# Nullstellensatz Real, Positivstellensatz, Nichnegativstellensatz: Problema XVII de Hilbert

*Real Nullstellensatz, Positivstellensatz, Nichnegativstellensatz: Hilbert's Seventeenth Problem*

***(Septiembre de 2024)***

**Pablo Muñoz Lara**

**Trabajo de Fin de Grado**

para acceder al

**Grado en Matemáticas**

Facultad de Ciencias

Universidad de Cantabria

Director: Luis Miguel Pardo Vasallo

Resumen. En este manuscrito se presenta el Problema XVII de Hilbert, junto con su resolución en 1927 dada por E. Artin y con otras variantes del problema. Esto requiere el desarrollo previo de la Teoría Artin-Schreier, a fin de poder reproducir una prueba del problema en detalle. En el primer capítulo se verá una herramienta que será útil en toda la memoria, el Teorema del Homomorfismo de Artin-Lang, y también se probará el Nullstellensatz Real, es decir, la versión del Nullstellensatz de Kronecker-Hilbert para cuerpos realmente cerrados. En el segundo capítulo se desarrolla la Teoría de Artin-Schreier para cuerpos ordenados y cuerpos realmente cerrados, y también se añade una prueba del Positivstellensatz y del Nichnegativstellensatz. Finalmente, se introduce el Problema XVII de Hilbert y algunas de sus variantes más conocidas. Cada una de ellas exige el desarrollo de una teoría previa, así como la respuesta original de Artin se basó en la Teoría de Artin-Schreier. Por motivos de espacio, no daremos las pruebas detalladas de algunas de estas variantes, pero sí que trataremos de resumir estos aspectos teóricos esenciales en la memoria.

**Palabras Clave:** Problema XVII de Hilbert, Nullstellensatz Real, Positivstellensatz, Nichnegativstellensatz, Teoría de Artin-Schreier.

Abstract. In this work, the Hilbert's Seventeenth Problem is presented, along with a proof for the original version solved by E. Artin in 1927 and other different variants of the problem. The given proof is solidly based on the Artin-Schreier Theory, and thus it shall be presented beforehand. The first chapter of this memory is an introduction to some topics about closed real fields, including the Arting-Lang Homomorphism Theorem and a Real Nullstellensatz, that is, a version of the Kronecker-Hilbert's Nullstellensatz for closed real fields. In the second chapter, the Artin-Schreier Theory is developed, and also proof for the Positivstellensatz and Negativstellensatz is given. The last chapter consists of a presentation on the most recognizable versions of the Hilbert's Seventeenth Problem. Proof for the original version solved by Artin is given in great detail since the Artin-Schreier Theory has been worked out in the previous chapters. For some other variants and due to the space restrictions, we only summarize the main results with no proof at all.

**Keywords:** Hilbert's Seventeenth Problem, Real Nullstellensatz, Positivstellensatz, Nichnegativstellensatz, Artin-Schreier Theory.

# Índice general

Capítulo 0

# Introducción y Resumen de Contenidos de la Memoria

## Índice



Este capítulo consiste en un resumen de los principales resultados de la memoria, junto con una breve exposición histórica del asunto y mencionando a las referencias originales. El tema principal escogido para este TFG es el Problema XVII de Hilbert, formulado en 1900 y que fue resulto por Artin en el año 1927. Con el paso de los años, surgirían además diversas generalizaciones de este resultado y avances en general. En esta introducción comenzaremos por resumir los contenidos de cada capítulo explicando la exposición de los resultados que se ha escogido, así como la motivación y contenidos de cada uno de los apéndices. Después, se presentará los resultados más relevantes desde una perspectiva histórica, siguiendo el orden cronológico y recogiendo las fuentes originales. Hablaremos del trabajo previo de Hilbert y del contexto de 1900 que motiva el enunciado de su Problema XVII, y también del trabajo de Artin que llevó a la solución del Problema XVII y que propiciaría avances posteriores en la Geometría Algebraica Real. Destacaremos el Teorema del Homomorfismo de Artin-Lang, ya que es la técnica que aporta Lang para renovar la solución de Artin al Problema XVII. Este puede probarse mediante las ideas de Tarski sobre eliminación de cuantificadores en la Teoría de Primer Orden para Cuerpos Realmente Cerrados. Finalmente se discutirá las otras versiones del Problema XVII que se exponen en este texto y se mencionará otros avances relevantes en relación al tema.

la bibliografía empleada para la elaboración del apartado histórico se basa en las notas bibliográficas de [**BCR, 1998**] y [**Pardo, 2023**], así como en las introducciones y discusiones que pueden encontrarse en [**Seidenberg, 1952**], en [**Guangxin, 1988**] y en [**Gentile, 1992**], y también en diversas entradas de [**Wikipedia**].

### 0.1. Resumen de Contenidos de la Memoria.

A continuación se resume el contenido de cada capítulo. El Capítulo 1 comienza con una introducción a la Geometría Algebraica Real. En una primera sección se describe tanto el formalismo y notación más elemental de la Geometría Algebraica, como las nociones básicas de cuerpos ordenados y cuerpos realmente cerrados que aparecieron como parte de la Teoría de Artin-Schreier. Seguidamente, se lleva a cabo una prueba del Teorema del Homomorfismo de Artin-Lang, que requiere del uso de terminología y resultados de la Teoría de Primer Orden para Cuerpos Realmente Cerrados. En particular se utilizará sin demostración el Principio de Tarski-Seidenberg y un corolario de este, que es el Principio de Trasferencia para Cuerpos Realmente Cerrados. Para finalizar el capítulo, se aporta una prueba del Nullstellensatz Real *à la Rabinowitsch*, introduciendo a los ideales radicales reales que definirán las clases de ideales en biyección con cada una de las variedades algebraicas de un cuerpo realmente cerrado. Se añadirá otra versión del Nullstellensatz Real al estilo del Nullstellensatz original de Hilbert-Kronecker.

El Capítulo 2 comienza con el desarrollo abreviado de la Teoría de Artin-Schreier. Se ha elaborado el Apéndice A para tratar de compensar la falta de ejemplos y añadir algunos aspectos extra para el lector curioso. El resto del capítulo se centra en la prueba del Positivstellensatz

Formal, para el que se introduce toda la terminología de conos primos e ideales $P$-convexos. A partir de este resultado se formula unas versiones geométricas del Positivstellensatz y del Nichnegativstellensatz, y también se hace una prueba del Nullstellensatz Real Débil.

El Capítulo 3 introduce el Problema XVII de Hilbert, así como soluciones a distintas versiones de este. En primer lugar, se completa la demostración del enunciado probado por Artin en respuesta al Problema XVII, la cual se ha ido desarrollando en los capítulos previos. No se trata de la prueba original que ofreció Artin, sino que esta se basa en el Teorema del Homomorfismo que introdujo S. Lang varios años más tarde. Se sigue con la prueba de una generalización a conjuntos algebraicos irreducibles, también dada por Artin en su trabajo original. Será necesario introducir la noción de dimensión para conjuntos semi-algebraicos y varias propiedades en relación con esto, lo cual requiere del uso de la Teoría de la Dimensión de Anillos o de la técnica de loncheado de conjuntos semi-algebraicos. A causa de esto y debido a las limitaciones de espacio, se dejan algunas de las pruebas en manos de [**BCR, 1998**] y se añade los Apéndices C, D y E para desarrollar aquellos temas que tocan en un plano menos esencial a la prueba que ofrece nuestro texto de referencia. Finalmente, se discuten las versiones Equivariante y Cuantitativa del Problema XVII de Hilbert, que de nuevo por limitaciones de espacio han de mostrarse de forma resumida. Ambas secciones se apoyan en temas de la Teoría de Formas Cuadráticas, motivo por el que se elabora el Apéndice F como un apoyo a la información que ya se da en el texto principal. En cuanto a la bibliografía empleada en la elaboración de esta memoria, podrá encontrarse un texto explicativo al inicio de cada capítulo y de cada sección del apéndice, así como en comentarios puntuales si así se requiere. Puede anticiparse que la principal fuente del trabajo consiste en los Capítulos del 1 al 6 de [**BCR, 1998**].

En algún caso precedente se ha discutido el estilo y la ortografía de las memorias presentadas como Trabajo de Fin de Grado en Matemáticas. En evitación de intervenciones innecesarias, se quiere clarificar algunos aspectos en relación con el estilo escogido en este texto. Se ha elegido el formato de libro (*book*) de la *American Mathematical Society (AMS)*. Aunque el idioma utilizado es el español, se ha tratado de seguir lo más fielmente posible las recomendaciones del Libro de Estilo de esta asociación,[1] en conjunto con las reglas de estilo recomendadas por D. E. Knuth y coautores para la *Mathematical Association of America (MAA)*.[2] Específicamente, he tratado de seguir las siguientes dos reglas básicas:

- *"Numbered theorems, lemmas, etc. are proper nouns and, thus, are capitalized: Theorem 2.3, Lemma 3.1, Figure 4.5"* (p. 79 del *AMS Style Guide*).
- *"Rule 19. Capitalize names like Theorem 1, Lemma 2, Algorithm 3, Method 4"* (en D. E. Knuth et al.).

## 0.2. Introducción Histórica de los Contenidos de la Memoria.

En este apartado veremos una breve explicación histórica en distintos bloques de los contenidos de la memoria. También aparecerán enunciados, sin demostración obviamente, los resultados más significativos que se verán a lo largo de este TFG.

**0.2.1. El Trabajo de David Hilbert y su Problema XVII.** David Hilbert (1862-1943) fue un matemático alemán reconocido por sus aportaciones en diversas áreas de las matemáticas. Durante su carrera temprana, Hilbert convivió con la aparición reciente de las Geometrías no Euclídeas y en general, el desarrollo del concepto de geometría que tuvo lugar durante el siglo XIX. Cabe destacar el trabajo de Felix Klein (1849-1925), titulado *"Vergleichende Betrachtungen über neuere geometrische Forschungen"* y publicado en 1872, en el que renueva el concepto de geometría entonces difuso debido a que las nuevas ideas sobre Geometría no Euclídea no eran compatibles con el paradigma que había seguido el estudio de la Geometría Euclídea anteriormente. La idea de Klein fue describir cada geometría distinta a través de una acción de grupo que deja invariante los objetos característicos de dicha geometría, por ejemplo en Geometría Afín se tienen los movimientos rígidos, que dejan invariantes a las distancias entre puntos y a los ángulos. Este artículo marcó el inicio de un programa de investigación conocido

[1] M. Letourneau, J. Wright Sharp, AMS Style Guide, Journals, October 2017, AMS, Providence, 2017.
[2] D. E. Knuth, T. Larrabee, P. M. Roberts, Mathematical Writing, MAA, 1989.

como el Programa Erlangen, y causó la popularización de la Teoría de Invariantes durante esta etapa final del siglo XIX.

Durante aquellos años, Hilbert presentó varios trabajos sobre la Teoría de Invariantes. Los más distinguidos son *"Über die Theorie der algebraischen Formen"* de 1890, en el que se encontraba el resultado popularizado como Bassisatz o Teorema de la Base, y también *"Über die vollen Invariantensysteme"* publicado en 1893 y en que se demuestra su famoso Nullstellensatz o Teorema de los Ceros. Durante esta lectura, atribuiremos también a Kronecker es resultado, dado que prueba una versión de este en su trabajo *"Grundzüge einer arithmetischen Theorie der algebraischen Grössen"* de 1882, pero dentro de un contexto diferente.

Su cercanía a Minkowski, quien afirmó durante la defensa de su tesis en 1885 que *"no parece que toda forma no negativa pueda representarse por una suma de cuadrados de formas"*, provocó que Hilbert trabajase en cuestiones acerca de la representación de polinomios reales como sumas de cuadrados de polinomios. En 1888 presenta su artículo *"Über die Darstellung definiter Formen als Summe von Formenquadraten"*, que versa sobre la descomposición de polinomios con coeficientes reales que sean homogéneos y no negativos en sumas de cuadrados de polinomios. El resultado que obtuvo es el siguiente y se conoce como el Teorema de las Formas Positivas.

TEOREMA. **(de las Formas Positivas de Hilbert)**
*Sean $n, d \geq 1$. Sea $\Sigma_{n,2d}$ el conjunto de sumas de cuadrados de elementos de $\mathbb{R}[X_1, \ldots, X_n]$ que sean polinomios de grado $2d$. Sea $P_{n,2d}$ el subconjunto de $\Sigma_{n,2d}$ que contiene tan solo a los polinomios homogéneos de grado $2d$. Entonces, se tiene la igualdad $P_{n,2d} = \Sigma_{n,2d}$ si y solamente si $n = 2$ o $2d = 2$ o $(n, 2d) = (3, 4)$.*

Sobre este resultado hay que destacar que la prueba de Hilbert deja pendiente probar la existencia de unos polinomios homogéneos en 3 y 4 variables y de grados 6 y 4, respectivamente, que no sean sumas de cuadrados. El primer ejemplo se debe a T. S. Motzkin, quien publica *"The arithmetic-geometric inequality"* en 1967. En 1893, Hilbert publicó un trabajo titulado *"Über ternäre definite Formen"* en el que se trata el aspecto cualitativo de esta descomposición, es decir, el mínimo número de cuadrados que es necesario para poder representar a un polinomio. Concluyó que es suficiente la suma de 4 cuadrados de cocientes de polinomios para poder representar a cualquier polinomio no negativo de $\mathbb{R}[X_1, X_2]$. Esta línea de trabajo acerca de la representación de polinomios reales inspiraría el enunciado de su Problema XVII años más tarde. En el año 1900, tuvo lugar el *International Congress of Mathematicians* celebrado en París, y en el que Hilbert anunció una lista de 10 que consideró relevantes para el desarrollo de las matemáticas. Durante el año siguiente, publicaría una edición de su conferencia con la afamada lista de 23 problemas que a día de hoy conocemos.De entre todos estos, tan solo nos ocuparemos del Problema XVII, que se puede enunciar del modo siguiente:

PROBLEMA CLÁSICO. **(Problema XVII de Hilbert)**
*Considérese el cuerpo de los números reales $\mathbb{R}$ y un polinomio $f$ en $n$ variables con coeficientes en dicho cuerpo. Si $f$ toma valores no negativos en todo $\mathbb{R}^n$, ¿puede afirmarse que $f$ sea una suma de cuadrados del cuerpo de fracciones de los polinomios?*

**0.2.2. Solución de Artin y el Desarrollo de la Geometría Algebraica Real.** Los trabajos de Hilbert sobre Teoría de Invariantes citados en el apartado anterior contienen las pruebas de un par de resultados, el Bassisatz y el Nullstellensatz, que son centrales en la Geometría Algebraica para cuerpos algebraicamente cerrados, como lo es el cuerpo $\mathbb{C}$ de los números complejos. La generalización de estos resultados al caso de los números reales $\mathbb{R}$ no es precisamente trivial, por lo que Hilbert no llegó a abordar el campo de la Geometría Algebraica Real con éxito. Sin embargo, su Problema XVII enunciado en 1900 propiciaría importantes avances durante la década de 1920. Entonces, el par de matemáticos austríacos Emil Artin (1898-1962) y Otto Schreier (1901-1929) desarrollaron lo que se conoce a día de hoy como la Teoría de Artin-Schreier. Esto fue originalmente escrito en dos trabajos escritos por ambos y titulados *"Algebraische Konstruktion reeller Körper"* de 1926 y *"Eine Kennzeichnung der reell abgeschlossenen Körper"* de 1927. En el año 1927, Artin publicó una solución al Problema XVII de Hilbert para el caso de un cuerpo realmente cerrado en su trabajo *"Über die Zerlegung definiter Funktionen in Quadrate"*.

TEOREMA. **(de Artin)** *Sea $R$ un cuerpo realmente cerrado y sea $f \in R[X_1, \ldots, X_n]$. Si $f$ es no negativo en $R^n$, es decir si $f(x) \geq 0$ para todo $x \in R^n$, entonces $f$ es una suma de cuadrados de elementos del cuerpo de fracciones $R(X_1, \ldots, X_n)$.*

El estudio de los cuerpos realmente cerrados floreció en diversas áreas, como por ejemplo con la aparición de la Teoría de Modelos y de resultados como el Principio de Tarski-Seidenberg que comentaremos en el apartado siguiente; y también en materia de la Geometría Algebraica Real y del Análisis Real. En la memoria probaremos algunos resultados notables, como lo es el Nullstellensatz Real. La primera versión de este resultado se debe a D. W. Dubois, quien lo muestra en su artículo *"A Nullstellensatz for Ordered Fields"* de 1969. Un año después, J.-J. Risler publica *"Une caracterisation des ideaux des varietes algebriques reelles"*, que contiene otra versión del Nullstellensatz Real al estilo de Rabinowitsch. Durante el texto probaremos tres versiones diferentes del Nullstellensatz Real, que nombraremos en analogía con las versiones del Nullstellensatz para cuerpos algebraicamente cerrados que se muestran en [**Pardo, 2023**].

TEOREMA. **(Nullstellensatz Real Versión Rabinowitsch)**
*Sea $R$ un cuerpo realmente cerrado. Sea $\mathfrak{a} \subset R[X_1, \ldots, X_n] = R[X]$ un ideal y sea $\sqrt[R]{\mathfrak{a}}$ su radical real. Entonces, se cumple que $\mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{a})) = \sqrt[R]{\mathfrak{a}}$.*

TEOREMA. **(Nullstellensatz Real Versión Hilbert-Kronecker)**
*Sea $R$ un cuerpo realmente cerrado. Sea $\mathfrak{a} \subset R[X_1, \ldots, X_n]$ un ideal. Entonces:*

$$\mathcal{Z}_{R^n}(\mathfrak{a}) = \emptyset \Leftrightarrow 1 \in \sqrt[R]{\mathfrak{a}}.$$

TEOREMA. **(Nullstellensatz Real Versión Débil)**
*Sea $R$ un cuerpo realmente cerrado y sea $V$ un conjunto algebraico de $R^n$. Sea $\mathcal{P}(V)$ el anillo de las funciones polinomiales de $V$ en $R$, y sea $MaxSpec^{(R)}(\mathcal{P}(V))$ el espectro maximal real de $\mathcal{P}(V)$. Entonces, la siguiente es una aplicación biyectiva:*

$$\begin{aligned} V &\longrightarrow MaxSpec^{(R)}(\mathcal{P}(V)) \\ x &\longmapsto \quad \mathcal{I}_{\mathcal{P}(V)}(\{x\}). \end{aligned}$$

El lector puede dirigirse al Capítulo 1 o al final de la Sección 2.4 para consultar las pruebas o las nociones de ideal real, radical real, así como el resto de notaciones que se utilizan. Con posterioridad se probó otro resultado para cuerpos realmente cerrados, que también demostraremos durante la memoria, conocido como Positivstellensatz o Positivstellensatz Formal para distinguirlo de su versión geométrica. La prueba original se atribuye a G. Stengle por una publicación titulada *"A Nullstellensatz and a Positivstellensatz in semialgebraic geometry"* de 1974, en la cual se demuestra el enunciado de la versión geométrica del Positivstellensatz. Puede consultarse en el texto *"An Introduction to Real Algebra"* escrito por T. Y. Lam en 1984 la distinción entre la versión formal (que ahí llaman abstracta) y la versión geométrica del Positivstellensatz y del Nichnegativstellensatz. Enunciamos estas versiones geométricas.

COROLARIO. **(Nichnegativstellensatz y Positivstellensatz Geométricos)**
*Sea $R$ un cuerpo realmente cerrado y sea $V$ un conjunto algebraico de $R^n$. Sean las funciones polinomiales $g_1, \ldots, g_r \in \mathcal{P}(V)$ y el conjunto $W = \{x \in V : g_1(x) \geq 0, \ldots, g_r(x) \geq 0\}$. Sea $P$ el cono de $\mathcal{P}(V)$ generado por $g_1, \ldots, g_r$. Entonces para cada $f \in \mathcal{P}(V)$ se cumple que:*

*(i)* $\forall x \in W, f(x) \geq 0 \Leftrightarrow \exists m \in \mathbb{N}, \exists g, h \in P, fg = f^{2m} + h,$
*(ii)* $\forall x \in W, f(x) > 0 \Leftrightarrow \exists g, h \in P, fg = 1 + h.$

**0.2.3. Principio de Tarski-Seidenberg y Referencias Constructivistas.** La prueba que se lleva a cabo de la solución de Artin al Problema XVII no sigue el hilo argumental de la prueba original. Se ha optado por una demostración que hace uso del Teorema del Homomorfismo de Artin-Lang, cuya prueba a su vez se basa en el Principio de Tarski-Seidenberg en forma de Principio de Trasferencia para Cuerpos Realmente Cerrados. Con posterioridad al desarrollo de la Teoría de Artin-Schreier surgió una subrama de la Teoría de Primer Orden para los cuerpos realmente cerrados, y que actualmente se formula en términos de la Teoría de Modelos introducida por Alfred Tarski (1901-1983) en 3 sucesivas publicaciones en los años 1954, 1955 y 1956, y tituladas *"Contributions to the theory of models I, II, III"*.

El principal resultado que se toma de la Teoría de Primer Orden para Cuerpos Realmente Cerrados es el llamado Principio de Tarski-Seidenberg, y es un resultado sobre la eliminación de cuantificadores en fórmulas de primer orden sobre cuerpos realmente cerrados. Se le conoce como 'principio' dado que fue postulado por Tarski en una publicación de 1930 que se tituló *"Liber Definierbare Mengen Rellerzahlen"* y que fue popularizada por su traducción al francés de 1931. El resultado fue probado en 1951 por el propio Tarski en su artículo *"A Decision Method for Elementary Algebra and Geometry"*. Al año siguiente, A. Seidenberg publicó *"A New Decision Method for Elementary Algebra"* con una prueba distinta del mismo resultado. En ambos casos se aportó una prueba constructivista del enunciado, esto es, una prueba que describe a un algoritmo y que en ocasiones se refiere como el Algoritmo de Tarski.

TEOREMA. **(Principio de Tarski-Seidenberg)**
*Sea $R$ un cuerpo realmente cerrado. Entonces para cada fórmula de primer orden $\Psi$ cuantificada y definida sobre el cuerpo $R$ y con variables libres $X_1, \ldots, X_n$, existe otra fórmula $\Phi$ libre de cuantificadores que es semánticamente equivalente a $\Psi$ sobre el cuerpo $R$. Más aún, dada cualquier extensión $R_1/R$ de cuerpos realmente cerrados, se tiene que $\Psi$ es semánticamente equivalente a $\Phi$ sobre $R_1$.*

COROLARIO. **(Principio de Transferencia)**
*Sea $R_1/R$ una extensión de cuerpo realmente cerrados. Sea $\Psi$ una fórmula de primer orden definida sobre $R$, cuantificada y sin variables libres. Entonces $\Psi$ se satisface en $R$ si y solamente si $\Psi$ se satisface en $R_1$.*

A modo de curiosidad diremos que para el caso de cuerpos algebraicamente cerrados con característica 0, se tiene el resultado análogo al Principio de Transferencia conocido como Principio de Lefschetz. El Principio de Transferencia permite demostrar el Teorema del Homomorfismo de Artin-Lang, el cual sirve para dar una prueba alternativa del resultado de Artin, pero que también resultará útil para otros muchos resultados como el Nullstellensatz Real. Este teorema puede verse en el trabajo original de S. Lang titulado *"The theory of real places"* de 1953 y al que se añade el nombre de Artin por las implicaciones que tuvo su trabajo de 1927 en la consecución de este resultado.

TEOREMA. **(Teorema del Homomorfismo de Artin-Lang)**
*Sea $R$ un cuerpo realmente cerrado y sea $A$ una $R-$álgebra finitamente generada. Si existe un homomorfismo de $R$-álgebras $\varphi$ de $A$ en alguna extensión $R_1$ del cuerpo $R$ que sea realmente cerrada, entonces existe un homomorfismo de $R$-álgebras $\psi : A \longrightarrow R$.*

Durante el último siglo ha emergido una tendencia hacia las pruebas constructivistas en todo resultado que pueda probarse por este tipo de argumentaciones. Las pruebas que se muestran no tienen en cuenta este aspecto, pero sí que se hará hincapié en aquellos lugares en los que se utilice el Axioma de Zorn. Seguidamente, se ofrece una bibliografía como alternativa constructivista a los resultados centrales de este texto. Nuestra prueba del Teorema del Homomorfismo de Artin-Lang utiliza la existencia de clausura real de cuerpos formalmente reales, que se probará utilizando el Axioma de Zorn. Puede verse una alternativa constructivista en *"Existence and uniqueness of the real closure of an ordered field without Zorn's Lemma"* de T. Sander, 1991. También se tiene una prueba constructivista del Positivstellensatz en *"Effective real Nullstellensatz and variants"* de H. Lombardi, 1990. El Problema XVII de Hilbert ha sido resuelto por argumentos constructivistas. Una primera prueba en estos términos viene dada por W. Habicht en su artículo *"Über die Zerlegung strikter definiter Formen in Quadrate"* de 1940, en el que se construye una representación para polinomios homogéneos positivos como suma de cuadrados de cocientes de polinomios. Más adelante en 1960, G. Kreisler publica una construcción para polinomios en general en su trabajo *"Sums of squares"*. Años más tarde, en 1984, C. N. Delzell escribió *"A continuous, constructive solution to Hilbert's 17th problem"* donde da una construcción de los polinomios no negativos como sumas de cuadrados que además es continua.

**0.2.4. Otras Versiones del Problema XVII.** En adición a la solución de Artin para cuerpos realmente cerrados, en este trabajo se presenta otras versiones del Problema XVII. En particular, se ve la generalización para conjuntos algebraicos irreducibles también probada por Artin y las versiones Equivariante y Cuantitativa del problema. Repasemos cada una de ellas.

La generalización a conjuntos algebraicos irreducibles utiliza una noción de dimensión de los conjuntos semi-algebraicos dada por la dimensión de anillos. El resultado es el siguiente.

TEOREMA. *Sean $R$ un cuerpo realmente cerrado, $V \subset \mathbb{A}^n(R)$ un conjunto algebraico irreducible de dimensión $d$, y $f \in \mathcal{P}(V)$ una función polinomial. Entonces, son equivalentes:*

*(i)* $f \in \sum \mathcal{K}(V)^2$,
*(ii)* $f$ *es no negativo en* $V^{(d)}$,
*(iii)* $f$ *es no negativo en* $Reg(V)$,
*(iv)* $f$ *es no negativo en algún abierto Zariski contenido en* $V$.

También se examina la posibilidad de generalizar el resultado a cuerpos formalmente reales en general, pero no es posible. El primer contraejemplo se vio en *"Note on Artin's solution of Hilbert's 17th problem"* que data de 1967 y fue escrito por D. W. Dubois. Existe una manera de adaptar el resultado a ciertos cuerpos formalmente reales, aquellos que presentan la llamada Propiedad Débil de Hilbert, en la que la descomposición no es una suma de cuadrados sino una especie de combinación lineal con coeficientes positivos. Dicho resultado se atribuye a K. McKenna y su artículo *"New facts about Hilbert's 17th Problem"* de 1975.

La Versión Equivariante del Problema XVII trata el caso de los polinomios simétricos. El resultado que veremos sin demostración viene del artículo titulado *"Positive Symmetric Functions"* y escrito por C. Procesi en 1978. El resultado en cuestión es el siguiente.

TEOREMA. **(Solución al Problema XVII de Hilbert Equivariante)**
*Sea $R$ un cuerpo realmente cerrado. Sea $f$ un polinomio simétrico de $R[X_1, \ldots, X_n]$. Si $f$ es no negativo en $\mathbb{A}^n(R)$, entonces puede escribirse como:*

$$f = \sum_{i=1}^{r} s_i \delta_i,$$

*para algunas $s_1, \ldots, s_r$ sumas de cuadrados de funciones racionales simétricas y siendo $\delta_i$ productos de la forma $\prod_{j=2}^{n} (\Delta_j(\sigma_1, \ldots, \sigma_n))^{\epsilon_{i,j}}$ con cada $\epsilon_{i,j}$ igual a 0 o a 1 y siendo $\Delta_2, \ldots, \Delta_n$ los menores principales de la matriz $\mathcal{H}(\sigma_1, \ldots, \sigma_n)$ definida en la Sección 3.4.*

La Versión Cuantitativa del Problema XVII de Hilbert consiste en encontrar el mínimo número de cuadrados necesario para representar a cualquier suma de cuadrados. Esta cantidad se define para cualquier anillo $A$ y se dice que es su número de Pitágoras $p(A)$. Esta es una cuestión sobre la que trabajó el propio Hilbert en 1893, quién comprobó que $p(R(X_1, X_2))$ está superiormente acotado por 4. El problema quedó en el aire hasta la década de 1960. En un primer trabajo de J. W. S. Cassels de 1964 titulado *"On the representation of rational functions as sums of squares"*, este encontraría la cota inferior $p(F(X_1, X_2)) \geq p(F) + n$ para $F$ cualquier cuerpo formalmente real. Se atribuye a cierto trabajo de J. Ax publicado en torno a 1966 la cota $p(R(X_1, X_2, X_3)) \leq 8$, pero tan solo algo después se tendría una generalización de esta cota dada por A. Pfister. Este matemático desarrolló un trabajo sobre formas cuadráticas que tienen la propiedad de ser multiplicativas y que a día de hoy se conocen como formas de Pfister. Dicho trabajo se titula *"Multiplikative quadratische Formen"* y es de 1965. La cota superior a $p(R(X_1, \ldots, X_n))$ viene escrita en un segundo artículo titulado *"Zur Darstellung definiter Funktionen als Summe von Quadraten"* y con fecha de 1967. En la Sección 3.5 veremos sin demostración el resultado siguiente con las cotas que hemos mencionado.

TEOREMA. *Sea $R$ un cuerpo realmente cerrado. Entonces, se cumplen las desigualdades:*

$$n + 1 \leq p(R(X_1 \ldots, X_n)) \leq 2^n.$$

La cota inferior de Cassels fue mejorada años más tarde, en vista del citado trabajo de T. S. Motzkin de 1967. En 1971, Cassels escribió *"On Sums of Squares and on Elliptic Curves over Function Fields"* junto a W. S. Ellison y a Pfister donde se mejora la cota inferior a que $p(R(X_1, X_2)) \geq n + 2$ para $R$ cualquier cuerpo realmente cerrado. La cuestión de representar a polinomios no negativos con sumas de cuadrados de polinomios quedó ya fuera de escena con el Teorema de las Formas Positivas de Hilbert, puesto que en muy pocos casos tenía sentido considerar esto. Existe un trabajo de 1982, [**CDLR, 1982**], que trata sobre los números de Pitágoras de diferentes tipos de anillos y que en particular demuestra que cuando $F$ es un cuerpo formalmente real y dado $n \geq 2$, se tiene que $p(F[X_1, \ldots, X_n]) = \infty$.

Capítulo 1

# Nullstellensatz Real.

## Índice



Este capítulo está dedicado a dar una prueba del Teorema de los Ceros (o Nullstellensatz) Real. En la primera sección, se introducirá el panorama general de las Geometrías Algebraicas y en particular, elementos y resultados centrales de la Geometría Algebraica Compleja como el Nullstellensatz de Hilbert-Kronecker. También se presentará los cuerpos realmente cerrados, noción central para la Geometría Algebraica Real, la cual incluye al Nullstellensatz Real. En el apartado siguiente, se exponen aspectos básicos de la Teoría de Primer Orden para Cuerpos Realmente Cerrados a fin de presentar el Principio de Tarski, los conjuntos semi-algebraicos y el Principio de Transferencia en Cuerpos Realmente Cerrados. Todo ello con tal de probar el Teorema del Homomorfismo de Artin-Lang, herramienta que resultará útil a lo largo de todo el texto. Finalmente, se abordará la prueba del Nullstellensatz Real en su versión como correspondencia biunívoca entre las variedades algebraicas y un tipo específico de ideales, llamados ideales reales. También se añade una versión del Nullstellensatz Real análoga al enunciado original del Nullstellensatz de Hilbert-Kronecker.

La bibliografía empleada en este capítulo se basa, fundamentalmente, en los Capítulos 1, 2 y 4 de [**BCR, 1998**], utilizados para elaborar la introducción a la Teoría de Cuerpos Realmente Cerrados y las pruebas del Teorema del Homomorfismo de Artin-Lang y el Nullstellensatz Real. La presentación de definiciones básicas y de la descomposición primaria de ideales están basadas en los Capítulos 6, 7 y 8 de [**Pardo, 2023**]. La introducción a la Teoría de Primer Orden para Cuerpos Realmente Cerrados se ha basado en [**Pardo, 1987**], y los resultados que se presentan están adaptados del Capítulo 5 de [**BCR, 1998**]. Para la discusión sobre $A$-álgebras se ha utilizado el Capítulo 2 de [**AtMac, 1969**]. Por motivos de espacio, deberá omitirse la prueba del Principio de Tarski-Seidenberg, que puede verse en la Proposición 5.2.2 de [**BCR, 1998**].

### 1.1. Introducción.

Una forma de definir objetos geométricos, a menudo referidos como variedades, consiste en tomar el conjunto de ceros de alguna función. Sea $X$ un conjunto, que será el espacio en el que se defina dicho objeto geométrico. Se denota por $D^X$ al conjunto de funciones de $X$ en un dominio de integridad $D$, que es anillo con las operaciones suma y producto de funciones. Para definir las variedades se considera tan solo una colección de estas funciones, escogiendo que sea una $D$-álgebra para poder identificar objetos geométricos con clases de ideales.

Definición 1. **(Conjunto de Ceros)**
*Sea $X$ un conjunto, $D$ un dominio de integridad y $A[X] \subset D^X$ una $D$-álgebra de funciones definidas en $X$ con valores en $D$. Sea $\mathcal{F}$ una familia de elementos de $A[X]$. Se define el conjunto de ceros de dicha familia y se denota por:*

$$\mathcal{Z}_X(\mathcal{F}) = \{x \in X : f(x) = 0, \forall f \in \mathcal{F}\}.$$

*Se dice variedad $A[X]$-definible a todo subconjunto de $X$ que sea el conjunto de ceros dado por alguna familia de $A[X]$. Dado un ideal $\mathfrak{a} \subset A[X]$, se denota al conjunto de ceros del ideal por $\mathcal{Z}_X(\mathfrak{a})$. Dada una familia finita de funciones $f_1, \ldots, f_r \in A[X]$, se denotará por $\mathcal{Z}_X(f_1, \ldots, f_r)$ a $\mathcal{Z}_X(\{f_1, \ldots, f_r\})$.*

En contextos de Geometría Algebraica, los conjuntos de ceros son a menudo referidos como variedades algebraicas o como conjuntos algebraicos. A continuación se define el conjunto de todas funciones que se anulan en cierto subconjunto de $X$. Este conjunto de funciones resulta ser siempre un ideal del anillo de funciones $A[X]$.

DEFINICIÓN 2. **(Ideal de Funciones con Ceros en un Subconjunto)**
*Sea $X$ un conjunto, $D$ un dominio de integridad y $A[X] \subset D^X$ una $D$-álgebra de funciones definidas en $X$ con valores en $D$. Sea $F$ un subconjunto de $X$. Se define el ideal de funciones con ceros en $F$ y se denota por:*

$$\mathcal{I}_{A[X]}(F) = \{f \in A[X] : f(x) = 0, \forall x \in F\}.$$

Todos los conjuntos de ceros de $X$ son conjuntos de la forma $\mathcal{Z}_X(\mathfrak{a})$, definidos por algún ideal $\mathfrak{a}$ de $A[X]$. Estos conjuntos son los cerrados de una topología, que se conoce como la Topología de Zariski sobre $X$. En general, la asociación entre los cerrados Zariski de $X$ y los ideales de $A[X]$ no es una biyección. Dentro de cada contexto particular, es de interés conocer algún resultado que relacione de manera biunívoca a los cerrados Zariski con alguna clase específica de ideales.

Estos resultados reciben el nombre de Teorema de los Ceros o Nullstellensatz en la Versión de Rabinowitsch. Existen otras versiones de Nullstellensatz como el original de Hilbert-Kronecker para cuerpos algebraicamente cerrados. Este enunciado clásico es el que da sentido al nombre de Nullstellensatz, dado que resuelve el problema de existencia de solución a una ecuación polinómica compleja multivariada que trabajaron Kronecker y Hilbert hacia finales del siglo XIX, pese a que típicamente se atribuya este resultado solo a Hilbert. Nótese además que el Problema X de la lista de Hilbert es precisamente este pero para ecuaciones diofánticas, o si se quiere, considerando el dominio de los enteros.

Un caso ampliamente estudiado es el de la Geometría Algebraica Compleja, donde $D = K$ es un cuerpo algebraicamente cerrado y se toma por $X$ al espacio afín de dimensión $n$ sobre $K$, que se denota por $\mathbb{A}^n(K)$ o $K^n$. También se considera $A[X] = \mathcal{P}(\mathbb{A}^n(K))$, que es la $K$-álgebra de las funciones polinomiales sobre $\mathbb{A}^n(K)$, es decir, aquellas funciones $f : \mathbb{A}^n(K) \to K$ tales que existe un polinomio $P \in K[X_1, \ldots, X_n]$ que cumpla $P(x) = f(x)$ para todo $x \in \mathbb{A}^n(K)$. Es por ello que habitualmente se habla de los ideales del anillo de polinomios $K[X_1, \ldots, X_n]$ en lugar de las funciones polinomiales.

La asociación de polinomios de $K[X_1, \ldots, X_n]$ con funciones polinomiales según lo expuesto, da lugar a un morfismo de anillos sobreyectivo $K[X_1, \ldots, X_n] \to \mathcal{P}(\mathbb{A}^n(K))$. En caso de que $K$ sea un cuerpo infinito, se tiene que el polinomio 0 es el único contenido en el núcleo del morfismo y, por lo tanto, se trata de un isomorfismo. Los cuerpos algebraicamente cerrados son infinitos,[1] y también lo son el tipo de cuerpos de los que nos ocuparemos aquí, lo que justifica el abuso de notación.

Dado que $K$ es un cuerpo, se utilizará el Teorema de la Base de Hilbert para poder asumir que todos sus ideales sean finitamente generados. Se deja escrito este resultado a continuación:[2]

TEOREMA 1.1.1. **(de la Base de Hilbert)**
*Sea $A$ un anillo noetheriano. Entonces el anillo $A[X_1, \ldots, X_n]$ es noetheriano.*

A continuación enunciaremos sin demostración el Nullstellensatz para cuerpos algebraicamente cerrados que muestra la correspondencia biunívoca entre las variedades algebraicas sobre estos cuerpos y los ideales radicales de los anillos de polinomios considerados, es decir, la versión que utiliza el conocido Truco de Rabinowitsch.[3]

TEOREMA 1.1.2. **(Nullstellensatz de Rabinowitsch)**
*Sea $K$ un cuerpo y $K$ su clausura algebraica. Sea $\mathfrak{a} \in K[X_1, \ldots, X_n] = K[X]$ un ideal y $V \subset \mathbb{A}^n(K)$ una variedad $K[X]$-definible. Entonces:*

$$\sqrt{\mathfrak{a}} = \mathcal{I}_{K[X]}(\mathcal{Z}_{\mathbb{A}^n(K)}(\mathfrak{a})), \qquad V = \mathcal{Z}_{\mathbb{A}^n(K)}(\mathcal{I}_{K[X]}(V)),$$

*donde $\sqrt{\mathfrak{a}}$ denota el ideal radical de $\mathfrak{a}$.*

[1] Véase en la Proposición 3.6.9 de [**Pardo, 2023**].
[2] Puede consultarse una prueba en el Capítulo 8 de [**Sharp, 1990**].
[3] Puede consultarse una prueba en el Capítulo 8 de [**Pardo, 2023**].

El contexto que nos interesa, sin embargo, es el de la Geometría Algebraica Real. El foco de este capítulo es, de hecho, llegar a probar el Nullstellensatz Real, pero antes de eso es necesario introducir $D$, $X$ y $A[X]$ para el caso que nos ocupa. En Geometría Algebraica Compleja se escoge $X$ como un espacio afín de dimensión finita sobre un cuerpo algebraicamente cerrado, por ejemplo, el cuerpo $\mathbb{C}$ de los complejos. La Geometría Algebraica Real tratará, como caso particular, a $X = \mathbb{A}^n(\mathbb{R})$. Para ello se introduce la noción de cuerpo realmente cerrado que, de alguna forma, modela las propiedades necesarias de $\mathbb{R}$ para emitir un resultado aplicable a este y más casos. Para llegar a dicha definición, comencemos por definir cuerpo formalmente real.

