Trabajo de Fin de Grado

Eliminación de cuantificadores

Por
Jokin Garitano Telleria

Dirigido por:
Elías Baro González

Universidad Complutense de Madrid
Facultad de Ciencias Matemáticas
Grado en Matemáticas

Febrero 2026

A Kiwi

Resumen

Este trabajo estudia la eliminación de cuantificadores en teoría de modelos y su relación con la geometría algebraica y la geometría algebraica real. Tras formalizar la noción y presentar criterios semánticos que la caracterizan, se prueba que la teoría de los cuerpos algebraicamente cerrados (ACF) y la teoría de los cuerpos realmente cerrados (RCF) tienen eliminación de cuantificadores. Desde este enfoque, se recuperan resultados clásicos: el Nullstellensatz de Hilbert, el Teorema de Ax y una solución al decimoséptimo problema de Hilbert.

Palabras clave: eliminación de cuantificadores; teoría de modelos; cuerpos algebraicamente cerrados; cuerpos realmente cerrados.

Abstract

This work studies quantifier elimination in model theory and its relation to algebraic geometry and real algebraic geometry. After formalizing the notion and presenting semantic criteria characterizing it, the theories of algebraically closed fields (ACF) and real closed fields (RCF) are shown to have quantifier elimination. Within this framework, classical results are recovered: Hilbert's Nullstellensatz, Ax's theorem, and a solution to Hilbert's seventeenth problem.

Keywords: quantifier elimination; model theory; algebraically closed fields; real closed fields.

Índice

1. Introducción

La lógica de primer orden proporciona un marco suficientemente flexible para formalizar una amplia variedad de teorías matemáticas, pero esa flexibilidad no es gratuita. La presencia de cuantificadores introduce un nivel de complejidad expresiva que, aunque necesaria en general, no siempre refleja la complejidad estructural real de los objetos descritos. En este sentido, parte sustancial del contenido de una teoría puede quedar oculta tras una formulación sintácticamente más compleja de lo necesario.

La eliminación de cuantificadores aborda precisamente este fenómeno. Una teoría tiene eliminación de cuantificadores cuando toda fórmula es equivalente, dentro de la teoría, a una fórmula libre de cuantificadores.

Dos ejemplos paradigmáticos son la teoría de los cuerpos algebraicamente cerrados y la teoría de los cuerpos realmente cerrados. En el primer caso, dicha propiedad conduce a la caracterización de los conjuntos definibles como conjuntos constructibles; en el segundo, como conjuntos semialgebraicos. En ambos contextos, la reducción a fórmulas sin cuantificadores hace que resultados clásicos de geometría algebraica y geometría algebraica real aparezcan como consecuencias naturales de la estructura lógica de las teorías.

Desde un punto de vista histórico, esta idea aparece de forma implícita mucho antes de ser formulada como tal. El Nullstellensatz de Hilbert permite sustituir afirmaciones sobre la existencia de ceros comunes de un sistema de ecuaciones polinómicas, es decir, sobre la no vacuidad del conjunto algebraico que dichas ecuaciones definen, por condiciones algebraicas sobre el ideal asociado. Se trata, sin embargo, de un fenómeno todavía ligado a un contexto matemático específico.

El primer uso consciente de la eliminación de cuantificadores como herramienta lógica se debe a Alfred Tarski, en su estudio de la decidibilidad en lógica de primer orden [13]. Mediante procedimientos algorítmicos, Tarski demuestra la eliminación de cuantificadores para cuerpos realmente cerrados. En este punto, la noción aparece ya de forma explícita, aunque fundamentalmente como un método técnico al servicio de la decidibilidad.

La lectura moderna de la eliminación de cuantificadores como propiedad estructural de una teoría se consolida con el desarrollo de la teoría de modelos [7]. Este marco desplaza el énfasis desde procedimientos particulares hacia propiedades globales de teorías. La eliminación de cuantificadores admite entonces una caracterización semántica, que permite reinterpretar de manera unificada los casos de los cuerpos algebraicamente cerrados y realmente cerrados.

El objetivo de este trabajo es, en primer lugar, probar una caracterización semántica de la eliminación de cuantificadores. Para ello se adopta una formulación concreta tomada de [2], cuya demostración constituye el núcleo técnico del trabajo y permite reformular la propiedad en términos estructurales.

En segundo lugar, se aplica este criterio para probar que las teorías de los cuerpos algebraicamente cerrados y de los cuerpos realmente cerrados tienen eliminación de cuantificadores. Este análisis requiere un estudio cuidadoso de ambas teorías, apoyado principalmente en [6] y [8], si bien para la unicidad de la clausura real se sigue el tratamiento más sucinto de [7]. En la exposición de resultados clásicos se han seguido formulaciones habituales en la literatura.

Por último, se muestran aplicaciones de dicha eliminación: en concreto, se obtienen el Nullstellensatz de Hilbert, el Teorema de Ax y una solución al decimoséptimo problema de Hilbert.

2. Teoría de modelos

En esta sección fijamos el marco formal sobre el que trabajaremos.

2.1. Lógica de primer orden: sintaxis y semántica

A continuación presentamos un repaso de los fundamentos de la lógica de primer orden, basado sobre todo en [1].

Un *lenguaje de primer orden* $\mathcal{L}$ se define como un conjunto de símbolos que consta de:
-Un conjunto C de símbolos de constantes.
-Un conjunto $F = \{F_n : n \in \mathbb{N}\}$ de símbolos de función, donde cada F_n agrupa los símbolos de aridad n.
-Un conjunto $R = \{R_k : k \in \mathbb{N}\}$ de símbolos de relación (o predicados), donde cada R_k agrupa los símbolos de aridad k.
Por convención, todo lenguaje $\mathcal{L}$ incluye además los símbolos auxiliares para formar fórmulas: paréntesis "(,)", la lista infinita de variables $x_1, x_2, \ldots$, las conectivas lógicas $\neg, \wedge, \vee, \to, \leftrightarrow$, los cuantificadores $\forall, \exists$ y el símbolo de igualdad lógica "$\doteq$".

Una vez establecemos el lenguaje, construimos las expresiones válidas en él. Los *términos de* $\mathcal{L}$, los cuales llamaremos $\mathcal{L}$*-términos*, se forman de manera inductiva:
- Toda variable x_i es un $\mathcal{L}$-término.
- Toda constante $c \in C$ es un $\mathcal{L}$-término.
- Si $f \in F_m$ y $t_1, \ldots, t_m$ son $\mathcal{L}$-términos, entonces $f(t_1, \ldots, t_m)$ es un $\mathcal{L}$-término.
Con los términos definidos, las *fórmulas atómicas* son aquellas de la forma $t_1 \doteq t_2$ o $R(t_1, \ldots, t_k)$, donde t_i son términos y $R \in R_k$. El conjunto de *fórmulas de* $\mathcal{L}$, que llamaremos $\mathcal{L}$*-fórmulas*, se obtiene cerrando las atómicas bajo las conectivas lógicas $\neg, \wedge$ y el cuantificador $\exists$, adoptando las abreviaturas usuales: escribimos $x \neq y$ en vez de $\neg(x \doteq y)$; también $\varphi \vee \psi$ en vez de $\neg(\neg\varphi \wedge \neg\psi)$, $\varphi \to \psi$ en vez de $\neg(\varphi \wedge \neg\psi)$, $\varphi \leftrightarrow \psi$ en vez de $(\varphi \to \psi) \wedge (\psi \to \varphi)$ y $\forall x\, \varphi$ en vez de $\neg\exists x\, \neg\varphi$.

Las reglas inductivas de formación de términos y fórmulas garantizan que la descomposición de un término o fórmula en sus subexpresiones es única,[1] eliminando cualquier ambigüedad en la manera de poner las paréntesis o en el orden de aplicación de conectivas y cuantificadores.[2]
Gracias a la lectura única, podemos definir de forma no ambigua medidas inductivas de una fórmula. En particular, definimos la *altura de una fórmula* φ, denotada $\mathrm{ht}(\varphi)$, así:
-Si φ es atómica, $\mathrm{ht}(\varphi) = 0$.
-Si $\varphi = \neg\psi$ o $\varphi = \exists x\psi$, entonces $\mathrm{ht}(\varphi) = 1 + \mathrm{ht}(\psi)$.
-Si $\varphi = (\psi \wedge \theta)$, entonces $\mathrm{ht}(\varphi) = 1 + \mathrm{máx}\{\mathrm{ht}(\psi), \mathrm{ht}(\theta)\}$.
De modo análogo se define la *altura de un término*: las variables y constantes tienen altura 0, y si $t \doteq f(t_1, \ldots, t_n)$, entonces $\mathrm{ht}(t) = 1 + \mathrm{máx}\{\mathrm{ht}(t_i) : 1 \leq i \leq n\}$.
Esta medida de altura permite realizar inducciones estructurales sobre fórmulas y términos, demostrando propiedades por inducción en la altura. Usaremos este tipo de razonamiento recurrentemente para probar resultados sobre todas las fórmulas de cierto lenguaje.[3]

Una variable en una fórmula φ se dice *libre* si aparece (al menos una vez) fuera del alcance de los cuantificadores, en caso contrario se dice *ligada*. Denotamos $lib(\varphi)$ al conjunto de variables

[1] (salvo renombre de variables ligadas)
[2] Ver las *Proposiciones 1.3.4 y 1.3.7* en [1].
[3] En [1] las inducciones se formulan sobre la complejidad $c(\cdot)$ (número de apariciones de símbolos de función en los términos y de $\neg, \wedge, \exists$ en las fórmulas). Ambas están bien definidas y decrecen estrictamente en subfórmulas y subtérminos; por tanto, las pruebas por inducción en c se trasladan sin pérdida a inducciones en ht.

libres de φ. Para indicar las variables libres de una fórmula, podemos escribir $\varphi(x_1, \dots, x_n)$ para expresar que las variables libres de φ están entre $x_1, \dots, x_n$. Una fórmula sin variables libres se denomina *sentencia* o *fórmula cerrada*. Un término sin variables se llama *término cerrado*.

Una *teoría* T es un conjunto arbitrario de sentencias de $\mathcal{L}$.

Para dotar de significado a los símbolos, introducimos la noción de $\mathcal{L}$-*estructura*: Una $\mathcal{L}$-estructura $\mathcal{A}$ consiste en un conjunto no vacío A (que llamamos *universo* de $\mathcal{A}$) junto con una interpretación de cada símbolo de $\mathcal{L}$:

- A cada constante $c \in C$ se asocia un elemento $c^{\mathcal{A}} \in A$.
- A cada símbolo de función $f \in F_m$ se asocia una función $f^{\mathcal{A}} \colon A^m \to A$.
- A cada símbolo de relación $R \in R_k$ se asocia un subconjunto $R^{\mathcal{A}} \subseteq A^k$.

Emplearemos letras caligráficas $\mathcal{A}, \mathcal{B}, \dots$ para denotar estructuras y letras romanas $A, B, \dots$ para sus universos.

Decimos que una $\mathcal{L}$-estructura $\mathcal{A}$ es *modelo* de T si *satisface* cada sentencia de T, es decir, si $\mathcal{A} \models \varphi$ para todo $\varphi \in T$. Recordamos la noción de *satisfacibilidad*.

Una *interpretación* en $\mathcal{A}$ es una función $\beta : \{x_1, x_2, \dots\} \to A$ que asigna a cada variable un elemento del universo A.

Vemos cómo se interpreta un término en una $\mathcal{L}$-estructura a partir de una interpretación β: si $t = c$ para una constante c, entonces $t^A[\beta] = c^A$; si $t = x_i$ para una variable, entonces $t^A[\beta] = \beta(x_i)$; y si $t = f(t_1, \dots, t_n)$, con f un símbolo de función de aridad n, se define recursivamente $t^A[\beta] = f^A\big(t_1^A[\beta], \dots, t_n^A[\beta]\big)$.

Con esta interpretación de los términos, podemos definir de forma inductiva la relación de satisfacibilidad para fórmulas:

$\mathcal{A} \models t_1 \doteq t_2[\beta] \Leftrightarrow t_1^{\mathcal{A}}[\beta] = t_2^{\mathcal{A}}[\beta]$, $\mathcal{A} \models R\,(t_1 \dots t_n)[\beta] \Leftrightarrow (t_1^{\mathcal{A}}[\beta], \dots, t_n^{\mathcal{A}}[\beta]) \in R^{\mathcal{A}}$,
$\mathcal{A} \models \neg\psi[\beta] \Leftrightarrow \mathcal{A} \not\models \psi[\beta]$ (no $\mathcal{A} \models \psi[\beta]$), $\mathcal{A} \models (\psi \wedge \chi)[\beta] \Leftrightarrow \mathcal{A} \models \psi[\beta]$ y $\mathcal{A} \models \chi[\beta]$
$\mathcal{A} \models \exists x\, \psi[\beta] \Leftrightarrow$ existe $a \in A$ con $\mathcal{A} \models \psi[\beta_{a/x}]$.

Aquí, $\beta_{a/x}$ denota la interpretación definida por $\beta_{a/x}(x) = a$ y $\beta_{a/x}(y) = \beta(y)$ para $y \neq x$.

Escribiremos $\mathcal{A} \models \varphi[a_1, \dots, a_n]$ para expresar que la fórmula $\varphi(x_1, \dots, x_n)$ se satisface en la estructura $\mathcal{A}$ cuando se interpreta $x_i = a_i$ para $i = 1, \dots, n$.[4]

Si φ es una *sentencia* (no tiene variables libres), entonces su satisfacibilidad no depende de ninguna interpretación: decimos simplemente que φ es *verdadera en* $\mathcal{A}$ (o que φ es *consecuencia lógica* de $\mathcal{A}$) y escribimos $\mathcal{A} \models \varphi$.

La definición anterior formaliza la noción intuitiva de "verdad" en un modelo: $\mathcal{A} \models \varphi$ significa que la estructura $\mathcal{A}$ cumple la propiedad expresada por φ.

Así aparece motivada la definición de *teoría* como conjunto de sentencias, cada una de ellas atrapando una propiedad de las estructuras que nos interesa estudiar.

Decimos que φ es *consecuencia lógica de* T, y escribimos $T \models \varphi$ si toda estructura que satisface todas las sentencias de T también satisface φ, es decir, si $\mathcal{A} \models T$ implica $\mathcal{A} \models \varphi$.

Sean $\mathcal{L} \subseteq \mathcal{L}'$ lenguajes de primer orden. Si $\mathcal{M}' = \langle A \,;$ interpretación de los símbolos de $\mathcal{L}' \rangle$ es una $\mathcal{L}'$-estructura, su *reducto* a $\mathcal{L}$ es $\mathcal{M}'|_{\mathcal{L}} := \langle A \,;$ interpretación de los símbolos de $\mathcal{L} \rangle$.[5] En este caso decimos que $\mathcal{M}'$ es una *expansión* de $\mathcal{M}$ al lenguaje $\mathcal{L}'$. Decimos que una $\mathcal{L}$-fórmula φ es *universalmente válida* (o *una tautología*), si es satisfacible en todas las $\mathcal{L}$-estructuras de la lógica de primer orden.

[4] Esto porque la verdad de una fórmula $\varphi = \varphi(x_1, \dots, x_n)$ en una estructura $\mathcal{A}$ con respecto a una interpretación β depende únicamente de los valores $\beta(x_1), \dots, \beta(x_n)$. Véase la Proposición 1.4.8 en [1].

[5] Interpretados igual que en $\mathcal{M}'$.

Lema 2.1.1. *Sea φ una $\mathcal{L}$-fórmula y $\mathcal{L}' \supseteq \mathcal{L}$. Entonces φ es universalmente válida como fórmula de $\mathcal{L}$ si y solo si lo es como fórmula de $\mathcal{L}'$.*

Demostración. Dada una interpretación α en el dominio A, la evaluación de φ en $\mathcal{M}'$ y en su reducto $\mathcal{M} = \mathcal{M}'|_{\mathcal{L}}$ coincide: $\mathcal{M}' \models \varphi[\alpha]$ si y solo si $\mathcal{M} \models \varphi[\alpha]$. Por tanto basta observar que toda $\mathcal{L}$-estructura $\mathcal{M}$ admite una expansión $\mathcal{M}'$ a $\mathcal{L}'$, lo cual es inmediato asignando arbitrariamente interpretaciones a los símbolos de $\mathcal{L}' \setminus \mathcal{L}$. □

Esto demuestra que la satisfacibilidad es invariante al ampliar el lenguaje, y por tanto no depende de este. Escribimos simplemente $T \models \varphi$ en vez de $T \models_{\mathcal{L}} \varphi$.

Sea s un $\mathcal{L}$-término. Decimos que la variable x es *libre para* s en la $\mathcal{L}$-fórmula φ cuando x aparece libre en φ y ninguna de sus ocurrencias queda bajo el alcance de un cuantificador que capture alguna variable que ocurra en s.

Denotamos por $t_{s/x}$ o $\varphi_{s/x}$ el resultado de sustituir[6] x por s en el término t o en la fórmula φ, respectivamente, entendiendo que la sustitución se realiza cuando x es libre para s en φ (renombrando variables ligadas en caso necesario), lo que permite demostrar el siguiente lema.

Lema 2.1.2. (Lema de sustitución). *Sea $\mathcal{A}$ una $\mathcal{L}$-estructura, y sea β una interpretación.*

1. *Para cualquier término t se cumple $(t_{s/x})^{\mathcal{A}}[\beta] = t^{\mathcal{A}}\big[\beta\ {}_{s^{\mathcal{A}}[\beta]/x}\big]$.*
2. *Para cualquier fórmula φ se cumple $\mathcal{A} \models \varphi_{s/x}[\beta]$ si y solo si $\mathcal{A} \models \varphi\big[\beta\ {}_{s^{\mathcal{A}}[\beta]/x}\big]$.*

Si $1 \leq i \leq n$ y s es un $\mathcal{L}$-término tal que x_i es *libre para s en φ*, nosotros escribiremos $\varphi(x_1, \ldots, x_{i-1}, s, x_{i+1}, \ldots, x_n)$ para denotar φ_{s/x_i}, y cuando el contexto lo permita abreviaremos simplemente por $\varphi(s)$. Análogamente, cuando un $\mathcal{L}$-término t involucre las variables $x_1, \ldots, x_n$, lo escribiremos como $t(x_1, \ldots, x_n)$ y entenderemos $t(x_1, \ldots, x_{i-1}, s, x_{i+1}, \ldots, x_n)$ como t_{s/x_i}.

Finalmente, como es habitual en Matemáticas, cuando se define una estructura lo siguiente que se hace es preguntarse cuándo dos objetos son los mismos desde ese punto de vista:

Sean $\mathcal{A}$ y $\mathcal{B}$ dos $\mathcal{L}$-estructuras. Un *$\mathcal{L}$-monomorfismo* de $\mathcal{A}$ en $\mathcal{B}$ es una función inyectiva $F\colon A \to B$ la cual preserva la interpretación de los símbolos del lenguaje $\mathcal{L}$, es decir:

- Para cada símbolo de constante c de $\mathcal{L}$ se cumple $F(c^A) = c^B$.
- Para cada símbolo de función f de $\mathcal{L}$ de aridad n y para cualesquiera elementos $a_1, \ldots, a_n$ de A se cumple: $F(f^A(a_1, \ldots, a_n)) = f^B(F(a_1), \ldots, F(a_n))$.
- Para cada símbolo de relación R de $\mathcal{L}$ de aridad m y para cualesquiera elementos $a_1, \ldots, a_m$ de A se cumple: $(a_1, \ldots, a_m) \in R^A$ si y solo si $(F(a_1), \ldots, F(a_m)) \in R^B$.

Un *isomorfismo* es un monomorfismo sobreyectivo. Decimos que dos $\mathcal{L}$-estructuras $\mathcal{A}$ y $\mathcal{B}$ son *isomorfas* si existe un isomorfismo entre ellas. Escribimos $\mathcal{A} \cong \mathcal{B}$.

En particular, si $\mathcal{A}$ y $\mathcal{B}$ son modelos de una misma teoría T, entonces $\mathcal{A} \cong \mathcal{B}$ como $\mathcal{L}$-estructuras equivale a que $\mathcal{A}$ y $\mathcal{B}$ son isomorfos según la noción propia de la teoría T.

Hasta ahora hemos enfocado la verdad lógica desde el punto de vista semántico, es decir, en términos de estructuras y satisfacibilidad en un modelo. Sin embargo, también se puede abordar desde una perspectiva *sintáctica*, tras definir un *sistema deductivo formal*: un conjunto de *axiomas lógicos* y *reglas de inferencia*.

En nuestro sistema incluímos como *axiomas lógicos* todas las *tautologías de la lógica proposicional* $((p \vee \neg p, (p \to q) \leftrightarrow (\neg p \vee q)...)$, *axiomas de la igualdad* $(\forall x x \doteq x, \forall x, y\ x \doteq y \to y \doteq x$

[6] La sustitución se define por inducción sobre la altura (complejidad) de términos y fórmulas; véase la sección 2.1 de [1].

etc.), y el *axioma de* $\exists$*-sustitución* ($(\varphi_{t/x} \to \exists x\, \varphi)$, con t un $\mathcal{L}$-término y x una variable libre para t en φ.) Cada una de estas fórmulas es universalmente válida.

Además, cuando trabajamos dentro de una teoría T, consideramos que todas las fórmulas de T están disponibles como premisas iniciales.

Un requisito esencial de cualquier sistema deductivo es que cada regla de inferencia debe preservar la validez universal: si las premisas son verdaderas en todos los modelos de T, entonces la conclusión inferida también lo será. Como reglas de inferencia fundamentales tomaremos *Modus Ponens* (MP) (de φ y $\varphi \to \psi$, inferir ψ) y la *regla de* $\exists$*-introducción* (de $\varphi \to \psi$ inferir $\exists x\varphi \to \psi$ con $x \notin lib(\psi)$).

Decimos que una $\mathcal{L}$-fórmula (generalmente una sentencia) φ es *demostrable* (o *derivable*) *en* T (y escribimos $T \vdash_{\mathcal{L}} \varphi$) si existe una secuencia finita de fórmulas $\varphi_1, \varphi_2, \ldots, \varphi_n = \varphi$ tal que cada φ_i es: o bien un axioma lógico del sistema, o una sentencia de T , o bien se obtiene de fórmulas anteriores de la secuencia mediante una aplicación de una regla de inferencia válida.

Tal secuencia se llama una *demostración* de φ a partir de T.

Además, diremos que una $\mathcal{L}$-fórmula φ es *demostrable* y escribiremos $\vdash_{\mathcal{L}} \varphi$ si existe una demostración de φ partiendo de $T = \emptyset$. En tal caso, φ se comporta efectivamente como un axioma lógico. Del mismo modo contamos con reglas de deducción que no forman parte del sistema primitivo pero cuya validez puede demostrarse dentro de él. Por ejemplo, usaremos la $\wedge - regla$ (para cualesquiera $\mathcal{L}$-fórmulas φ, ψ, $T \vdash_{\mathcal{L}} \varphi$ y $T \vdash_{\mathcal{L}} \psi$ si y solo si $T \vdash_{\mathcal{L}} (\varphi \wedge \psi)$).

La definición de *demostrabilidad* capta la noción de *prueba* en el sistema formal: partiendo de axiomas y usando reglas permitidas, llegamos a la fórmula φ. Nótese que esta es una noción de *verdad* completamente sintáctica, que no hace referencia a ninguna estructura o significado de las fórmulas, solo a la manipulación de símbolos según ciertas reglas.

Una teoría T es *consistente* si no prueba una contradicción ($T \nvdash \bot$). Equivalentemente, si no existe una fórmula φ tal que $T \vdash_{\mathcal{L}} \varphi$ y $T \vdash_{\mathcal{L}} \neg\varphi$. Por otra parte, diremos que una teoría T es *completa* si para toda sentencia ψ en el lenguaje, T demuestra ψ o demuestra $\neg\psi$.

Dado que la deducción formal pretende capturar el concepto de consecuencia lógica, esperamos que se cumpla al menos que *si* $T \vdash_{\mathcal{L}} \varphi$*, entonces* $T \models \varphi$.

Teorema 2.1.3 (Teorema de validez)**.** *Para cualquier teoría T (de primer orden) y cualquier fórmula φ, si $T \vdash_{\mathcal{L}} \varphi$ entonces $T \models \varphi$. En particular, ninguna teoría T permite demostrar una fórmula que no sea una de sus consecuencias lógicas.*

Idea de la demostración. El argumento se realiza por inducción sobre la longitud de la demostración de φ. Por construcción del sistema deductivo, cada paso de la demostración mantiene la propiedad de ser consecuencia lógica de T. Al alcanzar φ, concluimos que φ es verdadera en todo modelo de T, i.e. $T \models \varphi$. □

En 1929, Gödel demostró que el recíproco también es cierto.

Teorema 2.1.4 (Teorema de completitud de Gödel)**.** *Para cualquier teoría T de primer orden y cualquier fórmula φ, $T \models \varphi$ si y solo si $T \vdash_{\mathcal{L}} \varphi$.*

Observación 2.1.5. Una demostración de este resultado se incluye en el Apéndice A.1, donde se muestra su equivalencia con el Teorema de Henkin (Teorema A.1.4): una teoría es consistente si y solo si tiene un modelo.

2.2. Herramientas de teoría de modelos

Gracias a la completitud, nuestro enfoque semántico queda plenamente justificado: trabajaremos con estructuras y modelos, y emplearemos $\models$ en vez de $\vdash$. A continuación, desarrollaremos los resultados y herramientas propias de esta área que nos llevarán a caracterizar semánticamente la eliminación de cuantificadores, siguiendo el enfoque propuesto en [2].

El Teorema de compacidad

Otro metateorema principal de la lógica de primer orden es el Teorema de compacidad.

Teorema 2.2.1 (Compacidad)**.** *Sea T una $\mathcal{L}$-teoría. Entonces T tiene un modelo si y solo si todo subconjunto finito de T tiene un modelo.*

Demostración. Como $T \vdash \varphi$[7] si y solamente si existe un subconjunto finito $T_0 \subseteq T$ tal que $T_0 \vdash \varphi$ (Observación A.1.10), entonces una teoría es consistente si y solo si todos sus subconjuntos finitos lo son, y por el Teorema A.1.4 tenemos el resultado. □

Observación 2.2.2. Sea T una $\mathcal{L}$-teoría y Γ un conjunto de $\mathcal{L}$-fórmulas tales que $T \cup \Gamma \models \varphi$. Por el Teorema de compacidad junto a la Observación A.1.2, existe un entero $n \geq 1$ y fórmulas $\gamma_1, \ldots, \gamma_n \in \Gamma$ tales que $T \models (\gamma_1 \wedge \cdots \wedge \gamma_n) \to \varphi$.

El método del diagrama

Recordamos algunas nociones fundamentales más.

Sean $\mathcal{A}$ y $\mathcal{B}$ dos $\mathcal{L}$-estructuras. Decimos que $\mathcal{A}$ es *subestructura* de $\mathcal{B}$ (y escribimos $\mathcal{A} \subseteq \mathcal{B}$) si $A \subseteq B$ y la aplicación inclusión $\iota : A \hookrightarrow B$ es un $\mathcal{L}$-monomorfismo. Decimos que $\mathcal{B}$ es una *extensión* de $\mathcal{A}$.

Observación 2.2.3. Si $\mathcal{A} \subseteq \mathcal{B}$, $\psi(x_1, \ldots, x_n)$ es una fórmula libre de cuantificadores y $\bar{a} \in A^n$, entonces se tiene $\mathcal{A} \models \psi[\bar{a}]$ si y solo si $\mathcal{B} \models \psi[\bar{a}]$.

En efecto, al ser ψ libre de cuantificadores, su verdad depende únicamente de la evaluación de los términos y de las relaciones sobre los elementos de A, que coinciden en $\mathcal{A}$ y en $\mathcal{B}$. La afirmación se prueba formalmente por inducción sobre la altura de ψ.

Decimos que $\mathcal{A}$ es *subestructura elemental* de $\mathcal{B}$ (y escribimos $\mathcal{A} \preceq \mathcal{B}$) si $\mathcal{A} \subseteq \mathcal{B}$ y, además, para toda fórmula $\varphi(\bar{x})$ y todo $\bar{a} \in A^n$, $\mathcal{A} \models \varphi[\bar{a}]$ si y solo si $\mathcal{B} \models \varphi[\bar{a}]$.

En la práctica a menudo se desea construir un modelo de alguna teoría que contenga una estructura dada como subestructura o subestructura elemental. Vemos que estas propiedades pueden codificarse en teorías adecuadas.

Definición 2.2.4. Sea $\mathcal{M}$ una $\mathcal{L}$-estructura. Consideremos el lenguaje $\mathcal{L}_M$ obtenido de $\mathcal{L}$ añadiendo un nuevo símbolo de constante c_m por cada elemento $m \in M$. Entonces $\mathcal{M}$ admite una expansión natural al lenguaje $\mathcal{L}_M$, interpretando cada c_m por el propio m.

El *diagrama completo* de $\mathcal{M}$, denotado por $D(\mathcal{M})$, es el conjunto de las $\mathcal{L}_M$-sentencias de la forma $\varphi(c_{m_1}, \ldots, c_{m_n})$, donde $\varphi(x_1, \ldots, x_n)$ es una $\mathcal{L}$-fórmula y $m \in M^n$ es una n-tupla tal que $\mathcal{M} \models \varphi[m_1, \ldots, m_n]$. El *diagrama simple* de $\mathcal{M}$, denotado por $\Delta(\mathcal{M})$, se define de la misma manera, exigiendo además que φ sea una fórmula libre de cuantificadores.

[7] Como consecuencia del Teorema de completitud (y el Lema 2.1.1), escribimos $T \vdash \varphi$ en vez de $T \vdash_{\mathcal{L}} \varphi$, aunque en lo que sigue usaremos siempre $\models$.

Proposición 2.2.5. *Los reductos al lenguaje $\mathcal{L}$ de modelos de $D(\mathcal{M})$ corresponden, salvo $\mathcal{L}$-isomorfismo, a extensiones elementales de $\mathcal{M}$.*

Demostración. Sea $\mathcal{N}' \models D(\mathcal{M})$ y $\mathcal{N} := \mathcal{N}'|_{\mathcal{L}}$. Definimos $\iota\colon M \to N$ mediante $\iota(m) := c_m^{\mathcal{N}'}$.

Si $m \neq n$ en M, como la fórmula $x \neq y$ es verdadera en $\mathcal{M}$ para (m, n), la sentencia $c_m \neq c_n$ pertenece a $D(\mathcal{M})$, luego $\mathcal{N}' \models c_m \neq c_n$. Por tanto $c_m^{\mathcal{N}'} \neq c_n^{\mathcal{N}'}$ e $\iota(m) \neq \iota(n)$. Así, ι es inyectiva.

Ahora, para cada constante $d \in \mathcal{L}$, $c_{d^{\mathcal{M}}} \doteq d \in D(\mathcal{M})$, luego $\iota(d^{\mathcal{M}}) = c_{d^{\mathcal{M}}}^{\mathcal{N}'} = d^{\mathcal{N}'} = d^{\mathcal{N}}$.

