TRABAJO FIN DE GRADO

Eliminación de cuantificadores para cuerpos algebraicamente cerrados y cuerpos reales cerrados

Realizado por

Antonio Miguel Ruiz Cardoso

Para la obtención del título de
Grado en Matemáticas

Dirigido por
D. Andrés Cordón Franco

Realizado en el departamento de
Ciencias de la Computación e Inteligencia Artificial

Convocatoria de junio, curso 2021/22

Agradecimientos

Quiero expresar mi más sincero agradecimiento al profesor D. Andrés Cordón Franco. Sin su ayuda, esfuerzo y tiempo, realizar este trabajo no hubiese sido posible. Gracias por no dejar de confiar en mí.

Por otro lado, no puedo olvidar a mi familia y compañeros, cuyo apoyo y cariño he tenido siempre muy presentes.

De corazón, gracias.

Resumen

El proyecto tiene como objetivo estudiar la Teoría de Modelos de los cuerpos algebraicamente cerrados y los cuerpos reales cerrados. De este modo se pretende conseguir una axiomatización completa del cuerpo de los números complejos y el cuerpo de los números reales. Para ello se emplearán dos técnicas básicas de la Teoría de Modelos: λ-categoricidad y eliminación de cuantificadores, siendo esta última la que abordaremos con mayor profundidad. Finalmente, gracias a la axiomatización completa obtenida, se podrán estudiar otros aspectos de esta clase de cuerpos como la decibilidad y sus conjuntos definibles.

Abstract

The main objective of the present project is to study the Model Theory of algebraically closed fields and real closed fields. In this way, we aim at giving a complete axiomatization of the complex numbers field and the real numbers field. For this purpose, we will use two basic model-theoretic techniques: λ-categoricity and quantifier elimination, focussing on this last technique. Finally, thanks to the given axiomatizations, we will study different aspects of these field classes like decidability and definable sets.

Índice general

Introducción

El presente proyecto se desarrolla dentro del marco de la Lógica Matemática. En concreto, se estudia la teoría de modelos de los cuerpos algebraicamente cerrados y de los cuerpos reales cerrados. Pero, ¿qué es la Teoría de Modelos? ¿Qué papel desempeña dentro de las matemáticas? Intentemos responder brevemente a estas preguntas.

La Teoría de Modelos es una rama de la Lógica Matemática encargada del estudio de las distintas propiedades de las estructuras matemáticas mediante el uso de fórmulas y otros objetos que nos proporcionan los lenguajes de primer orden. A modo de eslogan, se podría decir que

$$\text{Teoría de Modelos} = \text{Álgebra universal} + \text{Lógica}$$

Pese a dar sus primeros pasos a principios del siglo XX (algunos autores datan el nacimiento de la Teoría de Modelos en torno a 1915 con los resultados de Löwenheim-Skolem), no es hasta la década de 1950, sobre todo de la mano del matemático polaco-americano Alfred Tarski, cuando comienza a ser considerada área independiente de las matemáticas. Tradicionalmente, el desarrollo de la Teoría de Modelos ha transcurrido por dos vertientes bien marcadas.

- En la primera de ellas, se parte de una estructura concreta de interés en matemáticas, como, por ejemplo, el cuerpo de los números reales $\mathbb{R}$, y se emplean técnicas propias de la Teoría de Modelos para obtener información nueva sobre dicha estructura y sobre los conjuntos definibles mediante fórmulas de la lógica de primer orden en la estructura.
- En la segunda de ellas, a priori de carácter más abstracto, se estudian clases de teorías de la lógica de primer orden que poseen buenas propiedades y se establecen teoremas de clasificación que describen la estructura general de los modelos de dichas teorías.

Nuestro trabajo se enmarca dentro de la primera de las dos vertientes anteriores, siendo el estudio del cuerpo de los números complejos $\mathbb{C}$ y del cuerpo de los números reales $\mathbb{R}$ desde el punto de vista de la Teoría de Modelos el eje fundamental del proyecto.

Más concretamente, los objetivos fundamentales del presente trabajo son:

(O1) Obtener una axiomatización completa, $\mathcal{T}_{\mathbb{C}}$, natural e informativa de la teoría del cuerpo de los números complejos.

(O2) Obtener una axiomatización completa, $\mathcal{T}_{\mathbb{R}}$, natural e informativa de la teoría del cuerpo de los números reales.

(O3) Emplear dichas axiomatizaciones para obtener nuevas propiedades de estas estructuras (decibilidad, conjuntos definibles en ellas,...)

Una axiomatización *completa* de una estructura no es más que un conjunto de fórmulas de la lógica de primer orden, que denominaremos axiomas, verdaderas en la estructura y a partir de las cuales pueda demostrarse cualquier propiedad de primer orden verdadera en la estructura. Esto es, se destaca una lista de propiedades

fundamentales de la estructura en cuestión de manera que cualquier otra propiedad (expresable en la lógica de primer orden) verdadera en la estructura es consecuencia lógica de la axiomatización dada.

Además, el interés de perseguir esa idea de completitud, y de los métodos que usaremos para ello, reside en que dotará a nuestra teoría de muy buenas propiedades, permitiéndonos el estudio de otros aspectos como la decibilidad o los conjuntos definibles en una estructura.

Para el logro de los objetivos propuestos son necesarias dos fases: 1) determinar una teoría candidata a ser una axiomatización completa de la estructura (en nuestro caso, y de manera natural, teorías de carácter algebraico), y 2) estudiar técnicas básicas de la Teoría de Modelos que nos permitan demostrar que las axiomatizaciones en cuestión son, de hecho, teorías de primer orden completas.

Respecto a la primera fase, consideraremos en este trabajo las siguientes teorías de primer orden (la descripción detallada de los axiomas de estas teorías se dará en el transcurso del trabajo):

- ACF = teoría de los cuerpos algebraicamente cerrados en la signatura $\{+, -, \cdot, 0, 1\}$.
- ACF_p = teoría de los cuerpos algebraicamente cerrados de característica p en la signatura $\{+, -, \cdot, 0, 1\}$ (con p=0 o *primo*).
- RCF = teoría de los cuerpos reales cerrados en la signatura $\{+, -, \cdot, 0, 1, <\}$.

En cuanto a la segunda fase, estudiaremos dos técnicas básicas de la Teoría de Modelos que nos permitirán demostrar la completitud de una teoría:

- La noción de *teoría λ-categórica* y el resultado conocido como el "Test de Vaught", el cual nos permitirá inferir completitud a partir de la noción de λ-categoricidad. Usando esta técnica, daremos una prueba de que las teorías ACF_p son teorías completas y, por tanto, obtenemos una primera solución para el objetivo (O1) (caso complejo). Aunque muy elegante, esta técnica resulta muy abstracta y hace uso de resultados algebraicos no triviales del estudio de los cuerpos algebraicamente cerrados. Además, esta técnica no es aplicable al caso real.
- El método de *eliminación de cuantificadores*. El estudio de esta técnica básica nos permitirá dar una solución tanto para el caso complejo (O1) como para el caso real (O2). Siendo la técnica más importante en el presente proyecto, damos a continuación una descripción un poco más detallada de la misma.

La idea de la eliminación de cuantificadores para una cierta teoría $\mathcal{T}$ es clara. Consiste en poder reducir cualquier fórmula de un lenguaje de primer orden que use cuantificadores (ya sea el existencial $\exists$ o el universal $\forall$) a otra fórmula equivalente (en la teoría $\mathcal{T}$) que no haga uso de los mismos.

Más formalmente, diremos que una teoría $\mathcal{T}$ admite eliminación de cuantificadores si, para toda fórmula de primer orden del lenguaje de la teoría, $\phi(\bar{v})$, existe una fórmula abierta (esto es, sin cuantificadores), $\phi'(\bar{v})$, tal que la teoría demuestra la equivalencia de ambas fórmulas: $T \vdash \forall \bar{v}\, (\phi(\bar{v}) \leftrightarrow \phi'(\bar{v}))$.

En un principio, podría parecer una técnica un poco artificiosa y difícil de conse-

guir en la práctica. Sin embargo, ilustremos la eliminación de cuantificadores con dos ejemplos a los que estamos muy acostumbrados en las matemáticas del día a día.

I) Supongamos que estamos estudiando las distintas raíces de un polinomio de segundo grado. La existencia de dichas raíces puede expresarse mediante la siguiente fórmula

$$\phi(a,b,c) = \exists x \ (ax^2 + bx + c = 0).$$

Evidentemente la expresión anterior hace uso del cuantificador existencial, pero lo interesante es que, gracias a la conocida fórmula para la resolución de ecuaciones de segundo grado, podemos expresar la existencia de raíces como sigue

$$\mathbb{R} \models \phi(a,b,c) \leftrightarrow [(a \neq 0 \wedge b^2 - 4ac \geq 0) \ \vee \ (a = 0 \wedge (b \neq 0 \vee c = 0))],$$

para el caso real, o

$$\mathbb{C} \models \phi(a,b,c) \leftrightarrow (a \neq 0 \vee b \neq 0 \vee c = 0),$$

para el caso complejo. En ambos casos, hemos obtenido una condición equivalente en la que no aparece ningún cuantificador de primer orden.

II) Ahora, supongamos que estamos estudiando la invertibilidad de una matriz genérica de orden 2×2

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

La existencia de una matriz inversa se expresa de manera natural por la fórmula

$$\phi(a,b,c,d) = \exists x \exists y \exists u \exists v \ (xa + yc = 1 \wedge xb + yd = 0 \wedge ua + vc = 0 \wedge ub + vd = 1).$$

De nuevo, podemos expresar la existencia de matriz inversa con una fórmula libre de cuantificadores, en este caso

$$F \models \phi(a,b,c,d) \leftrightarrow (ad - bc \neq 0),$$

gracias a la propiedad del determinante (válida en cualquier cuerpo F).

Tras la motivación y las ideas principales, estamos ya en condiciones de enunciar los dos teoremas primordiales que demostraremos en el presente trabajo y sus consecuencias más importantes.

Caso complejo:

Teorema (A.Tarski): La teoría ACF de los cuerpos algebraicamente cerrados admite eliminación de cuantificadores en el lenguaje $\mathcal{L} = \{+, -, \cdot, 0, 1\}$.

Corolario: Las teorías ACF_p de los cuerpos algebraicamente cerrados de característica p son completas y decidibles. En particular, ACF_0 proporciona una axiomatización completa del cuerpo de los números complejos.

Caso real:

Teorema (A.Tarski): La teoría RCF de los cuerpos reales cerrados admite eliminación de cuantificadores en el lenguaje $\mathcal{L} = \{+, -, \cdot, 0, 1, <\}$.

Corolario: La teoría RCF es completa y decidible. En particular, RCF proporciona una axiomatización completa del cuerpo ordenado de los números reales.

Motivada y ejemplificada la idea de nuestro proyecto, hagamos un estudio más detallado del contenido específico de cada capítulo.

- El capítulo 0, "Prefacio Algebraico", está destinado a recopilar algunos conceptos y resultados pertenecientes al álgebra que necesitaremos para el desarrollo teórico del trabajo. Dado que escapan del alcance del proyecto y son conceptos algebraicos muy bien conocidos, se pasa de forma rápida sin atender a mayores detalles.
- El capítulo 1, "Lenguajes y estructuras", sirve como capítulo introductorio a la lógica de primer orden y recoge conceptos fundamentales de la misma como el de *lenguaje de primer orden* y *estructura*, básicos para el desarrollo del proyecto. Se estudian además numerosos aspectos tanto sintácticos como semánticos de los mencionados lenguajes (satisfacción en una estructura, teoría de primer orden, modelo de una teoría, isomorfismos entre estructuras, equivalencia elemental, conjuntos definibles, ...)
- El capítulo 2, "Técnicas básicas", introduce resultados capitales de la lógica de primer orden como el "Teorema de Completitud de Gödel" o el "Teorema de compacidad". Además, se introduce la primera de las técnicas estudiadas para determinar la completitud de una teoría: λ-categoricidad y el conocido "Test de Vaught". Como aplicación, se da una primera prueba de la completitud y decibilidad de las teorías ACF_p, con $p = 0$ o *primo*.
- El capítulo 3, "Eliminación de cuantificadores", tal y como su nombre indica, presenta la técnica primordial del trabajo. Tras presentarla en su marco teórico, se da paso al primero de los resultados fundamentales del proyecto, la eliminación de cuantificadores para la teoría ACF de los cuerpos algebraicamente cerrados. A continuación, se extraen una serie de consecuencias del mismo: completitud de las teorías ACF_p, decibilidad de la teoría ACF y descripción de los conjuntos definibles en un cuerpo algebraicamente cerrado.
- Cerramos el proyecto con el capítulo 4, "El caso real". En el transcurso del mismo, tras contextualizar el concepto de cuerpo real cerrado, se esboza una demostración del segundo de los resultados fundamentales del trabajo, la eliminación de cuantificadores para la teoría de los cuerpos reales cerrados RCF. A continuación, se extraen las consecuencias pertinentes: completitud y decibilidad de la teoría RCF y descripción de los conjuntos definibles de un cuerpo real cerrado.

Por último, ha de señalarse que las dos fuentes principales que se han utilizado para la realización de este trabajo han sido los libros [6] y [5].

0. Prefacio Algebraico

Esta primera sección introductoria estará dedicada a la implementación del armamento algebraico que necesitaremos para el desarrollo del proyecto. Es decir, recopilaremos algunos de los conceptos y resultados pertenecientes al álgebra que se requiere conocer para poder entender en su totalidad la información aquí expuesta. Con ánimos de calmar al lector, notar que la mayoría de ellos son plenamente conocidos, por lo que no supondrán problema alguno.

Es importante aclarar que las particularidades de estos aspectos algebraicos escapan del alcance del presente trabajo, por ello, se pasará de forma rápida sin atender a mayores detalles.

Sin más dilación, comencemos con algunos conceptos elementales.

Definición 0.1. *Un anillo R es un conjunto donde están definidas las siguientes operaciones. Para $a, b \in R$:*

- *La suma,*
$$\begin{array}{rccc} + & : & R \times R & \to & R \\ & & (a,b) & \to & a+b \end{array}$$
- *El producto,*
$$\begin{array}{rccc} \cdot & : & R \times R & \to & R \\ & & (a,b) & \to & a \cdot b \end{array}$$

Estas operaciones satisfacen las propiedades de asociatividad y distributividad habituales. La suma ha de ser a su vez conmutativa. Además existen dos elementos, $0, 1 \in R$, los elementos neutros de sendas operaciones. Todos los elementos $a \in R$ deben poseer un elemento opuesto $-a$ para la suma. Los elementos $a \in R$ que posean elemento inverso a^{-1} para el producto se denominarán unidades.

Definición 0.2. *Un cuerpo F es un anillo donde $0 \neq 1$ y todo elemento no nulo es una unidad.*

Definición 0.3. *Se dice que un cuerpo F es algebraicamente cerrado si todo polinomio de grado positivo con coeficientes en F:*

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0, \ n > 0, \ a_i \in F \text{ con } 0 \leq i \leq n,$$

tiene al menos una raíz en F.

Veamos un par de ejemplos que serán de vital importancia a lo largo del trabajo.

Ejemplo 0.1.

- $\mathbb{R}$ (con la suma y el producto habituales) es un cuerpo.
- $\mathbb{C}$ también es un cuerpo, pero además, verifica la condición de ser algebraicamente cerrado (Teorema fundamental del álgebra).

Definición 0.4. *Se define la característica de un cuerpo F como el menor entero positivo k tal que $1+1+\ldots+1=0$ (k veces). En caso de no existir tal k, se dice que la característica de F es 0.*

Ejemplo 0.2.
- Tanto $\mathbb{R}$ como $\mathbb{C}$ son cuerpos de característica 0.
- En cambio, para cada p *primo*, $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo (finito) de característica p.

Nota 0.1. Es bien conocido que si un cuerpo F tiene característica $n>0$, entonces n ha de ser un número primo.

Llegados a este punto, estamos preparados para introducir algunos conceptos y resultados referentes a las extensiones de cuerpos.

Definición 0.5. *Una extensión de cuerpos*

$$F \subseteq K$$

es un par formado por un cuerpo K y un subanillo F de K que también es un cuerpo. En estas circunstancias, decimos que K es una extensión de F.

Ejemplo 0.3. Algunos ejemplos de extensiones son:

i) La conocida extensión trivial, $F \subseteq F$ (bien definida para todo cuerpo F).

ii) $F \subseteq F[x]$, con F cuerpo y $F[x]$ el cuerpo de los polinomios con coeficientes en F.

iii) Un ejemplo de extensión más específica puede ser $\mathbb{R} \subseteq \mathbb{C}$.

Para la siguiente definición, grado de una extensión, es importante resaltar que si tenemos una extensión

$$F \subseteq K,$$

podemos considerar K como un F-espacio vectorial.

Definición 0.6. *En las condiciones de la definición anterior, definimos el grado de la extensión como*

$$[K:F] = dim_F\ K.$$

Decimos que la extensión es finita si $dim_F\ K < +\infty$.

Definición 0.7. *Dada una extensión $F \subseteq K$, decimos que $\alpha \in K$ es algebraico si existe $p(x) \in F[x]$ no nulo tal que $p(\alpha)=0$. En caso contrario diremos que α es trascendente.*

Ejemplo 0.4.
- El elemento $\sqrt{2} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$, aunque $\sqrt{2} \notin \mathbb{Q}$.
- El elemento $\pi \in \mathbb{C}$ es algebraico sobre $\mathbb{R}$ pero es trascendente sobre $\mathbb{Q}$.

Nota 0.2. Decimos que una extensión $F \subseteq K$ es algebraica si cada elemento de K es algebraico sobre F.

Definición 0.8. *Una clausura algebraica de un cuerpo F es una extensión algebraica de F, $\bar{F}$, que es algebraicamente cerrada. Se puede demostrar que todo cuerpo F posee una clausura algebraica $\bar{F}$ que, además, es única salvo isomorfismos.*

Introduzcamos también un resultado bastante útil en cuanto a extensiones se refiere.

Proposición 0.1. Dadas dos extensiones finitas y consecutivas $F \subseteq K \subseteq L$, $F \subseteq L$ es también finita y de grado

$$[L : F] = [L : K] \cdot [K : F].$$

Pasaremos a introducir la definición de grado de trascendencia de una extensión, quizás, el concepto menos conocido entre todos los aquí expuestos. Con el fin de comprenderlo correctamente, pasemos antes por algunas nociones necesarias.

Definición 0.9. *Sea $F \subseteq K$ una extensión. Un conjunto $S \subseteq K$ es algebraicamente independiente sobre F si para todo polinomio $p(x_1, ..., x_n) \in F[x_1, ..., x_n]$ (no nulo), $p(s_1, ..., s_n) \neq 0$, para todo $s_1, ..., s_n \in S$. En caso contrario diremos que S es algebraicamente dependiente.*

Definición 0.10. *Sea $F \subseteq K$ una extensión. Una base de trascendencia de K sobre F es un conjunto $S \subseteq K$ algebraicamente independiente y maximal.*

Observación 0.1. Es interesante señalar el siguiente resultado, « $\{\alpha\} \subseteq K$ es un conjunto algebraicamente independiente si y solo si α es trascendente sobre F».

Definición 0.11. *Sea $F \subseteq K$ una extensión. Se define el grado de trascendencia de K sobre F como el cardinal de cualquier base de trascendencia de K sobre F.*

Más información sobre estos conceptos puede encontrarse en los libros y referencias [1], [3], [2] y [8]. En particular, podemos encontrar en [3] una prueba del siguiente resultado que será de vital importancia en el presente trabajo.

Teorema 0.1. *Sean F_1 y F_2 dos cuerpos algebraicamente cerrados. Entonces, F_1 y F_2 son isomorfos si, y solo si, tienen la misma característica y el mismo grado de trascendencia sobre su subcuerpo minimal.*

Finalicemos la sección con uno de los resultados más conocidos en cuanto al álgebra se refiere, y que nos garantiza que el cuerpo $\mathbb{C}$ es algebraicamente cerrado.

Teorema 0.2. *(**Teorema fundamental del Álgebra**) Todo polinomio no constante sobre el cuerpo de los números complejos tiene al menos una raíz compleja.*

1. Teorías y estructuras

1.1. Lenguajes y estructuras

En Lógica matemática, los lenguajes de primer orden desempeñan un papel primordial en el estudio y descripción de las diversas estructuras matemáticas.