Definición 3. **(Cuerpo Formalmente Real)**
*Un cuerpo $F$ se dice formalmente real cuando para cada $x_1, \ldots, x_p \in F$ se tiene que:*

$$x_1^2 + \ldots + x_p^2 = 0 \Rightarrow x_1 = \ldots = x_p = 0.$$

Se verá más adelante el Teorema de Artin-Schreier para Cuerpos Ordenados 2.1.11, que viene a decir que sobre este tipo de cuerpos puede definirse un orden total que sea compatible, en algún sentido, con las operaciones del cuerpo. Se llamará ordenación del cuerpo a dicho orden, para distinguirlo de lo que sea simplemente un orden, y se define rigurosamente a continuación:

Definición 4. **(Cuerpo Ordenado)**
*Sea $F$ un cuerpo. Se dice ordenación del cuerpo $F$ a una relación de orden total $\leq$ que cumpla:*

*(i)* $x \leq y \Rightarrow x + z \leq y + z$ *para cada* $x, y, z \in F$,
*(ii)* $0 \leq x \wedge 0 \leq y \Rightarrow 0 \leq xy$ *para cada* $x, y \in F$.

*En tal caso, se dice cuerpo ordenado al par $(F, \leq)$. Se denomina cono positivo al conjunto $P = \{x \in F : 0 \leq x\}$.*

Una ordenación de un cuerpo ha de satisfacer que $0 < 1$, ya que $0 \neq 1$ y si 1 fuese negativo, entonces de la Propiedad $(i)$ de cuerpos ordenados se tiene que $0 \leq -1$, y por la Propiedad $(ii)$ se sigue que $0 \leq (-1)(-1) = 1$, lo cual es absurdo y se tendrá $-1 < 0$ en todo cuerpo ordenado. De esto y de la Propiedad $(i)$ se deduce que, dado cualquier $n \in \mathbb{N}$, se cumple:

$$1 + \ldots + 1 = n1 < n1 + 1.$$

El cuerpo $\mathbb{R}$ de los números reales cumple ambas definiciones, y también lo hace $\mathbb{Q}$. Para ambos, además, se tendrá una ordenación única. Por otra parte, no todo cuerpo admite ordenación. El contraejemplo más evidente es cualquier cuerpo finito, o en general, con característica positiva. Si se tiene un cuerpo de característica positiva $n_0$, entonces $(n_0 - 1)1 < n_0 1 = 0$. Pero también ocurre que $0 \leq (n_0 - 1)1$ y se tiene una contradicción. Esto supone que los cuerpos ordenados son necesariamente infinitos y de característica 0. Otros cuerpos que no admiten ordenación son los cuerpos algebraicamente cerrados. El cuerpo $\mathbb{C}$ de los complejos, por ejemplo, no admite odenación porque si $i > 0$ entonces $-1 = i^2 > 0$, necesariamente, pero el caso contrario implica que $-i > 0$ y nuevamente se tendría que $-1 = (-i)^2 > 0$. Tras ver estos ejemplos, introduzcamos ahora a los cuerpos realmente cerrados.

Definición 5. **(Cuerpo Realmente Cerrado)**
*Se dice cuerpo realmente cerrado a todo cuerpo formalmente real que no tenga una extensión de cuerpos algebraica propia que además sea cuerpo formalmente real.*

Ahora sí, $\mathbb{R}$ es un ejemplo de cuerpo realmente cerrado mientras que $\mathbb{Q}$ no lo es. Por el Teorema Fundamental del Álgebra,[4] se sabe que el cuerpo $\mathbb{C}$ de los complejos es la clausura algebraica de $\mathbb{R}$. Puede escribirse $\mathbb{C}$ como la extensión del cuerpo $\mathbb{R}$, $\mathbb{R}[X]/(X^2 + 1) = \mathbb{R}[\sqrt{-1}]$, que por ser de grado 2 es la única extensión algebraica no trivial de $\mathbb{R}$. Como $\mathbb{C}$ no admite ordenación, se sigue que $\mathbb{R}$ es cuerpo realmente cerrado.

Pueden considerarse las extensiones algebraicas de un cuerpo ordenado, y de entre estas, aquellas que admitan una ordenación que extienda a la del cuerpo original en el sentido de la inclusión en la extensión de cuerpos. Ocurre que en este conjunto de extensiones algebraicas de un cuerpo ordenado, acotado por la clausura algebraica del cuerpo, aquellas extensiones que son maximales para la inclusión serán cuerpos realmente cerrados, y se las llama clausuras reales del cuerpo ordenado original.

[4] Puede consultarse https://es.wikipedia.org/wiki/Teorema_fundamental_del_lgebra.

DEFINICIÓN 6. **(Clausura Real)**
*Sea $F$ un cuerpo formalmente real junto con una ordenación $\leq$. Se dice clausura real de $F$ a toda extensión algebraica $R$ de $F$ que sea cuerpo realmente cerrado y cuya única ordenación extienda a la de $F$.*

Veremos más adelante, en la Proposición 2.1.15, que todo cuerpo ordenado posee alguna clausura real. Y también veremos en la Proposición 2.1.13 que los cuerpos realmente cerrados admiten una única ordenación.

Retomando el tema inicial, el contexto de la Geometría Algebraica Real consiste en tomar $D = R$ un cuerpo realmente cerrado, considerar algún espacio afín $\mathbb{A}^n(R)$ de dimensión finita $n$ sobre $R$, y tomar como anillo de funciones al de las funciones polinomiales $\mathcal{P}(\mathbb{A}^n(R))$, que por ser $R$ infinito, es isomorfo al anillo de polinomios $R[X_1, \ldots, X_n]$.

## 1.2. Teorema del Homomorfismo de Artin-Lang.

En esta sección se pretende probar el llamado Teorema del Homomorfismo de Artin-Lang, el cual será necesario más tarde para la prueba del Nullstellensatz Real. La demostración de este teorema se apoya en un resultado de la Teoría de la Eliminación, conocido como Principio de Transferencia. Antes de enunciarlo, se introducen algunos conceptos de Teoría de Primer Orden para Cuerpos Realmente Cerrados o TPOCRC de manera abreviada.

Una fórmula de primer orden libre de cuantificadores en TPOCRC, abreviadamente FLC, consiste en una combinación finita de conjunciones, disyunciones y negaciones que toma como fórmulas atómicas a expresiones de la forma $(f(X_1, \ldots, X_n) \geq 0)$, donde $f$ es un polinomio con coeficientes en algún cuerpo realmente cerrado $R$ y con variables $X_1, \ldots, X_n$. La clase de las FLC para un cuerpo realmente cerrado $R$ se denotará por $\mathcal{F}_R(X_1, \ldots, X_n)$, y se define como la menor clase que satisface las siguientes propiedades:

(*i*) Cada fórmula atómica $(f(X_1, \ldots, X_n) \geq 0)$, con $f$ un polinomio de coeficientes en $R$ y variables $X_1, \ldots, X_n$, pertenece a $\mathcal{F}_R(X_1, \ldots, X_n)$.
(*ii*) Dado cualquier par de fórmulas $\alpha, \beta \in \mathcal{F}_R(X_1, \ldots, X_n)$, se tiene que $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\neg\alpha) \in \mathcal{F}_R(X_1, \ldots, X_n)$.

Una fórmula de $\mathcal{F}_R(X_1, \ldots, X_n)$ puede denotarse simplemente por $\Phi$, o si se desea destacar las variables involucradas, también puede escribirse como $\Phi(X_1, \ldots, X_n)$.

NOTACIÓN 1.2.1. Es habitual el uso de las abreviaturas:

- $(f(X_1, \ldots, X_n) < 0)$ en lugar de $(\neg(f(X_1, \ldots, X_n) \geq 0))$,
- $(f(X_1, \ldots, X_n) = 0)$ en lugar de $((f(X_1, \ldots, X_n) \geq 0) \wedge (-f(X_1, \ldots, X_n) \geq 0))$,

así como aquellas que resultan evidentes para los símbolos $\leq$, $>$ y $\neq$.

A cada expresión de $\mathcal{F}_R(X_1, \ldots, X_n)$ puede asociarse una interpretación por cada posible combinación de valores de las variables. Llamamos $R_1$ a una extensión del cuerpo $R$ que además sea realmente cerrada. Sean $x = (x_1, \ldots, x_n) \in R_1^n$ y $\Phi \in \mathcal{F}_R(X_1, \ldots, X_n)$. Se definen las siguientes reglas de interpretación:

(*i*) Si $\Phi = (f(X_1, \ldots, X_n) \geq 0)$ es un fórmula atómica, entonces se define su interpretación en el punto $x$ y se denota por:

$$\Phi(x) = \begin{cases} 1 & \text{si se cumple } f(x_1, \ldots, x_n) \geq 0 \text{ en } R_1 \\ 0 & \text{en caso contrario} \end{cases} .$$

(*ii*) Si $\alpha, \beta \in \mathcal{F}_R(X_1, \ldots, X_n)$, se definen las interpretaciones de las siguientes fórmulas:

$$(\alpha \wedge \beta)(x) = \begin{cases} 1 & \text{si } \alpha(x) = \beta(x) = 1 \\ 0 & \text{en otro caso} \end{cases} ,$$

$$(\alpha \vee \beta)(x) = \begin{cases} 0 & \text{si } \alpha(x) = \beta(x) = 0 \\ 1 & \text{en otro caso} \end{cases} ,$$

$$(\neg\alpha)(x) = \begin{cases} 1 & \text{si } \alpha(x) = 0 \\ 0 & \text{en otro caso} \end{cases} .$$

Por la propia definición de la clase $\mathcal{F}_R(X_1,\ldots,X_n)$, se tiene que la interpretación en cada punto $x$ y para cada FLC está unívocamente determinada. Dada una FLC $\Phi \in \mathcal{F}_R(X_1,\ldots,X_n)$, diremos que se satisface en $x \in R_1^n$ cuando $\Phi(x) = 1$. Diremos también que $\Phi$ es satisfacible en $R_1^n$ si se satisface en algún punto de $R_1^n$, y que es tautología en $R_1^n$ si se satisface en todos los puntos de $R_1^n$. Un par de fórmulas $\Phi_1, \Phi_2$ de $\mathcal{F}_R(X_1,\ldots,X_n)$ se dirán semánticamente equivalentes en $R_1^n$ si se satisfacen en exactamente los mismos puntos de $R_1^n$, y se denotará por $\Phi_1 \equiv_{R_1} \Phi_2$, o simplemente utilizando $\equiv$ cuando no haya ambigüedad.

Se denomina conjunto semi-algebraico del espacio afín $R_1^n$ y definible sobre $R$ a cualquier subconjunto de $R_1^n$ que venga dado, por alguna FLC $\Phi \in \mathcal{F}_R(X_1,\ldots,X_n)$, de la siguiente forma:

$$\{x \in R_1^n : \Phi(x) = 1\}.$$

En el caso $R_1 = R$, estos conjuntos se dirán simplemente conjuntos semi-algebraicos de $R^n$. Cualquier FLC es semánticamente equivalente a otra FLC escrita en forma normal disyuntiva, esto es, disyunciones de cláusulas, que a su vez son conjunciones de literales, que a su vez son una fórmula atómica o la negación de una fórmula atómica. Por otra parte, el conjunto semi-algebraico que define la conjunción de un par de FLC es la intersección de los conjuntos individuales de cada fórmula, y la misma relación existe entre la disyunción de FLC y la unión de sus conjuntos asociados. Esto lleva a dar una definición de conjunto semi-algebraico equivalente a la que ya hemos visto, pero que no utiliza elementos de la TPOCRC.

Definición 7. **(Conjunto Semi-Algebraico)**
*Sea $R$ un cuerpo realmente cerrado y sea $R_1$ una extensión del cuerpo $R$ que además sea realmente cerrada. Se dice conjunto semi-algebraico de $R_1^n$ definible sobre $R$ a todo subconjunto de $R_1$ de la forma siguiente:*

$$\bigcup_{i=1}^{r} \bigcap_{j=1}^{s_i} \{x \in R_1^n : f_{i,j}(x) \epsilon_{i,j} 0\},$$

*donde $f_{i,j} \in R[X_1,\ldots,X_n]$ y $\epsilon_{i,j} \in \{\geq, <\}$ para cada $j = 1,\ldots,s_i$ y cada $i = 1,\ldots,r$. Si $R_1 = R$, estos conjuntos se dirán simplemente conjuntos semi-algebraicos de $R^n$.*

Nótese que la condición $f(x) < 0$ es equivalente a $\neg(f(x) \geq 0)$, como se vio en la Notación 1.2.1, de manera la definición que hemos dado coincide con una FLC en forma normal disyuntiva si se tienen en cuenta esta consideración y las relaciones entre la unión con la conectiva $\vee$ y la intersección con $\wedge$. En vista de la Notación 1.2.1, también se tiene que los conjuntos de la forma $\{x \in R^n : f(x) = 0\}$ son semi-algebraicos. Cualquier unión o intersección finita de semi-algebraicos es un semi-algebraico. En particular, lo son las intersecciones finitas de conjuntos tipo $\{x \in R^n : f(x) = 0\}$. Considerando que los cuerpos son noetherianos y que entonces el ideal asociado a un conjunto algebraico es finitamente generado para ese caso, se sigue que los conjuntos algebraicos de $R^n$ son un caso particular de conjunto semi-algebraico. El complementario de un conjunto semi-algebraico es también semi-algebraico, y entonces los abiertos de la topología de Zariski definida sobre $R^n$ también son semi-algebraicos. Veamos a continuación un ejemplo de conjunto semi-algebraico para el caso particular de $\mathbb{R}^2$.

Ejemplo 1.2.2. *En la Figura 1 se muestra el conjunto semi-algebraico de $\mathbb{R}^2$ descrito como la intersección de los siguientes conjuntos:*[5]

$$\left\{(x,y) \in \mathbb{R}^2 : \left(\frac{x}{5}\right)^2 + \left(\frac{y}{4}\right)^2 \leq 1\right\},$$

$$\left\{(x,y) \in \mathbb{R}^2 : (x+2)^2 + (y-2)^2 > 0\right\} \cap \left\{(x,y) \in \mathbb{R}^2 : (x-2)^2 + (y-2)^2 > 0\right\},$$

$$\left\{(x,y) \in \mathbb{R}^2 : x^2 + (y-1)^2 - 10 \neq 0\right\} \cup \left\{(x,y) \in \mathbb{R}^2 : y - 1 > 0\right\}.$$

*El primer conjunto son los puntos de la cabeza, el siguiente es el complementario de los ojos, y el último es el complementario de la boca.*

Una propiedad notable de los conjuntos semi-algebraicos, y de la que no gozan los conjuntos algebraicos en general, es que la proyección de un conjunto semi-algebraico es otro semi-algebraico. Este es uno de los principales resultados de la Teoría de Modelos y se debe a A. Tarski, aunque

[5]Figura y ejemplo tomados del Capítulo 2 de [**BCR, 1998**].

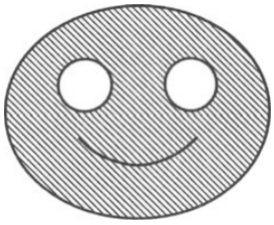

FIGURA 1. Un simpático conjunto semi-algebraico de $\mathbb{R}^2$.

lo que realmente produjo fue un algoritmo que permite la eliminación de cuantificadores en la TPOCRC. Una proyección viene a ser el caso particular de eliminación de un bloque de cuantificadores existenciales. Antes de presentar el resultado de Tarski, definamos las fórmulas cuantificadas. Nos limitaremos a fórmulas cuantificadas en forma prenexa, abreviadamente FCFP. Dado un cuerpo realmente cerrado $R$ y el conjunto $\{X_1, \ldots, X_n, Y_1, \ldots, Y_m\}$ de variables algebraicamente independientes sobre $R$, se define FCFP en la TPOCRC como una expresión de la forma:

$$\Psi = Q_1 Y_1, \ldots, Q_m Y_m, \Phi(X_1, \ldots, X_n, Y_1, \ldots, Y_m),$$

donde $\Phi \in \mathcal{F}_R(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$ y $Q_i \in \{\forall, \exists\}$ para cada $i = 1, \ldots, m$. Las variables $X_1, \ldots, X_n$ se dicen variables libres de la fórmula $\Psi$ y las variables $Y_1, \ldots, Y_m$ se dicen cuantificadas. Se denota por $\mathcal{F}_R^{(CFP)}(X_1, \ldots, X_n)$ a la clase de las FCFP con constantes en $R$ y variables libres $\{X_1, \ldots, X_n\}$, en la TPOCRC. El conjunto de las FCFP con constantes en $R$ y sin variables libres se denotará por $\mathcal{F}_R^{(CFP)}(\emptyset)$.

Sea $R_1$ una extensión del $R$ que también sea realmente cerrada. Podemos asignar interpretaciones en puntos de $R_1^n$ a las fórmulas de $\mathcal{F}_R^{(CFP)}(X_1, \ldots, X_n)$ basándonos en la interpretación de una FLC y añadiendo cuantificadores de manera inductiva. Se indica formalmente la interpretación de $\Psi \in \mathcal{F}_R^{(CFP)}(X_1, \ldots, X_n)$ en un punto $x \in R_1^n$ según cada caso:

(*i*) Si $\Psi$ es una FLC, es decir, si $\Psi \in \mathcal{F}_R(X_1, \ldots, X_n)$, entonces se define la interpretación $\Psi(x_1, \ldots, x_n)$ como en el caso anterior.

(*ii*) Si $\Psi$ posee una única variable cuantificada, es decir, si $\Psi = QY, \Phi(X_1, \ldots, X_n, Y)$ con $\Phi \in \mathcal{F}_R(X_1, \ldots, X_n, Y)$ y $Q \in \{\exists, \forall\}$, se distinguen dos casos:
- si $Q = \exists$, se define $\Psi(x_1, \ldots, x_n) = 1$ si $\Phi(X_1, \ldots, X_n, Y)$ es satisfacible en $R_1^{n+1}$, y $\Psi(x_1, \ldots, x_n) = 0$ en otro caso,
- si en cambio $Q = \forall$, se define $\Psi(x_1, \ldots, x_n) = 1$ si $\Phi(X_1, \ldots, X_n, Y)$ es tautología en $R_1^{n+1}$, y $\Psi(x_1, \ldots, x_n) = 0$ en caso contrario.

(*iii*) Si $\Psi$ tiene la forma general $\Psi = Q_1 Y_1, \ldots, Q_m Y_m, \Phi(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$, entonces, consideramos esta otra fórmula de $\mathcal{F}_R^{(CFP)}(X_1, \ldots, X_n, Y_1)$:

$$\Psi_1 = Q_2 Y_2, \ldots, Q_m Y_m, \Phi(X_1, \ldots, X_n, Y_1, \ldots, Y_m),$$

y definimos $S(\Psi_1, x) = \{y_1 \in R_1 : \Psi_1(x, y_1) = 1\}$. Entonces, podemos de nuevo distinguir dos casos:
- si $Q_1 = \exists$, se define $\Psi(x_1, \ldots, x_n) = 1$ cuando $S(\Psi_1, x) \neq \emptyset$ y $\Psi(x_1, \ldots, x_n) = 0$ en otro caso,
- si $Q_1 = \forall$, se define $\Psi(x_1, \ldots, x_n) = 1$ cuando $S(\Psi_1, x) = R_1$ y $\Psi(x_1, \ldots, x_n) = 0$ en caso contrario.

Claramente se puede ver el carácter de una definición inductiva en el punto (*iii*), por lo que la interpretación de una fórmula de $\mathcal{F}_R^{(CFP)}(X_1, \ldots, X_n)$ en un punto de $R_1^n$ queda bien definida. Una fórmula $\Psi \in \mathcal{F}_R^{(CFP)}(X_1, \ldots, X_n)$ se dice satisfacible cuando $\Psi(x) = 1$ para algún punto $x$ de $R_1^n$. La misma fórmula se dirá tautología si para cada punto $x$ de $R_1^n$ se cumple que $\Psi(x) = 1$. Un par de fórmulas $\Psi_1, \Psi_2 \in \mathcal{F}_R^{(CFP)}(X_1, \ldots, X_n)$ se dirán semánticamente equivalentes en $R_1$ si $\Psi_1(x) = \Psi_2(x)$ para todos los puntos $x$ de $R_1^n$, y en cuyo caso se denotará por $\Psi_1 \equiv_{R_1} \Psi_2$, o simplemente utilizando $\equiv$. Nótese que $\mathcal{F}_R(X_1, \ldots, X_n) \subset \mathcal{F}_R^{(CFP)}(X_1, \ldots, X_n)$ y que estas definiciones extienden a las dadas previamente para las FLC.

Tras este preámbulo, puede presentarse el resultado de Tarski. Se le conoce como Principio de Tarski, dado que lo publicó por primera vez en un trabajo de 1931 y no fue hasta otra publicación suya de 1951 que Tarski aportaría una prueba en forma del algoritmo que lleva su nombre. Se añade a A. Seidenberg al nombrar este resultado, ya que ofrecería otra prueba de este resultado un año después que Tarski. Se omite la demostración de este resultado, que puede encontrarse regada en varios capítulos de [**BCR, 1998**].

TEOREMA 1.2.3. **(Principio de Tarski-Seidenberg)**
*Sea $R$ un cuerpo realmente cerrado. Entonces, para cada fórmula $\Psi \in \mathcal{F}_R^{(CFP)}(X_1, \ldots, X_n)$ existe otra fórmula $\Phi \in \mathcal{F}_R(X_1, \ldots, X_n)$ tal que $\Psi \equiv_R \Phi$. Más aún, dada cualquier extensión realmente cerrada $R_1$ del cuerpo $R$, se tiene que $\Psi \equiv_{R_1} \Phi$.*

DEMOSTRACIÓN. Puede consultarse la Proposición 5.2.2 de [**BCR, 1998**]. □

Previamente se discutió la relación entre los conjuntos semi-algebraicos y las FLC. El Principio de Tarski puede reescribirse en el siguiente resultado, enunciado estrictamente en términos de conjuntos semi-algebraicos y sin tocar la TPOCRC, salvo en la prueba que aportaremos.

COROLARIO 1.2.4. **(Proyección de Conjuntos Semi-Algebraicos)**
*Sea $R$ un cuerpo realmente cerrado. Sea $\Pi : R^{n+m} \to R^n$ la proyección que olvida las $m$ últimas coordenadas, es decir, $\Pi(x_1, \ldots, x_n, y_1, \ldots, y_m) = (x_1, \ldots, x_n)$. Entonces, para cada conjunto semi-algebraico $S$ de $R^{n+m}$ se tiene que $\Pi(S)$ es un conjunto semi-algebraico de $R^n$.*

DEMOSTRACIÓN. Sea $S \subset R^{n+m}$ un conjunto semi-algebraico. Entonces, existirá una FLC $\Phi \in \mathcal{F}_R(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$ que define al conjunto semi-algebraico según:

$$S = \{(x, y) \in R^{n+m} : \Phi(x, y) = 1\}.$$

Por otro lado, se tiene que $x \in R^n$ pertenece a la proyección $\Pi(S)$ si y solamente si $(x, y) \in S$ para algún $y \in R^m$. Esto quiere decir que si tomamos la siguiente FCFP:

$$\Psi = \exists Y_1, \ldots, \exists Y_m, \Phi(X_1, \ldots, X_n, Y_1, \ldots, Y_m),$$

podemos establecer la igualdad $\Pi(S) = \{x \in R^n : \Psi(x) = 1\}$. Aquí, basta con aplicar el Principio de Tarski (Teorema 1.2.3) para tener una FLC $\Phi_1 \in \mathcal{F}_R(X_1, \ldots, X_n)$ tal que $\Pi(S)$ sea igual a $\{x \in R^n : \Phi_1(x) = 1\}$, y por lo tanto $\Pi(S)$ es un conjunto semi-algebraico de $R^n$. □

Nótese que, si bien puede asociarse una proyección con la eliminación de un bloque de cuantificadores existenciales, puede aplicarse igualmente para un bloque de cuantificadores universales sin más que considerar que el complementario de un conjunto semi-algebraico es semi-algebraico y que se tiene la siguiente equivalencia semántica:

$$\forall Y, \Phi(X_1, \ldots, X_n, Y) \equiv_{R_1} \nexists Y, \neg(\Phi(X_1, \ldots, X_n, Y)),$$

de fórmulas de $\mathcal{F}_R^{(CFP)}(X_1, \ldots, X_n)$ en alguna extensión $R_1$ realmente cerrada del cuerpo $R$.

En el enunciado del Principio de Tarski puede observarse el sutil detalle de que la FLC que es semánticamente equivalente a otra fórmula de $\mathcal{F}_R^{(CFP)}(X_1, \ldots, X_n)$, lo es para cualquier extensión realmente cerrada del cuerpo $R$. Si nos limitamos a fórmulas sin variables libres, es decir, a enunciados que tienen una interpretación única de verdad o falsedad, entonces se puede enunciar un resultado como el Principio de Transferencia para cuerpos realmente cerrados. Este resultado viene diciendo que la interpretación de un enunciado se transfiere a todos los cuerpos realmente cerrados en los que tenga sentido considerar dicho enunciado.

COROLARIO 1.2.5. **(Principio de Transferencia)**
*Sea $R$ un cuerpo realmente cerrado. Sea $R_1$ una extensión del cuerpo $R$ que también sea realmente cerrada. Sea $\Psi \in \mathcal{F}_R^{(CFP)}(\emptyset)$, es decir, una fórmula cuantificada y sin variables libres. Entonces $\Psi$ se satisface en $R$ si y solamente si $\Psi$ se satisface en $R_1$.*

DEMOSTRACIÓN. Dada la fórmula $\Psi \in \mathcal{F}_R^{(CFP)}(\emptyset)$, aplicando el Principio de Tarski (Teorema 1.2.3) se tiene un enunciado $\Phi \in \mathcal{F}_R(\emptyset)$ que es semánticamente equivalente a $\Psi$ en $R$ y en $R_1$. Como $\Phi$ tiene una interpretación única y que no depende de elementos de $R$ o $R_1$ en cada caso, entonces tendrá la misma interpretación en $R$ y en $R_1$. Es decir, se tendrá que $\Phi = 1$ en $R$ si y solamente si $\Phi = 1$ en $R_1$. Entonces, de $\Psi \equiv_R \Phi$ y $\Psi \equiv_{R_1} \Phi$ se sigue que $\Psi = 1$ en $R$ si y solamente si $\Psi = 1$ en $R_1$. □

Observación 1.2.6. En vista del resultado y de la lectura del resultado hecha previamente, se podría argumentar que alguna fórmula $\Psi \in \mathcal{F}_R^{(CFP)}(\emptyset)$ podría "tener sentido" en algún subcuerpo realmente cerrado $H$ de $R$, es decir, que $\Psi \in \mathcal{F}_H^{(CFP)}(\emptyset)$. En tales casos, la prueba es válida si se considera la FLC que proporciona el Algoritmo de Tarski en el cuerpo $H$.

Ahora, reescribamos el Principio de Transferencia en una forma que nos servirá para la prueba del Teorema del Homomorfismo de Artin-Lang.

Lema 1.2.7. *Sea $R$ un cuerpo realmente cerrado y sea $R_1$ una extensión del cuerpo $R$ que además sea realmente cerrada. Sea $\Phi \in \mathcal{F}_R(X_1, \ldots, X_n)$. Si existe $\overline{x} \in R_1^n$ tal que $\Phi(\overline{x}) = 1$, entonces también existirá $x \in R^n$ tal que $\Phi(x) = 1$.*

Demostración. La condición de que exista $x \in R^n$ o $\overline{x} \in R_1^n$ tales que $\Phi(x) = 1$ o $\Phi(\overline{x}) = 1$, respectivamente, puede escribirse sobre ambos cuerpos como la siguiente FCFP sin variables libres:

$$\Phi(Y_1, \ldots, Y_m) = \exists Y_1, \ldots, \exists Y_m, \phi(Y_1, \ldots, Y_m).$$

Aplicando el Principio de Transferencia (Corolario 1.2.5), se tendrá que si $\Phi = 1$ en $R_1$, entonces $\Phi = 1$ también en $R$. □

Antes de abordar el Teorema del Homomorfismo, veamos algunos aspectos necesarios sobre la noción de $A$-álgebra y los morfismos de $A$-álgebras. Una $A$-álgebra $B$ viene dada por un morfismo de anillos $f : A \to B$, que dota a $B$ de estructura de $A$-módulo definiendo una acción según $a \cdot x = f(a)x$ para $a \in A$ y $x \in B$. Es importante el morfismo $f$ que da estructura de $A$-álgebra a $B$, ya que es necesario para poder definir morfismo de $A$-álgebras. Podría definirse como morfismo de $A$-módulos, pero para evitar la terminología de módulos se elige esta definición equivalente.

Definición 8. **(Morfismo de $A$-álgebras)**
*Sea $A$ un anillo conmutativo. Sean $B_1$ y $B_2$ un par de $A$-álgebras dadas por los morfismos $f_1 : A \to B_1$ y $f_2 : A \to B_2$. Un morfismo de anillos $\psi : B_1 \to B_2$ se dice morfismo de $A$-álgebras si además cumple $\psi \circ f_1 = f_2$.*

Observación 1.2.8. Sean $B_1$, $B_2$ y $B_3$ tres $A$-álgebras dadas por los morfismos $f_1$, $f_2$ y $f_3$, respectivamente. Si $\psi : B_1 \to B_2$ y $\varphi : B_2 \to B_3$ son un par de morfismos de $A$-álgebras, entonces su composición $\varphi \circ \psi$ será un morfismo de $A$-álgebras de $B_1$ en $B_3$. Esto es debido a que, como $\psi \circ f_1 = f_2$ y $\varphi \circ f_2 = f_3$, entonces $\varphi \circ \psi \circ f_1 = \varphi \circ f_2 = f_3$.

Definición 9. **($A$-álgebra Finitamente Generada)**
*Sea $A$ un anillo conmutativo. Sea $B$ una $A$-álgebra. $B$ se dice finitamente generada si para algún ideal $\mathfrak{a} \subset A[X_1, \ldots, X_n]$ se tiene que $B$ sea isomorfa a $A[X_1, \ldots, X_n]/\mathfrak{a}$.*

Observación 1.2.9. En el caso particular en el que $A$ sea un cuerpo, cualquier morfismo de anillos $f : A \to B$ será inyectivo, pues $ker(f)$ es un ideal de $A$ y este solo puede ser $(0)$ o $A$. Si fuese $ker(f) = A$, entonces $f(1) = 0$ y se contradice que $f$ sea morfismo de anillos. Entonces el morfismo $f : A \to B$ es la inclusión de $A$ en $B$, en el sentido de que $f(A)$ es un cuerpo isomorfo a $A$ y contenido en $B$. Adicionalmente, si $B_1$ y $B_2$ son un par de $A$-álgebras que sean isomorfas como anillos, entonces existe algún isomorfismo entre $B_1$ y $B_2$ que sea morfismo de $A$-álgebras. Consideremos los morfismos $f_1 : A \to B_1$ y $f_2 : A \to B_2$ que dotan a $B_1$ y $B_2$ de estructura de $A$-álgebra. Entonces $A$, $f_1(A)$ y $f_2(A)$ son cuerpos isomorfos y puede darse un isomorfismo de anillos $\psi : B_1 \to B_2$ que restringido a $f_1(A)$ sea un isomorfismo entre $f_1(A)$ y $f_2(A)$.

Finalmente, pasemos a enunciar y probar el Teorema del Homomorfismo de Artin-Lang. Se habla de homomorfismo en lugar de morfismo para respetar la forma habitual de encontrar este resultado en la literatura, pero ambos términos se refieren al mismo tipo de objeto.

Teorema 1.2.10. **(Teorema del Homomorfismo de Artin-Lang)**
*Sea $R$ un cuerpo realmente cerrado y sea $A$ una $R-$álgebra finitamente generada. Si existe un homomorfismo de $R$-álgebras $\varphi$ de $A$ en alguna extensión $R_1$ del cuerpo $R$ que sea realmente cerrada, entonces existe un homomorfismo de $R$-álgebras $\psi : A \longrightarrow R$.*

Demostración. La $R$-álgebra finitamente generada $A$ es isomorfa a una $R$-álgebra de la forma $B = R[X_1, \ldots, X_n]/\mathfrak{a}$, donde $\mathfrak{a}$ es un ideal de $R[X_1, \ldots, X_n]$. Por ser $R$ cuerpo y de acuerdo con la Observación 1.2.9, existirá un isomorfismo de $R$-álgebras de $A$ en $B$. Llámese $\phi$.

Considerando el morfismo de $R$-álgebras $\varphi : A \longrightarrow R_1$ y la Observación 1.2.8, se tiene el morfismo de $R$-álgebras $\Psi = \varphi \circ \phi^{-1} : B \longrightarrow R_1$, que además cumple que $\Psi|_R = Id_R$. Sea $b = (b_1, \ldots, b_n) \in R_1^n$ definido por $b_i = \Psi(X_i + \mathfrak{a})$ para $i = 1, \ldots, n$. Dado cualquier polinomio $f + \mathfrak{a} \in B$ y teniendo en cuenta que $\Psi$ es morfismo de anillos, escribiendo a $f$ como suma finita de monomios se tienen las siguientes igualdades:

$$\Psi(f + \mathfrak{a}) = \sum_{\substack{\mu \leq d \\ \mu = \mu_1 + \ldots + \mu_n}} \alpha_{\mu_1, \ldots, \mu_n} \Psi((X_1 + \mathfrak{a})^{\mu_1}) \cdot \ldots \cdot \Psi((X_n + \mathfrak{a})^{\mu_n}) =$$

$$= \sum_{\substack{\mu \leq d \\ \mu = \mu_1 + \ldots + \mu_n}} \alpha_{\mu_1, \ldots, \mu_n} b_1^{\mu_1} \cdot \ldots \cdot b_n^{\mu_n} = f(b_1, \ldots, b_n).$$

Para cualquier $f \in \mathfrak{a}$ se tiene que $f + \mathfrak{a} = 0 + \mathfrak{a}$, y por lo tanto $0 = \Psi(0 + \mathfrak{a}) = \Psi(f + \mathfrak{a}) = f(b_1, \ldots, b_n)$. Entonces $(b_1, \ldots, b_n) \in \mathcal{Z}_{R_1^n}(\mathfrak{a})$, y este es un conjunto semi-algebraico descrito por la siguiente FLC sobre $R$, aunque vista como fórmula sobre $R_1$:

$$\Phi(X_1, \ldots, X_n) = (f_1(X_1, \ldots, X_n) = 0) \wedge \ldots \wedge (f_p(X_1, \ldots, X_n) = 0).$$

Como $\Phi(b_1, \ldots, b_n) = 1$, aplicando el Lema 1.2.7 existirá $a = (a_1, \ldots, a_n) \in R^n$ tal que $\Phi(a_1, \ldots, a_n) = 1$ y que, por lo tanto, pertenezca a $\mathcal{Z}_{R^n}(\mathfrak{a})$. Se considera el ideal maximal $\mathfrak{m}_a = (X_1 - a_1, \ldots, X_n - a_n)$. Este ideal es el núcleo del morfismo de evaluación en $a$, es decir, $\mathfrak{m}_a = \{f \in R[X_1, \ldots, X_n] : f(a) = 0\}$. Entonces se tiene el siguiente epimorfismo:

$$\begin{aligned} \pi : R[X_1, \ldots, X_n]/\mathfrak{m}_a &\longrightarrow R \\ f + \mathfrak{m}_a &\longmapsto f(a). \end{aligned}$$

Dado que todo $f \in \mathfrak{a}$ tiene a $a$ como raíz, se sigue que $\mathfrak{a} \subset \mathfrak{m}_a$, y al paso al cociente por $\mathfrak{a}$ se tiene que $\mathfrak{m}_a/\mathfrak{a} \in MaxSpec(B)$. Aplicando el Segundo Teorema de Isomorfía se tiene:

$$B \xrightarrow{\pi_1} B/(\mathfrak{m}_a/\mathfrak{a}) \cong R[X_1, \ldots, X_n]/\mathfrak{m}_a \xrightarrow{\pi} R,$$

donde $\pi_1$ es la proyección canónica en el anillo cociente de $B$ por el maximal $\mathfrak{m}_a/\mathfrak{a}$, que también es epimorfismo. En definitiva, se tiene el epimorfismo de anillos:

$$\begin{aligned} \Theta : \ B &\longrightarrow R \\ f + \mathfrak{a} &\longmapsto f(a). \end{aligned}$$

Finalmente, recuperando el isomorfismo de $R$-álgebras $\phi : A \to B$ se construye el morfismo de $R$-álgebras $\psi = \Theta \circ \phi : A \to R$, de lo que se concluye la propiedad del enunciado. □

## 1.3. Nullstellensatz Real.

El objetivo de todo el capítulo es completar la prueba de un Nullstellensatz Real, y es lo que se lleva a cabo en esta sección. Para el Nullstellensatz Real al estilo de Rabinowitsch, veremos un nuevo tipo de ideales que estarán en biyección con las variedades algebraicas de un cuerpo realmente cerrado, y que se definirá seguidamente. También veremos la versión del Nullstellensatz Real al estilo de Hilbert-Kronecker, la cual difiere del resultado para cuerpos algebraicamente cerrados.

Definición 10. **(Ideal Real)**
*Sea $A$ un anillo conmutativo. Un ideal $\mathfrak{a}$ contenido en $A$ se dice real si para todo $a_1, \ldots, a_r \in A$ se cumple que:*

$$a_1^2 + \ldots + a_r^2 \in \mathfrak{a} \Rightarrow a_i \in \mathfrak{a}, \text{ para cada } i = 1, \ldots, r.$$

Veamos que este tipo de ideales son radicales.

Proposición 1.3.1. *Sea $A$ un anillo conmutativo. Sea $\mathfrak{a}$ un ideal real de $A$. Entonces $\mathfrak{a}$ es ideal radical.*

Demostración. Tomemos $a^n \in \mathfrak{a}$ y veamos que $a \in \mathfrak{a}$. Sin pérdida de generalidad se toma $n$ como el elemento minimal de $\{k \in \mathbb{N} : a^k \in \mathfrak{a}, k \geq 1\}$. Si $n = 1$ no hay nada que probar, supongamos que $n > 1$. Por ser $\mathfrak{a}$ un ideal real, en el caso en que $n$ sea par, se tendría que $a^{\frac{n}{2}} \in \mathfrak{a}$. Si $n$ fuese impar, por ser $\mathfrak{a}$ ideal y $a \in A$, se tiene que $aa^n \in \mathfrak{a}$ y, entonces, $a^{\frac{n+1}{2}} \in \mathfrak{a}$. En ambos casos se tiene una contradicción con que $n$ sea elemento minimal y por lo tanto $a \in \mathfrak{a}$. □

Observación 1.3.2. No todo ideal radical es un ideal real. Basta con considerar el ejemplo del ideal radical $\mathfrak{a} = (X_1^2+1)$ de $R[X_1,\dots,X_n]$, que claramente no es ideal real porque $X_1^2+1^2 \in \mathfrak{a}$ pero $X_1 \notin \mathfrak{a}$. El ideal es radical porque es primo, y se trata de un ideal primo porque $X_1^2+1$ no tiene raíces en $R^n$, luego es irreducible y genera un ideal primo.

Antes de meternos de lleno con la prueba del Nullstellensatz Real, revisemos varios aspectos generales de la descomposición primaria de ideales en anillos noetherianos. En primer lugar se definen los ideales primarios. Ello requiere del uso de la siguiente familia de aplicaciones, que se definen para cada elemento $a$ de un anillo conmutativo $A$ y dado un ideal $\mathfrak{q} \subset A$:

$$\begin{aligned} \eta_a : A/\mathfrak{q} &\longrightarrow A/\mathfrak{q} \\ x+\mathfrak{q} &\longmapsto ax+\mathfrak{q}. \end{aligned}$$

La aplicación $\eta_a$ se conoce como homotecia de razón $a$. Puede probarse que el conjunto de homotecias en $A/\mathfrak{q}$ forma un anillo junto con la suma y la composición de aplicaciones, siendo que $\eta_a+\eta_b = \eta_{a+b}$ y que $\eta_a \circ \eta_b = \eta_{ab}$. En este sentido, $\eta_a$ se dirá nilpotente precisamente cuando $(\eta_a)^n = \eta_0$ para algún $n \in \mathbb{N}$.

Definición 11. **(Ideal Primario)**
*Sea $A$ un anillo conmutativo. Un ideal $\mathfrak{q}$ contenido en $A$ se dice primario si para todo $a \in A$ la aplicación homotecia de razón $a$, $\eta_a$, es inyectiva o nilpotente.*

Observación 1.3.3. Puede probarse que el radical de un ideal primario $\mathfrak{q}$ es un ideal primo $\mathfrak{p} = \sqrt{\mathfrak{q}}$. En tal caso $\mathfrak{q}$ se dice ideal $\mathfrak{p}$-primario.

Ahora se define una descomposición primaria de un ideal y también una descomposición primaria irredundante, que esencialmente es una descomposición primaria sin exceso de ideales.