Para f de aridad k y $m_1, \ldots, m_k \in M$, $c_{f^{\mathcal{M}}(m_1,\ldots,m_k)} \doteq f(c_{m_1}, \ldots, c_{m_k}) \in D(\mathcal{M})$, y al interpretar en $\mathcal{N}'$ obtenemos $\iota(f^{\mathcal{M}}(m_1, \ldots, m_k)) = f^{\mathcal{N}}(\iota(m_1), \ldots, \iota(m_k))$.

Finalmente, si $(m_1, \ldots, m_k) \in R^{\mathcal{M}}$, $R(c_{m_1}, \ldots, c_{m_k}) \in D(\mathcal{M})$ y $\mathcal{N}' \models R(c_{m_1}, \ldots, c_{m_k})$, luego $(\iota(m_1), \ldots, \iota(m_k)) \in R^{\mathcal{N}}$; de igual modo, si $(m_1, \ldots, m_k) \notin R^{\mathcal{M}}$, $\neg R(c_{m_1}, \ldots, c_{m_k}) \in D(\mathcal{M})$ y $\mathcal{N}' \models \neg R(c_{m_1}, \ldots, c_{m_k})$, esto es, $(\iota(m_1), \ldots, \iota(m_k)) \notin R^{\mathcal{N}}$.

Lo anterior demuestra que $\iota\colon \mathcal{M} \to \mathcal{N}$ es un $\mathcal{L}$-monomorfismo, y por tanto identificando $\mathcal{M}$ con su imagen obtenemos una copia isomorfa de $\mathcal{M}$ como subestructura de $\mathcal{N}$.

Veamos que es elemental. Sea $\varphi(x_1, \ldots, x_k)$ una $\mathcal{L}$-fórmula y $m_1, \ldots, m_k \in M$. Por definición de $D(\mathcal{M})$, $\mathcal{M} \models \varphi[m_1, \ldots, m_k]$ si y solo si $\varphi(c_{m_1}, \ldots, c_{m_k}) \in D(\mathcal{M})$. Como $\mathcal{N}' \models D(\mathcal{M})$, se tiene $\mathcal{N}' \models \varphi(c_{m_1}, \ldots, c_{m_k})$, y por el Lema de sustitución se obtiene $\mathcal{N} \models \varphi[\iota(m_1), \ldots, \iota(m_k)]$. En consecuencia, $\mathcal{M} \models \varphi[m_1, \ldots, m_k]$ si y solo si $\mathcal{N} \models \varphi[\iota(m_1), \ldots, \iota(m_k)]$, y por tanto $\iota(\mathcal{M}) \preceq \mathcal{N}$. En particular, $\mathcal{N}$ contiene una subestructura elemental $\mathcal{L}$-isomorfa a $\mathcal{M}$.

Por otra parte, si $\mathcal{M} \preceq \mathcal{N}$ es una extensión elemental, consideramos la expansión $\mathcal{N}'$ de $\mathcal{N}$ al lenguaje $\mathcal{L}_M$ que interpreta cada constante c_m por $m \in M$. Dada $\varphi(c_{m_1}, \ldots, c_{m_k}) \in D(\mathcal{M})$, por definición se tiene $\mathcal{M} \models \varphi[m_1, \ldots, m_k]$. Como $\mathcal{M} \preceq \mathcal{N}$, se sigue que $\mathcal{N} \models \varphi[m_1, \ldots, m_k]$, y por el Lema de sustitución obtenemos $\mathcal{N}' \models \varphi(c_{m_1}, \ldots, c_{m_k})$. En consecuencia, $\mathcal{N}' \models D(\mathcal{M})$. □

Proposición 2.2.6. *Los reductos al lenguaje $\mathcal{L}$ de modelos de $\Delta(\mathcal{M})$ corresponden, salvo $\mathcal{L}$-isomorfismo, a extensiones de $\mathcal{M}$.*

Demostración. La demostración de la primera parte es análoga a la de la proposición anterior, sustituyendo $D(\mathcal{M})$ por $\Delta(\mathcal{M})$.

Recíprocamente, si $\mathcal{M} \subseteq \mathcal{N}$ es una subestructura, la expansión natural $\mathcal{N}'$ de $\mathcal{N}$ al lenguaje $\mathcal{L}_M$ satisface $\Delta(\mathcal{M})$. En efecto, por la Observación 2.2.3, toda fórmula libre de cuantificadores con parámetros en M verdadera en $\mathcal{M}$ se preserva en $\mathcal{N}$, y por el Lema de sustitución se concluye que $\mathcal{N}' \models \Delta(\mathcal{M})$. □

Expansiones por definición

Suele ser útil enriquecer el lenguaje con símbolos para funciones, relaciones, o constantes definibles. Veamos esto formalmente.

Notación. $\exists! x\, \psi$ abrevia $\exists x\Big(\psi(x) \wedge \forall y\big(\psi(y) \to x \doteq y\big)\Big)$ ("existe un único x tal que ψ").

Definición 2.2.7 (Expansión por definición)**.** Sea T una teoría en un lenguaje $\mathcal{L}$ y sea $\mathcal{L}' \supseteq \mathcal{L}$. Supongamos que para cada símbolo de $\mathcal{L}' \setminus \mathcal{L}$ disponemos de:

- Para todo símbolo de relación $R \in \mathcal{L}' \setminus \mathcal{L}$ de aridad n, una $\mathcal{L}$-fórmula $\varphi_R(x_1, \ldots, x_n)$.
- Para todo símbolo de función $f \in \mathcal{L}' \setminus \mathcal{L}$ de aridad n, una $\mathcal{L}$-fórmula $\varphi_f(x_0, x_1, \ldots, x_n)$ tal que $T \models \forall x_1 \cdots \forall x_n\, \exists! x_0\, \varphi_f(x_0, x_1, \ldots, x_n)$.
- Para todo símbolo de constante $c \in \mathcal{L}' \setminus \mathcal{L}$, una $\mathcal{L}$-fórmula $\varphi_c(x_0)$ tal que $T \models \exists! x_0\, \varphi_c(x_0)$.

Entonces la $\mathcal{L}'$-teoría T' que se obtiene añadiendo a T los siguientes *axiomas definitorios*:

1. Para cada relación $R \in \mathcal{L}' \setminus \mathcal{L}$ de aridad n: $\forall x_1 \cdots \forall x_n \, \big(\varphi_R(x_1, \ldots, x_n) \leftrightarrow R(x_1, \ldots, x_n)\big)$.
2. Para cada función $f \in \mathcal{L}' \setminus \mathcal{L}$ de aridad n: $\forall x_1 \cdots \forall x_n \, \varphi_f\big(f(x_1, \ldots, x_n), x_1, \ldots, x_n\big)$.
3. Para cada constante $c \in \mathcal{L}' \setminus \mathcal{L}$: $\varphi_c(c)$.

es una *expansión por definición* de T.

Vamos a motivar esta noción.

Definición 2.2.8. Sea $\mathcal{L}$ un lenguaje de primer orden y sea $R \notin \mathcal{L}$ un símbolo de relación n-ario. Sea T una $\mathcal{L} \cup \{R\}$-teoría.

- Decimos que T *define implícitamente* R si, para toda $\mathcal{L}$-estructura $\mathcal{M}$ de universo M y cualesquiera relaciones $R_1, R_2 \subseteq M^n$ tales que $\langle \mathcal{M}, R_1 \rangle \models T$ y $\langle \mathcal{M}, R_2 \rangle \models T$, se tiene $R_1 = R_2$.
- Decimos que T *define explícitamente* R si existe una $\mathcal{L}$-fórmula $\varphi_R(x_1, \ldots, x_n)$ tal que

$$T \models \forall x_1 \cdots \forall x_n \big(\varphi_R(x_1, \ldots, x_n) \leftrightarrow \ R(x_1, \ldots, x_n)\big).$$

Proposición 2.2.9. *Si T define explícitamente R, entonces T define implícitamente R.*

Demostración. Supongamos que $T \models \forall \bar{x}\big(\varphi(\bar{x}) \leftrightarrow R(\bar{x})\big)$ para cierta $\mathcal{L}$-fórmula $\varphi(\bar{x})$. Sean $\mathcal{M}$ una $\mathcal{L}$-estructura y $R_1, R_2 \subseteq M^n$ dos interpretaciones de R tales que $\langle \mathcal{M}, R_i \rangle \models T$ para $i = 1, 2$. Entonces en cada uno de ellos, para todo $\bar{a} \in M^n$ se cumple que $R_i(\bar{a})$ si y solo si $\mathcal{M} \models \varphi[\bar{a}]$. Por tanto, ambas relaciones R_1 y R_2 coinciden con el conjunto de tuplas $\bar{a}$ tales que $\varphi(\bar{x})$ se satisface en $\mathcal{M}$, y en consecuencia $R_1 = R_2$. □

Observación 2.2.10. El recíproco también es cierto, y el enunciado completo se conoce como el *Teorema de definibilidad de Beth*: una teoría define R explicitamente si y solo si la define implícitamente. Este teorema se extiende de forma análoga a símbolos de función y de constante, y es muy útil porque garantiza que los axiomas definitorios fijan de manera única la interpretación de cualquier símbolo nuevo, lo que permite extender cualquier modelo de T a un modelo de T' de forma única y construir *expansiones conservativas.*

Definición 2.2.11. Sea T una teoría en un lenguaje $\mathcal{L}$ y sea T' una teoría en un lenguaje $\mathcal{L}' \supseteq \mathcal{L}$ tal que $T' \supseteq T$. Decimos que T' es una *expansión conservativa* de T si, para toda $\mathcal{L}$-sentencia ψ,

$$T \models \psi \quad \text{si y solo si} \quad T' \models \psi.$$

Proposición 2.2.12. *Toda expansión por definición T' de una teoría T es una expansión conservativa de T.*

Demostración. Consideremos una $\mathcal{L}$-sentencia ψ.
Si $T \models \psi$, entonces claramente $T' \models \psi$, ya que T' contiene a T. Supongamos ahora $T' \models \psi$. Sea $\mathcal{M}$ un modelo arbitrario de T. Como T' es una expansión por definición de T, existe una (y solo una) expansión $\mathcal{M}'$ de $\mathcal{M}$ al lenguaje $\mathcal{L}'$ que satisface todos los axiomas definitorios de T'. En efecto, para cada nuevo símbolo de relación $R \in \mathcal{L}' \setminus \mathcal{L}$ definimos $R^{\mathcal{M}'} = \big\{\bar{a} \in M^n : \mathcal{M} \models \varphi_R[\bar{a}]\big\}$, donde φ_R es la fórmula que lo definía en T'. Para cada nuevo símbolo de función $f \in \mathcal{L}' \setminus \mathcal{L}$ de aridad n tomamos $f^{\mathcal{M}'}(a_1, \ldots, a_n)$ como el único $b \in M$ tal que $\mathcal{M} \models \varphi_f[b, a_1, \ldots, a_n]$, que existe y es único porque $T' \models \forall \bar{x} \, \exists! x_0 \, \varphi_f(x_0, \bar{x})$. Finalmente, para cada nueva constante $c \in \mathcal{L}' \setminus \mathcal{L}$ definimos $c^{\mathcal{M}'}$ como el único $a \in M$ tal que $\mathcal{M} \models \varphi_c[a]$. De este modo queda determinada de manera única la expansión $\mathcal{M}'$. Dado que ψ no emplea símbolos de $\mathcal{L}' \setminus \mathcal{L}$, se cumple que $\mathcal{M}' \models \psi$ implica $\mathcal{M} \models \psi$. Esto prueba que ψ es verdadera en todo modelo de T, es decir $T \models \psi$. □

3. Eliminación de cuantificadores: criterios semánticos

Estamos listos para hablar sobre la eliminación de cuantificadores.

Recordamos que dada una $\mathcal{L}$-teoría T, dos $\mathcal{L}$-fórmulas $\varphi(\bar{x})$ y $\psi(\bar{x})$ se dicen *equivalentes en* T si $T \models \forall \bar{x}\ \big(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x})\big)$, lo que viene a decir que en T comparten el mismo valor de verdad, y escribimos $\varphi \sim_T \psi$. Se llaman *lógicamente equivalentes* si son equivalentes en la teoría vacía, es decir, se cumple $\models \forall \bar{x}\ \big(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x})\big)$, y escribimos $\varphi \sim \psi$.

Recordamos también que dada una $\mathcal{L}$-fórmula arbitraria φ, podemos transformarla en una fórmula equivalente en *forma prenexa*, es decir, de la forma

$$Q_1 x_1\, Q_2 x_2 \cdots Q_n x_n\, \psi(x_1, \ldots, x_n, \bar{y}),$$

donde cada $Q_i \in \{\forall, \exists\}$ y ψ no contiene cuantificadores. A continuación exponemos brevemente los pasos del procedimiento; seguimos [3].

1. *Rectificación.* Renombramos las variables ligadas para que ninguna aparezca ligada por más de un cuantificador y para evitar conflictos con variables libres.

   Ejemplo: $\forall x\, \exists x\, P(x) \ \rightsquigarrow\ \forall x\, \exists y\, P(y)$.

2. *Eliminación de bicondicionales.* Sustituimos $\varphi \leftrightarrow \psi$ por $(\varphi \to \psi) \wedge (\psi \to \varphi)$.

3. *Eliminación de condicionales.* Sustituimos $\varphi \to \psi$ por $\neg\varphi \vee \psi$.

4. *Empujar negaciones.* Usamos las leyes de De Morgan y las equivalencias con cuantificadores: $\neg(\varphi \wedge \psi) \sim \neg\varphi \vee \neg\psi$, $\neg(\varphi \vee \psi) \sim \neg\varphi \wedge \neg\psi$, $\neg\forall x\, \varphi \sim \exists x\, \neg\varphi$, $\neg\exists x\, \varphi \sim \forall x\, \neg\varphi$. De este modo las negaciones afectan solo a fórmulas atómicas.

5. *Extracción de cuantificadores.* Llevamos todos los cuantificadores al frente aplicando equivalencias como: $(\forall x\, \varphi) \wedge \psi \ \sim\ \forall x(\varphi \wedge \psi)$, $\psi \vee (\exists x\, \varphi) \ \sim\ \exists x(\psi \vee \varphi)$, con la precaución de renombrar variables ligadas para evitar captura.

Antes de pasar a demostrar un resultado clave, recordamos finalmente que dada una $\mathcal{L}$-estructura $\mathcal{A}$ de universo A y $S \subseteq A$, la *subestructura generada por* S *en* $\mathcal{A}$, denotada $\langle S \rangle_{\mathcal{A}}$, es la mínima subestructura de $\mathcal{A}$ cuyo universo contiene a S. El siguiente resultado corresponde al Lema 1.4.4. de [1].

Lema 3.0.1. *Sea $\mathcal{A}$ una $\mathcal{L}$-estructura de universo A y S un subconjunto no vacío de A. Entonces, el universo de $\langle S \rangle_{\mathcal{A}}$ es:*

$$X := \{\, t^{\mathcal{A}}[\alpha] : t \text{ es un } \mathcal{L}\text{-término},\ \alpha : \{x_1, x_2, \ldots\} \to X \text{ una interpretación}\}.$$

La eliminación de cuantificadores admite la siguiente caracterización semántica.

Teorema 3.0.2. *Sea T una $\mathcal{L}$-teoría, $n \geq 1$ un número natural y $\varphi(x_1, \ldots, x_n)$ una $\mathcal{L}$-fórmula. Las siguientes propiedades son equivalentes:*

1. *Existe una fórmula sin cuantificadores $\psi(x_1, \ldots, x_n)$ tal que φ y ψ son equivalentes en T.*

2. *Sean $\mathcal{M}$ y $\mathcal{N}$ dos modelos de T y sea $\mathcal{A}$ una subestructura común de $\mathcal{M}$ y $\mathcal{N}$. Entonces, para toda tupla $\bar{a} \in A^n$,*

$$\mathcal{M} \models \varphi[\bar{a}] \quad \textit{si y solo si} \quad \mathcal{N} \models \varphi[\bar{a}].$$

Demostración. Veamos que (1) implica (2). Si $\mathcal{M}$ y $\mathcal{N}$ son modelos de T que tienen a $\mathcal{A}$ como subestructura común y si $\varphi(x_1,\dots,x_n)$ es equivalente en T a la fórmula libre de cuantificadores $\psi(x_1,\dots,x_n)$, por la Observación 2.2.3, para $\bar{a}\in A^n$ se tiene

$$\mathcal{M}\models\varphi[\bar{a}] \iff \mathcal{M}\models\psi[\bar{a}] \iff \mathcal{A}\models\psi[\bar{a}] \iff \mathcal{N}\models\psi[\bar{a}] \iff \mathcal{N}\models\varphi[\bar{a}].$$

Finalmente, veamos que (2) implica (1). Sea $\varphi(x_1,\dots,x_n)$ una $\mathcal{L}$-fórmula que satisface (2). Sea el conjunto de $\mathcal{L}$-fórmulas $\Gamma(\bar{x}) := \{\chi(\bar{x}) \text{ sin cuantificadores} \mid T\models\forall\bar{x}(\varphi(\bar{x})\to\chi(\bar{x}))\}$. Sea $C:=\{c_1,\dots,c_n\}$ con $c_1,\dots,c_n$ constantes nuevas y sea $\Gamma(\bar{c}) = \{\chi(c_1,\dots,c_n) : \chi(\bar{x})\in\Gamma(\bar{x})\}$ una $\mathcal{L}\cup C$-teoría.

Afirmación. Se cumple que $T\cup\Gamma(\bar{c})\models\varphi(\bar{c})$.
Demostración. Si no fuera así, existiría un modelo $\mathcal{M}'\models T\cup\Gamma(\bar{c})\cup\{\neg\varphi(\bar{c})\}$.

Sea $\mathcal{A}' := \langle c_1^{\mathcal{M}'},\dots,c_n^{\mathcal{M}'}\rangle_{\mathcal{M}'}$ la $\mathcal{L}\cup C$-subestructura de $\mathcal{M}'$ generada por las interpretaciones de las constantes en C. Vamos a probar que $\Sigma := T\cup\Delta(\mathcal{A}')\cup\{\varphi(\bar{c})\}$ tiene un modelo.

En caso contrario, $T\cup\Delta(\mathcal{A}')\models\neg\varphi(\bar{c})$.

Por el lema anterior,

$$A' = \{\, t^{\mathcal{M}'}[\alpha] : t(\bar{x}) \text{ es un } \mathcal{L}\cup C\text{-término},\ \alpha:\{x_1,\dots,x_n\}\to\{c_1^{\mathcal{M}'},\dots,c_n^{\mathcal{M}'}\}\,\}.$$

Sea $C' = \{c_t : t \text{ es un } \mathcal{L}\cup C\text{-término cerrado }\}$.[8]

Por definición,

$$\Delta(\mathcal{A}') = \{\chi(c_{t_1},\dots,c_{t_m}) : \chi(x_1,\dots,x_m)\ \mathcal{L}\cup C\text{-fórmula s. c. y } \mathcal{A}'\models\chi[t_1^{\mathcal{M}'}[\bar{c}],\dots,t_m^{\mathcal{M}'}[\bar{c}]]\}.$$

Obsérvese que este diagrama simple define cada una de las constantes c_t en el lenguaje $\mathcal{L}\cup C'$, ya que para cada $\mathcal{L}\cup C$-término $t(\bar{x})$ podemos considerar la $\mathcal{L}\cup C$ -fórmula $\chi(y) : y\doteq t(c_1,\dots,c_n)$, y puesto que claramente $\mathcal{A}'\models\chi[t^{\mathcal{M}'}[\bar{c}]]$, deducimos que $c_t\doteq t(c_1,\dots,c_n)\in\Delta(\mathcal{A}')$.

Sea $\Delta_C(\mathcal{A}')$ el conjunto de las $\mathcal{L}\cup C$-sentencias que pertenecen a $\Delta(\mathcal{A}')$. Vemos que la $\mathcal{L}\cup C'$-teoría $\Delta(\mathcal{A}')$ es una expansión conservativa de $\Delta_C(\mathcal{A}')$. Sea ψ una $\mathcal{L}\cup C$-sentencia tal que $\Delta(\mathcal{A}')\models\psi$. Veamos que $\mathcal{U}\models\psi$ para cada $\mathcal{U}\models\Delta_C(\mathcal{A}')$. La idea de la demostración sigue los mismos pasos que la de la Proposición 2.2.12 (ya que $\Delta(\mathcal{A}')$ es esencialmente una expansión por definición de $\Delta_C(\mathcal{A}')$). En efecto, existe una única expansión $\mathcal{U}'$ de $\mathcal{U}$ al lenguaje $\mathcal{L}\cup C'$ interpretando las constantes nuevas en $C'\setminus C$ mediante las $\mathcal{L}\cup C$-fórmulas que hemos observado en el parrafo anterior. Basta por tanto demostrar que $\mathcal{U}'\models\Delta(\mathcal{A}')$. Si no fuese el caso, entonces existiría una $\mathcal{L}\cup C$-fórmula $\chi(y_1,\dots,y_m)$ sin cuantificadores y $\mathcal{L}$-términos $t_1,\dots,t_m$ tales que $\mathcal{A}'\models\chi[t_1^{\mathcal{M}'}[\bar{c}],\dots,t_m^{\mathcal{M}'}[\bar{c}]]$, pero sin embargo $\mathcal{U}'\models\neg\chi(c_{t_1},\dots,c_{t_m})$. En particular, tendríamos que $\mathcal{U}\models\neg\chi[t_1^{\mathcal{M}'}[\bar{c}],\dots,t_m^{\mathcal{M}'}[\bar{c}]]$, lo cual es una contradicción ya que $\chi(t_1(\bar{c}),\dots,t_m(\bar{c}))\in\Delta_C(\mathcal{A}')$.

Esto demuestra que $T\cup\Delta_C(\mathcal{A}')\models\neg\varphi(\bar{c})$.

Ahora, vemos que $\Gamma(\bar{c})\subseteq\Delta(\mathcal{A}')$. En efecto, como $\mathcal{A}'$ es una $\mathcal{L}\cup C$-subestructura de $\mathcal{M}'$, toda fórmula sin cuantificadores $\chi(\bar{c})$ que sea verdadera en $\mathcal{M}'$ también lo es en $\mathcal{A}'$. Dado que por definición $\Delta(\mathcal{A}')$ contiene exactamente las $\mathcal{L}\cup C'$-fórmulas sin cuantificadores satisfacibles en $\mathcal{A}'$, y que en la ampliación C' identificamos el símbolo que nombra a cada $c_i^{\mathcal{M}'}$ con el propio c_i, resulta que en este caso la fórmula que entra en $\Delta(\mathcal{A}')$ es precisamente $\chi(\bar{c})$, sin necesidad de modificaciones adicionales.

Por la Observación 2.2.2, existen $\xi_1(\bar{c}),\dots,\xi_k(\bar{c})\in\Delta_C(\mathcal{A}')$ con $T\models\xi(\bar{c})\to\neg\varphi(\bar{c})$, donde $\xi(\bar{c}) := \bigwedge_{i=1}^k\xi_i(\bar{c})$. Como los símbolos c_i no aparecen en T, ni en $\varphi(\bar{x})$ ni en $\xi(\bar{x})$, por la Observación A.1.6 $T\models\forall\bar{x}(\xi(\bar{x})\to\neg\varphi(\bar{x}))$, luego $T\models\forall\bar{x}(\varphi(\bar{x})\to\neg\xi(\bar{x}))$[9], y $\neg\xi(\bar{x})\in\Gamma(\bar{x})$ por

[8] Podemos identificar cada c_i con el símbolo que nombra a $c_i^{\mathcal{M}'}$, de modo que $C'\supseteq C$. Nótese también que no necesitamos arrastrar la referencia explícita a las distintas interpretaciones α, ya que toda interpretación de las variables de un término $s(\bar{x})$ en $\{c_1^{\mathcal{M}'},\dots,c_n^{\mathcal{M}'}\}$ queda recogida en algún término cerrado de $L\cup C$, obtenido al reordenar adecuadamente las variables en s y sustituir x_i por c_i.

[9] $(A\to B)\to(\neg B\to\neg A)$ es una tautología, y aplicamos MP.

definición. En particular, $\neg\xi(\bar{c}) \in \Gamma(\bar{c}) \subseteq \Delta(\mathcal{A}')$, pero también $\xi(\bar{c}) \in \Delta(\mathcal{A}')$, contradicción.

Lo anterior prueba que Σ tiene un modelo, a saber $\mathcal{N}'$, que también es modelo de $\Delta(\mathcal{A}')$. Por la Proposición 2.2.6, $\mathcal{N} := \mathcal{N}' \restriction_{\mathcal{L}}$ contiene cierto $\mathcal{B}' \cong \mathcal{A}'$ como subestructura, los identificamos.

Sean $\mathcal{M} := \mathcal{M}' \restriction_{\mathcal{L}}$, $\mathcal{A} := \mathcal{A}' \restriction_{\mathcal{L}}$.

Se tiene que $\mathcal{A} \subseteq \mathcal{N}, \mathcal{M}$ es una subestructura común de $\mathcal{N}$ y $\mathcal{M}$ tal que, con $a_i = c_i^{\mathcal{M}'}$, $\mathcal{N} \models \varphi[\bar{a}]$ y $\mathcal{M} \models \neg\varphi[\bar{a}]$, lo que contradice (2).

$\square_{\text{Afirmación}}$

Como $T \cup \Gamma(\bar{c}) \models \varphi(\bar{c})$, por las Observaciones 2.2.2 y A.1.6, existen $\psi_1(\bar{x}), ..., \psi_m(\bar{x}) \in \Gamma(\bar{x})$ tal que $T \models \forall\bar{x}(\psi(\bar{x}) \to \varphi(\bar{x}))$, donde $\psi(\bar{x}) := \bigwedge_{i=1}^{k} \psi_i(\bar{x})$. Por otra parte, como $\psi_i(\bar{x}) \in \Gamma(\bar{x})$ $\forall i$, $T \models \forall\bar{x}(\varphi(\bar{x}) \to \psi_i(\bar{x}))$ $\forall i$, luego $T \models \forall\bar{x}(\varphi(\bar{x}) \to \psi(\bar{x}))$.[10]

Por tanto, hemos encontrado una $\mathcal{L}$-fórmula sin cuantificadores ψ con $T \models \forall\bar{x}(\psi(\bar{x}) \leftrightarrow \varphi(\bar{x}))$. $\square$

Observación 3.0.3. Cuando $n = 0$ y φ es una sentencia, podemos considerar φ como $\varphi(x)$ y aplicar el teorema para obtener una fórmula sin cuantificadores $\psi(x)$ equivalente a $\varphi(x)$ en T. Por ejemplo, la sentencia $\exists y\,(y \doteq y)$ es equivalente en T a la fórmula $x \doteq x$.

Si el lenguaje $\mathcal{L}$ no contiene ningún símbolo de constante, no existen sentencias sin cuantificadores en $\mathcal{L}$. En tal caso, cuando a partir de ahora afirmemos la existencia de una fórmula sin cuantificadores ψ equivalente a una sentencia φ, permitiremos que ψ tenga una variable libre.

Definición 3.0.4. Sea T una $\mathcal{L}$-teoría. Se dice que T tiene *eliminación de cuantificadores* (en el lenguaje $\mathcal{L}$) si toda $\mathcal{L}$-fórmula φ es equivalente en T a una fórmula sin cuantificadores.

Lema 3.0.5. *Supongamos que para toda fórmula libre de cuantificadores φ y toda variable x existe una fórmula libre de cuantificadores ψ tal que $\exists x\,\varphi$ es equivalente en T a ψ. Entonces T tiene eliminación de cuantificadores.*

Demostración. Sean ψ y ψ' dos fórmulas equivalentes en T. Como $\neg\psi \sim_T \neg\psi'$, $\exists x\,\psi \sim_T \exists x\,\psi'$, $\chi \wedge \psi \sim_T \chi \wedge \psi'$ (con χ una fórmula cualquiera), argumentamos por inducción sobre la altura de la fórmula, considerando únicamente fórmulas en forma prenexa y eliminando un cuantificador a la vez. $\square$

Teorema 3.0.6. *Sea T una $\mathcal{L}$-teoría. Supongamos que para cualquier par de modelos $\mathcal{M}$ y $\mathcal{N}$ de T, para toda subestructura común $\mathcal{A} \subseteq \mathcal{M}, \mathcal{N}$ y para toda fórmula libre de cuantificadores $\varphi(x_0, \ldots, x_n)$, si existen $\bar{a} \in A^n$ y $b_0 \in M$ tales que $\mathcal{M} \models \varphi[b_0, \bar{a}]$, entonces existe $c_0 \in N$ con $\mathcal{N} \models \varphi[c_0, \bar{a}]$. Entonces T tiene eliminación de cuantificadores.*

El recíproco es inmediato: toda teoría que tiene eliminación de cuantificadores cumple la hipótesis anterior.

Demostración. Sea $\mathcal{A} \subseteq \mathcal{M}, \mathcal{N}$ con $\mathcal{M}, \mathcal{N} \models T$. Sea φ una fórmula libre de cuantificadores y sea $\chi := \exists x_0\,\varphi$. Por hipótesis, $\mathcal{M} \models \chi[\bar{a}]$ si y solo si $\mathcal{N} \models \chi[\bar{a}]$ para todo $\bar{a} \in A^n$. Del Teorema 3.0.2 se obtiene que χ es equivalente en T a una fórmula libre de cuantificadores. Por el lema anterior, T tiene eliminación de cuantificadores. $\square$

Proposición 3.0.7. *Sea T una teoría que tiene eliminación de cuantificadores.*

1. *Sean $\mathcal{M}$ y $\mathcal{N}$ modelos de T con una subestructura común. Entonces $\mathcal{M} \equiv \mathcal{N}$.*[11]

[10] $\big((A \to B_1) \wedge \cdots \wedge (A \to B_n)\big) \longrightarrow \big(A \to (B_1 \wedge \cdots \wedge B_n)\big)$ es una tautología, y aplicamos MP.

[11] Denota que son *elementalmente equivalentes* (satisfacen las mismas sentencias).

2. *Si* $\mathcal{M}, \mathcal{N} \models T$ *y* $\mathcal{M} \subseteq \mathcal{N}$, *entonces* $\mathcal{M} \preceq \mathcal{N}$.

Demostración. (1) Es un caso particular de la implicación fácil del Teorema 3.0.2. Toda sentencia φ es equivalente en T a una fórmula libre de cuantificadores $\psi(x)$. Si $\mathcal{A}$ es subestructura común de $\mathcal{M}$ y $\mathcal{N}$ y $a \in A$, entonces

$$\mathcal{M} \models \varphi \iff \mathcal{M} \models \psi[a] \iff \mathcal{A} \models \psi[a] \iff \mathcal{N} \models \psi[a] \iff \mathcal{N} \models \varphi.$$

(2) Es consecuencia directa del Teorema 3.0.2 ($\mathcal{M}$ es la subestructura común).