Pese a que a lo largo de esta sección nos detengamos en describir, con todo detalle, cada uno de estos conceptos, ofreceremos una primera intuición sobre los mismos. En primera instancia, podríamos decir que una estructura matemática es un conjunto (sobre el que resida algún interés de estudio) equipado con una serie de funciones, relaciones y elementos destacados. Tras ello, se escoge un lenguaje «adecuado» mediante el cual se estudie el comportamiento de las mencionadas funciones, relaciones y elementos destacados en el conjunto a estudiar.

Un ejemplo de estructura bastante simple podría ser $(\mathbb{N}, +, 0, 1)$, la estructura conformada por el conjunto de los números naturales y la función suma, además del 0 y 1 como elementos destacados. Para el estudio de la estructura anterior, un lenguaje conveniente sería uno que contase con el símbolo de una función binaria (para la suma) y otros dos símbolos para las constantes 0 y 1. Gracias a la elección de dicho lenguaje, podríamos escribir enunciados como:

$$\forall x \ (x = 0 \ \vee \ \exists y \ (x = y + 1)),$$

que podemos interpretar como la afirmación siguiente:

"todo natural distinto del 0, es sucesor de otro natural".

Una vez vislumbrado, en este pequeño ejemplo, tanto el interés como la utilidad de los lenguajes a la hora de describir propiedades de las estructuras matemáticas, comencemos introduciendo algunas definiciones básicas. La mayoría de conceptos y resultados de esta sección aparecen con todo detalle en [9]. Inauguremos este listado con un concepto fundamental, *lenguaje de primer orden*.

Definición 1.1. *Un lenguaje de primer orden $\mathcal{L}$ se compone de dos tipos de símbolos, lógicos y no lógicos.*

I) *Los símbolos lógicos son:*

- *una cantidad numerable de variables $x_0, x_1, x_2, ...,$*
- *los conectores lógicos $\neg$ y $\vee$, negación y disyunción respectivamente,*
- *el cuantificador existencial $\exists$ y el símbolo de igualdad $=$.*

II) *Los símbolos no lógicos son:*

- *un conjunto de símbolos de funciones $\mathcal{F}$, junto con un entero positivo n_f para cada $f \in \mathcal{F}$ que denota su aridad,*

- *un conjunto de símbolos de relaciones $\mathcal{R}$, junto con un entero positivo n_R para cada $R \in \mathcal{R}$ que denota su aridad,*
- *un conjunto de símbolos de constantes $\mathcal{C}$.*

Nota 1.1. I) El conjunto de los símbolos lógicos es común a todos los lenguajes de primer orden.

II) Los conjuntos $\mathcal{F}, \mathcal{R}$ y $\mathcal{C}$ pueden ser vacíos. Además el conjunto de los símbolos no lógicos es propio de cada lenguaje y en ocasiones se denomina *signatura* del lenguaje.

III) Aunque no aparezcan oficialmente en la definición anterior, es bien conocido que podemos suponer que un lenguaje de primer orden contiene todas las conectivas proposicionales habituales ($\neg$, $\wedge$, $\vee$, $\rightarrow$) y el cuantificador universal $\forall$. Los nuevos símbolos son definibles a partir de los anteriores (lo veremos con detalle más adelante). La razón para no incluir todos ellos en la definición oficial es que, de esta manera, se simplifican las pruebas por inducción en la construcción de las fórmulas.

IV) Por comodidad, a partir de ahora, llamaremos a los *lenguajes de primer orden* simplemente *lenguajes*.

Ejemplo 1.1. Algunos ejemplos de lenguajes son:

I) $\mathcal{L} = \{\in\}$, para la Teoría de Conjuntos. Siendo $\in$ el símbolo de una relación binaria.

II) $\mathcal{L}_g = \{e, \cdot\}$, para la Teoría de Grupos. Donde e es un símbolo de constante para el elemento neutro y $\cdot$ es un símbolo de función binaria para la operación del grupo.

III) $\mathcal{L}_r = \{+, -, \cdot, 0, 1\}$, para la Teoría de Anillos. Donde $+$, $-$ y $\cdot$ son símbolos de funciones binarias para denotar las operaciones naturales y $0, 1$ son símbolos de constante para denotar los correspondientes elementos destacados.

Nota 1.2. Las elecciones anteriores no son las únicas existentes. De hecho, para el estudio de una misma estructura matemática, usaremos un lenguaje u otro (siempre que sean adecuados) dependiendo del contexto.

Aclarado esto, demos una definición de estructura.

Definición 1.2. *Dado un lenguaje $\mathcal{L}$, una $\mathcal{L}$-estructura $\mathcal{M}$ viene determinada por:*

I) *un conjunto M (no vacío) denominado universo de $\mathcal{M}$;*

II) *una función $f^{\mathcal{M}} : M^{n_f} \rightarrow M$ para cada $f \in \mathcal{F}$;*

III) *un conjunto $R^{\mathcal{M}} \subseteq M^{n_R}$ para cada $R \in \mathcal{R}$;*

IV) *un elemento $c^{\mathcal{M}} \in M$ para cada $c \in \mathcal{C}$.*

Nota 1.3. I) Al conjunto universo definido anteriormente también suele hacerse referencia como dominio o conjunto subyacente de la estructura.

II) Una estructura como la de la definición anterior se denotará en ocasiones como $\mathcal{M} = (M, f^{\mathcal{M}}, R^{\mathcal{M}}, c^{\mathcal{M}})$.

III) Con $f^{\mathcal{M}}, R^{\mathcal{M}}$ y $c^{\mathcal{M}}$ nos referimos a las "interpretaciones" de los símbolos f, R y c respectivamente.

Estudiemos un par de ejemplos para intentar entender mejor el concepto de estructura.

Ejemplo 1.2. Supongamos que estamos interesados en estudiar la Teoría de Grupos.

Tal y como se expuso anteriormente, un lenguaje adecuado para ello podría ser: $\mathcal{L}_g = \{e, \cdot\}$.
Una $\mathcal{L}_g$-estructura $\mathcal{G} = (G, \cdot^{\mathcal{G}}, e^{\mathcal{G}})$ será un conjunto no vacío G acompañado de una función binaria $\cdot^{\mathcal{G}}$ y un elemento destacado $e^{\mathcal{G}}$. Así, por ejemplo, valdrían como $\mathcal{L}_g$-estructuras:

I) $\mathcal{G} = (\mathbb{R}, \cdot, 1)$, donde interpretamos $\cdot$ como la multiplicación habitual y e como el 1. Es decir, en este caso, $\cdot^{\mathcal{G}} = \cdot$ y $e^{\mathcal{G}} = 1$.

II) Por otro lado también podríamos considerar $\mathcal{N} = (\mathbb{N}, +, 0)$, donde interpretamos $\cdot$ como la suma habitual y e como el 0. Tomando en este caso, $\cdot^{\mathcal{N}} = +$ y $e^{\mathcal{N}} = 0$.

Este segundo ejemplo puede parecer controvertido en un principio pues, evidentemente, $\mathcal{N}$ no es un grupo, pero sí es una $\mathcal{L}_g$-estructura (de grupo).

Más aún, existe libertad de tomar una interpretación que nos aleje tanto como deseemos de la estructura a estudiar (hecho que no tiene mucho sentido en la práctica). Siguiendo el ejemplo anterior, otra $\mathcal{L}_g$-estructura válida podría ser:

- $G = \{$Plantilla oficial del Real Betis Balompié de la temporada 21/22$\}$.
- $\cdot^{\mathcal{G}} =$ La función que, dados dos jugadores, devuelva el que lleve más tiempo en la plantilla.
- $e^{\mathcal{G}} =$ Joaquín Sánchez Rodríguez.

De nuevo, la estructura anterior no es un grupo pero sí es una $\mathcal{L}_g$-estructura (de grupo).

Detengámonos en el estudiemos de aplicaciones (entre estructuras) que preserven la interpretación de un lenguaje $\mathcal{L}$.

Definición 1.3. *Sean $\mathcal{M}$ y $\mathcal{N}$ dos $\mathcal{L}$-estructuras cuyos conjuntos universo son M y N respectivamente. Una inmersión $\eta : \mathcal{M} \to \mathcal{N}$ es una aplicación inyectiva $\eta : M \to N$ que preserva la interpretación de todos los símbolos del lenguaje $\mathcal{L}$. Más concretamente:*

I) $\eta(f^{\mathcal{M}}(a_1, ..., a_{n_f})) = f^{\mathcal{N}}(\eta(a_1), ..., \eta(a_{n_f}))$, *para toda $f \in \mathcal{F}$ y $a_i \in M$;*

II) $(a_1, ..., a_{m_R}) \in R^{\mathcal{M}}$ *si y solamente si* $(\eta(a_1), ..., \eta(a_{m_R})) \in R^{\mathcal{N}}$, *para todo $R \in \mathcal{R}$ y $a_i \in M$;*

III) $\eta(c^{\mathcal{M}}) = c^{\mathcal{N}}$, *para todo $c \in \mathcal{C}$.*

Por otra parte, un isomorfismo entre dos $\mathcal{L}$-estructuras es una inmersión que, además, es biyectiva.

Nota 1.4. Es habitual llamar automorfismos a los isomorfismos de una $\mathcal{L}$-estructura en sí misma.

Definición 1.4. *Sean $\mathcal{M}$ y $\mathcal{N}$ $\mathcal{L}$-estructuras de dominios M y N respectivamente. Si $M \subseteq N$ y la inclusión $\eta : M \to N$ es una inmersión, decimos que $\mathcal{M}$ es una subestructura de $\mathcal{N}$ o equivalentemente que $\mathcal{N}$ es una extensión de $\mathcal{M}$.*

Ejemplo 1.3. I) $\mathcal{M}_1 = (\mathbb{Z}, +, 0)$ es una $\mathcal{L}_g$-subestructura de $\mathcal{M}_2 = (\mathbb{R}, +, 0)$.

II) Si definimos $\eta : \mathbb{Z} \to \mathbb{R}$ como la función $\eta(x) = e^x$, entonces η es una inmersión de $\mathcal{M}_1$ en la $\mathcal{L}_g$-estructura $\mathcal{M}_3 = (\mathbb{R}, \cdot, 1)$.

Definición 1.5. *Decimos que el cardinal de una $\mathcal{L}$-estructura $\mathcal{M}$ es $|M|$, es decir, el cardinal de su conjunto subyacente M. En este caso, si η es una inmersión de $\mathcal{M}$ en $\mathcal{N}$, el cardinal de $\mathcal{N}$ es, al menos, el cardinal de $\mathcal{M}$.*

Como dijimos previamente, la finalidad del uso de los lenguajes es la creación de fórmulas que sirvan para describir propiedades de las estructuras. Las fórmulas son cadenas finitas de símbolos, entre los que se encuentran los símbolos del lenguaje $\mathcal{L}$ acompañados de paréntesis y otros símbolos determinados atendiendo al contexto.

Realmente con los propios símbolo de $\mathcal{L}$ es suficiente. Por un lado, puede eliminarse el uso de paréntesis empleando por ejemplo la notación polaca. Sin embargo, expresiones tan sencillas de entender como $(a-b)\cdot c$ pasarían a expresarse como $\cdot - a\, b\, c$, las cuales pueden inducir a confusión. Por otro lado, con el fin de facilitar la escritura y el entendimiento de las fórmulas, suelen añadirse otros símbolos que no dejan de ser abreviaciones de los ya conocidos. Algunas de las abreviaciones más comunes son las siguientes.

- El símbolo $\forall$ (cuantificador universal). Así, son equivalentes las expresiones:

$$\forall x A$$

$$\neg \exists x \neg A$$

- El símbolo $\wedge$ (conjunción). Siendo equivalentes:

$$A \wedge B$$

$$\neg(\neg A \vee \neg B)$$

- El símbolo $\to$ (implicación). Puede expresarse equivalentemente:

$$A \to B$$

$$\neg A \vee B$$

- El símbolo $\leftrightarrow$ (si y solo si). Son equivalentes las expresiones:

$$A \leftrightarrow B$$

$$(A \to B) \wedge (B \to A)$$

En busca de definir el concepto de *fórmula* de un lenguaje, comencemos introduciendo algunas definiciones elementales.

Definición 1.6. *El conjunto de términos de un lenguaje $\mathcal{L}$ es el menor conjunto $\mathcal{T}$ que verifica:*

I) *$c \in \mathcal{T}$ para cada símbolo de constante $c \in \mathcal{C}$,*

II) *$x_i \in \mathcal{T}$ para cada símbolo de variable x_i,*

III) *si $t_1, ..., t_{n_f} \in \mathcal{T}$ y $f \in \mathcal{F}$ entonces $f(t_1, ...t_{n_f}) \in \mathcal{T}$.*

Ejemplo 1.4. Si consideramos el lenguaje de la Teoría de Anillos, $\mathcal{L}_r = \{+, -, \cdot, 0, 1\}$, algunos términos podrían ser:

- $\underline{m} = \underbrace{1 + \cdots + 1}_{m \text{ veces}}$, siendo $\underline{m}$ el término obtenido tras sumar 1, m veces consigo mismo.
- $t^n = \underbrace{t \cdot \cdots \cdot t}_{n \text{ veces}}$, siendo t^n el término obtenido tras multiplicar el término t, n veces consigo mismo.
- Así, cualquier expresión de la forma $p = \underline{m_0} + \underline{m_1} \cdot x + \cdots + \underline{m_n} \cdot x^n$, siendo x un término cualquiera (en particular, una variable), también será un nuevo término de nuestro lenguaje.

Definidos ya los términos de un lenguaje, pasemos al estudio de los *subtérminos* de un determinado término t.

Definición 1.7. *El conjunto de los subtérminos de un término t se define como sigue:*

- *t es un subtérmino de t.*
- *Si $f(t_1, ..., t_n)$, con $f \in \mathcal{F}$ y $t_1, ..., t_n \in \mathcal{T}$, es un subtérmino de t, entonces cada t_i, $i = 1, ..., n$, también es subtérmino de t.*

Ejemplo 1.5. Consideremos $t = x \cdot y \cdot z$ un término del lenguaje de la Teoría de grupos (anteriormente definido).
Los subtérminos de nuestro término t serían: $x \cdot y \cdot z,\ y \cdot z,\ x,\ y,\ z$.
Es importante recalcar que $x \cdot y$ no es un subtérmino de t, pues por convenio, asociamos a la derecha cuando se omiten paréntesis. Realmente podríamos haber escrito t como $t = x \cdot (y \cdot z)$.

Ejemplo 1.6. Estudiemos ahora el término $1 + (1 + (1 + 1)) \in \mathcal{L}_r$ del lenguaje de la Teoría de Anillos. Dicho término, dentro de la $\mathcal{L}_r$-estructura $(\mathbb{Z}, +, \cdot, 0, 1)$, lo entendemos como el nombre que recibe el elemento 4. De este mismo modo, dentro de esta

misma estructura, podemos entender el término $(x_1 + x_2) \cdot (x_3 + 1)$ como el nombre que recibe la función de forma $(x, y, z) \to (x + y) \cdot (z + 1)$.

Teniendo en cuenta lo anterior, sean $\mathcal{M}$ una cierta $\mathcal{L}$-estructura y t un término conformado por las variables $\bar{v} = (v_{i_1}, ..., v_{i_m})$. Queremos interpretar a t como una función $t^{\mathcal{M}} : M^m \to M$. Así, para cada subtérmino s de t y $\bar{a} = (a_{i_1}, ..., a_{i_m}) \in M$ definimos $s^{\mathcal{M}}(\bar{a})$ como sigue:

I) si s es el símbolo de una constante c, entonces, $s^{\mathcal{M}}(\bar{a}) = c^{\mathcal{M}}$,

II) si s es la variable v_{i_j}, entonces, $s^{\mathcal{M}}(\bar{a}) = a_{i_j}$,

III) si s es el término $f(t_1, ..., t_{n_f})$, donde f es el símbolo de una función de $\mathcal{L}$ y $t_1, ..., t_{n_f}$ son términos, entonces, $s^{\mathcal{M}}(\bar{a}) = f^{\mathcal{M}}(t_1^{\mathcal{M}}(\bar{a}), ..., t_{n_f}^{\mathcal{M}}(\bar{a}))$.

Intentemos aclarar esto con un ejemplo.

Ejemplo 1.7. Sea el lenguaje $\mathcal{L} = \{f, g, c\}$, donde f es el símbolo de función de aridad uno, g es el símbolo de función binaria y c es el símbolo de una constante.

Consideremos los siguientes términos de nuestro lenguaje:

$$t_1 = g(x_1, c),$$

$$t_2 = f(g(c, f(x_1))) \text{ y}$$

$$t_3 = g(f(g(x_1, x_2)), g(x_1, f(x_2))).$$

Si tomamos la $\mathcal{L}$-estructura $\mathcal{M} = (\mathbb{R}, exp, +, 1)$, es decir, considerando $f^{\mathcal{M}} = exp(\cdot)$, $g^{\mathcal{M}} = +$ y $c^{\mathcal{M}} = 1$, tendríamos que:

$$t_1^{\mathcal{M}}(a) = a + 1,$$

$$t_2^{\mathcal{M}}(a) = e^{1+e^a}, \text{ y por último}$$

$$t_3^{\mathcal{M}}(a, b) = e^{a+b} + (a + e^b).$$

Llegados a este punto, estamos preparados para introducir el concepto de *fórmula* de un lenguaje $\mathcal{L}$. Comencemos dando la noción de *fórmula atómica*.

Definición 1.8. *Decimos que ϕ es una fórmula atómica de $\mathcal{L}$ si presenta alguna de las siguientes formas:*

I) *$t_1 = t_2$, donde t_1, t_2 son términos de $\mathcal{L}$.*

II) *$R(t_1, ..., t_{n_R})$, donde $R \in \mathcal{R}$ y $t_1, ..., t_{n_R}$ son términos de $\mathcal{L}$.*

Ejemplo 1.8. $(x \in y)$ y $(x = y)$ son, esencialmente, las únicas dos fórmulas atómicas del lenguaje de la Teoría de Conjuntos, esto es, salvo renombramiento de variables.

Finalmente, estamos preparados para introducir la definición de fórmula de un lenguaje.

Definición 1.9. *El conjunto $\mathcal{W}$ de las fórmulas de un lenguaje $\mathcal{L}$ es el menor conjunto que contiene a las fórmulas atómicas y que verifica:*

I) *si $\phi \in \mathcal{W}$ entonces $\neg\phi \in \mathcal{W}$,*

II) *si $\phi,\ \psi \in \mathcal{W}$, entonces $(\phi \vee \psi) \in \mathcal{W}$,*

III) *si $\phi \in \mathcal{W}$, entonces $(\exists x_i\ \phi)$ pertenece a $\mathcal{W}$.*

Nota 1.5. Como hemos mencionado anteriormente, solo consideramos explícitamente en la definición las conectivas $\neg$, $\vee$ y $\exists$, pero en la práctica usaremos todas las conectivas habituales entendidas como las abreviaciones anteriormente reseñadas. Por otra parte, usaremos también los criterios de prioridad habituales entre conectivas que nos permitirán omitir paréntesis en la escritura de las fórmulas y, por convenio, a igualdad de prioridad se asociará por la derecha. A este respecto, consideraremos también las abreviaciones:

I) Escribiremos $\bigwedge_{i=1}^{n} \psi_i$ en lugar de $\psi_1 \wedge \psi_2 \wedge \cdots \wedge \psi_n$.

II) Equivalentemente, notaremos como $\bigvee_{i=1}^{n} \psi_i$ la expresión $\psi_1 \vee \psi_2 \vee \cdots \vee \psi_n$.

Ejemplo 1.9. Algunos ejemplos de fórmulas del lenguaje de la Teoría de grupos son:

I) $\forall x \forall y \forall z\ (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$,

II) $\forall x\ (x \cdot e = x \wedge e \cdot x = x)$,

III) $\forall x \exists y\ (x \cdot y = e \wedge y \cdot x = e)$.

Nota 1.6. Las tres fórmulas del ejemplo anterior *axiomatizan* la Teoría de Grupos. Más adelante, haremos uso de esta axiomatización.