Definición 12. **(Descomposición Primaria Irredundante)**
*Sea $A$ un anillo conmutativo. Sea $\mathfrak{a} \subset A$ un ideal. Se llama descomposición primaria de $\mathfrak{a}$ a una descripción del ideal como intersección de ideales primarios, es decir, $\mathfrak{q}_1,\dots,\mathfrak{q}_r$ ideales primarios tales que:*

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r.$$

*Sea $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ para cada $i = 1,\dots,r$, esto es, sea $\mathfrak{q}_i$ ideal $\mathfrak{p}_i$-primario. La descomposición previa se dice irredundante si además $i \neq j$ implica que $\mathfrak{p}_i \neq \mathfrak{p}_j$, y $\mathfrak{a}$ no puede describirse como la intersección de algún subconjunto propio de $\{\mathfrak{q}_1,\dots,\mathfrak{q}_r\}$.*

Por una parte, un ideal no siempre admite una descomposición primaria,[6] y por otra parte, el refinamiento de una descomposición primaria en una descomposición primaria irredundante no siempre lleva a una descomposición primaria irredundante que sea única. Para el caso de anillos noetherianos se tiene el llamado Teorema de Lasker-Noether, que asegura la existencia de descomposición primaria de cualquier ideal en estos anillos. Aunque en general la descomposición primaria irredundante de un ideal de un anillo noetheriano no sea única, este resultado también establece algunos aspectos que comparten todas las descomposiciones primarias irredundantes de cada ideal. A continuación se muestra el enunciado sin demostración:[7]

Teorema 1.3.4. **(de Lasker-Noether)**
*Sea $A$ un anillo noetheriano. Entonces todo ideal propio de $A$ admite una descomposición primaria irredundante. Además, dado un par de descomposiciones primarias irredundantes de un ideal $\mathfrak{a} \subset A$,*

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r = \tilde{\mathfrak{q}}_1 \cap \cdots \cap \tilde{\mathfrak{q}}_s$$

*donde $\mathfrak{q}_i$ es ideal $\mathfrak{p}_i$-primario para $i = 1,\dots,r$, y $\tilde{\mathfrak{q}}_j$ es ideal $\tilde{\mathfrak{p}}_j$-primario para $j = 1,\dots,s$; entonces $r = s$ y, salvo reordenación de subíndices, $\mathfrak{p}_i = \tilde{\mathfrak{p}}_i$ para $i = 1,\dots,r$. Es decir, la lista de ideales primos $\mathfrak{p}_1,\dots,\mathfrak{p}_r$ no depende de la descomposición primaria del ideal $\mathfrak{a}$, estos se dicen los primos asociados al ideal $\mathfrak{a}$ y se denota dicho conjunto por $Ass(\mathfrak{a})$.*

Observación 1.3.5. Puede probarse que si el ideal $\mathfrak{a}$ es radical, entonces $\mathfrak{a} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$. Considerando el resultado previo, se tiene además que esta es la única descomposición primaria irredundante que admite $\mathfrak{a}$. Además, esta descomposición primaria es la intersección de todos

[6] Puede consultarse un contraejemplo en los Apartados 2.21 y 8.16 de [**Sharp, 1990**].
[7] Puede encontrarse una prueba en el Capítulo 6 de [**Pardo, 2023**].

los ideales primos minimales que contienen a $\mathfrak{a}$. La justificación para esto último es la siguiente. Supongamos que para algún $k \in \{1, \ldots, r\}$, exista un ideal $\mathfrak{b}$ tal que $\mathfrak{a} \subset \mathfrak{b} \subset \mathfrak{p}_k$. Sin pérdida de generalidad, tomemos $k = r$. En tal caso $\mathfrak{a} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r \cap \mathfrak{b} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{r-1} \cap \mathfrak{b}$. El Teorema de Lasker-Noether (Teorema 1.3.4) asegura que $\mathfrak{p}_r$ y $\mathfrak{b}$ son ambos ideales $\mathfrak{p}_r$-primarios, y entonces como $\mathfrak{a}$ es ideal radical, $\mathfrak{b} = \sqrt{\mathfrak{b}} = \mathfrak{p}_r$.

Tras esta breve exposición de la descomposición primaria de ideales, pasemos a probar las siguientes propiedades que resultarán de utilidad más tarde.

LEMA 1.3.6. *Sea $A$ un anillo conmutativo. Entonces:*

*(i) todo ideal primo $\mathfrak{a}$ es real si y solamente si el cuerpo de fracciones de $A/\mathfrak{a}$ es un cuerpo formalmente real,*

*(ii) si además $A$ es noetheriano, entonces todos los ideales primos minimales que contienen a un ideal real son reales.*

DEMOSTRACIÓN. Para probar $(i)$, llamemos $F$ al cuerpo de fracciones del dominio $A/\mathfrak{a}$. Asumamos que $F$ sea formalmente real y veamos que entonces $\mathfrak{a}$ es ideal real. Sean $a_1, \ldots, a_r \in A$ tales que $a_1^2 + \ldots + a_r^2 \in \mathfrak{a}$. Para un elemento $a \in A$ denotamos su clase en el anillo cociente por $\bar{a}$, y también como elemento de $F$. Los elementos de $\mathfrak{a}$ estarán en la misma clase que $\bar{0}$, por lo tanto en $F$ se tendrá que $\overline{a_1^2 + \ldots + a_r^2} = \bar{0}$. Como $F$ es cuerpo formalmente real, por definición, se tiene que $\bar{a}_i = \bar{0}$ para cada $i = 1, \ldots, r$. Esto implica que $a_1, \ldots, a_r$ sean elementos de $\mathfrak{a}$ y por lo tanto $\mathfrak{a}$ sea ideal real.

Pasemos a probar el recíproco. Supongamos que $\mathfrak{a}$ sea ideal real y comprobemos que $F$ sea cuerpo formalmente real. Sean $\bar{a}_1, \ldots, \bar{a}_r \in F$ tales que $\bar{a}_1^2 + \ldots + \bar{a}_r^2 = \bar{0}$. Con las operaciones sobre las clases de $F$ puede escribirse $\overline{a_1^2 + \ldots + a_r^2} = \bar{0}$, por lo que $a_1^2 + \ldots + a_r^2$ es un elemento de $\mathfrak{a}$. Como $\mathfrak{a}$ es ideal real se tiene que $a_1, \ldots, a_r \in \mathfrak{a}$ y por lo tanto sus clases cumplen $\bar{a}_1 = \cdots = \bar{a}_r = \bar{0}$. Con esto se concluye que $F$ sea un cuerpo formalmente real.

Pasemos a probar $(ii)$. Sea $\mathfrak{p} \in Spec(A)$ un ideal minimal para la inclusión y que contenga a un ideal real $\mathfrak{a}$. Por la Proposición 1.3.1, se tiene que $\mathfrak{a}$ es ideal radical. El anillo $A$ es noetheriano y por ello, aplicando el Teorema de Lasker-Noether 1.3.4, se tiene que $\mathfrak{a}$ admite una descomposición primaria irredundante $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ donde cada ideal $\mathfrak{q}_i$ es $\mathfrak{p}_i$-primario, con $\mathfrak{p}_i \in Spec(A)$ y los $\mathfrak{p}_i$ dos a dos distintos. De hecho, por la Observación 1.3.5 se tendrá que $\mathfrak{a} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$ y además esta es la única descomposición primaria irredundante que admite el ideal. Como $\mathfrak{p}$ es minimal en $Spec(A)$, se tiene que $\mathfrak{p} \subset \mathfrak{p}_1$ y entonces $\mathfrak{a} = \mathfrak{p} \cap \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$, pero como la descomposición primaria irredundante de $\mathfrak{a}$ es única, se tiene que $\mathfrak{p} = \mathfrak{p}_i$ para algún $i \in \{1, \ldots, r\}$. Por lo tanto, es suficiente ver que cada $\mathfrak{p}_i$ sea un ideal real.

Supongamos ahora que, de entre los ideales primos minimales, exista alguno que no sea real. Sin pérdida de generalidad, supongamos que el ideal $\mathfrak{p}_1$ no es real. Entonces existirán $a_1, \ldots, a_r \in A$ tales que $a_1^2 + \ldots + a_s^2 \in \mathfrak{p}_1$, de tal modo que alguno de los $a_i$ no pertenezca a $\mathfrak{p}_1$. Sin pérdida de generalidad puede suponerse también que $a_1 \notin \mathfrak{p}_1$.

Como los $\mathfrak{p}_i$ son dos a dos distintos, puede escogerse $b_i \in \mathfrak{p}_i \setminus \mathfrak{p}_1$ para $i = 2, \ldots, r$. Se define el elemento $b = b_2 \cdot \ldots \cdot b_r$, que pertenece a $\mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_r$. Se observa que al tenerse $a_1^2 + \ldots + a_s^2 \in \mathfrak{p}_1$ y $b \in \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_r$ entonces $(a_1 b)^2 + \ldots + (a_s b)^2 \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r = \mathfrak{a}$.

El ideal $\mathfrak{a}$ es real y por lo tanto $a_1 b \in \mathfrak{a} \subset \mathfrak{p}_1$, pero esto no es posible porque $\mathfrak{p}_1$ es un ideal primo y $a_1, b \notin \mathfrak{p}_1$. En conclusión, no puede escogerse $a_1, \ldots, a_s \in A$ tales que $a_1^2 + \ldots + a_s^2 \in \mathfrak{p}_1$ y de tal modo que alguno de los $a_i$ no pertenezca a $\mathfrak{p}_1$, por lo tanto $\mathfrak{p}_1$ es un ideal real. □

Veamos ahora una versión preliminar del Nullstellensatz Real, que se enuncia como sigue.

TEOREMA 1.3.7. *Sea $R$ un cuerpo realmente cerrado. Sea $\mathfrak{a} \subset R[X_1, \ldots, X_n]$ un ideal. Entonces $\mathfrak{a} = \mathcal{I}_{R[X_1,\ldots,X_n]}(\mathcal{Z}_{R^n}(\mathfrak{a}))$ si y solamente si $\mathfrak{a}$ es ideal real.*

DEMOSTRACIÓN. Denotamos $R[X] = R[X_1, \ldots, X_n]$ y supongamos que $\mathfrak{a} = \mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{a}))$. Sean $f_1, \ldots, f_r$ polinomios de $R[X]$ tales que $f_1^2 + \ldots + f_r^2 \in \mathfrak{a}$. Se cumple $(f_1^2 + \ldots + f_r^2)(x) = 0$ para cada $x \in \mathcal{Z}_{R^n}(\mathfrak{a})$. Dado que $R$ es un cuerpo formalmente real, se tiene que $f_i(x) = 0$ para todo $x \in \mathcal{Z}_{R^n}(\mathfrak{a})$ y para cada $i = 1, \ldots, r$. Por lo tanto, $f_1, \ldots, f_r \in \mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{a})) = \mathfrak{a}$ luego $\mathfrak{a}$ es ideal real.

Ahora, supongamos que $\mathfrak{a}$ sea un ideal real. De manera trivial se tiene que $\mathfrak{a} \subset \mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{a}))$. Para probar el otro contenido, tomemos un polinomio $f \in R[X]$ tal que $f \notin \mathfrak{a}$ y veamos que $f \notin \mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{a}))$. Primero, probaremos esta afirmación para el caso en que $\mathfrak{a}$ sea un ideal primo de $R[X]$. Después, abordaremos la misma afirmación para el caso en que $\mathfrak{a}$ sea un ideal cualquiera, utilizando la descomposición primaria de $\mathfrak{a}$.

Supongamos que $\mathfrak{a}$ sea un ideal primo. Aplicando la Afirmación $(i)$ del Lema 1.3.6 se tiene que el cuerpo de fracciones $F = Frac(R[X]/\mathfrak{a})$ es un cuerpo formalmente real. Para cada polinomio $f \in R[X]$, se denotará su correspondiente clase de equivalencia en el anillo cociente $R[X]/\mathfrak{a}$ por $\overline{f}$. Sea $R_1$ la clausura real de $F$. Se define también el anillo de fracciones $A = M[\overline{f}]^{-1}R[X]/\mathfrak{a}$, donde $M[\overline{f}]$ denota el sistema multiplicativo generado por $\overline{f}$. Claramente, $A$ está contenido en $F$ y por lo tanto, también está contenido en $R_1$. Se considera la aplicación inclusión $\varphi : A \to R_1$, que se trata de un morfismo inyectivo de anillos. Considerando sendas inclusiones de $R$ en $A$ y $R_1$, se sigue que ambos son $R$-álgebras. Como $\varphi|_R = Id_R$, entonces $\varphi$ es morfismo de $R$-álgebras.

Vamos a probar que $A$ es una $R$-álgebra finitamente generada. Consideremos la aplicación:

$$\begin{aligned} \phi : \quad R[X][X_{n+1}] \quad &\longrightarrow \qquad A \\ \sum_{i=0}^{k} h_i(X) X_{n+1}^i \quad &\longmapsto \sum_{i=1}^{k} \overline{h_i(X)} \frac{\overline{1}}{\overline{f}^i}, \end{aligned}$$

y veamos que se trata de un morfismo de anillos. Está claro que $\phi(0) = \overline{0}$ y $\phi(1) = \overline{1}$. Sean $g,\ h \in R[X][X_{n+1}]$. Pueden escribirse como $g = \sum_{i=0}^{r} g_i X_{n+1}^i$ y $h = \sum_{j=0}^{s} h_j X_{n+1}^j$, donde $g_0, \ldots, g_r, h_0, \ldots, h_s \in R[X]$. Entonces, tomando $g_i = 0 = h_j$ para $i > r$, $j > s$:

$$\phi(g+h) = \sum_{i=0}^{r+s} \overline{(g_i + h_i)} \frac{\overline{1}}{\overline{f}^i} = \sum_{i=0}^{r} \overline{g}_i \frac{\overline{1}}{\overline{f}^i} + \sum_{j=0}^{s} \overline{h}_j \frac{\overline{1}}{\overline{f}^j} = \phi(g) + \phi(h).$$

Por otra parte:

$$\phi(gh) = \sum_{i=0}^{rs} \left( \sum_{j=0}^{i} \overline{g_{i-j} h_j} \right) \frac{\overline{1}}{\overline{f}^i} = \sum_{i=0}^{rs} \sum_{j=0}^{i} \overline{g}_{i-j} \frac{\overline{1}}{\overline{f}^{i-j}} \overline{h}_j \frac{\overline{1}}{\overline{f}^j} = \left( \sum_{i=0}^{r} \overline{g}_i \frac{\overline{1}}{\overline{f}^i} \right) \left( \sum_{j=0}^{s} \overline{h}_j \frac{\overline{1}}{\overline{f}^j} \right) = \phi(g)\phi(h).$$

Con esto terminamos de probar que $\phi$ es morfismo de anillos. Veamos que es además es sobreyectivo. Dado un elemento $\overline{g}/\overline{f}^k \in A$, con $g \in R[X]$ y $k \in \mathbb{N}$, se tiene que es imagen de $gX_{n+1}^k \in R[X][X_{n+1}]$. Esto supone un isomorfismo de $R[X][X_{n+1}]/ker(\phi)$ en $A$, y por lo tanto $A$ es $R$-álgebra finitamente generada.

Considerando que $A$ es una $R$-álgebra finitamente generada y que $R_1$ es una extensión de $R$, puede aplicarse el Teorema del Homomorfismo de Artin-Lang (Teorema 1.2.10) y tomarse el morfismo de $R$-álgebras $\psi : A \longrightarrow R$. Se define $x = (\psi(\bar{X}_1), \ldots, \psi(\bar{X}_n)) \in R^n$ y se observa que, dado $h \in R[X]$:

$$\psi(\overline{h}) = \sum_{\substack{\mu \leq d \\ \mu = \mu_1 + \ldots + \mu_n}} \alpha_{\mu_1, \ldots, \mu_n} \psi(\bar{X}_1)^{\mu_1} \cdot \ldots \cdot \psi(\bar{X}_n)^{\mu_n} = h(x).$$

En particular, para $g \in \mathfrak{a}$ se tiene que $\bar{g} = \bar{0}$ en $A$, y entonces $0 = \psi(\bar{0}) = \psi(\bar{g}) = g(x)$. De esto se sigue que $x \in \mathcal{Z}_{R^n}(\mathfrak{a})$. Volvamos al polinomio $f \notin \mathfrak{a}$. $\overline{f}$ es unidad en $A$, luego $1 = \psi(1) = \psi(\overline{f})\psi(\overline{1}/\overline{f})$ y, $\psi(\overline{f}) \neq 0$ necesariamente. Como entonces $f(x) \neq 0$, se concluye que $f \notin \mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{a}))$. Con esto queda probado el resultado en el caso de que $\mathfrak{a}$ sea un ideal primo.

Consideremos el caso general en que $\mathfrak{a}$ sea ideal real. El ideal $\mathfrak{a}$ es radical por la Proposición 1.3.1 y, considerando la Observación 1.3.5, se tendrá una descomposición primaria irredundante $\mathfrak{a} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$ donde los ideales $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ son los primos minimales que contienen a $\mathfrak{a}$. Con esto, aplicando la Afirmación $(ii)$ del Lema 1.3.6, se deduce que los ideales $\mathfrak{p}_i$ son reales.

Previamente se ha probado que $\mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{p}_i)) = \mathfrak{p}_i$ para $i = 1, \ldots, r$. Por otra parte, se tiene que $\mathfrak{a} \subset \mathfrak{p}_i$ para cada $i = 1, \ldots, r$, y se conoce que $\mathfrak{a} \subset \mathfrak{p}_i$ implica que $\mathcal{Z}_{R^n}(\mathfrak{p}_i) \subset \mathcal{Z}_{R^n}(\mathfrak{a})$, que a su vez implica que $\mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{a})) \subset \mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{p}_i))$. Ambos hechos llevan a que $\mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{a}))$ esté incluido en cada $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, y por lo tanto $\mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{a})) \subset \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r = \mathfrak{a}$. $\square$

Ahora se define el radical real de un ideal $\mathfrak{a}$ de un anillo conmutativo $A$, que además será el menor ideal real que contenga al ideal $\mathfrak{a}$.

PROPOSICIÓN 1.3.8. *Sea $A$ un anillo conmutativo y sea $\mathfrak{a}$ un ideal de $A$. Se define el siguiente conjunto:*

$$\sqrt[R]{\mathfrak{a}} = \{a \in A : \exists m \in \mathbb{N},\ \exists b_1, \ldots, b_r \in A\ a^{2m} + b_1^2 + \ldots + b_r^2 \in \mathfrak{a}\}.$$

*Entonces $\sqrt[R]{\mathfrak{a}}$ es el menor ideal real de $A$ que contiene a $\mathfrak{a}$ y se le llama radical real de $\mathfrak{a}$.*

DEMOSTRACIÓN. En primer lugar, se introduce como notación que $\sum A^2$ sea el conjunto de las sumas de cuadrados de elementos de $A$. Claramente, la suma de todo par de elementos de $\sum A^2$ pertenece a $\sum A^2$, y el producto también, observando que $(a_1^2 + \ldots + a_r^2)(b_1^2 + \ldots + b_s^2)$ es igual que $\sum_{i=1}^{r}\sum_{j=1}^{s}(a_i b_j)^2$. Entonces $x \in A$ pertenece a $\sqrt[R]{\mathfrak{a}}$ si y solo si existen $m \in \mathbb{N}$, $a \in \mathfrak{a}$ y $c \in \sum A^2$ tales que $x^{2m} = a - c$. Ahora, veamos que el subconjunto $\sqrt[R]{\mathfrak{a}}$ sea un ideal de $A$. Sean $x, y \in \sqrt[R]{\mathfrak{a}}$ y $b \in A$. Se tiene que $x^{2m} = a - c$ y que $x^{2m'} = a' - c'$ para algunos $m, m' \in \mathbb{N}$, $a, a' \in \mathfrak{a}$ y $c, c' \in \sum A^2$. Primero se observa que $(bx)^{2m} = b^{2m}a - b^{2m}c$, con $b^{2m}a \in \mathfrak{a}$ por ser un ideal y $b^{2m}c \in \sum A^2$ por ser $b^{2m}$ el cuadrado de $b^m$, por lo que $bx \in \sqrt[R]{\mathfrak{a}}$.

Falta probar que $x + y \in \sqrt[R]{\mathfrak{a}}$. Sea $k = m + m'$. Utilizando el Binomio de Newton, se deducen las identidades:

$$(x+y)^{2k} = \sum_{\substack{i=0\\ i+j=2k}}^{2k} \gamma_{i,j} x^i y^j, \qquad (x-y)^{2k} = \sum_{\substack{i=0\\ i+j=2k}}^{2k} (-1)^j \gamma_{i,j} x^i y^j,$$

donde los $\gamma_{i,j}$ son elementos de $\mathbb{Z}$ y el producto por un elemento de $A$ es notación aditiva. Observando que en cada término de las sumas $i$ y $j$ son pares o no simultáneamente, puede escribirse:

$$(x+y)^{2k} = \sum_{\substack{i=0\\ i+j=2k\\ i\in 2\mathbb{N}}}^{2k} \gamma_{i,j} x^i y^j + \sum_{\substack{i=0\\ i+j=2k\\ i\in 2\mathbb{N}+1}}^{2k} \gamma_{i,j} x^i y^j,$$

$$(x-y)^{2k} = \sum_{\substack{i=0\\ i+j=2k\\ i\in 2\mathbb{N}}}^{2k} \gamma_{i,j} x^i y^j - \sum_{\substack{i=0\\ i+j=2k\\ i\in 2\mathbb{N}+1}}^{2k} \gamma_{i,j} x^i y^j.$$

Entonces la suma de ambos queda así:

$$(x+y)^{2k} + (x-y)^{2k} = \sum_{\substack{i=0\\ i+j=2k\\ i\in 2\mathbb{N}}}^{2k} 2\gamma_{i,j} x^i y^j =$$

$$= x^{2m}\left(\sum_{\substack{i=2m\\ i+j=2k\\ i\in 2\mathbb{N}}}^{2k} 2\gamma_{i,j} x^{i-2m} y^j\right) + y^{2m'}\left(\sum_{\substack{i=0\\ i+j=2k\\ i\in 2\mathbb{N}}}^{2(m-1)} 2\gamma_{i,j} x^i y^{j-2m'}\right),$$

donde las sumas entre paréntesis son sumas de cuadrados de $A$ y se denotarán por $d$ y $d'$, respectivamente. Finalmente puede escribirse:

$$(x+y)^{2k} = x^{2m}d + y^{2m'}d' - (x-y)^{2k} = ad - cd + a'd' - c'd' - (x-y)^{2k} =$$
$$= (ad + a'd') - (cd + c'd' + (x-y)^{2k}),$$

y se tiene que $x + y \in \sqrt[R]{\mathfrak{a}}$. Con esto se concluye que $\sqrt[R]{\mathfrak{a}}$ sea un ideal.

Veamos que $\sqrt[R]{\mathfrak{a}}$ sea un ideal real. Sean $b_1, \ldots, b_r \in A$ tales que $b_1^2 + \ldots + b_r^2 \in \sqrt[R]{\mathfrak{a}}$. Entonces existen $m \in \mathbb{N}$, $a \in \mathfrak{a}$ y $c \in \sum A^2$ tales que $(b_1^2 + \ldots + b_r^2)^{2m} = a - c$. De nuevo, se usa el Binomio de Newton:

$$(b_1^2 + \ldots + b_r^2)^{2m} = \sum_{\substack{i=0\\ i+j=2m}}^{2m} \gamma_{i,j} b_1^{2i}(b_2^2 + \ldots + b_r^2)^j = b_1^{4m} + \sum_{\substack{i=1\\ i+j=2m}}^{2m} \gamma_{i,j} b_1^{2i}(b_2^2 + \ldots + b_r^2)^j,$$

considerando que $\gamma_{2m,0} = 1$. La suma del término de la derecha, que llamaremos $d$, pertenece a $\sum A^2$, dado que es suma y producto de elementos de $\sum A^2$. Entonces se tiene la igualdad $b_1^{4m} = a - (c + d)$ y por lo tanto $b_1 \in \sqrt[R]{\mathfrak{a}}$, de lo que se concluye que $\sqrt[R]{\mathfrak{a}}$ es un ideal real.

Veamos ahora que $\sqrt[R]{\mathfrak{a}}$ es el menor ideal real que contiene a $\mathfrak{a}$. Dado un elemento $a \in \mathfrak{a}$ se tiene que $a^2 \in \mathfrak{a}$, por lo tanto $a \in \sqrt[R]{\mathfrak{a}}$ y se deduce que $\mathfrak{a} \subset \sqrt[R]{\mathfrak{a}}$. Sea $\mathfrak{b}$ un ideal real de $A$ que contiene a $\mathfrak{a}$, y que además esté contenido en $\sqrt[R]{\mathfrak{a}}$. Es trivial que si $\mathfrak{a} \subset \mathfrak{b}$ entonces $\sqrt[R]{\mathfrak{a}} \subset \sqrt[R]{\mathfrak{b}}$. Para concluir que $\sqrt[R]{\mathfrak{a}}$ es el menor ideal real que contiene a $\mathfrak{a}$, probaremos que $\mathfrak{b} = \sqrt[R]{\mathfrak{b}}$ y así se tendrá que $\sqrt[R]{\mathfrak{a}} = \mathfrak{b}$. Por el argumento previo de que $\mathfrak{a}$ está contenido en $\sqrt[R]{\mathfrak{a}}$, está claro que $\mathfrak{b} \subset \sqrt[R]{\mathfrak{b}}$. Si $a \in \sqrt[R]{\mathfrak{b}}$, entonces existen $m \in \mathbb{N}$ y $c_1, \ldots, c_r \in A$ tales que $a^{2m} + c_1^2 + \ldots + c_r^2 \in \mathfrak{b}$. $\mathfrak{b}$ es ideal real y por la Proposición 1.3.1, es además radical, luego $a \in \mathfrak{b}$. Con esto queda probada la igualdad, y en consecuencia el enunciado. □

Conocido el radical real de un ideal, es posible establecer una versión del Nullstellensatz Real al estilo de Rabinowitsch.

COROLARIO 1.3.9. **(Nullstellensatz Real)**
*Sea $R$ un cuerpo realmente cerrado. Sea $\mathfrak{a} \subset R[X_1, \ldots, X_n] = R[X]$ un ideal. Entonces se cumple que $\mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{a})) = \sqrt[R]{\mathfrak{a}}$.*

DEMOSTRACIÓN. Como $\mathfrak{a} \subset \sqrt[R]{\mathfrak{a}}$, entonces $\mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{a})) \subset \mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\sqrt[R]{\mathfrak{a}})) = \sqrt[R]{\mathfrak{a}}$. Por otra parte, $\mathfrak{a} \subset \mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{a}))$. Por la Proposición 1.3.8, $\sqrt[R]{\mathfrak{a}}$ es el menor ideal real que contiene a $\mathfrak{a}$. Considerando además el Teorema 1.3.7, $\mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{a})) = \mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{a}))))$ es ideal real luego $\sqrt[R]{\mathfrak{a}} \subset \mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{a}))$. □

OBSERVACIÓN 1.3.10. En vista del resultado precedente y dado un cuerpo realmente cerrado $R$, se tiene la siguiente biyección:

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{conjuntos algebraicos} \\ \text{definidos sobre } R^n \end{array} \right\} & \longrightarrow & \left\{ \begin{array}{c} \text{ideales reales de} \\ R[X_1, \ldots, X_n] \end{array} \right\}, \\ V & \longmapsto & \mathcal{I}_{R[X]}(V) \end{array}$$

cuya aplicación inversa viene dada por $\mathfrak{a} \mapsto \mathcal{Z}_{R^n}(\mathfrak{a})$.

El Nullstellensatz Real puede formularse también al estilo de Hilbert-Kronecker, atendiendo al problema de si una ecuación polinómica definida por un polinomio con coeficientes en algún cuerpo realmente cerrado tiene alguna solución o, equivalentemente, como el problema de si la variedad definida por un polinomio o un ideal es vacía o no.

COROLARIO 1.3.11. **(Nullstellensatz Real)**
*Sea $R$ un cuerpo realmente cerrado. Sea $\mathfrak{a} \subset R[X_1, \ldots, X_n]$ un ideal. Entonces:*

$$\mathcal{Z}_{R^n}(\mathfrak{a}) = \emptyset \Leftrightarrow 1 \in \sqrt[R]{\mathfrak{a}}.$$

DEMOSTRACIÓN. Denotemos $R[X] = R[X_1, \ldots, X_n]$. Si $\mathcal{Z}_{R^n}(\mathfrak{a})$ es vacío, entonces se tiene que $\mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{a})) = \mathcal{I}_{R[X]}(\emptyset) = R[X]$. Aplicando el Nullstellensatz Real (Corolario 1.3.9), se sigue que $\sqrt[R]{\mathfrak{a}} = \mathcal{I}_{R[X]}(\mathcal{Z}_{R^n}(\mathfrak{a})) = R[X]$, y por lo tanto $1 \in \sqrt[R]{\mathfrak{a}}$.

Ahora, supongamos que $1 \in \sqrt[R]{\mathfrak{a}}$ y veamos que $\mathcal{Z}_{R^n}(\mathfrak{a})$ sea vacío. El ideal $\sqrt[R]{\mathfrak{a}}$ es real, luego existen $f_1, \ldots, f_r \in R[X]$ tales que $1 + f_1^2 + \cdots + f_r^2 \in \mathfrak{a}$. Supongamos que existe $x \in \mathcal{Z}_{R^n}(\mathfrak{a})$. Esta ha de cumplir que $1 + f_1^2(x) + \cdots + f_r^2(x) = 0$. Como $R$ es cuerpo formalmente real por ser realmente cerrado, y además $1, f_1(x), \ldots, f_r(x) \in R$, entonces ha de ser $1 = 0$, lo cual es absurdo y no puede existir elemento en $\mathcal{Z}_{R^n}(\mathfrak{a})$. □

OBSERVACIÓN 1.3.12. No se da, en general, la equivalencia $1 \in \sqrt[R]{\mathfrak{a}} \Leftrightarrow 1 \in \mathfrak{a}$. En el Nullstellensatz para cuerpos algebraicamente cerrados sí se da esta equivalencia para el radical del ideal. Un contraejemplo sencillo de que esto no ocurre con el radical real se tiene tomando el ideal propio $(1 + X_1^2)$, cuyo radical real claramente contiene a 1.

Capítulo 2

# Positivstellensatz y Nichnegativstellensatz.

## Índice



El objetivo central de este capítulo es probar un resultado conocido como Positivstellensatz, que es una caracterización de los polinomios que son positivos en todo un conjunto algebraico. En primer lugar, se presentará los resultados fundamentales de la Teoría de Artin-Schreier. En el capítulo anterior, ya se introdujeron los objetos centrales de esta teoría como lo son los cuerpos ordenados y los cuerpos realmente cerrados; y también se indicó algunos de sus resultados de manera sucinta. Aquí revisaremos y ampliaremos todo lo que se ha presentado en la Sección 1.1, desde cero y utilizando la noción de cono positivo, que permite redefinir las ordenaciones de los cuerpos. Para continuar, veremos una generalización del cono positivo de un cuerpo para anillos y el ideal que estos definen, su soporte. En este caso no podrá inducirse una ordenación en el anillo, en el sentido de la Definición 4, pero se verá como los conos primos pueden caracterizarse mediante la existencia de un morfismo en un cuerpo ordenado. Seguidamente ampliaremos el estudio de los conos primos de un anillo, y lo haremos por medio de la noción de ideal $P$-convexo, que modelará al ideal soporte de un cono primo. Allí se verá cómo la estructura del conjunto de los conos propios de un anillo difiere cualitativamente de la de los conos positivos de un cuerpo, y finalmente se dará una caracterización de estos a partir de ideales $P$-convexos. Con todo este bagaje teórico, pasaremos a probar el Positivstellensatz Formal primero, y después una versión geométrica del Positivstellensatz para cuerpos realmente cerrados. También se verá un resultado análogo que caracteriza a los polinomios no negativos en un conjunto algebraico, y que se conoce como Nichnegativstellensatz y para finalizar, se aplicará estos resultados para reformular el Nullstellensatz Real en su versión Débil.

Este capítulo se ha basado, fundamentalmente, en los Capítulos 1 y 4 de [**BCR, 1998**]. La Sección 2.1 presenta los elementos de la teoría que elaboraron E. Artin y O. Schreier durante la década de 1920 y contenida fundamentalmente en *"Algebraische Konstruktion reeller Körper"*, publicada en 1926, y en *"Eine Kennzeichnung der reell abgeschlossenen Körper"* de 1927. La versión presentada del Positivstellensatz Formal junto con la noción de ideal $P$-convexo se atribuye a G. Stengle y han sido publicadas en su artículo titulado *"A Nullstellensatz and Positivstellensatz in Semialgebraic Geometry"*. El enunciado del Nullstellensatz Real Débil se adapta del Nullstellensatz Débil para cuerpos algebraicamente cerrados, el cual puede encontrarse en el Capítulo 8 de [**Pardo, 2023**].

### 2.1. Conos y Ordenaciones de Cuerpos.

En esta sección presentaremos los aspectos fundamentales de la Teoría de Artin-Schreier para cuerpos ordenados y cuerpos realmente cerrados. Conviene tener presentes las definiciones elementales vistas en la Sección 1.1, que son las de cuerpo ordenado, cuerpo formalmente real, cuerpo realmente cerrado y clausura real de un cuerpo formalmente real. En primer lugar, hablaremos de las ordenaciones de un cuerpo en términos del cono positivo. Probaremos que es equivalente definir un cuerpo ordenado mediante su cono positivo en lugar de usar la propia ordenación, y además se verá que esta nueva definición resulta más provechosa al considerar las propiedades de los conos. Después, veremos los resultados de la obra conjunta de Artin y

Schreier. Principalmente, se trata de la equivalencia entre cuerpos que admiten una ordenación y cuerpos formalmente reales, y de la caracterización de los cuerpos realmente cerrados. El primer paso será definir los conos y los conos propios.

DEFINICIÓN 13. **(Cono, Cono Propio)**
*Sea $A$ un anillo conmutativo. Un subconjunto $P \subset A$ se dice cono si cumple:*

*(i)* $x + y \in P$ *para cada* $x, y \in P$,
*(ii)* $xy \in P$ *para cada* $x, y \in P$,
*(iii)* $x \in A \Rightarrow x^2 \in P$.

*$P$ se dice cono propio si además cumple:*

*(iv)* $-1 \notin P$.

El nombre de cono propio obedece a la siguiente propiedad para el caso particular en que el anillo es un cuerpo con característica 0. Recuérdese que, como se vio en la Sección 1.1, estos son los únicos cuerpos que pueden admitir una ordenación.

PROPOSICIÓN 2.1.1. *Sea $F$ un cuerpo de característica 0. Entonces, todo cono $P \subset F$ que no sea propio cumple que $P = F$ necesariamente.*

DEMOSTRACIÓN. Un cuerpo con característica 0 contiene a una copia isomorfa de $\mathbb{Q}$. Sea $a \in F$. Como $P$ es un cono, entonces $1 \in P$; y como no es un cono propio, también ocurre que $-1 \in P$. Se tiene que $(a+1)^2 + (-1)(a-1)^2 = 4a = 2^2 a$ es un elemento de $P$. Como además $1/2 \in F$, se sigue que $a = (1/2)^2 2^2 a$ pertenece a $P$ y entonces $P = F$. □

Veamos algunos ejemplos de conos y de conos propios. En particular, comprobemos que el apelativo de cono para el cono positivo de una ordenación dado en la Definición 4 se debe a que este conjunto es precisamente un cono.

EJEMPLO 2.1.2. *Los siguientes son ejemplos de conos sobre un anillo conmutativo $A$:*

(I) *Se denota por $\sum A^2$ al conjunto de las sumas de cuadrados de elementos de $A$, ya introducido en la prueba de la Proposición 1.3.8. Se tiene que $\sum A^2$ es un cono de $A$ que además está incluido en cualquier otro cono de $A$.*
(II) *Dada una familia de conos de $A$, se tiene que su intersección es también un cono de $A$. Si además alguno de los conos de la intersección es propio, la intersección de ellos será un cono propio.*
(III) *El ejemplo anterior permite definir el menor cono que contiene a otro cono $P$ y a la familia $\{a_j\}_{j\in J}$ de elementos de $A$, que se denota por:*

$$P[\{a_j\}_{j\in J}] = \bigcap_{\substack{P\cup\{a_j\}_{j\in J}\subset Q \\ Q\subset A \text{ cono}}} Q.$$

*Con esta notación, el menor cono que contiene a la familia $\{a_j\}_{j\in J}$ es $\sum A^2[\{a_j\}_{j\in J}]$.*
(IV) *El cono positivo de la ordenación de un cuerpo ordenado es un cono propio.*

A fin de aclarar cómo es el cono descrito en el Apartado (III) del anterior ejemplo, y porque resultará útil más adelante, probemos el siguiente resultado.

PROPOSICIÓN 2.1.3. *Sea $A$ un anillo conmutativo. Sea $P$ un cono de $A$ y considérese una familia $\{a_j\}_{j\in J}$ de elementos de $A$. Entonces, el cono $P[\{a_j\}_{j\in J}]$ puede escribirse como el conjunto siguiente:*

$$\left\{ p + \sum_{i=1}^{r} q_i b_i : r \in \mathbb{N},\ p, q_1, \ldots, q_r \in P,\ \forall i = 1, \ldots, r \Rightarrow \exists J_i \subset J \text{ finito tal que } b_i = \prod_{j\in J_i} a_j \right\}.$$

DEMOSTRACIÓN. Llamemos $Q$ al conjunto descrito en el enunciado y $\hat{P}$ a $P[\{a_j\}_{j\in J}]$. En primer lugar, veamos que $Q \subset P$. Sea el elemento $x = p + q_1 b_1 + \ldots + q_r b_r$ de $Q$. Como cada $b_i$ es un producto finito de elementos de $\hat{P}$, entonces pertenece a $\hat{P}$. Dado que además $p, q_1, \ldots, q_r \in P \subset \hat{P}$, entonces $x \in \hat{P}$ y en consecuencia $Q \subset \hat{P}$.

El otro contenido se probará viendo que $Q$ es un cono que contiene a $P$ y a la familia $\{a_j\}_{j\in J}$. Es claro, por la forma de los elementos de $Q$, que este contiene a $P$. Dado $a_j \in \{a_j\}_{j\in J}$, este puede

escribirse como $p+q_1b_1$ donde $p=0$, $q_1=1$ y $b_1=a_j$, luego se tiene que $Q$ contiene a la familia $\{a_j\}_{j\in J}$. Falta ver que $Q$ sea un cono de $A$. Dado $x\in A$, $x^2\in P\subset Q$. Sean $p+(q_1b_1+\ldots+q_rb_r)$, $p'+(q'_1b'_1+\ldots+q'_sb'_s)\in Q$. Se tiene que su suma, $(p+p')+(q_1b_1+\ldots+q_rb_r+q'_1b'_1+\ldots+q'_sb'_s)$, pertenece a $Q$. El producto tiene la siguiente pinta:

$$(p+\sum_{i=1}^{r}q_ib_i)(p'+\sum_{k=1}^{s}q'_kb'_k)=pp'+\sum_{i=1}^{r}(p'q_i)b_i+\sum_{k=1}^{s}(pq'_k)b'_k+\sum_{i=1}^{r}\sum_{k=1}^{s}q_iq'_kb_ib'_k,$$

donde el sumando $pp'$ pertenece a $P$ y el resto será una suma finita del tipo $\sum_{i=1}^{r'}q_ib_i$. Esto último resulta evidente salvo para los términos $q_iq'_kb_ib'_k$, pero basta con observar que $b_ib'_k$ es un producto de cuadrados de $\{a_j\}_{j\in J}$ y de elementos de $\{a_j\}_{j\in J}$. De esto se sigue que $Q$ es un cono que contiene a $P$ y a $\{a_j\}_{j\in J}$ y por lo tanto, $\hat{P}\subset Q$ y se tiene la igualdad de conjuntos. □

Observación 2.1.4. Nótese que en la proposición previa, los productos $b_i$ no repiten elementos de $\{a_j\}_{j\in J}$ y por ello se tiene, en particular, que dados $P$ un cono de un anillo conmutativo $A$ y una familia finita de elementos $\{a_1,\ldots,a_r\}\subset A$, que:

$$P[\{a_1,\ldots,a_r\}]=\{(p_1+q_1a_1)\cdot\ldots\cdot(p_r+q_ra_r):p_1,\ldots p_r,q_1,\ldots q_r\in P\}.$$

En el Apartado (iv) del Ejemplo 2.1.2 se dijo que el cono positivo de un cuerpo ordenado es un cono propio, pero no ocurre siempre que un cono propio de un cuerpo sea cono positivo para alguna de sus ordenaciones. A continuación, veremos cuáles de los conos propios de un cuerpo son conos positivos para alguna ordenación de dicho cuerpo, y también que definir una ordenación en un cuerpo equivale a dar el cono positivo de esta.