□

Dos de las teorías de primer orden más relevantes que tienen eliminación de cuantificadores son la teoría de los cuerpos algebraicamente cerrados (ACF) y la teoría de los cuerpos realmente cerrados (RCF). En la siguiente sección estudiaremos ACF.

4. ACF

Comenzamos desarrollando la teoría de los cuerpos algebraicamente cerrados y las herramientas algebraicas necesarias para la demostración de la eliminación de cuantificadores.

4.1. Cuerpos algebraicamente cerrados

En esta sección seguiremos esencialmente [6]. Incluímos un breve recorrido por las nociones de álgebra necesarias en el Apéndice A.2. Algunas de las demostraciones requieren nociones elementales de teoría de conjuntos, principalmente de cardinalidad, cuyo repaso general incluimos en el Apéndice A.4.

Proposición 4.1.1. *Sea K un cuerpo. Las siguientes condiciones son equivalentes:*

1. *Todo polinomio no constante de $K[x]$ tiene al menos una raíz en K.*
2. *Todo polinomio $f \in K[x]$ se factoriza en $K[x]$ como producto de factores lineales.*[12]
3. *Todo polinomio irreducible en $K[x]$ tiene grado 1.*
4. *K no tiene extensiones algebraicas propias.*

En tal caso, decimos que K es algebraicamente cerrado.

Demostración. La condición (1) implica (2) por inducción en el grado, extrayendo sucesivamente factores lineales; (2) implica (3), ya que si todo polinomio se factoriza en factores lineales, en particular todo polinomio irreducible debe tener grado 1. La condición (3) implica (4), porque si existiera una extensión algebraica propia $K \subsetneq L$, algún elemento $b \in L \setminus K$ tendría polinomio mínimo $m_{b,K}$ de grado mayor que 1. Finalmente, (4) implica (1), pues si existiera $f \in K[x]$ sin raíces en K, añadir una raíz α de f daría una extensión algebraica propia $K \subsetneq K(\alpha)$.[13] □

Observación 4.1.2. Sea $K \subseteq L$ una extensión de cuerpos, con K algebraicamente cerrado, y sea $b \in L \setminus K$. Entonces b es trascendente sobre K. En particular, para todo b algebraico sobre K, se cumple que $b \in K$, es decir, todas las raíces de los polinomios de $K[x]$ pertenecen a K.

Esto es consecuencia directa de (4): si $b \in L \setminus K$ es algebraico sobre K, $K \subsetneq K(b)$ es una extensión algebraica propia de K.

Definición 4.1.3. Sea K un cuerpo. Una *clausura algebraica* de K es un cuerpo $\overline{K}$ que es una extensión algebraica de K y es algebraicamente cerrado.

Lema 4.1.4. *Sea A un subcuerpo de un cuerpo algebraicamente cerrado L. Definimos*

$$A_L^{\text{alg}} := \{\, b \in L \mid b \text{ es algebraico sobre } A \,\}.$$

Entonces A_L^{alg} es una clausura algebraica de A.

Demostración. Por construcción, A_L^{alg} es una extensión algebraica de A. Sea $f \in A_L^{\text{alg}}[x]$ no constante y $b \in L$ una raíz de f. Si $c_1, \ldots, c_n$ son los coeficientes de f, el cuerpo $A(c_1, \ldots, c_n)$ es algebraico sobre A,[14] y como b es algebraico sobre $A(c_1, \ldots, c_n)$, por transitividad de la algebraicidad (Proposición A.2.9) b es algebraico sobre A, es decir, $b \in A_L^{\text{alg}}$. Por tanto, A_L^{alg} es algebraicamente cerrado. □

[12] Por "factores lineales" entendemos polinomios de grado 1, es decir, de la forma $x - a$ con $a \in K$.

[13] La existencia de esta extensión se justifica en la Proposición 4.1.5.

[14] En particular es finita pues son un número finito de coeficientes algebraicos sobre K (Teorema A.2.8), y toda extensión finita es algebraica (Proposición A.2.6).

Proposición 4.1.5. *Sea K un cuerpo y sea $f \in K[x]$ un polinomio de grado n. Entonces existe una extensión $F = K(u)$ de K tal que $u \in F$ cumple $f(u) = 0$.*

Demostración. Supongamos que f es irreducible (en caso contrario, lo reemplazamos por un factor irreducible). Entonces el ideal (f) es maximal y el cociente $K[x]/(f)$ es un cuerpo. Sea $\pi\colon K[x] \longrightarrow K[x]/(f)$ la proyección canónica. La restricción $\pi|_K$ es un monomorfismo: en efecto, si $\pi(k) = 0$ para algún $k \in K$, entonces $k \in (f)$, pero (f) es un ideal propio y k es constante, de modo que $k = 0$.

Definimos $F := K[x]/(f)$. Tenemos que $\pi(K) \subseteq F$, y por el isomorfismo $\pi|_K : K \to \pi(K)$ podemos, por abuso de notación, identificar K con $\pi(K)$ y considerar que $K \subseteq F$. De este modo F se interpreta como un cuerpo que extiende a K. Sea $u := \pi(x) \in F$. Como todo elemento de F es de la forma $\pi(g(x)) = g(\pi(x)) = g(u)$ para algún $g \in K[x]$, se sigue que F está generado por K y u, es decir, $F = K(u)$.

Finalmente, $f(u) = f(\pi(x)) = \pi(f(x)) = 0$, como queríamos. □

Definición 4.1.6. Sea $f \in K[x]$ un polinomio de grado positivo. Una extensión $K \subseteq F$ se dice *cuerpo de descomposición de f sobre K* si f se descompone en factores lineales en $F[x]$ y, además, $F = K(u_1, \ldots, u_n)$ donde $u_1, \ldots, u_n$ son las raíces de f en F. Más en general, si $S \subseteq K[x]$ es un conjunto de polinomios de grado positivo, diremos que F es un *cuerpo de descomposición de S sobre K* si cada polinomio de S se descompone en factores lineales en $F[x]$ y F es la extensión de K generada por todas las raíces de los polinomios de S.

Observación 4.1.7. Sea F un cuerpo de descomposición de un conjunto $S \subseteq K[x]$ sobre K, y sea E un cuerpo intermedio $K \subseteq E \subseteq F$. Entonces F es también un cuerpo de descomposición de S sobre E.

En efecto, dado que $K \subseteq E \subseteq F$, los polinomios de S, al estar en $K[x]$, también pertenecen a $E[x]$ y se descomponen en $F[x]$. Como $F = K(u_1, \ldots, u_n)$ con u_i raíces de S, y $E \subseteq F$, se tiene también $F = E(u_1, \ldots, u_n)$. Por tanto, F es cuerpo de descomposición de S sobre E.

Teorema 4.1.8 (Caracterización de clausuras algebraicas)**.** *Sea $K \subseteq F$ una extensión de cuerpos. Son equivalentes:*

1. *F es algebraico sobre K y algebraicamente cerrado.*

2. *F es un cuerpo de descomposición de la familia de todos los polinomios de $K[x]$.*

Demostración. Vemos que (1) implica (2). Si F es algebraicamente cerrado, por la Observación 4.1.2 sabemos que todas las raíces de los polinomios de $K[x]$ pertenecen a F, luego $E := K\big(\{\text{raíces de todos los polinomios de } K[x]\}\big)$, el cuerpo de descomposición de la familia de todos los polinomios de $K[x]$, cumple $E \subseteq F$. Como además $K \subseteq F$ es algebraica, todo elemento de F es raíz de algún polinomio de $K[x]$, de donde $E \supseteq F$ y por tanto $F = E$.

Vemos ahora que (2) implica (1). Si F es el cuerpo de descomposición de todos los polinomios de $K[x]$, entonces se obtiene a partir de K añadiendo raíces de polinomios de $K[x]$, todas ellas algebraicas sobre K. Puesto que la composición de extensiones algebraicas es algebraica, se sigue que $K \subseteq F$ es algebraica. Falta ver que F es algebraicamente cerrado. Sea $g \in F[x]$ un polinomio no constante y sea K' el subcuerpo de F generado por los coeficientes de g junto con K. Entonces $K \subseteq K'$ es algebraica, ya que $K \subseteq F$ lo es. Sea E el cuerpo de descomposición de g sobre K'. Por definición, $K' \subseteq E$ es algebraica, y por transitividad también lo es $K \subseteq E$. Así, cada raíz de g es algebraica sobre K, es decir, raíz de algún polinomio de $K[x]$, y por tanto pertenece a F. Como g era arbitrario, concluimos que F es algebraicamente cerrado. □

Vamos a demostrar que todo cuerpo tiene una clausura algebraica, y que esta es única salvo isomorfismo.

El siguiente lema acota la cardinalidad de las extensiones algebraicas.

Lema 4.1.9. *Sea $K \subseteq F$ una extensión algebraica. Entonces $|F| \leq \aleph_0 \cdot |K|$.*

Demostración. Sea T el conjunto de polinomios mónicos de grado positivo en $K[x]$. Vemos primero que $|T| = \aleph_0 \cdot |K|$.

Para cada $n \in \mathbb{N}^*$ sea T_n el conjunto de polinomios mónicos de grado n en T. Entonces $|T_n| = |K|^n$, pues cada polinomio de T_n está determinado por sus coeficientes $a_0, \ldots, a_{n-1} \in K$ en $x^n + a_{n-1}x^{n-1} + \cdots + a_0$.

Para cada $n \in \mathbb{N}^*$ sea $f_n : T_n \to K^n$ una biyección. Como los conjuntos T_n (resp. K^n) son disjuntos, la aplicación $f : T = \bigcup_{n\in\mathbb{N}^*} T_n \to \bigcup_{n\in\mathbb{N}^*} K^n$ dada por $f(t) = f_n(t)$ si $t \in T_n$ es una biyección bien definida. Por tanto $|T| = \left|\bigcup_{n\in\mathbb{N}^*} K^n\right| = \aleph_0 \cdot |K|$.

Vemos ahora que $|F| \leq |T|$. Para cada $g \in T$ irreducible, elegimos un orden de las raíces distintas de g en F.

Definimos la aplicación $\varphi : F \to T \times \mathbb{N}^*$ de la siguiente forma: dado $a \in F$, a es algebraico sobre K por hipótesis y existe un único polinomio irreducible $g \in T$ con $g(a) = 0$. Asignamos $a \mapsto (g, i)$, donde i es la raíz i-ésima de g en el orden escogido. Esta aplicación está bien definida y es inyectiva.

Como T es infinito, se cumple $|F| \leq |T \times \mathbb{N}^*| = |T| \cdot |\mathbb{N}^*| = |T| \cdot \aleph_0 = |T| = \aleph_0 \cdot |K|$. □

Teorema 4.1.10. *Sea K un cuerpo. Entonces K tiene una clausura algebraica; es decir, existe un cuerpo $\overline{K}$ que es algebraico sobre K y es algebraicamente cerrado.*

Demostración. Comenzamos eligiendo un conjunto S tal que $\aleph_0 \cdot |K| < |S|$, por ejemplo uno de cardinalidad $|\mathcal{P}(\aleph_0 \times K)|$. Como $|K| < |S|$, existe una función inyectiva $\theta : K \hookrightarrow S$. Mediante esta función inyectiva podemos, de ser necesario, reemplazar S por $S' = (S \setminus \theta(K)) \cup K$ para garantizar que $K \subseteq S$. A partir de ahora supondremos $K \subseteq S$.

Sea $\mathcal{S}$ la clase de todos los cuerpos E tales que $E \subseteq S$ y E es una extensión algebraica de K. Un cuerpo E de esta clase queda completamente determinado por el subconjunto $E \subseteq S$ y las operaciones binarias de suma y multiplicación en E. La suma (resp. multiplicación) es una función $\varphi : E \times E \to E$ (resp. $\psi : E \times E \to E$). Como identificamos una función con su grafo,[15] φ (resp. ψ) puede verse como un cierto subconjunto $E \times E \times E \subseteq S \times S \times S$.

En consecuencia, existe una función inyectiva

$$\tau : \mathcal{S} \longrightarrow \mathcal{P}\big(S \times (S \times S \times S) \times (S \times S \times S)\big), \ E \longmapsto (E, \varphi, \psi),$$

donde $\mathcal{P}(\cdot)$ denota el conjunto potencia. Ahora bien, $\operatorname{Im}\tau$ es un conjunto, ya que es una subclase del conjunto potencia anterior. Como $\mathcal{S}$ es la imagen del conjunto $\operatorname{Im}\tau$ bajo la función inversa $\tau^{-1} : \operatorname{Im}\tau \to \mathcal{S}$, los axiomas de la teoría de conjuntos garantizan que $\mathcal{S}$ es de hecho un conjunto.

Notemos que $\mathcal{S} \neq \emptyset$ pues $K \in \mathcal{S}$. Ordenamos $\mathcal{S}$ parcialmente definiendo $E_1 \leq E_2$ si y solo si E_2 es una extensión de E_1. Cada cadena en $\mathcal{S}$ tiene una cota superior (la unión de los cuerpos de la cadena es un cuerpo, que obviamente está contenido en S y sigue siendo extensión algebraica de K). Por el Lema de Zorn (Lema A.4.2), existe un elemento maximal $F \in \mathcal{S}$.

Afirmamos que F es algebraicamente cerrado. En efecto, si no lo fuera, existiría $f \in F[x]$ sin raíces en F. Por la Proposición 4.1.5 existe una extensión algebraica propia $F_0 = F(u)$ de

[15] Ver Apéndice A.4.

F, donde u es una raíz de f que no pertenece a F. Por la transitividad de la algebraicidad, F_0 es una extensión algebraica de K, luego $|F_0 - F| \leq |F_0| \leq \aleph_0|K| < |S|$ donde se tiene $|F_0| \leq \aleph_0 \cdot |K|$ por el lema anterior.

Como $|F| \leq |F_0| < |S|$ y $|S| = |(S - F) \cup F| = |S - F| + |F|$, al tratarse de cardinales infinitos tenemos $|S| = |S - F|$ y, por tanto, $|F_0 - F| < |S - F|$. En particular, la función identidad en F puede extenderse a una función inyectiva de conjuntos $\zeta : F_0 \longrightarrow S$.

Definimos $F_1 := \operatorname{Im}\zeta$. Mediante ζ, podemos dotar a F_1 de estructura de cuerpo con $\zeta(a)+\zeta(b) := \zeta(a+b)$, $\zeta(a)\cdot\zeta(b) := \zeta(ab)$. Así, F_1 es una extensión de F, $F_1 \subseteq S$, y $\zeta : F_0 \to F_1$ es un F-isomorfismo de cuerpos.[16] Como F_0 es una extensión algebraica propia de F (y por tanto de K), también lo es F_1. Por tanto, $F_1 \in \mathcal{S}$ y $F < F_1$, lo que contradice la maximalidad de F. Concluimos que F es algebraicamente cerrado.

Como además F es algebraico sobre K, se sigue que F es una clausura algebraica de K. □

Probada la existencia de clausuras algebraicas, abordamos su unicidad, que se deducirá como corolario de un resultado general sobre extensiones y cuerpos de descomposición, aprovechando la caracterización del Teorema 4.1.8. Comenzamos con el siguiente teorema auxiliar:

Teorema 4.1.11. *Sea $\sigma : K \to L$ un isomorfismo de cuerpos, u un elemento de alguna extensión de K y v un elemento de alguna extensión de L. Denotemos por $\widehat{\sigma} : K[x] \to L[x]$ la extensión de σ a polinomios, aplicada coeficiente a coeficiente: $\widehat{\sigma}(\sum_i a_i x^i) = \sum_i \sigma(a_i)x^i$, $\widehat{\sigma}(x) = x$. Nótese que $\widehat{\sigma}$ es un isomorfismo de anillos. Supongamos que se cumple una de las siguientes condiciones:*

1. *u es raíz de un polinomio irreducible $f \in K[x]$ y v es raíz de $\widehat{\sigma}(f) \in L[x]$; o*

2. *u es trascendente sobre K y v es trascendente sobre L.*

Entonces σ se extiende a un isomorfismo de cuerpos $\widetilde{\sigma} : K(u) \longrightarrow L(v)$ con $\widetilde{\sigma}_{|K} = \sigma$ y $\widetilde{\sigma}(u) = v$.

Demostración. Sean u y v algebraicos sobre K y L respectivamente con polinomios correspondientes $f \in K[x]$ y $\widehat{\sigma}(f) \in L[x]$. Podemos suponer f irreducible y mónico (dividiendo por su coeficiente principal). Entonces $\widehat{\sigma}(f)$ también es mónico e irreducible en $L[x]$.

Consideremos $\theta_u : K[x]/(f) \longrightarrow K(u)$, con $\theta_u\big(g + (f)\big) = g(u)$ y $\theta_v : L[x]/\big(\widehat{\sigma}(f)\big) \longrightarrow L(v)$, con $\theta_v\big(h + (\widehat{\sigma}(f))\big) = h(v)$, que son isomorfismos de cuerpos (ver Teorema A.2.4).

Definimos ahora $\Phi : K[x]/(f) \longrightarrow L[x]/\big(\widehat{\sigma}(f)\big)$, con $\Phi\big(g + (f)\big) = \widehat{\sigma}(g) + \big(\widehat{\sigma}(f)\big)$. Para ver que Φ está bien definida, si $g + (f) = g' + (f)$ entonces $g - g' = fh$ para algún h, y al aplicar $\widehat{\sigma}$ se obtiene $\widehat{\sigma}(g) - \widehat{\sigma}(g') \in (\widehat{\sigma}(f))$, por lo que $\Phi(g + (f)) = \Phi(g' + (f))$.

Además, Φ es claramente homomorfismo de anillos y es biyectiva, con inversa dada por $\Phi^{-1}\big(H + (\widehat{\sigma}(f))\big) = \widehat{\sigma}^{-1}(H) + (f)$, $H \in L[x]$. Por tanto, Φ es un isomorfismo de cuerpos. Definimos finalmente

$$\widetilde{\sigma} := \theta_v \circ \Phi \circ \theta_u^{-1} : K(u) \longrightarrow L(v),$$

el cual es un isomorfismo de cuerpos por ser composición de tales, y envía u a v. En efecto, $\theta_u^{-1}(u) = x+(f)$, por lo que $\Phi\big(\theta_u^{-1}(u)\big) = \Phi\big(x+(f)\big) = \widehat{\sigma}(x)+(\widehat{\sigma}(f)) = x+(\widehat{\sigma}(f))$, y finalmente $\widetilde{\sigma}(u) = \theta_v\big(x + (\widehat{\sigma}(f))\big) = v$.

Sean ahora u y v trascendentes sobre K y L, respectivamente. Vemos que $\widehat{\sigma}$ se extiende a un isomorfismo de cuerpos $\bar{\sigma} : K(x) \longrightarrow L(x)$ entre los cuerpos de fracciones de $K[x]$ y $L[x]$, respectivamente.

[16] Un *F-isomorfismo de cuerpos* es un isomorfismo de cuerpos entre extensiones de F que fija F.

Definimos $\bar{\sigma}$ sobre los elementos de $K(x)$ mediante $\bar{\sigma}\left(\frac{f}{g}\right) := \frac{\widehat{\sigma}(f)}{\widehat{\sigma}(g)}$, donde $f, g \in K[x]$ y $g \neq 0$. Este cociente está bien definido, pues $\widehat{\sigma}$ es un isomorfismo de anillos y, en particular, preserva el hecho de que $g \neq 0$ implica que $\widehat{\sigma}(g) \neq 0$.

Definimos la inversa de $\bar{\sigma}$ como $\bar{\sigma}^{-1}\left(\frac{F}{G}\right) := \frac{\widehat{\sigma}^{-1}(F)}{\widehat{\sigma}^{-1}(G)}$, $F, G \in L[x]$, $G \neq 0$. Esta aplicación está bien definida por la misma razón que antes: $\widehat{\sigma}^{-1}$ preserva el hecho de ser no nulo. Es inmediato comprobar que $\bar{\sigma}^{-1} \circ \bar{\sigma} = \mathrm{id}_{K(x)}$ y $\bar{\sigma} \circ \bar{\sigma}^{-1} = \mathrm{id}_{L(x)}$, de modo que $\bar{\sigma}$ es biyectiva. Por tanto, $\bar{\sigma} : K(x) \to L(x)$ es un isomorfismo de cuerpos que extiende a $\widehat{\sigma}$.

Como u es trascendente sobre K y v es trascendente sobre L, sabemos que $K(u) \cong K(x)$ y $L(v) \cong L(x)$ (ver Teorema A.2.5). Por tanto, $K(u) \cong K(x) \cong L(x) \cong L(v)$. Verificar que la composición de estos isomorfismos, que denotaremos por $\widetilde{\sigma}$, envía u en v es análogo al caso algebraico.

Finalmente, en ambos casos $\widetilde{\sigma}_{|K} = \sigma$, ya que todos los isomorfismos involucrados son extensiones de $\sigma : K \to L$. □

Teorema 4.1.12. *Sea $\sigma : K \to L$ un isomorfismo de cuerpos, $S \subseteq K[x]$ un conjunto de polinomios de grado positivo y $\sigma(S) := \{\widehat{\sigma}(f) : f \in S\} \subseteq L[x]$, donde $\widehat{\sigma} : K[x] \to L[x]$ es la extensión a polinomios de σ. Sea F un cuerpo de descomposición de S sobre K y M un cuerpo de descomposición de $\sigma(S)$ sobre L. Entonces σ se extiende a un isomorfismo de cuerpos $\widetilde{\sigma} : F \to M$.*

Demostración. Veamos primero el caso en el que $S = \{f\}$ con $f \in K[x]$. Procedemos por inducción en $n = [F : K]$, donde F es un cuerpo de descomposición de f sobre K.

Si $n = 1$, entonces $F = K$ y f se descompone completamente en $K[x]$. Por tanto, $\widehat{\sigma}(f)$ se descompone completamente en $L[x]$, de modo que L es también un cuerpo de descomposición de f, y en este caso σ es el isomorfismo buscado ($F = K \xrightarrow{\sigma} L = M$).

Supongamos por hipótesis de inducción que el resultado es válido para todas las extensiones de grado menor que n. Si $n > 1$, entonces f tiene un factor irreducible $g \in K[x]$ de grado mayor que 1. Sea u una raíz de g en F. Entonces $\widehat{\sigma}(g)$ es irreducible en $L[x]$, y si v es una raíz de $\widehat{\sigma}(g)$ en M, por el teorema anterior σ se extiende a un isomorfismo $\tau : K(u) \to L(v)$ con $\tau(u) = v$. Puesto que $[K(u) : K] = \deg g > 1$ (Teorema A.2.4), se sigue de la transitividad del grado que $[F : K(u)] < [F : K] = n$. Además, F es un cuerpo de descomposición de f sobre $K(u)$ y M es un cuerpo de descomposición de $\widehat{\sigma}(f)$ sobre $L(v)$ (Observación 4.1.7). Por hipótesis de inducción, τ se extiende entonces a un isomorfismo $\widetilde{\tau} : F \to M$.

Caso general. Sea $\mathcal{S}$ la clase de todas las tripletas (E, N, τ), donde E es un cuerpo intermedio $K \subseteq E \subseteq F$, N es un cuerpo intermedio $L \subseteq N \subseteq M$, y $\tau : E \to N$ es un isomorfismo de cuerpos que extiende a σ. Un argumento análogo al de la prueba del Teorema 4.1.10 muestra que $\mathcal{S}$ es un conjunto: basta identificar τ con su grafo y considerar la aplicación

$$(E, N, \tau) \longmapsto E \cup N \cup \mathrm{grafo}(\tau) \in \mathcal{P}\big(F \cup M \cup (F \times M)\big),$$

que es inyectiva. La imagen es un subconjunto del conjunto potencia anterior, y aplicando la inversa de esta correspondencia recuperamos $\mathcal{S}$ como conjunto.

Definimos el orden parcial

$$(E_1, N_1, \tau_1) \leq (E_2, N_2, \tau_2) \quad \text{si y solo si} \quad E_1 \subseteq E_2,\ N_1 \subseteq N_2,\ \tau_2|_{E_1} = \tau_1.$$

El conjunto $\mathcal{S}$ es no vacío (pues contiene (K, L, σ)) y toda cadena $\mathcal{C} \subseteq \mathcal{S}$ tiene una cota superior dada por $(E_*, N_*, \tau_*) := \left(\bigcup_{(E,N,\tau)\in\mathcal{C}} E,\ \bigcup_{(E,N,\tau)\in\mathcal{C}} N,\ \bigcup_{(E,N,\tau)\in\mathcal{C}} \tau\right)$, donde

$$\tau_* := \bigcup_{(E,N,\tau)\in\mathcal{C}} \tau = \{\, (x,\tau(x)) : x \in E,\ (E,N,\tau) \in \mathcal{C} \,\}$$

es la unión de los grafos de todos los isomorfismos de la cadena. La condición $\tau_2|_{E_1} = \tau_1$ para $(E_1,N_1,\tau_1) \leq (E_2,N_2,\tau_2)$ asegura que la unión es una función bien definida. Como cada τ es un isomorfismo de cuerpos, su unión τ_* también lo es, luego (E_*,N_*,τ_*) en efecto constituye una cota superior de $\mathcal{C}$. Por el Lema de Zorn, existe un elemento maximal $(F_0,M_0,\tau_0) \in \mathcal{S}$.

Afirmamos que $F_0 = F$ y $M_0 = M$, de modo que $\tau_0 : F \xrightarrow{\cong} M$ es la extensión deseada de σ. Supongamos, por el contrario, que $F_0 \subsetneq F$. Entonces existe $f \in S$ que no se descompone sobre F_0. Como todas las raíces de f están en F, existe un cuerpo de descomposición F_1 de f sobre F_0 con $F_0 \subsetneq F_1 \subseteq F$. De forma análoga, M contiene un cuerpo de descomposición M_1 de $\tau_0(f) = \widehat{\sigma}(f)$ sobre M_0. Por el caso de un solo polinomio, τ_0 se extiende a un isomorfismo $\tau_1 : F_1 \to M_1$ con $\tau_1|_{F_0} = \tau_0$. Así, $(F_1,M_1,\tau_1) \in \mathcal{S}$ y $(F_0,M_0,\tau_0) < (F_1,M_1,\tau_1)$, lo que contradice la maximalidad de (F_0,M_0,τ_0).

De modo análogo, si $M_0 \subsetneq M$, aplicamos el mismo argumento a τ_0^{-1} y obtenemos una contradicción. Por tanto, debe cumplirse $F_0 = F$ y $M_0 = M$, lo que completa la prueba. □

Corolario 4.1.13. *Sea K un cuerpo y $S \subseteq K[x]$ un conjunto de polinomios de grado positivo. Entonces cualesquiera dos cuerpos de descomposición de S sobre K son K-isomorfos. En particular, cualesquiera dos clausuras algebraicas de K son K-isomorfas.*

Demostración. Aplicamos el teorema anterior con $\sigma = \mathrm{id}_K$. La unicidad de las clausuras algebraicas se sigue del hecho de que una clausura algebraica es un cuerpo de descomposición de la familia de todos los polinomios de $K[x]$ de grado positivo (Teorema 4.1.8). □

Vamos a extender estos resultados al caso de subanillos de un cuerpo (o dominios de integridad), pues son precisamente las subestructuras de los modelos de ACF. Como vimos en el Teorema 3.0.2, la caracterización de la eliminación de cuantificadores depende en gran medida de cómo se comportan dichas subestructuras.

Definición 4.1.14. Sea A un dominio de integridad con cuerpo de fracciones $F = \mathrm{Frac}(A)$. Llamaremos *clausura algebraica de A* a cualquier clausura algebraica de F, es decir, a un cuerpo algebraicamente cerrado F^{alg} que contenga a F y sea extensión algebraica de F.

Observación 4.1.15. Sea A un subanillo de un cuerpo algebraicamente cerrado K, y sea $F = \mathrm{Frac}(A)$ su cuerpo de fracciones. Definimos $A_K^{\mathrm{alg}} := \{\, b \in K : b \text{ es algebraico sobre } F \,\}$. Entonces A_K^{alg} es una clausura algebraica de A (concretamente, de F) contenida en K, y por tanto es única salvo isomorfismo que fija F, y en particular A. Se sigue del Lema 4.1.4 y el corolario anterior.

Observación 4.1.16 (Clasificación de cuerpos algebraicamente cerrados)**.** Un subconjunto $S \subseteq K$ se dice *algebraicamente independiente* sobre un subcuerpo K_0 de K si para cualesquiera elementos $s_1,\ldots,s_n \in S$ y todo polinomio no nulo $P \in K_0[X_1,\ldots,X_n]$ se tiene

$$P(s_1,\ldots,s_n) \neq 0.$$

Una *base de trascendencia* de K sobre K_0 es un subconjunto $B \subseteq K$ algebraicamente independiente tal que K es algebraico sobre $K_0(B)$. Equivalentemente, B es un subconjunto algebraicamente independiente maximal con respecto a la inclusión. Un argumento basado en el Lema de Zorn garantiza la existencia de una base de trascendencia. Su cardinal es independiente de la elección de la base, y se denomina *grado de trascendencia* de K sobre K_0.

En el contexto de cuerpos algebraicamente cerrados, el *Teorema de Steinitz* afirma que dos cuerpos algebraicamente cerrados son isomorfos si y solo si tienen la misma característica y el mismo grado de trascendencia sobre su subcuerpo primo. Dicho de otro modo, la característica y el grado de trascendencia clasifican completamente los cuerpos algebraicamente cerrados (salvo isomorfismo), de manera que, fijada la característica, los modelos de ACF quedan determinados por su grado de trascendencia.

Vemos la idea de la demostración. Para una exposición detallada, véase [6, §6.1].

Sean K y L cuerpos algebraicamente cerrados de la misma característica, y sean $B \subseteq K$ y $B' \subseteq L$ bases de trascendencia sobre su subcuerpo primo K_0, con $|B| = |B'|$. Fijemos una biyección $\varphi\colon B \to B'$.

Para cada subconjunto finito $F = \{b_1, \dots, b_n\} \subseteq B$, la restricción $\varphi|_F\colon F \to \varphi(F)$ induce un isomorfismo de cuerpos $K_0(F) \xrightarrow{\widetilde{\sigma}_F} K_0(\varphi(F))$, obtenido identificando ambos cuerpos con cuerpos de fracciones de anillos de polinomios en n variables.

Estos isomorfismos son compatibles al variar F. En consecuencia, definen una aplicación bien definida $\widetilde{\sigma}\colon K_0(B) \longrightarrow K_0(B')$ dada por $\widetilde{\sigma}(x) = \widetilde{\sigma}_F(x)$ si $x \in K_0(F)$, donde $F \subseteq B$ es cualquier subconjunto finito tal que $x \in K_0(F)$. Dicha aplicación es un isomorfismo de cuerpos, cuya inversa se construye de forma análoga a partir de φ^{-1}.