Definición 1.10. *Se define el conjunto de las subfórmulas de una determinada fórmula ϕ como sigue:*

I) *ϕ es subfórmula de ϕ,*

II) *si $\neg\psi$ o $\exists x\ \psi$ es subfórmula de ϕ, entonces, ψ es subfórmula de ϕ,*

III) *si $\psi_1 \vee \psi_2$ es subfórmula de ϕ, entonces, ψ_1 y ψ_2 son subfórmulas de ϕ.*

Es importante saber que dentro de una fórmula ϕ podemos clasificar las apariciones de las variables en dos tipos. Si una variable x_i aparece en una subfórmula de ϕ bajo el alcance de un cuantificador de primer orden $\exists x_i$ o $\forall x_i$ entonces la aparición de dicha variable se dice que es ligada (en la fórmula). En caso contrario, diremos que la aparición es libre.
Se dice que una variable x_i es libre en ϕ si tiene, al menos, una aparición libre en ϕ.

Ejemplo 1.10. En el lenguaje de la Teoría de conjuntos, podemos considerar la siguiente fórmula:

$$x \in y\ \vee\ \exists x\ (x \in y)$$

Todas las apariciones de la variable y son libres mientras que sólo la primera aparición de la variable x es libre, siendo el resto ligadas.
En este caso, x, y serían las variables libres de la fórmula (obsérvese que una variable bien puede tener tanto ocurrencias libres como ligadas en una misma fórmula).
Si consideramos ahora la fórmula:

$$\forall x\ \exists y\ (x \cdot y = e)$$

podemos observar que no tiene ninguna variable libre.
Este tipo de fórmulas se denominan *fórmulas cerradas* o sentencias. Por otra parte, las fórmulas que no poseen cuantificadores se denominan *fórmulas abiertas.*

Más adelante, intentaremos incluir la noción de "verdad" dentro de una $\mathcal{L}$-estructura, pudiendo determinar qué fórmulas cerradas de dicha $\mathcal{L}$-estructura son ciertas y cuáles son falsas.

Por otro lado, si ϕ es una fórmula que sí tenga variables libres $v_1, ..., v_n$, que en ocasiones denotaremos $\phi(v_1, ..., v_n)$ (enfatizando así dichas variables), podemos interpretarla como la expresión de cierta propiedad de elementos de M^n. Por tanto, tenemos que definir qué significa para $\phi(v_1, ..., v_n)$ que valide un cierto $(a_1, ..., a_n) \in M^n$.

Definición 1.11. *Consideremos $\mathcal{M}$ una cierta $\mathcal{L}$-estructura y sean ϕ una fórmula de $\mathcal{M}$ con variables libres $\bar{v} = (v_{i_1}, ..., v_{i_m})$ y $\bar{a} = (a_{i_1}, ..., a_{i_m})$ elementos de M. Inductivamente definimos $\mathcal{M} \models \phi(\bar{a})$ como sigue:*

I) *Si ϕ es de la forma $t_1 = t_2$, entonces, $\mathcal{M} \models \phi(\bar{a})$ si $t_1^{\mathcal{M}}(\bar{a}) = t_2^{\mathcal{M}}(\bar{a})$, con t_1, t_2 términos.*

II) *Si ϕ es de la forma $R(t_1, ..., t_{n_R})$, entonces, $M \models \phi(\bar{a})$ si $(t_1^{\mathcal{M}}(\bar{a})), ..., t_{n_R}^{\mathcal{M}}(\bar{a})) \in R^{\mathcal{M}}$.*

III) *Si ϕ es de la forma $\neg\psi$, entonces, $\mathcal{M} \models \phi(\bar{a})$ si $\mathcal{M} \not\models \psi(\bar{a})$.*

IV) *Si ϕ es de la forma $\psi \wedge \theta$, entonces, $\mathcal{M} \models \phi(\bar{a})$ si $\mathcal{M} \models \psi(\bar{a})$ y $\mathcal{M} \models \theta(\bar{a})$.*

V) *Si ϕ es de la forma $\psi \vee \theta$, entonces, $\mathcal{M} \models \phi(\bar{a})$ si $\mathcal{M} \models \psi(\bar{a})$ o $\mathcal{M} \models \theta(\bar{a})$.*

VI) *Si ϕ es de la forma $\exists v_j\ \psi(\bar{v}, v_j)$, entonces, $\mathcal{M} \models \phi(\bar{a})$ si existe un cierto $b \in M$ tal que $\mathcal{M} \models \psi(\bar{a}, b)$.*

VII) *Si ϕ es de la forma $\forall v_j\ \psi(\bar{v}, v_j)$, entonces, $\mathcal{M} \models \phi(\bar{a})$ si $\mathcal{M} \models \psi(\bar{a}, b)$, para todo $b \in M$.*

En caso de que $\mathcal{M} \models \phi(\bar{a})$, diremos que $\mathcal{M}$ satisface $\phi(\bar{a})$ o que $\phi(\bar{a})$ es verdadero (o cierto) en $\mathcal{M}$.

Nota 1.7. Por comodidad del lector, hemos preferido dar la definición de validez de una fórmula en una estructura contemplando un mayor número de conectivas y no solo las que "oficialmente" aparecen en la definición de lenguaje de primer orden. Por otra parte, y aunque debe estar claro por el contexto, la notación $\mathcal{M} \not\models \phi$ significa "no se cumple que $\mathcal{M} \models \phi$".

Veamos ahora un primer resultado de satisfacibilidad. Más allá de la información que nos proporciona, el siguiente resultado es importante pues introduce en su prueba un método de demostración que usaremos a menudo, la inducción en la construcción de términos, fórmulas...

Proposición 1.1. Supongamos que $\mathcal{M}$ es una subestructura de $\mathcal{N}$, $\overline{a} \in M$ y $\phi(\overline{v})$ una fórmula sin cuantificadores, es decir, abierta. Entonces:

$$\mathcal{M} \models \phi(\overline{a}) \iff \mathcal{N} \models \phi(\overline{a}).$$

Demostración. Comencemos viendo un pequeño resultado que usaremos más tarde. Probemos, por inducción en los términos, que si $t(\overline{v})$ es un término y $\overline{b} \in M$, entonces, $t^{\mathcal{M}}(\overline{b}) = t^{\mathcal{N}}(\overline{b})$.

I) Si t es el símbolo de la constante c, entonces, $c^{\mathcal{M}} = c^{\mathcal{N}}$.

II) Si t es la variable x_i, entonces, $t^{\mathcal{M}}(\overline{b}) = b_i = t^{\mathcal{N}}(\overline{b})$.

III) Supongamos que t es de la forma $t = f(t_1, ..., t_n)$, con f el símbolo de cierta función de aridad n y $t_1, ..., t_n$ términos, de forma que $t_i^{\mathcal{M}}(\overline{b}) = t_i^{\mathcal{N}}(\overline{b})$, con $i = 1, ..., n$. Como tenemos que $\mathcal{M} \subseteq \mathcal{N}$, $f^{\mathcal{M}} = f^{\mathcal{N}} \mid M^n$. Por consiguiente,

$$\begin{aligned} t^{\mathcal{M}}(\overline{b}) &= f^{\mathcal{M}}(t_1^{\mathcal{M}}(\overline{b}), ..., t_n^{\mathcal{M}}(\overline{b})) \\ &= f^{\mathcal{N}}(t_1^{\mathcal{M}}(\overline{b}), ..., t_n^{\mathcal{M}}(\overline{b})) \\ &= f^{\mathcal{N}}(t_1^{\mathcal{N}}(\overline{b}), ..., t_n^{\mathcal{N}}(\overline{b})) \\ &= t^{\mathcal{N}}(\overline{b}). \end{aligned}$$

Visto esto, concluyamos nuestra prueba. Por inducción en las fórmulas:

I) Si ϕ es de la forma $t_1 = t_2$, con t_1, t_2 términos, entonces,

$$\mathcal{M} \models \phi(\overline{a}) \iff t_1^{\mathcal{M}}(\overline{a}) = t_2^{\mathcal{M}}(\overline{a}) \iff t_1^{\mathcal{N}}(\overline{a}) = t_2^{\mathcal{N}}(\overline{a}) \iff \mathcal{N} \models \phi(\overline{a}).$$

II) Si ϕ es de la forma $R(t_1, ..., t_n)$, donde R es el símbolo de una relación de aridad n y $t_1, ..., t_n$ son términos, entonces

$$\begin{aligned} \mathcal{M} \models \phi(\overline{a}) &\iff (t_1^{\mathcal{M}}(\overline{a}), ..., t_n^{\mathcal{M}}(\overline{a})) \in R^{\mathcal{M}} \\ &\iff (t_1^{\mathcal{M}}(\overline{a}), ..., t_n^{\mathcal{M}}(\overline{a})) \in R^{\mathcal{N}} \\ &\iff (t_1^{\mathcal{N}}(\overline{a}), ..., t_n^{\mathcal{N}}(\overline{a})) \in R^{\mathcal{N}} \\ &\iff \mathcal{N} \models \phi(\overline{a}). \end{aligned}$$

Queda ya probada la proposición para fórmulas atómicas.

Supongamos ahora que se tiene el resultado para ψ, siendo $\psi = \neg\phi$. Entonces,

$$\mathcal{M} \models \neg\phi(\overline{a}) \iff \mathcal{M} \not\models \psi(\overline{a}) \iff \mathcal{N} \not\models \psi(\overline{a}) \iff \mathcal{N} \models \phi(\overline{a}).$$

Finalmente, supongamos que se verifica la proposición para ψ_1 y ψ_2, siendo $\phi = \psi_1 \vee \psi_2$. Entonces,

$$\begin{array}{rcl} \mathcal{M} \models \phi(\overline{a}) & \iff & \mathcal{M} \models \psi_1(\overline{a}) \text{ o } \mathcal{M} \models \psi_2(\overline{a}) \\ & \iff & \mathcal{N} \models \psi_1(\overline{a}) \text{ o } \mathcal{N} \models \psi_2(\overline{a}) \\ & \iff & \mathcal{N} \models \phi(\overline{a}). \end{array}$$

Hemos probado así que la proposición es cierta para fórmulas atómicas. Además, si esta se verifica para ϕ y ψ, también lo hará para $\neg\phi$ y $\phi \vee \psi$. Como el conjunto de las fórmulas abiertas es el menor conjunto que contiene a las fórmulas atómicas y es cerrado bajo la negación y la disyunción, se tiene el resultado que deseábamos.

Q.E.D.

1.1.1. Isomorfismos y equivalencia elemental

En esta sección consideraremos estructuras que satisfagan el mismo conjunto de sentencias.

Definición 1.12. *Dado un lenguaje $\mathcal{L}$, diremos que dos $\mathcal{L}$-estructuras, $\mathcal{M}$ y $\mathcal{N}$, son elementalmente equivalentes, que escribiremos como $\mathcal{M} \equiv \mathcal{N}$, si verifican:*

$$\mathcal{M} \models \phi \iff \mathcal{N} \models \phi, \text{ para todas las sentencias } \phi \in \mathcal{L}.$$

Nota 1.8. Recordemos que llamamos sentencias o fórmulas cerradas de un lenguaje a las fórmulas que no contienen variables libres.

Denotaremos como $Th(\mathcal{M})$ al conjunto de las fórmulas cerradas que son verdaderas en $\mathcal{M}$, es decir, $Th(\mathcal{M}) = \{\phi \mid \phi \text{ fórmula cerrada y } \mathcal{M} \models \phi\}$. Este conjunto recibe el nombre de teoría completa de la $\mathcal{L}$-estructura $\mathcal{M}$.

Es sencillo ver por tanto que, $\mathcal{M} \equiv \mathcal{N} \iff Th(\mathcal{M}) = Th(\mathcal{N})$. Además, veamos que la teoría completa de una estructura $\mathcal{M}$ es invariante bajo isomorfismos. Para probarlo, usaremos de nuevo la técnica de inducción en la construcción de las fórmulas.

Teorema 1.1. *Sea $j : \mathcal{M} \to \mathcal{N}$ un isomorfismo de $\mathcal{L}$-estructuras. Entonces, $\mathcal{M}$ y $\mathcal{N}$ son elementalmente equivalentes, i.e, $\mathcal{M} \equiv \mathcal{N}$.*

Demostración. Probaremos por inducción en las fórmulas que $\mathcal{M} \models \phi(a_1, ..., a_n) \iff \mathcal{N} \models \phi(j(a_1), ..., j(a_n))$, para cualquier fórmula ϕ de $\mathcal{L}$.

Para ello, comprobemos antes que el comportamiento de los términos t es el esperado bajo isomorfismos. Veamos así que, si t es un término de variables libres $\overline{v} = (v_1, ..., v_n)$, entonces, $j(t^{\mathcal{M}}(\overline{a})) = t^{\mathcal{N}}(j(\overline{a}))$, siendo $j(\overline{a}) = (j(a_1), ..., j(a_n))$ con $\overline{a} = (a_1, ..., a_n) \in M^n$. Demostraremos este resultado previo por inducción en los términos.

I) Si $t = c$, entonces, $j(t^{\mathcal{M}}(\overline{a})) = j(c^{\mathcal{M}}) = c^{\mathcal{N}} = t^{\mathcal{N}}(j(\overline{a}))$.

II) Si $t = v_i$, entonces, $j(t^{\mathcal{M}}(\overline{a})) = j(a_i) = t^{\mathcal{N}}(j(\overline{a}))$.

III) Si $t = f(t_1, ..., t_m)$, entonces,

$$\begin{aligned} j(t^{\mathcal{M}}(\overline{a})) &= j(f^{\mathcal{M}}(t_1^{\mathcal{M}}(\overline{a}), ..., t_m^{\mathcal{M}}(\overline{a}))) \\ &= f^{\mathcal{N}}(j(t_1^{\mathcal{M}}(\overline{a})), ..., j(t_m^{\mathcal{M}}(\overline{a}))) \\ &= f^{\mathcal{N}}(t_1^{\mathcal{N}}(j(\overline{a})), ..., t_m^{\mathcal{N}}(j(\overline{a}))) \\ &= t^{\mathcal{N}}(j(\overline{a})). \end{aligned}$$

Tal y como dijimos anteriormente, procedamos a la demostración del teorema usando inducción en fórmulas.

I) Si $\phi(\overline{v})$ es de la forma $t_1 = t_2$, entonces,

$$\begin{aligned} \mathcal{M} \models \phi(\overline{a}) &\iff t_1^{\mathcal{M}}(\overline{a}) = t_2^{\mathcal{M}}(\overline{a}) \\ &\iff j(t_1^{\mathcal{M}}(\overline{a})) = j(t_2^{\mathcal{M}}(\overline{a})), \text{ pues } j \text{ es inyectivo} \\ &\iff t_1^{\mathcal{N}}(j(\overline{a})) = t_2^{\mathcal{N}}(j(\overline{a})) \\ &\iff \mathcal{N} \models \phi(j(\overline{a})). \end{aligned}$$

II) Si $\phi(\overline{v})$ es de la forma $R(t_1, ..., t_n)$, entonces,

$$\begin{aligned} \mathcal{M} \models \phi(\overline{a}) &\iff (t_1^{\mathcal{M}}(\overline{a}), ..., t_n^{\mathcal{M}}(\overline{a})) \in R^{\mathcal{M}} \\ &\iff (j(t_1^{\mathcal{M}}(\overline{a})), ..., j(t_n^{\mathcal{M}}(\overline{a}))) \in R^{\mathcal{N}} \\ &\iff (t_1^{\mathcal{N}}(j(\overline{a})), ..., t_n^{\mathcal{N}}(j(\overline{a}))) \in R^{\mathcal{N}} \\ &\iff \mathcal{N} \models \phi(j(\overline{a})). \end{aligned}$$

III) Si ϕ es de la forma $\neg\psi$, entonces,

$$\mathcal{M} \models \phi(\overline{a}) \iff \mathcal{M} \not\models \psi(\overline{a}) \iff \mathcal{N} \not\models \psi(j(\overline{a})) \iff \mathcal{N} \models \phi(j(\overline{a})).$$

IV) Si ϕ es de la forma $\psi_1 \vee \psi_2$, entonces,

$$\begin{aligned} \mathcal{M} \models \phi(\overline{a}) &\iff \mathcal{M} \models \psi_1(\overline{a}) \text{ o } \mathcal{M} \models \psi_2(\overline{a}) \\ &\iff \mathcal{N} \models \psi_1(j(\overline{a})) \text{ o } \mathcal{N} \models \psi_2(j(\overline{a})) \\ &\iff \mathcal{N} \models \phi(j(\overline{a})). \end{aligned}$$

V) Por último, si $\phi(\overline{v})$ es de la forma $\exists w\ (\psi(\overline{v}, w))$, entonces

$$\begin{aligned} \mathcal{M} \models \phi(\overline{a}) &\iff \mathcal{M} \models \psi(\overline{a}, b) \text{ para cierto } b \in M \\ &\iff \mathcal{N} \models \psi(j(\overline{a}), c) \text{ para cierto } c \in M \text{ pues } j \text{ es sobreyectiva} \\ &\iff \mathcal{N} \models \phi(j(\overline{a})). \end{aligned}$$

Tal y como queríamos demostrar. Q.E.D.

1.2. Teorías de primer orden

Definición 1.13. *Una teoría de primer orden $\mathcal{T}$ consiste en un conjunto de fórmulas cerradas de un determinado lenguaje $\mathcal{L}$ (de primer orden). Dichas fórmulas son conocidas como los axiomas no lógicos (o simplemente axiomas) de la teoría $\mathcal{T}$. Además, denotaremos al lenguaje de $\mathcal{T}$ como $L(\mathcal{T})$ y diremos que $\mathcal{T}$ es una $\mathcal{L}$-teoría.*

Una vez definido el concepto de Teoría, pasemos a conocer qué es un *modelo*.

Definición 1.14. *Dado un lenguaje $\mathcal{L}$ y una $\mathcal{L}$-teoría $\mathcal{T}$, decimos que una $\mathcal{L}$-estructura $\mathcal{M}$ es un modelo de $\mathcal{T}$, que escribiremos como $\mathcal{M} \models \mathcal{T}$, si se verifica que $\mathcal{M} \models \phi$, para toda sentencia ϕ perteneciente a los axiomas no lógicos de $\mathcal{T}$. Decimos que una teoría $\mathcal{T}$ es satisfacible si posee, al menos, un modelo.*

Ejemplo 1.11. Consideremos el siguiente conjunto:

$$\mathcal{T} = \{\forall x\ (x = 0),\ \exists x\ (x \neq 0)\}.$$

Dicho conjunto conforma una teoría. Sin embargo, como ambas fórmulas son contradictorias, no existe ningún modelo para dicha teoría. Decimos que no es satisfacible.

Definición 1.15. *Decimos que una clase de $\mathcal{L}$-estructuras $\mathcal{K}$ es una clase elemental si existe una $\mathcal{L}$-teoría $\mathcal{T}$ de forma que $\mathcal{K} = \{\mathcal{M} : \mathcal{M} \models \mathcal{T}\}$.*

Una forma sencilla de obtener teorías es considerar el conjunto, $Th(\mathcal{M})$, de la teoría completa de una cierta $\mathcal{L}$-estructura $\mathcal{M}$; noción introducida en un epígrafe anterior. En este caso en concreto, la clase elemental de modelos de $Th(\mathcal{M})$ coincide exactamente con la clase de $\mathcal{L}$-estructuras elementalmente equivalentes a $\mathcal{M}$.

Demos ahora algunos ejemplos tanto de teorías como de clases elementales de modelos básicos.

Ejemplo 1.12. I) Comencemos trabajando con los conjuntos infinitos.

Sea $\mathcal{L} = \emptyset$. Consideremos la teoría conformada por los siguientes axiomas.

$$\text{Para cada } n \in \mathbb{N},\ \phi_n = \exists x_1 \exists x_2 ... \exists x_n\ (\bigwedge_{i<j\leq n} x_i \neq x_j).$$

La fórmula ϕ_n afirma que existen al menos n elementos distintos. Una $\mathcal{L}$-estructura $\mathcal{M}$ será modelo de esta teoría si y solo si su conjunto subyacente M es infinito.

II) Estudiemos ahora los conjuntos ordenados.