Proposición 2.1.5. *Sea $(F,\leq)$ un cuerpo ordenado y sea $P$ su cono positivo. Sea el conjunto $-P=\{x\in F:-x\in P\}$. Entonces se cumple la siguiente propiedad:*

*(v) $P\cup -P=F$.*

*Por otro lado, si $Q$ es un cono propio de algún cuerpo $H$ que satisface la Propiedad $(v)$, la siguiente relación define una ordenación sobre $H$:*

$$x\preceq y\Leftrightarrow y-x\in Q,$$

*y además $Q$ es cono positivo para el cuerpo ordenado $(H,\preceq)$. Se dirá cono positivo a todo cono propio de un cuerpo que además satisfaga $(v)$.*

Demostración. Supongamos que existe $x\in F\setminus(P\cup -P)$. Como $x\notin P$, se tiene que $x\not\geq 0$. Como la ordenación de un cuerpo es un orden total, necesariamente se cumple que $x\leq 0$. Por las propiedades de ordenación, se sigue que $x+(-x)\leq 0+(-x)=-x$, es decir, $0\leq -x$ y $-x\in P$, lo que a su vez implica que $x\in -P$, y es una contradicción. Por lo tanto, $F\setminus(P\cup -P)$ es vacío y $F=P\cup -P$.

Veamos que la relación definida sea un orden total sobre $H$. Sean $x$, $y$, $z\in H$. Por la Propiedad $(iii)$ de la Definición 13, se tiene que $0\in Q$ y de esto se deduce que la relación es reflexiva. Supongamos $x\preceq y$ y $y\preceq x$, y también que $x$, $y$ sean elementos distintos. Entonces $y-x$, $x-y\in Q$. Como $Q$ es un cono, $(y-x)(x-y)=(-1)(y-x)^2\in Q$. Pero $H$ es un cuerpo, luego existe el elemento inverso multiplicativo $(y-x)^{-1}$ en $H$ y además $(y-x)^{-2}\in Q$. Todo esto implica que $-1\in Q$, lo que es una contradicción por la Propiedad $(iv)$ de la Definición 13 y, por lo tanto, $x$ e $y$ han de ser iguales y se satisface $\preceq$ la Propiedad Antisimétrica. Si $x\preceq y$ y $y\preceq z$, entonces $y-x$, $z-y\in Q$. Aplicando la Propiedad $(i)$ de la Definición 13, se tiene que $(z-y)+(y-x)=z-x\in Q$ y la relación es transitiva. Con esto se tiene que $\preceq$ es una relación de orden sobre $H$, que además es total por la Propiedad $(v)$, pues si $x\not\preceq y$, entonces $y-x\in -Q$ y en tal caso $x-y\in Q$.

Finalmente se comprueba que este orden defina una ordenación sobre $H$. Supongamos $x\preceq y$, lo que equivale a $y-x\in Q$. Como $y-x=(y+z)-(x+z)\in Q$, entonces $x+z\preceq y+z$. Supongamos ahora que $0\preceq x$ y $0\preceq y$. Entonces $x$, $y\in Q$, y por la Propiedad $(ii)$ de la Definición 13 se tiene que $xy\in Q$ y en definitiva, que $0\preceq xy$. Con esto se termina de probar que el orden $\preceq$ satisface las propiedades de ordenación de la Definición 4. □

Observación 2.1.6. De la proposición precedente, se sigue que existe una biyección entre el conjunto de ordenaciones que admite un cuerpo y el conjunto de conos positivos del cuerpo.

El conjunto de los conos de un cuerpo mantiene cierta estructura respecto a la relación de inclusión. Por ejemplo, todo cono contenido en otro cono propio es un cono propio. En la proposición siguiente se verá que los conos positivos de las ordenaciones son, de hecho, los elementos maximales del conjunto de los conos propios.

PROPOSICIÓN 2.1.7. *Sea $F$ un cuerpo, y sea $\Lambda$ el conjunto de los conos propios de $F$, que viene parcialmente ordenado por la relación de inclusión $\subset$. Asumiendo el Lema de Zorn y si $\Lambda$ es no vacío, el conjunto parcialmente ordenado $(\Lambda, \subset)$ tendrá elementos maximales. Además, el conjunto de elementos maximales de $(\Lambda, \subset)$ será el conjunto de conos positivos de cada una de las ordenaciones que admita el cuerpo $F$.*

DEMOSTRACIÓN. Supongamos que $\Lambda$ sea no vacío y tomemos alguna cadena $\mathcal{C} \subset \Lambda$, es decir, algún subconjunto de $\Lambda$ que sea totalmente ordenado por la relación de inclusión. Veamos que existe una cota superior de $\mathcal{C}$ en $\Lambda$. Para ello, se define el conjunto siguiente:

$$P = \bigcup_{P_i \in \mathcal{C}} P_i,$$

el cual se verá que es un cono propio y en cuyo caso será una cota de $\mathcal{C}$. Sea el par de elementos $x, y \in P$ y sean $P_i, P_j \in \mathcal{C}$ tales que $x \in P_i$ y $y \in P_j$. Como $\mathcal{C}$ está totalmente ordenado por la inclusión, entonces $P_i \subset P_j$ o $P_j \subset P_i$. Sin pérdida de generalidad podemos suponer que $P_j \subset P_i$ y que, por lo tanto, $x, y \in P_i$. Como $P_i$ es un cono, entonces $x + y, xy \in P_i \subset P$. Dado cualquier $a \in F$, se tiene que $a^2$ pertenece a cualquier elemento de $\mathcal{C}$, y entonces $a^2$ será un elemento de $P$. Con esto ya tenemos que $P$ es un cono. Para ver que sea un cono propio, basta con observar que si $-1 \in P$, necesariamente ha de existir $P_i \in \mathcal{C}$ tal que $-1 \in P_i$, lo cual es una contradicción. En definitiva, $P \in \Lambda$ y es cota superior de $\mathcal{C}$.

Ahora si, por el Axioma de Zorn[1] se tendrá la existencia de elementos maximales de $(\Lambda, \subset)$. Tomemos un elemento maximal $P \in \Lambda$ y veamos que es cono positivo para alguna ordenación de $F$, para lo cual bastará con probar que $P$ cumpla la Propiedad $(v)$ de la Proposición 2.1.5. Sea $a \in F \setminus P$, y veamos que $-a \in P$. Se considera el cono $P[-a] = \{x + (-a)y : x, y \in P\}$, que tiene esa forma de acuerdo con la Observación 2.1.4. Probemos que $P[-a] \in \Lambda$, es decir, que $-1 \notin P[-a]$. Supongamos que pueda escribirse $-1 = x - ay$ con $x, y \in P$. Se observa que $ay = x + 1 = 0$ solo si $x = -1$, lo cual no es posible. Entonces $y \neq 0$ y existe $y^{-1} \in F$. Más aún, $y^{-1} = y(y^{-1})^2$ pertenece a $P$. Pero esto lleva a que $a = (x + 1)y^{-1} \in P$, lo cual es absurdo, y entonces $P[-a]$ es cono propio. Como además $P \subset P[-a]$ y $P$ es maximal para la inclusión en $\Lambda$, se tiene que $P = P[-a]$ y en consecuencia $-a \in P$. En definitiva, el cono propio maximal $P$ es un cono positivo de $F$.

Recíprocamente, si $P$ es el cono positivo de alguna ordenación de $F$, queremos probar que sea un elemento maximal de $\Lambda$. Nótese que todo cono positivo de alguna ordenación de $F$ pertenece a $\Lambda$ por ser un cono propio. Supongamos que existe otro cono propio $Q \subset F$ que contiene estrictamente a $P$. Tomamos $x \in Q \setminus P$, que ha de ser no nulo por $0 \in P$ y además existirá $x^{-1}$ en $F$. Como $P$ es cono positivo y $x \notin P$, entonces $x \in -P$ y $-x \in P$. Adicionalmente, $x^{-2} \in P$ y entonces $-x^{-1} = (-x)(x^{-2}) \in P \subset Q$. En consecuencia, $-1 = x(-x^{-1}) \in Q$, y esto contradice que $Q$ sea un cono propio. Entonces no existe ningún cono propio que contenga estrictamente a $P$ y este será un elemento maximal de $(\Lambda, \subset)$. □

OBSERVACIÓN 2.1.8. Dado un cono propio $Q$ de un cuerpo $F$ que admita ordenación, se tiene que existe un cono positivo $P$ de alguna ordenación de $F$ que además contenga a $Q$. Esto se deduce del resultado precedente, ya que si no existe algún cono propio maximal para la inclusión y que contenga a $Q$, entonces $Q$ será maximal, luego también será un cono positivo.

Este resultado implica que si el conjunto de las sumas de cuadrados de un cuerpo es un cono positivo, entonces dicho cuerpo admitirá una única ordenación. El cuerpo $\mathbb{R}$ de los números reales cumple que para cada $x \in \mathbb{R}$ positivo se tiene que $\sqrt{x} \in R$, es decir, todo elemento positivo de $\mathbb{R}$ es un cuadrado y entonces este admitirá una única ordenación. Para el cuerpo $\mathbb{Q}$ de los racionales podemos adaptar el siguiente resultado clásico.[2]

[1] Puede verse el Axioma 4.2.7 de [**Pardo, 2023**].

[2] Puede verse la prueba original en https://es.wikipedia.org/wiki/Teorema_de_los_cuatro_cuadrados.

TEOREMA 2.1.9. **(de los Cuatro Cuadrados de Lagrange)**
*Todo entero positivo puede escribirse como la suma de* 4 *cuadrados de enteros.*

Tomemos $n/m \in \mathbb{Q}$ con $m \neq 0$ y $m, n$ positivos, y entonces se tendría:

$$\frac{n}{m} = \frac{nm}{m^2} = \frac{a^2+b^2+c^2+d^2}{m^2} = \left(\frac{a}{m}\right)^2 + \left(\frac{b}{m}\right)^2 + \left(\frac{c}{m}\right)^2 + \left(\frac{d}{m}\right)^2.$$

De esto se sigue que los elementos positivos de $\mathbb{Q}$ son todos sumas de cuadrados. En consecuencia, $\sum \mathbb{Q}^2$ es el único cono positivo de $\mathbb{Q}$ y este admitirá una única ordenación. De forma general se tendrá que la intersección de todos los conos positivos de un cuerpo coincida con las sumas de cuadrados, como vemos en el siguiente resultado.

PROPOSICIÓN 2.1.10. *Sea $F$ un cuerpo que admite ordenación y sea $P$ un cono propio de $F$. Entonces:*

$$P = \bigcap_{\substack{P \subset Q \subset F \\ Q \text{ cono positivo}}} Q.$$

*En particular, si $x \in F$ es un elemento positivo para todas las ordenaciones sobre $F$, entonces $x$ es una suma de cuadrados de $F$.*

DEMOSTRACIÓN. Llamaremos $X$ a la intersección de los conos positivos que contienen a $P$. Dado que $P$ es un cono propio, este estará contenido en algún cono positivo por la Proposición 2.1.7 y la intersección es no vacía. Es trivial que $P \subset X$. Para ver que se tiene la igualdad de conjuntos, supongamos que existe algún elemento $a \in X \setminus P$. Se considera el cono generado $P[-a]$, que como veremos es un cono propio. Supongamos que $-1 \in P[-a]$, y de la Observación 2.1.4 se tiene la existencia de $x, y \in P$ tales que $-1 = x - ay$. Si $y = 0$, se tendría que $x = -1$. Esto es imposible porque $x \in P$ cono propio. Entonces $y \neq 0$. Despejando $a$, puede escribirse $a = y(x+1)(1/y)^2$, que claramente es un elemento de $P$ y es una contradicción. En definitiva, $P[-a]$ es un cono propio y como $-a \in P[-a]$, entonces $a \notin P[-a]$. Como además $P \subset P[-a]$, entonces $P[-a]$ está contenido en algún cono positivo que contiene a $P$, luego el elemento $a$ no puede estar en la intersección y se sigue que $P = X$. □

Artin y Schreier introdujeron los cuerpos formalmente reales (véase la Definición 3), y se dieron cuenta de que un cuerpo formalmente real siempre admite ordenación y viceversa. Presentamos este resultado añadiendo el hecho de que el conjunto de los conos propios de un cuerpo es no vacío si y solamente si $-1$ no es una suma de cuadrados.

TEOREMA 2.1.11. *Sea $F$ un cuerpo. Son equivalentes:*

*(i)* *$F$ es cuerpo formalmente real, es decir, se cumple que para cada $x_1, \ldots, x_n \in F$, $\sum x_i^2 = 0$ implica que $x_1 = \cdots = x_n = 0$,*
*(ii)* *$-1 \notin \sum F^2$,*
*(iii)* *$F$ admite ordenación.*

DEMOSTRACIÓN. Primero probaremos que $(i) \Rightarrow (ii)$. Supongamos $(i)$ y también que para ciertos $x_1, \ldots, x_r \in F$ se tiene que $-1 = x_1^2 + \ldots + x_r^2$. Entonces $x_1^2 + \ldots + x_r^2 + 1^2 = 0$ y se contradice que $F$ sea formalmente real, por lo que queda probada la implicación.

Ahora supongamos $(ii)$ y veamos que $F$ sea formalmente real. Se tiene que el cono $\sum F^2$ es propio y entonces, aplicando la Proposición 2.1.7 se concluye que existe alguna ordenación de $F$. Sea $\leq$ una ordenación de $F$ cuyo cono positivo sea $P$. Supongamos que existen $x_1, \ldots, x_r \in F$ tales que $x_1^2 + \ldots + x_r^2 = 0$ y $x_k \neq 0$ para algún $k \in \{1, \ldots, r\}$. Sin pérdida de generalidad suponemos que $k = 1$. Se observa que $x_i^2 \in \sum F^2 \subset P$ para $i = 1, \ldots, r$, de lo que se deduce que $x_2^2 + \cdots + x_r^2 \geq 0$, pero también que $x_1^2 = -(x_2^2 + \cdots + x_r^2) \geq 0$. Por la Propiedad Antisimétrica del orden se sigue que $x_2^2 + \cdots + x_r^2 = 0$. Entonces ha de ser $x_1^2 = 0$, pero esto no es posible dado que $x_1 \neq 0$ y un cuerpo no tiene elementos nilpotentes distintos de 0.

Finalmente, veamos por qué $(ii)$ y $(iii)$ son equivalentes. Si el cuerpo $F$ admite ordenación, el mismo cono positivo de tal ordenación será un cono propio, y dado que $\sum F^2$ está incluido en cualquier cono, este ha de ser cono propio, contradiciendo que $-1$ pueda escribirse como suma de cuadrados en tal caso. Por el contrario, si se sabe que $-1 \notin \sum F^2$, es decir, que $\sum F^2$ es un cono propio, entonces puede aplicarse la Proposición 2.1.7 por la cual se tiene que $F$ admite ordenación. □

A partir de aquí, veremos algunas propiedades de los cuerpos realmente cerrados (véase la Definición 6) que serán útiles durante todo el texto. En primer lugar, veremos que los elementos positivos de un cuerpo realmente cerrado son el cuadrado de otro elemento del cuerpo.

LEMA 2.1.12. *Sea $R$ un cuerpo realmente cerrado. Entonces $R$ contiene a la raíz cuadrada de todo elemento positivo.*

DEMOSTRACIÓN. Supongamos que $R$ sea cuerpo realmente cerrado. Sea $a \in R$, y supongamos que $\sqrt{a} \notin R$. Esto significa que $R[\sqrt{a}]$ es una extensión algebraica no trivial y que no admite ordenación. Entonces puede escribirse:

$$-1 = \sum_{i=1}^{r}(x_i + \sqrt{a}y_i)^2 = \left(\sum_{i=1}^{r} x_i^2 + ay_i^2\right) + \sqrt{a}\sum_{i=1}^{r} 2x_iy_i,$$

en $R[\sqrt{a}]$, y entonces $-1 = \sum_{i=1}^{r} x_i^2 + a\sum_{i=1}^{r} y_i^2$ en $R$. El cuerpo $R$ es un cuerpo ordenado y no puede darse que $-1$ sea una suma de cuadrados de $R$. Entonces $\sum_{i=1}^{r} y_i^2 \neq 0$ y se tiene que $-a = \left(1 + \sum_{i=1}^{r} x_i^2\right)\left(\sum_{i=1}^{r} y_i^2\right)^{-1} \in \sum R^2$. En definitiva, se tiene que si $\sqrt{a}$ no pertenece a $R$ entonces es negativo, por lo que $R$ contiene a las raíces de sus elementos positivos. □

Esta propiedad permite distinguir claramente el hecho de que $\mathbb{R}$ sea un cuerpo realmente cerrado pero $\mathbb{Q}$ sea tan solo un cuerpo ordenado. Como se vio, los elementos positivos de $\mathbb{Q}$ son sumas de hasta 4 cuadrados, mientras que los de $\mathbb{R}$ son suma de uno solo. La propiedad del lema precedente también permite generalizar la topología euclídea sobre algún espacio afín de los reales $\mathbb{A}^n(\mathbb{R})$ al caso de un cuerpo $R$ realmente cerrado cualquiera. Se define la aplicación siguiente:

$$\begin{array}{rccc} ||\cdot|| : & \mathbb{A}^n(R) & \longrightarrow & R \\ & x = (x_1, \ldots, x_n) & \longmapsto & ||x|| = \sqrt{x_1^2 + \ldots + x_n^2}, \end{array}$$

que está bien definida en vista del Lema 2.1.12, y además es una norma sobre el espacio afín $\mathbb{A}^n(R)$. Se llama topología euclídea sobre $\mathbb{A}^n(R)$ a la topología que induce esta norma. Esta topología es más fina que la de Zariski sobre $\mathbb{A}^n(R)$, y además se cumple que las funciones polinomiales son continuas para esta topología. Puede consultarse el Apéndice E para ver más detalles. Ambas topologías serán de utilidad en el capítulo siguiente.

Otra propiedad de los cuerpos realmente cerrados es la unicidad de ordenación que admite dicho cuerpo. Además, teniendo en cuenta la Proposición 2.1.10, la unicidad de ordenación en un cuerpo que admite ordenación equivale a que este tenga como único cono positivo al conjunto de sumas de cuadrados de sus elementos.

PROPOSICIÓN 2.1.13. *Todo cuerpo realmente cerrado admitirá una única ordenación en la que sus elementos positivos serán los cuadrados de sus elementos.*

DEMOSTRACIÓN. Sea $P$ el cono positivo de alguna ordenación de $R$. Denotemos por $sq(R)$ al conjunto de los cuadrados de $R$. En virtud del Lema 2.1.12 se tiene que $P \subset sq(R)$, y además ocurre que $sq(R) \subset \sum R^2 \subset P$, de lo que se deduce que $P = sq(R)$. En definitiva, todo cono positivo de $R$ ha de ser $sq(R)$ y por eso es que admite una única ordenación, siendo los elementos positivos los cuadrados de $R$. □

El recíproco de este resultado no es cierto, y basta con observar que $\mathbb{Q}$ admite una única ordenación y no es cuerpo realmente cerrado. Es decir, la unicidad de ordenación no es suficiente para caracterizar a los cuerpos realmente cerrados. Una caracterización clásica de la Teoría de Artin-Schreier viene dada a continuación. Se omite la prueba de este resultado.[3]

TEOREMA 2.1.14. *Un cuerpo $R$ es realmente cerrado si y solamente si $R[X]/(X^2+1)$ es algebraicamente cerrado.*

Para finalizar, comprobemos la existencia de la clausura real de un cuerpo ordenado, que se sigue de la existencia de su clausura algebraica.

[3]Puede consultarse en el Teorema 1.2.2 de [**BCR, 1998**], junto a otro criterio equivalente que añade a la unicidad de ordenación la propiedad de que todo polinomio con coeficientes en el cuerpo y de grado impar tenga al menos una raíz en dicho cuerpo.

PROPOSICIÓN 2.1.15. *Todo cuerpo formalmente real tiene clausura real.*

DEMOSTRACIÓN. Del Teorema 2.1.11 se sigue que $F$ admite ordenación. Sea $\leq$ una ordenación de $F$. Llamemos $K$ a la clausura algebraica de $F$. Sea $\Omega$ el conjunto de los subcuerpos de $K$ que extiendan al cuerpo $F$. Como $K$ es una extensión algebraica de $F$, todo elemento de $\Omega$ será también una extensión algebraica de $F$. Se define también el conjunto $\Gamma$ de extensiones algebraicas de $F$ que sean cuerpos formalmente reales y el conjunto $\Lambda$ de extensiones algebraicas de $F$ para las que se tenga alguna ordenación que extienda a la de $F$. Es claro que $\Lambda \subset \Gamma \subset \Omega$. El conjunto $\Omega$ queda acotado por $K$ para la relación de inclusión. Como todas las extensiones son algebraicas, estas tendrán un grado finito; y como además se cumple que el grado de una extensión $L/H$ es el producto de los grados de las extensiones $L/L'$ y $L'/H$ para cualquier cuerpo intermedio $L'$, se tiene que $\Gamma$ y $\Lambda$ también serán acotados. Imponiendo el Axioma de Zorn, puede escogerse $R \in \Lambda$ maximal para la relación de inclusión. La prueba consiste en ver que $R$ sea maximal para la inclusión en $\Gamma$, pues los elementos maximales de $\Gamma$ son, por definición, cuerpos realmente cerrados. Veamos que todo elemento positivo de $R$ (para cualquier ordenación dada que extienda a la de $F$) sea el cuadrado de algún elemento de $R$. Supongamos que existe $a \in R$ positivo tal que $R[\sqrt{a}]$ sea una extensión propia de $R$. Se considera el cono generado $\sum R[\sqrt{a}]^2[P]$, cuyos elementos pueden describirse de acuerdo a la Proposición 2.1.3. Se trata de un cono propio. Para ver esto, escribimos $-1 = p + q_1 b_1 + \ldots + q_r b_r$ con $p, q_1, \ldots, q_r \in P$ y $b_1, \ldots, b_r \in \sum R[\sqrt{a}]^2$, y entonces, para algunos $p, \hat{q}_1, \ldots, \hat{q}_s \in P$ y $c_1, \ldots, c_s, d_1, \ldots, d_s \in F$:

$$-1 = p + \hat{q}_1(c_1 + \sqrt{a}d_1)^2 + \ldots + \hat{q}_s(c_s + \sqrt{a}d_s)^2,$$

de lo que se deduce que:

$$-1 = p + \hat{q}_1(c_1^2 + ad_1^2) + \ldots + \hat{q}_s(c_s^2 + ad_s^2).$$

Es decir, que $-1$ es un elemento de $P$; pero es una contradicción porque $P$ es un cono propio. Entonces $R[\sqrt{a}]$ contiene a un cono propio con los elementos positivos de $R$, y por la Proposición 2.1.7 se tiene la existencia de una ordenación de $R[\sqrt{a}]$ que extienda a la de $R$. Como $R$ es maximal en $\Lambda$, ha de ser $R = R[\sqrt{a}]$. De esto se deduce que $R$ admite una única ordenación cuyos elementos positivos son cuadrados de $R$ y que además extiende a la ordenación de $F$. Sea $R_1 \in \Gamma$ un cuerpo realmente cerrado que sea extensión de $R$. Por el Teorema 2.1.14, se cumple que $K = R[\sqrt{-1}]$. La extensión $R_1/R$ es algebraica, luego $R_1 = R[\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_s}]$ y como $R_1 \neq K$, $\alpha_1, \ldots, \alpha_s$ son elementos positivos de $R$. Entonces $R = R_1$ y se tiene que $R$ es maximal en $\Gamma$. Por lo tanto, $R$ es un cuerpo realmente cerrado cuya única ordenación extiende a la del cuerpo $F$, es decir, $R$ es una clausura real de $F$. □

OBSERVACIÓN 2.1.16. La clausura real de un cuerpo ordenado $(F, \leq)$ no es única en general, pero cada par de clausuras reales de $F$ serán $F$-isomorfas.[4]

## 2.2. Conos Primos.

En esta sección se introducen los conceptos de cono primo y su soporte. En el caso de cuerpos, los conos primos son equivalentes a los conos positivos. Para el caso más general de un anillo conmutativo, se verá una caracterización de sus conos primos mediante la existencia de un morfismo en un cuerpo ordenado. Comenzamos por dar la definición de cono primo.

DEFINICIÓN 14. **(Cono Primo)**
*Sea $A$ un anillo conmutativo y sea $P \subset A$ un cono. $P$ se dice cono primo si es cono propio y además cumple que:*

$$ab \in P \Rightarrow a \in P \text{ o } -b \in P \text{ para cada } a, b \in A.$$

Veamos ahora que los conos primos de un cuerpo son siempre conos positivos de ordenaciones. También se define el soporte de un cono primo.

PROPOSICIÓN 2.2.1. *Sea $P$ un cono primo de un anillo conmutativo $A$. Se define el conjunto $-P = \{a \in A : -a \in P\}$. Entonces:*

*(i)* $P \cup -P = A$,

*(ii)* $P \cap -P$ *es ideal primo de* $A$.

[4] Véase el Teorema 1.3.2 de [**BCR, 1998**].

*Se dice soporte de $P$ al ideal $supp(P) = P \cap -P$.*

DEMOSTRACIÓN. Como $P \cup -P \subset A$, para probar $(i)$ basta con ver que $A \setminus (P \cup -P)$ sea vacío. Supongamos que existe $a \in A \setminus (P \cup -P)$. Entonces $a$, $-a \notin P$. $P$ es un cono luego $a^2 \in P$, y como además es primo se tendría que $a \in P$ o $-a \in P$, lo cual es una contradicción.

Pasemos a ver $(ii)$. Primero comprobemos que $supp(P)$ sea subgrupo aditivo. Sean los elementos $a$, $b \in P \cap -P$, y queremos determinar que $a + (-b) \in P \cap -P$. Se tiene que $a$, $b$ son elementos de $P$ y de $-P$ por estar en su intersección. Por definición de $-P$, se tiene que $-b$ pertenece a $P$ y a $-P$. Como ambos son conos, $a + (-b)$ es elemento de $P$ y de $-P$, luego pertenece a su intersección. Entonces $supp(P)$ es subgrupo aditivo y para terminar de comprobar que sea un ideal, tomemos $a \in A$ y $p \in P \cap -P$, y veamos que $ap \in P \cap -P$. Aplicando $(i)$ se tiene que $a$ es un elemento de $P$ o de $-P$. Supongamos que $a \in P$. También se conoce que $p$, $-p \in P$. Esto implica que $ap$, $-ap \in P$, luego $ap \in -P$ y entonces $ap \in P \cap -P$. El razonamiento es análogo al suponer que $a \in -P$, y entonces se concluye que $P \cap -P$ es un ideal.

Finalmente, probemos que $P \cap -P$ sea primo. Sean $a$, $b \in A$ tales que $ab \in P \cap -P$. Si $a$ pertenece al ideal, entonces no hay nada que probar. Supongamos que $a \notin P \cap -P$. Si $ab \in P \cap -P$, entonces $ab$, $-ab$ son elementos de $P$. Si además suponemos que $a \notin P$, entonces $-b \in P$ y se sigue que $b \in -P$. Por otra parte, $-ab = a(-b) \in P$ y así $b \in P$. Entonces $b \in P \cap -P$ y el ideal es primo. Por el contrario, si suponemos que $a \in P$, que implica que $a \notin -P$, basta con repetir el argumento para $-P$ considerando que $ab$, $-ab \in -P$, para deducir de nuevo que $b \in P \cap -P$. □

La Afirmación $(i)$ del resultado precedente implica que todo cono primo de un cuerpo es cono positivo. Veamos que el recíproco de esta afirmación también se cumple.

PROPOSICIÓN 2.2.2. *Para todo cuerpo, el conjunto de sus conos primos coincide con el conjunto de los conos positivos de sus ordenaciones.*

DEMOSTRACIÓN. Considerando la Afirmación $(i)$ de la Proposición 2.2.1, es evidente que todo cono primo de un cuerpo es, a su vez, el cono positivo de alguna ordenación que admita el cuerpo. Probemos que los conos positivos de un cuerpo sean conos primos. Sea $P$ un cono positivo de $F$. Supongamos que existen $x$, $y \in F$ tales que $xy \in P$ pero $x$, $-y \notin P$. Entonces $x$, $-y \in F \setminus P \subset -P$, luego $-x$, $y \in P$ y se sigue que $-xy \in P$. Como $F$ es cuerpo, $(xy)^{-1} \in F$ y por ser $P$ un cono, se tendría que $(xy)^{-2} \in P$ y que $(-xy)(xy)(xy)^{-2} = -1 \in P$. Pero esto contradice que $P$ sea cono propio y, por lo tanto, $P$ ha de ser un cono primo. □

OBSERVACIÓN 2.2.3. El soporte de un cono primo de un cuerpo es el ideal (0). Esto es consecuencia de que los conos primos de un cuerpo sean los conos positivos y de la Propiedad Antisimétrica de la ordenación que define el cono primo en cuestión.

Llegados a este punto, hemos comprobado que la noción de cono primo de un cuerpo coincide con la de cono positivo. En el caso general de un anillo conmutativo $A$, un cono primo no define una ordenación en el sentido de la relación de orden dada en la Proposición 2.1.5. Prueba de esto es que el soporte de un cono primo $P$ de $A$ no es siempre el ideal (0) pues, si consideramos la relación $\leq$ definida por $P$ según la Proposición 2.1.5, se tiene que todo elemento $x \in P \cap -P$ satisface $x \leq 0$ y $x \geq 0$. Si $x \neq 0$, esta relación no puede ser de orden porque no cumple la Propiedad Antisimétrica.

A partir de aquí revisaremos propiedades de los conos primos para anillos en general. Comencemos por ver cómo es la estructura de los conos primos de un anillo dentro del conjunto de los conos propios. En el caso particular de un cuerpo, se tendrá el comportamiento de los conos positivos descrito en la Proposición 2.1.7. Veremos que, si bien los conos propios maximales de un anillo son conos primos, estos no serán los únicos.

PROPOSICIÓN 2.2.4. *Sea $A$ un anillo conmutativo. Entonces:*

- $(i)$ *todo cono propio de $A$ maximal para la relación de inclusión es un cono primo,*
- $(ii)$ *todo cono propio de $A$ que contiene a un cono primo de $A$ es también primo,*
- $(iii)$ *si $P$ y $Q$ son un par de conos primos de $A$ tales que $P \subset Q$, entonces $Q = P \cup supp(Q)$.*

Demostración. Probemos $(i)$. Sea $P$ un elemento maximal del conjunto $\Lambda$ de los conos propios de $A$. Veamos que $P$ es un cono primo. Supongamos que $P$ no sea un cono primo. En tal caso existe $ab \in P$ con $a \notin P$ y $-b \notin P$, por lo que los conos generados $P[a]$ y $P[-b]$ que contienen a $P$ no pueden ser conos propios, o de lo contrario $P$ no sería maximal en $\Lambda$. En vista de la Observación 2.1.4, existen $p$, $q$, $p'$, $q' \in P$ tales que $-1 = p + aq = p' - bq'$. Considerando la igualdad siguiente:

$$(1+p)(1+p') = 1 + p + p' + pp' = -aqbq',$$

puede escribirse $-1 = p + p' + pp' + abqq' \in P$, que contradice que $P$ sea cono propio. Por lo tanto, $P$ es un cono primo de $A$.

Pasamos a probar $(ii)$. Sea $Q$ un cono propio de $A$ que contenga a un cono primo $P$ de $A$. Por la Afirmación $(i)$ de la Proposición 2.2.1, tenemos que ver que $A = Q \cap -Q$. Se tiene que $Q \cap -Q \subset A$. También conocemos que $P \subset Q$ y $A = P \cap -P$. Si $x \in -P$, entonces $-x \in P \subset Q$ y se deduce que $x \in -Q$, luego $-P \subset -Q$. Entonces $A = P \cap -P \subset Q \cap -Q$ y con esto terminamos de probar la igualdad. Hemos visto que $Q$ es cono primo.

Para acabar, veamos que se cumple $(iii)$. Sean $P$ y $Q$ un par de conos primos de $A$ tales que $P \subset Q$. Se quiere probar que $Q = P \cup supp(Q)$. Se conoce que $supp(Q) \cup P \subset Q$. Sea $a \in Q$. Si $a \in supp(Q)$ habríamos probado el otro contenido, supongamos que no es así. Entonces $a \notin -Q$, que implica $-a \notin Q$. Si $a \in -P$ se tendría que $-a \in P \subset Q$, lo cual es imposible. Entonces $a \in P$, y acabamos de probar que $a \in P \cup supp(Q)$ en todo caso, es decir, $Q = P \cup supp(Q)$. □

A continuación, probaremos que la existencia de un cono primo en un anillo equivale a la existencia de un morfismo de anillos en algún cuerpo ordenado. Antes de eso, veamos en qué sentido respeta un morfismo de anillos la propiedad de ser cono primo.

Proposición 2.2.5. *Sean $A$ y $B$ anillos. Sea $\varphi : A \to B$ un morfismo de anillos. Si $Q$ es un cono primo de $B$, entonces $\varphi^{-1}(Q)$ es un cono primo de $A$ de soporte $\varphi^{-1}(supp(Q))$.*

Demostración. En primer lugar, comprobemos que si $P = \varphi^{-1}(Q)$, entonces $P$ es un cono primo de $A$. Sean $a$, $b \in P$. Como $Q$ es cono, $\varphi(a) + \varphi(b) = \varphi(a+b)$ y $\varphi(a)\varphi(b) = \varphi(ab)$ son ambos elementos de $Q$ y entonces, como sus anti imágenes están contenidas en $P$, se tiene que $a + b$, $ab \in P$. Por el mismo argumento, dado $a \in A$, como $\varphi(a)\varphi(a) = \varphi(a^2)$, se tiene que $a^2 \in P$. Con esto ya sabemos que $P$ es cono. Para ver que es propio, supongamos que $-1 \in P$. Entonces $\varphi(-1) = -\varphi(1) = -1_F \in Q$, pero eso no puede ser porque $Q$ es propio. Se concluye que $P$ es cono propio. Por último veamos que sea cono primo. Supongamos que existen $a$, $b \in P$ tales que $ab \in P$ pero $a$, $-b \notin P$. Se tiene que $\varphi(ab) = \varphi(a)\varphi(b) \in Q$ y por ser $Q$ primo se tiene que, o $\varphi(a) \in Q$, o $\varphi(-b) \in Q$. Si $\varphi(a) \in Q$ entonces $a \in \varphi^{-1}(\varphi(a)) \subset P$, lo cual es imposible. Si $\varphi(-b) \in Q$ se tiene que $-b \in P$, que también es imposible. Por lo tanto, $P$ es un cono primo.

Sea $\mathfrak{a} = \varphi^{-1}(supp(Q))$. Veamos que $supp(P) = \mathfrak{a}$. Sea $a \in supp(P)$. Entonces $a \in P$, que implica que $\varphi(a) \in Q$. También $-a \in P$ por ser $a \in -P$, luego $\varphi(-a) = -\varphi(a) \in Q$ y en definitiva $\varphi(a) \in -Q$. Por lo tanto, $\varphi(a) \in supp(Q) = Q \cap -Q$. Entonces $a \in \varphi^{-1}(\varphi(a)) \subset \mathfrak{a}$. Esto prueba que $supp(P) \subset \mathfrak{a}$. Tomemos $a \in \mathfrak{a}$. Entonces $\varphi(a) \in supp(Q)$, lo que implica que $\varphi(a) \in Q$, $-Q$. Se sigue que $\varphi(a), \varphi(-a) \in Q$, luego $a, -a \in P$; y como también $a \in -P$, entonces $a \in supp(P)$. Esto prueba el otro contenido. □

Observación 2.2.6. En las condiciones de la proposición precedente y dado $P$ un cono primo de $A$, no se tiene en general que $\varphi(P)$ sea un cono primo de $B$. Basta con considerar la inclusión del anillo $\mathbb{Z}$ de los enteros, para el que $\sum \mathbb{Z}^2$ es un cono primo (se prueba con el Teorema de los Cuatro Cuadrados de Lagrange 2.1.9), en $\mathbb{Q}$. Claramente, la imagen de $\sum \mathbb{Z}^2$ no satisface la Propiedad $(i)$ de la Proposición 2.2.1 como subconjunto de $\mathbb{Q}$.

El siguiente lema muestra la construcción de un morfismo de un anillo en un cuerpo ordenado que, dado un cono primo del anillo, cumple que los elementos de este cono los únicos cuyas imágenes sean elementos del cono positivo del cuerpo.

Lema 2.2.7. *Sea $P$ un cono primo del anillo conmutativo $A$, y sea $\mathfrak{a} = supp(P)$. Sea $F$ el cuerpo de fracciones de $A/supp(P)$. Entonces el conjunto $Q = \{(a+\mathfrak{a})/(b+\mathfrak{a}) \in F : ab \in P\}$ es cono positivo de alguna ordenación de $F$ y $P = \pi^{-1}(Q)$ siendo $\pi : A \to F$ la proyección en $A/\mathfrak{a}$ compuesta con la inclusión en el cuerpo de fracciones.*

Demostración. En un primer lugar, veamos que la pertenencia a $Q$ de un elemento de $F$ esté bien definida, en el sentido de que no dependa de los elementos de $A$ utilizados para representar su clase en el cuerpo de fracciones. Sea $x = \frac{a+\mathfrak{a}}{b+\mathfrak{a}} = \frac{c+\mathfrak{a}}{d+\mathfrak{a}} \in F$ donde $a$, $b$, $c$, $d \in A$ y $b$, $d \notin \mathfrak{a}$. Comprobemos que $ab \in P$ si y solamente si $cd \in P$. Como los pares $a$, $b$ y $c$, $d$ son arbitrarios, basta con ver que $ab \in P$ lleva a que $cd \in P$. La igualdad de las clases $\frac{a+\mathfrak{a}}{b+\mathfrak{a}} = \frac{c+\mathfrak{a}}{d+\mathfrak{a}}$ se traduce en que $ad + \mathfrak{a} = bc + \mathfrak{a}$. Por lo tanto, existe $z \in \mathfrak{a}$ tal que $ad + z = bc$. Se tiene que $z$, $-z \in P$ por lo que $ad - bc$, $bc - ad \in P$. Se cumple la igualdad $2abcd = c^2b^2 + a^2d^2 + (ad - cb)(cb - ad)$ y como $P$ es cono, $2abcd \in P$. Como $P$ es primo, escribiendo $(2cd)(ab) \in P$ se tiene $2cd \in P$ o $-ab \in P$. Supongamos que $2cd \notin P$, luego $cd \notin P$ y $-ab \in P$. Entonces $ab \in \mathfrak{a}$ y $a \in \mathfrak{a}$ por ser $\mathfrak{a}$ primo y $b \notin \mathfrak{a}$. Recuperando $bc = ad + z$, como $ad \in \mathfrak{a}$, se tiene que $bc \in \mathfrak{a}$ y entonces $c \in \mathfrak{a}$. En consecuencia $cd \in \mathfrak{a} \subset P$, pero es una contradicción dentro de lo expuesto. Entonces $2cd \in P$ y también sabemos que si $-ab \in P$, entonces $cd \in P$. Supongamos ahora que $-ab \notin P$ y veamos que en tal caso también se cumple $cd \in P$. Si escribimos $(cd)(2ab) \in P$, entonces $cd \in P$ o $-2ab \in P$. Si se diese la segunda, entonces $-ab = ab - 2ab \in P$, por lo que no es posible. Necesariamente se tiene que $cd \in P$.

Ahora probemos que el conjunto $Q$ sea un cono positivo de $F$. Para ver que $Q$ sea cono, denotemos $x = \frac{a+\mathfrak{a}}{b+\mathfrak{a}}$, $y = \frac{c+\mathfrak{a}}{d+\mathfrak{a}} \in Q$, de modo que $ab$, $cd \in P$. Por un lado se tiene que $x+y = \frac{(ad+cb)+\mathfrak{a}}{bd+\mathfrak{a}}$. $P$ es cono luego $b^2$, $d^2 \in P$ y así $(ad+cb)bd = abd^2 + cdb^2 \in P$. Esto concluye que $x + y \in Q$. Por otro lado, $xy = \frac{ac+\mathfrak{a}}{bd+\mathfrak{a}}$ y como $acbd = abcd \in P$, se tiene que $xy \in Q$. Si $x = \frac{a+\mathfrak{a}}{b+\mathfrak{a}} \in F$, entonces $x^2 = \frac{a^2+\mathfrak{a}}{b^2+\mathfrak{a}}$ y como $P$ contiene a los cuadrados de elementos de $A$ se tiene $a^2b^2 \in P$, por lo que $x^2 \in Q$. Con esto se concluye que $Q$ sea un cono de $F$. Veamos que $Q$ es cono propio. Supongamos que $-1_F = \frac{-1+\mathfrak{a}}{1+\mathfrak{a}} \in Q$. Entonces $(-1)1 = -1 \in P$, pero esto no es posible porque $P$ es cono propio. Se concluye que $Q$ es un cono propio. Finalmente, comprobemos que $Q \cup -Q = F$. Supongamos que existe $x = \frac{a+\mathfrak{a}}{b+\mathfrak{a}} \in F \setminus (Q \cup -Q)$. Por $x \notin Q$ sabemos que $ab \notin P$, y además $x \notin -Q$ supone que $-x = \frac{-a+\mathfrak{a}}{b+\mathfrak{a}} \notin Q$ luego $-ab \notin P$. $ab$ es un elemento de $A$ y $P$ es un cono así que $(ab)^2 \in P$. Pero $P$ es cono propio y necesariamente se tendría que $ab \in P$ o $-ab \in P$. Es una contradicción luego no existe $x \in F \setminus (Q \cup -Q)$, y se cumple la igualdad de conjuntos dado que $Q \cup -Q \subset F$.