Dado que K y L son clausuras algebraicas de $K_0(B)$ y $K_0(B')$, respectivamente, este isomorfismo se extiende a un isomorfismo de cuerpos $K \cong L$.[17]

Introducimos finalmente algunos resultados sobre cuerpos finitos, necesarios para el estudio de ACF_p (la teoría de los cuerpos algebraicamente cerrados de característica p); los preliminares se incluyen en el apéndice. La exposición sigue parcialmente a [5] y [6], con algunas adaptaciones y simplificaciones propias.

Lema 4.1.17. *Sea K un cuerpo finito de p^n elementos. Entonces, todo $x \in K$ cumple $x^{p^n} = x$.*

Demostración. Recordemos que para cualquier cuerpo K, el conjunto de sus elementos no nulos forma un grupo multiplicativo $(K^*, \cdot)$, pues el producto es asociativo, 1 actúa como elemento neutro y todo $a \in K^*$ tiene inverso $a^{-1} \in K^*$. Si K tiene p^n elementos, entonces $|K^*| = p^n - 1$.

Por el Teorema de Lagrange, el orden de cada elemento $a \in K^*$ divide el orden del grupo, es decir, $\mathrm{ord}(a) \mid (p^n - 1)$, y por tanto $a^{p^n-1} = 1$. Multiplicando por a se obtiene $a^{p^n} = a$, y la igualdad también vale para $a = 0$. □

Teorema 4.1.18. *Sea p primo y $n \geq 1$. El cuerpo de descomposición de $f_n(t) = t^{p^n} - t \in \mathbb{F}_p[t]$ sobre $\mathbb{F}_p$ tiene p^n elementos, que son precisamente las raíces de f_n.*

Demostración. Sea L el cuerpo de descomposición de f_n sobre $\mathbb{F}_p$ y $M := \{a \in L : a^{p^n} = a\}$ el conjunto de sus raíces. Si $a, b \in M$, por el Lema A.2.10 se tiene $(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b$ y $(ab)^{p^n} = ab$, por lo que $a + b, ab \in M$; además $0, 1 \in M$ y si $a \neq 0$, entonces

$$1 = (aa^{-1})^{p^n} = a^{p^n} (a^{-1})^{p^n} = a\,(a^{-1})^{p^n},$$

luego multiplicando por a^{-1} obtenemos $a^{-1} = (a^{-1})^{p^n}$, es decir, $a^{-1} \in M$. Además, si $a \in M$, entonces $(-a)^{p^n} = (-1)^{p^n} a^{p^n} = \begin{cases} -a, & \text{si } p \neq 2, \\ a, & \text{si } p = 2, \end{cases}$ y si $p = 2$, la caracteristica es 2 y se tiene $-a = a$. En todo caso, $-a \in M$ para todo $a \in M$. Así, M es un subcuerpo de L que contiene a $\mathbb{F}_p$, y por tanto $M = L$.

[17] En efecto, si dos cuerpos son isomorfos, entonces sus clausuras algebraicas también lo son. Esto se deduce del Teorema 4.1.12 y la caracterización de las clausuras algebraicas.

Por el Lema A.2.2, $|M| \leq \deg f_n = p^n$. Como $f_n'(t) = -1$, por el Lema A.2.11 todas sus raíces son simples, luego $|M| = p^n$. □

Corolario 4.1.19. *Todos los cuerpos finitos con el mismo número de elementos son isomorfos entre sí.*

Demostración. Sea K un cuerpo finito. Entonces $\mathrm{car}(K) = p$ para cierto primo p, y $|K| = p^n$ para algún $n \geq 1$. Su subcuerpo primo K_0 es isomorfo a $\mathbb{F}_p$, aunque no necesariamente coincide con él. Por el Lema 4.1.17, los elementos de K son precisamente las raíces de $f_n(t) = t^{p^n} - t$ en K_0, y un argumento análogo al del teorema anterior muestra que K es un cuerpo de descomposición de f_n sobre K_0. Por el Teorema 4.1.12, el isomorfismo $\mathbb{F}_p \cong K_0$ se extiende a un isomorfismo entre los cuerpos de descomposición de $f_n(t)$ sobre ambos (observando que dicho isomorfismo deja fijo f_n). Por tanto, todo cuerpo finito con p^n elementos es isomorfo a $\mathbb{F}_{p^n}$. □

Corolario 4.1.20. *Sea $\mathbb{F}_p^{\mathrm{alg}}$ una clausura algebraica de $\mathbb{F}_p$. Entonces $\mathbb{F}_p^{\mathrm{alg}} = \bigcup_{k\geq 1} \mathbb{F}_{p^k}$.*

Demostración. Sea $a \in \mathbb{F}_p^{\mathrm{alg}}$. Su polinomio mínimo $m_{a,\mathbb{F}_p}(t) \in \mathbb{F}_p[t]$ tiene grado finito d. El cuerpo $\mathbb{F}_p(a)$ es una extensión finita de grado d, por lo que tiene p^d elementos y por el corolario anterior, es isomorfo a $\mathbb{F}_{p^d}$. Por el Teorema 4.1.18, el cuerpo $\mathbb{F}_{p^d}$ también está contenido en $\mathbb{F}_p^{\mathrm{alg}}$ y por tanto $\mathbb{F}_p(a) = \mathbb{F}_{p^d}$. En efecto, si fueran distintos, habríamos encontrado más de p^d raíces de $(t^{p^d} - t)$. Así, todo elemento de $\mathbb{F}_p^{\mathrm{alg}}$ pertenece a algún $\mathbb{F}_{p^k}$, y por tanto $\mathbb{F}_p^{\mathrm{alg}} \subseteq \bigcup_{k\geq 1} \mathbb{F}_{p^k}$. Recíprocamente, cada $\mathbb{F}_{p^k}$ es una extensión finita de $\mathbb{F}_p$, y toda extensión finita es algebraica. Por tanto, todo elemento de $\mathbb{F}_{p^k}$ es algebraico sobre $\mathbb{F}_p$, de donde se sigue que $\bigcup_{k\geq 1} \mathbb{F}_{p^k} \subseteq \mathbb{F}_p^{\mathrm{alg}}$. □

Observación 4.1.21. Se tiene que $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^\ell}$ si y solo si $k \mid \ell$ (Proposición A.2.12). Así, con $F_N := \mathbb{F}_{p^{N!}}$ para $N \geq 1$, podemos escribir $\mathbb{F}_p^{\mathrm{alg}}$ como la unión creciente de los F_N.

Observación 4.1.22. Si K es un cuerpo de característica $p > 0$ algebraicamente cerrado, es una clausura algebraica de su subcuerpo primo, luego es isomorfo a $\mathbb{F}_p^{\mathrm{alg}}$. Por tanto, todos los cuerpos algebraicamente cerrados de característica p son, salvo isomorfismo, el cuerpo $\mathbb{F}_p^{\mathrm{alg}}$.

Corolario 4.1.23. *Todo cuerpo algebraicamente cerrado es infinito.*

Demostración. Si un cuerpo finito K fuera algebraicamente cerrado, coincidiría con su clausura algebraica, la cual es infinita por el corolario anterior. □

Terminamos la sección con una observación elemental pero crucial.

Observación 4.1.24. Sea $\mathbb{F}_q$ un cuerpo finito, $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ una aplicación. Si f es inyectiva, entonces f es sobreyectiva.

En efecto, como $|\mathbb{F}_q^n| = q^n$, una aplicación inyectiva $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ satisface $|f(\mathbb{F}_q^n)| = q^n$, por lo que su imagen coincide con el conjunto total.

4.2. Eliminación de cuantificadores en ACF

Entramos ya en el estudio de la teoría de los cuerpos algebraicamente cerrados. Comenzamos por formalizarla en el marco de la lógica de primer orden.

Sea $\mathcal{L}_{\mathrm{anillo}} = \{+, \cdot, 0, 1\}$ el lenguaje de primer orden donde:

- $+$ y $\cdot$ son símbolos de función binaria (aridad 2) que representarán la suma y el producto.
- 0 y 1 son símbolos de constante para los elementos neutro aditivo y multiplicativo.

Sea T_{anillo} el conjunto de sentencias en $\mathcal{L}_{\text{anillo}}$ que expresan las propiedades de un anillo conmutativo con 1:

- $\forall x\, \forall y\ (x + y \doteq y + x)$ (conmutatividad de la suma)
- $\forall x\, \forall y\ (x \cdot y \doteq y \cdot x)$ (conmutatividad del producto)
- $\forall x\, \forall y\, \forall z\ ((x + y) + z \doteq x + (y + z))$ (asociatividad de la suma)
- $\forall x\, \forall y\, \forall z\ ((x \cdot y) \cdot z \doteq x \cdot (y \cdot z))$ (asociatividad del producto)
- $\forall x\ (x + 0 \doteq x)$ (elemento neutro aditivo)
- $\forall x\ (x \cdot 1 \doteq x)$ (elemento neutro multiplicativo)
- $\forall x\ \exists y\ (x + y \doteq 0)$ (existencia de inverso aditivo)
- $\forall x\, \forall y\, \forall z\ (x \cdot (y + z) \doteq x \cdot y + x \cdot z)$ (distributividad)

Una $\mathcal{L}_{\text{anillo}}$-estructura $\mathcal{A}$ es modelo de T_{anillo} si y solo si $\mathcal{A}$ es un anillo conmutativo unitario. Para obtener la teoría T_{cuerpo} de cuerpos, basta añadir a T_{anillo} la siguiente sentencia:

$$\forall x\ (x \doteq 0\ \vee\ \exists y\ (x \cdot y \doteq 1)) \quad \text{(Todo elemento no nulo tiene inverso multiplicativo).}$$

La *teoría de los cuerpos algebraicamente cerrados*, que denotaremos ACF, se obtiene añadiendo a T_{cuerpo} infinitos axiomas que expresan la *clausura algebraica* de la siguiente forma:

$$\forall a_0, \ldots, a_n\ \exists x\ \big(x^n + a_{n-1}x^{n-1} + \cdots + a_0 \doteq 0\big),$$

para cada $n \geq 1$.

Podemos fijar la característica de la siguiente manera. Si es $p > 0$, añadimos a ACF el axioma

$$\underbrace{1 + 1 + \cdots + 1}_{p \text{ veces}} \doteq 0$$

y denotamos por ACF_p la teoría resultante. Si la característica es cero, añadimos para cada primo p el axioma

$$\neg\big(\underbrace{1 + 1 + \cdots + 1}_{p \text{ veces}} \doteq 0\big),$$

y escribimos ACF_0. De este modo, ACF_p (o ACF_0) axiomatiza exactamente la clase de los cuerpos algebraicamente cerrados de característica p (o de característica cero).

Observación 4.2.1. En el lenguaje puro de anillos $\mathcal{L}_{\text{anillo}} = \{0, 1, +, \cdot\}$, los únicos símbolos de constante son 0 y 1. A partir de 1 pueden construirse todos los términos $n = 1 + \cdots + 1$ (n veces), y los axiomas de anillo garantizan la existencia de sus opuestos aditivos. Así, los únicos coeficientes que pueden aparecer en una fórmula del lenguaje son los enteros, que al interpretarse en un modelo K se leen mediante el homomorfismo canónico $\mathbb{Z} \to K,\ n \mapsto n \cdot 1_K$.

Si se desea trabajar con coeficientes arbitrarios en un subanillo $A \subseteq K$ (o en el propio K), se entiende que el lenguaje ha sido ampliado con constantes para los elementos de A;[18] entonces las fórmulas atómicas corresponden a igualdades $P(x_1, \ldots, x_n) = 0$, con $P \in A[x_1, \ldots, x_n]$, y sus coeficientes se interpretan en K mediante la inclusión $A \hookrightarrow K$.

[18] La adición de constantes para los elementos de A no modifica la fuerza deductiva de la teoría (véase el Lema A.1.5 y la Observación A.1.6), por lo que se trata de una expansión conservativa.

Teorema 4.2.2 (Chevalley–Tarski)**.** ACF *tiene eliminación de cuantificadores.*

Demostración. Como toda subestructura de un cuerpo en el lenguaje $\mathcal{L}_{\text{anillo}}$ no es sino un subanillo, por el Teorema 3.0.6 basta probar lo siguiente: si K y L son cuerpos algebraicamente cerrados que contienen un subanillo común A, y si $\varphi(x_0, \ldots, x_n)$ es una fórmula sin cuantificadores, entonces para cada $\overline{a} \in A^n$ se tiene que, si existe $b \in L$ tal que

$$L \models \varphi[b, \overline{a}],$$

entonces existe $c \in K$ tal que

$$K \models \varphi[c, \overline{a}].$$

Podemos reducirnos al caso en que $A = K \subseteq L$. En efecto, en el caso general las clausuras algebraicas A_K^{alg} y A_L^{alg} de A sobre K y L son isomorfas. Supongamos probado el resultado en el caso particular $A = K$. Entonces, aplicado a la extensión $A \subseteq A_K^{\text{alg}}$, se tiene

$$K \models \exists x\, \varphi(x, \bar{a}) \text{ si y solo si } A_K^{\text{alg}} \models \exists x\, \varphi(x, \bar{a}).$$

Como $A_K^{\text{alg}} \cong A_L^{\text{alg}}$ sobre A, y la fórmula tiene parámetros en A, se tiene

$$A_K^{\text{alg}} \models \exists x\, \varphi(x, \bar{a}) \text{ si y solo si } A_L^{\text{alg}} \models \exists x\, \varphi(x, \bar{a}).$$

Finalmente, aplicando de nuevo el caso $A = K$, ahora a la extensión $A \subseteq A_L^{\text{alg}}$, obtenemos

$$A_L^{\text{alg}} \models \exists x\, \varphi(x, \bar{a}) \text{ si y solo si } L \models \exists x\, \varphi(x, \bar{a}).$$

Encadenando estas equivalencias se concluye el caso general.

Además, toda fórmula sin cuantificadores es lógicamente equivalente a una disyunción finita de conjunciones de fórmulas atómicas o negaciones de atómicas, por simples equivalencias de la lógica proposicional clásica. Por consiguiente, la fórmula φ es lógicamente equivalente a una fórmula de la forma

$$\bigvee_i \bigwedge_j \chi_{i,j}(x_0, \ldots, x_n),$$

donde cada $\chi_{i,j}(x_0, \ldots, x_n)$ es atómica o la negación de una atómica. Si $L \models \varphi[b, \overline{a}]$, existe un índice i tal que $L \models \bigwedge_j \chi_{i,j}[b, \overline{a}]$. Por tanto, basta considerar el caso en que φ es una conjunción de fórmulas atómicas y negaciones de fórmulas atómicas, es decir, de la forma

$$\varphi(\bar{x}) \equiv \bigwedge_{i=1}^{n} P_i(\bar{x}) = 0 \ \wedge \ \bigwedge_{j=1}^{m} Q_j(\bar{x}) \neq 0,$$

donde por la observación anterior los P_i, Q_j pueden considerarse polinomios en $K[x_1, \ldots, x_n]$.

Si alguno de los $P_i(x_0, \overline{a}) \in K[x_0]$ es no nulo, entonces b es algebraico sobre K, lo que implica que $b \in K$ (Observación 4.1.2), y hemos terminado. Por tanto, podemos suponer que

$$\varphi(\bar{x}) = \bigwedge_{i=1}^{m} Q_i(\bar{x}) \neq 0.$$

Por la existencia de b, cada polinomio $Q_i(x_0, \overline{a}) \in K[x_0]$ es no nulo y tiene, por tanto, un número finito de raíces. Como K es algebraicamente cerrado, es infinito (Corolario 4.1.23), y por tanto existe $c \in K$ tal que $K \models \varphi[c, \overline{a}]$. □

Vamos a ligar este teorema con dos resultados clásicos de geometría algebraica.

Definición 4.2.3. Sea K un cuerpo. Un subconjunto $X \subseteq K^n$ se dice *definible* (con parámetros) si existe una fórmula $\varphi(x_1, \ldots, x_n, \bar{a})$ en el lenguaje de anillos, con $\bar{a} \in K$, tal que $X = \{\, \bar{b} \in K^n : K \models \varphi(\bar{b}, \bar{a}) \,\}$.

Definición 4.2.4. Desde el punto de vista de la geometría algebraica, un conjunto se dice *constructible* si puede obtenerse como combinación booleana (es decir, mediante uniones, intersecciones y complementos) de conjuntos de ceros de polinomios con coeficientes en K.

El Teorema de Chevalley–Tarski admite la siguiente caracterización semántica:

Corolario 4.2.5. *Sea $K \models$ ACF. Entonces, en K los conjuntos definibles coinciden exactamente con los constructibles.*

Observación 4.2.6. Más adelante veremos que este resultado encuentra su "paralelo" en el caso de los cuerpos realmente cerrados: allí los conjuntos definibles coinciden exactamente con los *semialgebraicos*, es decir, aquellos descritos por combinaciones booleanas de desigualdades polinómicas.

El Nullstellensatz de Hilbert

En particular, del Teorema de Chevalley–Tarski se deduce el Nullstellensatz de Hilbert.

Corolario 4.2.7 (Nullstellensatz de Hilbert)**.** *Sea K un cuerpo algebraicamente cerrado, y*

$$P_1(\bar{x}), \ldots, P_m(\bar{x}) \in K[x_1, \ldots, x_n].$$

Si el sistema de ecuaciones polinómicas

$$P_1(\bar{x}) = P_2(\bar{x}) = \cdots = P_m(\bar{x}) = 0$$

tiene una solución en algún cuerpo $L \supseteq K$, entonces tiene una solución en K.

Demostración. Sea $L \supseteq K$ y $\bar{a} \in L^n$ tal que $P_i(\bar{a}) = 0$ para todo $i = 1, \ldots, m$. Ampliando L si es necesario, podemos suponer que L es algebraicamente cerrado. Como ACF tiene eliminación de cuantificadores, tenemos $K \preceq L$ por la Proposición 3.0.7.

Escogemos ahora $\mathcal{L}_{\text{anillo}}$-términos $F_i(\bar{x}, \bar{z}_i)$ y tuplas $\bar{b}_i$ en K tales que $P_i(\bar{x}) = F_i(\bar{x}, \bar{b}_i)$, lo cual es posible porque los términos del lenguaje de anillos representan precisamente polinomios con coeficientes (parámetros) en K. Entonces

$$L \models \exists \bar{x} \bigwedge_i F_i(\bar{x}, \bar{b}_i) = 0,$$

y por tanto también

$$K \models \exists \bar{x} \bigwedge_i F_i(\bar{x}, \bar{b}_i) = 0,$$

pues $K \preceq L$. De aquí se concluye que el sistema ya tiene una solución en K. □

Este teorema constituye una de las conexiones más profundas entre la lógica y la geometría algebraica: la existencia de soluciones en una extensión algebraicamente cerrada se refleja ya en el propio cuerpo de partida. Desde un punto de vista conceptual, en este contexto la existencia de soluciones de un sistema de ecuaciones polinómicas depende únicamente del ideal generado por los polinomios.

El Teorema de Ax

Nos dirigimos ahora a otro resultado de gran interés: el Teorema de Ax, que se apoya en la relación entre las teorías ACF_p (para $p > 0$) y ACF_0.

Teorema 4.2.8. *Sea p un número primo o $p = 0$. La teoría ACF_p es completa.*

Demostración. Todo cuerpo de característica $p > 0$ contiene un cuerpo isomorfo a $\mathbb{F}_p$ como subcuerpo. Podemos, sin pérdida de generalidad, identificar dichas copias y suponer que los modelos considerados comparten literalmente ese subcuerpo. Si K y L son cuerpos algebraicamente cerrados de característica p, entonces $K \equiv L$ por el Teorema de Chevalley-Tarski y la Proposición 3.0.7(1). Por tanto, acabamos de ver que todo par de modelos de ACF_p son elementalmente equivalentes. Por el Corolario A.1.15, concluimos que ACF_p es completa.

Para el caso ACF_0, el argumento es análogo reemplazando $\mathbb{F}_p$ por $\mathbb{Q}$. □

Teorema 4.2.9 (Principio de Lefschetz)**.** *Sea φ una $\mathcal{L}_{\text{anillo}}$-sentencia. Son equivalentes:*

1. $\mathbb{C} \models \varphi$.
2. *Existe un cuerpo algebraicamente cerrado de característica 0 en el que se satisface φ.*
3. *Todo cuerpo algebraicamente cerrado de característica 0 satisface φ.*
4. *Existe $N \in \mathbb{N}$ tal que φ se satisface en cualquier cuerpo algebraicamente cerrado de característica $p > N$.*
5. *Existe un conjunto infinito de números primos $\mathcal{P}$ tal que para todo $p \in \mathcal{P}$ existe un cuerpo algebraicamente cerrado de característica p en el que se satisface φ.*

Demostración. Las equivalencias entre (1), (2) y (3) se deducen del teorema anterior y del Corolario A.1.15.

Vemos que (3) implica (4). Como $\mathrm{ACF}_0 = \mathrm{ACF} \cup \{\chi_p \mid p \text{ primo}\}$, donde χ_p expresa que $p = 1 + \cdots + 1 \neq 0$, si $\mathrm{ACF}_0 \models \varphi$, por compacidad existe un subconjunto finito $\Delta \subseteq \mathrm{ACF}_0$ tal que $\Delta \models \varphi$. Como Δ contiene solo un número finito de sentencias χ_p, existe $N \in \mathbb{N}$ tal que todo cuerpo algebraicamente cerrado K de característica $p > N$ satisface Δ, y por tanto $K \models \varphi$.

Es inmediato ver que (4) implica (5).

Para ver que (5) implica (3), sea $p \in \mathcal{P}$ y $K_p \models \mathrm{ACF}_p$ tal que $K_p \models \varphi$. Si $\mathrm{ACF}_0 \not\models \varphi$, entonces $\mathrm{ACF}_0 \models \neg\varphi$ por completitud. Como (3) implica (4), existe $N \in \mathbb{N}$ tal que $\neg\varphi$ se satisface en todo cuerpo algebraicamente cerrado de característica $p > N$. Esto obliga a que $\mathcal{P}$ sea finito, contradicción. □

Definición 4.2.10. Una *cadena de $\mathcal{L}$-estructuras* es una sucesión $(\mathcal{M}_i)_{i\in\mathbb{N}}$ de $\mathcal{L}$-estructuras tal que $\mathcal{M}_i \subseteq \mathcal{M}_{i+1}$ para todo i.

Si $(\mathcal{M}_i)_{i\in\mathbb{N}}$ es tal cadena, existe una única $\mathcal{L}$-estructura $\mathcal{M}$ con universo $M = \bigcup_{i\in\mathbb{N}} M_i$ tal que $\mathcal{M}_i \subseteq \mathcal{M}$ para todo i. En efecto, los símbolos del lenguaje se interpretan poniendo

$$c^{\mathcal{M}} = c^{\mathcal{M}_0}, \quad f^{\mathcal{M}} = \bigcup_{i\in\mathbb{N}} f^{\mathcal{M}_i}, \quad R^{\mathcal{M}} = \bigcup_{i\in\mathbb{N}} R^{\mathcal{M}_i},$$

lo cual está bien definido. La $\mathcal{L}$-estructura obtenida así se denota $\mathcal{M} = \bigcup_{i\in\mathbb{N}} \mathcal{M}_i$.

Definición 4.2.11. Una fórmula de la forma $\forall x_1 \ldots \forall x_n \exists y_1 \ldots \exists y_m \ \varphi(\bar{x}, \bar{y})$, con φ libre de cuantificadores y $m, n \geq 0$, se denomina *$\forall\exists$-fórmula*.

Lema 4.2.12. *Sea ψ una $\forall\exists$-sentencia en $\mathcal{L}$ y $(\mathcal{M}_i)_{i\in\mathbb{N}}$ una cadena de $\mathcal{L}$-estructuras tal que $\mathcal{M}_i \models \psi$ para todo i. Entonces la unión $\mathcal{M} = \bigcup_{i\in\mathbb{N}} \mathcal{M}_i$ también satisface ψ.*

Demostración. Sea ψ la sentencia $\forall x_1, \dots, x_n \, \exists y_1, \dots, y_m \, \varphi(\bar{x}, \bar{y})$, con φ libre de cuantificadores. Tenemos que probar que $\mathcal{M} \models \exists y_1, \dots, y_m \, \varphi(\bar{a}, \bar{y})$ para todo $\bar{a} \in M^n$.

Como la cadena $(M_i)_{i\in\mathbb{N}}$ es creciente, existe $k \in \mathbb{N}$ tal que $\bar{a} \in M_k^n$. Por hipótesis, $\mathcal{M}_k \models \psi$, así que existen $b_1, \dots, b_m \in M_k$ con $\mathcal{M}_k \models \varphi(\bar{a}, \bar{b})$. De aquí se deduce que $\mathcal{M} \models \varphi(\bar{a}, \bar{b})$, pues φ es libre de cuantificadores y $\mathcal{M}_k \subseteq \mathcal{M}$ (Observación 2.2.3). □

Observación 4.2.13. De hecho, es posible probar que una sentencia se preserva bajo uniones de cadenas (cumple la propiedad del lema anterior) si y solo si es lógicamente equivalente a una $\forall\exists$-sentencia.

Proposición 4.2.14. *Sea φ una $\forall\exists$-sentencia en el lenguaje $\mathcal{L}_{\text{anillo}}$ que se satisface en todo cuerpo finito. Entonces* ACF $\models \varphi$. *En particular, φ se satisface en $\mathbb{C}$.*

Demostración. Por la Observación 4.1.21, $\mathbb{F}_p^{\text{alg}}$ es la unión de una cadena de cuerpos finitos. Por la proposición anterior, se tiene que $\mathbb{F}_p^{\text{alg}} \models \varphi$ para todo primo p; luego φ se satisface en todo cuerpo algebraicamente cerrado de característica $p > 0$ (por la Observación 4.1.22), y el Principio de Lefschetz implica entonces que φ se satisface también en todo cuerpo algebraicamente cerrado de característica 0, en particular en $\mathbb{C}$. □

Teorema 4.2.15 (Ax)**.** *Sea $f : \mathbb{C}^n \to \mathbb{C}^n$ una aplicación polinómica, es decir, de la forma $f = (f_1, \dots, f_n)$ con $f_i \in \mathbb{C}[x_1, \dots, x_n]$ polinomios. Si f es inyectiva, entonces f es sobreyectiva.*

Demostración. La siguiente sentencia $\psi_{n,d}$ es una $\forall\exists$-fórmula y formaliza en el lenguaje de anillos la afirmación "toda aplicación polinómica inyectiva $f : K^n \to K^n$ de grado a lo sumo d es sobreyectiva":

$$\forall \bar{z}_1, \dots, \bar{z}_n, \bar{u} \; \exists \bar{x}, \bar{x}' \left[\left(\bigwedge_{i=1}^{n} P_{n,d}(\bar{z}_i, \bar{x}) = u_i \right) \; \vee \; \left(\bigwedge_{i=1}^{n} P_{n,d}(\bar{z}_i, \bar{x}) = P_{n,d}(\bar{z}_i, \bar{x}') \wedge \neg \bigwedge_{i=1}^{n} x_i = x_i' \right) \right].$$

Los términos $P_{n,d}(\bar{z}_i, \bar{x})$ representan los polinomios f_i, y la disyunción expresa que para todo $\bar{u}$ existe una preimagen $\bar{x}$ o bien que f no es inyectiva. Además, identificamos la conjunción $\bigwedge_i P_{n,d}(\bar{z}_i, \bar{x}) = u_i$ con la aplicación polinómica $f = (f_1, \dots, f_n) : K^n \to K^n$.

Nótese que el parámetro d se introduce para permitir formalizar la afirmación en el lenguaje de anillos, pues en caso contrario la expresión "para toda aplicación polinómica" implicaría cuantificar sobre polinomios de grado arbitrario, es decir, sobre colecciones infinitas de coeficientes, algo que no puede expresarse mediante una fórmula de primer orden.

Como $\psi_{n,d}$ se satisface en todo cuerpo finito (Observación 4.1.24), se sigue por la proposición anterior que ACF $\models \psi_{n,d}$, y en particular $\mathbb{C} \models \psi_{n,d}$. Dado que esto ocurre para todo n y todo d, obtenemos el resultado. □

Aunque no nos detendremos demasiado en él, este teorema también es importante: en el marco de ACF, una propiedad algebraica a priori tan fuerte como la sobreyectividad de una aplicación polinómica puede deducirse a partir de la inyectividad, normalmente mucho más sencilla de verificar.

En cualquier caso, lo desarrollado hasta aquí refleja claramente la potencia de la eliminación de cuantificadores en ACF.

Pasamos ahora al estudio de la teoría de los cuerpos realmente cerrados.

5. RCF

Al igual que en el caso de ACF, antes de demostrar la eliminación de cuantificadores en RCF debemos desarrollar varios resultados propios de la teoría de los cuerpos realmente cerrados.

5.1. Cuerpos realmente cerrados

En esta sección seguiremos de cerca el Apéndice B.1 de [7], aunque para la parte más constructiva (existencia del orden y existencia de la clausura real) adoptaremos el enfoque más explícito de [8]. Solo para la unicidad de la clausura real retomaremos el tratamiento de [7], lo que nos permitirá ser más sucintos.

Definición 5.1.1. Sea A un dominio de integridad. Una relación de orden total $<$ en A se dice *compatible con las operaciones* (o compatible con la estructura de anillo) si para todo $x, y \in A$ satisface las siguientes propiedades:

1. Si $x < y$, entonces $x + z < y + z$ para todo $z \in A$.
2. Si $0 < x$ y $0 < y$, entonces $0 < xy$.

Un cuerpo $(F, <)$ con un orden compatible es un *cuerpo ordenado*.

Observación 5.1.2. En un cuerpo ordenado todo cuadrado es no negativo.[19] En particular, por la propiedad (1) de la definición, se sigue que toda suma de cuadrados es no negativa.

Si $0 < x$, entonces $0 < x \cdot x$ por hipótesis; si $x = 0$, entonces $x^2 = 0$; y si $x < 0$, entonces $0 < -x$, por lo que $0 < (-x)(-x)$. Basta justificar que $(-x)^2 = x^2$: como $0 = 1+(-1)$, multiplicando por (-1) y usando la distributividad se obtiene $0 = (1 + (-1))(-1) = (-1) + (-1)(-1)$, de donde $1 = (-1)(-1)$. Así, $(-x)^2 = (-1)^2x^2 = x^2$. En todos los casos, $0 < x^2 \vee x^2 = 0$.

Como $0 < 1^2 = 1$, todo cuerpo ordenado tiene característica cero.

A partir de ahora escribiremos $\leq$ en lugar de $(0 < x \vee x = 0)$, y denotaremos el cuerpo ordenado por $(F, \leq)$ en lugar de $(F, <)$. También escribiremos $1/x$ para denotar el inverso multiplicativo.

Vamos a caracterizar los cuerpos que admiten un orden compatible con las operaciones. Para ello, expresamos la noción de *no negatividad* de manera algebraica.

Definición 5.1.3. Sea R un cuerpo (no necesariamente ordenado). Un subconjunto $P \subseteq R$ se llama *cono* de R si se cumplen las siguientes condiciones:

1. si $x, y \in P$ entonces $x + y \in P$,
2. si $x, y \in P$ entonces $xy \in P$,
3. si $x \in R$ entonces $x^2 \in P$.