En este caso $\mathcal{L} = \{<\}$, un símbolo de relación binaria. La clase de los órdenes lineales se axiomatiza como sigue:

a) $\forall x\ \neg(x < x)$,

b) $\forall x \forall y \forall z\ ((x < y\ \wedge\ y < z) \rightarrow x < z)$,

c) $\forall x \forall y\ (x < y\ \vee\ x = y\ \vee\ y < x)$.

Este conjunto de fórmulas conforman la teoría de conjuntos linealmente ordenados. Partiendo de esta como base, existen numerosas extensiones de dicha teoría interesantes. Por ejemplo, si añadimos a la lista de axiomas (no lógicos) el siguiente:

$$\forall x \forall y\ (x < y \rightarrow \exists z\ (x < z \wedge z < y))$$

obtenemos la teoría de los órdenes lineales densos.

Y, si en lugar del anterior, añadimos el siguiente axioma:

$$\forall x \exists y \ (x < y \wedge \forall z \ (x < z \rightarrow (z = y \vee y < z)))$$

obtenemos la teoría de los conjuntos lineales ordenados en los que cada elemento posee un único sucesor.

III) Relaciones de equivalencia.

Consideremos ahora $\mathcal{L} = \{E\}$, con E un símbolo de relación binaria. Los axiomas de la teoría de las relaciones de equivalencia son:

a) $\forall x \ E(x, x)$,

b) $\forall x \forall y \ (E(x, y) \rightarrow E(y, x))$,

c) $\forall x \forall y \forall z \ ((E(x, y) \wedge E(y, z)) \rightarrow E(x, z))$.

Como antes, estudiemos algunas extensiones atractivas. Añadiendo la siguiente fórmula:

$$\forall x \exists y \ (x \neq y \wedge E(x, y) \wedge \forall z (E(x, z) \rightarrow (z = x \vee z = y)))$$

obtenemos la teoría de las relaciones de equivalencia en las que cada clase de equivalencia tiene exactamente dos elementos.

IV) Siguiendo con el ejemplo 1.9 (donde se usó un lenguaje $\mathcal{L}_g$ propio de la Teoría de Grupos), ya advertimos que dichas fórmulas axiomatizaban la teoría de grupos. Para el caso de la clase de los grupos abelianos basta con añadir:

$$\forall x \forall y \ (x \cdot y = y \cdot x).$$

Consideramos ahora la fórmula:

$$\phi_n(x) = \underbrace{x \cdot x \cdots x = e}_{n \ veces}$$

la cual esencialmente expresa que $n \cdot x = e$. Podemos axiomatizar la clase de los grupos sin torsión añadiendo a los axiomas de la teoría de grupos el siguiente conjunto de fórmulas:

$$\{\forall x \ (x = e \vee \neg \phi_n(x) \ : \ n \geq 2\}.$$

También podemos axiomatizar la clase de los grupos cuyos elementos tienen, a lo sumo, orden $N > 0$. Esto se consigue añadiendo a la lista de axiomas la fórmula:

$$\forall x \bigvee_{n \leq N} \phi_n(x).$$

Un detalle a destacar es que esta misma idea no funciona para axiomatizar la clase de los grupos con torsión, pues la correspondiente fórmula tendría longitud infinita.

v) Anillos y cuerpos.

Adoptemos en este caso el lenguaje $\mathcal{L}_r = \{+, -, \cdot, 0, 1\}$ usual para anillos. (Añadimos el símbolo de la función binaria " $-$ " pues nos será de utilidad en el futuro). El conjunto de axiomas de la la clase de los cuerpos es:

Nota 1.9. Por separado, los siete primeros axiomas forman la teoría de los anillos.

a) Los axiomas correspondientes a la clase de los grupos aditivos abelianos,

b) $\forall x \forall y \forall z\ (x - y = z \leftrightarrow x = y + z)$,

c) $\forall x\ (x \cdot 0 = 0)$,

d) $\forall x \forall y \forall z\ (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$,

e) $\forall x\ (x \cdot 1 = 1 \cdot x = x)$,

f) $\forall x \forall y \forall z\ (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$,

g) $\forall x \forall y \forall z\ (x + y) \cdot z = (x \cdot z) + (y \cdot z))$,

h) $\forall x \forall y\ (x \cdot y = y \cdot x)$,

i) $\forall x\ (x \neq 0 \rightarrow \exists y\ (x \cdot y = 1))$,

j) $0 \neq 1$.

Si a esta lista le sumamos las fórmulas de la forma

$$\forall a_0 \forall a_1 ... \forall a_{n-1} \exists x\ (x^n + \sum_{i=0}^{n-1} a_i x^i = 0),\ \text{para cada } n \in \mathbb{N},$$

conseguimos los axiomas correspondientes a la clase de los cuerpos algebraicamente cerrados, teoría que denotaremos por ACF. Más aún, si añadimos el axioma:

$$\psi_p \equiv \forall x\ (\underbrace{x + \cdots + x}_{p\ veces} = 0),\ \text{para cierto primo } p,$$

que formaliza el hecho de que el cuerpo tiene característica p, entonces conseguimos la teoría de la clase de cuerpos algebraicamente cerrados y característica p, que denotaremos como ACF_p. Por último, la teoría de los cuerpos algebraicamente cerrados de característica 0, ACF_0, vendrá dada por $ACF + \{\neg\psi_p : p > 0\}$.

El estudio de las teorías ACF, ACF_p, ACF_0 es uno de los objetivos primordiales del presente trabajo.

1.2.1. Consecuencia Lógica

Definición 1.16. *Sean $\mathcal{T}$ y ϕ una teoría y una fórmula cerrada, respectivamente, de un determinado lenguaje $\mathcal{L}$. Decimos que ϕ es una consecuencia lógica de $\mathcal{T}$, que escribiremos como $\mathcal{T} \models \phi$, si se verifica que $\mathcal{M} \models \phi$, para cualquier $\mathcal{L}$-estructura $\mathcal{M}$ que sea modelo de $\mathcal{T}$.*

Veamos un par de ejemplos de consecuencias lógicas:

Ejemplo 1.13. i) Sea $\mathcal{L} = \{+, <, 0\}$ y sea $\mathcal{T}$ la teoría que de manera natural axiomatiza la clase de los grupos abelianos ordenados. Esto es, la teoría dada por los axiomas de grupo (aditivo) abeliano, los axiomas de orden lineal y el axioma $\forall x \forall y \forall z\,(x < y \to x + z < y + z)$. Entonces, $\phi \equiv \forall x\ (x \neq 0 \to x + x \neq 0)$ es una consecuencia lógica de $\mathcal{T}$.

Demostración. Supongamos que $\mathcal{M} = (M, +, <, 0)$ es un grupo abeliano ordenado. Sea $a \in M \setminus \{0\}$. Tenemos que demostrar que $a + a \neq 0$. Dado que $(M, <)$ es un conjunto lineal ordenado, tenemos que $a < 0 \vee 0 < a$. Si $a < 0$, entonces $a + a < 0 + a = a < 0$. Como $\neg(0 < 0)$, se tiene que $a + a \neq 0$. Por otro lado, si $0 < a$, entonces $0 < a = 0 + a < a + a$, obteniendo de nuevo que $a + a \neq 0$. Q.E.D.

ii) Sea $\mathcal{T}$ la teoría de los grupos en los que todos los elementos tienen orden 2. Entonces, $\phi \equiv \exists x \exists y \exists z\ (x \neq y \wedge y \neq z \wedge x \neq z)$ no es consecuencia lógica de $\mathcal{T}$.

Demostración. En este caso, basta observar que:

$$\mathbb{Z}/2\mathbb{Z} \models \mathcal{T} \quad \text{y} \quad \mathbb{Z}/2\mathbb{Z} \not\models \exists x_1 \exists x_2 \exists x_3\ (x_1 \neq x_2 \wedge x_2 \neq x_3 \wedge x_1 \neq x_3)$$

Q.E.D.

En la práctica matemática general, como se ilustra en los ejemplos anteriores, para demostrar que $\mathcal{T} \models \phi$ es suficiente con dar una prueba (esto es, "un argumento matemático") de que $\mathcal{M} \models \phi$ para un modelo $\mathcal{M}$ fijo pero arbitrario.

Mientras que para demostrar que $\mathcal{T} \not\models \phi$, basta con ofrecer un contraejemplo. Esto es, una estructura concreta que sea modelo de la teoría $\mathcal{T}$ en la que la fórmula ϕ resulte falsa.

1.3. Conjuntos definibles

Definición 1.17. *Sea $\mathcal{M}$ una cierta $\mathcal{L}$-estructura de dominio M. Decimos que un conjunto $X \subseteq M^n$ es definible si y solo si existe una fórmula $\phi(v_1, ..., v_n, w_1, ..., w_m)$ y $\overline{b} \in M^m$ tal que $X = \{\overline{a} \in M^n : \mathcal{M} \models \phi(\overline{a}, \overline{b})\}$. En este caso decimos que $\phi(\overline{v}, \overline{b})$ define X en $\mathcal{M}$.*

Asimismo, decimos que X es A-definible o definible sobre $A \subseteq M$ si existe una fórmula $\psi(\overline{v}, w_1, ..., w_l)$ y $\overline{b} \in A^l$ tal que $\psi(\overline{v}, \overline{b})$ define X en $\mathcal{M}$.

Ejemplo 1.14. Tomando $\mathcal{L}_r$ como lenguaje, esto es, el lenguaje de la Teoría de Anillos, demos algunos ejemplos de conjuntos que sean definibles:

i) Sea $\mathcal{M} = (\mathbb{N}, +, -, \cdot, 0, 1)$. El conjunto de los números primos es definible en $\mathcal{M}$. Basta considerar

$$\phi(x) \equiv x \neq 1 \wedge \forall y \forall z\,(x = y \cdot z \to y = 1 \vee z = 1)$$

II) Sea $\mathcal{M} = (\mathbb{Z}, +, -, \cdot, 0, 1)$ el anillo de los enteros. Consideremos $X = \{(m, n) \in \mathbb{Z}^2 \ : \ m < n\}$. El conjunto X es definible (concretamente, $\emptyset$-definible).

En efecto, el Teorema de Lagrange nos garantiza que todo entero no negativo puede expresarse como la suma de cuatro cuadrados. De este modo, si consideramos $\phi(x, y)$ la fórmula:

$$\exists z_1 \exists z_2 \exists z_3 \exists z_4 \ (z_1 \neq 0 \wedge y = x + z_1^2 + z_2^2 + z_3^2 + z_4^2),$$

entonces podemos expresar X como:

$$X = \{(m, n) \in \mathbb{Z}^2 \ : \ \mathcal{M} \models \phi(x, y)\}.$$

III) Sea $\mathcal{M} = (\mathbb{Q}, +, -, \cdot, 0, 1)$ el cuerpo de los número racionales. Si consideramos la siguiente fórmula:

$$\phi(x, y, z) = \exists a \exists b \exists c \ (x \cdot y \cdot z^2 + 1 + 1 = a^2 + x \cdot y^2 - y \cdot c^2),$$

podemos construir a partir de ella, la nueva fórmula $\psi(x)$

$$\psi(x) = \forall y \forall z \ ([\phi(y, z, 0) \wedge (\forall w \ (\phi(y, z, w) \rightarrow \phi(y, z, w + 1)))] \rightarrow \phi(y, z, x)).$$

De manera realmente sorprendente, puede demostrarse que $\psi(x)$ define el conjunto de los enteros en $\mathbb{Q}$. (Este notable resultado es obra de Julia Robinson, puede consultarse en [7]).

IV) Consideremos de nuevo $\mathcal{M} = (\mathbb{N}, +, -, \cdot, 0, 1)$. Los conjuntos definibles en esta estructura son muy complejos. De hecho, es bien conocido que existe una $\mathcal{L}_r$-fórmula $T(e, x, s)$ tal que $\mathcal{M} \models T(e, x, s)$ si y solo si la máquina de Turing con programa de código e para en, a lo más, s pasos sobre el dato de entrada x. Por tanto, la fórmula $\exists s \ T(e, x, s)$ define en $\mathcal{M}$ las computaciones de parada.

V) Sea $\mathcal{M} = (\mathbb{C}, +, -, \cdot, 0, 1)$ el cuerpo de los números complejos. En contraste con el ejemplo anterior, los conjuntos $X \subseteq \mathbb{C}$ definibles en esta estructura son muy simples: los conjuntos finitos o cofinitos. Este resultado se seguirá del teorema de eliminación de cuantificadores para la teoría ACF que demostraremos en el tercer capítulo.

2. Técnicas Básicas

2.1. El teorema de Compacidad

En este nuevo capítulo, trataremos sobre algunos de los conceptos más importantes de la Lógica Matemática. Escapa del alcance del presente trabajo dar una presentación completamente formal de todos estos conceptos. En su lugar, optamos por incluir una descripción intuitiva que permita entender el resto del desarrollo del trabajo.

Comencemos abordando la idea de *demostración formal*.

Consideremos $\mathcal{T}$ una cierta $\mathcal{L}$-teoría y ϕ una fórmula cerrada del lenguaje de $\mathcal{T}$. Para ver si $\mathcal{T} \models \phi$, es decir, comprobar si ϕ es *consecuencia lógica* de $\mathcal{T}$, deberíamos probar que ϕ es verdadera en cualquier modelo $\mathcal{M}$ de $\mathcal{T}$. La tarea de comprobar modelo a modelo si se satisface dicha fórmula es, en principio, bastante desalentadora. Sin embargo, en la práctica se comprueba que $\mathcal{T} \models \phi$ mediante una prueba o argumento matemático, a veces presentado de manera intuitiva y no completamente rigurosa, en la que se comprueba que ϕ es cierta en cada posible modelo de $\mathcal{T}$. Uno de los logros más importantes en Lógica Matemática fue la introducción de una definición de *prueba* estrictamente rigurosa, la cual recogía íntegramente la noción de consecuencia lógica.

De esta manera podríamos definir la demostración de una cierta sentencia ϕ de $\mathcal{T}$ como una sucesión finita de fórmulas (fórmulas de nuestro lenguaje base), llámense $\psi_1, \psi_2, ..., \psi_m$, tales que $\psi_m = \phi$ y además ψ_i o bien pertenece a $\mathcal{T}$ o bien se sigue mediante reglas lógicas simples a partir de $\psi_1, ..., \psi_{i-1}$. En el caso de que tal prueba exista, escribiremos $\mathcal{T} \vdash \phi$ y diremos que ϕ es un *teorema* de la teoría $\mathcal{T}$.

Nota 2.1. Con reglas lógicas simples nos referimos, por ejemplo, a:

I) Concluir $\phi \wedge \psi$ a partir de ϕ y ψ.

II) Concluir ϕ a partir de $\phi \wedge \psi$.

III) Concluir $\phi \vee \psi$ a partir de ϕ.

IV) Concluir ψ a partir de ϕ y $\phi \to \psi$ (modus ponens).

$\vdots$

V) Concluir ϕ directamente si ϕ es un axioma lógico (válido en cualquier estructura).

No indagaremos demasiado en los detalles de este sistema de prueba, pues de dicha tarea se encarga la Teoría de la Demostración (otra rama distinta de la Lógica Matemática). No obstante, sí enfatizaremos sobre algunos aspectos importantes del mismo.

- Las pruebas deben ser finitas.
- Una prueba ha de ser *adecuada*; es decir, si $\mathcal{T} \vdash \phi$, entonces, $\mathcal{T} \models \phi$.

- Si $\mathcal{T}$ es un conjunto finito de fórmulas cerradas, entonces existe un algoritmo que, dada una sucesión de fórmulas σ y una fórmula cerrada ϕ, concluya si σ es o no una prueba para ϕ en $\mathcal{T}$.

Nota 2.2. Es importante destacar que el último de los puntos anteriores no garantiza la existencia de un algoritmo que decida si $\mathcal{T} \vdash \phi$. Simplemente evidencia la existencia de un algoritmo que dada una sentencia ϕ y un candidato a prueba σ, compruebe la presunta prueba.

Definición 2.1. *Decimos que un lenguaje $\mathcal{L}$ es recursivo si existe un algoritmo que decida si una sucesión de símbolos dada es o no una fórmula de $\mathcal{L}$.*

Por otro lado, decimos que una $\mathcal{L}$-teoría $\mathcal{T}$ es recursiva si existe un algoritmo que, dada una $\mathcal{L}$-fórmula cerrada ϕ, decida si $\phi \in \mathcal{T}$ (esto es, si ϕ es un axioma de $\mathcal{T}$).

Proposición 2.1. Si $\mathcal{L}$ es un lenguaje recursivo y además $\mathcal{T}$ es una $\mathcal{L}$-teoría recursiva, entonces el conjunto $\{\phi : \mathcal{T} \vdash \phi\}$ es recursivamente enumerable, esto es, existe un algoritmo que, tomando una sentencia ϕ como entrada, pare si $\mathcal{T} \vdash \phi$, y no pare si $\mathcal{T} \nvdash \phi$.

Nota 2.3. Sin embargo, es importante recalcar que del hecho de que una teoría sea recursiva no se deduce, en general, que el conjunto de los teoremas de la teoría sea también computable. Como veremos más adelante, reservaremos el término de *teoría decidible* para aquellas teorías cuyo conjunto de teoremas resulte computable.

Introduzcamos ahora uno de los resultados más fundamentales de la Lógica Matemática: los conceptos de "demostrable en una teoría $\mathcal{T}$" y "consecuencia lógica de una teoría $\mathcal{T}$" coinciden para la lógica de primer orden.

Teorema 2.1. ***(Teorema de Completitud de Gödel, 1930)***

Sea $\mathcal{T}$ una $\mathcal{L}$-teoría y ϕ una fórmula cerrada de $\mathcal{L}$. Entonces, $\mathcal{T} \models \phi \iff \mathcal{T} \vdash \phi$.

El Teorema de Completitud nos proporciona un criterio para comprobar si una $\mathcal{L}$-teoría es satisfacible. Decimos que una $\mathcal{L}$-teoría $\mathcal{T}$ es *inconsistente* si $\mathcal{T} \vdash (\phi \wedge \neg\phi)$, para alguna $\mathcal{L}$-sentencia ϕ. En caso contrario, diremos que $\mathcal{T}$ es *consistente*.

Dado que nuestro sistema de prueba es adecuado, cualquier teoría satisfacible es consistente. Además, el Teorema de Completitud nos garantiza a su vez el recíproco.

Corolario 2.1. $\mathcal{T}$ es consistente $\iff$ $\mathcal{T}$ es satisfacible.

Demostración. $\boxed{\Longleftarrow}$ Tal y como dijimos previamente, esta implicación se tiene por las buenas propiedades del sistema de demostración.

$\boxed{\Longrightarrow}$ Para probar dicha implicación, supongamos que $\mathcal{T}$ no es satisfacible. De este modo, no existe ninguna estructura que sea modelo de $\mathcal{T}$; cumpliéndose por tanto que cualquier modelo de $\mathcal{T}$ será también modelo de $(\phi \wedge \neg\phi)$, para una fórmula cerrada ϕ. Entonces, $\mathcal{T} \models (\phi \wedge \neg\phi)$ y, por el Teorema de Completitud 2.1, deducimos que: $\mathcal{T} \vdash (\phi \wedge \neg\phi)$, lo que prueba que $\mathcal{T}$ es inconsistente. Q.E.D.

Un teorema que puede extraerse como consecuencia del Corolario anterior, y que es un resultado de importancia capital en el estudio de la Teoría de Modelos, es el siguiente:

Teorema 2.2. ***(Teorema de Compacidad, Gödel 1930-Maltsev 1936)*** *Sea $\mathcal{T}$ una $\mathcal{L}$-teoría. $\mathcal{T}$ es satisfacible $\iff$ todo subconjunto finito de $\mathcal{T}$ es satisfacible.*

Demostración. $\boxed{\Longrightarrow}$ De forma trivial, pues, si $\mathcal{T}$ es satisfacible, entonces, cualquier subconjunto suyo también lo será.

$\boxed{\Longleftarrow}$ Por otro lado, supongamos que $\mathcal{T}$ no es satisfacible. En ese caso, $\mathcal{T}$ es también inconsistente por el Teorema de Completitud 2.1. Sea σ la demostración de una contradicción de $\mathcal{T}$. Como σ es una prueba, en particular, ha de ser finita. Así, podemos deducir que la cantidad de fórmulas de $\mathcal{T}$ que aparecen en la prueba σ ha de ser finita. Por lo tanto, existe un subconjunto finito $\mathcal{T}_0 \subseteq \mathcal{T}$ tal que σ es la prueba de una contradicción de $\mathcal{T}_0$. Podemos concluir de esta manera que $\mathcal{T}_0$ es un subconjunto de $\mathcal{T}$ no satisfacible. Q.E.D.