Finalmente veamos que $P = \pi^{-1}(Q)$. Sea $a \in P$. Entonces $\pi(a) = \frac{a+\mathfrak{a}}{1+\mathfrak{a}}$, y dado que $a1 = a \in P$ se cumple que $\pi(a) \in Q$. En consecuencia $a \in \pi^{-1}(\pi(a)) \subset \pi^{-1}(Q)$. Esto prueba la inclusión $P \subset \pi^{-1}(Q)$. Sea $a \in \pi^{-1}(Q)$. Entonces $\pi(a) = \frac{a+\mathfrak{a}}{1+\mathfrak{a}} \in Q$, luego $a1 = a \in P$. Con esto termina de probarse la igualdad de conjuntos. □

El siguiente resultado es la mencionada caracterización de los conos primos de un anillo por medio de la existencia de un morfismo en un cuerpo ordenado. La propiedad característica de este morfismo es que aplica a los elementos del cono del anillo en elementos del cono positivo del cuerpo ordenado, y que el resto de elementos del anillo tienen imagen negativa.

Proposición 2.2.8. *Sea $A$ un anillo conmutativo y $P \subset A$ un subconjunto. Entonces $P$ es un cono primo si y solamente si existe un cuerpo ordenado $(F, \leq)$ y un morfismo de anillos $\varphi : A \to F$ tal que $P = \{a \in A : \varphi(a) \geq 0\}$.*

Demostración. Si $P$ es un cono primo, se sigue del Lema 2.2.7 que existe un morfismo $\varphi : A \to F$ para algún cuerpo ordenado $(F, \leq)$ y cuyo cono positivo tenga a $P$ de anti imagen por $\varphi$. Pasemos a probar el recíproco. Sea $(F, \leq)$ un cuerpo ordenado y $\varphi : A \to F$ morfismo de anillos. Se define el conjunto $P = \{a \in A : \varphi(a) \geq 0\}$. Sea $Q$ el cono positivo de $(F, \leq)$, es decir, $Q = \{x \in F : x \geq 0\}$. Entonces $P = \varphi^{-1}(Q)$, y aplicando la Proposición 2.2.5 se tiene que $P$ es cono primo. □

Observación 2.2.9. Si $F$ es un cuerpo ordenado, entonces, todo subcuerpo $K$ admite ordenación. Para ver esto basta con considerar la inclusión de $K$ en $F$ y la proposición anterior.

Anteriormente se ha dicho que la ordenación de un cuerpo no es única en general, pero hasta ahora no se ha dado ningún argumento en contra de la unicidad de las posibles ordenaciones de un cuerpo. Utilizando el resultado que acabamos de probar, puede darse el siguiente ejemplo.

EJEMPLO 2.2.10. *Llamemos $\mathbb{Q}(X)$ al cuerpo de fracciones sobre el dominio $\mathbb{Q}[X]$. Dado un elemento $\alpha \in \mathbb{R}$ que sea trascendente sobre $\mathbb{Q}$, se define el morfismo siguiente:*

$$\begin{aligned} ev_\alpha : \quad \mathbb{Q}(X) \quad &\longrightarrow \quad \mathbb{Q}(\alpha) \\ f(X)/g(X) &\longmapsto f(\alpha)/g(\alpha), \end{aligned}$$

*que lo denotamos así porque restringido a $\mathbb{Q}[X]$ es el morfismo de evaluación en $\alpha$. Esta restricción es un isomorfismo porque $\alpha$ es trascendente sobre $\mathbb{Q}$, luego $ev_\alpha$ es también un isomorfismo porque puede obtenerse a partir de la restricción y haciendo que respete las operaciones. Como $\mathbb{Q}(\alpha)$ es un subcuerpo de $\mathbb{R}$, se tiene el morfismo $\tilde{\imath}$ inclusión de $\mathbb{Q}(\alpha)$ en $\mathbb{R}$, y entonces se tendrá una ordenación de $\mathbb{Q}(\alpha)$ con el cono positivo $\tilde{\imath}^{-1}(\sum \mathbb{R}^2)$ por la Proposición 2.2.8. Ahora veremos que distintos $\mathbb{Q}(\alpha)$ llevan a distintas ordenaciones de $\mathbb{Q}(X)$ por el morfismo $ev_\alpha$. Sean $X$, $3 \in \mathbb{Q}(X)$ y consideremos los casos $\alpha = \pi$ y $\alpha = e$. Con la ordenación de $\mathbb{Q}(\pi)$ como subcuerpo de $\mathbb{R}$, se tiene que $ev_\pi(X-3) \geq 0$ y entonces la ordenación que $\mathbb{Q}(\pi)$ define para $\mathbb{Q}(X)$ lleva a que $X - 3 \geq 0$, es decir, $X \geq 3$. Análogamente, la ordenación que $\mathbb{Q}(e)$ define para $\mathbb{Q}(X)$ lleva a que $X \leq 3$, y por ende se tiene dos ordenaciones distintas de $\mathbb{Q}(X)$.*

## 2.3. Ideales $P$-convexos e Ideales $P$-radicales.

En esta sección veremos dos tipos de ideales, los $P$-convexos y los $P$-radicales. Los ideales del primer tipo, como se verá al final, caracterizan a los conos primos que contengan a otro cono primo $P$. Los ideales $P$-radicales generalizan de cierta manera el concepto de ideal real, pero aquí tan solo se usarán en el proceso de dar dicha caracterización de los conos primos. Pasemos a dar una primera definición.

DEFINICIÓN 15. **(Ideal $P$-convexo)**
*Sea $P$ un cono de un anillo conmutativo $A$. Un ideal $\mathfrak{a} \subset A$ se dice $P$-convexo si para todo par de elementos $p_1$, $p_2 \in P$ tales que $p_1 + p_2 \in \mathfrak{a}$ se tiene que $p_1 \in \mathfrak{a}$.*

OBSERVACIÓN 2.3.1. De la propia definición se sigue que, dado un cono $P$ de un anillo, el ideal soporte $supp(P) = P \cap -P$ es un ideal $P$-convexo.

Veamos algunas propiedades sencillas de los ideales $P$-convexos.

PROPOSICIÓN 2.3.2. *Sea $P \subset A$ un cono. Si existe algún ideal propio $P$-convexo de $A$, entonces $P$ es un cono propio.*

DEMOSTRACIÓN. Sea $\mathfrak{a} \subset A$ un ideal propio $P$-convexo. Supongamos que $P$ no sea un cono propio. Se tiene que $-1 \in P$ y que $0 = 1 + (-1) \in \mathfrak{a}$ luego $1 \in \mathfrak{a}$ por ser un ideal $P$-convexo. Esto contradice que $\mathfrak{a}$ sea un ideal propio y en consecuencia, $P$ ha de ser un cono propio. □

PROPOSICIÓN 2.3.3. *Sean $P$, $Q \subset A$ conos y sea $\mathfrak{a} \subset A$ ideal. Entonces, se cumplen las siguientes propiedades:*

(*i*) *Si $\mathfrak{a}$ es ideal $Q$-convexo y $P \subset Q$, entonces $\mathfrak{a}$ es ideal $P$-convexo.*
(*ii*) *Si $\mathfrak{a}$ es un ideal primo $P \cap Q$-convexo entonces, o bien $\mathfrak{a}$ es $P$-convexo, o bien es $Q$-convexo, o bien se dan ambas cosas.*

DEMOSTRACIÓN. Para probar (*i*), se toma $p_1$, $p_2 \in P$ tales que $p_1 + p_2 \in \mathfrak{a}$. Como $p_1$, $p_2 \in Q$, entonces $p_1 \in \mathfrak{a}$ por ser $\mathfrak{a}$ ideal $Q$-convexo. Para probar (*ii*), supongamos que $\mathfrak{a}$ no sea $P$-convexo ni $Q$-convexo. En tal caso existen $a$, $p \in P$ con $a + p \in \mathfrak{a}$ y $a \notin P$, y también existen $b$, $q \in Q$ tales que $b + q \in \mathfrak{a}$ y $b \notin \mathfrak{a}$. Se define $r = (a+p)^2b^2 + a^2(b+q)^2$, que por ser $a + p$, $b + q \in \mathfrak{a}$ se tiene que $r \in \mathfrak{a}$. Por ser producto de cuadrados, se tiene que $a^2b^2 \in P$, $Q$ luego $a^2b^2 \in P \cap Q$. Veamos ahora que $r - a^2b^2$ pertenece a $P$ y a $Q$. Para ello se reescribe como $r - a^2b^2 = b^2(2ap + p^2) + a^2(b+q)^2 = (a+p)^2b^2 + (2bq + b^2)a^2$.

Utilizando la primera igualdad, dado que $a$, $p \in P$ y es un cono, se tiene que $r - a^2b^2 \in P$. Por medio de la segunda igualdad y un razonamiento análogo, se tiene también que $r - a^2b^2 \in Q$. Entonces $r - a^2b^2 \in P \cap Q$. Aplicando que $\mathfrak{a}$ es un ideal $P \cap Q$-convexo y que $r = a^2b^2 + (r - a^2b^2)$ pertenece a $\mathfrak{a}$, se deduce que $a^2b^2 \in \mathfrak{a}$. Como además es un ideal primo, necesariamente $a \in \mathfrak{a}$ o $b \in \mathfrak{a}$. Esto es imposible, luego $\mathfrak{a}$ ha de ser $P$-convexo o $Q$-convexo. □

Ahora definamos lo que es un ideal $P$-radical. Este tipo de ideales generalizan la noción de ideal real introducida en la Proposición 1.3.8, aunque aquí solo nos interesarán para el estudio de ideales $P$-convexos.

DEFINICIÓN 16. **(Ideal $P$-radical)**
*Sea $A$ un anillo conmutativo, $\mathfrak{a}$ un ideal de $A$ y $P \subset A$ un cono. $\mathfrak{a}$ se dice $P$-radical si para todo $a \in A$ y todo $p \in P$, $a^2 + p \in \mathfrak{a}$ implica que $a \in \mathfrak{a}$.*

OBSERVACIÓN 2.3.4. En vista de la Proposición 1.3.8, se tiene que los ideales reales de un anillo conmutativo $A$ son un ejemplo de ideales $\sum A^2$-radicales.

El siguiente resultado muestra la relación entre los ideales $P$-radicales y los ideales $P$-convexos.

PROPOSICIÓN 2.3.5. *Sea $A$ un anillo conmutativo y $P \subset A$ un cono. Un ideal $\mathfrak{a}$ es $P$-radical si y solamente si es un ideal radical y $P$-convexo.*

DEMOSTRACIÓN. Supongamos que $\mathfrak{a}$ sea ideal $P$-radical. Para ver que sea ideal radical, tomemos $a^n \in \mathfrak{a}$ con $n$ elemento minimal del conjunto $\{n \in \mathbb{N} : a^n \in \mathfrak{a}\} \setminus \{0\}$. Si $n = 1$ hemos terminado. Supongamos que $n > 1$. Si $n$ es par entonces $a^n = (a^{n/2})^2 + 0 \in \mathfrak{a}$, y por ser $\mathfrak{a}$ ideal $P$-radical se tiene que $a^{n/2} \in \mathfrak{a}$, contradiciendo que $n$ sea minimal. Si $n$ es impar, entonces $a^{n+1} \in \mathfrak{a}$ por ser ideal. Reescribiendo $a^{n+1} = (a^{(n+1)/2})^2 + 0$, es claro que $a^{(n+1)/2} \in \mathfrak{a}$, contradiciendo de nuevo que $n$ sea minimal. Para ver que $\mathfrak{a}$ es $P$-convexo, tomemos $a$, $b \in P$ tales que $a + b \in \mathfrak{a}$. Por ser ideal, se tiene que $a(a + b) = a^2 + ab \in \mathfrak{a}$. Como además $ab \in P$ por ser un cono, se tiene que $a \in \mathfrak{a}$ por ser ideal $P$-radical.

Supongamos ahora que $\mathfrak{a}$ es un ideal radical y $P$-convexo. Sean $a \in A$ y $p \in P$ tales que $a^2 + p \in \mathfrak{a}$, y veamos que $a \in \mathfrak{a}$. $a^2 \in P$ por ser un cono, y como $\mathfrak{a}$ es $P$-convexo, se tiene que $a^2 \in \mathfrak{a}$. Como además es radical, se tiene que $a \in \mathfrak{a}$. □

Es momento de dar la caracterización de los conos primos que contengan a otro cono $P$ que se venía advirtiendo, una que relacione cada uno de estos conos primos con un ideal $P$-convexo, que será el propio soporte del cono primo.

PROPOSICIÓN 2.3.6. *Sea $A$ un anillo conmutativo y sea $P$ un cono primo de $A$. Entonces la siguiente aplicación es biyectiva:*

$$\begin{array}{ccc} \left\{ \begin{array}{c} \textit{conos primos que} \\ \textit{contienen a } P \end{array} \right\} & \longrightarrow & \left\{ \begin{array}{c} \textit{ideales primos} \\ P\textit{-convexos} \end{array} \right\} . \\ Q & \longmapsto & \textit{supp}(Q) \end{array}$$

DEMOSTRACIÓN. Sea $Q$ un cono primo de $A$ que contiene al cono $P$. Considerando la Observación 2.3.1, se tendrá que el soporte $supp(Q)$ sea un ideal $Q$-convexo. Si además se tiene en cuenta la Afirmación $(i)$ de la Proposición 2.3.3, se concluye que $supp(Q)$ es un ideal $P$-convexo. Entonces la imagen de $Q$ es un ideal primo $P$-convexo y la aplicación está bien definida. Probemos que la aplicación es inyectiva. Sean un par de conos primos $Q$, $Q'$ que contengan a $P$ y tales que $supp(Q) = supp(Q')$. De la Afirmación $(iii)$ de la Proposición 2.2.4 se sigue esta cadena de igualdades: $Q' = supp(Q') \cup P = supp(Q) \cup P = Q$, y por ende la aplicación es inyectiva.

Ahora veamos que la aplicación sea sobreyectiva, es decir, probaremos que dado $\mathfrak{a}$ un ideal $P$-convexo existe algún cono primo que contenga a $P$ y cuyo soporte sea $\mathfrak{a}$. Sea $\Lambda$ el conjunto de los conos $Q$ de $A$ que contengan a $P$ y tales que $\mathfrak{a}$ sea ideal $Q$-convexo. El conjunto $\Omega$ de todos los conos de $A$ es un conjunto acotado por $A$ para la relación de inclusión. Aceptando el Axioma de Zorn, dado que $\Lambda$ es un subconjunto de $\Omega$ y es no vacío por $P \in \Lambda$, es que puede tomarse $Q \in \Lambda$ que sea maximal para la relación de inclusión. El ideal $\mathfrak{a}$ es propio, dado que es primo, y por la Proposición 2.3.2, $Q$ es cono propio. Probemos que $Q \cap -Q = \mathfrak{a}$. Si $a \in Q \cap -Q$, entonces $a$, $-a \in Q$. Como $a + (-a) = 0 \in \mathfrak{a}$, $a \in \mathfrak{a}$ por ser $Q$-convexo. Esto demuestra que $Q \cap -Q \subset \mathfrak{a}$. Ahora tomamos $a \in \mathfrak{a}$. La idea es ver que $\mathfrak{a}$ es ideal $Q[a]$-radical y $Q[-a]$-radical. Si esto fuese así, por la Proposición 2.3.5 se tendría que $\mathfrak{a}$ es $Q[a]$-convexo y $Q[-a]$-convexo, luego $Q[a], Q[-a] \in \Lambda$. Dado que $Q$ es maximal, se tendría que $Q = Q[a] = Q[-a]$. Así $a$, $-a \in Q$, y en definitiva se tendría que $a \in Q \cap -Q$. Sean $c \in A$ y $p$, $q \in Q$ tales que $c^2 + (p + aq) \in \mathfrak{a}$ y probemos que $c \in \mathfrak{a}$. Como $a \in \mathfrak{a}$, entonces $qa \in \mathfrak{a}$ y así $c^2 + p \in \mathfrak{a}$. Como $\mathfrak{a}$ es $Q$-convexo,

$c^2 \in \mathfrak{a}$ y como además es primo, $c \in \mathfrak{a}$. Por todo lo expuesto, se concluye que $\mathfrak{a} = Q \cap -Q$. Para finalizar, dado que $Q$ es un cono propio que contiene al cono primo $P$, aplicando la Afirmación $(ii)$ de la Proposición 2.2.4 se tiene que $Q$ es cono primo. □

## 2.4. Positivstellensatz y Nichnegativstellensatz.

En esta sección se va a enunciar y probar un resultado que sirve para caracterizar a los polinomios con coeficientes en un cuerpo realmente cerrado y que sean estrictamente positivos en todo un conjunto algebraico, conocido como Positivstellensatz. En primer lugar, se verá la versión más generalizada conocida como Positivstellensatz Formal. Después, pasaremos al caso particular de un cuerpo realmente cerrado y enunciaremos una versión geométrica del Positivstellensatz junto con el Nichnegativstellensatz, que sirve para la caracterización de polinomios no negativos en un conjunto algebraico. Finalmente, veremos una versión más del Nullstellesatz Real, que en este caso relaciona los puntos del espacio afín con los ideales del espectro maximal real del anillo de funciones polinomiales considerado. Primeramente, vemos un resultado que será útil en la demostración del Positivstellensatz Formal.

TEOREMA 2.4.1. *Sea $A$ un anillo conmutativo. Entonces, son equivalentes:*

- $(i)$ *$A$ contiene algún cono propio,*
- $(ii)$ *$A$ contiene algún cono primo,*
- $(iii)$ *existe $\varphi : A \to R$ morfismo de anillos, para algún cuerpo realmente cerrado $R$,*
- $(iv)$ *$A$ contiene algún ideal real primo,*
- $(v)$ *$-1 \notin \sum A^2$.*

DEMOSTRACIÓN. Comprobemos que $(i) \Rightarrow (ii)$. Sea $\Lambda$ el conjunto de los conos propios del anillo $A$, que en este caso es no vacío. Considerando que $A$ es también un cono, se tendrá que el conjunto de los conos de $A$ está acotado por $A$ y por el mismo razonamiento con el Axioma de Zorn que el de la prueba de la Proposición 2.1.7 se tiene que $\Lambda$ posee elementos maximales para la inclusión. Sea $P \in \Lambda$ maximal. Entonces $P$ es cono primo por la Afirmación $(i)$ de la Proposición 2.2.4.

La implicación $(ii) \Rightarrow (iii)$ se sigue de la existencia de clausura real para cuerpos ordenados. Como existe un cono primo de $A$, entonces existirá un morfismo de $A$ en algún cuerpo ordenado $F$. Llámese $\varphi$. Por la Proposición 2.1.15, podemos tomar $R$ la clausura real del cuerpo $F$ junto con el morfismo inclusión $\tilde{\imath} : F \to R$, y se tendrá el morfismo de anillos $\tilde{\imath} \circ \varphi$ del anillo $A$ en el cuerpo realmente cerrado $R$.

Ahora se demuestra que $(iii) \Rightarrow (iv)$. Sea $\varphi$ morfismo de anillos de $A$ en algún cuerpo realmente cerrado $R$. Por la Proposición 2.1.13 se tiene que $R$ admite una única ordenación cuyo cono positivo son los cuadrados $R$, y este conjunto además coincide con $\sum R^2$ por ser el menor cono. Aplicando la Proposición 2.2.2, se tiene que $\sum R^2$ es un cono primo, además con soporte el ideal $(0)$, en virtud de la Observación 2.2.3. Entonces, fijándonos ahora en la Proposición 2.2.5, $P = \varphi^{-1}(\sum R^2)$ será un cono primo de $A$ de soporte el ideal $\mathfrak{a} = ker(\varphi)$. Veamos que $\mathfrak{a}$ sea ideal real, o equivalentemente, ideal $\sum A^2$-radical. Por la Afirmación $(ii)$ de la Proposición 2.2.1, el soporte de un cono primo es un ideal primo, luego $\mathfrak{a}$ es primo. Considerando la Proposición 2.3.5, basta con probar que $\mathfrak{a}$ sea ideal $\sum A^2$-convexo para ver que sea real, por todo lo expuesto. Sean $p, q \in \sum A^2$ tales que $p + q \in \mathfrak{a}$, y veamos que $p \in \mathfrak{a}$. El ideal $\mathfrak{a}$ es el soporte de $P$, es decir, que $\mathfrak{a} = P \cap (-P)$. Esto implica que $p + q \leq 0$, luego $p + q \leq q$ y se sigue que $p \leq 0$. Entonces $p \in (-P)$, pero también se sabe que $p \in \sum A^2 \subset P$ y se tiene que $p \in \mathfrak{a}$. Entonces $\mathfrak{a}$ es $\sum A^2$-convexo y también es real.

Pasemos a probar $(iv) \Rightarrow (v)$. Sea $\mathfrak{a}$ un ideal real primo de $A$. Que $\mathfrak{a}$ sea ideal real equivale a que sea un ideal $\sum A^2$-radical por lo expuesto en la Observación 2.3.4. Supongamos que $-1 \in \sum A^2$. Entonces $1 \in \mathfrak{a}$, dado que $1^2 + (-1) \in \mathfrak{a}$, y se tendría que $\mathfrak{a}$ no es un ideal propio, lo cual es absurdo porque es un ideal primo. En definitiva, $-1$ no puede ser una suma de cuadrados de $A$.

Finalmente $(v) \Rightarrow (i)$ se sigue de que, si $-1 \notin \sum A^2$, entonces $\sum A^2$ es un cono propio. □

Dicho esto, pasamos a probar el Positivstellensatz Formal.

TEOREMA 2.4.2. **(Positivstellensatz Formal)**
*Sea $A$ un anillo conmutativo y sean $\{a_i\}_{i\in I}$, $\{b_j\}_{j\in J}$, $\{c_k\}_{k\in C}$ familias de elementos de $A$. Se define el cono $P = \sum A^2[\{a_i\}_{i\in I}]$, el monoide multiplicativo $M$ generado por la familia $\{b_j\}_{j\in J}$ y el ideal $\mathfrak{a}$ generado por la familia $\{c_k\}_{k\in C}$. Entonces, son equivalentes:*

(*i*) *No existe $Q \subset A$ cono primo tal que $a_i \in Q$, $b_j \notin supp(Q)$, $c_k \in supp(Q)$ para todo $i \in I$, $j \in J$, $k \in C$.*
(*ii*) *No existe $\varphi$ morfismo de anillos de $A$ en algún cuerpo realmente cerrado $R$ tal que $\varphi(a_i) \geq 0$, $\varphi(b_j) \neq 0$, $\varphi(c_k) = 0$ para todo $i \in I$, $j \in J$, $k \in C$.*
(*iii*) *Existen $p \in P$, $b \in M$, $c \in \mathfrak{a}$ tales que $p + b^2 + c = 0$.*

DEMOSTRACIÓN. Veamos que $(i) \Rightarrow (ii)$. Supongamos que existe un morfismo de anillos $\varphi$ de $A$ en algún cuerpo realmente cerrado $R$ que contradiga $(ii)$. Aplicando la Proposición 2.2.8, el conjunto $Q = \{a \in A : \varphi(a) \geq 0\}$ es un cono primo de $A$. Además, como de la Proposición 2.1.13 se tiene que $R$ admite una única ordenación, $\sum R^2$ es el cono positivo de $R$ y se cumple que $Q = \varphi^{-1}(\sum R^2)$. Considerando la Proposición 2.2.5, se tiene que $supp(Q) = \varphi^{-1}(supp(\sum R^2))$. Para cada $i \in I$, $\varphi(a_i) \geq 0$ implica que $\varphi(a_i) \in \sum R^2$, y entonces $a_i \in Q$. También, dado $j \in J$ y considerando que $supp(\sum R^2) = (0)$, $\varphi(b_j) \neq 0$ implica que o bien $\varphi(b_j) \in \sum R^2$, o bien $\varphi(b_j) \in -Q_R$, exclusivamente. Entonces se tendrá que $b_j \in Q$ o $-b_j \in Q$, pero no ambas de manera simultánea. Por lo tanto, $b_j \notin supp(Q)$. Tomando $k \in C$, se tiene que $\varphi(c_k) = 0$, luego $c_k \in supp(Q)$. Hemos probado que $Q$ incumple las condiciones de $(i)$ y entonces se satisface $(ii)$ necesariamente.

Probemos ahora que $(ii) \Rightarrow (i)$. Supongamos que existe un cono primo $Q \subset A$ contradiciendo $(i)$. De la Proposición 2.2.8 se sigue la existencia de algún morfismo $\phi$ de $A$ en algún cuerpo ordenado $(F, \leq)$, y que además cumple que $Q = \{a \in A : \phi(a) \geq 0\}$. Sea $R$ la clausura real de $F$, que existe por la Proposición 2.1.15, y llamemos $\tilde{\imath}$ al morfismo de inclusión de $F$ en $R$. Se define otro morfismo $\varphi = \tilde{\imath} \circ \phi$ de $A$ en el cuerpo realmente cerrado $R$. Como $\tilde{\imath}$ es un morfismo inyectivo que preserva el orden $\leq$, se tiene que $\tilde{\imath}^{-1}(\sum R^2) = \{x \in F : x \geq 0\}$, que se trata del cono positivo de $F$. Por esto se tiene que $\varphi^{-1}(\sum R^2) = Q$. Además, de la Proposición 2.2.5 se sigue que $supp(Q) = \varphi^{-1}(supp(\sum R^2))$. Entonces $a_i \in Q$ implica que $\varphi(a_i) \in \sum R^2$, dado que se cumple $\varphi(a_i) \geq 0$, para todo $i \in I$. Sea $j \in J$. Como $b_j \notin supp(Q)$, entonces $\varphi(b_j) \notin supp(\sum R^2) = (0)$. Dado $k \in C$, si $c_k \in supp(Q)$ entonces $\varphi(c_k) \in supp(\sum R^2) = (0)$. En definitiva, la aplicación $\varphi$ contradice $(ii)$ y, por lo tanto, se ha de cumplir $(i)$.

Pasemos a probar que $(ii) \Rightarrow (iii)$. La idea de la demostración consiste en encontrar elementos $p \in P$, $b \in M$ tales que $p + b^2 \in \mathfrak{a}$, de modo que entonces existe $c = -(p + b^2) \in \mathfrak{a}$ y este satisface $p + b^2 + c = 0$. Observemos que si el ideal $\mathfrak{a}$ no es un ideal propio, es decir si $\mathfrak{a} = A$, entonces existe $c = -(p + b^2)$ en el anillo y en el ideal, y habríamos terminado. También, si existiese algún $x \in M \cap \mathfrak{a}$, entonces podemos tomar $p = 0, b = x^2$ y $c = -x^2$ y se concluye la propiedad del enunciado. Entonces, podemos suponer que $\mathfrak{a}$ es un ideal propio de $A$ y que $M \cap \mathfrak{a} = \emptyset$.

Dicho esto, se tiene que $M$ es un sistema multiplicativamente cerrado porque $1 \in M$ y dados $m_1, m_2 \in M$ se tiene $m_1 m_2 \in M$, y además $0 \notin M$ porque $0 \in \mathfrak{a}$ y son disjuntos. Entonces, podemos considerar el anillo cociente $A/\mathfrak{a}$ y el conjunto de clases $M + \mathfrak{a} = \{m + \mathfrak{a} : m \in M\}$. Ocurre que $M + \mathfrak{a}$ es un sistema multiplicativamente cerrado del anillo $A/\mathfrak{a}$, pues la clase $1 + \mathfrak{a} \in M + \mathfrak{a}$ y dados $m_1 + \mathfrak{a}, m_2 + \mathfrak{a} \in M + \mathfrak{a}$, como $m_1 m_2 \in M$, entonces $m_1 m_2 + \mathfrak{a} \in M + \mathfrak{a}$. Además, se satisface que $0 + \mathfrak{a} \notin M + \mathfrak{a}$ porque de lo contrario se tendría que $0 = m + a$ para algunos $m \in M$ y $a \in \mathfrak{a}$, y como $a = -m$, necesariamente $m \in \mathfrak{a}$, contradiciendo que $M \cap \mathfrak{a}$ sea vacío. Por lo tanto, podemos definir el anillo de fracciones no trivial $B_1 = (M + \mathfrak{a})^{-1} A/\mathfrak{a}$ y considerar el morfismo natural $\phi_1$ de $A$ en $B_1$ dado por la composición de la proyección de $A$ en $A/\mathfrak{a}$ y la inclusión de este último en el anillo de fracciones $(M + \mathfrak{a})^{-1} A/\mathfrak{a}$.

Ahora, consideremos el conjunto arbitrario $\{X_i\}_{i\in I}$ de variables algebraicamente independientes sobre el anillo $B_1$, y definimos el anillo de polinomios siguiente:

$$B_1[\{X_i\}_{i\in I}] = \bigcup_{I' \subset I \text{ finito}} B_1[\{X_i\}_{i\in I'}],$$

siendo cada anillo de polinomios de la unión definido sobre un número finito de variables y considerando las operaciones suma y producto como la operación suma o producto definida en cualquier anillo de polinomios con un número finito de variables que contenga a ambos operandos.

Sobre el anillo $B_1[\{X_i\}_{i\in I}]$ consideraremos el ideal $\mathfrak{b}$ generado por la familia $\{X_i^2-(a_i+\mathfrak{a})\}_{i\in I}$. Llamamos $B_2$ al anillo cociente $B_1[\{X_i\}_{i\in I}]/\mathfrak{b}$ y denotamos por $\phi_2$ al morfismo natural de $B_1$ en $B_2$ dado por la inclusión de $B_1$ en el anillo de polinomios $B_1[\{X_i\}_{i\in I}]$ compuesta con la proyección de este en $B_2$.

Por la existencia de un morfismo $\phi_2\circ\phi_1$ de $A$ en $B_2$ se tiene que no es posible un morfismo $\phi_3$ de $B_2$ en algún cuerpo realmente cerrado $R$ de manera que $\phi=\phi_3\circ\phi_2\circ\phi_1$ contradiga $(ii)$. Entonces, del contrarrecíproco de la Implicación $(v)\Rightarrow(iii)$ del Teorema 2.4.1 se sigue la existencia de $\alpha_1,\ldots,\alpha_r\in B_2$ tales que $-1_{B_2}=\alpha_1^2+\ldots+\alpha_r^2$. Cada elemento $\alpha_k$ es la clase de un polinomio, por lo que puede escribirse como una suma finita de monomios como sigue:

$$\alpha_k=\sum_{l=1}^{s_k} w_{k,l}\prod_{i\in I_l}(X_i+\mathfrak{b}),$$

donde $w_{k,l}\in B_1$ y $I_l$ es un conjunto finito de elementos de $I$, posiblemente repetidos, para cada $l=1,\ldots,s_k$ y para cada $k=1,\ldots,r$. Si alguno de los $I_l$ es vacío, se considerará que $\prod_{i\in I_l}X_i=1$. Ahora, dado que para cada $i\in I$ se tiene que $(a_i+\mathfrak{a})-X_i^2\in\mathfrak{b}$, se cumplirá la igualdad de clases de $B_2$ $(a_i+\mathfrak{a})+\mathfrak{b}=X_i^2+\mathfrak{b}$ y por ende, que $\phi_2(a_i+\mathfrak{a})=X_i^2+\mathfrak{b}$. De esto se sigue la siguiente igualdad en $B_2$, para cada $k=1,\ldots,r$:

$$\phi_2\left(\sum_{l=1}^{s_k} w_{k,l}^2\prod_{i\in I_l}(a_i+\mathfrak{a})\right)=\sum_{l=1}^{s_k} w_{k,l}^2\prod_{i\in I_l}\phi_2(a_i+\mathfrak{a})=\alpha_k^2.$$

En definitiva, considerando que $\phi_2(-1_{B_1})=-1_{B_2}$, puede escribirse en $B_1$ la igualdad:

$$-1_{B_1}=\sum_{k=1}^{r}\sum_{l=1}^{s_k} w_{k,l}^2\prod_{i\in I_l}(a_i+\mathfrak{a}).$$

Cada elemento $w_{k,l}$ de $B_1$ puede escribirse como el cociente de clases $w_{k,l}=(y_{k,l}+\mathfrak{a})/(m_{k,l}+\mathfrak{a})$ con $y_{k,l}+\mathfrak{a}\in A/\mathfrak{a}$ y $m_{k,l}+\mathfrak{a}\in M+\mathfrak{a}$. Como $-1_{B_1}$ puede escribirse como una suma con finitos términos, puede definirse $m+\mathfrak{a}\in M+\mathfrak{a}$ como el producto finito de todos los $m_{k,l}$. De esta forma, al multiplicar $-1_{B_1}$ por la clase de $m^2$ se tendrá la expresión siguiente en $A/\mathfrak{a}$:

$$-m^2+\mathfrak{a}=-1_{B_1}(m^2+\mathfrak{a})=m^2\left(\sum_{k=1}^{r}\sum_{l=1}^{s_k} q_{k,l}^2\prod_{i\in I_l}a_i\right)+\mathfrak{a},$$

para algunos $q_{k,l}\in A$ y donde todos los cocientes son $1+\mathfrak{a}$ y por ello se omiten. Llamemos $p=m^2(\sum_{k=1}^{r}\sum_{l=1}^{s_k}q_{k,l}^2\prod_{i\in I_l}a_i)$, como es una suma de productos de elementos del cono $P$ y de cuadrados de $A$, se tiene que $p\in P$. De la igualdad de clases $-m^2+\mathfrak{a}=p+\mathfrak{a}$ se sigue que $p+m^2\in\mathfrak{a}$ y entonces, si tomamos $b=m$ y $c=-(p+m^2)$, se cumple que $p+b^2+c=0$, probando la propiedad que queríamos.

Finalmente, veamos que $(iii)\Rightarrow(ii)$. Sean $p\in P$, $b\in M$ y $c\in\mathfrak{a}$ tales que $p+b^2+c=0$ y supongamos que existe alguna aplicación $\varphi$ en algún cuerpo realmente cerrado $R$ que contradiga $(ii)$. En virtud de la Proposición 2.2.5 se tiene $Q=\varphi^{-1}(\sum R^2)$ que es cono primo de $A$ y cuyo soporte es el ideal $supp(Q)=\varphi^{-1}(supp(\sum R^2))=\varphi^{-1}((0))=ker(\varphi)$. Sabemos que $Q$ contiene tanto a $\sum A^2$ por ser un cono y a la familia $\{a_i\}_{i\in I}$ por la hipótesis $\varphi(a_i)\geq 0$ dado $i\in I$. Por la propia definición de $P$ (véase el Apartado (III) del Ejemplo 2.1.2), se tendrá que $P\subset Q$ y se sigue que $\varphi(p)\geq 0$. Por otro lado, se tiene $b\in M$ que será, o bien un producto finito de elementos (posiblemente repetidos) $b_1',\ldots,b_s'\in\{b_j\}_{j_J}$, o bien $b=1$. Si $b=1$, entonces $\varphi(b)=1\neq 0$, y dado el otro caso, como $R$ es un cuerpo y por ello no tiene divisores de cero, se sigue que:

$$\varphi(b)=\varphi(b_1'\ldots b_s')=\varphi(b_1')\ldots\varphi(b_s')\neq 0.$$

Como consecuencia, se cumple además que $\varphi(b^2)=(\varphi(b))^2>0$. Por último se tiene $c\in\mathfrak{a}$, que será $c=a_1'c_1'+\ldots+a_t'c_t'$ para una subfamilia finita y no vacía $c_1',\ldots,c_t'$ de $\{c_k\}_{k\in C}$ y para $a_1',\ldots,a_t'\in A$, o en otro caso $c=0$. Si $c=0$, entonces $\varphi(c)=0$, y en el otro caso sucede que:

$$\varphi(c)=\varphi(a_1')\varphi(c_1')+\ldots+\varphi(a_t')\varphi(c_t')=\varphi(a_1')0+\ldots+\varphi(a_t')0=0.$$

Llegados a este punto, sabemos que $p+b^2+c=0$, luego $\varphi(p+b^2+c)=\varphi(p)+\varphi(b^2)+\varphi(c)=0$. Como $\varphi(c)=0$, ocurre que $\varphi(p)+\varphi(b^2)=0$ y entonces $\varphi(b^2)=-\varphi(p)>0$, pero esto contradice $\varphi(p)\geq 0$ y por lo tanto, $(iii)\Rightarrow(ii)$. □

El Positivstellensatz Formal es una propiedad que, en el contexto de Geometría Algebraica Real, se usa sobre el anillo de las funciones polinómicas para reescribir el resultado en una versión geométrica. Ahora daremos una reescritura del Positivstellensatz Formal para cuerpos realmente cerrados. A partir de este resultado, seremos capaces de dar las versiones geométricas del Positivstellensatz y del Nichnegativstellensatz, así como un Nullstellensatz Real Débil.

TEOREMA 2.4.3. *Sea $R$ un cuerpo realmente cerrado. Sean las familias finitas $\{f_1, \ldots, f_r\}$, $\{g_1, \ldots, g_s\}$ y $\{h_1, \ldots, h_t\}$ de polinomios de $R[X_1, \ldots, X_n]$. Sean $P = \sum R^2[\{f_1, \ldots, f_r\}]$, $M$ el monoide multiplicativo generado por $\{g_1, \ldots, g_s\}$ y $\mathfrak{a}$ el ideal generado por $\{h_1, \ldots, h_t\}$. Entonces son equivalentes:*

(*i*) $\{x \in R^n : f_i(x) \geq 0, i = 1, \ldots, r,\ g_j(x) \neq 0, j = 1, \ldots, s,\ h_k(x) = 0, k = 1, \ldots, t\}$ *es vacío,*

(*ii*) *existen $f \in P$, $g \in M$ y $h \in \mathfrak{a}$ tales que $f + g^2 + h = 0$.*

DEMOSTRACIÓN. La prueba de este resultado consiste en ver que (*i*) es equivalente a la Afirmación (*ii*) del Positivstellensatz Formal 2.4.2, ya que tomando el anillo $A = R[X_1, \ldots, X_n]$ se tiene que (*ii*) es literalmente la Afirmación (*iii*) de dicho resultado. La equivalencia entre (*i*) y (*ii*) se seguiría de la equivalencia de las Afirmaciones (*ii*) y (*iii*) del Positivstellensatz Formal 2.4.2. Denotamos por (II) a la Afirmación (*ii*) del Positivstellensatz Formal 2.4.2, y se quiere probar que (*i*) y (II) son equivalentes. En primer lugar, veamos que (II)$\Rightarrow$ (*i*). Supongamos que existe $x \in R^n$ perteneciente al conjunto descrito en (*i*). Entonces, el morfismo de evaluación $ev_x$ es un morfismo del anillo $R[X_1, \ldots, X_n]$ en el cuerpo realmente cerrado $R$ que incumple (II), y por lo tanto, se tiene que (II)$\Rightarrow$ (*i*).