El cono P se dice *propio* si además cumple que $-1 \notin P$.

Definición 5.1.4. Sea $(F, \leq)$ un cuerpo ordenado. El subconjunto $P = \{\, x \in F \mid 0 \leq x \,\}$ se llama el *cono positivo* de $(F, \leq)$.

[19] Como es habitual, diremos que un elemento x es *no negativo* si $x = 0$ o $0 < x$, y que un elemento es un *cuadrado* si puede escribirse como $x = y^2$ para algún y.

Proposición 5.1.5. *Sea $(F, \leq)$ un cuerpo ordenado. El cono positivo P de $(F, \leq)$ es un cono propio que cumple: $P \cup (-P) = F$, donde $-P = \{ x \in F \mid -x \in P \}$. Recíprocamente, si P es un cono propio de un cuerpo R que cumple $P \cup (-P) = R$, entonces R puede ordenarse definiendo: $x \leq_P y$ si y solo si $y - x \in P$.*

Demostración. Vemos primero que P es un cono propio. Si $x, y \in P$, entonces $0 \leq x$ y $0 \leq y$, de modo que $0 \leq x + y$ y $0 \leq xy$ por compatibilidad del orden. Además, para todo $x \in F$, se tiene $0 \leq x^2$, luego $x^2 \in P$. Así, P es un cono. Es propio porque si $-1 \in P$, tendríamos $0 \leq -1$, y sumando 1 se obtendría $1 = 1^2 \leq 0$, contradicción.

Por definición de orden total, para todo $x \in F$ ocurre exactamente una de las siguientes: $0 < x$, $x = 0$ o $x < 0$, de donde se sigue que $P \cup (-P) = F$.

Recíprocamente, sea P un cono propio de un cuerpo R que satisface $P \cup (-P) = R$.

Definimos una relación en R por $x \leq_P y$ si y solo si $y - x \in P$. Vemos que $\leq_P$ es un orden total compatible con las operaciones.

1. *Reflexividad:* para todo $x \in R$ se tiene $x \leq_P x$, pues por definición $x \leq_P x$ si y solo si $x - x \in P$, y $x - x = 0 \in P$ por hipótesis.

2. *Antisimetría:* observamos que para cualquier cono propio P, se cumple que $P \cap (-P) = \{0\}$. En efecto, si $x \in P \cap (-P)$, entonces $x \in P$ y $-x \in P$. Si $x \in P \setminus \{0\}$, entonces $(1/x)^2 \in P$, y por tanto $x \cdot (1/x)^2 = 1/x \in P$, de donde $-1 = \frac{1}{x}(-x) \in P$, contradicción.

   Por tanto, si $x \leq_P y$ e $y \leq_P x$, entonces $y - x \in P$ y $x - y \in P$, luego $x - y = -1 \cdot (y - x) \in -P$, de donde $x - y \in P \cap (-P)$. De aquí $x - y = 0$, luego $x = y$.

3. *Transitividad:* si $x \leq_P y$ e $y \leq_P z$, entonces $y - x \in P$ y $z - y \in P$. Como $P + P \subseteq P$, se tiene $(z - y) + (y - x) = z - x \in P$, y por tanto $x \leq_P z$.

4. *Totalidad:* dados $x, y \in R$, como $P \cup (-P) = R$, o bien $y - x \in P$ o bien $x - y \in P$. En el primer caso $x \leq_P y$, en el segundo $y \leq_P x$.

5. *Compatibilidad con la suma:* si $x \leq_P y$, entonces $y - x \in P$, y para todo $z \in R$ se tiene $(y + z) - (x + z) = y - x \in P$, luego $x + z \leq_P y + z$.

6. *Compatibilidad con el producto:* si $0 \leq_P x$ y $0 \leq_P y$, entonces $x \in P$ e $y \in P$. Como $P \cdot P \subseteq P$, se tiene $xy \in P$.

Así, $\leq_P$ es un orden compatible con las operaciones de R, y el correspondiente cono positivo es precisamente P. □

Observación 5.1.6. Sea R un cuerpo. Denotamos por $\Sigma R^2 := \{ x_1^2 + \cdots + x_n^2 \mid n \in \mathbb{N},\ x_i \in R \}$ al conjunto de sumas de cuadrados de elementos de R.

El conjunto ΣR^2 es un cono, y por las propiedades (1) y (3) de la Definición 5.1.3 se sigue que está contenido en todo cono de R.

Lema 5.1.7. *Sea P un cono propio de un cuerpo R.*

1. *Si $-a \notin P$, entonces $P[a] := \{ x + ay \mid x, y \in P \}$ es también un cono propio de R.*

2. *P está contenido en el cono positivo de algún orden de R.*

Demostración. Es fácil ver que $P[a]$ es un cono. Vemos que $-1 \notin P[a]$. Si $-1 = x + ay$ con $x, y \in P$, entonces o bien $y = 0$, en cuyo caso $-1 = x \in P$, contradicción; o bien $y \neq 0$, en cuyo caso $-a = (\frac{1}{y})^2 y(1 + x)$. Como $(\frac{1}{y})^2 \in P$ por ser un cuadrado, y además $y, 1 + x \in P$, se sigue que $-a \in P$, contradicción.

Para la otra implicación, sea $\mathcal{C} = \{\, Q \subseteq R \mid Q \text{ es un cono propio de } R \text{ y } P \subseteq Q \,\}$, ordenado por la inclusión. Entonces $(\mathcal{C}, \subseteq)$ es un conjunto parcialmente ordenado no vacío, pues $P \in \mathcal{C}$.

Para toda cadena $\mathcal{D}$ en $\mathcal{C}$ podemos obtener una cota superior definiendo $Q^* := \bigcup_{Q \in \mathcal{D}} Q$. Por el Lema de Zorn, existe un elemento maximal $Q \in \mathcal{C}$, es decir, un cono propio maximal de R que contiene a P. Si probamos que $Q \cup (-Q) = R$, por la proposición anterior habremos terminado. Sea $a \notin Q$. Por (1), $Q[-a]$ es un cono propio, y como Q es maximal, se sigue que $Q = Q[-a]$, de donde $-a \in Q$. □

Proposición 5.1.8. *Sea R un cuerpo de característica distinta de 2 y sea $a \in R$. Entonces existe un orden en R respecto del cual $a < 0$ si y solo si a no es suma de cuadrados en R.*

Demostración. Como toda suma de cuadrados es no negativa (Observación 5.1.2), si existe un orden en R tal que $a < 0$, a no puede ser suma de cuadrados en R.

Recíprocamente, supongamos que $a \notin \Sigma R^2$. Como $\operatorname{car} R \neq 2$, si $-1 \in \Sigma R^2$ entonces todo elemento de R es suma de cuadrados (y en particular lo es a): en efecto, de $-1 = \sum u_i^2$ se deduce $-y^2 = \sum (y u_i)^2$, luego $x^2 - y^2 \in \Sigma R^2$ para cualesquiera $x, y \in R$. Como $a = \left(\frac{a+1}{2}\right)^2 - \left(\frac{a-1}{2}\right)^2$, se tendría entonces $a \in \Sigma R^2$, contradicción. Por tanto, $-1 \notin \Sigma R^2$, y ΣR^2 es un cono propio.

Definimos $P := \Sigma R^2 - a\,\Sigma R^2 = \{x + (-a)y : \ x, y \in \Sigma R^2\} = (\Sigma R^2)[-a]$. Puesto que $a \notin \Sigma R^2$, por el Lema 5.1.7 (1) P es un cono propio. Por el Lema 5.1.7 (2), existe un orden $\leq$ en R cuyo cono positivo contiene a P. En particular, $0 < -a$ en este orden, de donde $a < 0$. □

Usaremos este resultado más adelante.

Teorema 5.1.9. *Sea R un cuerpo. Son equivalentes:*

1. *R puede ordenarse.*
2. *R posee un cono propio.*
3. *$-1 \notin \Sigma R^2$.*

En tal caso decimos que R es un cuerpo real.

Demostración. Por la Proposición 5.1.5, si R es un cuerpo ordenado, su cono positivo es un cono propio, luego (1) implica (2). Por la Observación 5.1.6, si R posee un cono propio P, entonces $\Sigma R^2 \subseteq P$, y como $-1 \notin P$, también $-1 \notin \Sigma R^2$, luego (2) implica (3). Si $-1 \notin \Sigma R^2$, entonces ΣR^2 es un cono propio de R, y por el Lema 5.1.7 (2) sabemos que ΣR^2 está contenido en el cono positivo de algún orden de R, luego (3) implica (1). □

Definición 5.1.10. Sea R un cuerpo real. R es un *cuerpo realmente cerrado* si no admite ninguna extensión algebraica real propia $R \subsetneq R_1$.

Antes de enunciar la caracterización de los cuerpos realmente cerrados, citamos un lema auxiliar sobre polinomios que utilizaremos en la demostración.

Decimos que un polinomio $g(X_1, \ldots, X_n)$ es *simétrico* en las variables $X_1, \ldots, X_n$ si es invariante bajo sus permutaciones, es decir, $g(X_1, \ldots, X_n) = g(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$ para toda $\sigma \in S_n$.

Lema 5.1.11. *Sea $p(T) \in R[T]$ un polinomio mónico de grado n, y sean $y_1, \ldots, y_n$ sus raíces en una clausura algebraica de R. Si $g(X_1, \ldots, X_n)$ es un polinomio simétrico en $X_1, \ldots, X_n$ con coeficientes en R, entonces $g(y_1, \ldots, y_n) \in R$.*

Idea de la demostración. Los *polinomios simétricos elementales* en n variables vienen dados por:

$$f_k(X_1, \ldots, X_n) = \sum_{1 \leq i_1 < \cdots < i_k \leq n} X_{i_1} \cdots X_{i_k}, \ 1 \leq k \leq n,$$

en particular $f_1 = X_1 + \cdots + X_n$ y $f_n = X_1 \cdots X_n$.

Sea ahora $p(X) \in R[X]$ un polinomio mónico cuyo conjunto de raíces es $\{y_1, \ldots, y_n\}$. Su factorización en una clausura algebraica de R es

$$p(X) = \prod_{i=1}^{n} (X - y_i) = X^n - f_1(y_1, \ldots, y_n)X^{n-1} + \cdots + (-1)^n f_n(y_1, \ldots, y_n).$$

Como $p(X)$ tiene coeficientes en R y es mónico, por unicidad de los coeficientes se sigue que $f_k(y_1, \ldots, y_n) \in R$ $1 \leq k \leq n$.

Por el Teorema fundamental de los polinomios simétricos [6, §2.2], existe un único polinomio $G \in R[T_1, \ldots, T_n]$ tal que, como polinomios en n variables,

$$g(X_1, \ldots, X_n) = G(f_1(X_1, \ldots, X_n), \ldots, f_n(X_1, \ldots, X_n)).$$

Evaluando en $(y_1, \ldots, y_n)$ se obtiene $g(y_1, \ldots, y_n) = G\big(f_1(y_1, \ldots, y_n), \ldots, f_n(y_1, \ldots, y_n)\big) \in R$. □

Observación 5.1.12. En las hipótesis anteriores, si consideramos un polinomio $Q(x)$ en una variable libre x cuyos coeficientes son expresiones simétricas en los y_i (lo que ocurre, en particular, cuando el polinomio es simétrico formalmente en las variables que representan esos y_i), el lema garantiza que dichos coeficientes pertenecen a R; de este modo, $Q(x) \in R[x]$.

Teorema 5.1.13. *Sea R un cuerpo. Son equivalentes:*

1. *R es realmente cerrado.*
2. *Existe un único orden en R cuyo cono positivo es el conjunto de cuadrados de R, y todo polinomio de grado impar de $R[X]$ posee una raíz en R.*
3. *El anillo $R[i] := R[X]/(X^2 + 1)$ es un cuerpo algebraicamente cerrado.*

Demostración. Vemos que (1) implica (2). Sea $a \in R$. Si a no es un cuadrado en R, entonces $R[\sqrt{a}] = R[X]/(X^2 - a)$ es una extensión algebraica propia de R, y por tanto $R[\sqrt{a}]$ no es real. Así, $-1 = \sum_{i=1}^{n}(x_i + \sqrt{a}\, y_i)^2 = \sum_{i=1}^{n} x_i^2 \ + \ 2\sqrt{a}\sum_{i=1}^{n} x_i y_i \ + \ a\sum_{i=1}^{n} y_i^2$.

Como la descomposición de -1 respecto de la base $\{1, \sqrt{a}\}$ de $R[\sqrt{a}]$ es única, el coeficiente de $\sqrt{a}$ debe ser nulo. Por tanto,$-1 = \sum_{i=1}^{n} x_i^2 + a\sum_{i=1}^{n} y_i^2$.

Si $\sum_{i=1}^{n} y_i^2 = 0$, se tendría $-1 = \sum_{i=1}^{n} x_i^2 \in R$, pero R es real, contradicción. Por tanto, $\sum_{i=1}^{n} y_i^2 \neq 0$, y despejando obtenemos $-a = \frac{\left(1+\sum_{i=1}^{n} x_i^2\right)}{\left(\sum_{i=1}^{n} y_i^2\right)} \in \Sigma R^2$.

Esto muestra, por un lado, que $\Sigma R^2 \cup (-\Sigma R^2) = R$, de modo que, por la Proposición 5.1.5, existe un único orden en R cuyo cono positivo es precisamente ΣR^2. Por otro lado, todo elemento que no sea un cuadrado resulta negativo para dicho orden, de donde se sigue que todo elemento positivo es un cuadrado.

Falta demostrar que, si $f \in R[X]$ tiene grado impar, entonces f tiene una raíz en R. Lo haremos por inducción en el grado d de f. Para $d = 1$ está claro. Sea f un polinomio de grado $d > 1$ tal que todo polinomio de grado impar $< d$ tiene una raíz en R. Supongamos que f no tiene raíces en R. Como todo polinomio de grado impar tiene al menos un factor irreducible de grado impar, pues en caso contrario el grado de f sería par al ser la suma de estos, podemos suponer que f es irreducible. El cociente $R[X]/(f)$ es una extensión algebraica no trivial de R. Por tanto, no es real, de donde $-1 = \sum_{i=1}^n \overline{h_i}^2$ en $R[X]/(f)$, y podemos tomar los representantes de grado $< d$.

Sea $\pi : R[X] \to R[X]/(f)$ la proyección canónica. Aplicando la definición de π, la igualdad anterior equivale a $\pi(-1) = \pi(\sum_{i=1}^n h_i^2)$, de donde $\pi(-1 - \sum_{i=1}^n h_i^2) = 0$. Como $\ker \pi = (f)$, existe $g \in R[X]$ tal que $-1 = \sum_{i=1}^n h_i^2 + fg$ en $R[X]$. $(*)$

Sea $m_i = deg(h_i)$. Como $\deg(h_i^2) = 2m_i$, se tiene que $\deg(\sum_{i=1}^n h_i^2) = 2\,\text{máx}_i\, m_i < 2d$. De $-1 = \sum_{i=1}^n h_i^2 + fg$ se sigue que $\deg(fg) = \deg(\sum_{i=1}^n h_i^2)$, de donde $\deg(g) = 2\,\text{máx}_i\, m_i - d$. Como $2\,\text{máx}_i\, m_i$ es par y d es impar, $deg(g)$ es un número impar, y como $2\,\text{máx}_i\, m_i < 2d$, se tiene que $\deg(g) < d$. Por hipótesis de inducción, el polinomio g tiene una raíz $a \in R$.

Evaluando $(*)$ en a se obtiene $-1 = \sum_{i=1}^n h_i(a)^2 \in R$, contradicción.

Vemos ahora que (2) implica (3). Empezaremos demostrando que todo polinomio en $R[x]$ tiene alguna raíz en $R[i]$. Sea $f \in R[X]$ de grado $d = 2^m n$ con n impar. Procedemos por inducción en m. Para $m = 0$, sabemos que f tiene una raíz en R. Supongamos ahora que el resultado es cierto para $m - 1$. Tomemos $y_1, \ldots, y_d$ las raíces de f en una clausura algebraica de R y definamos $g_h(X) := \prod_{1 \le \lambda < \mu \le d} \big(X - (y_\lambda + y_\mu + h\, y_\lambda y_\mu)\big)$, para $h \in \mathbb{Z}$.

Como g_h es invariante al permutar $y_1, \ldots, y_d$, por la observación anterior $g_h \in R[X]$, de grado $\deg g_h = |\{(\lambda, \mu) : 1 \le \lambda < \mu \le d\}| = \binom{d}{2} = \frac{d(d-1)}{2} = \frac{2^m n(2^m n - 1)}{2} = 2^{m-1} n(2^m n - 1) = 2^{m-1} n'$, donde $n' := n(2^m n - 1)$. Como n es impar y $2^m n$ es par, $2^m n - 1$ es un número impar, de modo que n' es producto de dos números impares, y por tanto también impar. Por inducción, cada g_h tiene una raíz en $R[i]$, de la forma $y_\lambda + y_\mu + h\, y_\lambda y_\mu$ con λ, μ fijos entre $\{1, \ldots, d\}$.

Como el conjunto de pares $\{(\lambda, \mu) : 1 \le \lambda < \mu \le d\}$ es finito, por el principio del palomar podemos elegir $h_1 \neq h_2$ y un par fijo (λ, μ) tales que $y_\lambda + y_\mu + h_1 y_\lambda y_\mu \in R[i]$ e $y_\lambda + y_\mu + h_2 y_\lambda y_\mu \in R[i]$. Restando ambas expresiones se obtiene $(h_1 - h_2)\, y_\lambda y_\mu \in R[i]$. Como $h_1 - h_2 \in \mathbb{Z} \setminus \{0\} \subset R[i]$, dicho elemento es invertible en $R[i]$. Por tanto, $y_\lambda y_\mu \in R[i]$. Como $y_\lambda + y_\mu + h_1 y_\lambda y_\mu \in R[i]$, restando $h_1 y_\lambda y_\mu$ se obtiene $y_\lambda + y_\mu \in R[i]$. Queremos ver que y_λ e y_μ pertenecen a $R[i]$.

Demostramos primero que todo elemento de $R[i]$ tiene raíz cuadrada en $R[i]$.

Sea $z = a + bi \in R[i]$, con $a, b \in R$. Como $a^2 + b^2 \ge 0$, por hipótesis existe $r \in R$ tal que $r^2 = a^2 + b^2$. Definimos $u^2 = \frac{r+a}{2}$, $\quad v^2 = \frac{r-a}{2}$. Ambos términos son no negativos, luego existen $u, v \in R$ cumpliendo estas igualdades. Además, $(uv)^2 = \frac{r^2 - a^2}{4} = \frac{b^2}{4}$, y podemos escoger los signos de u y v de modo que $2uv = b$. Entonces $(u + vi)^2 = u^2 - v^2 + 2uvi = a + bi = z$.

Esto prueba que, dados $b, c \in R[i]$ cualesquiera, la ecuación $x^2 + bx + c = 0$ tiene sus dos soluciones en $R[i]$. En efecto, el discriminante $\Delta = b^2 - 4c$ pertenece a $R[i]$, y por lo anterior existe $\delta \in R[i]$ tal que $\delta^2 = \Delta$. Por la fórmula cuadrática, las soluciones son $\frac{-b \pm \delta}{2} \in R[i]$. Aplicando este resultado al polinomio $p(X) = X^2 - (y_\lambda + y_\mu)X + y_\lambda y_\mu \in R[i][X]$, como y_λ e y_μ son precisamente sus raíces, se tiene que $y_\lambda, y_\mu \in R[i]$. En particular, f tiene una raíz en $R[i]$.

Sea $q \in R[i][X]$. Entonces $q(X) = a_0 + a_1 X + \cdots + a_n X^n$, con $a_k = u_k + v_k i$, $u_k, v_k \in R$. Definimos $\bar{q}(X) = \bar{a}_0 + \bar{a}_1 X + \cdots + \bar{a}_n X^n$, donde $\bar{a}_k = u_k - v_k i$. Entonces $q\bar{q} = \sum_{k=0}^{2n} c_k X^k$, donde $c_k = \sum_{i+j=k} a_i \bar{a}_j$. Observamos que $\overline{a_i \bar{a}_j} = \bar{a}_i a_j$. Por tanto, $\overline{c_k} = \sum_{i+j=k} \overline{a_i \bar{a}_j} = \sum_{i+j=k} \bar{a}_i a_j$. Intercambiando i y j en la suma obtenemos $\overline{c_k} = c_k$, de donde $c_k \in R$. Se sigue que $q\bar{q} \in R[X]$, por lo que el polinomio $q\bar{q}$ tiene una raíz $x \in R[i]$. Entonces, o bien $q(x) = 0$, o bien $\bar{q}(x) = 0$; en este último caso, $\bar{q}(x) = 0 \;\Rightarrow\; \overline{\bar{q}(x)} = 0 \;\Rightarrow\; q(\bar{x}) = 0$, de modo que $\bar{x}$ es raíz de q. En cualquier caso, q tiene una raíz en $R[i]$.

Terminamos viendo que (3) implica (1). Ya sabemos que -1 no es un cuadrado en R, pues si lo fuera, X^2+1 tendría una raíz en R, el ideal (X^2+1) no sería maximal y $R[i]$ no sería un cuerpo. Veamos ahora que en R una suma de cuadrados vuelve a ser un cuadrado. Sean $a, b \in R$. Como $R[i]$ es algebraicamente cerrado, el polinomio $X^2-(a+ib) \in R[i][X]$ tiene una raíz $c+id \in R[i]$, con $c, d \in R$. Entonces $(c+id)^2 = c^2-d^2+2cd\,i = a+ib$, de donde $a = c^2-d^2$ y $b = 2cd$, y se obtiene $a^2+b^2 = (c^2+d^2)^2$. Iterando el caso binario, se concluye que toda suma finita de cuadrados en R es un cuadrado. En particular, si -1 fuese suma de cuadrados en R, sería un cuadrado, contradicción. Por tanto, $-1 \notin \Sigma R^2$ y R es real.

Falta ver que R no admite extensiones algebraicas reales propias. Sea K una extensión algebraica de R y supongamos que K es real. Entonces $K[i]$ es una extensión algebraica de $R[i]$. Como $R[i]$ es algebraicamente cerrado, se tiene $K[i] = R[i]$. Por tanto, $[R[i] : R] = [R[i] : K]\,[K : R]$. Como $[R[i] : R] = 2$, se sigue que $[K : R]$ divide a 2, esto es, $[K : R] = 1$ o $[K : R] = 2$. Si $[K : R] = 1$, entonces $K = R$. Si $[K : R] = 2$, entonces $K = R[i]$, de modo que -1 es cuadrado en K, pero K es real, contradicción. □

Observación 5.1.14 (Teorema Fundamental del Álgebra)**.** En esencia, el teorema muestra que la relación entre un cuerpo realmente cerrado R y la extensión $R[i]$ es la versión abstracta de la relación entre $\mathbb{R}$ y $\mathbb{C}$; en ese sentido, $\mathbb{R}$ es el ejemplo paradigmático de cuerpo realmente cerrado. En particular, obtenemos una versión más general del Teorema Fundamental del Álgebra: si R es realmente cerrado, entonces $R[i]$ es algebraicamente cerrado.

Corolario 5.1.15. *Sea R un cuerpo realmente cerrado. Entonces, los únicos polinomios mónicos irreducibles de $R[X]$ son:*

$$X - a \ (a \in R),$$

y

$$(X-b)^2 + c \ (b, c \in R,\ 0 < c).$$

En particular, todo polinomio de $R[X]$ se descompone de manera única como producto de factores lineales y cuadráticos de la forma anterior.

Demostración. Por el teorema anterior, todo polinomio $f \in R[X]$ se factoriza en $R[i][X]$ como producto de términos lineales $f(X) = \prod_k (X-\alpha_k)$, $\alpha_k \in R[i]$. Escribimos cada raíz como $\alpha = u+vi$, con $u, v \in R$. Si $v = 0$, entonces $\alpha \in R$ y el factor correspondiente es $X-u$. Si $v \neq 0$, $\overline{\alpha}$ también es raíz de f, y por tanto el factor $X-\overline{\alpha}$ aparece en la factorización. El producto de ambos factores es $(X-\alpha)(X-\bar{\alpha}) = X^2-2uX+(u^2+v^2) = (X-u)^2+v^2$. □

Definición 5.1.16. Sea $(F, \leq)$ un cuerpo ordenado. Sea R una extensión algebraica de F tal que R es realmente cerrado y su orden único extiende el orden de F (es decir, para todo $x, y \in F$, si $x \leq y$ entonces $x \leq_R y$). Decimos que $(R, \leq_R)$ es una clausura real de $(F, \leq)$.

Teorema 5.1.17. *Sea $(F, \leq)$ un cuerpo ordenado. Entonces $(F, \leq)$ tiene una clausura real.*

Demostración. Sea $F \subset \overline{F}$ una clausura algebraica de F. Consideramos la clase

$$\mathcal{E} = \left\{ (E, \leq_E) \;\middle|\; \begin{array}{l} F \subset E \subset \overline{F} \text{ son extensiones de cuerpos,} \\ \leq_E \text{ es tal que } (E, \leq_E) \text{ es un cuerpo ordenado y } \ \leq_E \cap (F \times F) = \leq \end{array} \right\}.$$

Identificando $\leq_E$ con $E \times E \in \mathcal{P}(\overline{F} \times \overline{F})$, un razonamiento análogo al del Teorema 4.1.10 muestra que existe una función inyectiva $\tau : \mathcal{E} \longrightarrow \mathcal{P}\big(\bar{F} \times (\bar{F} \times \bar{F} \times \bar{F}) \times (\bar{F} \times \bar{F} \times \bar{F})\big) \times \mathcal{P}\big(\bar{F} \times \bar{F}\big)$, que muestra que $\mathcal{E}$ es un conjunto. Ordenamos $\mathcal{E}$ parcialmente por

$$(E_1, \leq_{E_1}) \preceq (E_2, \leq_{E_2}) \text{ si y solo si } E_1 \subseteq E_2 \text{ y } \ \leq_{E_2} \cap (E_1 \times E_1) = \leq_{E_1}.$$

Sea $\mathcal{C} \subseteq \mathcal{E}$ una cadena y escribamos $\mathcal{C} = \{(E_i, \leq_{E_i}) : i \in I\}$. Definimos $E_\mathcal{C} := \bigcup_{i\in I} E_i$. Como cada E_i es un subcuerpo de $\overline{F}$ con $F \subseteq E_i$, la unión es de nuevo un subcuerpo de $\overline{F}$ que contiene a F. Definimos una relación de orden $\leq_\mathcal{C}$ en $E_\mathcal{C}$ poniendo

$$x \leq_\mathcal{C} y \quad \text{si y solo si} \quad \text{existe } i \in I \text{ tal que } x, y \in E_i \text{ y } x \leq_{E_i} y.$$

Esta relación está bien definida, pues si $x, y \in E_i \cap E_j$, al ser $\mathcal{C}$ una cadena uno de los cuerpos está contenido en el otro y los órdenes coinciden en la intersección. Como cada $(E_i, \leq_{E_i})$ es un cuerpo ordenado, la compatibilidad del orden se hereda a la unión. En particular, $(E_C, \leq_C) \in \mathcal{E}$ y es una cota superior de $\mathcal{C}$. Por el Lema de Zorn, existe un elemento maximal $(R, \leq_R)$.

Vemos que R es realmente cerrado.

Sea $a \in R$ un elemento positivo que no es un cuadrado en R, y sea P el conjunto de elementos de la forma $\sum_{i=1}^n b_i\,(c_i + d_i\sqrt{a})^2$, con $c_i, d_i \in R$ y b_i en el cono positivo de $(R, \leq_R)$. Entonces P es un cono y es propio porque, si $-1 = \sum_{i=1}^n b_i(c_i + d_i\sqrt{a})^2$, tendríamos que $-1 = \sum_{i=1}^n b_i(c_i^2 + ad_i^2)$ pertenecería al cono positivo de $(R, \leq_R)$, que sabemos que es un cono propio, contradicción. Por el Lema 5.1.7 (2), P está contenido en el cono positivo de un orden de $R[\sqrt{a}]$, que extiende el orden de R. Esto contradice la maximalidad de $(R, \leq_R)$. Por tanto, el cuerpo R tiene un único orden, cuyos elementos positivos son exactamente los cuadrados de R.

Lo anterior implica que, si E es un cuerpo real con $R \subset E \subset \overline{F}$, entonces cualquier orden de E extiende el orden de R, y por tanto $(E, \leq_E) \in \mathcal{E}$. La maximalidad de $(R, \leq_R)$ fuerza entonces $E = R$, luego R es un cuerpo real que no admite extensiones algebraicas reales propias.

Hemos probado que R es realmente cerrado. Por construcción, $F \subseteq R \subseteq \overline{F}$, R es algebraico sobre F, y $\leq_R \cap (F \times F) = \leq$, de modo que $(R, \leq_R)$ es una clausura real de $(F, \leq)$. □

Pasamos ahora a demostrar que toda clausura real de un cuerpo ordenado $(F, \leq)$ es única salvo F-isomorfismo de cuerpos ordenados.[20] Introducimos un par de proposiciones que clarifican los pasos que seguiremos.

Proposición 5.1.18. *Sea R un cuerpo y sean L y L' dos extensiones algebraicas de R. Supongamos que se cumple lo siguiente:*

1. *Para toda subextensión E con $R \subseteq E \subseteq L$ y $R \subseteq E$ finita, existe una subextensión E' con $R \subseteq E' \subseteq L'$ tal que $E \cong_R E'$.*

2. *Recíprocamente, para toda subextensión E' con $R \subseteq E' \subseteq L'$ y $R \subseteq E'$ finita, existe una subextensión E con $R \subseteq E \subseteq L$ tal que $E \cong_R E'$.*

Entonces existe un R-isomorfismo $L \cong_R L'$.

Demostración. Sean $\mathcal{L}$ el lenguaje que amplía el lenguaje de anillos $\{+, \cdot, 0, 1\}$ con dos símbolos de predicado U y V de aridad uno, símbolos de constante c_r para cada $r \in R$, símbolos de constante c_a para cada $a \in L \setminus R$, símbolos de constante $c_{a'}$ para cada $a' \in L' \setminus R$, y un símbolo de relación Γ de aridad dos.

Consideramos $\mathcal{L}$-estructuras cuyo universo está formado por la unión disjunta de dos copias, una de L y otra de L'. Los predicados U y V distinguen estas dos copias. Las operaciones $\{+, \cdot, 0, 1\}$ coinciden con las operaciones de cuerpo habituales al restringirse a cada copia, sin imponerse condiciones fuera de ellas. Sea $\mathcal{L}_U := \{+, \cdot, 0, 1\} \cup \{c_r \mid r \in R\} \cup \{c_a \mid a \in L \setminus R\}$, y análogamente $\mathcal{L}_V := \{+, \cdot, 0, 1\} \cup \{c_r \mid r \in R\} \cup \{c_{a'} \mid a' \in L' \setminus R\}$.