2.2. Teorías Completas

Definición 2.2. *Decimos que una $\mathcal{L}$-teoría $\mathcal{T}$ es completa si es satisfacible y, para cualquier $\mathcal{L}$-fórmula cerrada ϕ, se verifica que o bien $\mathcal{T} \models \phi$ o bien $\mathcal{T} \models \neg\phi$.*

Nota 2.4. Por el teorema de Completitud, en la definición anterior podemos cambiar *satisfacible* por *consistente* y la condición *o bien $\mathcal{T} \models \phi$ o bien $\mathcal{T} \models \neg\phi$*, por la condición *o bien $\mathcal{T} \vdash \phi$ o bien $\mathcal{T} \vdash \neg\phi$*.

Consideremos una $\mathcal{L}$-estructura $\mathcal{M}$ cualquiera. Entonces, la teoría de $\mathcal{M}$

$$Th(M) = \{\phi \ : \ \phi \text{ es fórmula cerrada y } \mathcal{M} \models \phi\}$$

es un ejemplo de una teoría completa.

Normalmente, no es baladí determinar con exactitud cuáles son las sentencias pertenecientes a $Th(M)$. Por ello, para comprender mejor el conjunto $Th(M)$, la clave está en buscar una nueva $\mathcal{L}$-teoría $\mathcal{T}$ más simple de forma que $\mathcal{M} \models \mathcal{T}$ y que $\mathcal{T}$ sea completa. Esto funciona bien pues, de esta forma,

$$\mathcal{M} \models \phi \iff \mathcal{T} \models \phi \iff \mathcal{T} \vdash \phi,$$

dado que si $\mathcal{T} \not\models \phi$, entonces $\mathcal{T} \models \neg\phi$ por ser $\mathcal{T}$ completa, y $\mathcal{M} \models \neg\phi$.

De hecho, para cerrar el presente capítulo, aplicaremos esta idea para obtener una axiomatización natural e informativa del cuerpo de los números complejos $(\mathbb{C}, +, -, \cdot, 0, 1)$. Por el teorema fundamental del Álgebra 0.2, sabemos que $\mathbb{C}$ es un cuerpo algebraicamente cerrado de característica cero. Esto es, $\mathbb{C} \models ACF_0$. Si somos capaces de demostrar que la teoría ACF_0 es completa, entonces, aplicando la idea anterior, tendríamos que $Th(\mathbb{C}) \equiv ACF_0$, obteniendo así la deseada axiomatización de $\mathbb{C}$.

Nota 2.5. Dadas dos teorías en el mismo lenguaje, $\mathcal{T}_1$ y $\mathcal{T}_2$, escribiremos $T_1 \equiv T_2$ para significar que las teorías son *deductivamente equivalentes*, esto es, poseen el mismo conjunto de teoremas (o, alternativamente, consecuencias lógicas).

El nuevo problema que debemos abordar ahora es: ¿cómo podemos demostrar que una determinada teoría $\mathcal{T}$ es completa? ¿Qué técnicas básicas nos ofrece la Teoría de Modelos para ello?

Cerramos este capítulo con la exposición de una de esas técnicas básicas. Veremos que una aplicación del Teorema de Compacidad 2.2 nos ofrece un interesante método para demostrar que varias teorías naturales son completas vía la noción de *teoría λ-categórica*.

Definición 2.3. *Sean λ un cardinal infinito y $\mathcal{T}$ una teoría. Decimos que $\mathcal{T}$ es λ-categórica si cualesquiera dos modelos de $\mathcal{T}$ de cardinal λ son isomorfos.*

Entendamos mejor esto con un par de ejemplos simples.

Ejemplo 2.1.

- Si consideramos $\mathcal{L}$ como el lenguaje vacío (esto es, $\mathcal{L} = \emptyset$), entonces la $\mathcal{L}$-teoría correspondiente a un conjunto infinito es λ-categórica para cualquier cardinal λ.
- Considérese en este caso $\mathcal{L} = \{E\}$, con E el símbolo de una relación binaria. Denotemos por $\mathcal{T}$ la $\mathcal{L}$-teoría correspondiente a una relación de equivalencia de exactamente dos clases y con cada una de ellas infinita. Es sencillo observar que, dados dos modelos cualesquiera numerables de $\mathcal{T}$, estos son isomorfos. Por lo tanto, la teoría $\mathcal{T}$ es $\aleph_0$-categórica. Por otro lado, $\mathcal{T}$ no es λ-categórica para $\lambda > \aleph_0$. Veamos esto con más detenimiento.

  Sea $\mathcal{M}_0$ un modelo de la teoría en el que ambas clases de equivalencia tengan cardinal λ, y denotemos por $\mathcal{M}_1$ a un modelo cuyas clases tengan cardinal λ y $\aleph_0$, respectivamente. Es claro que $\mathcal{M}_0$ y $\mathcal{M}_1$ tienen cardinal λ y, sin embargo, $\mathcal{M}_0$ y $\mathcal{M}_1$ no son isomorfos.

Recordemos que $|\mathcal{L}|$ denota el cardinal de un lenguaje, esto es, el máximo entre $\aleph_0$ y el cardinal de los símbolos no lógicos de $\mathcal{L}$.

Proposición 2.2. Sea $\mathcal{T}$ una $\mathcal{L}$-teoría con modelos infinitos. Si $|\mathcal{L}| \leq \lambda$, siendo λ un cardinal infinito, entonces existe un modelo de $\mathcal{T}$ con cardinal exactamente λ.

Demostración. Véase la proposición 2.2.2 del libro [6]. Q.E.D.

Teorema 2.3. ***(Test de Vaught)*** *Sea $\mathcal{T}$ una teoría satisfacible, sin modelos finitos y λ-categórica para un cierto cardinal $\lambda \geq |\mathcal{L}|$. Entonces, $\mathcal{T}$ es una teoría completa.*

Demostración. Por reducción al absurdo, supongamos que $\mathcal{T}$ no es una teoría completa. De este modo, deberá existir una fórmula cerrada ϕ de forma que $\mathcal{T} \not\models \phi$ y además $\mathcal{T} \not\models \neg\phi$. Dado que se cumple que $\mathcal{T} \not\models \psi$ si y solo si $\mathcal{T} \cup \{\neg\psi\}$ es satisfacible, las teorías $\mathcal{T}_0 = \mathcal{T} \cup \{\phi\}$ y $\mathcal{T}_1 = \{\neg\phi\}$ son ambas satisfacibles. Además, como $\mathcal{T}$ no tiene modelos finitos, todos los modelos de $\mathcal{T}_0$ y $\mathcal{T}_1$ han de ser infinitos. Por la proposición

2.2, existen $\mathcal{M}_0$ y $\mathcal{M}_1$ modelos de $\mathcal{T}_0$ y $\mathcal{T}_1$, respectivamente, ambos de cardinal λ. Como $\mathcal{M}_0 \models \phi$ pero $\mathcal{M}_1 \not\models \phi$, no existe equivalencia elemental entre las estructuras y, por el teorema 1.1, deducimos que $\mathcal{M}_0$ y $\mathcal{M}_1$ no son isomorfos. Contradicción, pues teníamos que $\mathcal{T}$ es λ-categórica. Q.E.D.

Por lo tanto, el test de Vaught nos proporciona un método para demostrar que ACF_0 es completa: demostrar que la teoría es λ-categórica para algún cardinal infinito. Antes de estudiar este resultado fundamental, tratamos el caso de los grupos abelianos libres de torsión divisibles como un ejemplo previo del uso del test de Vaught.

Sea $\mathcal{L} = \{+, 0\}$ un lenguaje adecuado para los grupos aditivos y consideremos $\mathcal{T}$ la $\mathcal{L}$-teoría correspondiente a la clase de los grupos abelianos libres de torsión y divisibles. Los axiomas de dicha teoría están conformados por:

- Los axiomas de la teoría de grupos abelianos (que describimos anteriormente),
- Las siguientes fórmulas:

  I) $\forall x\ (x \neq 0\ \rightarrow \underbrace{x + \cdots + x}_{n\ veces} \neq 0)$, con $n = 1, 2, ...$

  II) $\forall y \exists x\ (\underbrace{x + \cdots + x}_{n\ veces} = y)$, con $n = 1, 2, ...$

Proposición 2.3. La teoría correspondiente a la clase de grupos abelianos libres de torsión y divisibles es λ-categórica para todo $\lambda > \aleph_0$.

Nota 2.6. Por comodidad, llamaremos (durante el transcurso de la siguiente prueba) $\mathcal{T}$ a la teoría correspondiente a la clase de grupos abelianos libres de torsión y divisibles.

Demostración. En primer lugar, veamos que los modelos de $\mathcal{T}$ son esencialmente espacios vectoriales sobre el cuerpo $\mathbb{Q}$ de los números racionales.

Por una parte, no es difícil ver que, dado un $\mathbb{Q}$-espacio vectorial V, el grupo aditivo subyacente de V es un modelo de $\mathcal{T}$.

Por otro lado, si $G \models \mathcal{T}$, con $g \in G$ y $n \in \mathbb{N}$ con $n > 0$, podemos garantizar la existencia de un elemento $h \in G$ cumpliendo que $nh = g$. Si $g = nk$ entonces $n(h-k) = 0$. Dado que G es un grupo libre de torsión, existe un único elemento $h \in G$ tal que $nh = g$. Llamemos por tanto a este elemento g/h. Así, podemos entender G como un $\mathbb{Q}$-espacio vectorial bajo la acción $\frac{m}{n}g = m(g/n)$.

Como dos $\mathbb{Q}$-espacios vectoriales son isomorfos si y solo si sus dimensiones coinciden, tenemos que los modelos de $\mathcal{T}$ están determinados bajo isomorfismos por su dimensión. Si el cardinal de G es λ, con λ no numerable, entonces, G tiene necesariamente dimensión λ. Así, para $\lambda > \aleph_0$, cualesquiera dos modelos de $\mathcal{T}$ de cardinal λ son isomorfos. Q.E.D.

Observación 2.1. Es importante percatarse de que $\mathcal{T}$ no es, sin embargo, $\aleph_0$-categórica. Ciertamente, existen $\aleph_0$ modelos de $\mathcal{T}$ que no son isomorfos entre sí, pues corresponden a $\mathbb{Q}$-espacios vectoriales de dimensiones $1, 2, ..., \aleph_0$, respectivamente.

Corolario 2.2. La teoría de los grupos abelianos libres de torsión y divisibles anteriormente descrita es completa.

Puede aplicarse un razonamiento similar para la teoría de los cuerpos algebraicamente cerrados. Considérese por tanto ACF_p la teoría de los cuerpos algebraicamente cerrados de característica p (con p cero o un número primo).

Proposición 2.4. Sea $p = 0$ o primo. La teoría ACF_p es λ-categórica para cualquier cardinal λ no numerable.

Demostración. Esto es esencialmente una consecuencia del análisis de Steinitz de los cuerpos algebraicamente cerrados. De hecho, este análisis demuestra que dos cuerpos algebraicamente cerrados son isomorfos si y solo si tienen igual característica y grado de transcendencia (véase 0.1). Un cuerpo algebraicamente cerrado con grado de transcendencia κ tiene cardinal $\kappa + \aleph_0$. Si $\lambda > \aleph_0$, un cuerpo algebraicamente cerrado de cardinal λ tendrá también pues grado de transcendencia λ. Así, cualesquiera dos cuerpos algebraicamente cerrados de igual cardinal no numerable e igual característica serán isomorfos. Q.E.D.

Observación 2.2. Obsérvese que la teoría ACF_p tiene

- $\aleph_0$ modelos numerables no isomorfos dos a dos (correspondientes a los grados de trascendencia $0, 1, \ldots, \aleph_0$),
- un único modelo (salvo isomorfismo) para cada cardinal no numerable λ.

Esto es, ACF_p es λ-categórica para cualquier cardinal λ no numerable pero no $\aleph_0$-categórica.

Corolario 2.3. Sea $p = 0$ o primo. La teoría ACF_p es completa.

Demostración. Aplicaremos el test de Vaught. Claramente, ACF_p es satisfacible. Por otra parte, un cuerpo algebraicamente cerrado $\mathcal{K}$ es siempre infinito. De hecho, si $\mathcal{K} = \{a_0, \ldots, a_n\}$ entonces el polinomio $1 + (x - a_0) \cdot (x - a_1) \cdot \cdots \cdot (x - a_n)$ no tendría ninguna raíz en $\mathcal{K}$. Por tanto, ACF_p no tiene modelos finitos. Finalmente, por el Corolario anterior, se sigue que ACF_p es λ-categórica. En consecuencia, por el test de Vaught (teorema 2.3), la teoría ACF_p es completa.

Q.E.D.

El hecho de que la teoría ACF_p sea completa tendrá consecuencias importantes para el estudio de los cuerpos algebraicamente cerrados. Por ejemplo, podemos inferir la existencia de un algoritmo para decidir si una sentencia del lenguaje de la Teoría de Anillos es o no verdadera en el cuerpo de los complejos $\mathbb{C}$.

Definición 2.4. *Sea $\mathcal{T}$ una $\mathcal{L}$-teoría . Decimos que $\mathcal{T}$ es decidible si existe un algoritmo que, dada una formula cerrada ϕ de $\mathcal{L}$, concluya si $\mathcal{T} \models \phi$ o no.*

Nota 2.7. De nuevo, por el teorema de Completitud, en la definición anterior podemos sustituir la condición $\mathcal{T} \models \phi$ por $\mathcal{T} \vdash \psi$.

Lema 2.1. Sea $\mathcal{T}$ una teoría recursiva y completa en un lenguaje $\mathcal{L}$ recursivo. Entonces, $\mathcal{T}$ es decidible.

Demostración. Por hipótesis tenemos que:

- Por ser $\mathcal{T}$ satisfacible (ya que es completa), los conjuntos $A = \{\phi \ : \ \mathcal{T} \models \phi\}$ y $B = \{\phi \ : \ \mathcal{T} \models \neg\phi\}$ verifican que $A \cap B = \emptyset$, i.e., son disjuntos.
- Por ser $\mathcal{T}$ completa, $A \cup B$ coincide con el conjunto de todas las fórmulas cerradas de $\mathcal{L}$.
- El hecho de que $\mathcal{T}$ sea recursiva unido a que $\mathcal{L}$ también lo sea, nos permite poder usar la proposición 2.1, que nos garantiza que los conjuntos A y B son recursivamente enumerables.

Como cualquier conjunto recursivamente enumerable cuyo complementario es a su vez recursivamente enumerable es recursivo, tenemos que, en particular, los conjuntos A y B son recursivos. Con esto deducimos que $\mathcal{T}$ es decidible. Q.E.D.

De forma informal, para decidir si ϕ es consecuencia lógica de una teoría que sea completa y recursiva, se enumeran posibles pruebas en $\mathcal{T}$ hasta encontrar una demostración de ϕ o, en su defecto, de $\neg\phi$. Como $\mathcal{T}$ es satisfacible, es imposible encontrar ambas pruebas a la vez. Sin embargo, como $\mathcal{T}$ es completa, antes o después, encontraremos alguna de las dos pruebas.

Corolario 2.4. Sea $p = 0$ o un número primo. Entonces, ACF_p es decidible. En particular, $Th(\mathbb{C})$, la teoría completa del cuerpo de los números complejos, es decidible.

La completitud de ACF_p puede contemplarse también como una versión del principio de Lefschetz, un resultado de geometría algebraica. En efecto, se tiene que:

Corolario 2.5. Sea ϕ una fórmula cerrada del lenguaje de la Teoría de Anillos. Son equivalentes:

I) ϕ es verdadera en $\mathbb{C}$.

II) ϕ es verdadera en cualquier cuerpo algebraicamente cerrado de característica cero.

III) ϕ es verdadera en algún cuerpo algebraicamente cerrado de característica cero.

IV) Existen primos p arbitrariamente grandes de forma que ϕ es verdadera en algún cuerpo algebraicamente cerrado de característica p.

V) Existe un cierto m tal que, para todo primo $p > m$, ϕ es verdadera en todos los cuerpos algebraicamente cerrados de característica p.

Demostración. La implicación $V) \Rightarrow IV)$ es trivial. Además, las equivalencias entre $I), II)$ y $III)$ se deducen de la completitud de ACF_0.

Comencemos probando que $II) \Rightarrow V)$. Supongamos que $ACF_0 \models \phi$. Es una consecuencia del Teorema de Compacidad que existe un conjunto finito $\triangle \subseteq ACF_0$ de forma que $\triangle \models \phi$. Así, tomando un p primo lo suficientemente grande, se tiene

que $ACF_p \models \triangle$. De este modo, concluimos que $ACF_p \models \phi$, para todo primo p lo suficientemente grande.

Pasemos ahora a ver que $IV) \Rightarrow II)$. Supongamos que $ACF_0 \not\models \phi$. Dado que ACF_0 es completa, $ACF_0 \models \neg\phi$. Siguiendo el argumento anteriormente expuesto, se sigue que $ACF_p \models \neg\phi$, para un p primo lo suficientemente grande. Lo que está en contradicción con $IV)$.

Q.E.D.

Es bien conocido que el Corolario anterior tiene una consecuencia realmente sorprendente: permite dar una elegante prueba del siguiente teorema.

Teorema 2.4. *Toda función polinómica inyectiva de $\mathbb{C}^n$ en $\mathbb{C}^n$ es sobreyectiva.*

Demostración. Véase el teorema 2.2.11 del libro [6]. Q.E.D.

El análisis anterior de las teorías ACF_p no es autocontenido, pues exige el uso de resultados algebraicos no triviales (cuyas pruebas escapan del alcance del presente trabajo). Sin embargo, y este es el objetivo principal del trabajo, en el siguiente capítulo daremos una prueba autocontenida basada en una nueva (y muy importante) técnica básica de la Teoría de Modelos: el método de eliminación de cuantificadores.

3. Eliminación de cuantificadores

En este capítulo introducimos, en un contexto general, el método de la eliminación de cuantificadores, una herramienta básica en el estudio de la Teoría de Modelos, y aplicaremos esta técnica para obtener una nueva prueba de la completitud y decibilidad de las teorías ACF_p, con $p = 0$ o primo.

3.1. Conjuntos de eliminación

Cuando nos encontramos trabajando con las fórmulas de un lenguaje $\mathcal{L}$, puede ocurrir que dos de ellas, ϕ y ψ, admitan el mismo significado en una cierta $\mathcal{L}$-estructura $\mathcal{M}$, o en una clase de $\mathcal{L}$-estructuras en general, como podrían ser los modelos de una determinada $\mathcal{L}$-teoría. Estudiemos algunos ejemplos donde ocurra este fenómeno:

Ejemplo 3.1.

- Considérese el cuerpo ordenado de los números reales. Tienen el mismo significado las fórmulas:

  I) $\phi \;=\; x \geq 0$.

  II) $\psi \;=\; \exists y\ (x = y^2)$.

  La primera de ellas se refiere a la propiedad de ser mayor o igual a cero. Por su parte, la segunda de ellas significa ser el cuadrado de un número.

  Un detalle de vital relevancia que hay que tener en cuenta es la importancia del conjunto ambiente en el que estemos trabajando. Mientras que en $\mathbb{R}$ se verifica $\phi \iff \psi$, en $\mathbb{Q}$ sólo podríamos garantizar que $\psi \Rightarrow \phi$.

- Considérese ahora el anillo ordenado de los números enteros. Coinciden en significado:

  I) $\phi \;=\; x \geq 0$.

  II) $\psi \;=\; \exists y_1 \exists y_2 \exists y_3 \exists y_4\ (x = \sum_{i=1}^{4} y_i^2)$.

  De nuevo la primera fórmula significa ser positivo, mientras que la segunda significa "ser suma de cuatro cuadrados".

Obsérvese que en ambos casos se ha establecido la *equivalencia de significado* entre una fórmula con cuantificadores y una fórmula abierta, y que esta equivalencia no es necesariamente cierta para cualquier estructura $\mathcal{M}$, sino que solo puede garantizarse para ciertas estructuras o clases de estructuras.

