemma B-2.50]. ❒

Definición 4.7. Si E/K es una extensión, entonces una base de trascendencia es un subconjunto de E algebraicamente independiente sobre K máximo.

Aquí, que H sea algebraicamente independiente sobre K máximo significa que H es algebraicamente inependiente sobre K y si $H \subseteq H'$ y H' es algebraicamente independiente sobre K, entonces $H = H'$.

Ahora podemos demostrar la existencia de bases de trascendencia empleando el teorema de recursión.

Teorema 4.8. *Si E/K es un campo extensión, entonces E tiene una base de trascendencia. De hecho, todo subconjunto algebraicamente independiente es parte de una base de trascendencia.*

Demostración. Sea $B \subseteq E$ un conjunto algebraicamente independiente dado. En cualquier caso, podemos tomar $B = \emptyset$. Estamos trabajndo en ZFC, por lo que se cumple el axioma de elección, en particular el principio del buen orden. Esto es, cualquier conjunto, E por ejemplo, es isomorfo a un ordinal. En consecuencia, podemos enumerar E mediante ese ordinal. Digamos

$$E = \{e_\alpha : \alpha < \mu\}$$

para algún ordinal μ.

Por recursión en μ construimos una cadena creciente de subconjuntos de E

$$B = B_0 \subseteq B_1 \subseteq B_2 \cdots \subseteq B_\alpha \subseteq \cdots$$

cada uno de los cuales es algebraicamente idependiente. Empezamos, como ya se dijo, con $B = B_0$ y considere el primer e_α (aquí el primer e_α significa el elemento de E con el menor índice posible) que sea trascendente sobre $K(B_0)$. De no existir ninguno, la recursión termina.

En general, si ya construimos B_α, buscamos el primer e_γ que sea trascendente sobre $K(B_\alpha)$ y formamos $B_{\alpha+1} = B_\alpha \cup \{e_\gamma\}$. Según el teorema 4.6, $B_{\alpha+1}$ es algebraicamente independiente.

Si λ es un ordinal límite > 0 y construimos B_α para cada $\alpha < \lambda$, hacemos $B_\lambda = \bigcup_{\alpha<\lambda} B_\alpha$. Note que al ser λ un ordinal límite > 0, necesariamente es infinito.

Afirmación 1. B_λ es algebraicamente independiente.

Prueba de 1. Todos y cada uno de los B_α, $\alpha < \lambda$, son algebraicamente independientes. Supongamos que B_λ no lo es. Entonces existe $e \in B_\lambda$ que es algebraicamente indepndiente, lo que de acuerdo con la terminología arriba descrita, da lugar a $e \preccurlyeq B_\lambda - \{e\}$. Recurrimos al teorema 4.4(2) para encontrar un subconjunto finito $\{e_{\gamma_1}, \ldots, e_{\gamma_n}\} \subseteq B_\lambda - \{e\}$ tal que $e \preccurlyeq \{e_{\gamma_1}, \ldots, e_{\gamma_n}\}$. Antes llamamos la atención al hecho de que λ debe ser infinito; como cada e_{γ_i}, $0 < i \leq n$ debe aparecer en B_λ, que es la unión de los B_α, debe existir un ordinal $\gamma < \lambda$ tal que $\{e, e_{\gamma_1}, \ldots, e_{\gamma_n}\} \subseteq B_\gamma$, pues los B_α conforman una cadena $\subseteq$-creciente y e también pertenece a B_λ. Pero esto no es posible, pues, por hipótess de inducción, cada B_α, $\alpha < \lambda$, es algebraicamente independiente. Este razonamiento absurdo, confirma la afirmación 1. $\boxed{\checkmark}$ (1)

Una vez efectuada la recursión sobre μ, hacemos

$$W = \bigcup_{\alpha<\eta} B_\alpha,$$

donde η es el primer ordinal donde se «detuvo» la recursión, es decir, donde ya no pudimos encontrar un elemento e_γ que fuese trascendente sobre el campo generado en E por K y los B_α construidos previamente. Nada impide que $\eta = \mu$, pero también puede ocurrir que $\eta < \mu$.