Sea T la $\mathcal{L}$-teoría formada por:

[20] Un F-isomorfismo de cuerpos ordenados es un isomorfismo de cuerpos $f\colon K_1 \to K_2$ entre extensiones de F que fija F y preserva el orden, esto es, cumple que $x \leq_{K_1} y$ si y solo si $f(x) \leq_{K_2} f(y)$ para todo $x, y \in K_1$.

- el diagrama simple de L, considerado como $\mathcal{L}_U$-estructura, cuyas sentencias se interpretan exigiendo que todas las constantes involucradas satisfagan el predicado U;
- el diagrama simple de L', considerado como $\mathcal{L}_V$-estructura, cuyas sentencias se interpretan exigiendo que todas las constantes involucradas satisfagan el predicado V;
- axiomas que expresan que Γ es el grafo de un isomorfismo de cuerpos entre las partes U y V, y que dicho isomorfismo fija R.

Sea $T_0 \subseteq T$ finito. Sean $A \subseteq L$ y $A' \subseteq L'$ los conjuntos finitos de elementos cuyos símbolos de constante c_a y $c_{a'}$ aparecen en T_0, y pongamos $E := R(A) \subseteq L$, $E' := R(A') \subseteq L'$. Por (1) existe una subextensión finita $F' \subseteq L'$ y un R-isomorfismo $\varphi : E \to F'$.

Consideremos en L' la subextensión finita $G' := R(F' \cup E') \subseteq L'$. Por (2) existe una subextensión finita $G \subseteq L$ y un R-isomorfismo $\theta\colon G \to G'$.

Sea $\mathcal{M}$ una $\mathcal{L}$-estructura definida como sigue. El universo de $\mathcal{M}$ es la unión disjunta $G \cup G'$. Para cada $a \in A \subseteq G$, el símbolo de constante c_a se interpreta como a en la copia de G; para cada $a' \in A' \subseteq G'$, $c_{a'}$ se interpreta como a' en la copia de G'. Asimismo, para cada $r \in R$, la constante c_r se interpreta como r en ambas copias. Definimos $U^{\mathcal{M}} = G$ y $V^{\mathcal{M}} = G'$. Finalmente, interpretamos Γ como el subconjunto $\Gamma^{\mathcal{M}} := \{(x, \theta(x)) \mid x \in G\} \subseteq G \times G'$.

Por construcción, la relación $\Gamma^{\mathcal{M}}$ es el grafo de un R-isomorfismo entre G y G', y las interpretaciones fijadas garantizan que todas las sentencias del diagrama simple de L y de L' contenidas en T_0 se satisfacen en $\mathcal{M}$. Por tanto, $\mathcal{M} \models T_0$.

Hemos probado que todo subconjunto finito $T_0 \subseteq T$ es satisfacible.

Por compacidad, la teoría T es satisfacible, de donde se sigue que existe una $\mathcal{L}$-estructura en la que Γ define un R-isomorfismo entre copias de L y L'. □

Observación 5.1.19. En resultados anteriores hemos utilizado el Lema de Zorn explícitamente para construir extensiones máximas. En este caso preferimos usar compacidad, tal como se propone en [7], para mostrar cómo el enfoque modélico recupera el mismo tipo de resultados. Nótese, en cualquier caso, que la compacidad utilizada descansa en el Teorema de completitud, previamente demostrado mediante Zorn.

Antes de seguir, conviene fijar algunas nociones algebraicas básicas como las de extensión simple y separabilidad. Recogemos estas definiciones y hechos en el Apéndice A.2.

Proposición 5.1.20. *Sea R un cuerpo y sean L y L' extensiones algebraicas de R. Son equivalentes:*

1. *Para todo polinomio irreducible $p(X) \in R[X]$, p tiene una raíz en L si y solo si tiene una raíz en L'.*
2. *L y L' contienen, salvo isomorfismo sobre R, las mismas extensiones simples.*

Demostración. Vemos primero que (2) implica (1). Sea $p(X) \in R[X]$ irreducible y supongamos que tiene una raíz $a \in L$. Entonces $R(a) \subseteq L$ es una extensión simple de R. Por hipótesis, existe $b \in L'$ tal que $R(a) \cong_R R(b) \subseteq L'$. En particular, b satisface el mismo polinomio irreducible que a, luego $p(b) = 0$, y p tiene una raíz en L'. La implicación recíproca se obtiene intercambiando los papeles de L y L'.

Vemos ahora que (1) implica (2). Sea $R(\alpha) \subseteq L$ una extensión simple algebraica y sea $p \in R[X]$ el polinomio mínimo de α sobre R. Por hipótesis, p tiene una raíz $\beta \in L'$. La evaluación $f \mapsto f(\beta)$ define un homomorfismo $R[X] \to L'$ cuyo núcleo es (p); por el Primer Teorema de Isomorfía, $R[X]/(p) \cong R(\beta) \subseteq L'$. Identificando $R(\alpha) \cong R[X]/(p)$, se obtiene un R-isomorfismo $R(\alpha) \cong_R R(\beta)$. El mismo argumento vale intercambiando L y L'. □

Observación 5.1.21. Por la Proposición 5.1.18, dos extensiones algebraicas de un cuerpo R son R-isomorfas si y solo si todas sus subextensiones finitas lo son. Por la Observación 5.1.2, todo cuerpo real tiene característica 0, y por tanto toda extensión finita sobre él es simple (Observación A.2.15). En consecuencia, por la proposición anterior, para probar la unicidad de la clausura real de R como extensión algebraica de R basta ver que los mismos polinomios irreducibles de $R[X]$ tienen raíces en cualesquiera dos clausuras reales de R.

En este punto, necesitamos un criterio eficaz para detectar la presencia de raíces en extensiones. En lugar de recurrir a procedimientos clásicos como el algoritmo de Sturm, emplearemos la noción de *traza* y algunas herramientas de K-álgebras (cuyo repaso conciso se recoge en el Apéndice A.3), que permiten cerrar la prueba de forma directa.

Lema 5.1.22 (Lema de Sylvester)**.** *Sea f un polinomio irreducible en $F[X]$ y sea $(K, \leq)$ una extensión realmente cerrada de $(F, \leq)$. El número de raíces de f en K es igual a la signatura de la forma traza de la F-álgebra $F[X]/(f)$.*

Demostración. Consideramos la F-álgebra finita $A = F[X]/(f)$.

Para cada $a \in A$, denotamos por $\ell_a \colon A \to A$ el endomorfismo F-lineal dado por la multiplicación por la izquierda por a. Definimos la *traza* de a sobre F como $tr_F(a) := tr(\ell_a)$, donde $\mathrm{tr}(\ell_a)$ denota la traza usual del endomorfismo F-lineal ℓ_a, es decir, la suma de los elementos de la diagonal de cualquiera de sus matrices asociadas.

Esta aplicación induce una forma bilineal simétrica sobre A, llamada la *forma traza*, definida por $(a, b)_F := tr_F(ab)$.

Como $(F, \leq)$ es un cuerpo real (en particular, de característica 0), y A es un espacio vectorial finito sobre F, la forma traza puede diagonalizarse. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base de A respecto de la cual la matriz de la forma es diagonal, y sean $\lambda_1, \ldots, \lambda_n \in F$ las entradas diagonales correspondientes. Definimos la *signatura* de la forma traza como

$$\mathrm{sign}(A) := \#\{0 < \lambda_i\} - \#\{\lambda_i < 0\}.$$

Por el Teorema de inercia de Sylvester sobre formas bilineales simétricas sobre cuerpos ordenados [11, §4.1], esta cantidad es independiente de la base diagonalizante elegida.

Tensorizando A con K, obtenemos la K-álgebra $A_K := A \otimes_F K \cong K[X]/(f)$. Identificando cada $\alpha_i \in A$ con $\alpha_i \otimes 1 \in A_K$, se tiene

$$(\alpha_i \otimes 1, \alpha_j \otimes 1)_K = \mathrm{tr}_K\big((\alpha_i \otimes 1)(\alpha_j \otimes 1)\big) = \mathrm{tr}_K(\alpha_i\alpha_j \otimes 1) = \mathrm{tr}_F(\alpha_i\alpha_j) = (\alpha_i, \alpha_j)_F = \lambda_i\delta_{ij}.$$

Por tanto, la base $\{\alpha_1, \ldots, \alpha_n\}$ sigue siendo una base diagonalizante para la forma traza de A_K. En particular, la forma traza de A y la de A_K tienen la misma signatura.

Por el Corolario 5.1.15, f se descompone en $K[X]$ como producto de factores lineales y cuadráticos irreducibles, $f = g_1 \cdots g_m$. Como $car_F = 0$, f no tiene raíces múltiples en K, los factores irreducibles $g_1, \ldots, g_m$ son distintos, y por tanto son dos a dos coprimos. Por el Teorema Chino del Resto, existe un isomorfismo de K-álgebras

$$K[X]/(f) \cong K[X]/(g_1) \times \cdots \times K[X]/(g_m).$$

Bajo esta identificación, todo elemento de $K[X]/(f)$ puede verse como una familia $(a_1, \ldots, a_m)$, con $a_i \in K[X]/(g_i)$. Si $a = (a_1, \ldots, a_m)$ y $x = (x_1, \ldots, x_m)$, entonces la multiplicación viene dada por

$$ax = (a_1x_1, \ldots, a_mx_m).$$

El endomorfismo de multiplicación por a es, por tanto, la suma directa de los endomorfismos de multiplicación por a_i en cada uno de los factores. Su traza es la suma de las trazas correspondientes. En consecuencia, la forma traza de $K[X]/(f)$ es la suma directa de las formas traza de las K-álgebras $K[X]/(g_i)$, y su signatura coincide con la suma de las signaturas de dichas formas. Así, basta calcular la signatura asociada a cada polinomio irreducible g_i.

Si g es un factor lineal, entonces existe un isomorfismo de K-álgebras $K[X]/(g) \cong K$, dado por la aplicación $\overline{p(X)} \mapsto p(a)$, donde $g(X) = X - a$. Bajo esta identificación, respecto de la base $\{1\}$ de K como espacio vectorial sobre sí mismo, para cada $x \in K$ la matriz asociada a ℓ_x es (x), y por tanto $\mathrm{tr}_K(x) = x$. La forma traza viene dada por $(x, y) \longmapsto \mathrm{tr}_K(xy) = xy$. Respecto de la base $\{1\}$, la matriz de la forma es (1). Por tanto, la signatura de la forma traza en este caso es 1.

Supongamos ahora que g es irreducible de grado 2, de la forma $(X-b)^2 + c$ con $0 < c$. En $K[X]/(g)$ se tiene $\overline{(X-b)}^2 = \overline{-c}$. Definiendo $i := \frac{1}{\sqrt{c}}\,\overline{(X-b)} \in K[X]/(g)$, se cumple $i^2 = -1$. La aplicación $K[X]/(g) \to K[i]$, $\overline{p(X)} \mapsto p(i)$ define un isomorfismo de K-álgebras. Mediante este isomorfismo, todo elemento de $K[X]/(g)$ puede escribirse de manera única como $x + yi$, con $x, y \in K$.

Para calcular la traza, consideramos el endomorfismo K-lineal $\ell_{x+yi}\colon K[i] \to K[i]$ dado por la multiplicación (por la izquierda) por $x + yi$. Para cualesquiera $x', y' \in K$,

$$\ell_{x+yi}(x' + y'i) = (xx' - yy') + (xy' + x'y)i.$$

Respecto de la base $\{1, i\}$, se tiene $\ell_{x+yi}(1) = x + yi, \quad \ell_{x+yi}(i) = -y + xi$, por lo que la matriz asociada a ℓ_{x+yi} es $\begin{pmatrix} x & -y \\ y & x \end{pmatrix}$. En consecuencia, la traza de dicho endomorfismo es $2x$, y por definición $\mathrm{tr}_K(x+yi) = 2x$. La forma traza es $(x+yi,\ x'+y'i) \longmapsto \mathrm{tr}_K\left((x+yi)(x'+y'i)\right) = 2(xx'-yy')$. Respecto de la base $\{1, i\}$, la matriz de la forma traza viene dada por $\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$. Por tanto, la signatura de la forma traza en este caso es 0.

Hemos probado que la signatura de la forma traza de $A_K = A \otimes_F K \cong K[X]/(f)$, la cual coincide con la de A, es igual al número de factores lineales en la descomposición de f en $K[X]$. En particular, coincide con el número de raíces de f en K. □

Corolario 5.1.23. *Sea $(F, \leq)$ un cuerpo ordenado. Entonces la clausura real de $(F, \leq)$ es única salvo F-isomorfismo de cuerpos ordenados.*

Demostración. Por el Lema de Sylvester, para todo polinomio irreducible $f \in F[X]$, el número de raíces de f en una clausura real de F coincide con la signatura de la forma traza asociada, y en particular es independiente de la clausura real considerada. En consecuencia, un polinomio irreducible de $F[X]$ tiene raíz en una clausura real de F si y solo si la tiene en cualquier otra.

Además, el orden de un cuerpo realmente cerrado es único y queda caracterizado por su cono positivo, que coincide con el conjunto de los cuadrados. Como los cuadrados se preservan por homomorfismos de cuerpos, todo F-isomorfismo entre clausuras reales preserva el orden.

El resultado se deduce entonces de la Observación 5.1.21. □

Observación 5.1.24. La unicidad de la clausura real es más rígida que la unicidad de la clausura algebraica: mientras que en el caso algebraicamente cerrado los modelos se clasifican (una vez fijada la característica) por el grado de trascendencia sobre el subcuerpo primo, en el caso de los cuerpos realmente cerrados, cuya característica es necesariamente cero, la clasificación de los modelos requiere, además del grado de trascendencia, tener en cuenta el orden subyacente.

Extendemos finalmente estos resultados al caso de los subanillos ordenados de un cuerpo ordenado (o dominios de integridad ordenados), ya que son precisamente las subestructuras de los modelos de RCF.

Proposición 5.1.25. *Sea A un dominio de integridad ordenado mediante una relación $<$ compatible con las operaciones. Entonces el orden se puede extender a su cuerpo de fracciones* $\mathrm{Frac}(A)$ *de forma única definiendo* $0 < \frac{a}{b}$ *si y solo si* $0 < ab$, *para todo* $a, b \in A$ *con* $b \neq 0$.

Idea de la demostración. La definición no depende del representante: si $\frac{a}{b} = \frac{c}{d}$, entonces $ad = bc$, lo que implica que a y d tienen el mismo signo si y solo si b y c lo tienen; de aquí se deduce que a y b tienen el mismo signo si y solo si c y d lo tienen, es decir, $0 < ab$ si y solo si $0 < cd$.

Las propiedades del orden en A permiten comprobar que la relación definida es un orden total compatible con la suma y el producto en $\mathrm{Frac}(A)$, y que extiende el orden de A: en efecto, para $a, b \in A$ se tiene $a < b$ si y solo si $0 < b - a$ si y solo si $0 < \frac{b-a}{1}$ si y solo si $\frac{a}{1} < \frac{b}{1}$, donde la última equivalencia se obtiene de la compatibilidad con la suma. □

Observación 5.1.26. Sea $(A, \leq)$ un subanillo ordenado de un cuerpo realmente cerrado $(K, \leq)$, y sea $F := \mathrm{Frac}(A) \subseteq K$ su cuerpo de fracciones, provisto del orden inducido por el de A. Definimos $A_K^{\mathrm{alg}} := \{\, b \in K \mid b \text{ es algebraico sobre } F \,\}$. Entonces $(A_K^{\mathrm{alg}}, \leq)$ es una clausura real de $(F, \leq)$, contenida en K. En particular, es única salvo F-isomorfismo de cuerpos ordenados, y por tanto única salvo A-isomorfismo de cuerpos ordenados.

En efecto, que $F \subseteq A_K^{\mathrm{alg}}$ es una extensión algebraica es inmediato por definición. Como $A_K^{\mathrm{alg}} \subseteq K$ y K es un cuerpo ordenado, el orden de K se restringe a un orden en A_K^{alg}, de modo que A_K^{alg} es un cuerpo real cuyo orden extiende a su vez el de F.

Vemos que A_K^{alg} es realmente cerrado verificando las dos propiedades características del Teorema 5.1.13 (2). Sea $p(X) \in A_K^{\mathrm{alg}}[X]$ un polinomio de grado impar. Como K es realmente cerrado, existe $\alpha \in K$ tal que $p(\alpha) = 0$.En particular, α es algebraico sobre A_K^{alg}. Como por definición $F \subseteq A_K^{\mathrm{alg}}$ es algebraica, se sigue que α es algebraico sobre F, y por tanto $\alpha \in A_K^{\mathrm{alg}}$. Por otro lado, sea $a \in A_K^{\mathrm{alg}}$ con $0 < a$. Como K es realmente cerrado, existe $\beta \in K$ tal que $\beta^2 = a$. Entonces β es algebraico sobre A_K^{alg}, al ser raíz de $X^2 - a \in A_K^{\mathrm{alg}}[X]$, y nuevamente, como $F \subseteq A_K^{\mathrm{alg}}$ es algebraica, se sigue que $\beta \in A_K^{\mathrm{alg}}$.

5.2. Eliminación de cuantificadores en RCF

Entramos en el estudio de la teoría de los cuerpos realmente cerrados. Comenzamos por formalizarla en el marco de la lógica de primer orden. Seguimos [7].

Sea $\mathcal{L}_{\mathrm{anillo}} = \{+, \cdot, 0, 1\}$ el lenguaje de anillos, y sea T_{cuerpo} la teoría de cuerpos. Consideramos el lenguaje de anillos ordenados

$$\mathcal{L}_{\mathrm{ord}} = \mathcal{L}_{\mathrm{anillo}} \cup \{\leq\}.$$

Sea $T_{\mathrm{cuerpo}}^{ord}$ la $\mathcal{L}_{\mathrm{ord}}$-teoría obtenida añadiendo a T_{cuerpo} los axiomas que expresan que $\leq$ es un orden total compatible con las operaciones del cuerpo, es decir,

- $\forall x\,(x \leq x)$ (reflexividad)
- $\forall x\,\forall y\,\big((x \leq y \wedge y \leq x) \to x \doteq y\big)$ (antisimetría)
- $\forall x\,\forall y\,\forall z\,\big((x \leq y \wedge y \leq z) \to x \leq z\big)$ (transitividad)
- $\forall x\,\forall y\,\big(x \leq y \vee y \leq x\big)$ (totalidad)
- $\forall x\,\forall y\,\forall z\,\big(x \leq y \to x + z \leq y + z\big)$ (compatibilidad con la suma)

- $\forall x\,\forall y\,\big((0 \le x \wedge 0 \le y) \to 0 \le x \cdot y\big)$ (compatibilidad con el producto)

La *teoría de los cuerpos realmente cerrados*, que denotaremos RCF, se obtiene añadiendo a T^{ord}_{cuerpo} axiomas que expresan que todo polinomio de grado impar tiene una raíz y que todo elemento positivo es un cuadrado, es decir,

- Para cada $n \ge 0$, añadimos $\forall a_0, \dots, a_{2n}\,\exists x\,\big(x^{2n+1} + a_{2n}x^{2n} + \cdots + a_0 \doteq 0\big)$.
- $\forall x\,\big(0 \le x \to \exists y\,(y^2 \doteq x)\big)$.

Finalmente, definimos $x < y$ si y solo si $x \le y \wedge x \ne y$. Actuaremos como si el símbolo $<$ formara parte del lenguaje, entendiéndolo siempre como abreviatura de la fórmula anterior.

Teorema 5.2.1 (Tarski-Seidenberg)**.** RCF *tiene eliminación de cuantificadores.*

Demostración. Usaremos el criterio de eliminación de cuantificadores del Teorema 3.0.6. Sean $(K_1, \le)$ y $(K_2, \le)$ dos modelos de RCF que contienen una subestructura común $(A, \le)$. Sea $\varphi(x_0, x_1, \dots, x_n)$ una fórmula sin cuantificadores, sean parámetros $\bar{a} \in A$, y supongamos que existe $b_1 \in K_1$ tal que $K_1 \models \varphi[b_1, \bar{a}]$. Mostraremos entonces que $(K_2, \le) \models \exists x\,\varphi[x, \bar{a}]$.

Como $(A, \le)$ es una subestructura de un cuerpo ordenado, es un dominio de integridad ordenado. Para $i = 1, 2$, sea $F_i := \operatorname{Frac}(A) \subseteq K_i$ el cuerpo de fracciones correspondiente, provisto del único orden que extiende el de A. Por la unicidad del cuerpo de fracciones, existe un único A-isomorfismo de cuerpos $f\colon F_1 \to F_2$, y por la unicidad de la extensión del orden, dicho isomorfismo preserva el orden. En consecuencia, f es un A-isomorfismo de cuerpos ordenados.

Aplicando la Observación 5.1.26 a cada K_i, obtenemos para cada $i = 1, 2$ una clausura real $G_i := (A^{\text{alg}}_{K_i}, \le)$ de $(F_i, \le)$, contenida en K_i. Por la unicidad de la clausura real, el isomorfismo f se extiende de manera única a un A-isomorfismo de cuerpos ordenados $g\colon (G_1, \le) \to (G_2, \le)$.

Sea $b_1 \in K_1$ tal que $(K_1, \le) \models \varphi[b_1, \bar{a}]$. Distinguimos dos casos.

Si $b_1 \in G_1$, como g es un A-isomorfismo, $(G_1, \le) \models \varphi[b_1, \bar{a}]$ si y solo si $(G_2, \le) \models \varphi[g(b_1), \bar{a}]$. Dado que $(G_2, \le)$ es una subestructura de $(K_2, \le)$ y φ es una fórmula libre de cuantificadores, por la Observación 2.2.3 se sigue que $(K_2, \le) \models \varphi[g(b_1), \bar{a}]$.

Si $b_1 \notin G_1$, entonces b_1 es trascendente sobre G_1. En efecto, como $F_1 \subseteq G_1$ es algebraica, si b_1 fuese algebraico sobre G_1 lo sería sobre F_1 y pertenecería a G_1.

Definimos $G_1^- := \{a \in G_1 : a < b_1\}$ y $G_1^+ := \{a \in G_1 : b_1 < a\}$, y consideramos sus imágenes $\alpha := g(G_1^-)$ y $\beta := g(G_1^+)$ en G_2. Se tiene que $\alpha < \beta$, y ambos conjuntos son no vacíos.

Sea el lenguaje obtenido añadiendo a $\mathcal{L}_{\text{ord}}$ una constante c_z para cada $z \in K_2$, y consideramos el diagrama completo $D((K_2, \le))$ de $(K_2, \le)$. Sea $\Sigma(x) := \{\, c_a < x : a \in \alpha \,\} \cup \{\, x < c_d : d \in \beta \,\}$. Tomamos $\Sigma_0(x) \subseteq \Sigma(x)$ un subconjunto finito. Entonces existen $a_1, \dots, a_n \in \alpha$ y $d_1, \dots, d_m \in \beta$ tales que $\Sigma_0(x) = \{c_{a_1} < x, \dots, c_{a_n} < x,\ x < c_{d_1}, \dots, x < c_{d_m}\}$. Esta familia es equivalente a la doble desigualdad $c_{\max\{a_1,\dots,a_n\}} < x < c_{\min\{d_1,\dots,d_m\}}$. Como $\alpha < \beta$, se tiene $\max\{a_i\} < \min\{d_j\}$. Por ejemplo, tomando $x_0 := \frac{\max\{a_i\}+\min\{d_j\}}{2} \in K_2$, la expansión canónica de $(K_2, \le)$ al lenguaje ampliado satisface todas las fórmulas de $\Sigma_0(c_{x_0})$.

De este modo, hemos probado que dicha expansión satisface toda subfamilia finita de la teoría $T := D((K_2, \le)) \cup \Sigma(x)$. Por compacidad, existe un modelo $(K_2', \le)$ en el lenguaje ampliado que satisface T. Al tomar el reducto de $(K_2', \le)$ al lenguaje $\mathcal{L}_{ord}$, obtenemos una $\mathcal{L}_{\text{ord}}$-estructura que contiene una copia isomorfa de $(K_2, \le)$ como subestructura elemental (Proposición 2.2.5); identificando ambas copias, podemos considerar que $(K_2, \le) \preceq (K_2', \le)|_{\mathcal{L}_{\text{ord}}}$, y existe un elemento $b_2 \in K_2'$ tal que $\alpha < b_2 < \beta$.

Si b_2 perteneciera a G_2, existiría $d \in G_1$ tal que $b_2 = g(d)$. Aplicando g^{-1} a las desigualdades anteriores obtendríamos $G_1^- < d < G_1^+$, que fuerza que $d = b_1$, de donde $b_1 \in G_1$, contradicción.

Así, $b_2 \notin G_2$. Un razonamiento análogo al de G_1 muestra que b_2 es trascendente sobre G_2.

Como b_1 y b_2 son trascendentes sobre G_1 y G_2, respectivamente, por el Teorema 4.1.11 $g\colon G_1 \to G_2$ se extiende a un A-isomorfismo de cuerpos $h\colon G_1(b_1) \to G_2(b_2)$, que envía b_1 a b_2.

Vamos a probar que h preserva el orden. Para ello, basta probar que preserva el orden para todos los elementos de la forma $p(b_1)$ con $p(X) \in G_1[X]$.

Por el Corolario 5.1.15, existe una descomposición de $p(X)$ en $G_1[X]$ de la forma

$$p(X) = \varepsilon \prod_i (X - a_i) \prod_j \big((X - c_j)^2 + d_j\big), \text{con } 0 < d_j.$$

Los factores cuadráticos son siempre positivos, por lo que el signo de $p(b_1)$ depende únicamente de ε y de la posición de b_1 respecto a los a_i.

El factor ε pertenece a G_1, y, como h extiende a g, su signo se preserva. Por otro lado, para todo i, se cumple que $b_1 < a_i$ si y solo si $b_2 < h(a_i)$, de donde $0 < p(b_1)$ si y solo si $0 < \widehat{h}(p)(b_2)$, donde $\widehat{h}\colon G_1[X] \to G_2[X]$ denota la extensión natural de h a polinomios.

Así, h preserva el orden y es por tanto un A-isomorfismo de cuerpos ordenados.

De este modo, se tiene la cadena de equivalencias

$$\begin{aligned}(K_1, \leq) \models \varphi[b_1, \bar{a}] &\iff (G_1(b_1), \leq) \models \varphi[b_1, \bar{a}] \iff (G_2(b_2), \leq) \models \varphi[b_2, \bar{a}] \\ &\implies (K_2', \leq) \models \varphi[b_2, \bar{a}] \implies (K_2, \leq) \models \exists x\, \varphi[x, \bar{a}].\end{aligned}$$

□

Corolario 5.2.2. RCF *es completa.*

Demostración. Sean $(K_1, \leq)$ y $(K_2, \leq)$ dos modelos de RCF. Como $\mathrm{car}(K_i) = 0$, cada K_i contiene el subanillo generado por 1 isomorfo a $\mathbb{Z}$, y su subcuerpo primo K_{0i}, isomorfo a $\mathbb{Q}$. El orden sobre dicho subanillo queda determinado por $0 < 1$, luego el orden inducido en cada K_{0i} es el único orden en $\mathbb{Q}$. Identificamos $(K_{01}, \leq)$ y $(K_{02}, \leq)$ mediante un isomorfismo de cuerpos ordenados, y consideramos que ambos modelos comparten una copia isomorfa de $(\mathbb{Q}, \leq)$.

Por la eliminación de cuantificadores y la Proposición 3.0.7 (1), se tiene que $(K_1, \leq) \equiv (K_2, \leq)$. Por el Corolario A.1.15, concluimos que RCF es completa. □

Vamos a relacionar el Teorema de Tarski–Seidenberg con algunos resultados fundamentales de geometría algebraica real.

Definición 5.2.3. Desde el punto de vista de la geometría algebraica real, un subconjunto $S \subseteq K^n$ se dice *semialgebraico* si puede obtenerse como combinación booleana finita de conjuntos de la forma $\{x \in K^n \mid g(x) \leq 0\}$, con $g \in K[X_1, \ldots, X_n]$, donde $(K, \leq)$ es un cuerpo ordenado.

El Teorema de Tarski–Seidenberg admite la siguiente caracterización semántica.

Corolario 5.2.4. *Sea $(K, \leq) \models$ RCF. Entonces, en $(K, \leq)$ los conjuntos definibles (con parámetros) coinciden exactamente con los semialgebraicos.*

Observación 5.2.5. En el caso de los cuerpos algebraicamente cerrados, la eliminación de cuantificadores permite obtener de manera directa el Nullstellensatz clásico. En el contexto de la geometría algebraica real, en cambio, resultados como el *Nullstellensatz real* y el *Positivstellensatz* ponen de manifiesto que la información geométrica relevante no queda determinada únicamente por los ideales, sino que interviene de forma esencial la estructura de orden del cuerpo base. En este marco, las sumas de cuadrados constituyen el objeto algebraico fundamental para describir nociones de positividad. Para una exposición detallada, véase [12, §2.3].

El decimoséptimo problema de Hilbert

En particular, como consecuencia de la eliminación de cuantificadores en RCF, obtenemos el siguiente resultado, que resuelve el decimoséptimo problema de Hilbert.

Corolario 5.2.6 (Decimoséptimo problema de Hilbert)**.** *Sea $(K, \leq)$ un cuerpo realmente cerrado y sea $f \in K[X_1, \ldots, X_n]$. Entonces f es suma de cuadrados de funciones racionales, es decir,*

$$f = g_1^2 + \cdots + g_m^2 \text{ con } g_i \in K(X_1, \ldots, X_n),$$

si y solo si

$$0 \leq f(a_1, \ldots, a_n) \text{ para todo } a_1, \ldots, a_n \in K.$$

Demostración. Si f es suma de cuadrados en $K(X_1, \ldots, X_n)$, entonces no puede tomar valores negativos en ningún cuerpo ordenado.

Recíprocamente, supongamos que f no es suma de cuadrados en $K(X_1, \ldots, X_n)$. Por la Proposición 5.1.8, existe un orden en $K(X_1, \ldots, X_n)$ respecto del cual $f < 0$. Sea L una clausura real de $K(X_1, \ldots, X_n)$; dicho orden se extiende a L, y en consecuencia la sentencia

$$\exists x_1, \ldots, x_n \, (f(x_1, \ldots, x_n) < 0)$$

es verdadera en L.

Como K y L son cuerpos realmente cerrados y K es una subestructura de L, por la eliminación de cuantificadores en RCF y la Proposición 3.0.7 (2) se tiene $K \preceq L$. Por tanto, la sentencia anterior es verdadera en K, contradicción. □

Declaración sobre el uso de IA

En la elaboración del presente trabajo se ha utilizado inteligencia artificial generativa (ChatGPT, versiones 4.5–5.2) como apoyo en tareas de redacción, reformulación lingüística y clarificación expositiva, especialmente en la revisión de borradores de la introducción, transiciones entre secciones y mejora de la presentación de algunas demostraciones.

El contenido matemático, incluyendo definiciones, enunciados, pruebas y decisiones estructurales, ha sido desarrollado, comprendido y verificado íntegramente por el autor.