A partir de este momento, cuando hagamos referencia a una teoría $\mathcal{T}$, supondremos que es una teoría consistente (y no necesariamente completa) de un determinado lenguaje que supondremos numerable.

Definición 3.1. *Decimos que dos fórmulas $\phi(\bar{x})$ y $\psi(\bar{x})$ son equivalentes con respecto a una teoría $\mathcal{T}$ (o simplemente $\mathcal{T}$-equivalentes), y lo denotaremos como $\phi \sim_{\mathcal{T}} \psi$, si se cumple que*

$$\mathcal{T} \models \forall \bar{x}\ (\phi(\bar{x}) \leftrightarrow \psi(\bar{x}))$$

o, equivalentemente,

$$\phi(\mathcal{M}^n) = \psi(\mathcal{M}^n), \text{ para todo } \mathcal{M} \text{ modelo de } \mathcal{T},$$

donde $\theta(\mathcal{M}^n)$ denota el subconjunto de M^n definido por la fórmula $\theta(\bar{x})$.

Nuestro siguiente paso será definir uno de los conceptos clave de esta sección, la noción de *conjunto de eliminación*. Además, este es un concepto que surge de manera natural tras conocer la idea de equivalencia entre fórmulas.

Definición 3.2. *Un conjunto de eliminación para una teoría $\mathcal{T}$ es un conjunto F de $\mathcal{L}$-fórmulas que cumple que cada fórmula ϕ de $\mathcal{L}$ es $\mathcal{T}$-equivalente a una determinada combinación Booleana de fórmulas de F.*

Evidentemente, siempre podemos considerar como conjunto de eliminación de $\mathcal{T}$ el conjunto de todas las $\mathcal{L}$-fórmulas. Sin embargo, este caso es trivial y no aporta ninguna información nueva. Razonablemente, el interés reside en encontrar conjuntos F de eliminación más simples, lo que tendrá numerosas aplicaciones en cuanto al estudio de la teoría en cuestión.

En particular, cuando el conjunto de fórmulas atómicas de $\mathcal{L}$ es un conjunto de eliminación para $\mathcal{T}$, decimos que $\mathcal{T}$ posee eliminación de cuantificadores en $\mathcal{L}$ (recordemos que, por el algoritmo de paso a forma normal disyuntiva, toda fórmula abierta puede ser reescrita como una combinación Boolenana de fórmulas atómicas). Formalicemos esta idea:

Definición 3.3. *Sea $\mathcal{T}$ una $\mathcal{L}$-teoría. Decimos que $\mathcal{T}$ tiene eliminación de cuantificadores en $\mathcal{L}$ si, y solo si, cada fórmula $\phi(\bar{x}) \in \mathcal{L}$ es equivalente en $\mathcal{T}$ a una fórmula $\psi(\bar{x})$ sin cuantificadores de $\mathcal{L}$, es decir, a una fórmula abierta.*

En principio, la propiedad de tener eliminación de cuantificadores puede parecer que queda reservada para teorías muy concretas. Sin embargo, esta es una idea totalmente errónea, pues cualquier $\mathcal{L}$-teoría $\mathcal{T}$ consigue la eliminación de cuantificadores en una extensión de $\mathcal{L}$ adecuada. Sin embargo, sí es cierto que, dependiendo de la teoría en cuestión, en ocasiones se debe recurrir a lenguajes algo complejos.

Introduzcamos un procedimiento que justifique lo anterior: «Tomemos $\mathcal{L} = \mathcal{L}_0$ y $\mathcal{T} = \mathcal{T}_0$. Ampliemos $\mathcal{L}_0$ añadiendo un nuevo símbolo de relación R_ϕ para cada fórmula $\phi(\bar{x})$ de $\mathcal{L}_0$, consiguiendo un nuevo lenguaje que denotaremos como $\mathcal{L}_1$. Por otro lado, añadiremos a $\mathcal{T}_0$ la siguiente fórmula cerrada

$$\forall \bar{x}\ (\phi(\bar{x}) \leftrightarrow R_\phi(\bar{x})) \text{ para cada fórmula } \phi(\bar{x}),$$

obteniendo una nueva teoría $\mathcal{T}_1$. Es claro que las fórmulas atómicas de $\mathcal{L}_1$ forman un conjunto de eliminación en $\mathcal{T}_1$ para las fórmulas de $\mathcal{L}_0$. Repitiendo dicho proceso el

número de veces necesarias, conseguimos finalmente un lenguaje $\mathcal{L}' \supseteq \mathcal{L}$ y una teoría $\mathcal{T}'$ de $\mathcal{L}'$ (que es extensión de $\mathcal{T}$) que cuenta con eliminación de cuantificadores (en $\mathcal{L}'$)».

Desafortunadamente, este no es un proceso que pueda llevarse tan fácilmente a la práctica. Realmente, lo óptimo sería que, dada una $\mathcal{L}$-teoría $\mathcal{T}$, comprobásemos directamente si $\mathcal{T}$ tiene eliminación de cuantificadores en $\mathcal{L}$, o, en su defecto, determinar la menor extensión $\mathcal{L}' \supseteq \mathcal{L}$ donde $\mathcal{T}$ sí tenga eliminación de cuantificadores (o un conjunto de eliminación de fórmulas de $\mathcal{L}'$ lo suficientemente simple).

Puede ocurrir que, en primera instancia, no se adviertan las ventajas de los conjuntos de eliminación. Hecho nada más lejos de la realidad, pues estos nos abren un nuevo abanico de posibilidades en cuanto al estudio de las teorías se refiere. Por ello, uno de los objetivos fundamentales, tanto de esta como de la siguiente sección, será introducir algunas de las consecuencias y aplicaciones más importantes que estos nos ofrecen.

I) La principal, o al menos lo es históricamente, es la obtención de pruebas de decibilidad.

Nota 3.1. Recordemos que una teoría $\mathcal{T}$ es decidible si existe un algoritmo que, dada una fórmula cerrada ϕ de $\mathcal{L}$, determine si $\mathcal{T} \models \phi$ o no.

Supongamos que F es un conjunto de eliminación para $\mathcal{T}$ y que se dispone de:

- Un procedimiento efectivo mediante el cual, cualquier $\mathcal{L}$-fórmula cerrada pueda expresarse como combinación Booleana de sentencias de F.
- Un algoritmo que, dada una combinación Booleana de fórmulas cerradas de F, concluya si es consecuencia lógica o no de la teoría $\mathcal{T}$.

Entonces, se deduce que $\mathcal{T}$ es decidible, consiguiendo además un *algoritmo de decisión* (basta aplicar sucesivamente los dos procedimientos anteriores).

II) Otra aplicación muy importante de la eliminación de cuantificadores de una teoría $\mathcal{T}$ es que nos permite describir los conjuntos $\mathcal{L}$-definibles en un modelo de $\mathcal{T}$. Supongamos que que F es un conjunto de eliminación de para $\mathcal{T}$. Entonces, los conjuntos $\mathcal{L}$-definibles de un modelo $\mathcal{M}$ de $\mathcal{T}$ se reducen a

$$\phi(\mathcal{M}^n, \bar{a}) = \{\bar{b} : \mathcal{M} \models \phi(\bar{b}, \bar{a})\},$$

donde $\phi(\bar{v}, \bar{w})$ es una combinación Booleana finita de fórmulas de F y $\bar{a} \in \mathcal{M}$ son los parámetros de dicha definición. Además, si $\mathcal{T}$ tiene eliminación de cuantificadores en $\mathcal{L}$, los conjuntos $\mathcal{L}$-definibles de un modelo $\mathcal{M}$ de $\mathcal{T}$ son de la forma

$$\phi(\mathcal{M}^n, \bar{a}),$$

donde $\phi(\bar{v}, \bar{w})$ es una fórmula abierta y $\bar{a} \in \mathcal{M}$.

Por tanto, si podemos describir de manera informativa los conjuntos definibles por fórmulas sin cuantificadores, tendremos también una descripción de los conjuntos definibles en la estructuras usando fórmulas de complejidad tan grande como queramos.

3.2. Reducción a fórmulas sencillas

Ya conocemos, aunque de forma genérica, algunas de las virtudes que poseen las teorías con eliminación de cuantificadores. En las secciones venideras, nos centraremos en el caso de algunas teorías concretas, sin embargo, en esta sección trataremos una cuestión distinta. ¿Cómo sabemos si una teoría $\mathcal{T}$ tiene eliminación de cuantificadores en un determinado lenguaje $\mathcal{L}$?

Para responder a esto, deberíamos estudiar si, dada una fórmula $\phi(\bar{v})$ de $\mathcal{L}$ cualquiera, existe otra $\mathcal{L}$-fórmula $\phi'(\bar{v})$ sin cuantificadores cumpliéndose que

$$\phi(\bar{v}) \sim_{\mathcal{T}} \phi'(\bar{v}).$$

Esto puede parecer una tarea imposible, pues la diversidad de las fórmulas de un lenguaje puede ser extremadamente grande. Sin embargo, introduciremos un resultado que nos permitirá reducir el estudio de la eliminación de cuantificadores a una serie de fórmulas muy concretas.

Lema 3.1. Sea $\mathcal{T}$ una determinada $\mathcal{L}$-teoría. Para demostrar que $\mathcal{T}$ admite eliminación de cuantificadores sobre $\mathcal{L}$, es suficiente con demostrar que las fórmulas de la forma

$$\exists w \ (\bigwedge_{i \leq r} \alpha_i(\bar{v}, w)),$$

son equivalentes a una fórmula abierta, donde cada $\alpha_i(\bar{v}, w)$ es una fórmula atómica o su negación y w es una variable que aparece en $\alpha_i(\bar{v}, w)$, para todo $i \leq r$.

Demostración. Sea $\phi(\bar{v})$ una fórmula genérica con cuantificadores. Podemos suponer por tanto que será de la forma

$$Q_1 w_1 \cdots Q_m w_m \ \alpha(\bar{v}, \bar{w}),$$

donde $\bar{w} = (w_1, ..., w_m)$, Q_j denota un cuantificador (ya sea el existencial $\exists$ o el universal $\forall$) para $1 \leq j \leq m$ y $\alpha(\bar{v}, \bar{w})$ es una fórmula abierta. Incluso más, aplicando un algoritmo de reescritura en forma normal disyuntiva si fuese necesario, podemos suponer que $\alpha(\bar{v}, \bar{w})$ es una disyunción de conjunciones de fórmulas atómicas y negaciones de atómicas.

Nuestra estrategia consistirá en eliminar, en primer lugar, el cuantificador Q_m y, posteriormente, repetir el proceso hasta alcanzar el resultado deseado. Es decir, eliminar por completo la cadena de cuantificadores.

Sin pérdida de generalidad, podemos suponer que $Q_m = \exists$, pues tal y como se vio en el primer capítulo el símbolo $\forall$ no es más que una abreviación de $\neg\exists\neg$. De este modo, para obtener un procedimiento de eliminación de cuantificadores, nos podemos reducir al caso

$$\exists w \ \alpha(\bar{v}, w),$$

donde α es una disyunción de conjunciones de fórmulas atómicas y negaciones.

Ahora bien, puesto el cuantificador existencial verifica las propiedades de distributividad en relación a la disyunción, tenemos que

$$\exists w\ (\beta \vee \gamma) \text{ es equivalente a } (\exists w\ \beta) \vee (\exists w\ \gamma).$$

Por tanto, también podemos suponer sin pérdida de generalidad que α es simplemente una conjunción de fórmulas atómicas y negaciones.

En resumen, para obtener un procedimiento de eliminación de cuantificadores para cualquier fórmula del lenguaje, podemos reducirnos al caso:

$$\exists w\ (\bigwedge_{i\leq r} \alpha_i(\bar{v}, w)),$$

donde $\alpha_i(\bar{v}, w)$ es una fórmula atómica o su negación. Tan solo nos resta justificar que podemos suponer que además la variable w aparece en $\alpha_i(\bar{v}, w)$ para todo $i \leq r$. Para ello, observemos que si $j \leq r$ es uno de los subíndices que no cumplen la condición anterior, entonces son equivalentes las fórmulas

$$1.\ \exists w\ (\bigwedge_{i\leq r} \alpha_i(\bar{v}, w)) \text{ y } 2.\ \alpha_j(\bar{v}) \wedge \exists w\ (\bigwedge_{i\neq j} \alpha_i(\bar{v}, w)),$$

siendo así únicamente necesario eliminar el cuantificador de la fórmula

$$\exists w\ (\bigwedge_{i\neq j} \alpha_i(\bar{v}, w)).$$

En cualquier caso, hemos llegado a una fórmula de la forma que buscábamos. Q.E.D.

Tal y como indicamos anteriormente, este resultado será de gran utilidad para las secciones próximas. En particular, lo usaremos como herramienta para probar los dos resultados más importantes del presente proyecto.

3.3. Eliminación de cuantificadores para cuerpos algebraicamente cerrados

En la década de los años 1930, Alfred Tarski completó su procedimiento de eliminación de cuantificadores para el cuerpo de los números complejos y el cuerpo ordenado de los números reales. Sin embargo, no fue hasta 1948 cuando publicó sus resultados, como consecuencia del estallido de la Segunda Guerra Mundial. A lo largo de esta sección, estudiaremos con detenimiento el caso de la eliminación de cuantificadores en los complejos, dejando para el siguiente capítulo el caso real.

Es importante destacar que Tarski trabajó con las teorías de estructuras concretas, la de los reales y los complejos, en lugar de con clases axiomatizables, como los cuerpos algebraicamente cerrados. Aun así, un detenido estudio de sus pruebas señaló qué tipo de condiciones algebraicas han de darse para que se garantice el resultado de la eliminación de cuantificadores y se observó que sus resultados son válidos para las correspondientes clases de estructuras y no solo para las estructuras concretas de los complejos o de los reales. De hecho:

- En el caso complejo, la propiedad fundamental es la de ser algebraicamente cerrado.
- En el caso real, la propiedad del valor intermedio para polinomios garantiza el resultado (u otras propiedades equivalentes a esta).

La importancia de este impresionante resultado reside, entre otras cosas, en que nos permite conseguir una axiomatización óptima tanto para la teoría del cuerpo de los complejos, como para la de los números reales.

Demos paso así al primero de los resultados esenciales del proyecto, en el cual garantizaremos la eliminación de cuantificadores, no solamente para el cuerpo de los complejos $\mathbb{C}$, sino para los cuerpos algebraicamente cerrados en general.

Teorema 3.1. *La teoría ACF de los cuerpos algebraicamente cerrados posee eliminación de cuantificadores en el lenguaje* $\mathcal{L} = \{+, -, \cdot, 0, 1\}$.

Demostración. Consideremos $\phi(\bar{v})$ una fórmula arbitraria del lenguaje $\mathcal{L}$. Tenemos como objetivo encontrar una fórmula $\phi'(\bar{v})$ equivalente y libre de cuantificadores. Tal y como probamos anteriormente, véase el lema 3.1, podemos reducir nuestro estudio al caso de las fórmulas de la forma:

$$\exists w \ \alpha(\bar{v}, w),$$

donde $\alpha(\bar{v}, w)$ es una conjunción (finita) de fórmulas atómicas y sus negaciones, apareciendo la variable w en todas ellas.

En nuestro lenguaje $\mathcal{L}$, las fórmulas atómicas se reducen únicamente a las ecuaciones resultantes de igualar términos entre sí. Además, gracias a la incorporación del símbolo " $-$ ", podemos expresarlas como sigue

$$p(\bar{v}, w) = 0,$$

donde $p(\bar{y}, x)$ es un polinomio en x de coeficientes enteros. Por consiguiente, nuestra fórmula $\phi(\bar{v})$ será de la forma

$$\exists w \ (\bigwedge_{i \leq k} p_i(\bar{v}, w) = 0 \ \wedge \ \bigwedge_{j \leq h} \neg(q_j(\bar{v}, w) = 0)),$$

donde, tanto $p_i(\bar{y}, x)$ como $q_i(\bar{y}, x)$ son polinomios en x de coeficientes enteros y grado (positivo) n_i y m_j respectivamente.

Es bien sabido que una sucesión de elementos de un cuerpo no contiene al 0 si y solo si el producto de todos ellos no es nulo (esto ocurre ya que no existen divisores de cero en un cuerpo). Por tanto, podemos reducirnos al caso en el que, como mucho, se da en $\phi(\bar{v}, w)$ una sola inecuación, digamos

$$\neg(q(\bar{v}, w) = 0),$$

donde $q(\bar{y}, x)$ es el polinomio resultante de multiplicar todos los polinomios $q_j(\bar{y}, x)$, para $j \leq h$. Denotemos por m al grado de dicho polinomio en x.

Llegados a este punto, podríamos pensar en reducir el número de ecuaciones de la fórmula $\phi(\bar{v}, w)$ hasta conseguir que sea una única ecuación. Efectivamente, esto es posible y podemos demostrarlo haciendo un uso muy sutil de las propiedades de la Teoría de Cuerpos.

La idea es que, dado un cuerpo K y una sucesión $\bar{b}$ en K, las raíces comunes de los polinomios $p_i(\bar{b}, x)$ son, simplemente, las raíces de su máximo común divisor, y que existe una fórmula abierta en $\bar{v}$ (independientemente de K y $\bar{b}$) que define los coeficientes (en x) del máximo común divisor de los polinomios. Veamos con detalle esto último. Consideremos $p_i(\bar{y}, x)$, con $i \leq k$. Para todo i, escribiremos $p_i(\bar{y}, x)$ como un polinomio (en x) perteneciente a $(\mathbb{Z}[\bar{y}])[x]$

$$p_i(\bar{y}, x) = \sum_{r \leq n_i} p_{i,r}(\bar{y}) \cdot x^r.$$

Tomemos dos de estos polinomios, por ejemplo p_0 y p_1. Sin pérdida de generalidad supongamos que $gr(p_0) = n_0 \geq n_1 = gr(p_1)$, donde $gr(\cdot)$ denota el grado de los polinomios.

Justifiquemos la existencia de una fórmula abierta con variables $\bar{v}$ que, siempre y cuando $p_1(\bar{v}, x)$ no sea el polinomio nulo, nos proporcione los coeficientes del cociente y el resto de la división $\frac{p_0(\bar{v},x)}{p_1(\bar{v},x)}$. Para conseguir esta fórmula, basta con seguir el algoritmo habitual para la división de polinomios. Esto es un procedimiento tedioso pero efectivo. Por ejemplo, el primer paso es recalcar que, bien $p_{1,n_1}(\bar{v}) = 0$, o bien los coeficientes de $p_0(\bar{v}, x)$ y $p_1(\bar{v}, x)$ satisfacen:

$$p_{1,n_1}(\bar{v}) \cdot p_0(\bar{v}, x) = p_{0,n_0}(\bar{v}) \cdot p_1(\bar{v}, x) \cdot x^{n_0 - n_1} + P(\bar{v}, x),$$

siendo $P(\bar{y}, x)$ un polinomio de grado (en x) menor que n_0 y

$$p_{0,n_0}(\bar{v}) \cdot (p_{1,n_1}(\bar{v}))^{-1} \cdot x^{n_0 - n_1}$$

su término líder.

Recordemos que, gracias al algoritmo de la división euclídea, podemos hallar el máximo común divisor de los polinomios $p_i(\bar{y}, x)$ como el último resto no nulo tras una sucesión finita de divisiones. De nuevo, una fórmula abierta con variables $\bar{v}$ apropiada nos proporciona los coeficientes del máximo común divisor, siempre que $p_i(\bar{v}, x)$ no se anule, para todo $i \leq k$.

Así, podemos suponer sin pérdida de generalidad que la fórmula $\phi(\bar{v}, w)$ será de una de las siguientes formas:

I) $\exists w \ (p(\bar{v}, w) = 0)$,

II) $\exists w \ \neg(p(\bar{v}, w) = 0)$,

III) $\exists w \ (p(\bar{v}, w) = 0 \ \wedge \ \neg(q(\bar{v}, w) = 0))$,

siendo p y q los polinomios definidos anteriormente.

Estudiemos por separado cada uno de los casos anteriores.