Ahora probaremos que (*i*) $\Rightarrow$(II). Supongamos que existe $\varphi$ un morfismo del anillo $R[X_1, \ldots, X_n]$ en algún cuerpo realmente cerrado $R_1$ y que incumple (II). Podemos considerar el morfismo de anillos $\varphi_{|R} : R \to R_1$ dado por la restricción de $\varphi$ al subcuerpo $R$. En vista de la Observación 1.2.9, $\varphi_{|R}$ se trata de un morfismo inyectivo, luego $R_1/R$ es una extensión de cuerpos realmente cerrados y $\varphi$ es un morfismo de $R$-álgebras. Se define el punto $z = (z_1, \ldots, z_n) \in R_1^n$ por $z_i = \varphi(X_i)$ para cada $i = 1, \ldots, n$. Para cualquier $f \in R[X_1, \ldots, X_n]$ se tiene que:

$$\varphi(f) = \sum_{\substack{\mu \leq d \\ \mu = \mu_1 + \ldots + \mu_n}} \alpha_{\mu_1, \ldots, \mu_n} \varphi(X_1^{\mu_1}) \cdot \ldots \cdot \varphi(X_n^{\mu_n}) = \sum_{\substack{\mu \leq d \\ \mu = \mu_1 + \ldots + \mu_n}} \alpha_{\mu_1, \ldots, \mu_n} z_1^{\mu_1} \cdot \ldots \cdot z_n^{\mu_n} = f(z),$$

siendo $d$ el grado del polinomio $f$. En términos de las nociones de lógica de primer orden introducidas en la Sección 1.2, se tiene que se satisface la siguiente fórmula cuantificada y sin variables libres en $R_1$:

$$\exists X_1, \ldots, \exists X_n, f(X_1, \ldots, X_n) - \varphi(f) = 0,$$

de modo que aplicando el Principio de Transferencia (Corolario 1.2.5) para cuerpos realmente cerrados, se tiene la existencia de $x = (x_1, \ldots, x_n) \in R^n$ tal que $f(x) = \varphi(f)$, y el argumento es válido para cualquier $f \in R[X_1, \ldots, X_n]$. De este modo, si $\varphi$ es un morfismo de anillos que contradice (II), entonces $x$ será un elemento que pertenece al conjunto descrito en la Afirmación (*i*). Esto se debe a que $f_i(x) = \varphi(f_i) \geq 0$, $g_j(x) = \varphi(g_j) \neq 0$ y $h_k(x) = \varphi(h_k) = 0$ para $i = 1, \ldots, r$, $j = 1, \ldots, s$, $k = 1, \ldots, t$. En conclusión, el conjunto descrito en la Afirmación (*i*) es no vacío y esto termina de probar la implicación. □

Durante la Sección 1.1 se introdujeron las funciones polinomiales definidas en todo $R^n$. Aquí, en cambio, se va a definir el conjunto de las funciones polinomiales que van de un subconjunto algebraico $V$ de $R^n$ en $R$:

$$\mathcal{P}(V) = \{P : V \to R \text{ aplicación} : \exists f \in R[X_1, \ldots, X_n] \text{ tal que } P(x) = f(x), \forall x \in V\}.$$

Como además cada polinomio de $R[X_1, \ldots, X_n]$ define una única aplicación polinomial, se tiene una aplicación $\Phi : R[X_1, \ldots, X_n] \to \mathcal{P}(V)$ que es sobreyectiva. De hecho, se tiene que con las operaciones suma y producto de funciones, $\mathcal{P}(V)$ es un anillo y que además, $\Phi$ es un morfismo de anillos sobreyectivo cuyo núcleo es $\mathcal{I}_{R[X_1, \ldots, X_n]}(V)$. En conclusión, $\mathcal{P}(V)$ y $R[X_1, \ldots, X_n]/\mathcal{I}_{R[X_1, \ldots, X_n]}(V)$ son isomorfos. Con esto, pasamos a ver las versiones geométricas del Positivstellensatz y del Nichnegativstellensatz.

COROLARIO 2.4.4. **(Nichnegativstellensatz y Positivstellensatz Geométricos)** *Sea $R$ un cuerpo realmente cerrado y sea $V$ un conjunto algebraico de $R^n$. Sean unos elementos $g_1, \ldots, g_r \in \mathcal{P}(V)$ y el conjunto $W = \{x \in V : g_1(x) \geq 0, \ldots, g_r(x) \geq 0\}$. Sea $P$ el cono de $\mathcal{P}(V)$ generado por $g_1, \ldots, g_r$. Entonces para cada $f \in \mathcal{P}(V)$ se cumple que:*

*(i)* $\forall x \in W, f(x) \geq 0 \Leftrightarrow \exists m \in \mathbb{N}, \exists g, h \in P, fg = f^{2m} + h$,
*(ii)* $\forall x \in W, f(x) > 0 \Leftrightarrow \exists g, h \in P, fg = 1 + h$.

DEMOSTRACIÓN. Una consideración previa necesaria es que $W$, por definición, es un subconjunto de $V$, y $V$ a su vez está definido como el conjunto de ceros del ideal $\mathfrak{a} = \mathcal{I}_{R[X]}(V)$. Se trata de un ideal finitamente generado, dado que $R[X_1, \ldots, X_n]$ es noetheriano. Si $u_1, \ldots, u_r$ es una familia de generadores de $\mathfrak{a}$, entonces $W$ puede redefinirse de la siguiente manera:

$$W = \{x \in R^n : g_1(x) \geq 0, \ldots, g_r(x) \geq 0, u_1(x) = 0, \ldots, u_r(x) = 0\}.$$

Probemos $(i)$. La condición $f(x) \geq 0$ para todo $x \in W$ es equivalente a escribir que el siguiente conjunto sea vacío:

$$\{x \in R^n : g_1(x) \geq 0, \ldots, g_r(x) \geq 0, -f(x) \geq 0, f(x) \neq 0, u_1(x) = 0, \ldots, u_r(x) = 0\}.$$

Si se aplica el Teorema 2.4.3, esto es equivalente a que $h_1 + h_2 + h_3^2 = 0$ para algún $h_1 \in P[-f]$, algún $h_2 \in \mathfrak{a}$ y algún otro polinomio $h_3$ que pertenezca al monoide multiplicativo generado por $f$, es decir, $h_3 = f^m$ para algún $m \in \mathbb{N}$. Como $h_2 \in \mathfrak{a}$, en el anillo $\mathcal{P}(V)$ será $h_2 = 0$. Como también $h_1 \in P[-f]$, por la Observación 2.1.4, este será de la forma $h_1 = -fg + h$ para algunos $g$, $h \in P$. Entonces la condición dada sobre polinomios de $R[X_1, \ldots, X_n]$ se sobrescribe por: existen $m \in \mathbb{N}$ y $g$, $h \in P$ tales que $0 = -fg + h + f^{2m}$. Esta lista de equivalencias prueba $(i)$.

Para probar $(ii)$ se procede de forma similar. La condición $f(x) > 0$ para todo $x \in W$ es equivalente a decir que el siguiente es un conjunto vacío:

$$\{x \in R^n : g_1(x) \geq 0, \ldots, g_r(x) \geq 0, -f(x) \geq 0, u_1(x) = 0, \ldots, u_r(x) = 0\}.$$

En virtud del Teorema 2.4.3, esto equivale a que se tenga $h_1 + h_2 + h_3^2 = 0$ con algunos $h_1 \in P[-f]$, $h_2 \in \mathfrak{a}$ y $h_3$ perteneciente al monoide multiplicativo trivial, formado por únicamente por 1. De nuevo, $h_2 = 0$ para el anillo $\mathcal{P}(V)$ y $h_1$ puede escribirse como $-fg + h$ con $g$, $h \in P$. Entonces la condición dada es equivalente a que existan $g$, $h \in P$ tales que $0 = -fg + h + 1$, y esto prueba $(ii)$. □

Ahora, veamos un ejemplo de aplicación del Positivstellensatz.

EJEMPLO 2.4.5. *Consideremos un cuerpo realmente cerrado $R$ y el conjunto algebraico $V = R^2$ de $R^2$. Definamos el conjunto $W = \{(x, y) \in R^2 : x \geq 0, y \geq 0\}$. Aplicando el Positivstellensatz (Afirmación $(ii)$ del Corolario 2.4.4), puede encontrarse una caracterización del los polinomios $f \in R[X, Y]$ que son positivos en todo $W$.*

*Dicho polinomio cumple la igualdad $fg = 1 + h$ para algunos $g$, $h \in \sum R[X, Y]^2[\{X, Y\}]$. Entonces, estos serán de la forma $g = p + qX + rY + sXY$ y $h = p' + q'X + r'Y + s'XY$, con $p$, $p'$, $q$, $q'$, $r$, $r'$, $s$, $s' \in \sum R[X, Y]^2$. En definitiva, $f$ ha de ser:*

$$f = \frac{1 + p' + q'X + r'Y + s'XY}{p + qX + rY + sXY}.$$

Finalizaremos esta sección con otra versión del Nullstellensatz Real, cuya prueba está basada en el Teorema 2.4.3. Para el caso de un cuerpo algebraicamente cerrado $K$ se tiene el Nullstellensatz Débil, que consiste en la identificación de los puntos de un conjunto algebraico $V$ del espacio afín $\mathbb{A}^n(K)$ con el espectro maximal del anillo de polinomios $\mathcal{P}(V)$. Es decir, dado algún punto $x = (x_1, \ldots, x_n) \in V$, se considera el ideal maximal $\mathfrak{m}_x = (X_1 - x_1, \ldots, X_n - x_n)$, de modo que la siguiente es una aplicación biyectiva:[5]

$$\begin{array}{ccc} V & \longrightarrow & MaxSpec(\mathcal{P}(V)) \\ x & \longmapsto & \mathfrak{m}_x. \end{array}$$

En el caso de un cuerpo realmente cerrado $R$ no ocurre lo mismo. Nótese que todo ideal maximal es primo, luego también es radical, pero no todo ideal maximal es real y eso motiva la definición del espectro maximal real de los anillos de polinomios.

[5]Este resultado puede consultarse en el Capítulo 8 de [**Pardo, 2023**].

DEFINICIÓN 17. **(Espectro Maximal Real)**
*Sea $R$ un cuerpo realmente cerrado y $V$ un conjunto algebraico de $R$. Se define el espectro maximal real del anillo $\mathcal{P}(V)$ como el conjunto:*

$$MaxSpec^{(R)}(\mathcal{P}(V)) = \{\mathfrak{m} \in MaxSpec(\mathcal{P}(V)) : \mathfrak{m} \text{ es ideal real}\}.$$

Dado un conjunto algebraico $V$ de $\mathbb{A}^n(R)$, se probará que existe una biyección entre los puntos de $V$ y los ideales de $MaxSpec^{(R)}(\mathcal{P}(V))$. Antes de hacer esto, veamos el siguiente lema.

LEMA 2.4.6. *En las mismas condiciones que el Corolario 2.4.4, para cada $f \in \mathcal{P}(V)$ se cumple:*

$$\forall x \in W, f(x) = 0 \Leftrightarrow \exists m \in \mathbb{N}, \exists g \in P, f^{2m} + g = 0.$$

DEMOSTRACIÓN. Como en la prueba del Corolario 2.4.4, se tendrá que el ideal $\mathfrak{a} = \mathcal{I}_{R[X]}(V)$ es generado por alguna familia finita, llámese $u_1, \ldots, u_r$ y entonces $W$ se redefine como:

$$W = \{x \in R^n : g_1(x) \geq 0, \ldots, g_r(x) \geq 0, u_1(x) = 0, \ldots, u_r(x) = 0\}.$$

La afirmación $f(x) = 0$ para cada $x \in W$ equivale a que el conjunto siguiente sea vacío:

$$\{x \in R^n : g_1(x) \geq 0, \ldots, g_r(x) \geq 0, f(x) \neq 0, u_1(x) = 0, \ldots, u_r(x) = 0\}.$$

Por el Teorema 2.4.3, esto es igual que decir que $h_1 + h_2 + h_3^2 = 0$ para ciertos $h_1 \in P$, $h_2 \in \mathfrak{a}$ y $h_3$ perteneciente al monoide multiplicativo generado por $f$. Se tiene que $h_2 = 0$ en $\mathcal{P}(V)$, y $h_3$ es de la forma $f^m$ para algún $m \in \mathbb{N}$. Además, por la Observación 2.1.4, se tiene que $h_1 = -fg + h$ para algunos $g$, $h \in P$. Entonces la condición $h_1 + h_2 + h_3^2 = 0$ es equivalente a que existan $m \in \mathbb{N}$, $g \in P$ tales que $0 = g + f^{2m}$. □

Con todo lo expuesto pasemos a enunciar y probar el Nullstellensatz Real Débil.

COROLARIO 2.4.7. **(Nullstellensatz Real Débil)**
*Sea $R$ un cuerpo realmente cerrado y sea $V$ un conjunto algebraico de $R^n$. Entonces, la siguiente es una aplicación biyectiva:*

$$\begin{aligned} V &\longrightarrow MaxSpec^{(R)}(\mathcal{P}(V)) \\ x &\longmapsto \quad \mathcal{I}_{\mathcal{P}(V)}(\{x\}). \end{aligned}$$

DEMOSTRACIÓN. En primer lugar, comprobemos que la aplicación está bien definida. Tomemos $x \in V$, y queremos ver que $\mathcal{I}_{\mathcal{P}(V)}(\{x\})$ sea un ideal maximal que además sea real. Se considera el morfismo de evaluación en $x$, definido por $ev_x(f) = f(x)$ y que es un morfismo sobreyectivo dado que $ev_x(a) = a$ para todo $a \in R$. Si además se tiene en cuenta que $ker(ev_x) = \mathcal{I}_{\mathcal{P}(V)}(\{x\})$, se sigue del Primer Teorema de Isomorfía que $R$ es isomorfo a $\mathcal{P}(V)/\mathcal{I}_{\mathcal{P}(V)}(\{x\})$. En particular, este último será un cuerpo y el ideal $\mathcal{I}_{\mathcal{P}(V)}(\{x\})$ es maximal. Ahora, definamos el conjunto $W = \{x \in V : g_x(x) \geq 0, -g_x(x) \geq 0\} = \{x\}$ donde:

$$g_x(X_1, \ldots, X_n) = (X_1 - x_1)^2 + \ldots + (X_n - x_n)^2,$$

siendo $x = (x_1, \ldots, x_n)$. Aplicando el Lema 2.4.6 sobre $V$ y los polinomios $g_1 = g_x$ y $g_2 = -g_x$ que definen a $W$, se obtiene que $f(x) = 0$ (es decir, la pertenencia de $f$ a $\mathcal{I}_{\mathcal{P}(V)}(\{x\})$) equivale a que existan $g \in \sum \mathcal{P}(V)^2[g_1, g_2]$ y $m \in \mathbb{N}$ tales que $f^{2m} + g = 0$. Como además $g_x \in \sum \mathcal{P}(V)^2$ y en vista de la Observación 2.1.4, se tendrá que esto último equivale a que existan unos $h_1, h_2 \in \sum \mathcal{P}(V)^2$ tales que $f^{2m} + h_1 = h_2 g_x$. Recordando la Proposición 1.3.8 y dado que $h_2 g_x \in (g_x)$, se tendrá que $f \in \sqrt[R]{(g_x)}$. Es decir, que $\mathcal{I}_{\mathcal{P}(V)}(\{x\}) \subset \sqrt[R]{(g_x)}$ y se tiene la igualdad por ser $\mathcal{I}_{\mathcal{P}(V)}(\{x\})$ maximal, concluyendo que la aplicación está bien definida.

Ahora, veamos que se trata de una aplicación biyectiva. Para ver que es inyectiva, fijémonos en que $\{x\} = \mathcal{Z}_V((g_x))$ y que $x \in \mathcal{Z}_V(\mathcal{I}_{\mathcal{P}(V)}(\{x\})) = \mathcal{Z}_V(\sqrt[R]{(g_x)})$. Como $(g_x) \subset \sqrt[R]{(g_x)}$, entonces $\mathcal{Z}_V(\sqrt[R]{(g_x)}) \subset \mathcal{Z}_V((g_x)) = \{x\}$ y se tiene además la igualdad $\mathcal{Z}_V(\mathcal{I}_{\mathcal{P}(V)}(\{x\})) = \{x\}$. Entonces, si tomamos $x, y \in V$ tales que $\mathcal{I}_{\mathcal{P}(V)}(\{x\}) = \mathcal{I}_{\mathcal{P}(V)}(\{y\})$, se tiene que $\{x\} = \{y\}$, luego $x = y$ y de ahí se sigue que la aplicación es inyectiva. Para ver que es sobreyectiva, tomemos un ideal maximal y real $\mathfrak{m} \in MaxSpec^{(R)}(\mathcal{P}(V))$ y comprobemos que sea de la forma $\mathcal{I}_{\mathcal{P}(V)}(\{x\})$ para algún $x \in V$. Por el Nullstellensatz Real (Corolario 1.3.11) se tiene que, dado que $\mathfrak{m}$ es ideal real propio, $\mathcal{Z}_V(\mathfrak{m})$ es no vacío y puede escogerse un $x \in \mathcal{Z}_V(\mathfrak{m})$. De otra versión del Nullstellensatz Real (Corolario 1.3.9) se sabe que $\mathfrak{m} = \mathcal{I}_{\mathcal{P}(V)}(\mathcal{Z}_V(\mathfrak{m}))$, y como $\{x\} \subset \mathcal{Z}_V(\mathfrak{m})$, entonces $\mathfrak{m} \subset \mathcal{I}_{\mathcal{P}(V)}(\{x\})$ y se da la igualdad por ser $\mathfrak{m}$ maximal. De ello se deduce que la aplicación es biyectiva. □

Capítulo 3

# El Problema XVII de Hilbert.

## Índice



En este capítulo, se trata el Problema XVII de Hilbert en su versión original y también algunas de sus variantes más reconocibles. Primeramente, se introduce históricamente el enunciado del Problema XVII y se examina la solución propuesta por Artin, fuertemente basada en las nociones de la Teoría de Artin-Schreier ya introducida en los capítulos precedentes. Se verá también una generalización que Artin dio en la propia respuesta al Problema XVII para el caso de polinomios definidos sobre subvariedad algebraica irreducible. Esto requiere hablar de la dimensión de conjuntos semi-algebraicos, que se introducirá en dicha sección. También puede verse de manera ampliada en los apéndices C, D y E. A esto le sigue una presentación del Problema XVII de Hilbert en su Versión Equivariante, que es la que se encarga de responder al problema para el caso de polinomios simétricos. Se concluye el capítulo con la Versión Cuantitativa del Problema XVII de Hilbert, que responde a la cuestión de cuál es el mínimo número de cuadrados que se requiere para poder escribir cualquier polinomio no negativo. Estas dos últimas secciones tratan tanto a los polinomios simétricos como la Teoría de Formas Cuadráticas de forma reducida, pero puede consultarse el Apéndice F para disponer de más información.

La elaboración del capítulo se ha basado fundamentalmente en el Capítulo 6 de [**BCR, 1998**]. Sin embargo, se han consultado otras fuentes para poder desarrollar los temas que tocan transversalmente al hilo principal y que puede consultarse de forma ampliada en los apéndices citados. Para la dimensión de semi-algebraicos, basada en la dimensión de anillos, se han utilizado [**AtMac, 1969**], [**Kunz, 1985**] y [**González, 2022**]. Para formas cuadráticas, se han seguido [**Gantmacher, 1959**] y [**Lam, 1973**].

### 3.1. Introducción al Problema XVII de Hilbert.

En el año 1900, tuvo lugar en París el *International Congress of Mathematicians*, donde el matemático alemán David Hilbert propuso algunos de los problemas que publicaría más tarde en su famosa lista [**Hilbert, 1900**]. Se trata de una recopilación de problemas que toca distintas áreas de las matemáticas, como la Teoría de Números o la Geometría, y que estaban entonces por resolver. No todos ellos han sido resueltos a día de hoy. Aquellos que sí lo han sido, han influido notablemente en el desarrollo de la matemática del siglo XX. Algunos de los que no han sido resueltos, se encuentran en una lista actualizada propuesta por el matemático estadounidense Steve Smale, la cual fue publicada en el año 1998 y cuenta con un total de 18 problemas.[1] También se destaca la lista propuesta por el *"Clay Mathematics Institute"* de los llamados problemas del milenio.[2]

El decimoséptimo problema de Hilbert lidia con una cuestión sobre funciones polinómicas con coeficientes reales que él mismo trató de atajar anteriormente. En el año 1888, presentó su trabajo *"Über die Darstellung definiter Formen als Summe von Formenquadraten"* sobre la descomposición de polinomios homogéneos con coeficientes reales y no negativos en sumas de

[1] S. Smale, *"Mathematical problems for the next century"*. Mathematical Intelligencer, Vol.20, pp7-15, 1998.
[2] https://www.claymath.org/millennium-problems/.

cuadrados de polinomios. Años más tarde, en 1893, publicó *"Über ternäre definite Formen"* donde se aborda la misma cuestión para polinomios en general y en el que tan solo llega a probarse afirmativamente para polinomios bivariados. Todo esto dio lugar al llamado Teorema de las Formas Positivas de Hilbert, el cual puede verse enunciado en la Subsección 0.2.1.

Una de las limitaciones de este planteamiento fue que ningún polinomio de grado impar podía ser descrito de esta forma. Otra clara limitación es que, salvo para casos con un número muy bajo de variables, la existencia de una descomposición en cuadrados de polinomios sencillamente no da lugar. Con todo esto sobre la mesa, Hilbert planteó el problema de la siguiente manera, ampliando la descomposición de cuadrados al cuerpo de fracciones de polinomios:

Problema Clásico 3.1.1. **(Problema XVII de Hilbert)**
*Considérese el cuerpo de los números reales $\mathbb{R}$ y un polinomio $f$ en $n$ variables con coeficientes en dicho cuerpo. Si $f$ toma valores no negativos en todo $\mathbb{R}^n$, ¿puede afirmarse que $f$ sea una suma de cuadrados del cuerpo de fracciones de los polinomios?*

Durante la década de 1920, Emil Artin y Otto Schreier, un par de matemáticos austriacos, lograron sucesivos avances en la Teoría de Cuerpos Ordenados y de Cuerpos Realmente Cerrados. En 1927, publicaron conjuntamente el trabajo *"Eine Kennzeichnung der reell abgeschlossenen Körper"*, que contiene lo que se conoce a día de hoy como Teoría de Artin-Schreier. En capítulos previos se ha visto y trabajado con varios elementos de esta teoría, ya que este formalismo hizo posible que Artin lograse dar solución al problema XVII de Hilbert. Dicha respuesta fue publicada en su trabajo *"Über die Zerlegung definiter Funktionen in Quadrate"*, en el año 1927.

Hilbert, durante su carrera, logró importantes avances para la Geometría Algebraica de los números complejos. Son conocidos el Teorema de la Base y el Nullstellensatz de Hilbert, resultados que publicó en 1890 y 1893, respectivamente. Sin embargo, la dificultad que presenta la Geometría Algebraica en los reales frente a la de los complejos, fue suficiente para que Hilbert no pudiese aportar una generalización de sus resultados para el caso real. La Teoría de Artin-Schreier introduce las nociones de cuerpo formalmente real y cuerpo realmente cerrado, que han sido centrales en el desarrollo de la Geometría Algebraica Real como se ha visto, por ejemplo, en la prueba del Nullstellensatz Real dada en el primer capítulo.

## 3.2. Solución al Problema XVII de Hilbert.

En esta sección veremos la solución de Artin al Problema XVII de Hilbert, que sirve para cualquier cuerpo realmente cerrado. En el planteamiento del problema se habla de polinomios no negativos. Un polinomio $f \in R[X_1, \ldots, X_n]$ se dice no negativo (o positivo) en $R^n$, si la evaluación de $f$ en todo punto $x \in R^n$ es no negativa (o positiva). En general, se entiende que $f$ es no negativo (o positivo) en un subconjunto de $R^n$ si la evaluación de $f$ en cada punto de dicho subconjunto es no negativa (o positiva). El problema XVII para cuerpos realmente cerrados, queda resuelto con el siguiente teorema:

Teorema 3.2.1. **(de Artin)** *Sea $R$ un cuerpo realmente cerrado y sea $f \in R[X_1, \ldots, X_n]$. Si $f$ es no negativo en $R^n$, entonces $f$ es una suma de cuadrados de elementos del cuerpo de fracciones $R(X_1, \ldots, X_n)$.*

Demostración. Supongamos que $f$ no sea una suma de cuadrados de $R(X_1, \ldots, X_n)$, lo que implica además que $f \neq 0$. Aplicando el Lema 2.1.10, se tiene la existencia de alguna ordenación $\leq$ de $R(X_1, \ldots, X_n)$ en la que $f < 0$. Sea $R_1$ clausura real de $R(X_1, \ldots, X_n)$ que extiende a la ordenación $\leq$, cuya existencia viene garantizada por la Proposición 2.1.15. Se tiene que $-f \geq 0$ y como $R_1$ es cuerpo realmente cerrado, por el Lema 2.1.12 se tendrá que $\sqrt{-f}$ pertenece a $R_1$, y también que $1/\sqrt{-f} \in R_1$.

El polinomio $fT^2 + 1$ de $R_1[T]$ tiene como raíz a $1/\sqrt{-f}$. Se define el morfismo de anillos $\phi : R[X_1, \ldots, X_n][T] \to R_1$ que cumple que $\phi(T) = 1/\sqrt{-f}$ y que $\phi(g) = g$ para cada $g \in R[X_1, \ldots, X_n]$. Entonces, se cumple que el ideal $\mathfrak{a} = (fT^2 + 1)$ está incluido en $ker(\phi)$ sin más que observar que $\Phi(fT^2+1) = f \cdot (\Phi(T))^2 + 1 = f \cdot (-1/f) + 1 = 0$. Se define el anillo cociente $B = R[X_1, \ldots, X_n][T]/(fT^2+1)$ y se tiene, por la Propiedad Universal del Anillo Cociente, un morfismo $\overline{\phi}$ de $B$ en $R_1$ tal que $\overline{\phi} \circ \pi = \phi$, siendo $\pi$ a proyección de $R[X_1, \ldots, X_n][T]$ en $B$. Se tiene que $\overline{\phi}$ es un morfismo de $R$-álgebras dado que $\overline{\phi}(x+(fT^2+1)) = \phi(x) = x$ para todo $x \in R$,

es decir, que $\overline{\phi}$ restringido a $R$ es la identidad en $R$. Aplicando el Teorema del Homomorfismo de Artin-Lang 1.2.10, se tiene la existencia de otro morfismo de $R$-álgebras $\psi : B \to R$. Por una parte, $0 = \psi(0 + \mathfrak{a}) = \psi(fT^2 + 1 + \mathfrak{a})$, pero también se tiene $\psi(fT^2 + 1 + \mathfrak{a}) = t^2\psi(f + \mathfrak{a}) + 1$ siendo $t = \psi(T + \mathfrak{a}) \in R$. Aplicando que $\psi$ es un morfismo de anillos y escribiendo $f$ como suma de monomios, se deduce que $\psi(f + \mathfrak{a}) = f(x_1, \ldots, x_n)$ para $x_i = \psi(X_i + \mathfrak{a}) \in R$. Entonces se tiene que $(x_1, \ldots, x_n)$ pertenece a $R^n$ y cumple que $f(x_1, \ldots, x_n) = -1/t^2 < 0$, lo que contradice que $f$ sea no negativo en todo $R^n$ y en consecuencia, $f$ será una suma de cuadrados en $R(X_1, \ldots, X_n)$. □

Este y resultados posteriores pueden generalizarse a funciones racionales en general de manera sencilla. Se considera el elemento $f/g$ del cuerpo de fracciones $R(X_1, \ldots, R_n)$. Si además $g$ no se anula en todo el conjunto para el que $f/g$ se requiere no negativa, entonces puede sustituirse el representante $f/g$ por el equivalente $fg/g^2$. Dado que $g^2$ es un cuadrado y por ende es no negativo en todo $R^n$, bastaría con trabajar sobre el polinomio $fg$.

No se tiene la generalización del Teorema 3.2.1 para todo cuerpo ordenado. El primer contraejemplo tomó algo de tiempo en obtenerse y se atribuye a D. W. Dubois, quien lo publicó en un artículo titulado *"Note on Artin's solution of Hilbert's 17th problem"* en 1967. Sin embargo, puede darse una descomposición de los polinomios no negativos con coeficientes en un cuerpo ordenado como combinaciones lineales de cuadrados y con coeficientes positivos. Este resultado de 1975 se debe a K. McKenna y puede verse en su artículo *"New facts about Hilbert's 17th Problem"*. Antes de enunciar y probar este resultado, es necesario introducir este tipo de elementos de una extensión de cuerpos ordenados y dar una descomposición parecida.

Definición 18. **(Elemento Relativamente Positivo)**
*Sea $(F, \leq)$ un cuerpo ordenado y sea $F_1$ una extensión de cuerpo de $F$ que admita alguna ordenación que extienda a la de $F$. Un elemento $x \in F_1$ se dice positivo en relación con $F$ cuando pertenece a todo cono primo de $F_1$ cuya ordenación extienda a la de $F$.*

Dicho de otra forma, el conjunto de elementos positivos en relación con $F$ es la intersección de todos los conos positivos de las posibles ordenaciones de $F_1$ que extiendan a la de $F$. Dicho conjunto no necesariamente coincide con el de las sumas de cuadrados. Veamos ahora la descomposición de estos elementos de una extensión de cuerpos ordenados.

Lema 3.2.2. *Sea $(F, \leq)$ un cuerpo ordenado y sea $F_1$ una extensión de cuerpo de $F$ que admita alguna ordenación que extienda a la de $F$. Entonces, para cada elemento $x \in F_1$ positivo en relación con $F$ existen $a_1, \ldots, a_r \in F$ elementos positivos y también $y_1, \ldots, y_r \in F_1$ tales que $x = a_1y_1^2 + \ldots + a_ry_r^2$.*

Demostración. Sea $\tilde{\imath}$ la inclusión de $F$ en $F_1$, que es un morfismo inyectivo. El conjunto de elementos de $F_1$ positivos en relación con $F$ es intersección de conos positivos, y por ello es un cono propio. Si llamamos $P$ al cono positivo de la ordenación de $F$, el conjunto de elementos positivos en relación con $F$ ha de ser el mínimo cono que contenga a $\tilde{\imath}(P)$, es decir, se trata de $\sum F_1^2[\tilde{\imath}(P)]$. Por otro lado, sea $X = \{a_1y_1^2 + \ldots + a_ry_r^2 \in F_1 : a_1, \ldots, a_r \in \tilde{\imath}(P), y_1, \ldots, y_r \in F_1\}$. Se desea probar que $X$ sea igual a $\sum F_1^2[i(P)]$.

Se observa que $\sum F_1^2[\tilde{\imath}(P)]$ contiene tanto a $\sum F_1^2$ como a $\tilde{\imath}(P)$, y entonces $X \subset \sum F_1^2[\tilde{\imath}(P)]$. Para probar el otro contenido, veamos que $X$ contiene a $\sum F_1^2$ y a $\tilde{\imath}(P)$, y que además es un cono. En tal caso, ocurriría que $\sum F_1^2[\tilde{\imath}(P)] \subset \sum F_1^2[X] = X$. Un elemento $y_1^2 + \ldots + y_r^2$ de $\sum F_1^2$ puede reescribirse como $1y_1^2 + \ldots + 1y_r^2$, luego $\sum F_1^2 \subset X$ por $1 \in \tilde{\imath}(P)$. Un elemento $x$ de $\tilde{\imath}(P)$ puede escribirse como $x1^2$, luego pertenece a $X$.

Nos falta comprobar que $X$ sea un cono. Claramente, una suma de elementos de $X$ es otro elemento de $X$. Para ver el producto, tomemos $a_1x_1^2 + \ldots + a_rx_r^2, b_1y_1^2 + \ldots + b_sy_s^2 \in X$. Entonces:

$$(a_1x_1^2 + \ldots + a_rx_r^2)(b_1y_1^2 + \ldots + b_sy_s^2) = \sum_{i=1}^{r}\sum_{j=1}^{s}(a_ib_j)(x_i^2y_j^2),$$

y como cada $a_ib_j$ pertenece a $P$ y cada $x_i^2y_j^2$ puede escribirse como $(x_iy_j)^2$, el producto pertenece a $X$. Finalmente, dado $x \in F_1$, $x^2 = 1x^2 \in X$. De esto se deduce que $X$ coincide con el conjunto de los elementos de $F_1$ positivos en relación con $F$. □

Si se tiene una extensión $F_1$ del cuerpo $F$ que no disponga de una ordenación que extienda a la de $F$, se observa que todo elemento de $F_1$ es de la forma $a_1y_1^2 + \ldots + a_ry_r^2$ con $y_1, \ldots, y_r \in F_1$ y $a_1, \ldots, a_r \in F$. Esto lleva al siguiente resultado, que consiste en una forma de caracterizar la existencia de una ordenación para la extensión de cuerpos que extienda a la del cuerpo original, y se conoce como Criterio de Serre.

COROLARIO 3.2.3. **(Criterio de Serre)**
*Sea la extensión de cuerpos $F_1/F$ y sea $P \subset F$ el cono positivo de alguna ordenación de $F$. Entonces, son equivalentes:*

(*i*) *existe $Q \subset F_1$ cono positivo de alguna ordenación de $F_1$ que extienda a la de $F$,*
(*ii*) *$-1 \notin \sum F_1^2[P]$, donde se entiende que $P$ es el subconjunto de $F_1$ que viene dado como la imagen de $P$ por la inclusión de $F$ en $F_1$.*

DEMOSTRACIÓN. En primer lugar, obsérvese que la Proposición 2.1.3 lleva a deducir que los elementos de $\sum F_1^2[P]$ son de la forma $a_1g_1^2 + \cdots + a_rg_r^2$ con $a_1, \ldots, a_r \in P$ y con $g_1, \ldots, g_r \in F_1$. Probemos que $(i) \Rightarrow (ii)$. Si llamamos $\tilde{\imath}$ a la inclusión de $F$ en $F_1$, se tiene que $\tilde{\imath}(P) \subset Q$, de modo que $\sum F_1^2[\tilde{\imath}(P)] \subset Q$. No puede darse que $-1$ pertenezca a $\sum F_1^2[\tilde{\imath}(P)]$ porque $Q$ es un cono propio. Esto prueba la implicación. Probemos ahora que $(ii) \Rightarrow (i)$. Suponiendo $(ii)$ se tiene que $\sum F_1^2[\tilde{\imath}(P)]$ es un cono propio. Si se considera la Observación 2.1.8, se tiene la existencia de un cono propio maximal $Q \subset F_1$ que contiene a $\sum F_1^2[\tilde{\imath}(P)]$, que será el cono positivo de alguna ordenación de $F_1$. Como además $\tilde{\imath}(P) \subset Q$, ocurre que esta ordenación de $F_1$ extiende a la ordenación de $F$ dada por el cono positivo $P$. Con esto se concluye la prueba. □

Con todo esto, ya podemos dar la prueba del anunciado resultado de McKenna pero con cierta limitación, y es que resultará conveniente asumir que el polinomio $f$ $F[X_1, \ldots, X_n]$ escogido sea no negativo no solo en $F^n$ sino en todo $R^n$, con $R$ alguna clausura algebraica de $F$.

TEOREMA 3.2.4. *Sea $(F, \leq)$ un cuerpo ordenado y sea $R$ su clausura real. Sea $f \in F[X_1, \ldots, X_n]$. Si $f$ es no negativo en $R^n$, entonces existen $a_1, \ldots, a_r \in F$ elementos positivos y también $g_1, \ldots, g_r \in F(X_1, \ldots, X_n)$ tales que $f = a_1g_1^2 + \ldots + a_rg_r^2$.*

DEMOSTRACIÓN. Se considera la extensión de cuerpos $F(X_1, \ldots, X_n)/F$, y además se tiene una ordenación específica para $F$. Supongamos que el polinomio $f \in F[X_1, \ldots, X_n]$ no pueda escribirse como $f = a_1g_1^2 + \ldots + a_rg_r^2$ para con $a_1, \ldots, a_r$ y $g_1, \ldots, g_r$ como los del enunciado. Entonces, aplicando el Lema 3.2.2, se tiene que $f$ no es un elemento de $F(X_1, \ldots, X_n)$ positivo en relación con $F$, es decir, que existirá alguna ordenación de $F(X_1, \ldots, X_n)$ que extienda a la de $F$ y para la que $f$ será negativo. Sea $R_1$ la clausura real de $F(X_1, \ldots, X_n)$, que será una extensión del cuerpo $R$ (la clausura real de $F$) y cuya ordenación extiende a la de $R$ de modo que el elemento $f$ es negativo. Desde este punto, se sigue el mismo razonamiento que para la prueba del Teorema de Artin 3.2.1 hasta obtener un punto $x \in R^n$ para el que $f(x) < 0$. □

La hipótesis de que $f$ sea no negativo en $R^n$ en lugar de solo en $F^n$ es necesaria para poder utilizar el Principio de Transferencia para cuerpos realmente cerrados. Veamos ahora un ejemplo sencillo en el que la propiedad de densidad de un cuerpo en su clausura real es suficiente para relajar esta hipótesis.

EJEMPLO 3.2.5. *Sea $F$ un subcuerpo de $\mathbb{R}$. Como $\mathbb{R}$ es un cuerpo realmente cerrado, este admite una única ordenación. Considerando $i$ la inclusión de $F$ en $\mathbb{R}$ y la Proposición 2.2.5, se tiene que $i^{-1}(\sum \mathbb{R}^2)$ es un cono primo de $F$ que da lugar a una ordenación que es extendida por la de $\mathbb{R}$. Entonces se cumple las condiciones del Teorema 3.2.4 para $F$ y su extensión $\mathbb{R}$.*

*Por otra parte, se tiene que $\mathbb{Q}$ está contenido en $F$ en el sentido de que existe una copia isomorfa de $\mathbb{Q}$ en $F$. Utilizando que $\mathbb{Q}$ es denso en $\mathbb{R}$, veamos que la condición de que un polinomio $f \in F[X_1, \ldots, X_n]$ sea no negativo en $F^n$ implica que también lo sea en $\mathbb{R}^n$. Como $\mathbb{Q}^n \subset F^n$, entonces $f$ es no negativo en $\mathbb{Q}^n$. Se conoce que $\mathbb{Q}^n$ es denso en $\mathbb{R}^n$ con la topología usual, y también que las funciones polinómicas son continuas con esta topología.*

*Sea $\hat{f} \in \mathcal{P}(\mathbb{R}^n)$ la función polinómica que define $f$ visto desde $\mathbb{R}[X_1, \ldots, X_n]$, que como sabemos es continua y toma valores no negativos para puntos del conjunto $\mathbb{Q}^n$. Supongamos que existe $x \in \mathbb{R}^n$ tal que $\hat{f}(x) < 0$. Como $\hat{f}$ es continua, dado el valor positivo $\varepsilon = -\hat{f}(x)$, existe $\delta_\varepsilon > 0$ en $\mathbb{R}$ tal que $|x-y| < \delta_\varepsilon \Rightarrow |\hat{f}(x) - \hat{f}(y)| < \varepsilon$ para cada $y \in \mathbb{R}^n$. Como $\mathbb{Q}^n$ es denso en $\mathbb{R}^n$, puede*

*escogerse* $y \in \mathbb{Q}^n$ *tal que* $|x-y| < \delta_\varepsilon$. *Considerando que* $\hat{f}(y)$, $-\hat{f}(x)$ *son positivos, se tiene que* $|\hat{f}(x) - \hat{f}(y)| = \hat{f}(y) - \hat{f}(x) < -\hat{f}(x) = \varepsilon$, *de lo que se sigue la contradicción* $0 \leq \hat{f}(y) < 0$. *Entonces,* $\hat{f}(x)$ *ha de ser no negativo y en definitiva,* $f$ *es no negativa en* $\mathbb{R}^n$.

En el caso de los números reales $\mathbb{R}$, es justo el hecho de que todos sus subcuerpos sean densos en él lo que permite relajar esta condición. En el artículo original de McKenna y también en algún artículo posterior como *"Sums of squares over fields"* de 1979 y escrito por A. Prestel, se discute que esta hipótesis pueda relajarse para los casos en que el cuerpo $F$ cumpla la llamada Propiedad Débil de Hilbert. Esta será una cuestión que no abordaremos, pero que se menciona para el lector curioso.

## 3.3. Generalización a Conjuntos Algebraicos Irreducibles.

Artin también dio solución al Problema XVII de Hilbert para el caso de anillos de polinomios $\mathcal{P}(V)$ que sean dominios, y que, por lo tanto, tengan un cuerpo de fracciones asociado $\mathcal{K}(V)$. El resultado obtenido es que las sumas de cuadrados de cocientes de polinomios de $\mathcal{P}(V)$ son los polinomios no negativos en casi todo $V$ y viceversa, donde casi todo quiere decir que lo son para un conjunto semi-algebraico que tenga la misma dimensión que la variedad $V$. Por lo tanto, será necesario introducir la dimensión de los conjuntos algebraicos y los semi-algebraicos. Por motivos de espacio, presentaremos sin demostración los resultados sobre dimensión de conjuntos semi-algebraicos, cuya prueba puede seguirse en [**BCR, 1998**] y además se añade material de apoyo en los Apéndices C, D y E. Para comenzar, veamos la condición necesaria y suficiente que hace al anillo de polinomios $\mathcal{P}(V)$ un dominio. Se basa en la siguiente definición.

Definición 19. **(Conjunto Algebraico Irreducible)**
*Sea* $R$ *un dominio y sea* $V$ *un conjunto algebraico de* $\mathbb{A}^n(R)$. $V$ *se dice irreducible si para cada* $V_1, V_2 \subset \mathbb{A}^n(R)$ *algebraicos tales que* $V = V_1 \cup V_2$ *se tiene que* $V \neq V_1 \Rightarrow V = V_2$. *En caso contrario,* $V$ *se dice reducible.*

Los conjuntos algebraicos de este tipo comparten la propiedad de que el ideal asociado por la aplicación $\mathcal{I}_{R[X]}(V)$ es un ideal primo, luego $\mathcal{P}(V)$ será un dominio de integridad y puede considerarse su cuerpo de fracciones, que denotaremos por $\mathcal{K}(V)$ y se conoce como el cuerpo de las funciones racionales de $V$ en $R$.