En todo caso, W es algebraicamente independiente, lo que se confirma mediante una prueba como la de la afirmación 1. Dado que la recursión se detuvo ante la imposibilidad de encontrar un elemento trascendente, es claro que W es un subconjunto $\subseteq$-máximo de E.

Afirmación 2. W es una base de trascendencia para E.

Prueba de 2. Ya vimos que W es máximo. Resta constatar que W genera a E. Supongamos que no es el caso. Entonces existe $e \in E$ tal que $e \not\subseteq W$. Apelamos otra vez al teorema 4.6 para confirmar que $W \cup \{e\}$ es algebraicamente independiente. Pero esto se opone a lo recién establecido, que W es máximo. Por lo tanto, W es una base para E. $\boxed{\checkmark}$ (3) ❒

Definición 4.9. Sea $\mathfrak{K}$ una clase de $\mathscr{L}$-modelos. Un $\mathscr{L}$-modelo $\mathfrak{A}$ es una estructura primitiva de $\mathfrak{K}$, si $\mathfrak{A}$ se encaja en toda estructura $\mathfrak{B}$ de $\mathfrak{K}$.

Que $\mathfrak{A}$ se encaje en $\mathfrak{B}$ significa que existe un monomorfismo $\varphi : \mathfrak{A} \longrightarrow \mathfrak{B}$.

Como se sabe, los números racionales y los campos $\mathfrak{F}_p$ (es decir, $\mathbb{Z}_p$ para p primo con la suma y el producto) son subcampo de todo campo de característica cero o de característica p, respectivamente.

Nuestra intención es demostrar que dos campos algebraicamente cerrados de las mismas cardinalidad no numerable y característica, son isomorfos.

Lema 4.10. *Sean K un campo y L un subcampo de K a lo sumo numerable. Si $A \subseteq K$ es numerable, el subcampo generado por $L \cup A$ en K es numerable.*

Demostración. Sabemos que L es subcampo de K. Al añadir elementos a L, es claro que puede perder su cualidad de ser subcampo. Esto puede ocurrir por varias razones. A saber, si tomamos $B = L \cup A$,

- Si $a \in A - L$, $a \neq 0$, puede no existir el inverso multiplicativo de a en B.
- Si $a, b \in B$, puede ocurrir que $a + b \notin B$.
- Si $a, b \in B$, puede ocurrir que $a \cdot b \notin B$.
- Si $a \in B$, el inverso aditivo de a puede no vivir en B.

Por ello debemos generar un campo a partir de B. De hecho, buscamos el subcampo de K que contenga a B y sea el menor posible respecto a ser subcampo y contener a B. Esto se logra, por recursión transfinita sobre ω, de la siguiente manera.

Se construye una cadena $\subseteq$-creciente de subconjuntos de K, empezando con $B = B_0$,

$$B = B_0 \subseteq B_1 \subseteq \cdots B_n \subseteq \cdots$$

Como ya se dijo, sea $B_0 = B$. El siguiente conjuto, B_1, se define como

$$B_1 = B_0 \cup f_1[B_0] \cup f_2[B_0 \times B_0] \cup f_3[B_0 \times B_0] \cup f_4[B_0],$$

donde $f_1(x)$ consigue el inverso multiplicativo de $x \in K$, cuando $x \neq 0$; $f_2(x,y) = x + y$, $f_3(x,y) = x \cdot y$ y $f_4(x)$ es el inverso aditivo de x. Esto es, B_1 contiene a los inversos aditivos y multiplicativos de los elementos en B_0, así como las sumas y productos de elementos de B_0. Por supuesto, B_1 no necesariamente es un campo, pues aparecen alementos nuevos y no sabemos si sus inversos, sumas y productos están en B_1.

En general, si ya construimos B_n, sea

$$B_{n+1} = B_n \cup f_1[B_n] \cup f_2[B_n \times B_n] \cup f_3[B_n \times B_n] \cup f_4[B_n],$$

y tomamos $F = \bigcup_{n \in \mathbb{N}} B_n$. Es fácil comprobar que F es un subcampo de K. Por ejemplo, F es cerrado respecto a la suma, pues si tomamos $x, y \in F$, estos deben pertenecer a algún B_n (la cadena es creciente), y su suma aparece en B_{n+1}.