Referencias

[1] D. Palacín. *Apuntes de Lógica Matemática*. UCM, 2023. Disponible en https://www.ucm.es/dpalacin/file/apunteslm/.

[2] M. Hils y F. Loeser. *A First Journey through Logic*. Student Mathematical Library, vol. 89. AMS, Providence, RI, 2019.

[3] A. Gavilanes. *Apuntes de Lógica Matemática*. UCM, 2024.

[4] D. Palacín. *Apuntes de Estructuras Algebraicas*. UCM, 2023.

[5] P. D. González. *Apuntes de Ecuaciones Algebraicas*. UCM, 2024.

[6] T. W. Hungerford. *Algebra*. Graduate Texts in Mathematics, vol. 73. Springer, 2012.

[7] K. Tent y M. Ziegler. *A Course in Model Theory*. Cambridge University Press, 2012.

[8] J. Bochnak, M. Coste y M. F. Roy. *Real Algebraic Geometry*. Springer, 1998.

[9] M. E. Alonso. *Apuntes de Álgebra Conmutativa*. UCM, 2025.

[10] M. Atiyah y I. G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley, 1969.

[11] S. Lang. *Algebra*. Graduate Texts in Mathematics, vol. 211. Springer, 2002.

[12] J. F. Fernando y J. M. Gamboa. *Real Algebra from Hilbert's 17th Problem*. Lecture notes, 2012. Disponible en https://www.mat.ucm.es/~josefer/articulos/rgh17.pdf.

[13] A. Tarski. *A Decision Method for Elementary Algebra and Geometry*. University of California Press, 1951.

Apéndice

A.1. El método de Henkin para la completitud

A continuación se presenta una demostración del Teorema 2.1.4, siguiendo el enfoque propuesto por Leon Henkin en 1949 (una simplificación de la prueba original de Gödel). Una exposición más detallada puede encontrarse en [1].

La demostración clásica del Teorema de completitud (y de otros metateoremas fundamentales) se desarrolla en el marco de un sistema de estilo Hilbert para la lógica de primer orden, esto es, el sistema deductivo introducido previamente con sus axiomas y reglas de inferencia. Existen otros enfoques deductivos, como la *deducción natural*, donde no se postulan axiomas, solo reglas de inferencia.

Una *teoría de Henkin* (respecto de un lenguaje $\mathcal{L}$) es una $\mathcal{L}$-teoría T en la que, para toda $\mathcal{L}$-fórmula de la forma $\exists x\, \phi(x)$, existe un símbolo constante c (llamado *constante de Henkin*) en $\mathcal{L}$ tal que el siguiente *axioma de Henkin* pertenece a T: $(\exists x\, \phi(x)) \to \phi(c))$.

Introducimos algunos resultados preliminares:

Lema A.1.1. (Lema de deducción). *Sean χ una $\mathcal{L}$-sentencia, T una $\mathcal{L}$-teoría y ψ una $\mathcal{L}$-fórmula. Entonces*

$$T \cup \{\chi\} \vdash_{\mathcal{L}} \psi \quad \textit{si y solo si} \quad T \vdash_{\mathcal{L}} (\chi \to \psi).$$

Observación A.1.2. A partir de este lema, es fácil ver, por inducción en n, que para todo $n \geq 1$ se tiene: $T \cup \{\gamma_1, \ldots, \gamma_n\} \vdash_{\mathcal{L}} \varphi$ implica $T \vdash_{\mathcal{L}} (\gamma_1 \wedge \cdots \wedge \gamma_n) \to \varphi$.

También se demuestra el siguiente resultado:

Lema A.1.3. *Sea T una $\mathcal{L}$-teoría y χ una $\mathcal{L}$-sentencia. Entonces,*

$$T \vdash_{\mathcal{L}} \chi \quad \textit{si y solo si} \quad T \cup \{\neg\chi\} \textit{ es inconsistente.}$$

La idea general de la demostración del Teorema de completitud es la siguiente: si φ es consecuencia lógica de T pero no es demostrable a partir de T, consideramos la teoría $T \cup \{\neg\varphi\}$. Como por hipótesis $T \nvdash_{\mathcal{L}} \varphi$, por el lema anterior la teoría $T \cup \{\neg\varphi\}$ es consistente, y nuestro objetivo será construir un modelo de esta teoría (en particular, un modelo de T que haga φ falsa), llegando a una contradicción. Para lograr esto partimos de $T \cup \{\neg\varphi\}$ y le añadimos axiomas de Henkin para todas las fórmulas existenciales, generando una teoría de Henkin T^+; luego, mediante un proceso de extensión basado en el Lema de Zorn (Lema A.4.2), obtenemos una teoría de Henkin completa T^* que contiene a T^+. Finalmente, vemos que es posible construir un modelo para toda teoría de Henkin completa, en particular para T^* (y por ende para T y $\neg\varphi$), alcanzando la contradicción deseada.

Por tanto, en realidad la demostración del Teorema de completitud surgirá como consecuencia de este resultado equivalente:[21]

Teorema A.1.4 (Teorema de Henkin)**.** *Una $\mathcal{L}$-teoría T es consistente si y solo si tiene un modelo.*

[21] El Teorema de Henkin se sigue del Teorema de completitud. Supongamos que, para toda fórmula φ, se tiene $T \models \varphi$ si y solo si $T \vdash \varphi$. Aplicándolo a $\bot$ y tomando contrapositivos, se obtiene $T \nvdash \bot$ si y solo si $T \not\models \bot$. Por definición de satisfacibilidad, se tiene que $T \models \bot$ si y solo si toda estructura que es modelo de T satisface $\bot$. Como $\bot$ no se satisface en ninguna estructura, esta condición se cumple cuando no existen modelos de T. Por tanto, $T \not\models \bot$ si y solo si T tiene un modelo. En consecuencia, T es consistente si y solo si tiene un modelo.

Paso 1: Construcción de una teoría de Henkin T^+.
La adición de constantes no altera la fuerza deductiva de la teoría en el lenguaje original. La prueba de este resultado corresponde al Lema 2.3.19 de [1].

Lema A.1.5. (Simulación de constantes por variables). *Sean T una $\mathcal{L}$-teoría, φ una $\mathcal{L}$-fórmula, c un símbolo de constante con $c \notin \mathcal{L}$. Si x es una variable, entonces:*

$$T \vdash_{\mathcal{L}} \varphi(x) \quad \textit{si y solo si} \quad T \vdash_{\mathcal{L}\cup\{c\}} \varphi(c).$$

Observación A.1.6. Sea C un conjunto de símbolos de constante tales que $\mathcal{L} \cap C = \emptyset$. Entonces $T \vdash_{\mathcal{L}} \psi$ si y solo si $T \vdash_{\mathcal{L}\cup C} \psi$.

Esto se sigue directamente del lema. Como toda prueba en $\mathcal{L} \cup C$ utiliza únicamente un número finito de símbolos de C, podemos suponer que C es finito y concluir por inducción sobre la cardinalidad de C.

Ahora, vemos que agregar un solo nuevo símbolo constante con su correspondiente axioma de Henkin no genera inconsistencias. Más precisamente:

Lema A.1.7. (Lema de Henkin). *Sea c un símbolo de constante* nuevo *(que no aparece en $\mathcal{L}$) y sea $\varphi(x)$ una $\mathcal{L}-$fórmula (con $x \in lib(\varphi)$). Consideremos la teoría ampliada*

$$T' = T \cup \{ (\exists x\, \varphi(x) \to \varphi(c)) \}.$$

Afirmamos que T' es consistente.

Demostración. Supongamos lo contrario. Entonces, la $\mathcal{L} \cup \{c\}$-fórmula $\neg(\exists x\, \varphi(x) \to \varphi(c))$ es demostrable en T por el Lema A.1.3. Como $\neg(\exists x\, \varphi(x) \to \varphi(c)) = \big(\neg(\exists x\, \varphi \to \varphi)\big)(c)$, el lema anterior implica $T \vdash_{\mathcal{L}} \neg(\exists x\, \varphi \to \varphi)$, luego $T \vdash_{\mathcal{L}} (\exists x\, \varphi \wedge \neg\varphi)$[22], y por la $\wedge-$ *regla* $T \vdash_{\mathcal{L}} \exists x\, \varphi$ y $T \vdash_{\mathcal{L}} \neg\varphi$. Con $\theta = \forall x\, x \doteq x$, claramente $T \cup \{\theta\} \vdash_{\mathcal{L}} \neg\varphi$, luego $T \vdash_{\mathcal{L}} \theta \to \neg\varphi$ por el Lema de deducción, de donde $T \vdash_{\mathcal{L}} (\varphi \to \neg\theta)$.[23] Como $\neg\theta$ es una $\mathcal{L}$-sentencia, por $\exists$-introducción deducimos $T \vdash_{\mathcal{L}} (\exists x\, \varphi \to \neg\theta)$, y por tanto $T \vdash_{\mathcal{L}} \neg\theta$ por MP. Sin embargo, esto implica que T es inconsistente (θ es demostrable), contradicción. □

Teorema A.1.8. *Cualquier $\mathcal{L}$-teoría T consistente está contenida en una $\mathcal{L} \cup C$-teoría de Henkin T^+ consistente, donde C es un conjunto de símbolos de constante tal que $\mathcal{L} \cap C = \emptyset$.*

Demostración. Partimos de la teoría original T en el lenguaje $\mathcal{L} = \mathcal{L}_0$ y enumeramos todas las fórmulas $\varphi_i(x)$ con variable libre x; a cada una le asignamos una constante nueva c_i y añadimos el correspondiente axioma de Henkin $(\exists x\, \varphi_i(x) \to \varphi_i(c_i))$, de modo que, por el lema anterior, cada extensión $T_{0,i}$ sigue siendo consistente en cada paso, y podemos tomar su unión para obtener una nueva teoría consistente T_1 en el lenguaje ampliado $\mathcal{L}_1$. En este nuevo lenguaje aparecen nuevas fórmulas existenciales, por lo que repetimos el procedimiento y obtenemos T_2. De manera análoga, iteramos el proceso en cada ampliación sucesiva, construyendo así

$$T_1 = \bigcup_i T_{0,i}, \quad T_2 = \bigcup_j T_{1,j}, \quad \ldots, \quad T_n = \bigcup_k T_{n-1,k},$$

cada una consistente en su lenguaje $\mathcal{L}_n$. Finalmente definimos

$$T^+ = \bigcup_{n\in\mathbb{N}} T_n \quad \text{en el lenguaje} \quad \mathcal{L}^+ = \bigcup_{n\in\mathbb{N}} \mathcal{L}_n,$$

[22] $\neg\big(\exists x\, A \to A\big) \to \big(\exists x\, A \wedge \neg A\big)$ es demostrable, y aplicamos MP.
[23] $(A \to \neg B) \to (B \to \neg A)$ es demostrable, y aplicamos MP.

y vemos que toda contradicción finita habría aparecido ya en algún T_n, luego T^+ es consistente y, al contener para cada fórmula existencial su axioma de Henkin, resulta ser una teoría de Henkin que extiende a T. □

Paso 2: Extensión a una teoría de Henkin completa T^*. El siguiente paso es usar el *Lema de Lindenbaum* (que emplea Zorn) para extender T^+ a una teoría de Henkin completa sin perder consistencia.

Decimos que T es *maximalmente consistente* si es consistente y para cualquier $\mathcal{L}$-teoría T' con $T \subseteq T'$ se tiene que T' es inconsistente.

Lema A.1.9. *Toda $\mathcal{L}$-teoría maximalmente consistente es completa.*

Demostración. Sea T una teoría maximalmente consistente y χ una $\mathcal{L}$-sentencia. Si $T \nvdash_{\mathcal{L}} \chi$, entonces $T \cup \{\neg\chi\}$ es consistente por el Lema A.1.3 y por maximalidad $T = T \cup \{\neg\chi\}$, de donde $T \vdash_{\mathcal{L}} \neg\chi$. □

Observación A.1.10. Para cualquier $\mathcal{L}$-teoría T y toda fórmula φ,

$$T \vdash_{\mathcal{L}} \varphi \quad \text{si y solo si} \quad \text{existe un subconjunto finito } T_0 \subseteq T \text{ tal que } T_0 \vdash_{\mathcal{L}} \varphi.$$

Basta tomar T_0 como el conjunto de las sentencias de T empleadas en la demostración de φ. La otra dirección es obvia.

Lema A.1.11 (Lema de Lindenbaum)**.** *Sea T_c una $\mathcal{L}$-teoría consistente. Entonces existe una $\mathcal{L}$-teoría maximalmente consistente T_{max} que contiene a T_c. En particular, T_{max} es completa.*

Demostración. Consideremos el conjunto $\mathscr{F} = \{T : T_c \subset T,\ T \text{ consistente}\}$, parcialmente ordenado por inclusión. Dada una cadena $(T_i)_{i\in I}$ en $\mathscr{F}$, su unión $\bigcup_{i\in I} T_i$ contiene a T_c y, por la observación anterior, sigue siendo consistente. Por el Lema de Zorn, $\mathscr{F}$ tiene un elemento maximal T_{max}, que es una teoría maximalmente consistente. Por el lema anterior, T_{max} es completa. □

Por supuesto, toda extensión de una teoría de Henkin en el mismo lenguaje sigue siendo una teoría de Henkin. Extendemos T^+ a T^*.

Paso 3: Construcción de un modelo para T^*. Antes, introducimos un par de resultados:

Lema A.1.12 (Aserto I)**.** *Sea $\varphi(x_1, \ldots, x_n)$ una $\mathcal{L}$-fórmula sin cuantificadores y sean $t_1, \ldots, t_n$ $\mathcal{L}$-términos sin variables libres. Si $T \vdash_{\mathcal{L}} \forall x_1 \cdots x_n\, \varphi(x_1, \ldots, x_n)$, entonces $T \vdash_{\mathcal{L}} \varphi(t_1, \ldots, t_n)$.*

Lema A.1.13 (Aserto II)**.** *Sea T una $\mathcal{L}$-teoría de Henkin. Para cada símbolo de función f de $\mathcal{L}$ de aridad n y para cualesquiera $c_1, \ldots, c_n \in C$, existe $c \in C$ tal que $T \vdash_{\mathcal{L}} f(c_1, \ldots, c_n) \doteq c$.*

Recordamos también los axiomas de la igualdad para los símbolos de función y de relación:

$$\forall x_1, \ldots, x_{2n} \left(\bigwedge_{i=1}^{n} x_i \doteq x_{n+i} \ \rightarrow\ f(x_1, \ldots, x_n) \doteq f(x_{n+1}, \ldots, x_{2n}) \right), \text{ donde } f \in F_n;$$

$$\forall x_1, \ldots, x_{2n} \left(\left(\bigwedge_{i=1}^{n} x_i \doteq x_{n+i} \wedge R(x_1, \ldots, x_n) \right) \ \rightarrow\ R(x_{n+1}, \ldots, x_{2n}) \right), \text{ donde } R \in R_n.$$

Teorema A.1.14. *Cualquier $\mathcal{L}$-teoría de Henkin* completa T^* *tiene un modelo cuyo universo está formado únicamente por las interpretaciones de los símbolos de constante del lenguaje. Además, este modelo es único salvo isomorfía.*

Demostración. Existencia. Sea C el conjunto de símbolos de constante del lenguaje de T^*. Definimos una relación $\sim$ en C por $c_1 \sim c_2$ si y solo si $T^* \vdash_{\mathcal{L}} c_1 \doteq c_2$.

i) A partir del *Aserto I*, es fácil ver que $\sim$ es una relación de equivalencia.

ii) Denotamos por $\bar{c}$ la clase de equivalencia de $c \in C$. Sea $A = C/\sim$ el conjunto de clases. Queremos dotar a A de la estructura de una $\mathcal{L}$-estructura que sea modelo de T^*.

Definimos la $\mathcal{L}$-estructura $\mathcal{A}$ como sigue: Para cada símbolo de constante c, $c^{\mathcal{A}} = \bar{c}$. Para cada símbolo de función f de aridad n, $f^{\mathcal{A}}(\bar{c}_1, \ldots, \bar{c}_n) = \bar{c}$ con $c \in C$ tal que $T^* \vdash_{\mathcal{L}} f(c_1, \ldots, c_n) \doteq c$ (la existencia está garantizada por el *Aserto II*). Para cada símbolo de relación R de aridad m, $(\bar{c}_1, \ldots, \bar{c}_m) \in R^{\mathcal{A}}$ si y solo si $T^* \vdash_{\mathcal{L}} R(c_1, \ldots, c_m)$.

Las interpretaciones no dependen de los representantes elegidos: si $c_i \sim d_i$ (i.e. $T^* \vdash_{\mathcal{L}} c_i \doteq d_i$ para todo i), por los axiomas de la igualdad y el *Aserto I* $T^* \vdash_{\mathcal{L}} f(c_1, \ldots, c_n) \doteq f(d_1, \ldots, d_n)$, de modo que las clases coinciden. Análogamente, de $T^* \vdash_{\mathcal{L}} c_i \doteq d_i$ y $T^* \vdash_{\mathcal{L}} R(c_1, \ldots, c_m)$ se deduce $T^* \vdash_{\mathcal{L}} R(d_1, \ldots, d_m)$.

Antes de demostrar que es un modelo para T^*, vemos que para todo término t sin variables libres y toda constante c,

$$t^{\mathcal{A}} = \bar{c} \quad \text{si y solo si} \quad T^* \vdash_{\mathcal{L}} t \doteq c.$$

En efecto, si $t = d$ entonces se sigue de la definición de $\sim$. Si $t = f\,(t_1 \ldots t_n)$ para un símbolo de función de aridad n, donde $t_i^{\mathcal{A}} = \bar{c}_i$ para $i = 1, \ldots, n$, entonces tenemos por inducción en la altura del término que $T^* \vdash_{\mathcal{L}} t_i \doteq c_i$. Por el *Aserto I* y el axioma de igualdad para funciones deducimos $T^* \vdash_{\mathcal{L}} t \doteq f\,(c_1, \ldots, c_n)$. Por otro lado, como

$$t^{\mathcal{A}} = \bar{c} \iff f^{\mathcal{A}}(t_1^{\mathcal{A}}, \ldots, t_n^{\mathcal{A}}) = \bar{c} \iff f^{\mathcal{A}}(\bar{c}_1, \ldots, \bar{c}_n) = \bar{c} \iff T^* \vdash_{\mathcal{L}} f(c_1 \ldots c_n) \doteq c,$$

por el *Aserto I* aplicado al axioma $((x \doteq y \wedge y \doteq z) \to x \doteq z)$ con los términos $t, f(c_1, \ldots, c_n)$ y c, se tiene que $t^{\mathcal{A}} = \bar{c}$ si y solo si $T^* \vdash_{\mathcal{L}} f(c_1 \ldots c_n) \doteq c$ si y solo si $T^* \vdash_{\mathcal{L}} t \doteq c$.

iii) Vemos finalmente que $\mathcal{A}$ es un modelo para T^*. Para ello, vemos que para toda $\mathcal{L}$-sentencia χ,

$$\mathcal{A} \models \chi \quad \text{si y solo si} \quad T^* \vdash_{\mathcal{L}} \chi.$$

Demostración. Por inducción en la altura de χ.
Si $\chi \equiv (t_1 \doteq t_2)$, donde t_1 y t_2 son términos sin variables libres, entonces existen constantes c_1 y c_2 tales que $t_1^A = \bar{c}_1$ y $t_2^A = \bar{c}_2$, ya que t_1^A y t_2^A son elementos de A. En particular, tenemos que $T^* \vdash_{\mathcal{L}} t_i \doteq c_i$ para $i = 1, 2$ por el resultado anterior, y por tanto $T^* \vdash_{\mathcal{L}} (t_1 \doteq c_1) \wedge (t_2 \doteq c_2)$ por la $\wedge$-*regla*. Por tanto,

$$\mathcal{A} \models t_1 \doteq t_2 \iff t_1^{\mathcal{A}} = t_2^{\mathcal{A}} \iff \bar{c}_1 = \bar{c}_2 \iff T^* \vdash_{\mathcal{L}} c_1 \doteq c_2 \iff T^* \vdash_{\mathcal{L}} t_1 \doteq t_2.$$

Si $\chi \equiv R(t_1, \ldots, t_n)$. La demostración es similar, y el caso $\chi \equiv (\chi_1 \wedge \chi_2)$ es inmediato por la $\wedge$-*regla*.

Si $\chi \equiv \neg\psi$. Entonces, por hipótesis de inducción obtenemos

$$\mathcal{A} \models \neg\psi \iff \mathcal{A} \not\models \psi \iff T^* \nvdash_{\mathcal{L}} \psi \iff T^* \vdash_{\mathcal{L}} \neg\psi \iff T^* \vdash_{\mathcal{L}} \chi;$$

donde la última equivalencia se cumple porque T^* es completa.

Si $\chi \equiv \exists x\, \psi$, finalmente, vemos ambas direcciones por separado:[24]

$\mathcal{A} \models \chi$ si y solo si $\bar{c} \in A$ tal que $\mathcal{A} \models \psi[\bar{c}]$, con $c \in C$. Con esta notación, el *Lema de sustitución* implica $\mathcal{A} \models \psi[\bar{c}]$ si y solo si $\mathcal{A} \models \psi_{c/x}$, ya que $c^{\mathcal{A}} = \bar{c}$. Por tanto, $\mathcal{A} \models \psi_{c/x}$ y $T^* \vdash_{\mathcal{L}} \psi_{c/x}$ por inducción. Claramente la variable x es libre para c en ψ, luego $T^* \vdash_{\mathcal{L}} (\psi_{c/x} \to \exists x\, \psi)$ por el axioma de $\exists$-sustitución, con lo que $T^* \vdash_{\mathcal{L}} \exists x\, \psi$ por MP.

Por otra parte, si $T^* \vdash_{\mathcal{L}} \chi$, como T^* es una teoría de Henkin $T^* \vdash_{\mathcal{L}} (\exists x\, \psi \to \psi_{c/x})$ para algún símbolo de constante c. Por MP deducimos que $T^* \vdash_{\mathcal{L}} \psi_{c/x}$, y por tanto $\mathcal{A} \models \psi_{c/x}$ por inducción, de donde $\mathcal{A} \models \psi[\bar{c}]$ por el Lema de sustitución, es decir, $\mathcal{A} \models \chi$. □

Unicidad. Sean $\mathcal{A}, \mathcal{B} \models T$ con $A = \{c^{\mathcal{A}}\}_{c \in C}$, $B = \{c^{\mathcal{B}}\}_{c \in C}$. Como T es completa, $\mathcal{A}$ y $\mathcal{B}$ satisfacen las mismas sentencias.[25]

Definamos $F : A \to B$ por $c^{\mathcal{A}} \mapsto c^{\mathcal{B}}$, $\forall c \in C$. Para toda constante c,

$$c^{\mathcal{A}} = d^{\mathcal{A}} \text{ si y solo si } \mathcal{A} \models c \doteq d \text{ si y solo si } \mathcal{B} \models c \doteq d \text{ si y solo si } c^{\mathcal{B}} = d^{\mathcal{B}}.$$

Esto demuestra que F está bien definida y es biyectiva. Vemos que también es isomorfismo. Para toda función f de aridad n, $f^{\mathcal{A}}(c_1^{\mathcal{A}}, \ldots, c_n^{\mathcal{A}}) = c_{n+1}^{\mathcal{A}}$ si y solo si $\mathcal{A} \models f(c_1, \ldots, c_n) \doteq c_{n+1}$ si y solo si $\mathcal{B} \models f(c_1, \ldots, c_n) \doteq c_{n+1}$ si y solo si $f^{\mathcal{B}}(c_1^{\mathcal{B}}, \ldots, c_n^{\mathcal{B}}) = c_{n+1}^{\mathcal{B}}$.

Para toda relación R de aridad m, $(c_1^{\mathcal{A}}, \ldots, c_m^{\mathcal{A}}) \in R^{\mathcal{A}}$ si y solo si $\mathcal{A} \models R(c_1, \ldots, c_m)$ si y solo si $\mathcal{B} \models R(c_1, \ldots, c_m)$ si y solo si $(c_1^{\mathcal{B}}, \ldots, c_m^{\mathcal{B}}) \in R^{\mathcal{B}}$. □

Como todo modelo de T^* es también modelo de T, estos tres pasos prueban el Teorema de Henkin (A.1.4).

Demostración del Teorema de completitud de Gödel

1. El Teorema de validez asegura que $T \vdash_{\mathcal{L}} \varphi$ implica $T \models \varphi$.

2. Para ver que $T \models \varphi$ implica $T \vdash_{\mathcal{L}} \varphi$, supongamos que $T \models \varphi$ pero $T \nvdash_{\mathcal{L}} \varphi$. Por el Lema A.1.3, la extensión $T \cup \{\neg\varphi\}$ es consistente. Por Henkin tiene un modelo, contradicción. □

Corolario A.1.15. *Sea T una $\mathcal{L}$-teoría consistente. Entonces, T es completa si y solo si cualesquiera dos de sus modelos son elementalmente equivalentes.*

Demostración. Sean $\mathcal{A}$ y $\mathcal{B}$ dos modelos cualesquiera de una teoría T y sea χ una $\mathcal{L}$-sentencia. Supongamos que $\mathcal{A} \models \chi$ pero $\mathcal{B} \not\models \chi$; luego $\mathcal{B} \models \neg\chi$. Pero entonces $T \not\vdash \chi$ y $T \not\vdash \neg\chi$, lo cual implica por el Teorema de validez que T no es completa.

Para demostrar la otra dirección, consideremos una $\mathcal{L}$-teoría T consistente y sea χ una $\mathcal{L}$-sentencia tal que $T \nvdash \chi$. Veamos que $T \vdash \neg\chi$. Por el Teorema de completitud, basta probar que $T \models \neg\chi$. Si esto no se cumpliera, existiría un modelo $\mathcal{A}$ de T tal que $\mathcal{A} \models \chi$. Por otro lado, como $T \nvdash \chi$, el conjunto $T \cup \{\neg\chi\}$ es consistente por el Lema A.1.3, con lo que existe un modelo $\mathcal{B}$ de T tal que $\mathcal{B} \models \neg\chi$ por el Teorema A.1.4. En particular, tendríamos dos modelos de T que no son elementalmente equivalentes, contradicción. □

[24] En esta prueba volvemos por claridad a la notación clásica para la sustitución.
[25] Es consecuencia de la implicación fácil del Corolario A.1.15.

A.2. Resultados de teoría de cuerpos

En esta sección recordamos algunas definiciones y resultados básicos para el desarrollo del trabajo. Nos basamos en [4] y [5].

Extensiones de cuerpos

Lema A.2.1. *Sea K un cuerpo y $f \in K[t]$. Entonces, $f(a) = 0$ si y solo si $(t-a)$ divide a $f(t)$.*

Demostración. Como $K[t]$ es un DE con función grado, aplicamos el algoritmo de división para f y $g(t) = t - a$. Existen $q(t), r(t) \in K[t]$ únicos tales que $f(t) = (t-a)q(t) + r(t)$, donde $\deg r < \deg(t-a) = 1$. Por tanto $r(t) = r \in K$ es una constante. Evaluando en $t = a$ obtenemos $f(a) = r$. En particular, $f(a) = 0$ si y solo si $r = 0$, es decir, si y solo si $(t-a) \mid f(t)$. □

Una *extensión de cuerpos* $K \subseteq L$ significa que L es un cuerpo que contiene a K como subcuerpo.

Lema A.2.2. *Sea K un cuerpo y $f \in K[t]$ un polinomio no nulo de grado $d \geq 1$. Entonces f tiene a lo sumo d raíces en cualquier extensión de cuerpos $L \supseteq K$.*

Demostración. Podemos asumir que $L = K$. Procedemos por inducción sobre d. Para $d = 1$, $f(t) = a(t-b)$ con $a \neq 0$, y f tiene exactamente una raíz, b.

Supongamos cierto el resultado para polinomios de grado $d-1$, y sea f de grado d. Si f no tiene raíces en K, no hay nada que probar. Si las tiene, sea $a \in K$ tal que $f(a) = 0$. Por el Lema anterior, existe $q(t) \in K[t]$ tal que $f(t) = (t-a)q(t)$, con $\deg q = d - 1$. Toda raíz $b \neq a$ de f satisface $q(b) = 0$, y por hipótesis inductiva, q tiene a lo sumo $d-1$ raíces distintas. Incluyendo a, concluimos que f tiene a lo sumo d raíces distintas en K. □

Toda extensión de cuerpos $K \subseteq L$ induce en L la estructura de K-espacio vectorial. Si la dimensión de L como K-espacio vectorial es finita, se llama *grado de la extensión* y se denota por $[L : K]$.

Proposición A.2.3 (Transitividad del grado)**.** *Sean $K \subseteq F \subseteq L$ extensiones de cuerpos. Se cumple que $[L : K] = [L : F]\,[F : K]$.*

Demostración. Sea $\{v_1, \ldots, v_m\}$ una base de L como F-espacio vectorial y $\{w_1, \ldots, w_n\}$ una base de F como K-espacio vectorial. Entonces el conjunto $\{v_i w_j : 1 \leq i \leq m,\ 1 \leq j \leq n\}$ es una base de L como K-espacio vectorial, de donde se deduce la igualdad anterior. □

Sea L una extensión de cuerpos de K y sea $\alpha \in L$. Definimos el *ideal de anulación* de α como $I_\alpha := \{f \in K[x] : f(\alpha) = 0\}$. Como $K[x]$ es un DIP (pues es un DE), existe un único polinomio mónico $g \in K[x]$ tal que $I_\alpha = (g)$. Decimos que α es *algebraico sobre K* si $I_\alpha \neq (0)$; es decir, si existe un polinomio no nulo $f \in K[x]$ tal que $f(\alpha) = 0$. En este caso, g es necesariamente irreducible y se denomina el *polinomio mínimo de α sobre K*, denotado $m_{\alpha,K}$. Si α no es algebraico sobre K, decimos que α es *trascendente sobre K*.

Teorema A.2.4. *Sea $K \subseteq L$ una extensión de cuerpos y $\alpha \in L$ algebraico sobre K. Sea $K(\alpha)$ el menor subcuerpo de L que contiene a K y a α. Entonces $K[\alpha] = K(\alpha)$ y el homomorfismo natural $K[x]/(m_{\alpha,K}) \longrightarrow K[\alpha]$, $\overline{f} \mapsto f(\alpha)$, es un isomorfismo de cuerpos. Además, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es una base de $K(\alpha)$ sobre K, donde $n = \deg m_{\alpha,K}$.*

Demostración. Consideramos la evaluación $\mathrm{ev}_\alpha : K[x] \longrightarrow K[\alpha],\ f \longmapsto f(\alpha)$. Por definición, la imagen de ev_α es todo $K[\alpha]$. Su núcleo es $I_\alpha = \{f \in K[x] : f(\alpha) = 0\} = (m_{\alpha,K})$, donde $m_{\alpha,K}$ es el polinomio mínimo de α sobre K.