Pasamos a definir la dimensión de un conjunto semi-algebraico $S$ de $\mathbb{A}^n(R)$ para $R$ un cuerpo realmente cerrado. Para ello, es útil tener en cuenta una descomposición especial para los conjuntos semi-algebraicos. Para un par de elementos $a, b \in R$ tales que $a < b$, se define el intervalo abierto $(a,b) = \{x \in R : a < x < b\}$. Con esta notación, se define el conjunto $(0,1)^d \subset \mathbb{A}^d(R)$ como el producto cartesiano de $d$ intervalos de la forma $(0,1)$. Este conjunto tendrá una dimensión topológica $d$, y por ello se le conoce como el hipercubo de dimensión $d$. La descomposición de un semi-algebraico $S$ a la que nos referimos, consiste en una partición finita de conjuntos $S_1, \ldots, S_r$ semi-algebraicos tales que cada $S_i$ sea homeomorfo a un hipercubo $(0,1)^{d_i}$. Este homeomorfismo será, además, una aplicación del tipo siguiente.

Definición 20. **(Aplicación Semi-Algebraica)**
*Sea* $R$ *un cuerpo realmente cerrado. Sean* $S$ *y* $T$ *conjuntos semi-algebraicos de* $\mathbb{A}^n(R)$ *y* $\mathbb{A}^m(R)$, *respectivamente. Una aplicación* $f : S \longrightarrow T$ *se dice semi-algebraica si su grafo, es decir, el conjunto:*

$$Graf(f) = \{(x,y) \in \mathbb{A}^{n+m}(R) : f(x) = y\}$$

*es un conjunto semi-algebraico de* $\mathbb{A}^{n+m}(R)$.

Estas aplicaciones cuentan con la propiedad de que las imágenes y las anti imágenes de conjuntos semi-algebraicos son también semi-algebraicos. Con esto, puede enunciarse el teorema de la descomposición mencionada.

Teorema 3.3.1. *Sea* $R$ *un cuerpo realmente cerrado y sea* $S \subset \mathbb{A}^n(R)$ *un conjunto semi-algebraico. Existe una partición finita de* $S$ *en los conjuntos semi-algebraicos* $S_1, \ldots, S_r$, *de tal forma que* $S_i$ *sea semi-algebraicamente homeomorfo al hipercubo* $(0,1)^{d_i}$ *de* $\mathbb{A}^{d_i}(R)$, *con* $d_i \in \mathbb{N}$ *y para cada* $i = 1, \ldots, r$; *y siendo que semi-algebraicamente homeomorfo significa que se tiene un homeomorfismo que además sea aplicación semi-algebraica.*

DEMOSTRACIÓN. Véase el Teorema 2.3.6 de [**BCR, 1998**]. □

Entonces, ante esta propiedad de los semi-algebraicos, uno esperaría de cualquier noción de dimensión que se defina que la dimensión de un semi-algebraico coincida con el máximo de las dimensiones de las componentes semi-algebraicas dadas por esta descomposición, dimensión que heredan por la relación de homeomorfía con sus respectivos hipercubos. Sin entrar en detalles, veremos una idea de dimensión para conjuntos semi-algebraicos que cumple con esta propiedad deseable y que se basa en la siguiente noción de dimensión de un anillo.

DEFINICIÓN 21. **(Dimensión de Krull de un Anillo)**
*Sea $A$ un anillo conmutativo. Se dice dimensión de Krull de $A$ y se denota por $dim_{Krull}(A)$ al máximo de los $r \in \mathbb{N}$ para los que existe alguna cadena de ideales primos tales que:*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_r.$$

*En caso de no existir dicho máximo, se define $dim_{Krull}(A) = +\infty$.*

Con esta idea, daremos la dimensión de un conjunto algebraico $V \subset \mathbb{A}^n(R)$ como la dimensión del anillo de polinomios $\mathcal{P}(V)$ asociado. Más aún, como para un semi-algebraico $S \subset \mathbb{A}^n(R)$ se tiene la igualdad $\mathcal{I}_{R[X]}(S) = \mathcal{I}_{R[X]}(clau_{\mathcal{Z}}(S))$, donde $clau_{\mathcal{Z}}(S)$ denota a la clausura de $S$ en la topología de Zariski sobre $\mathbb{A}^n(R)$, entonces puede definirse una dimensión para conjuntos semi-algebraicos en general como sigue.

DEFINICIÓN 22. **(Dimensión de un Conjunto Semi-Algebraico)**
*Sea $R$ un cuerpo realmente cerrado y sea $S$ un conjunto semi-algebraico de $\mathbb{A}^n(R)$. Se define la dimensión de $S$ como:*

$$dim(S) = dim_{Krull}(\mathcal{P}(clau_{\mathcal{Z}}(S))).$$

Veamos una serie de propiedades sobre esta definición de dimensión. Aquí van un par de las más sencillas.

PROPOSICIÓN 3.3.2. *Sea $R$ un cuerpo realmente cerrado. Se cumple las siguientes propiedades:*

(*i*) $dim(\mathbb{A}^n(R)) = n$.
(*ii*) *Sean $S_1, S_2 \subset \mathbb{A}^n(R)$ unos conjuntos semi-algebraicos tales que $S_1 \subset S_2$. Entonces:*

$$dim(S_1) \leq dim(S_2).$$

DEMOSTRACIÓN. Puede consultarse en la Sección 2.8 de [**BCR, 1998**].
□

Continuamos con otra serie de resultados sobre dimensión en relación con las topologías sobre $\mathbb{A}^n(R)$.

PROPOSICIÓN 3.3.3. *Sea $R$ un cuerpo realmente cerrado. Entonces, se cumple que:*

(*i*) *Si $U \subset \mathbb{A}^n(R)$ es un conjunto semi-algebraico no vacío y abierto para la topología euclídea sobre $\mathbb{A}^n(R)$, entonces:*

$$dim(U) = n.$$

(*ii*) *Si $S \subset \mathbb{A}^n(R)$ es un conjunto semi-algebraico, se tendrá que:*

$$dim(clau_{\mathcal{Z}}(S) \setminus S) < dim(S).$$

(*iii*) *Si $V_1, V_2 \subset \mathbb{A}^n(R)$ son un par de conjuntos algebraicos tales que $V_1 \subsetneq V_2$, se sigue que:*

$$dim(V_1) < dim(V_2).$$

DEMOSTRACIÓN. Véase la Proposición 2.8.4 y la Proposición 2.8.13 de [**BCR, 1998**]. □

Para terminar con este despliegue de propiedades, veamos algunas sobre operaciones de semi-algebraicos que dan lugar a otros semi-algebraicos: unión, intersección, proyección y producto cartesiano. Esta última se basa en el hecho de que la clausura Zariski del producto de semi-algebraicos es igual que el producto cartesiano de sus clausuras Zariski.

PROPOSICIÓN 3.3.4. *Sea $R$ un cuerpo realmente cerrado. Se tienen las siguientes propiedades para la dimensión de semi-algebraicos:*

(*i*) *Si* $S_1, \ldots, S_r$ *son conjuntos semi-algebraicos de* $\mathbb{A}^n(R)$*, entonces:*

$$dim(S_1 \cup \cdots \cup S_r) = \max_{i=1,\ldots,r}(\{dim(S_i)\}).$$

(*ii*) *Si* $S_1, \ldots, S_r$ *son conjuntos semi-algebraicos de* $\mathbb{A}^n(R)$*, entonces:*

$$dim(S_1 \cap \cdots \cap S_r) \leq \min_{i=1,\ldots,r}(\{dim(S_i)\}).$$

(*iii*) *Si* $S \subset \mathbb{A}^{n+m}(R)$ *es un conjunto semi-algebraico y* $\pi$ *es la proyección de* $\mathbb{A}^{n+m}(R)$ *en* $\mathbb{A}^n(R)$ *que olvida las* $m$ *últimas coordenadas, entonces:*

$$dim(\pi(S)) \leq dim(S).$$

(*iv*) *Si* $S \subset \mathbb{A}^n(R)$ *y* $T \subset \mathbb{A}^m(R)$ *son conjuntos semi-algebraicos, entonces:*

$$dim(S \times T) = dim(S) + dim(T),$$

*entendiendo la dimensión de* $S \times T$ *como la de un semi-algebraico de* $\mathbb{A}^{n+m}(R)$*.*

Demostración. Véase la Proposición 2.8.5 y la Proposición 2.8.6 de [**BCR, 1998**]. □

Ahora vamos a ver la definición de punto regular de una variedad, junto con alguna de sus formulaciones equivalentes. Empezamos por definir las derivadas parciales de un polinomio.

Definición 23. **(Derivada de un Polinomio en un Anillo)**
*Sea* $A$ *un anillo conmutativo y sea* $f \in A[X_1, \ldots, X_n]$*. Supongamos que existen* $d_i \in \mathbb{N}$ *y unos polinomios* $\hat{f}_0, \ldots, \hat{f}_{d_i} \in A[X_1, \ldots, X_n]$ *que no dependen de la variable* $X_i$*, de tal modo que:*

$$f = \sum_{k=0}^{d_i} \hat{f}_k X^k.$$

*Entonces, se define la derivada de* $f$ *respecto de* $X_i$ *como el polinomio siguiente:*

$$\frac{\partial f}{\partial X_i}(X_1, \ldots, X_n) = \sum_{k=0}^{d_i - 1} (k+1)\hat{f}_{k+1} X^k.$$

Se hablará de regularidad para un punto $p$ de una variedad algebraica $V$ irreducible que esté incluida en un espacio $\mathbb{A}^n(R)$ con $R$ algún cuerpo realmente cerrado. Se define el gradiente de un polinomio $f \in R[X_1, \ldots, X_n]$ en el punto $p$ como el siguiente vector de $\mathbb{A}^n(R)$:

$$\nabla_p f = \left( \frac{\partial f}{\partial X_1}(p), \ldots, \frac{\partial f}{\partial X_n}(p) \right).$$

Con esto, se define el espacio tangente a un punto de una variedad de la manera siguiente.

Definición 24. **(Espacio Tangente Zariski)**
*Sea* $R$ *un cuerpo realmente cerrado. Sean* $V$ *un conjunto algebraico irreducible de* $\mathbb{A}^n(R)$ *y* $p \in V$ *un punto de la variedad. Sean también* $f_1, \ldots, f_r \in R[X_1, \ldots, X_n]$ *unos generadores del ideal* $\mathcal{I}_{R[X_1,\ldots,X_n]}(V)$*. Se define el espacio tangente al punto* $p$ *en* $V$ *como el* $R$*-espacio vectorial:*

$$T_p V = \bigcap_{i=1}^{r} \left\{ v \in \mathbb{A}^n(R) : (\nabla f_i(p))^T v = 0 \right\}.$$

Puede probarse que la definición del espacio tangente a un punto en una variedad no depende de la familia de generadores del ideal asociado a la variedad, y también que se trata de un $R$-espacio vectorial. Estamos interesados en estudiar su dimensión como $R$-espacio vectorial, que se denotará por $dim_R(T_p V)$.

Proposición 3.3.5. *Sea* $R$ *un cuerpo realmente cerrado. Sea* $\mathfrak{p}$ *un ideal primo de* $R[X_1, \ldots, X_n]$ *y sea* $\{f_1, \ldots, f_r\} \subset R[X_1, \ldots, X_n]$ *una familia de generadores del ideal* $\mathfrak{p}$*. Se considera el anillo cociente* $R[X_1, \ldots, X_n]/\mathfrak{p}$ *con dimensión* $d = dim_{Krull}(R[X_1, \ldots, X_n]/\mathfrak{p})$ *y a su cuerpo de fracciones* $k(\mathfrak{p}) = Frac(R[X_1, \ldots, X_n]/\mathfrak{p})$*. Se define esta matriz con coordenadas en* $k(\mathfrak{p})$*:*

$$DF = \left( \frac{\partial f_i}{\partial X_j} + \mathfrak{p} \right)_{\substack{i=1,\ldots,r \\ j=1,\ldots,n}} \in \mathcal{M}_{r \times n}(k(\mathfrak{p})).$$

*Entonces,* $DF$ *es una matriz de rango* $n - d$ *en* $\mathcal{M}_{r \times n}(k(\mathfrak{p}))$*.*

DEMOSTRACIÓN. Consúltese la Sección 3.3 de [**BCR, 1998**]. □

La matriz $DF$ definida en la proposición previa permite calcular la dimensión del espacio tangente a un punto en una variedad, como veremos a continuación. Utilizando las notaciones precedentes, si definimos a la matriz $DF(p) \in \mathcal{M}_{r\times n}(R)$ como la matriz $DF$ con sus entradas evaluadas en el punto $p$, entonces puede definirse la siguiente aplicación lineal:

$$\begin{aligned} DF(p) : \mathbb{A}^n(R) &\longrightarrow \quad \mathbb{A}^r(R) \\ v \quad &\longmapsto DF(p)\cdot v, \end{aligned}$$

cuyo núcleo es el espacio tangente $T_pV$. Por este motivo, se tiene que:

$$dim_R(T_pV) = n - rank(DF(p)).$$

Nótese que cualquier menor nulo de la matriz $DF$, también será nulo en la matriz $DF(p)$, pero no necesariamente al revés. Por lo tanto, se tiene la siguiente desigualdad:

$$dim_R(T_pV) \geq n - rank(DF).$$

Esto lleva a dar la siguiente definición de un punto regular en una variedad.

DEFINICIÓN 25. **(Punto Regular de una Variedad)**
*Sea $R$ un cuerpo realmente cerrado y sea $V$ un conjunto algebraico irreducible de $\mathbb{A}^n(R)$. Un punto $p \in V$ se dice regular en $V$ cuando:*

$$dim_R(T_pV) = dim(V),$$

*o equivalentemente si:*

$$rank(DF(p)) = n - dim(V).$$

*Se denota por $Reg(V)$ al conjunto de puntos regulares de $V$. Un punto que no es regular en su variedad se dice singular, y se denota por $Sing(V)$ a los puntos singulares de la variedad $V$.*

Pasemos a dar una definición puntual de dimensión. Consideremos un punto $p$ de una variedad algebraica $V$ de $\mathbb{A}^n(R)$. Llamaremos entorno algebraico de $p$ en $V$ a cualquier conjunto $U$ algebraico tal que $p \in U \subset V$. Por la noetherianidad de $R[X_1, \ldots, X_n]$, que hereda de $R$ por el Teorema de la Base 1.1.1, para una cadena descendente $U_1 \supset U_2 \supset \ldots$ de entornos algebraicos del punto $p$ en $V$, se tendrá que sus ideales asociados formen una cadena ascendente de ideales que se estabilice en algún ideal. En consecuencia, puede tomarse como dimensión de la variedad $V$ en un punto $x$ la dimensión de algún entorno algebraico lo suficientemente pequeño, y esto es también aplicable a conjuntos semi-algebraicos.

DEFINICIÓN 26. **(Dimensión Puntual en un Conjunto Semi-Algebraico)**
*Sea $R$ un cuerpo realmente cerrado. Sea $S$ un conjunto algebraico de $\mathbb{A}^n(R)$ y sea $p$ un punto de $S$. Se dice dimensión de $S$ en el punto $p$ a la dimensión de un entorno algebraico $U$ de $p$ en $S$ tal que cada $U' \subset U$ entorno algebraico de $p$ en $S$ cumple que $dim(U') = dim(U)$. La dimensión de $S$ en el punto $p$ se denota por $dim(S_p)$.*

La dimensión de un conjunto semi-algebraico en un punto sigue la siguiente propiedad, que obviamente tiene que cumplirse.

PROPOSICIÓN 3.3.6. *Sea $R$ un cuerpo realmente cerrado y sea $S \subset \mathbb{A}^n(R)$ un conjunto semi-algebraico. Entonces se cumple que:*

$$dim(S) = max(\{dim(S_p) : p \in S\}).$$

DEMOSTRACIÓN. Puede consultarse en la Sección 2.8 de [**BCR, 1998**]. □

Otra propiedad de la dimensión puntual, es que el conjunto de puntos en los que la variedad tiene dimensión máxima es un cerrado Zariski.

PROPOSICIÓN 3.3.7. *Sea $R$ un cuerpo realmente cerrado. Sea $S$ un conjunto algebraico de $\mathbb{A}^n(R)$ de dimensión $d$. Entonces, este conjunto es un cerrado Zariski no vacío de dimensión $d$:*

$$S^{(d)} = \{x \in S : dim(S_x) = d\}.$$

DEMOSTRACIÓN. Puede verse la Proposición 2.8.12 de [**BCR, 1998**]. □

En el caso de una variedad algebraica, este conjunto resulta ser la clausura Zariski de los puntos regulares de dicha variedad.

PROPOSICIÓN 3.3.8. *Sea $R$ un cuerpo realmente cerrado y sea $V$ un conjunto algebraico de $\mathbb{A}^n(R)$ de dimensión $d$. Entonces, se cumple que:*

$$clau_{\mathcal{Z}}(Reg(V)) = V^{(d)},$$

*y en particular, se tiene la inclusión:*

$$Reg(V) \subset V^{(d)}.$$

DEMOSTRACIÓN. Puede consultarse en la Sección 3.3 de [**BCR, 1998**]. □

Con las notaciones precedentes, se tiene que $Reg(V)$ es un abierto Zariski para la topología sobre $V$ heredada por la topología Zariski de $\mathbb{A}^n(R)$. Su dimensión y la de $Sing(V)$ pueden verse en el resultado siguiente.

COROLARIO 3.3.9. *Sea $R$ un cuerpo realmente cerrado y sea $V$ un conjunto algebraico de $\mathbb{A}^n(R)$. Se satisface que:*

$$dim(Sing(V)) < dim(Reg(V)) = dim(V),$$

*y en particular, se tiene que $Reg(V)$ es un abierto semi-algebraico de $\mathbb{A}^n(R)$ para la topología euclídea y también para la topología de Zariski.*

DEMOSTRACIÓN. Puede consultarse en la Sección 3.3 de [**BCR, 1998**], o deducirse a partir de las proposiciones 3.3.6, 3.3.8 y la Afirmación $(ii)$ de la Proposición 3.3.3. □

Finalmente, tras todas estas consideraciones sobre dimensión de conjuntos semi-algebraicas y regularidad, puede enunciarse el resultado que resuelve afirmativamente el Problema XVII de Hilbert para el caso de un dominio de funciones polinomiales $\mathcal{P}(V)$.

TEOREMA 3.3.10. *Sean $R$ un cuerpo realmente cerrado, $V \subset \mathbb{A}^n(R)$ un conjunto algebraico irreducible de dimensión $d$, y $f \in \mathcal{P}(V)$ una función polinomial. Entonces las siguientes propiedades son equivalentes:*

$(i)$ $f \in \sum \mathcal{K}(V)^2$,
$(ii)$ $f$ *es no negativo en* $V^{(d)}$,
$(iii)$ $f$ *es no negativo en* $Reg(V)$,
$(iv)$ $f$ *es no negativo en algún abierto Zariski contenido en* $V$.

DEMOSTRACIÓN. Comencemos por probar que $(i) \Rightarrow (ii)$. Si $f$ es una suma de cuadrados de $\mathcal{K}(V)$, entonces existen $g_1, \ldots, g_r$ y $h_1, \ldots, h_r$ en $\mathcal{P}(V)$, con los $h_i$ no nulos, tales que:

$$f = (g_1/h_1)^2 + \ldots + (g_r/h_r)^2.$$

Sea $Z \subset V$ el conjunto de puntos en que se anulen todos los $h_i$ simultáneamente, que puede escribirse como $Z = \mathcal{Z}_{R^n}(h_1, \ldots, h_r) \cap V$. Observamos que si $p \in V \setminus Z$, es decir si no se anulan todos los $h_i$, entonces $f(p) \geq 0$, dado que $f$ es una suma de cuadrados. Más aún, la función polinomial que define $f$ es continua para la topología euclídea sobre $\mathbb{A}^n(R)$, y ha de tenerse que $f(p) \geq 0$ para cada $p \in clau_{Euc}(V \setminus Z)$. El conjunto $Z$ es intersección de cerrados Zariski, por lo que será también un cerrado Zariski, y además está estrictamente contenido en $V$, por lo que aplicando la Afirmación $(iii)$ de la Proposición 3.3.3 se tendrá que $dim(Z) < d$. Si tomamos $p \in V$ con $dim(V_p) = d$, entonces ningún entorno semi-algebraico para la topología euclídea puede estar contenido en $Z$ y se sigue que $V^{(d)} \subset clau_{\mathcal{Z}}(V \setminus Z)$. Por esto último, se tiene que $f$ es no negativa en todo $V^{(d)}$.

La implicación $(ii) \Rightarrow (iii)$ se sigue de la Proposición 3.3.8, dado que $Reg(V) \subset V^{(d)}$; mientras que $(iii) \Rightarrow (iv)$ se cumple porque $Reg(V)$ es un abierto Zariski no vacío.

Terminemos viendo que $(iv) \Rightarrow (i)$. Sea $U \subset \mathbb{A}^n(R)$ un abierto Zariski no vacío tal que $f$ sea no negativo en $U$. Sea $Z = V \setminus U = V \cap (\mathbb{A}^n(R) \setminus U)$, que será un cerrado Zariski y por ende son los ceros de una familia finita de polinomios $h_1, \ldots, h_r$. Se define otro polinomio $h = h_1^2 + \ldots + h_r^2$, que satisface $h^{-1}(0) = Z$ y por ello es distinto de 0 como elemento de $\mathcal{P}(V)$. Supongamos que $f \notin \sum \mathcal{K}(V)^2$. Aplicando la Proposición 2.1.10, se tiene la existencia de alguna ordenación $\leq$ de $\mathcal{K}(V)$ para la que $f$ es negativo. Sea $R_1$ una clausura real de $(\mathcal{K}(V), \leq)$. Entonces, por el Lema 2.1.12, se tiene que $\sqrt{-f}$ es un elemento de $R_1$. Se define el morfismo de $R$-álgebras $\phi : (\mathcal{P}(V)_h)[T]/(fT^2+1) \to R_1$ tal que $\phi(g + (fT^2+1)) = g$ para cada $g \in \mathcal{P}(V)_h$ y $\phi(T) = 1/\sqrt{-f}$. Aplicando ahora el Teorema del Homomorfismo de Artin-Lang

1.2.10, se tendrá otro morfismo de $R$-álgebras $\psi : (\mathcal{P}(V)_h)[T]/(fT^2+1) \to R$. Se define el punto $x = (\psi(X_1), \ldots, \psi(X_n))$, el cual cumple que $h(0) \neq 0$ y entonces $x \in U$. Se cumple que:

$$\psi(f) = f(\psi(X_1), \ldots, \psi(X_n)) = f(x) < 0 = \psi(0),$$

de lo que se deduce que si $f \notin \sum \mathcal{K}(V)^2$, no se tendría que $f$ sea no negativa en el abierto $U$, y en conclusión, ha de cumplirse que $f$ sea una suma de cuadrados de $\mathcal{K}(V)$. □

## 3.4. Problema de Hilbert Equivariante.

En esta sección se muestra en forma de resumen la Versión Equivariante del Problema XVII de Hilbert. Se escoge hacerlo de manera abreviada, sin pruebas, dado que excede el tamaño permitido para este TFG; aunque puede consultarse todas ellas en [**BCR, 1998**] o en las fuentes que allí se citan. Esta versión del problema consiste en que todo polinomio simétrico $f \in R[X_1, \ldots, X_n]$ donde $R$ es un cuerpo realmente cerrado y no negativo en $\mathbb{A}^n(R)$ puede escribirse en la forma:

$$f = \sum_{i=1}^{r} s_i \delta_i,$$

siendo cada $s_i$ una suma de cuadrados de polinomios simétricos y los $\delta_1, \ldots, \delta_r$ unos polinomios simétricos no negativos en $\mathbb{A}^n(R)$ que no dependen del polinomio $f$ escogido. La prueba se basa en el hecho de que el conjunto de los $(a_1, \ldots, a_n) \in \mathbb{A}^n(R)$ tales que el polinomio siguiente:

$$X_1^n - a_1 X_1^{n-1} + \ldots + (-1)^n a_n,$$

escinde completamente en $R$ es un conjunto cerrado básico salvo por un semi-algebraico de dimensión inferior a $n$. Primero, es necesario definir a un conjunto cerrado básico.

Definición 27. **(Conjunto Cerrado Básico y Conjunto Abierto Básico)** *Sea $R$ un cuerpo realmente cerrado y sea $V \subset \mathbb{A}^n(R)$ un conjunto algebraico. Se dice conjunto cerrado básico de $V$ a todo subconjunto de la forma:*

$$\{x \in V : f_1(x) \geq 0, \ldots, f_r(x) \geq 0\},$$

*donde $f_1, \ldots, f_r$ son polinomios de $\mathcal{P}(V)$. Se dice conjunto abierto básico de $V$ a cada subconjunto del tipo:*

$$\{x \in V : f_1(x) > 0, \ldots, f_r(x) > 0\},$$

*con $f_1, \ldots, f_r \in \mathcal{P}(V)$.*

Observación 3.4.1. Todo conjunto algebraico $V$ de $\mathbb{A}^n(R)$ es cerrado básico, pues si $V$ es el conjunto de ceros del ideal $(f_1, \ldots, f_r)$, entonces:

$$V = \{x \in \mathbb{A}^n(R) : f_1(x) \geq 0, -f_1(x) \geq 0, \ldots, f_r(x) \geq 0, -f_r(x) \geq 0\}.$$

Además, se observa que su complementario es de la forma:

$$\mathbb{A}^n(R) \setminus V = \{x \in \mathbb{A}^n(R) : f_1^2(x) > 0, \ldots, f_r^2(x) > 0\},$$

de modo que los abiertos Zariski de $\mathbb{A}^n(R)$ son conjuntos abiertos básicos en $\mathbb{A}^n(R)$.

Nótese que los conjuntos cerrados básicos y los conjuntos abiertos básicos son clases de conjuntos semi-algebraicos, y de hecho se ha definido a los conjuntos semi-algebraicos como unión finita de cerrados básicos.[3] Ahora, se define una relación de equivalencia entre los conjuntos semi-algebraicos contenidos en alguna variedad algebraica irreducible que distingue clases de semi-algebraicos que sean iguales salvo por un conjunto de dimensión inferior a la de la variedad.[4]

[3] En [**Recio, 1978**] se prueba que los conjuntos semi-algebraicos cerrados para la topología euclídea sobre $\mathbb{A}^n(R)$ son de hecho uniones finitas de conjuntos cerrados básicos, hecho que parece trivial por nuestra presentación de los semi-algebraicos, pero que no lo es en un contexto en el que llamamos conjunto prealgebraico a un conjunto dado por la Definición 7 y los semi-algebraicos eran uniones finitas de intersecciones finitas de condiciones de la forma $f_i > 0$ y $g_j = 0$.

[4] Esta noción fue introducida por L. M. Pardo en su Tesis Doctoral titulada *"Aspectos computacionales en la variación de las raíces de un polinomio: Curvas Algebraicas Reales y Componentes Analíticas"* y con fecha de 1987.

Definición 28. **(Conjunto Genéricamente Básico)**
*Sea $R$ un cuerpo realmente cerrado y sea $V$ un conjunto algebraico irreducible de $\mathbb{A}^n(R)$. Un par de conjuntos $S$ y $T$ semi-algebraicos contenidos en $V$ se dicen genéricamente iguales en $V$ cuando $dim(S\Delta T) < dim(V)$, siendo $\Delta$ el operador diferencia simétrica de conjuntos. Un conjunto $S \subset V$ semi-algebraico se dice genéricamente básico en $V$ si es genéricamente igual con algún conjunto cerrado básico de $V$.*

Observación 3.4.2. La relación de igualdad genérica para subconjuntos semi-algebraicos de una variedad algebraica irreducible es de equivalencia. Además, se tiene que todo conjunto semi-algebraico de dimensión estrictamente menor que la variedad que lo contiene, es genéricamente igual al vacío por la relación definida sobre dicha variedad.

Se tiene el siguiente resultado que caracteriza a los conjuntos genéricamente básicos.

Teorema 3.4.3. *Sea $R$ un cuerpo realmente cerrado y sea $V$ un conjunto algebraico irreducible de $\mathbb{A}^n(R)$. Sea $S \subset V$ un conjunto semi-algebraico. Entonces, son equivalentes:*

(*i*) *$S$ es genéricamente básico en $V$,*
(*ii*) *existe una familia $f_1, \ldots, f_r \in \mathcal{P}(V)$ de funciones polinomiales no negativas en $S$ tales que, para cada $f \in \mathcal{P}(V)$ no negativo en $S$, existen $g_1, \ldots, g_r \in \sum \mathcal{K}(V)^2$ satisfaciendo:*

$$f = \sum_{i=1}^{r} g_i f_i.$$

Demostración. Vease el Teorema 6.2.3 de [**BCR, 1998**]. □

Este resultado se utilizará en la forma siguiente, adecuada al caso del anillo de polinomios simétricos que es una sub-$R$-álgebra del anillo de polinomios $R[X_1, \ldots, X_n]$.

Corolario 3.4.4. *Sea $R$ un cuerpo realmente cerrado y sea $V$ un conjunto algebraico irreducible de $\mathbb{A}^n(R)$. Sea $A$ una $R$-álgebra que también es subanillo de $\mathcal{P}(V)$ y sea $Frac(A)$ su cuerpo de fracciones. Sea $\alpha_1, \ldots, \alpha_r \in \mathcal{P}(V)$ una familia de generadores de $A$ como $R$-álgebra, y se define la aplicación:*

$$\begin{aligned} \alpha : V &\longrightarrow \mathbb{A}^n(R) \\ p &\longmapsto (ev_p(\alpha_1), \ldots, ev_p(\alpha_r)). \end{aligned}$$

*Se define también $Z$ como la clausura Zariski de $\alpha(V)$ respecto de la topología de Zariski sobre $\mathbb{A}^n(R)$. Entonces, se tienen las siguientes propiedades equivalentes:*

(*i*) *El conjunto $\alpha(V)$ es genéricamente básico en $Z$.*
(*ii*) *Existe una familia de funciones polinomiales $f_1, \ldots, f_r \in A$ no negativas en $V$ tales que cada $f \in A$ no negativo en $V$ es de la forma:*

$$f = \sum_{i=1}^{r} g_i f_i,$$

*con $g_1, \ldots, g_r$ pertenecientes a $\sum Frac(A)^2$.*

Demostración. Puede consultarse el Corolario 6.2.4 de [**BCR, 1998**]. □

Ahora, comencemos a tratar el caso particular de los polinomios simétricos. Sea $R$ un cuerpo realmente cerrado. Un polinomio $f \in R[X_1, \ldots, X_n]$ se dice simétrico si, ante cualquier permutación $\tau$ del conjunto de las variables $\{X_1, \ldots, X_n\}$, se cumple que:

$$f(X_1, \ldots, X_n) = f(\tau(X_1), \ldots, \tau(X_n)).$$

Para este conjunto de variables, se definen los siguientes polinomios simétricos:

$$\sigma_k = \sum_{1 \leq j_1 \leq \ldots \leq j_k \leq n} X_{j_1} \cdot \ldots \cdot X_{j_k}, \text{ para cada } k = 1, \ldots, n,$$

que se conocen como los polinomios simétricos elementales. Esta familia de polinomios es algebraicamente independiente sobre $R$, y también ocurre que todo polinomio simétrico $f$ de $R[X_1, \ldots, X_n]$ puede escribirse de manera única en función de los polinomios simétricos elementales como $f = \sum_{i=1}^{n} a_i \sigma_i$ para algunos $a_1, \ldots, a_n \in R$. Es decir, el anillo de los polinomios

simétricos es la $R$-álgebra finita $R[\sigma_1, \ldots, \sigma_n]$ generada por los polinomios simétricos elementales, y además es un subanillo del anillo de polinomios $R[X_1, \ldots, X_n]$. Nótese que todas estas observaciones llevan a que pueda usarse el Corolario 3.4.4 para el caso de $\mathbb{A}^n(R)$ y la $R$-álgebra de polinomios simétricos en $n$ variables y con coeficientes en $R$. En estos términos, se denotaría por $\sigma$ a la aplicación definida por $\sigma(p) = (ev_p(\sigma_1), \ldots, ev_p(\sigma_n))$ para cada $p \in \mathbb{A}^n(R)$. Si recordamos la introducción de esta sección, nos fijábamos en el conjunto de los $(a_1, \ldots, a_n) \in \mathbb{A}^n(R)$ para los que el polinomio $f(X_1) = X_1^n - a_1 X_1^{n-1} + \ldots + (-1)^n a_n$ escinde completamente en $R$. Precisamente, si aplicamos las Fórmulas de Cardano-Vieta sobre este polinomio mónico, encontraremos que $ev_x(\sigma_j) = a_j$, y en ese caso $\sigma(\mathbb{A}^n(R))$ será el conjunto de las posibles tuplas $(a_1, \ldots, a_n)$ de coeficientes de polinomios de la forma $f(X_1)$ que escinden en $R$. En definitiva, para poder utilizar el Corolario 3.4.4 necesitaremos probar que el conjunto $\sigma(\mathbb{A}^n(R))$ sea genéricamente básico en $\mathbb{A}^n(R)$.

A continuación, introducimos un método sobre el conteo de raíces reales que se atribuye a Hermite y a Sylvester. Con este, podremos ver no solo que $\sigma(\mathbb{A}^n(R))$ es genéricamente básico en $\mathbb{A}^n(R)$, sino también dar de forma explícita algún conjunto cerrado básico que sea genéricamente igual a $\sigma(\mathbb{A}^n(R))$; e incluso llegar a dar $\sigma(\mathbb{A}^n(R))$ como un conjunto cerrado básico. Consideramos el polinomio mónico de $R[X_1]$:

$$f(X_1) = X_1^n - a_1 X_1^{n-1} + \ldots + (-1)^n a_n.$$

Supongamos que tiene todas sus raíces en $R$ y que estas son $x_1, \ldots, x_n$. Dado un $k \in \mathbb{N}$, se define la $k$-ésima suma de Newton de las raíces de $f$ como:

$$N_k = \sum_{i=1}^{n} x_i^k,$$

que es un polinomio simétrico en las variables $x_1, \ldots, x_n$. Las sumas de Newton se pueden transformar, primero, en la evaluación en el punto $x = (x_1, \ldots, x_n)$ de los polinomios simétricos elementales utilizando las Identidades de Newton-Girard, y luego, en los coeficientes $a_1, \ldots, a_n$ por medio de las Fórmulas de Cardano-Vieta. De este modo, se tiene una transformación lineal de las coordenadas $x_1, \ldots, x_n$ a $a_1, \ldots, a_n$, y con esto se define la matriz:

$$\mathcal{H}(a_1, \ldots, a_n) = (N_{(i-1)+(j-1)})_{\substack{i=1,\ldots,n \\ j=1,\ldots,n}},$$

que es una matriz simétrica y por ello tiene asociada una forma cuadrática real $Q$, es decir, un polinomio homogéneo de grado 2 de $R[X_1, \ldots, X_n]$ donde $R$ es algún cuerpo realmente cerrado. Dicha forma cuadrática satisface la ecuación matricial:

$$Q(X_1, \ldots, X_n) = X^T \mathcal{H}(a_1, \ldots, a_n) X,$$

donde $X$ denota al vector columna $(X_1, \ldots, X_n)$. Esta relación entre formas cuadráticas de $R[X_1, \ldots, X_n]$ y matrices simétricas de $\mathcal{M}_{n\times n}(R)$ es biyectiva. Esto permite definir una relación de equivalencia en las formas cuadráticas a partir de la relación de congruencia de matrices. Es decir, un par de formas cuadráticas se dicen equivalentes si y solo si sus matrices asociadas son congruentes. Para el caso de formas cuadráticas reales, ocurre que estas clases de equivalencia se identifican de manera biunívoca dando el rango y la signatura de alguna de sus formas cuadráticas. Se define el rango de una forma cuadrática $Q \in R[X_1, \ldots, X_n]$ como el rango de la matriz simétrica asociada y se denota por $rank(Q)$. Para una forma cuadrática real $Q \in R[X_1, \ldots, X_n]$, se tendrá siempre otra forma cuadrática equivalente a $Q$ cuya matriz asociada sea la matriz diagonal $diag(1, \ldots, 1, -1, \ldots, -1, 0, \ldots, 0)$. En tal caso, se define la signatura de la forma $Q$ como el número de 1 menos el número de $-1$ de la matriz $diag(1, \ldots, 1, -1, \ldots, -1, 0, \ldots, 0)$ asociada a $Q$ y se denota por $sign(Q)$. Además, la suma del número de 1 y del número de $-1$ es $rank(Q)$. La buena definición de la signatura y el hecho de que rango y signatura caractericen a las clases de formas cuadráticas reales equivalentes se debe al conocido Teorema de Inercia de Sylvester, que puede verse en el Apéndice F. Con esta terminología ya puede entenderse el siguiente resultado, que es la base del citado método de conteo de raíces reales.

PROPOSICIÓN 3.4.5. *Sea el polinomio mónico univariado $f(X_1) = X_1^n - a_1 X_1^{n-1} + \ldots + (-1)^n a_n$ con coeficientes en un cuerpo $R$ realmente cerrado. Entonces:*

(*i*) *La signatura de la forma cuadrática cuya matriz asociada es $\mathcal{H}(a_1, \ldots, a_n)$ es igual al número de raíces distintas de $f$ en $R$.*

(*ii*) *El rango de la matriz* $\mathcal{H}(a_1,\ldots,a_n)$ *es igual al número de raíces distintas de* $f$ *en la clausura algebraica de* $R$.

DEMOSTRACIÓN. Puede verse la Proposición 6.2.6 de [**BCR, 1998**]. □

En realidad, no estamos interesados en el conteo de raíces, sino en caracterizar a los elementos de $\sigma(\mathbb{A}^n(R))$. Se dice que una forma cuadrática real $Q \in R[X_1,\ldots,X_n]$ es semidefinida positiva cuando $Q(x) \geq 0$ para todo $x \in \mathbb{A}^n(R)$, y se caracterizan por la condición $rank(Q) = sign(Q)$. El resultado precedente permite probar la caracterización siguiente del conjunto $\sigma(\mathbb{A}^n(R))$.

COROLARIO 3.4.6. *Sea* $R$ *un cuerpo realmente cerrado. Un elemento* $(a_1,\ldots,a_n) \in \mathbb{A}^n(R)$ *pertenece a* $\sigma(R^n)$ *si y solamente si* $\mathcal{H}(a_1,\ldots,a_n)$ *es la matriz asociada a una forma cuadrática real semidefinida positiva.*

Existe otra caracterización de las formas cuadráticas reales semidefinidas positivas que se basa en los menores principales de la matriz asociada. Si $Q \in R[X_1,\ldots,X_n]$ es una forma cuadrática real y denotamos por $\Delta_1,\ldots,\Delta_n$ a los menores principales de la matriz simétrica asociada a $Q$, entonces $Q$ será semidefinida positiva si y solamente si $\Delta_1 \geq 0,\ldots,\Delta_n \geq 0$. Este hecho aplicado a cada matriz $\mathcal{H}(a_1,\ldots,a_n)$, y considerando que $\Delta_1 = n$ en este caso, lleva a probar el lema siguiente.