Afirmación 1. F es el menor subcampo que contiene a B.

Prueba de 1. Ya vimos que F es subcampo de K y $B \subseteq F$. Sea F' otro subcampo de K que contiene a B. Mostraremos que $B_n \subseteq F'$ para toda $n \in \mathbb{N}$ por inducción en ω. Por hipótesis $B_0 = B \subseteq F'$. supongamos que $B_n \subseteq F'$ y verifiquemos que $B_{n+1} \subseteq F'$. Si $z \in B_{n+1}$, por construcción $z \in B_n \subseteq F'$ o z aparece como resultado de haber aplicado algunas de las operaciones $f_1, \ldots, f_4$ a elementos de $B_n \subseteq F'$. Pero estas operaciones son la de campo, y F' es campos, así que $z \in F'$.

Se sigue que todos los B_n están contenidos en F', por lo que su unión también lo está. $\boxed{\checkmark}$ (1)

Ahora no ocupamos de los tamaños. L es a lo sumo numerable y A es numerable, por lo que $B = L \cup A$ es numerable, lo mismo que $B \times B$.

Afirmación 2. F es numerable.

Prueba de 2. Se verifica que cada B_n es numerable por inducción en ω. B_0 es numerable por hipótesis. Suponga que B_n es numerable. El conjunto B_{n+1} se obtiene al unir B_n que es numerable con la unión de una cantidad finita de uniendos. Cada uno de estos uniendos es B_n o la imagen de B_n o de $B_n \times B_n$ respecto a una función; esta imágenes son numerables, de donde se deduce que B_{n+1} es numerable. Aquí usamos el hecho conocido de que si $f : C \longrightarrow D$ es una función sobre, entonces $|D| \leq |C|$.

Entonces, F es la unión de una cantidad numerable de conjuntos numerables, por lo que es numerable. $\boxed{\checkmark}$ (2) ❒

Con una prueba análoga se puede demostrar el teorema, pero en lugar de tomar a L a lo sumo numerable, y a A numerable, se considera L de tamaño κ o $\leq \kappa$, lo mismo que A. Se corrobora que el subcampo F resultante tiene tamaño $\leq \kappa$.

Lema 4.11. *Sean E/K y M/K extensiónes, y $B \subseteq E, B' \subseteq M$ conjuntos algebraicamente independientes sobre K. Suponga que existe una biyección $b : B \longrightarrow B'$. Entonces, b se puede extender a un isomorfismo $\varphi : K(B) \longrightarrow K(B')$.*

Demostración. Sabemos que $K(B)$ es el menor subcampo de E generado por K y B. Algo correspondiente ocurre con K y B'. En la prueba del lema 4.10 construimos el campo F generado por K y A. Aquí usaremos esa misma construcción para $K(B)$ y $K(B')$ en términos de K y B o B' según sea el caso.

Pera construir $K(B)$ se empieza con $C = B \cup K$, mientras que para $K(B')$ se comienza con $C' = K \cup B'$. Sin perder generalidad alguna, suponemos que $B \cap K = \emptyset = B' \cap K$. En consecuencia, tenemos una biyección $l : C \longrightarrow C'$, que extiende a b.

Ahora, en el paso 1 se constuye C_1, respectivamente C_1' como la unión de $C = C_0$ con la imagen de $C_0 \times C_0$ respecto a $f_1, \ldots, f_4$, y lo correspondiente para C_1'. Extendemos $l = l_0$ a $l_1 : C_1 \longrightarrow C_1'$ de la siguiente manera. Primero establecemos que $l_1 \restriction C_0 = l_0$. Sea $z \in C_1 - C_0$. Entonces $z = f_1(x)$ o $z = f_2(x,y)$, o $z = f_3(x,y)$ o $z = f_4(x)$, donde $x, y \in C_0$. Hacemos $l_1(z) = z'$, donde $z' = f_1(l(x))$ o $z = f_2(l(x), l(y))$, o $z = f_3(l(x), l(y))$ o $z = f_4(l(x))$, según sea el caso para z. En general, si extendimos l a $l_n : C_n \longrightarrow C_n'$, la podemos extender a $l_{n+1} : C_{n+1} \longrightarrow C_{n+1}'$ mediante un procedimiento como el recién descrito.