Aplicando el Primer Teorema de Isomorfía, $K[x]/(m_{\alpha,K}) \cong K[\alpha]$. Como $m_{\alpha,K}$ es irreducible en el DIP $K[x]$, el ideal $(m_{\alpha,K})$ es maximal; por tanto el cociente es un cuerpo. Así, $K[\alpha]$ ya es un cuerpo y, por definición, $K[\alpha] = K(\alpha)$.

Sea $n = \deg m_{\alpha,K}$. Por el algoritmo de división, para todo $f \in K[x]$ existen $q, r \in K[x]$ únicos con $\deg r < n$ tales que $f = q\, m_{\alpha,K} + r$. En el cociente $K[x]/(m_{\alpha,K})$ se tiene $\bar{f} = \bar{r}$, por lo que cada clase tiene un único representante de grado $< n$. En consecuencia, los elementos de $K(\alpha)$ se escriben de manera única como

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}\ (a_i \in K),$$

lo que muestra que $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es una base de $K(\alpha)$ como K-espacio vectorial y que $[K(\alpha) : K] = n$. □

Teorema A.2.5. *Sea $K \subseteq L$ una extensión de cuerpos y $\alpha \in L$ trascendente sobre K. Entonces se tiene un isomorfismo de cuerpos $K(\alpha) \cong K(x)$, donde $K(x)$ denota el cuerpo de fracciones de $K[x]$.*

Demostración. Como α es trascendente, para todo $f \in K[x] \setminus \{0\}$ se cumple $f(\alpha) \neq 0$, por lo que el homomorfismo $\varphi : K[x] \to K[\alpha],\ f \mapsto f(\alpha)$, es inyectivo. Extendiéndolo al cuerpo de fracciones de $K[x]$, obtenemos un homomorfismo de cuerpos $\varphi : K(x) \to L,\ \frac{f}{g} \mapsto f(\alpha)g(\alpha)^{-1}$, bien definido e inyectivo, cuya imagen es precisamente $K(\alpha)$. Por tanto, $K(\alpha) \cong K(x)$. □

Una extensión $K \subseteq L$ se dice *finita* si $[L : K] < \infty$, y *algebraica* si todo elemento de L es algebraico sobre K.

Proposición A.2.6. *Toda extensión finita es algebraica. Además, si $\alpha \in L$ es algebraico sobre K con polinomio mínimo $m_{\alpha,K}$ de grado n, entonces $[K(\alpha) : K] = n$ y $n \mid [L : K]$.*

Demostración. Si $[L : K] = m < \infty$, para cualquier $\alpha \in L$ el conjunto $\{1, \alpha, \ldots, \alpha^m\}$ es linealmente dependiente sobre K, lo que proporciona una relación polinómica no trivial $a_0 + a_1\alpha + \cdots + a_m\alpha^m = 0, a_i \in K$, que demuestra que α es algebraico sobre K. Por otro lado, con $K \subseteq K(\alpha) \subseteq L$, por la transitividad del grado se tiene $[L : K] = [L : K(\alpha)]\,[K(\alpha) : K]$, y ya sabemos que $[K(\alpha) : K] = \deg m_{\alpha,K}$, de donde se deduce la divisibilidad. □

Observación A.2.7. Si algún $\gamma \in L$ no es algebraico sobre K, entonces los elementos $1, \gamma, \gamma^2, \ldots$ son linealmente independientes sobre K, por lo que $\dim_K K(\gamma) = \infty$. Por otro lado, no toda extensión algebraica es finita. Por ejemplo, el cuerpo $K := \mathbb{Q}\big(\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots\big)$ obtenido al adjuntar simultáneamente las raíces cuadradas de todos los números primos es una extensión algebraica infinita de $\mathbb{Q}$.

Teorema A.2.8 (Caracterización de extensiones finitas)**.** *Sea $K \subseteq L$ una extensión de cuerpos. Son equivalentes:*

1. *$K \subseteq L$ es una extensión finita.*
2. *Existen $\gamma_1, \ldots, \gamma_s \in L$ algebraicos sobre K tales que $L = K(\gamma_1, \ldots, \gamma_s)$.*

Demostración. Veamos primero que (1) implica (2). Supongamos que $[L : K] < \infty$ y sea $s = [L : K]$. Entonces, existe una base $\{\gamma_1, \ldots, \gamma_s\}$ de L como K-espacio vectorial, y por la proposición anterior cada γ_i es algebraico sobre K. Por otro lado, cualquier $\alpha \in L$ puede escribirse como $\alpha = a_1\gamma_1 + \cdots + a_s\gamma_s$, $a_i \in K$, lo que implica $L \subseteq K(\gamma_1, \ldots, \gamma_s)$. Como por construcción $K(\gamma_1, \ldots, \gamma_s) \subseteq L$, concluimos que $L = K(\gamma_1, \ldots, \gamma_s)$.

Vemos ahora que (2) implica (1). Procedemos por inducción sobre s. Si $L = K(\gamma_1)$ con γ_1 algebraico sobre K, por la proposición anterior $[L : K] = \deg m_{\gamma_1,K} < \infty$. Supongamos que el resultado vale para $s-1$ generadores. Sea $L = K(\gamma_1, \ldots, \gamma_{s-1}, \gamma_s)$. Por la transitividad del grado, $[L : K] = [L : K(\gamma_1, \ldots, \gamma_{s-1})]\,[K(\gamma_1, \ldots, \gamma_{s-1}) : K]$. Por hipótesis inductiva, el segundo factor es finito, y como γ_s es algebraico sobre $K(\gamma_1, \ldots, \gamma_{s-1})$, el primer factor también lo es. Por tanto, $[L : K] < \infty$. □

Demostramos finalmente la transitividad de la algebraicidad.

Proposición A.2.9 (Transitividad de la algebraicidad)**.** *Sean $F \subseteq K \subseteq L$ extensiones de cuerpos. Si K es algebraico sobre F y L es algebraico sobre K, entonces L es algebraico sobre F.*

Demostración. Sea $\gamma \in L$. Como L es algebraico sobre K, existe un polinomio mínimo $m_{\gamma,K} \in K[t]$ tal que $m_{\gamma,K}(\gamma) = 0$, que podemos escribir como $m_{\gamma,K}(t) = t^n + a_1t^{n-1} + \cdots + a_n$. Como K es algebraico sobre F, cada coeficiente a_i es algebraico sobre F, y por la caracterización anterior $F \subseteq F(a_1, \ldots, a_n)$ es una extensión finita. El mismo polinomio $m_{\gamma,K}$ pertenece a $F(a_1, \ldots, a_n)[t]$, por lo que γ es algebraico sobre $F(a_1, \ldots, a_n)$. Aplicando de nuevo la caracterización de extensiones finitas, $F(a_1, \ldots, a_n) \subseteq F(a_1, \ldots, a_n)(\gamma)$ es una extensión finita. Por transitividad del grado, $[F(a_1, \ldots, a_n)(\gamma) : F] = [F(a_1, \ldots, a_n)(\gamma) : F(a_1, \ldots, a_n)]\cdot[F(a_1, \ldots, a_n) : F]$. Como ambos factores son finitos, la extensión $F \subseteq F(a_1, \ldots, a_n)(\gamma)$ es finita. En consecuencia, γ es algebraico sobre F. Como γ era arbitrario, concluimos que L es algebraico sobre F. □

Característica de un cuerpo y cuerpos finitos

Sea K un cuerpo y consideremos el homomorfismo de grupos

$$\varphi : (\mathbb{Z}, +) \longrightarrow (K, +),\ n \longmapsto n \cdot 1 := \underbrace{1 + \cdots + 1}_{n \text{ veces}}.$$

Si $\ker\varphi = \{0\}$, decimos que $\operatorname{car}(K) = 0$; en caso contrario, $\ker\varphi = n\mathbb{Z}$ para algún $n \geq 1$, y definimos $\operatorname{car}(K) = n$. Si $n = ab$ con $1 < a, b < n$, entonces $(a \cdot 1)(b \cdot 1) = 0$ en K con $a \cdot 1, b \cdot 1 \neq 0$, contradiciendo que K sea cuerpo; por tanto, n es primo.

Si $\operatorname{car}(K) = p > 0$, el homomorfismo induce un isomorfismo $\mathbb{Z}/p\mathbb{Z} \cong \operatorname{im}\varphi \subseteq K$; el cociente $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo, denotado $\mathbb{F}_p$, llamado el *cuerpo finito de p elementos*. Si $\operatorname{car}(K) = 0$, la imagen de φ es un subanillo isomorfo a $\mathbb{Z}$; su cuerpo de fracciones, isomorfo a $\mathbb{Q}$, puede identificarse naturalmente con un subcuerpo de K.[26]

En ambos casos, llamamos *subcuerpo primo de K* al menor subcuerpo de K, isomorfo a $\mathbb{Q}$ si $\operatorname{car}(K) = 0$ o a $\mathbb{F}_p$ si $\operatorname{car}(K) = p > 0$. Si K es finito, por tanto, existe un único primo p tal que $\mathbb{F}_p \cong \operatorname{im}\varphi \subseteq K$; dado que $\operatorname{im}\varphi \subseteq K$ y ambos son cuerpos finitos, se sigue que K es una *extensión finita* de $\operatorname{im}\varphi$. Escribiendo $m = [K : \operatorname{im}\varphi]$, toda base $\{\alpha_1, \ldots, \alpha_m\}$ de K sobre $\operatorname{im}\varphi$

[26] En particular, todo monomorfismo de anillos $f\colon A \hookrightarrow K$ en un cuerpo K se extiende de manera única a un homomorfismo de cuerpos $\widetilde{f}\colon \operatorname{Frac}(A) \to K$, poniendo $\widetilde{f}(a/b) = f(a)f(b)^{-1}$. En consecuencia, todo isomorfismo de dominios se extiende de manera única a un isomorfismo entre sus cuerpos de fracciones, y si A es un dominio de integridad, cualesquiera dos cuerpos de fracciones de A son A-isomorfos.

proporciona una descomposición única $x = a_1\alpha_1 + \cdots + a_m\alpha_m$, $a_i \in \operatorname{im}\varphi$, y hay p posibles elecciones de los coeficientes. Así, para todo cuerpo finito K, $|K| = p^m$, $m = [K : \operatorname{im}\varphi]$.

Lema A.2.10 (Frobenius)**.** *Si K tiene característica $p > 0$, entonces para todo $a, b \in K$ y todo $k \geq 1$:*

$$(a+b)^{p^k} = a^{p^k} + b^{p^k}, \ (ab)^{p^k} = a^{p^k} b^{p^k}.$$

Demostración. Por el binomio de Newton, $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p$, ya que $\binom{p}{i} \equiv 0$ (mód p) para $1 \leq i \leq p-1$. Además, $(ab)^p = a^p b^p$, sin más que reordenar pues K es un cuerpo. Por inducción sobre k, suponiendo que las igualdades valen para p^{k-1}, se tiene

$$(a+b)^{p^k} = \big((a+b)^{p^{k-1}}\big)^p = (a^{p^{k-1}} + b^{p^{k-1}})^p = a^{p^k} + b^{p^k},$$

y análogamente $(ab)^{p^k} = (a^{p^{k-1}} b^{p^{k-1}})^p = a^{p^k} b^{p^k}$. □

Lema A.2.11. *Sea K un cuerpo y $f(t) = a_0 + \cdots + a_n t^n \in K[t]$. Definimos su* derivada formal *por $f'(t) = a_1 + 2a_2 t + \cdots + n a_n t^{n-1}$. Si L es un cuerpo de descomposición de f sobre K, entonces f tiene solo raíces simples en L si y solo si $\operatorname{mcd}(f, f') = 1$ en $K[t]$.*

Demostración. Sea $a \in L$ una raíz de f. Entonces puede escribirse $f(t) = (t-a)^m h(t)$, $h(a) \neq 0$, donde $m \geq 1$ es la multiplicidad de a, y recordemos que decimos que a es simple si y solo si $m = 1$. Por la regla de Leibniz,

$$f'(t) = m(t-a)^{m-1} h(t) + (t-a)^m h'(t) = (t-a)^{m-1}\big(m h(t) + (t-a) h'(t)\big).$$

Evaluando en $t = a$ se obtiene

$$f'(a) = \begin{cases} h(a) \neq 0, & \text{si } m = 1, \\ 0, & \text{si } m \geq 2. \end{cases}$$

En particular, $f'(a) \neq 0$ si y solo si a es una raíz simple, y equivalentemente

$$(t-a) \mid f' \quad \text{si y solo si} \quad (t-a)^2 \mid f.$$

Por tanto, f y f' tienen un factor común no trivial si y solo si f posee alguna raíz múltiple. □

Proposición A.2.12. *Sean $n_1, n_2 \geq 1$. Se cumple que $\mathbb{F}_{p^{n_1}} \subseteq \mathbb{F}_{p^{n_2}}$ si y solo si $n_1 \mid n_2$.*

Demostración. Probamos primero que con $n, m \geq 1$ enteros, se cumple que $n \mid m$ si y solo si $x^n - 1 \mid x^m - 1$.

En efecto, si $m = d \cdot n$, tenemos $\tau^d - 1 = (\tau - 1)(\tau^{d-1} + \tau^{d-2} + \cdots + \tau + 1)$ para todo τ. Sustituyendo $\tau = x^n$ se obtiene $x^{nd} - 1 = (x^n - 1)\,(\cdots)$, y por tanto $x^n - 1 \mid x^m - 1$.

Por otro lado, sea $A = \frac{\mathbb{F}_p[x]}{(x^n - 1)}$ y sea $a = \bar{x}$.

Entonces $a^n = 1$ y $n = \operatorname{ord}(a)$ en el grupo $(A^*, \cdot)$. Por hipótesis, $x^m - 1 = g(x)\,(x^n - 1)$, y evaluando en a obtenemos $a^m - 1 = g(a)\,(a^n - 1) = 0$, de donde $a^m = 1$. Luego $n \mid m$.

Ahora, si $\mathbb{F}_p \subseteq \mathbb{F}_{p^{n_1}} \subseteq \mathbb{F}_{p^{n_2}}$, por transitividad del grado

$$n_2 = [\mathbb{F}_{p^{n_2}} : \mathbb{F}_p] = [\mathbb{F}_{p^{n_2}} : \mathbb{F}_{p^{n_1}}]\,[\mathbb{F}_{p^{n_1}} : \mathbb{F}_p] = [\mathbb{F}_{p^{n_2}} : \mathbb{F}_{p^{n_1}}] \cdot n_1.$$

Luego $n_1 \mid n_2$.

Por otra parte, si $n_1 \mid n_2$, entonces $x^{p^{n_1}} - x \mid x^{p^{n_2}} - x$ en $\mathbb{F}_p[x]$. Por tanto, todas las raíces de $x^{p^{n_1}} - x$ son también raíces de $x^{p^{n_2}} - x$, y el conjunto de raíces de $x^{p^{n_1}} - x$ es precisamente $\mathbb{F}_{p^{n_1}}$ y el de $x^{p^{n_2}} - x$ es $\mathbb{F}_{p^{n_2}}$ por el Teorema 4.1.18. Luego $\mathbb{F}_{p^{n_1}} \subseteq \mathbb{F}_{p^{n_2}}$. □

Separabilidad y extensiones simples

Sea $K \subseteq L$ una extensión de cuerpos y sea $\alpha \in L$ algebraico sobre K. Decimos que α es *separable sobre* K si su polinomio mínimo $m_{\alpha,K}$ no tiene raíces múltiples en alguna (equivalente, en toda) clausura algebraica de K.

La extensión $K \subseteq L$ se dice *separable* si todo elemento de L algebraico sobre K es separable sobre K.

Proposición A.2.13. *Sea $K \subseteq L$ una extensión de cuerpos. Si $\mathrm{car}(K) = 0$, entonces la extensión $K \subseteq L$ es separable.*

Demostración. Sea $\alpha \in L$ algebraico sobre K y sea $m_{\alpha,K} \in K[X]$ su polinomio mínimo. Como $\mathrm{car}(K) = 0$, la derivada formal $m'_{\alpha,K}$ es no nula. Dado que $m_{\alpha,K}$ es irreducible y $\deg(m'_{\alpha,K}) < \deg(m_{\alpha,K})$, se sigue que $mcd(m_{\alpha,K}, m'_{\alpha,K}) = 1$. Por el Lema A.2.11, se deduce que $m_{\alpha,K}$ tiene únicamente raíces simples. □

Teorema A.2.14 (Teorema del elemento primitivo)**.** *Sea $K \subseteq L$ una extensión finita y separable. Entonces existe $\alpha \in L$ tal que $L = K(\alpha)$.*

Demostración. Si K es finito, entonces L también lo es. Sea $p = \mathrm{car}(K)$; entonces K y L son extensiones finitas de $\mathbb{F}_p$. Por el Lema 4.1.17, el grupo multiplicativo L^* es cíclico, luego existe $\delta \in L^*$ tal que $L^* = \langle \delta \rangle$. En particular, $L = \mathbb{F}_p(\delta)$. Como K contiene a $\mathbb{F}_p$, se tiene $L = K(\delta)$.

Supongamos que K es infinito. Como $K \subseteq L$ es finita, existen $\gamma_1, \ldots, \gamma_n \in L$ algebraicos sobre K tales que $L = K(\gamma_1, \ldots, \gamma_n)$, para cierto $n \in \mathbb{N}$. Basta tratar el caso $n = 2$, pues si $n > 2$, iterando el caso binario se obtiene un único generador. Sea entonces $L = K(\beta, \gamma)$, con β, γ algebraicos sobre K. Denotamos por $f = m_{\beta,K}$ y $g = m_{\gamma,K}$ sus polinomios mínimos.

Por separabilidad, f y g no tienen raíces múltiples; denotamos sus raíces por $\beta_1, \ldots, \beta_e$ y $\gamma_1, \ldots, \gamma_m$ respectivamente.

Para todo $\lambda \in K$ se tiene $K(\beta+\lambda\gamma) \subseteq K(\beta, \gamma)$. Buscamos $\lambda_0 \in K$ tal que $K(\beta+\lambda_0\gamma) = K(\beta, \gamma)$.

Fijado $\lambda \in K$, definimos $F(T) = f(\beta+\lambda\gamma-\lambda T) \in K(\beta+\lambda\gamma)[T]$. Se cumple $F(\gamma) = f(\beta) = 0$ y $g(\gamma) = 0$. Sea $h = mcd(F, g) \in K(\beta + \lambda\gamma)[T]$.

Si $\deg h > 1$, existe $\gamma_i \neq \gamma$ tal que $F(\gamma_i) = g(\gamma_i) = h(\gamma_i) = 0$, luego $f(\beta + \lambda\gamma - \lambda\gamma_i) = 0$. Así, existe β_j con $\beta_j = \beta + \lambda(\gamma - \gamma_i)$, y despejando $\lambda = \dfrac{\beta_j - \beta}{\gamma - \gamma_i}$.

Como K es infinito, podemos elegir $\lambda_0 \in K$ tal que $\lambda_0 \neq \dfrac{\beta_j - \beta}{\gamma - \gamma_i}$ para todo i, j. Para ese λ_0 se tiene $\deg h = 1$ y $h(T) = T - \gamma \in K(\beta + \lambda_0\gamma)[T]$, de donde $\gamma \in K(\beta + \lambda_0\gamma)$. Como también $\beta \in K(\beta + \lambda_0\gamma)$, concluimos que $K(\beta, \gamma) \subseteq K(\beta + \lambda_0\gamma)$.

La inclusión inversa es trivial, luego $K(\beta + \lambda_0\gamma) = K(\beta, \gamma)$, y tomando $\alpha = \beta + \lambda_0\gamma$ se concluye la prueba. □

Decimos que una extensión $K \subseteq L$ es *simple* si existe $\alpha \in L$ tal que $L = K(\alpha)$.

Observación A.2.15. Por el teorema anterior, toda extensión finita y separable es simple. En particular, por la Proposición A.2.13, toda extensión finita sobre un cuerpo de característica cero es simple.

A.3. K-álgebras y producto tensorial

En este apéndice reunimos algunas nociones algebraicas que serán utilizadas en la prueba del Lema de Sylvester (Lema 5.1.22). Nos basamos en [4] y [9], con apoyo en [10].

Sea K un cuerpo. Una *K-álgebra* es un anillo conmutativo A con unidad, junto con un homomorfismo de anillos unitario $\varphi\colon K \longrightarrow A$.

Mediante φ, se define una operación externa de K sobre A, $K \times A \longrightarrow A,\ (\lambda, a) \longmapsto \varphi(\lambda)\, a$, que dota a A de estructura de espacio vectorial sobre K. Diremos que una K-álgebra A es *finita* si es de dimensión finita como espacio vectorial sobre K.

Un ejemplo fundamental para nosotros es el siguiente. Dado un polinomio no constante $f \in K[X]$, el cociente $K[X]/(f)$ es una K-álgebra mediante el homomorfismo de anillos $\varphi\colon K \longrightarrow K[X]/(f),\ \lambda \longmapsto \lambda + (f)$. Si $\deg f = n$, las clases de $1, X, \ldots, X^{n-1}$ forman una base de $K[X]/(f)$ como espacio vectorial sobre K.

Sea A un anillo conmutativo con unidad. Un *A-módulo* es un grupo abeliano $(M, +)$ provisto de una aplicación $A \times M \to M,\ (a, m) \mapsto am$, que satisface, para todo $a, b \in A$ y $m, n \in M$,

$$a(m+n) = am + an,\ \ (a+b)m = am + bm,\ \ (ab)m = a(bm),\ \ 1m = m.$$

Sea A un anillo conmutativo y sean M y N dos A-módulos. Una aplicación $b\colon M \times N \longrightarrow P$, con valores en un A-módulo P, se dice *A-bilineal* si es lineal en cada variable, es decir, si para todo $m, m' \in M$, $n, n' \in N$ y $\lambda \in A$ se cumple que

$$b(m+m', n) = b(m,n)+b(m',n),\ \ b(m, n+n') = b(m,n)+b(m,n'),\ \ b(\lambda m, n) = \lambda b(m,n) = b(m, \lambda n).$$

El *producto tensorial* de M y N sobre A es un A-módulo $M \otimes_A N$, junto con una aplicación A-bilineal $\otimes\colon M \times N \longrightarrow M \otimes_A N$, que satisface la siguiente propiedad universal: para todo A-módulo P y toda aplicación A-bilineal $b\colon M \times N \to P$, existe un único homomorfismo A-lineal $\tilde{b}\colon M \otimes_A N \longrightarrow P$ tal que $b = \tilde{b} \circ \otimes$.

Sea ahora R un cuerpo, A una R-álgebra y $R \subseteq K$ una extensión de cuerpos. Recordemos que toda R-álgebra es, en particular, un R-módulo. El producto tensorial $A \otimes_R K$ es una K-álgebra de manera natural; es un anillo con multiplicación $(a \otimes \lambda) \cdot_{A \otimes_R K} (b \otimes \mu) = ab \otimes \lambda\mu$, y la estructura de K-álgebra viene dada por la operación $\lambda \cdot (a \otimes \mu) = a \otimes (\lambda\mu)$.

Si A es una R-álgebra finita, entonces $A \otimes_R K$ es una K-álgebra finita. En efecto, si $\{\alpha_1, \ldots, \alpha_n\}$ es una base de A como R-espacio vectorial, entonces $\{\alpha_1 \otimes 1, \ldots, \alpha_n \otimes 1\}$ es una base de $A \otimes_R K$ como K-espacio vectorial. En el caso particular $A = R[X]/(f)$, existe un isomorfismo natural de K-álgebras $R[X]/(f) \otimes_R K \cong K[X]/(f)$, dado por $(\overline{g(X)}) \otimes \lambda \longmapsto \lambda\, \overline{g(X)}$.

Recordamos finalmente una versión del Teorema Chino del Resto en el contexto de anillos conmutativos. Sean A un anillo conmutativo y $I_1, \ldots, I_r \subseteq A$ ideales dos a dos coprimos, es decir, tales que $I_i + I_j = A$ para todo $i \neq j$. Entonces la aplicación canónica $A \longrightarrow A/I_1 \times \cdots \times A/I_r,\ a \longmapsto (a + I_1, \ldots, a + I_r)$, es un homomorfismo de anillos sobreyectivo cuyo núcleo es la intersección $I_1 \cap \cdots \cap I_r$, y en particular induce un isomorfismo de anillos $A/(I_1 \cap \cdots \cap I_r) \cong A/I_1 \times \cdots \times A/I_r$.

En particular, si K es un cuerpo y $f \in K[X]$ se factoriza como producto de polinomios dos a dos coprimos $f = f_1 \cdots f_r$, entonces existe un isomorfismo natural de K-álgebras $K[X]/(f) \cong K[X]/(f_1) \times \cdots \times K[X]/(f_r)$.

A.4. Cardinalidad

A continuación presentamos un breve repaso de resultados básicos de teoría de cardinales. Una exposición más detallada puede encontrarse en la introducción de [6].

Trabajaremos en el marco axiomático de ZFC, utilizando, como en [6], la distinción entre *conjuntos* y *clases* del marco axiomático de Gödel–Bernays. Intuitivamente, toda colección definida por una propiedad se llama clase; una clase es un conjunto si puede ser elemento de otra, y una *clase propia* si no puede serlo. En la práctica, seguiremos este uso y hablaremos de "clases" de modo informal dentro de ZFC, donde solo se trabaja con conjuntos. Esta distinción es relevante, pues no suele ser evidente que una clase dada sea o no un conjunto, y resultados como el Lema de Zorn solo se aplican a conjuntos parcialmente ordenados, no a clases propias.

Dados dos conjuntos A y B, decimos que A y B son *equipotentes* si existe una biyección $A \to B$. La equipotencia es una relación de equivalencia sobre la clase de todos los conjuntos. El *cardinal* de un conjunto A, denotado $|A|$, se define como la clase de todos los conjuntos equipotentes a A, es decir, su clase de equivalencia bajo la relación de equipotencia.

Para motivar que hablamos de "números", observemos que los conjuntos finitos $I_n = \{1, \dots, n\}$ e $I_m = \{1, \dots, m\}$ son equipotentes si y solo si $n = m$. De este modo, decimos que un conjunto A tiene n elementos si es equipotente a I_n para algún $n \in \mathbb{N}$, en cuyo caso decimos que A es *finito*; si no es equipotente a ningún I_n, decimos que A es *infinito*. Identificamos el cardinal de un conjunto finito con el número natural n correspondiente.

El orden entre cardinales se introduce diciendo que $|A| \leq |B|$ si y solo si existe una función inyectiva $A \hookrightarrow B$, lo que equivale a decir que A es un subconjunto de B, que escribimos $A \subseteq B$. Con estas nociones, la clase de los cardinales queda totalmente ordenada, de modo que cualquier par de conjuntos es comparable en tamaño. Dados cardinales $\alpha = |A|$ y $\beta = |B|$, definimos la suma y el producto cardinales como

$$\alpha + \beta = |A \cup B| \text{ (con } A \text{ y } B \text{ disjuntos)}, \ \alpha \cdot \beta = |A \times B| \text{ (para cualesquiera } A \text{ y } B).$$

Estas operaciones coinciden con la suma y el producto habituales de números naturales y satisfacen las leyes conmutativa, asociativa y distributiva.

En el caso de conjuntos infinitos, se cumplen algunos hechos fundamentales: todo conjunto infinito contiene un subconjunto numerable, de modo que $\aleph_0 \leq |A|$ siempre que A sea infinito; si α es infinito y $\beta \leq \alpha$, entonces $\alpha + \beta = \alpha$, y si además $\beta \neq 0$, se tiene también $\alpha \cdot \beta = \alpha$. En particular, $\alpha + n = \alpha$ para todo $n \in \mathbb{N}$ y $\alpha \cdot \aleph_0 = \alpha$ para todo α infinito.

Sea ahora A un conjunto y, para cada entero $n \geq 1$, definamos $A^n = A \times \cdots \times A$ el producto cartesiano de n factores. Si A es finito, se tiene $|A^n| = |A|^n$, mientras que si A es infinito se cumple $|A^n| = |A|$. Además, el cardinal de la unión de todos estos productos cartesianos es $\left|\bigcup_{n\geq 1} A^n\right| = \aleph_0 \, |A|$, y por tanto, si A es infinito, la unión numerable de copias de A tiene el mismo cardinal que A.

Un hecho fundamental es que no existe un conjunto de cardinalidad máxima. Este resultado se formaliza en el siguiente teorema clásico.

Teorema A.4.1 (Cantor)**.** *Para cualquier conjunto A se cumple $|A| < |\mathcal{P}(A)|$, donde $\mathcal{P}(A)$ denota el conjunto potencia de A, es decir, el conjunto de todos los subconjuntos de A.*

Idea de la demostración. La aplicación $a \mapsto \{a\}$ define una función inyectiva de A en $\mathcal{P}(A)$, por lo que $|A| \leq |\mathcal{P}(A)|$.

Supongamos que existe una biyección $f : A \to \mathcal{P}(A)$ y consideremos el subconjunto $B = \{\, a \in A : a \notin f(a) \,\} \subseteq A$. Como $B \in \mathcal{P}(A)$, existe $a_0 \in A$ tal que $f(a_0) = B$.

Por definición de B, se tiene

$$a_0 \in B \quad \text{si y solo si} \quad a_0 \notin f(a_0),$$

lo que implica que $a_0 \in B \quad$ si y solo si $\quad a_0 \notin B$, contradicción.

Por tanto, no existe una biyección entre A y $\mathcal{P}(A)$, y en consecuencia $|A| < |\mathcal{P}(A)|$. □

Adoptaremos la convención habitual de identificar las funciones con sus grafos.

Convención. Sean A y B conjuntos. Una *función* de A en B es un subconjunto $f \subseteq A \times B$ tal que

$$\forall a \in A \; \exists! \, b \in B \, ((a, b) \in f).$$

En este contexto, f *es* su grafo: no distinguimos entre la función y el conjunto de pares ordenados que la representan. Para cada $a \in A$, el único $b \in B$ tal que $(a, b) \in f$ se denota $f(a)$.

De este modo, una función puede tratarse como un conjunto y es legítimo razonar sobre ella dentro de la teoría de conjuntos. En particular, si $X \subseteq A$ e $Y \subseteq B$, se definen la imagen de X y la preimagen de Y como los subconjuntos

$$f[X] := \{\, f(x) : x \in X \,\} \subseteq B, \;\; f^{-1}[Y] := \{\, x \in A : f(x) \in Y \,\} \subseteq A.$$

Algunos de los resultados enunciados en esta sección requieren el Axioma de Elección, mientras que otros se demuestran en ZF puro. Por ello trabajamos en el marco de ZFC (ZF más el Axioma de Elección). Recordamos que el Axioma de Elección es equivalente, sobre ZF, al Lema de Zorn.

Lema A.4.2 (Lema de Zorn)**.** *Sea $(P, \leq)$ un conjunto parcialmente ordenado tal que toda cadena, es decir, todo subconjunto totalmente ordenado de P, tiene una cota superior en P. Entonces P contiene al menos un elemento maximal.*

Este lema se emplea en varias construcciones del trabajo, de forma explícita o implícita, en argumentos de maximalidad y existencia.