I) Considérese que $\phi(\bar{v}, w) \equiv \exists w\ (p(\bar{v}, w) = 0)$. En cualquier cuerpo algebraicamente cerrado, $\phi(\bar{v}, w)$ es equivalente a decir que, si $\bar{v}$ anula todos los coeficientes de $p(\bar{y}, x)$, entonces $\bar{v}$ también asocia el valor 0 al término independiente; lo que puede ser expresado mediante una fórmula en $\bar{v}$ sin uso de cuantificadores.

II) Considérese que $\phi(\bar{v}, w) \equiv \exists w\ \neg(p(\bar{v}, w) = 0)$. En este caso, $\phi(\bar{v}, w)$ es equivalente, en cualquier cuerpo infinito, a expresar que $\bar{v}$ no anula todos los coeficientes del polinomio $p(\bar{y}, x)$. De nuevo, podemos expresar la última propiedad mediante una fórmula con variables $\bar{v}$ que sea abierta.

III) Finalmente, consideremos que $\phi(\bar{v}, w) \equiv \exists w\ (p(\bar{v}, w) = 0 \wedge \neg(q(\bar{v}, w) = 0))$. En este caso, en cualquier cuerpo algebraicamente cerrado, $\phi(\bar{v}, w)$ es equivalente a la siguiente expresión

$$(*) \quad p(\bar{v}, x) \text{ no divide a } q(\bar{v}, x)^n,$$

donde n es el grado del polinomio $p(\bar{y}, x)$ con respecto a x. La expresión $(*)$ es fácilmente expresable mediante una fórmula sin cuantificadores, basta usar algunas propiedades de la divisibilidad. Dado que la equivalencia entre III) y $(*)$ no es tan directa, evidenciémosla.

III) $\Rightarrow$ $(*)$

Sea K un cuerpo. Dada una sucesión $\bar{b}$ contenida en K, si el conjunto de las raíces de $p(\bar{b}, x)$ no está contenido en el conjunto de las raíces de $q(\bar{b}, x)$, entonces $p(\bar{b}, x)$ no divide a $q(\bar{b}, x)$, y, por consiguiente, tampoco dividirá a $q(\bar{b}, x)^n$.

$(*)$ $\Rightarrow$ III)

Sean de nuevo K y $\bar{b}$ como antes. Supongamos $\neg$III), esto es, que cualquier raíz de $p(\bar{b}, x)$ es también raíz de $q(\bar{b}, x)$. En cualquier cuerpo algebraicamente cerrado, esto implica que todo factor lineal de $p(\bar{b}, x)$ divide a $q(\bar{b}, x)$ y, por tanto, $p(\bar{b}, x)$ divide a $q(\bar{b}, x)^n$.

Esto finaliza la prueba del teorema.

Q.E.D.

Tras demostrar este resultado capital, estudiaremos algunas de sus consecuencias más relevantes. Antes de eso, nos permitimos destacar que la propiedad de eliminación de cuantificadores caracteriza a los cuerpos algebraicamente cerrados en el marco de los cuerpos infinitos. De hecho, este es un resultado muy célebre de *Macintyre, McKenna* y *Van den Dries* (véase [4]): « Un cuerpo infinito cuya teoría posea eliminación de cuantificadores en el lenguaje $\mathcal{L} = \{+, -, \cdot, 0, 1\}$ es necesariamente algebraicamente cerrado ».

Los principales resultados que derivan del teorema 3.1 atienden a los conceptos de completitud, decibilidad y conjuntos definibles. Antes de comentar algunos de ellos, introduzcamos algunos conceptos y resultados que necesitaremos más adelante.

Definición 3.4. *Dadas dos $\mathcal{L}$-estructuras $\mathcal{M}_1$, $\mathcal{M}_2$, decimos que $\mathcal{M}_1$ es subestructura elemental de $\mathcal{M}_2$, y lo escribiremos como $\mathcal{M}_1 \prec \mathcal{M}_2$, si se cumple:*

I) *$\mathcal{M}_1$ es subestructura de $\mathcal{M}_2$ ($\mathcal{M}_1 \subseteq \mathcal{M}_2$),*

II) *para toda fórmula $\phi(\bar{v})$ y todo $\bar{a} \in \mathcal{M}_1$,*

$$\mathcal{M}_1 \models \phi(\bar{a}) \text{ si y solo si } \mathcal{M}_2 \models \phi(\bar{a}).$$

Nota 3.2. Obsérvese que si $\mathcal{M}_1$ es una subestructura elemental de $\mathcal{M}_2$, entonces, en particular, se cumple que $\mathcal{M}_1$ y $\mathcal{M}_2$ son estructuras elementalmente equivalentes (basta considerar fórmulas sin parámetros $\bar{a} \in \mathcal{M}_1$ en la definición anterior).

Definición 3.5. *Decimos que una teoría $\mathcal{T}$ es modelo completa si, para cualesquiera dos modelos de $\mathcal{T}$, $\mathcal{M}_1$ y $\mathcal{M}_2$, se tiene que:*

$$\mathcal{M}_1 \subseteq \mathcal{M}_2 \Rightarrow \mathcal{M}_1 \prec \mathcal{M}_2.$$

Proposición 3.1. Si una teoría $\mathcal{T}$ admite eliminación de cuantificadores, entonces es modelo completa.

Demostración. Puesto que $\mathcal{T}$ admite eliminación de cuantificadores, cualquier fórmula que consideremos posee su correspondiente fórmula abierta $\mathcal{T}$-equivalente. Por otra parte, por el resultado 1.1 probado en el primer capítulo, las fórmulas abiertas se preservan entre subestructuras. Juntando estos dos hechos, tenemos el resultado deseado. Q.E.D.

Corolario 3.1. La teoría ACF de los cuerpos algebraicamente cerrados es modelo completa.

Finalmente, demos paso a los resultados que tanto estábamos buscando.

Corolario 3.2. Para $p = 0$ o p primo, se verifica que la teoría ACF_p es completa.

Demostración. Sea $p = 0$ o primo fijo. Existe un cuerpo (minimal) algebraicamente cerrado $\mathcal{K}_p$ de característica p; el cual, es la clausura algebraica del subcuerpo primo de característica p.

Consideremos la inmersión de $\mathcal{K}_p$ en cualquier cuerpo algebraicamente cerrado de la misma característica. Debido a que la teoría ACF es modelo completa, dicha inmersión da lugar a una subestructura elemental. Por tanto, todos los cuerpos algebraicamente cerrados de característica p son elementalmente equivalentes a $\mathcal{K}_p$ y, por consiguiente, también son elementalmente equivalentes entre sí. Se tiene pues que, para cualquier fórmula cerrada ϕ,

$$ACF_p \models \phi \text{ si y solo si } \mathcal{K}_p \models \phi.$$

En consecuencia, ACF_p es una teoría completa. Q.E.D.

Nota 3.3. El resultado anterior también puede demostrarse haciendo uso del test de Vaught (teorema 2.3) como se vio anteriormente.

En el capítulo anterior obtuvimos que las teorías ACF_p son decidibles. Ahora, somos capaces de demostrar el siguiente resultado.

Corolario 3.3. La teoría ACF de los cuerpos algebraicamente cerrados es decidible.

Demostración. Puesto que ACF admite eliminación de cuantificadores y el proceso de eliminación de cuantificadores dado es efectivo, basta con justificar que es decidible el problema de determinar si una fórmula cerrada y sin cuantificadores es o no consecuencia de la teoría ACF.

Sea σ una fórmula cerrada y sin cuantificadores del lenguaje de la Teoría de Anillos. Sin pérdida de generalidad (mediante reescritura en forma normal conjuntiva), supongamos que σ es una conjunción de disyunciones de fórmulas atómicas y sus negaciones. Como una conjunción es consecuencia de una teoría si y solo si cada uno de sus términos lo es, podemos suponer, de nuevo sin pérdida de generalidad, que σ es de la forma

$$(\bigvee_i m_i = 0) \ \vee \ (\bigvee_j \neg(n_j = 0)),$$

donde $m_i,\ n_j$ son enteros positivos. Así, nuestra fórmula viene a expresar que la característica bien divide a $\prod_i m_i$, o bien, es coprima con algún n_j (o pequeñas variantes de ello cuando alguno de los dos términos de la disyunción más arriba es vacío). En ambos casos, es posible comprobar de manera efectiva si una tal fórmula es o no consecuencia de la teoría. Q.E.D.

Nota 3.4. Tal y como aparece en la prueba, una fórmula puede ser abierta y cerrada simultáneamente.

Por último, tratemos el tema de los conjuntos definibles en un cuerpo algebraicamente cerrado. Como anticipamos en uno de los ejemplos del primer capítulo, se obtiene una clase de conjuntos definibles bastante sencilla.

Corolario 3.4. Consideremos $\mathcal{K}$ un cuerpo algebraicamente cerrado y $X \subseteq K$ un conjunto definible en $\mathcal{K}$ usando el lenguaje de la Teoría de Anillos. Entonces, X es finito o es cofinito.

Nota 3.5. Con conjunto cofinito nos referimos a un conjunto cuyo complementario es finito.

Demostración. Sea $q(x, \bar{a}) \in K[x]$. La expresión $q(v, \bar{a}) = 0$ define todo K si $q(x, \bar{a})$ es el polinomio nulo y, en caso contrario, define un conjunto finito. Por tanto, toda fórmula abierta define un conjunto finito o cofinito, pues una combinación Booleana de finitos y cofinitos continúa siéndolo. Luego, el resultado se tiene porque, en $\mathcal{K}$, toda fórmula es equivalente a una fórmula abierta (ACF admite eliminación de cuantificadores). Q.E.D.

Nota 3.6. Obsérvese que, en realidad, del argumento anterior se sigue que en cualquier cuerpo (algebraicamente cerrado o no) las fórmulas abiertas del lenguaje de la Teoría de anillos definen conjuntos finitos o cofinitos. Mientas que la eliminación de cuantificadores para ACF extiende esta propiedad a *cualquier* fórmula.

4. El caso real

En este sección abordamos el segundo objetivo fundamental del presente trabajo: dar una axiomatización natural e informativa del cuerpo de los números reales $\mathbb{R}$. Para ello, seguiremos la misma estrategia que en el capítulo anterior. Esto es, determinar una teoría (recursiva) $\mathcal{T}_{\mathbb{R}}$ que aglutine una serie de propiedades básicas del cuerpo de los reales y demostrar después que dicha teoría es completa (vía un procedimiento de eliminación de cuantificadores). Pero, ¿qué teoría natural $\mathcal{T}_{\mathbb{R}}$ hemos de considerar en este caso? La teoría de los *cuerpos reales cerrados*.

4.1. Cuerpos reales cerrados

Comencemos estudiando algunas definiciones y resultados básicos que nos harán entender mejor la clase de los cuerpos reales cerrados. Para más información consúltese [10].

Definición 4.1. *Sea R un anillo. Decimos que R es un anillo ordenado si está equipado con una relación de orden lineal " $\leq$ " compatible con las operaciones del anillo, esto es, verificando que:*

I) *si $a \leq b$, entonces $a + c \leq b + c$;*

II) *si $a \leq b$ y $0 \leq c$, entonces $a \cdot c \leq b \cdot c$;*

para cualesquiera a, b, $c \in R$.

Nota 4.1. La definición anterior está generalizada al caso de que R sea simplemente un anillo. Evidentemente, cuando R sea en particular un cuerpo, lo denominaremos *cuerpo ordenado*.

Definición 4.2. *Decimos que un cuerpo F es ordenable si existe un orden lineal $\leq$ sobre F de forma que $(F, \leq)$ resulte un cuerpo ordenado.*

Pasemos ahora a ofrecer una caracterización de los cuerpos ordenables.

Definición 4.3. *Decimos que F es un cuerpo formalmente real si el elemento -1 no puede expresarse como suma de cuadrados de elementos de F.*

Es evidente que en cualquier cuerpo ordenado los cuadrados son siempre no negativos, lo que nos indica que los cuerpos ordenados son cuerpos formalmente reales. Además, el recíproco también es cierto, dándose la caracterización que comentamos anteriormente.

Teorema 4.1. *Si F es un cuerpo formalmente real, entonces F es un cuerpo ordenable. En efecto, si $a \in F$ y $-a$ no es suma de cuadrados de elementos de F, entonces existe una ordenación de F para la que a es positivo.*

Corolario 4.1. Un cuerpo F es ordenable si y solo si F es formalmente real.

Nota 4.2. El cuerpo de los complejos $\mathbb{C}$ no es formalmente real ($i^2 = -1$). Se sigue pues que no es posible dar un orden lineal sobre $\mathbb{C}$ compatible con la suma y el producto de números complejos.

Es bien sabido que, centrándonos en el estudio general de los cuerpos, los cuerpos algebraicamente cerrados ocupan una posición privilegiada. En cierto modo son los cuerpos "más ricos", pues el hecho de contener todas las raíces de cualquier polinomio los dotan de muy buenas propiedades.

Siguiendo esta idea, quisiéramos encontrar una clase similar de cuerpos ordenables que también sea "muy rica" y tal que $\mathbb{R}$ sea el ejemplo canónico de dicha clase. El inconveniente que se nos plantea para directamente adaptar la idea anterior es el siguiente: los cuerpos formalmente reales no cumplen la propiedad anteriormente mencionada sobre las raíces de sus polinomio, basta con examinar el ejemplo de $p(x) = x^2 + 1$. Por ello, tendremos que centrar nuestra analogía en otra característica de los cuerpos algebraicamente cerrados. Esta será: *Un cuerpo es algebraicamente cerrado si no posee ninguna extensión algebraica propia.*

La ventaja que nos plantea esta condición de maximalidad es que sí la podemos extrapolar al marco de los cuerpos formalmente reales.

Definición 4.4. *Un cuerpo F se dirá real cerrado si es formalmente real y, además, no posee ninguna extensión algebraica propia que sea formalmente real.*

Presentemos ahora el ejemplo canónico de cuerpo real cerrado.

Ejemplo 4.1. Como era de esperar, $\mathbb{R}$ es un cuerpo real cerrado. En efecto, sea una extensión algebraica K de $\mathbb{R}$, de forma que

$$\mathbb{R} \subseteq K \subseteq \mathbb{C}.$$

Por el teorema de las extensiones intermedias, sabemos que

$$[\mathbb{C} : K] \cdot [K : \mathbb{R}] = [\mathbb{C} : \mathbb{R}] = 2.$$

Esto nos plantea dos opciones,

I) bien $[K : \mathbb{R}] = 1$, deduciéndose por tanto que $K = \mathbb{R}$ y la extensión no es propia;

II) o bien, $[\mathbb{C} : K] = 1$, deduciéndose por tanto que $K = \mathbb{C}$ y la extensión no es formalmente real.

Ahora sí estamos preparados para presentar una caracterización de esta clase de cuerpos.

Teorema 4.2. *(Artin-Schreier)*

Sea F un cuerpo. Son equivalentes:

I) *F es un cuerpo real cerrado.*

II) *F es formalmente real, todo polinomio de grado impar de $F[x]$ tiene al menos una raíz en F y, para todo $a \in F$, bien a es un cuadrado, o bien lo es $-a$.*

III) *F no es algebraicamente cerrado, pero la extensión $F[i]$ sí, con $i^2 = -1$.*

Una propiedad interesante de los cuerpos reales cerrados es la siguiente.

Proposición 4.1. Si F es un cuerpo real cerrado, entonces F admite un único orden. Este será

$$a \leq b \iff (b-a) \text{ es un cuadrado.}$$

Demostración. En primer lugar, como F es formalmente real, sabemos que este admite un orden. Sean $a,\ b \in F$. En este caso, o $(b-a)$ es un cuadrado, o lo será $-(b-a) = (a-b)$. Supongamos que $(b-a)$ es un cuadrado. Entonces, para cualquier orden $\leq$ en F, tendremos que

$$0 \leq b-a, \text{ lo que implica que } a \leq b.$$

El otro caso es análogo al anterior. Q.E.D.

Tal como indicamos en el capítulo anterior, la eliminación de cuantificadores en el caso real giraba en torno a la propiedad del valor medio para polinomios. Definámosla de manera formal.

Definición 4.5. *Sea F un cuerpo ordenado. Decimos que F satisface el teorema del valor medio para polinomios si, para todo $f \in F[x]$ y $a,\ b \in F$ cumpliendo que $a < b$ y que $f(a)$ y $f(b)$ tengan distinto signo, existe un elemento $c \in F$ tal que*

$$a < c < b \ y \ f(c) = 0.$$

Esta propiedad, nos permite enunciar una nueva caracterización de los cuerpos reales cerrados.

Teorema 4.3. *Sea F un cuerpo ordenado. Entonces, F es un cuerpo real cerrado si y solo si satisface la propiedad del valor medio para polinomios.*

Finalicemos el estudio descriptivo de los cuerpos reales cerrados definiendo la teoría sobre la que demostraremos el resultado de la eliminación de cuantificadores.

Una primera axiomatización, quizá la más natural, vendrá dada por la condición II) del teorema 4.2 anterior.

Definición 4.6. *Consideremos el lenguaje $\mathcal{L}_{or}$ de los anillos ordenados. Definimos la $\mathcal{L}_{or}$-teoría de los cuerpos reales cerrados, que denotaremos como RCF, como el conjunto de los siguientes axiomas:*

I) *los axiomas de la teoría de cuerpos,*

II) *los axiomas de los órdenes lineales para $<$,*

III) *los axiomas de los cuerpos ordenados, esto es:*

$$\forall x \forall y \forall z \ (x < y \to x + z < y + z),$$

$$\forall x \forall y \forall z \ ((x < y \wedge z > 0) \to x \cdot z < y \cdot z),$$

IV) $\forall x_1 \cdots \forall x_n \ (x_1^2 + \cdots + x_n^2 + 1 \neq 0)$, *para todo* $n \geq 1$,

V) $\forall x \exists y \ (y^2 = x \vee y^2 = -x)$,

VI) $\forall x_1 \cdots \forall x_{2n} \exists y \, (y^{2n+1} + \sum_{i=0}^{2n} x_i y^i = 0)$.

Sin embargo, como ya hemos señalado, la propiedad clave de $\mathbb{R}$ que usaremos en nuestra prueba de eliminación de cuantificadores será la propiedad del valor medio para polinomios. Es por ello que consideramos una segunda axiomatización de los cuerpos reales cerrados en el lenguaje de los Anillos ordenados, que, por abuso de notación, también denotaremos RCF. (En todo caso, el teorema 4.3 nos garantiza que ambas axiomatizaciones son equivalentes).

Definición 4.7. *Consideremos el lenguaje* $\mathcal{L}_{or}$ *de los anillos ordenados. Definimos la* $\mathcal{L}_{or}$*-teoría de los cuerpos reales cerrados (segunda versión), que denotaremos como* RCF*, como el conjunto de los siguientes axiomas:*

I) *los axiomas de la teoría de cuerpos,*

II) *los axiomas de los órdenes lineales para* $<$,

III) *los axiomas de los cuerpos ordenados, esto es:*

$$\forall x \forall y \forall z \ (x < y \to x + z < y + z),$$

$$\forall x \forall y \forall z \ ((x < y \wedge z > 0) \to x \cdot z < y \cdot z),$$

IV) *(Valor intermedio) para cada natural* n*,*

$$\forall x_0 \forall x_1 \ldots \forall x_n \forall u \forall w \exists v \ (x_0 + x_1 \cdot u + \cdots + x_n \cdot u^n + u^{n+1} < 0 \wedge$$

$$\wedge 0 < x_0 + x_1 \cdot w + \cdots + x_n \cdot w^n + w^{n+1} \wedge u < w \to$$

$$\to u < v \wedge v < w \wedge x_0 + x_1 \cdot v + \cdots + x_n \cdot v^n + w^{n+1} = 0)$$

Estamos ya preparados para el estudio de la eliminación de cuantificadores en la teoría RCF. Una primera aproximación a este problema nos conduciría a pensar que RCF presenta eliminación de cuantificadores sobre el lenguaje de la teoría de Anillos $\mathcal{L} = \{+, -, \cdot, 0, 1\}$ (sin orden). Nótese que la primera axiomatización de RCF dada puede adaptarse de manera directa a este lenugaje más restrictivo.