Es fácil corroborar que estas extensiones preservan las operaciones de grupo (por inducción en n, probando que cada extensión l_n preserva las operaciones de campo), por lo que

$$l_\infty = \bigcup_{n \in \mathbb{N}} : K(B) \longrightarrow K(B')$$

es un isomorfismo. ❒

En lo sucesivo, diremos que la extensión de b a $K(B)$ es la extensión natural.

Ahora demostraremos que las teorías de los campos algebraicamente cerrados de característica p o cero son $\aleph_1$-categóricas. A partir de este resultado obtendremos la completud de nuestras teorías así como el teorema de Steinitz.

Teorema 4.12. *Sean $\mathfrak{K},\mathfrak{M}$ campos algebaicamente cerrados de característica p (respectivamente, cero) y cardinalidad $\aleph_1$. Entonces $\mathfrak{K}$ y $\mathfrak{M}$ son isomorfos.*

Demostración. Sea $\mathfrak{K}$ un campo algebraicamente cerrado con $|\mathfrak{K}| = \aleph_1$. Si $\mathfrak{K}'$ es el campo primo de $\mathfrak{K}$ y $\mathscr{B}$ es una base de trascendencia de $\mathfrak{K}/\mathfrak{K}'$, entonces $\mathfrak{K}$ es la cerradura algebraica de $\mathfrak{K}'(\mathscr{B})$. Observemos que $\mathfrak{K}'$ es $\mathfrak{F}_p$ para algún primo p, o es $\mathbb{Q}$. Si $|\mathscr{B}| = \aleph_0$, entonces $|\mathfrak{K}'(\mathscr{B})| = \aleph_0$, según el lema 4.10. Por tanto, $|\mathfrak{K}| = \aleph_0$, lo cual es imposible. Se sigue que $|\mathscr{B}| = \aleph_1$.

Si $\mathfrak{M}$ es otro campo algebraicamente cerrado con $|\mathfrak{M}| = \aleph_1$ y $car(\mathfrak{K}) = car(\mathfrak{M})$, entonces $\mathfrak{K}$ y $\mathfrak{M}$ tienen el mismo campo primo. Sea $\mathscr{B}'$ base de trascendencia de $\mathfrak{M}/\mathfrak{K}'$. Como vimos antes,$|\mathscr{B}| = |\mathscr{B}'| = \aleph_1$. Así que tenemos una biyección $\phi : \mathscr{B} \longrightarrow \mathscr{B}'$. Extendemos esta biyección a un isomorfismo de campos

$$\tilde{\phi} : k(\mathscr{B}) \longrightarrow \mathfrak{K}'(\mathscr{B}')$$

de manera natural.

Por la unicidad de las cerraduras algebraicas, $\tilde{\phi}$ se extiende a un isomorfismo

$$\hat{\phi} : \mathfrak{K} \longrightarrow \mathfrak{M}.$$

❐

Teorema 4.13. *Sean $\mathfrak{K},\mathfrak{M}$ campos algebaicamente cerrados de característica p (respectivamente, cero) y cardinalidad $\kappa \geq \aleph_1$. Entonces $\mathfrak{K}$ y $\mathfrak{M}$ son isomorfos.*

Demostración. La prueba del teorema 4.12 funciona *mutatis mutandi* para campos de cardinalidad $\kappa > \aleph_1$. ❐

Sólo nos queda comentar qué sucede si $|\mathfrak{K}| = \aleph_0$. Sean α,β trascendentes algebraicamente independientes sobre $\mathfrak{K}' = \mathfrak{F}_p$ o $\mathbb{Q}$. Es claro que $\mathfrak{K}'(\alpha) \ncong \mathfrak{K}'(\alpha,\beta)$ y por lo tanto las cerraduras algebraicas respectivas tienen cardinalidad $\aleph_0$, pero no son isomorfas.

Para completar el artículo describimos la prueba usual del teorema 4.13 en teoría de modelos.