En un principio, no sería una idea descabellada, pues como vimos en la sección anterior, para la teoría ACF es cierto. Sin embargo, este lenguaje es demasiado restrictivo para la teoría de cuerpos reales cerrados, no permitiéndonos la eliminación de cuantificadores. Para dar una idea intuitiva de ello, nos basta estudiar el siguiente ejemplo. Consideremos las raíces de un polinomio $ax^2 + bx + c$ de grado 2 y coeficientes

reales (de hecho, con coeficientes en cualquier cuerpo real cerrado). Para garantizar la existencia de dichas raíces, hacemos uso de la inecuación

$$b^2 - 4ac \geq 0.$$

Luego, para eliminar el cuantificador existencial en un caso tan simple como

$$\exists x \ (ax^2 + bx + c = 0),$$

hemos tenido que hacer un uso esencial de la relación de orden $\leq$.

A la vista del ejemplo, parece razonable estudiar la propiedad de eliminación de cuantificadores sobre el lenguaje $\mathcal{L} = \{+, -, \cdot, <, 0, 1\}$, al que simplemente le añadimos el símbolo de la relación binaria de orden.

Efectivamente, este nuevo lenguaje cumple todos los requisitos para que nuestra teoría sí pueda eliminar cuantificadores. Demos paso por tanto al segundo de los resultados capitales en cuanto al proyecto se refiere.

4.2. Eliminación de cuantificadores en *RCF*

Teorema 4.4. *La teoría RCF de los cuerpos reales algebraicamente cerrados tiene eliminación de cuantificadores en el lenguaje* $\mathcal{L} = \{+, -, \cdot, <, 0, 1\}$.

Demostración. En esta prueba, procederemos de forma muy similar a como lo hicimos en el caso de la teoría de cuerpos algebraicamente cerrados, pero, atendiendo a las particularidades de este caso. De nuevo, el *quid* de la cuestión es eliminar el cuantificador existencial de la fórmula

$$\exists w \ \alpha(w, \bar{v}),$$

donde $\alpha(w, \bar{v})$ es una conjunción de, a lo sumo, una ecuación $p(w, \bar{v}) = 0$ y un conjunto finito (que puede ser vacío) de inecuaciones de la forma $q_j(w, \bar{v}) > 0$, siendo $p(x, \bar{y})$ y $q_j(x, \bar{y})$ $(j \leq m)$ polinomios de coeficientes enteros.

Dejemos, momentáneamente, de lado la prueba para estudiar detenidamente un polinomio genérico $f(x) = \sum_{i \leq t} f_i x^i$, con coeficientes en un cuerpo real cerrado. Si fijamos un determinado t, los objetos que definiremos a continuación (a los que haremos referencia por I, II y III respectivamente) verifican que son definibles uniformemente en cualquier cuerpo ordenado K. Los objetos a los que nos referimos son (para todo r y s verificando que $1 \leq r \leq s \leq t$):

I) una función que calcule; para cada polinomio de la forma $f(x)$ y para cualquier sucesión $(f_0, ..., f_t)$ de k^{t+1}, cuantas raíces tiene $f(x)$,

II) el conjunto de sucesiones $(f_0, ..., f_t) \in K^{t+1}$ de forma que el polinomio $f(x)$ tenga exactamente s raíces,

III) la función que asocia cada sucesión $(f_0, ..., f_t)$ a la r-ésima raíz de $f(x)$.

Destacar que, para todo t, los objetos anteriores son definibles mediante fórmulas sin cuantificadores de forma uniforme en cualquier cuerpo real cerrado K. Esto se prueba haciendo uso del Teorema de Sturm referente al recuento de raíces reales.

Procederemos por inducción en t, el grado de $f(x)$.

- $t = 0$

El caso $t = 0$ es sencillo. Si $f_0 \neq 0$, el número de raíces de $f(x)$ es cero, en caso contrario indefinido. Por otra parte, el resto de objetos (los anteriormente mencionados) son vacíos.

- $t > 0$

Pasemos al caso $t > 0$. Supongamos cierto para todo natural de valor menor que t. La idea que seguiremos en este caso será relacionar cada cero de $f(x)$ con las raíces de su derivada y el signo de estas en $f(x)$. Construyamos formalmente la derivada $f'(x)$ de $f(x)$:

$$f'(x) = \sum_{0<i\leq t} i \cdot f_i x^{i-1}.$$

Es importante destacar que $f'(x) = 0$ si y solo si $(f_1, ..., f_t) = (0, ..., 0)$. Exceptuando este caso, la inducción nos permite definir mediante fórmulas abiertas (siendo $1 \leq r \leq s < t$) :

I) la función que halla el número de raíces de $f'(x)$, para cualquier sucesión $(f_0, ..., f_t)$ con $(f_1, ..., f_t) \neq (0, ..., 0)$,

II) el conjunto de sucesiones $(f_0, ..., f_t) \in K^{t+1}$ que cumplen que no sean la sucesión nula y haga que $f'(x)$ tenga exactamente s raíces,

III) la función que encía cada sucesión $(f_0, ..., f_t)$ no nula a la raíz r-ésima de $f'(x)$.

Por comodidad, denotemos por

$$\rho_1 < \cdots < \rho_s,$$

a las raíces de $f'(x)$.

Haciendo uso del teorema del valor intermedio, que se puede emplear sin problema en cualquier cuerpo real cerrado, deducimos que el signo del polinomio $f'(x)$ no puede cambiar entre dos raíces consecutivas, esto es, en el intervalo $(\rho_i,\ \rho_{i+1})$. Además, podemos garantizar que $f(x)$ es monótona (creciente o decreciente dependiendo del valor del signo de la derivada) en cada uno de los intervalos de la forma $(\rho_i,\ \rho_{i+1})$ con $1 \leq i < s$. Lo anterior podemos asegurarlo, en cualquier cuerpo real cerrado, gracias a resultados elementales del análisis real. También puede ofrecerse una prueba de carácter íntegramente algebraico haciendo uso de los axiomas de la teoría RCF, sin embargo, esta sería de elevada complejidad.

Ahora, prestemos atención a los valores $f(\rho_i)$ y $f(\rho_{i+1})$. Estudiemos todos los posibles casos:

I) Si tanto $f(\rho_i)$ como $f(\rho_{i+1})$ son distintos de cero y además tienen el mismo signo, entonces, el intervalo $(\rho_i,\ \rho_{i+1})$ no contiene ninguna raíz de $f(x)$. Esto ocurre debido a la monotonía del polinomio en dicho intervalo.

II) Si el signo de $f(\rho_i)$ es distinto del signo de $f(\rho_{i+1})$, entonces, el intervalo $(\rho_i,\ \rho_{i+1})$ sí que contiene una raíz de $f(x)$. Además, podemos garantizar la unicidad de la misma haciendo uso del Teorema de Rolle, el cual puede emplearse sin problemas en los cuerpos reales cerrados. De nuevo, también puede ofrecerse una demostración algebraica, pero el análisis nos vuelve a facilitar dicha tarea.

III) Por último supongamos que $f(\rho_i) = f(\rho_{i+1}) = 0$. En este caso, el Teorema de Rolle nos elimina la posibilidad de la existencia de una nueva raíz intermedia.

Este razonamiento nos permite contar el número de raíces del polinomio $f(x)$ en el intervalo $[\rho_1,\ \rho_s]$. Sin embargo, el mismo razonamiento nos asegura que $f(x)$ es monótona en las semirectas $(-\infty,\ \rho_1)$ y $(\rho_s,\ +\infty)$ y que en cada una de ellas, existe al menos una raíz.

En principio, el estudio en estas semirectas será diferente, pues estas no son acotadas y los intervalos de la forma $(\rho_i,\ \rho_{i+1})$ sí. Para abordar este problema nos ayudaremos del siguiente resultado:

« Sea $f(x) = \sum_{i\leq t} f_i x^i$. Entonces, $f(x)$ no tiene raíces fuera del intervalo $[-a, a]$, donde $a = 3t \cdot max\{|\ f_{t-i} f_t^{-1}\ | : 0 < i \leq t\} + 1$ ». La prueba de este resultado se deduce a partir de los axiomas de los cuerpos ordenados.

Así, una raíz de $f(x)$ que sea menor que ρ_1 debe encontrarse en el intervalo $[-a,\ \rho_1)$, mientras que una que sea mayor que ρ_s debe pertenecer a $(\rho_s,\ a]$. Esto nos permite trasladar nuestro estudio, de nuevo, a intervalos acotados, por lo que el razonamiento seguido anteriormente es totalmente válido. El único detalle que en principio podría fallar es el uso de la función valor absoluto. Pero como esta puede definirse como sigue:

$$\text{Sea } b \in K,\ |b| = b \text{ si } b \geq 0 \text{ y } |b| = -b \text{ en caso contrario,}$$

sin el uso de cuantificadores, todo funciona correctamente.

Tras demostrar lo anterior, volvamos a centrarnos en la eliminación de cuantificadores. Recordemos que podemos suponer que nuestras fórmulas son de la forma

$$a)\ \exists w\ (p(w, \bar{v}) = 0\ \wedge \bigwedge_{j\leq m} q_j(w, \bar{v}) > 0)$$

$$b)\ \exists w \bigwedge_{j\leq m} q_j(w, \bar{v}) > 0,$$

donde $p(x, \bar{y})$ y $q_j(x, \bar{y})$ $(j \leq m)$ son polinomios de coeficientes enteros. Además, cada uno de ellos puede expresarse como un polinomio (en x) de coeficientes en $\mathbb{Z}[\bar{y}]$ como sigue:

$$p(x, \bar{y}) = \sum_{i\leq t} p_i(\bar{y}) x^i,$$

$$q_j(x, \bar{y}) = \sum_{i\leq t_j} q_{j,i}(\bar{y}) x^i.$$

El caso $a)$ puede reducirse al $b)$, pues, su fórmula es equivalente a

$$(\bigwedge_{i\leq t} p_i(\bar{v}) = 0\ \wedge\ \exists w\ (\bigwedge_{j\leq m} q_j(w, \bar{v}) > 0))\ \vee ...$$

$$\ldots \vee \Big(\bigvee_{1 \leq r \leq s \leq t} ((p(x, \bar{v}) \text{ tiene } s \text{ raíces}) \wedge \ldots$$

$$\ldots \wedge (\text{la raíz } r - \text{ésima } \rho_r(\bar{v}) \text{ satisface que } \bigwedge_{j \leq m} q_j(\rho_r(\bar{v}, \bar{v}) > 0))),$$

donde la última conjugación puede expresarse como una fórmula abierta.

Por tanto, nos reduciremos al caso b). Para cada $j \leq m$ y $s_j \leq t_j$, existen fórmulas abiertas que definen, para todo cuerpo K real cerrado, el conjunto de sucesiones $\bar{b}$ tal que $q(x, \bar{b})$ tenga s_j raíces, siendo estas,

$$\rho_{j,1} < \cdots < \rho_{j,s_j}.$$

Además, podemos cuadrar los signos de $q_j(x, \bar{b})$ en los siguientes intervalos

$$(-\infty,\ \rho_{j,1}(\bar{b})),$$

$$(\rho_{j,i}(\bar{b}),\ \rho_{j,i+1}(\bar{b})),\ \text{con } 1 \leq i < s_j \text{ y}$$

$$(\rho_{j,s_j}(\bar{b}),\ +\infty),$$

fijándonos simplemente en los valores de

$$q_j(\rho_{j,1}(\bar{b}) - 1, \bar{b}),$$

$$q_j(\frac{\rho_{j,i}(\bar{b}) + \rho_{j,i+1}(\bar{b})}{2}, \bar{b}),$$

$$q_j(\rho_{j,s_j}(\bar{b}) + 1, \bar{b})$$

respectivamente.

Finalmente, el siguiente procedimiento, que es independiente de K y $\bar{b}$, nos proporciona la fórmula abierta equivalente deseada. En primer lugar, se listan todos los posibles órdenes de las raíces (en x) de los polinomios q_j $(j \leq m)$ y, en cada caso, dividimos K en intervalos finitos de forma que cada q_j tenga signo constante en cada uno de ellos. Por último, basta con comprobar dichos signos para realizar una disyunción adecuada entre los que tengan signo positivo. Q.E.D.

Es importante destacar que la propiedad de eliminación de cuantificadores caracteriza a los cuerpos reales cerrados. De nuevo, un resultado de Macintyre, McKenna y Van des Dries (véase [4]) nos asegura que: « Un cuerpo ordenado cuya teoría admita eliminación de cuantificadores sobre el lenguaje $\mathcal{L} = \{+, -, \cdot, \leq, 0, 1\}$ es un cuerpo real cerrado».

Estudiaremos ahora algunas de las consecuencias más importantes de esta propiedad sobre la teoría RCF. Estos atienden a cuestiones de completitud, decibilidad y definibilidad de conjuntos. Primero observemos la siguiente consecuencia inmediata.

Corolario 4.2. La teoría de los cuerpos reales cerrados RCF es modelo completa.

Comencemos estudiando la completitud de RCF.

Corolario 4.3. La teoría RCF es completa. En particular, RCF es la teoría del cuerpo ordenado de los números reales $\mathbb{R}$.

Demostración. Por resultados algebraicos, sabemos que existe un cuerpo real cerrado minimal inmerso en cualquier modelo de RCF. Este se trata del cuerpo $\mathbf{R}_0$ de los números reales algebraicos. Dado que RCF es modelo completa, cualquier cuerpo real cerrado es una extensión elemental de $\mathbf{R}_0$. En particular, todos los cuerpos reales cerrados son elementalmente equivalentes a $\mathbf{R}_0$ y, en consecuencia, a cada uno de ellos. De ahí se sigue la completitud de la teoría. Q.E.D.

Nota 4.3. Puede pensarse que también podría usarse para probar este resultado el Test de Vaught. Sin embargo, RCF no es λ-categórica para ningún cardinal λ infinito.

Nota 4.4. Usando la completitud de RCF, podemos dar un argumento más riguroso del hecho de que RCF no elimina cuantificadores en el lenguaje sin orden. Cuando introdujimos el concepto de equivalencia entre fórmulas de un lenguaje, ya vimos que las fórmulas

I) $\phi(v) \ = \ v \geq 0$,

II) $\phi'(v) \ = \ \exists w \ (v = w^2)$,

son equivalentes en $\mathbb{R}$. Puesto que RCF es completa, tal y como acabamos de ver, ambas fórmulas también son equivalentes en RCF. De esta forma, la fórmula

$$\phi'(v) \ = \ \exists w \ (v = w^2)$$

define el conjunto de los elementos no negativos de cualquier cuerpo real cerrado. Sin embargo, $\phi'(v)$ no puede ser RCF-equivalente a ninguna fórmula abierta del lenguaje sin orden. En efecto, es claro que $\phi'(\mathbb{R}) = [0, +\infty)$ y sin embargo, como demostramos en el último resultado del capítulo anterior (véase la nota 3.6), las fórmulas abiertas del lenguaje sin orden solo pueden definir conjuntos finitos o cofinitos sobre cualquier cuerpo.

Pasemos ahora al estudio de la decibilidad.

Corolario 4.4. La teoría RCF es decidible.

Demostración. Debido a la eliminación de cuantificadores de RCF en el lenguaje $\mathcal{L} = \{+, -, \cdot, <, 0, 1\}$, cualquier $\mathcal{L}$-sentencia σ es equivalente (en RCF) a una combinación Booleana de fórmulas cerradas de la forma $m = n$ o $m < n$, donde m y n son enteros. Así, debido a la eliminación de cuantificadores, es muy sencillo comprobar el resultado. Q.E.D.

Nota 4.5. También podríamos dar una prueba alternativa usando que toda teoría recursiva y completa es decidible, como vimos en el capítulo anterior.

Antes de resolver la cuestión referente a la definibilidad de conjuntos, introduzcamos el siguiente concepto.

Definición 4.8. *Sea K un cuerpo ordenado. Decimos que $X \subseteq F^n$ es un conjunto semialgebraico si es una combinación Booleana de conjuntos de la forma $\{\bar{x} : p(\bar{x}) > 0\}$, donde $p(\bar{x}) \in K[x_1, ..., x_n]$.*

Corolario 4.5. Sea $\mathcal{K}$ un cuerpo real cerrado. Los conjuntos definibles coinciden exactamente con los conjuntos semialgebraicos.

Demostración. Sea n un entero positivo y consideremos $X \subseteq K^n$ un conjunto definible de $\mathcal{K}$. De este modo, existirá una fórmula $\phi(\bar{v}, \bar{w})$ de $\mathcal{L}$ y una sucesión $\bar{a}$ de forma que:

$$X = \phi(K^n, \bar{a}).$$

Debido a la eliminación de cuantificadores de la teoría RCF, podemos suponer que $\phi(\bar{v}, \bar{w})$ no tiene cuantificadores. Por tanto será una combinación Booleana de desigualdades de la forma

$$q(\bar{v}, \bar{w}),$$

siendo $q(\bar{x}, \bar{y}) \in \mathbb{Z}[\bar{x}, \bar{y}]$. Por consiguiente, X es el conjunto de soluciones de una combinación Booleana finita de desigualdades de la forma

$$q(\bar{v}, \bar{a}) \geq 0,$$

siendo, por tanto, un conjunto semialgebraico. Q.E.D.

Cerramos el capítulo con la siguiente observación.

Nota 4.6. Hemos presentado una axiomatización elegante e informativa del cuerpo de los números reales $\mathbb{R}$ en el lenguaje de los anillos ordenados $\mathcal{L}_{or} = \{+, -, \cdot, 0, 1, <\}$. Pero es natural preguntarse: ¿podríamos dar una axiomatización completa en el lenguaje original de la Teoría de anillos $\mathcal{L}_r = \{+, -, \cdot, 0, 1\}$? Es fácil ver que la respuesta es afirmativa. Para ello basta considerar una versión de la primera axiomatización de la teoría RCF dada *que no incluya ninguna referencia a la relación de orden.* Esto es:

I) los axiomas de la teoría de cuerpos,

II) $\forall x_1 \cdots \forall x_n \ (x_1^2 + \cdots + x_n^2 + 1 \neq 0)$, para todo $n \geq 1$,

III) $\forall x \exists y \ (y^2 = x \vee y^2 = -x)$,

IV) $\forall x_1 \cdots \forall x_{2n} \exists y \, (y^{2n+1} + \sum_{i=0}^{2n} x_i y^i = 0)$.

Puesto que todo cuerpo formalmente real es ordenable (y ese orden compatible existente es único en un cuerpo formal cerrado), se deduce que toda $\mathcal{L}_r$-estructura que sea modelo del conjunto anterior de axiomas puede extenderse de manera canónica a una $\mathcal{L}_{or}$-estructura que es modelo de RCF. Tomemos ahora dos $\mathcal{L}_r$-modelos cualesquiera, $\mathcal{M}_1$ y $\mathcal{M}_2$, de la teoría anterior. Extendámoslo a $\mathcal{L}_{or}$-modelos de RCF. Puesto que hemos probado que RCF es completa, se tiene que $\mathcal{M}_1$ y $\mathcal{M}_2$ son elementalmente equivalentes para el lenguaje $\mathcal{L}_{or}$. Pero entonces también lo son para el lenguaje más restrictivo $\mathcal{L}_r$.

Puesto que dos modelos cualesquiera de la $\mathcal{L}_r$-teoría anterior son elementalmente equivalentes, la teoría es completa.

Bibliografía

[1] Artin, M. *Algebra*, Pearson, 2014.

[2] Equipo docente de la asignatura. *Apuntes de Estructuras Algebraicas*, Universidad de Sevilla, 2021.

[3] Lang, S. *Algebra*, Springer, 2002.

[4] Macintyre, A., McKenna, K., van den Dries, L. *Elimination of Quantifiers in Algebraic Structures*, Advances in Mathematics, 47, 74–87, 1983.

[5] Marcja, A., Toffalori, C. *A Guide to Classical and Modern Model Theory*, Kluwer Academic Publishers, 2003.

[6] Marker, D. *Model Theory: An Introduction*. Springer, 2002.

[7] Robinson, J. *Definability and decision problems in arithmetic*. The Journal of Symbolic Logic, 14, 98—114, 1949.

[8] Sayed, A.O.M. *Model Theory of Algebraically Closed Fields and The Ax-Grothendieck Theorem*, African Institute for Mathematical Science South Africa, 2020.

[9] Srivastava, S.M. *A course on Mathematical Logic*, Springer, 2008.

[10] Kruckman, A. *Lecture Notes: Model theory of the real numbers*, Wesleyan University, 2020.