Teorema 4.14 (Criterio de Vaught)**.** *Sea $\boldsymbol{T}$ una L-teoría que no tiene modelos finitos. Si existe $\kappa \geq |L|$ tal que $\boldsymbol{T}$ es κ-categórica, entonces $\boldsymbol{T}$ es completa.*

Demostración. Sea $\kappa \geq |L|$ con $\boldsymbol{T}$ κ-categórica. Supongamos que $\boldsymbol{T}$ no es completa. Entonces existe un L-enunciado φ que no pertenece a $\boldsymbol{T}$ y tampoco $\neg\varphi$ pertenece a $\boldsymbol{T}$. En consecuencia, $\boldsymbol{T} \cup \{\varphi\}$ y $\boldsymbol{T} \cup \{\neg\varphi\}$ son consistentes; por consiguiente, son satisfacibles. Puesto que $\boldsymbol{T}$ carece de modelos finitos, ambos conjuntos tienen modelos infinitos. Del teorema de Löwenheim-Skolem obtenemos un modelos $\mathfrak{A}$ de $\boldsymbol{T} \cup \{\neg\varphi\}$ y un modelos $\mathfrak{B}$ de $\boldsymbol{T} \cup \{\varphi\}$, ambos de cardinalidad κ. Claramente estas estructuras no son elementalmente equivalentes y mucho menos isomorfas. En consecuencia, $\boldsymbol{T}$ no es κ- categórica, lo que contradice nuestra hipótesis. ❐

Corolario 4.15. *La teoría de los campos algebraicamente cerrados de característica p (respectivamente, cero) es completa.*

Demostración. Ya vimos que esta teoría es $\aleph_1$-categórica (teorema 4.12), y que carece de modelos finitos. Del criterio de Vaught se desprende que la teoría es completa. ❐

Ahora podemos demostrar el teorema de Steinitz 4.13.

Teorema 4.16 (Teorema de Steinitz)**.** *Sean $\mathfrak{K}_1$ y $\mathfrak{K}_2$ dos campos algebraicamente cerrados de característica p o cero, de la misma cardinalidad no numerable κ. Entonces $\mathfrak{K}_1$ es isomorfo a $\mathfrak{K}_2$.*

Demostración. El resultado es inmediato de los teoremas 4.12 y 4.14 pues de éllos concluimos que la teoría de los campos algebraicamente cerrados de característica p o cero es completa y $\aleph_1$-categórica. El teorema de Morley [CK93, 7.1.14, pp. 494] o[TrZi12, Corollary 5.8.2] asegura que toda L-teoría completa con $|L| \leq \aleph_0$ es κ categórica si y sólo si es $\aleph_1$-categórica, para todo cardinal $\kappa \geq \aleph_0$. En consecuencia, los campos dados en el enunciado del teoema deben ser isomorfos. ❐

Esta última prueba es ciertamente elegante y recurre a un teorema fundamental de la teoría de modelos; a saber, el Teorema de categoricidad de Morley.

REFERENCES

[Ar88] E. Artin, *Galoische Theorie*, Verlag Harri Deutsch, Frankfurt/Main, 1988.
[CK93] C. Chang, H. J. Keisler, *Model Theory*, Third Ed., North-Holland, 1993.
[FeVill13] M. Fernández de Castro, L. M. Villegas Silva, *Teoría de conjuntos, lógica y temas afines I*, Universidad Autónoma Metropolitana Iztapalapa, CDMX, México, 2013.
[FeVi17] M. Fernández de Castro, L. M. Villegas Silva, *Teoría de conjuntos, lógica y temas afines II*, Universidad Autónoma Metropolitana Iztapalapa, CDMX, México, 2017.
[Ro15] J. Rotman, *Advanced Modern Algebra, Part 1*, AMS, 2015.
[St10] E. Steinitz, *Algebraische Theorie der Körper*, J. f. Reine u. Angew. Math. **137**(1910), 167–309.
[TrZi12] K. Trent, M. Ziegler, *A course in Model Theory*, Cambridge University Press, 2012.
[Wa66] B. L. van der Waerden, *Algebra I*, Springer-Verlag, Berlin, 1966.
[We06] S. Weintraub, *Galois Theory*, Springer-Velag, N. Y., 2006

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD AUTÓNOMA METROPOLITANA IZTAPALAPA, CDMX, MÉXICO

E-mail address: lmvs@xanum.uam.mx