LEMA 3.4.7. *Sea* $R$ *un cuerpo realmente cerrado. Sea* $\mathcal{H}(a_1,\ldots,a_n)$ *la matriz definida previamente a partir de las sumas de Newton y para cada* $(a_1,\ldots,a_n) \in \mathbb{A}^n(R)$, *y denotamos por* $\Delta_1(a_1,\ldots,a_n),\ldots,\Delta_n(a_1,\ldots,a_n)$. *El conjunto* $\sigma(\mathbb{A}^n(R))$ *es genéricamente igual al conjunto cerrado básico de* $\mathbb{A}^n(R)$ *siguiente:*

$$\{(a_1,\ldots,a_n) \in \mathbb{A}^n(R) : \Delta_2(a_1,\ldots,a_n) \geq 0,\ldots,\Delta_n(a_1,\ldots,a_n) \geq 0\}.$$

DEMOSTRACIÓN. Consúltese el Lema 6.2.8 de [**BCR, 1998**]. □

Con esto ya puede probarse la Versión Equivariante del Problema XVII de Hilbert:

TEOREMA 3.4.8. **(Solución al Problema XVII de Hilbert Equivariante)**
*Sea* $R$ *un cuerpo realmente cerrado. Sea* $f$ *un polinomio simétrico de* $R[X_1,\ldots,X_n]$. *Si* $f$ *es no negativo en* $\mathbb{A}^n(R)$, *entonces puede escribirse como:*

$$f = \sum_{i=1}^{r} s_i\delta_i,$$

*para algunas* $s_1,\ldots,s_r$ *sumas de cuadrados de funciones racionales simétricas y siendo* $\delta_i$ *productos de la forma* $\prod_{j=2}^{n}(\Delta_j(\sigma_1,\ldots,\sigma_n))^{\epsilon_{i,j}}$ *con cada* $\epsilon_{i,j}$ *igual a* 0 *o a* 1 *y siendo* $\Delta_2,\ldots,\Delta_n$ *los menores principales de la matriz* $\mathcal{H}(\sigma_1,\ldots,\sigma_n)$ *definida a partir de las sumas de Newton de los polinomios simétricos elementales.*

DEMOSTRACIÓN. Por el Lema 3.4.7, sabemos que el conjunto $\sigma(\mathbb{A}^n(R))$ es genéricamente igual a un conjunto cerrado básico de $\mathbb{A}^n(R)$, es decir, $\sigma(\mathbb{A}^n(R))$ es genéricamente básico. Entonces, puede aplicarse el Corolario 3.4.4 tomando $V = \emptyset$ y a los polinomios simétricos elementales como generadores de la $R$-álgebra que es el anillo de los polinomios simétricos, de modo que el resultado queda probado. □

OBSERVACIÓN 3.4.9. El conjunto $\sigma(\mathbb{A}^n(R))$ puede de hecho escribirse como un conjunto cerrado básico. Si llamamos $D_1,\ldots,D_{2^n-1}$ a los menores simétricos de la matriz $\mathcal{H}(\sigma_1,\ldots,\sigma_n)$, entonces $\sigma(\mathbb{A}^n(R))$ son los elementos $x \in \mathbb{A}^n(R)$ que cumplen las desigualdades $D_i(x) \geq 0$ para cada $i = 1,\ldots,2^n-1$.

## 3.5. Problema de Hilbert Cuantitativo.

Para finalizar el capítulo, se discute la Versión Cualitativa del Problema XVII de Hilbert, también de manera resumida por las limitaciones de espacio. Esta versión del problema ataja la cuestión del número mínimo de cuadrados que se necesita para representar a cualquier suma de cuadrados. Actualmente, se trata de un problema abierto y con mucha literatura detrás. Aquí solo se presentará con cierto detalle una cota inferior para el caso de cuerpos formalmente reales, basada en la Teoría de Formas Cuadráticas, y una cota superior para cuerpos realmente cerrados basada en las formas multiplicativas de Pfister. Al terminar, trataremos de comentar

los avances posteriores más significativos. Estos son esencialmente cotas o ejemplos para un número de variables muy bajo, ya que, insistimos, el problema sigue abierto. Comencemos por definir la cantidad mínima necesaria de cuadrados para representar a cualquier cuadrado para un anillo en general.

DEFINICIÓN 29. **(Número de Pitágoras)**
*Sea $A$ un anillo conmutativo. Se dice número de Pitágoras de $A$, y se denota por $p(A)$, al mínimo $r \in \mathbb{N}$ tal que todo elemento de $\sum A^2$ tiene una representación en $A$ como suma de $r$ cuadrados o menos. Si no existe, se define $p(A) = +\infty$.*

Veamos algunos ejemplos que ya conocemos. Se observa que el Nichnegativstellensatz ayuda a resolver esta cuestión para el caso de anillos de polinomios.

EJEMPLO 3.5.1. *Veamos ejemplos de algunos números de Pitágoras.*

(I) *Utilizando el Teorema de Lagrange de los Cuatro Cuadrados 2.1.9, se concluye que $p(\mathbb{Z}) = p(\mathbb{Q}) = 4$.*
(II) *Si $R$ es un cuerpo realmente cerrado, por el Lema 2.1.12 se sabe que $p(R) = 1$.*
(III) *Aplicando el Nichnegativstellensatz como en el Ejemplo 2.4.5, pueden encontrarse los números de Pitágoras $p(R(X)) = 2$ y $p(R(X,Y)) = 4$.*
(IV) *Puede verse en [CDLR, 1982] que si $F$ es un cuerpo formalmente real y dado $n \geq 2$, se tiene que $p(F[X_1, \ldots, X_n]) = +\infty$.*

Veamos ahora una cota inferior al número de Pitágoras para anillos de polinomios $F[X_1, \ldots, X_n]$ con $F$ un cuerpo formalmente real. Para ello, añadimos algunas ideas de la Teoría de las Formas Cuadráticas a lo que ya se introdujeron en la sección anterior, y que puede verse con más detalle en el Apéndice F. Dados un cuerpo $K$ con característica distinta de 2 y una forma cuadrática $Q \in K[X_1, \ldots, X_n]$, ya dijimos que se tiene una única matriz simétrica asociada a la forma $Q$ y que denotaremos por $M_Q$. Esta matriz es la que satisface la igualdad $Q(x) = x^T M_Q x$. Ocurre que la matriz $M_Q$ también define una forma bilineal simétrica $\phi_Q$ sobre el $K$-espacio vectorial $K^n$. De hecho, la relación entre las formas bilineales simétricas de $K^n$ y las formas cuadráticas de $K[X_1, \ldots, X_n]$ es biyectiva. Se puede dar la siguiente expresión explícita de la forma bilineal simétrica $\phi_Q$ asociada a una forma cuadrática $Q$:

$$\phi_Q(x, y) = \frac{1}{2}(Q(x + y) - Q(x - y)),$$

dados $x, y \in K^n$. Una forma cuadrática se dirá regular si el determinante de la matriz asociada es no nulo, y se dirá singular en caso contrario. Se introduce la operación suma ortogonal de un par de formas cuadráticas $Q_1 \in K[X_1, \ldots, X_n]$ y $Q_2 \in K[X_1, \ldots, X_m]$ como sigue:

$$Q_1 \perp Q_2(x \oplus y) = Q_1(x) + Q_2(y),$$

para cada $x \in K^n$ y cada $y \in K^m$. Esta operación permite expresar las formas cuadráticas cuya matriz asociada sea diagonal de la manera siguiente. Si se denota por $\langle u \rangle$ a la forma $uX_1^2$ de $K[X_1]$, entonces una forma $Q(X_1, \ldots, X_n) = u_1X_1^2 + \ldots + u_nX_n^2$ de $K[X_1, \ldots, X_n]$ vendrá expresada por $\langle u_1 \rangle \perp \ldots \perp \langle u_n \rangle$, y se denotará por $\langle u_1, \ldots, u_n \rangle$. Ahora se define la representación de un elemento $u \in K$ no nulo por una forma cuadrática. Los elementos no nulos de $K$ coinciden con el conjunto $K^*$ de las unidades de $K$.

DEFINICIÓN 30. **(Representación de Unidades por una Forma Cuadrática)**
*Sea $K$ un cuerpo con característica distinta de 2 y sea $Q \in K[X_1, \ldots, X_n]$ una forma cuadrática. Sea $K_1$ una $K$-álgebra y sea $u$ una unidad de $K_1$. Se dice que $Q$ representa a $u$ sobre $K_1$ cuando existe $x \in K_1^n$ tal que $Q(x) = u$. Se denota por $D_{K_1}(Q)$ al conjunto de unidades de $K_1$ que vienen representadas por $Q$ sobre $K_1$. La forma $Q$ se dirá universal sobre $K_1$ si $D_{K_1}(Q)$ contiene a todas las unidades de $K_1$.*

La idea de representación de una unidad $u \in K^*$ sirve, por ejemplo, para determinar si puede escribirse como una suma de $n$ cuadrados. Si consideramos la forma cuadrática $Q = \langle 1, \ldots, 1 \rangle$ perteneciente a $K[X_1, \ldots, X_n]$, se tendrá que $D_K(Q)$ es el conjunto de las sumas de $n$ cuadrados de elementos de $K$, o también puede considerarse el conjunto $D_{K(Y_1)}(Q)$ de sumas de $n$ cuadrados de elementos de $K(Y_1)$. La representación de unidades está relacionada con la propiedad de isotropía que definimos a continuación.

DEFINICIÓN 31. **(Isotropía y Anisotropía de una Forma Cuadrática)**
*Sea $K$ un cuerpo con característica distinta de 2. Una forma cuadrática $Q \in K[X_1, \ldots, X_n]$ se dice isótropa si existe algún $x \in K^n$ no nulo tal que $Q(x) = 0$. Si esto se cumple para todo $x \in K^n$ no nulo, entonces $Q$ se dice totalmente isótropa. En caso de no ser isótropa, $Q$ se dice anisótropa.*

La propiedad de isotropía de una forma cuadrática viene dada por dos vías diferentes. Consideremos los siguientes ejemplos de formas isótropas.

EJEMPLO 3.5.2. *Dado un cuerpo $K$ con característica distinta de 2, se definen las siguientes formas cuadráticas isótropas:*

(I) *$\langle 0 \rangle$ o cualquier suma directa de esta varias veces es una forma totalmente isótropa.*
(II) *El llamado plano hiperbólico $\langle 1, -1 \rangle$ es una forma isótropa y regular. Además, es universal por ser equivalente con la forma $X_1 X_2$.*
(III) *Se dice forma hiperbólica a cualquier suma directa de planos hiperbólicos, y también son formas isótropas regulares y universales.*
(IV) *Una forma $Q \in K[X_1, \ldots, X_n]$ será isótropa únicamente si es equivalente a $\langle 0 \rangle \perp Q'$ con $Q' \in K[X_1, \ldots, X_{n-1}]$ o a $\langle 1, -1 \rangle \perp Q''$ donde $Q'' \in K[X_1, \ldots, X_{n-2}]$.*

El Apartado (IV) del ejemplo precedente es un corolario de la descomposición de Witt, que puede verse en el Apéndice F. Esta consiste en que cualquier forma puede descomponerse en una suma directa de una forma totalmente isótropa $\langle 0, \ldots, 0 \rangle$, una forma hiperbólica y otra forma anisótropa, y la descomposición es única salvo equivalencia de las formas. Si la forma en cuestión es regular, por ejemplo, entonces no tendría componente totalmente isótropa, pero el caso es que puede descomponerse a lo sumo en 3 de estas componentes elementales. A continuación vemos un par de propiedades para formas regulares que no han de sorprendernos mucho después del ejemplo anterior. En particular se comprueba que toda forma regular e isótropa es universal.

TEOREMA 3.5.3. *Sea $K$ un cuerpo con característica distinta de 2 y sea $Q \in K[X_1, \ldots, X_n]$ una forma cuadrática regular. Se satisface las siguientes propiedades:*

*(i) Si $Q$ es isótropa, entonces es equivalente a la forma $\langle 1, -1, a_3, \ldots, a_n \rangle$ para algunos $a_3, \ldots, a_n \in K$ no nulos.*
*(ii) Si $Q$ es isótropa, entonces es universal.*

DEMOSTRACIÓN. Véase la prueba del Teorema 3.4 del Capítulo 1 de [**Lam, 1973**]. □

Para dar la cota inferior deseada de $p(F[X_1, \ldots, X_n])$, se utilizará unos resultados sobre representación de unidades conocidos como Teoremas de Representación. El primero de ellos puede probarse a partir del resultado precedente y queda escrito a continuación.

COROLARIO 3.5.4. **(Primer Teorema de Representación)**
*Sean $K$ un cuerpo con característica distinta de 2, $Q \in K[X_1, \ldots, X_n]$ una forma cuadrática regular y $u \in K^*$ una unidad. Entonces, $u \in D_K(Q)$ si y solamente si $Q$ es equivalente a otra forma $\langle u \rangle \perp Q'$ donde $Q'$ es a su vez una forma cuadrática de $K[X_1, \ldots, X_{n-1}]$.*

DEMOSTRACIÓN. Véase el Corolario 3.5 del Capítulo 1 de [**Lam, 1973**]. □

Para dar el Segundo Teorema de Representación, es necesario introducir antes el siguiente resultado conocido como el Teorema de Cassels-Pfister.

TEOREMA 3.5.5. **(de Cassels-Pfister)**
*Sea $K$ un cuerpo con característica distinta de 2 y sea $Q \in K[X_1, \ldots, X_n]$ una forma cuadrática. Sea un polinomio no nulo $f \in K[Y_1]$ representado por la forma $Q$ sobre el cuerpo de funciones racionales $K(Y_1)$, es decir, $f \in D_{K(Y_1)}(Q) \cap K[Y_1]$. Entonces, se tiene que:*

*(i) El polinomio $f$ está representado por la forma $Q$ sobre $K[Y_1]$, es decir, $f \in D_{K[Y_1]}(Q)$.*
*(ii) Si $a \in K$ no es una raíz de $f$, entonces $f(a) \in D_K(Q)$.*

DEMOSTRACIÓN. Puede encontrarse una prueba del resultado completo en el Teorema 1.3 del Capítulo 9 de [**Lam, 1973**], pero también puede seguirse la prueba de la Afirmación $(i)$ del Teorema 6.4.5 de [**BCR, 1998**]. □

En realidad, nos interesa únicamente la Afirmación $(i)$ del resultado precedente para seguir la prueba de [**BCR, 1998**]. El siguiente resultado es la versión que se muestra en [**BCR, 1998**] del llamado Segundo Teorema de Representación, que puede enunciarse de forma alternativa como el Teorema 2.1 del Capítulo 9 de [**Lam, 1973**].

PROPOSICIÓN 3.5.6. **(Segundo Teorema de Representación)**
*Sea $K$ un cuerpo con característica distinta de 2 y sea $Q \in K[X_1, \ldots, X_n]$ una forma cuadrática regular con $n > 1$. Sea $a \in K$ un elemento cualquiera y sean $b_1, \ldots, b_n \in K^*$ las unidades tales que $Q = \langle b_1, \ldots, b_n \rangle$. Entonces, son equivalentes las siguientes dos propiedades:*

*(i) la forma $Q$ representa a $b_1 Y_1^2 + a$ sobre $K(Y_1)$, es decir, $b_1 Y_1^2 + a \in D_{K(Y_1)}(Q)$,*
*(ii) o bien $a \in D_K(\langle b_2, \ldots, b_n \rangle)$, o bien $Q$ es isótropa.*

DEMOSTRACIÓN. Consúltese la Proposición 6.4.7 de [**BCR, 1998**]. □

En vista de los dos resultados precedentes, puede hacerse un argumento de inducción en el número de variables $n$ del anillo $F[X_1, \ldots, X_n]$ para ver la propiedad siguiente. Esencialmente basta con tomar $b_1 = \ldots = b_n = 1$ en la Proposición 3.5.6 y darse cuenta de que si $Y_1^2 + a$ se una suma de $n > 1$ cuadrados en $F[Y_1]$ entonces, o bien $-1$ es una suma de $n - 1$ cuadrados en $F$, o bien $a$ es suma de $n - 1$ cuadrados de $F$. Por esto es que se pide que $F$ sea un cuerpo formalmente real.

COROLARIO 3.5.7. *Sea $F$ un cuerpo formalmente real. Entonces:*

*(i) el polinomio $1+X_1^2+\ldots+X_n^2$ es una suma de cuadrados de elementos de $F(X_1, \ldots, X_n)$ que no puede expresarse como suma de $n$ cuadrados,*
*(ii) $p(F(X_1, \ldots, X_n)) \geq p(F) + n$.*

DEMOSTRACIÓN. Puede consultarse el Corolario 6.4.8 de [**BCR, 1998**]. □

De la Afirmación $(ii)$ de este resultado y teniendo en cuenta que todo elemento positivo de un cuerpo realmente cerrado es un cuadrado, se sigue que si $F = R$ es un cuerpo realmente cerrado, entonces $p(R(X_1, \ldots, X_n)) \geq n+1$. Pasemos a ver una cota superior para el número de Pitágoras de $R(X_1, \ldots, X_n)$. Para ello se expone algunos aspectos de las formas cuadráticas multiplicativas de Pfister, de los que se sirve [**BCR, 1998**] para dar una prueba que no reproduciremos aquí. Comencemos por definir otra operación de formas cuadráticas, el producto tensorial.

Sean $K$ un cuerpo con característica distinta de 2 y $Q_1 \in K[X_1, \ldots, X_n]$, $Q_2 \in K[Y_1, \ldots, Y_m]$ un par de formas cuadráticas. Entonces, se define la forma producto tensorial $Q = Q_1 \otimes Q_2$ como aquella que satisface la ecuación:

$$Q(x \otimes y) = Q_1(x)Q_2(y),$$

para todo $x \in K^n$ y todo $y \in K^m$. Nótese que la forma cuadrática $Q$ pertenece al anillo $K[X_1, \ldots, X_{nm}]$. En caso de utilizarse la notación $Q_1 = \langle a_1, \ldots, a_n \rangle$, $Q_2 = \langle b_1, \ldots, b_m \rangle$, se tendrá que el producto tensorial de formas es:

$$Q = Q_1 \otimes Q_2 = \langle a_1 b_1, \ldots, a_1 b_m, a_2 b_1, \ldots, a_n b_m \rangle.$$

Ahora pasamos a definir a las formas de Pfister haciendo uso de este producto tensorial.

DEFINICIÓN 32. **(Forma de Pfister)**
*Sea $K$ un cuerpo con característica distinta de 2. Una forma cuadrática $Q \in K[X_1, \ldots, X_{2^n}]$ se dice de Pfister cuando existen unas unidades $u_1, \ldots, u_n \in K^*$ tales que:*

$$Q = \langle 1, u_1 \rangle \otimes \ldots \otimes \langle 1, u_n \rangle.$$

*De forma abreviada se escribirá $Q = \langle\langle u_1, \ldots, u_n \rangle\rangle$. También se define la forma asociada a $Q$:*

$$Q' = \langle u_1, \ldots, u_n, u_1 u_2, \ldots, u_1 \cdot \cdots \cdot u_n \rangle,$$

*que se dice forma o subforma pura de la forma de Pfister $Q$.*

OBSERVACIÓN 3.5.8. Siguiendo la notación de la definición previa, se tiene que la forma pura de Pfister $Q'$ es exactamente la forma $Q$ si se desarrolla iterativamente como sigue:

$$\langle 1, u_1 \rangle \otimes \langle 1, u_2 \rangle = \langle 1, u_1, u_2, u_1 u_2 \rangle,$$

pero quitando la componente $\langle 1 \rangle$ al final del proceso. Es decir, que $Q = Q' \perp \langle 1 \rangle$.

Las formas de Pfister tienen la propiedad de ser formas multiplicativas. Que una forma cuadrática $Q \in K[X_1, \ldots, X_n]$ sea multiplicativa significa que para todo $x \in K^n$ tal que $Q(x) \neq 0$, la forma $Q$ es equivalente a $Q(X)Q$. Puede probarse que las formas de Pfister son multiplicativas. La prueba que se sigue en [**BCR, 1998**] utiliza el siguiente lema.

LEMA 3.5.9. *Sea $K$ un cuerpo con característica distinta de 2 y sea la forma cuadrática definida como $Q = \langle a, b\rangle$ a partir de $a, b \in K$. Si una unidad $u \in K^*$ viene representada por $Q$ sobre $K$, esto es si $u \in D_K(Q)$, entonces la forma cuadrática $Q$ será equivalente a $u\langle 1, ab\rangle$.*

DEMOSTRACIÓN. Puede seguirse la prueba en el Lema 6.4.9 de [**BCR, 1998**]. □

TEOREMA 3.5.10. *Toda forma de Pfister es multiplicativa.*

DEMOSTRACIÓN. La demostración se encuentra en el Teorema 6.4.11 de [**BCR, 1998**]. □

Una forma de Pfister definida sobre un cuerpo $K$ tiene asociado un subgrupo multiplicativo de $K^*$, que es el conjunto de unidades de $K$ representadas por dicha forma de Pfister.

COROLARIO 3.5.11. *Sea $K$ un cuerpo con característica distinta de 2 y sea $Q = \langle\langle a_1, \ldots, a_n\rangle\rangle$ una forma de Pfister definida por $a_1, \ldots, a_n \in K$. Entonces, $D_K(Q)$ es un subgrupo multiplicativo de $(K^*, \cdot)$ y se denota por $G_Q$.*

DEMOSTRACIÓN. La prueba se encuentra en el Corolario 6.4.12 de [**BCR, 1998**]. □

Este resultado puede usarse para deducir propiedades de las sumas de $2^n$ cuadrados sin más que considerar la forma de Pfister $Q = \langle\langle 1, \ldots, 1\rangle\rangle$ definida sobre un cuerpo $K$ con característica distinta de 2. Como $G_Q$ es un grupo con la operación producto y sus elementos son las sumas de $2^n$ cuadrados, es decir los elementos que vienen representados por $X_1^2 + \ldots + X_{2^n}^2$, entonces el producto de sumas de $2^n$ cuadrados de elementos de $K$ será otra suma de $2^n$ cuadrados de $K$. Pasamos a ver un lema que precede a la prueba del resultado de Pfister.

LEMA 3.5.12. *Sea $K$ un cuerpo con característica distinta de 2, y sea $Q = \langle\langle a_1, \ldots, a_n\rangle\rangle$ una forma de Pfister regular, es decir con $a_1, \ldots, a_n \in K^*$. Sea $Q'$ la forma pura de $Q$ y sea $b \in D_K(Q')$. Entonces, existen unas unidades $u_2, \ldots, u_n \in K^*$ tales que $Q$ es equivalente a la forma de Pfister $\langle\langle b, u_2, \ldots, u_n\rangle\rangle$.*

DEMOSTRACIÓN. Véase el Lema 6.4.15 de [**BCR, 1998**]. □

Otro resultado que será necesario a la hora de probar la cota de Pfister es aquel que se conoce como el Teorema de Tsen-Lang. Enunciaremos sin demostración este teorema tal y como puede encontrarse como el Teorema 6.4.16 de [**BCR, 1998**]. Se hablará de grado de trascendencia de una extensión, noción que fue introducida en el Apéndice C pero que resumimos brevemente. En el contexto de una extensión de cuerpos $L/K$, una familia $\{a_1, \ldots, a_r\} \subset L$ se dirá algebraicamente independiente sobre $K$ si para cada $f \in K[X_1, \ldots, X_r]$ que satisface $f(a_1, \ldots, a_r) = 0$ se tiene necesariamente que $f = 0$. Salvando algunas consideraciones previas que han de hacerse utilizando el Lema de Normalización de Noether (puede verse en el Apéndice C), indicamos simplemente el resultado conocido como Teorema de Intercambio de Steinitz, que es crucial en la definición de la base y del grado de trascendencia de una extensión de cuerpos.

TEOREMA 3.5.13. **(de Intercambio de Steinitz)**
*Sea $L/K$ una extensión finitamente generada. Sean $\{a_1, \ldots, a_r\}$ y $\{b_1, \ldots, b_s\}$ dos familias finitas de elementos de $L$ que son algebraicamente independientes sobre $K$ y tales que las extensiones de cuerpos $L/K(a_1, \ldots, a_r)$ y $L/K(b_1, \ldots, b_s)$ sean finitas. Entonces $r = s$.*

DEMOSTRACIÓN. Véase el Lema 18.5 de [**Stewart, 1972**]. □

Este resultado viene a decir algo así como que en una extensión de cuerpos $L/K$ trascendente, cualquier cuerpo intermedio $H$ tal que la extensión $L/H$ sea finita, es decir que se elimine la 'parte trascendente' que hay entre $K$ y $L$, sea una $K$-álgebra finitamente generada por una familia de elementos que son algebraicamente independientes y en particular, trascendentes. Estos generadores del cuerpo intermedio $H$ hacen las veces de una base, y se denominan una base de trascendencia de la extensión, siendo el grado de trascendencia el tamaño de dicha base, que no necesariamente será única. Se definen ambos conceptos a continuación.

DEFINICIÓN 33. **(Base y Grado de Trascendencia)**
*Sea $L/K$ una extensión de cuerpos finitamente generada. Se dice base de trascendencia de $L$ sobre $K$ a cualquier conjunto finito $\mathcal{B} \subset L$ algebraico sobre $K$ y tal que $L/K(\mathcal{B})$ es una extensión de cuerpos finita. Se dice grado de trascendencia de la extensión al cardinal de cualquiera de sus bases de trascendencia, y denota por $grTr_K(L)$.*

Con todo esto ya puede comprenderse el enunciado siguiente.

TEOREMA 3.5.14. **(de Tsen-Lang)**
*Sea $K$ un cuerpo algebraicamente cerrado y sea $L/K$ una extensión de cuerpos con grado de trascendencia $n$. Sea $f \in L[X_1, \dots X_m]$ un polinomio homogéneo de grado $d$ de manera que $m > d^n$. Entonces existe $x \in L^m \setminus \{0\}$ tal que $f(x)$.*

DEMOSTRACIÓN. Puede consultarse el Teorema 6.4.16 de [**BCR, 1998**]. □

La propiedad destacable de este resultado para el contexto en el que nos movemos es la siguiente.

COROLARIO 3.5.15. *Sea $K$ un cuerpo algebraicamente cerrado y sea $L/K$ una extensión de cuerpos con grado de trascendencia $n$. Entonces, toda forma cuadrática definida sobre $L[X_1, \dots, X_m]$ con $m > 2^n$ ha de ser isótropa.*

DEMOSTRACIÓN. Es una deducción inmediata del Teorema 3.5.14 tomando $d = 2$. □

El siguiente resultado se basa en el Teorema de Tsen-Lang y su corolario, y será central en la prueba de la cota de Pfister.

TEOREMA 3.5.16. *Sea $R$ un cuerpo realmente cerrado y sea $L/R$ una extensión de cuerpos con grado de trascendencia $n$. Sea la forma de Pfister regular $Q = \langle\langle u_1, \dots, u_n\rangle\rangle$ dada por las unidades $u_1, \dots, u_n \in R^*$. Entonces, cada $b \in \sum L^2$ viene representado por la forma de Pfister $Q$ sobre $L$, es decir, $b \in D_L(Q)$.*

DEMOSTRACIÓN. Puede verse el Teorema 6.4.17 de [**BCR, 1998**]. □

Finalmente, tenemos el resultado de Pfister. Veremos que su redacción nos recuerda al Teorema 3.3.10 de la generalización de Artin a variedades algebraicas irreducibles, y que efectivamente es una mejora que introduce una cota superior del número de cuadrados con que puedan escribirse los polinomios no negativos.

TEOREMA 3.5.17. **(de Pfister)**
*Sea $R$ un cuerpo realmente cerrado y sea $V \subset \mathbb{A}^m(R)$ una variedad algebraica irreducible con $n = dim(V)$. Entonces, toda función polinomial $f \in \mathcal{P}(V)$ que sea no negativa en algún abierto Zariski de $V$ puede escribirse como suma de $2^n$ cuadrados de elementos de $\mathcal{K}(V)$.*

DEMOSTRACIÓN. Aplicando el Teorema 3.3.10, se tiene que las funciones polinomiales de $\mathcal{P}(V)$ que sean no negativas en algún abierto Zariski de $V$ son exactamente los elementos de $\sum \mathcal{K}(V)^2$. Para ver que dichos elementos sean sumas de $2^n$ cuadrados, se usa el Teorema 3.5.16 con la forma de Pfister $Q = \langle\langle 1, \dots, 1\rangle\rangle$ y con $L = \mathcal{K}(V)$. Tan solo queda probar que la extensión de cuerpos $\mathcal{K}(V)/R$ tiene grado de trascendencia $n$, que se indica en el Corolario C.31. □

Para concluir la sección, hagamos acopio de lo que se ha probado hasta ahora.

COROLARIO 3.5.18. *Sea $R$ un cuerpo realmente cerrado. Entonces, el número de Pitágoras de $R(X_1 \dots, X_n)$ viene acotado por las siguientes desigualdades:*

$$n + 1 \leq p(R(X_1, \dots, X_n)) \leq 2^n.$$

DEMOSTRACIÓN. Se sigue de aplicar el Corolario 3.5.7 tomando $F = R$ y el Teorema 3.5.17 con $V = \emptyset$. □

La cota inferior de $p(R(X_1, \dots, X_n))$ que hemos visto se atribuye a Cassels. Varios años después de dar este resultado, estableció una cota más estricta junto con W. S. Elliston y Pfister. La cota en cuestión es la siguiente, con las notaciones del resultado anterior:

$$p(R(X_1, \dots, X_n)) \geq n + 2,$$

para $n \geq 2$. En particular se tiene que $p(R(X_1, X_2)) = 4$, aunque el problema de conocer $p(R(X_1, \dots, X_n))$ para $n \geq 3$ sigue abierto.

Apéndice A

# Teoría de Artin-Schreier.

En esta sección veremos aspectos fundamentales de la Teoría de Cuerpos Ordenados y de la Teoría de Cuerpos Realmente Cerrados que surgen a raíz del trabajo de Artin y Schreier. La noción de cuerpo ordenado se remonta a la década de 1890 y la presentó Hilbert en alguno de sus numerosos trabajos.[1] La definición que dio se basaba en una relación de orden sobre un cuerpo que además fuese compatible con sus operaciones de cuerpo. En la década de 1920 apareció lo que a día de hoy se conoce como la Teoría de Artin-Schreier, publicada en sus trabajos conjuntos de 1926 y 1927. En estos se hablaría de cuerpos ordenados en términos de conos positivos en lugar de un orden explícito. Esta formalidad permite un estudio más sistemático de las ordenaciones que admite un cuerpo, y es uno de los objetos de estudio principales de la Teoría de Cuerpos Ordenados. También introdujeron la idea de cuerpo realmente cerrado, como una generalización del cuerpo $\mathbb{R}$ de los reales y como una especie de clausura de los cuerpos ordenados.

Dedicaremos los dos primeros apartados a revisar los resultados principales de la Teoría de Artin-Schreier, que esencialmente será una recopilación ordenada de las ideas que aparecen en las Secciones 1.1 y 2.1. Cada apartado culminará con uno de los Teoremas de Artin-Schreier, siendo el primero sobre la equivalencia entre cuerpos ordenados y cuerpos formalmente reales y el segundo sobre una caracterización de los cuerpos realmente cerrados a través de su clausura algebraica. Seguidamente, veremos ejemplos muy distintos de cuerpos ordenados y algún resultado útil para estudiar a las ordenaciones de un cuerpo ordenado. También mencionaremos al Principio de Transferencia como una propiedad de los cuerpos realmente cerrados. Para terminar, se añade algunos resultados de análisis real que son válidos para cuerpos realmente cerrados y tratará de explicarse que la Propiedad de Arquimedianidad de un cuerpo ordenado es lo que distingue a $\mathbb{R}$ del resto de cuerpos realmente cerrados y hace que no todo el análisis real sea válido para estos cuerpos.

Para la elaboración de este apéndice se ha seguido las notas de [**Gentile, 1992**], el Capítulo 1 de [**BCR, 1998**] y el Capítulo 2 de [**BaSh, 2000**].

**Cuerpos Ordenados.**

En esta subsección presentaremos las definiciones y resultados elementales en relación con el Teorema de Artin-Schreier para Cuerpos Ordenados, que esencialmente supone la equivalencia entre los cuerpos formalmente reales y los cuerpos que admiten ordenación. Los cuerpos formalmente reales se definen por una propiedad que distingue a los cuerpos $\mathbb{Q}$ y $\mathbb{R}$ de $\mathbb{C}$, como vemos a continuación.

Definición 34. **(Cuerpo Formalmente Real)**
*Un cuerpo $F$ se dice formalmente real cuando para cada $x_1, \ldots, x_p \in F$ se tiene que:*

$$x_1^2 + \ldots + x_p^2 = 0 \Rightarrow x_1 = \ldots = x_p = 0.$$

Los cuerpos $\mathbb{Q}$ y $\mathbb{R}$ son ejemplos de cuerpos formalmente reales, mientras que el cuerpo $\mathbb{C}$ de los complejos no lo es por $i^2 + 1 = 0$. Se observa además que los cuerpos con característica finita no pueden ser formalmente reales, dado que si $F$ es un cuerpo con característica $n \in \mathbb{N}$, entonces

[1] Puede verse en el Enunciado 2.1.5 de [**BaSh, 2000**] las propiedades del orden de $\mathbb{R}$ que señalaba Hilbert. Estas difieren en la llamada Propiedad de Tricotomía de la presentación que se hace de ellas hoy día como la definición de cuerpo ordenado que veremos en el texto, más adecuada a la idea de cono positivo de una ordenación.

puede escribirse que:

$$n1 = 1^2 + \ldots + 1^2 = 0.$$

En particular esto implica que ningún cuerpo finito es formalmente real. Ahora pasamos a definir a un cuerpo ordenado. Lo haremos a partir de una ordenación, es decir, un orden de los elementos del cuerpo que sea compatible con sus operaciones.

DEFINICIÓN 35. **(Cuerpo Ordenado)**
*Sea $F$ un cuerpo. Se dice ordenación del cuerpo $F$ a una relación de orden total $\leq$ que cumpla:*

*(i)* $x \leq y \Rightarrow x + z \leq y + z$ *para cada* $x, y, z \in F$,
*(ii)* $0 \leq x \wedge 0 \leq y \Rightarrow 0 \leq xy$ *para cada* $x, y \in F$.

*En tal caso, se dice cuerpo ordenado al par $(F, \leq)$. Se dirá que $F$ no admite ordenación si no existe alguna ordenación $\leq$ de $F$.*

OBSERVACIÓN A.1. Las propiedades de cuerpo ordenado implican que $-1 \leq 0$. Más aún, esto combinado con la Propiedad $(i)$ de la definición precedente implica que:

$$n1 = 1 + \ldots + 1 < n1 + 1.$$

Veamos algunos ejemplos básicos de cuerpos ordenados.

EJEMPLO A.2. *Se muestra ejemplos de cuerpos que son y que no son ordenables:*

(I) *Los cuerpos $\mathbb{Q}$ y $\mathbb{R}$ son cuerpos que admiten una única ordenación.*
(II) *El cuerpo $\mathbb{C}$ de los complejos no admite ordenación.*
(III) *En vista de la Observación A.1, los cuerpos con característica finita, y en particular los cuerpos finitos, no admiten ordenación.*

Como se anticipó, esta definición de cuerpo ordenado no es la más funcional a la hora de probar las propiedades de esta clase de cuerpos. Introducimos a continuación la noción de cono, que como veremos estará relacionada con las ordenaciones de un cuerpo.

DEFINICIÓN 36. **(Cono, Cono Propio)**
*Sea $A$ un anillo conmutativo. Un subconjunto $P \subset A$ se dice cono si cumple:*

*(i)* $x + y \in P$ *para cada* $x, y \in P$,
*(ii)* $xy \in P$ *para cada* $x, y \in P$,
*(iii)* $x \in A \Rightarrow x^2 \in P$.

*$P$ se dice cono propio si además cumple:*

*(iv)* $-1 \notin P$.

Veamos, antes que nada, algunos ejemplos básicos de conos y conos primos.

EJEMPLO A.3. *Los siguientes son ejemplos de conos sobre un anillo conmutativo $A$:*

(I) *Se denota por $\sum A^2$ al conjunto de las sumas de cuadrados de elementos de $A$ (algunas de sus propiedades ya se vio en la prueba de la Proposición 1.3.8), el cual es un cono de $A$ que está incluido en cualquier otro cono de $A$.*
(II) *Dada una familia de conos de $A$, se tiene que su intersección es también un cono de $A$. Si además alguno de los conos de la intersección es propio, la intersección de ellos será un cono propio.*
(III) *El ejemplo anterior permite definir el menor cono que contiene a otro cono $P$ y a la familia $\{a_j\}_{j\in J}$ de elementos de $A$, que se denota por:*

$$P[\{a_j\}_{j\in J}] = \bigcap_{\substack{P\cup\{a_j\}_{j\in J}\subset Q \\ Q\subset A \text{ cono}}} Q.$$

*Puede verse en la Proposición 2.1.3 que los elementos de $P[\{a_j\}_{j\in J}]$ son de la forma $p + \sum_{i=1}^{r} q_i b_i$ con $p, q_1, \ldots, q_r \in P$ y siendo cada $b_i$ un producto finito de elementos del conjunto $\{a_j\}_{j\in J}$. En particular se tiene que los elementos de $P[a]$ para cualquier $a \in A$ serán de la forma $p+qa$ con $q, p \in A$. Con la notación de menor cono generado, el menor cono que contiene a la familia $\{a_j\}_{j\in J}$ sería $\sum A^2[\{a_j\}_{j\in J}]$.*
(IV) *Dado un cuerpo ordenado $(F, \leq)$, se define al conjunto de los elementos no negativos de $F$ como $P = \{x \in F : x \geq 0\}$. El conjunto $P$ es un cono propio de $F$, independientemente de su ordenación, y se dice el cono positivo asociado a $\leq$.*

Es destacable que el conjunto de los elementos no negativos de una ordenación sea precisamente un cono propio. Si se dispone de un conjunto $P$ de los elementos positivos de un cuerpo ordenado $(F, \leq)$, la relación entre un par de elementos $x, y \in F$ viene dada por $x \leq y$ cuando $y - x \in P$, y por $x \geq y$ si $x - y \in P$. Sin embargo, para definir la ordenación a partir de un cono no basta con que este sea propio, sino que además tiene que poder definir un orden total en todo el cuerpo. Esto se traduce en el siguiente resultado.

PROPOSICIÓN A.4. *Sea $(F, \leq)$ un cuerpo ordenado y sea $P = \{x \in F : x \geq 0\}$ su cono positivo. Se define al conjunto $-P = \{x \in F : -x \in P\}$ y con esto, se cumple la siguiente propiedad:*

*(v) $P \cup -P = F$.*

*Por otro lado, si $Q$ es un cono propio de algún cuerpo $H$ que satisface $(v)$, la siguiente relación define una ordenación sobre $H$:*

$$x \preceq y \Leftrightarrow y - x \in Q,$$

*y además $Q$ es cono positivo para el cuerpo ordenado $(H, \preceq)$. Se dirá cono positivo a todo cono propio de un cuerpo que además satisfaga la propiedad $(v)$.*

La relación que existe entre el conjunto de los conos positivos de un cuerpo con el conjunto de sus ordenaciones es biunívoca, es decir, una ordenación da lugar a un único cono positivo y recíprocamente un cono positivo define a una única relación de orden que es ordenación del cuerpo. La importancia de la noción de cono positivo radica en conocer la estructura del conjunto de los conos de un cuerpo. Para llevar esto acabo, es conveniente observar que si $P$ es un cono del cuerpo $F$ que no es cono propio, es decir que si $-1 \in P$, entonces $P = F$.[2] Dicho de otra forma, los conos propios de $F$ coinciden con los subconjuntos propios de $F$ que son conos. Entonces basta con estudiar al conjunto $\Lambda_F$ de los conos propios de un cuerpo y para ello es útil la proposición siguiente.

PROPOSICIÓN A.5. *Sea $F$ un cuerpo, y sea $\Lambda_F$ el conjunto de los conos propios de $F$. Si $\Lambda_F$ es no vacío, entonces $F$ admite ordenación. Además, el conjunto de conos propios maximales para la inclusión será el conjunto de conos positivos de cada una de las ordenaciones que admite $F$.*

De este resultado se deducen varias cosas sobre la estructura del conjunto $\Lambda_F$ de los conos propios de un cuerpo $F$. En primer lugar, como $\sum F^2$ es un cono que está contenido en cualquier otro cono de $F$, se tiene la equivalencia siguiente:

$$\Lambda_F = \emptyset \Leftrightarrow -1 \in \sum F^2.$$

También, el cono $\sum F^2$ es el elemento minimal de $\Lambda_F$ ordenado por la relación de inclusión y los conos positivos de $F$ serán los elementos maximales. Hay un detalle más, y es que si este elemento maximal es único, entonces existe un único cono propio y cono positivo $\sum F^2$.

PROPOSICIÓN A.6. *Sea $F$ un cuerpo, y sea $\Lambda_F$ el conjunto de los conos propios de $F$. Si $\Lambda_F$ es no vacío, entonces $\sum F^2$ es la intersección de los elementos maximales de $\Lambda_F$ respecto de la relación de inclusión.*

En consecuencia, los cuerpos que admiten una ordenación única vendrán ordenados por el conjunto de sus sumas de cuadrados, como es el caso de $\mathbb{Q}$ para el que puede verse el Teorema de Lagrange de los 4 Cuadrados 2.1.9, o de $\mathbb{R}$ para el que se verá que toda suma de cuadrados es de hecho un cuadrado. Con este preámbulo, ya sería posible dar una prueba del resultado de Artin y Schreier sobre cuerpos ordenados, el cual establece la equivalencia entre cuerpo formalmente real y cuerpo que admite ordenación.

TEOREMA A.7. **(de Artin-Schreier para Cuerpos Ordenados)**
*Sea $F$ un cuerpo. Son equivalentes:*

*(i) $F$ es cuerpo formalmente real, es decir, se cumple que para cada $x_1, \ldots, x_n \in F$, $\sum x_i^2 = 0$ implica que $x_1 = \cdots = x_n = 0$,*
*(ii) $-1 \notin \sum F^2$,*
*(iii) $F$ admite ordenación.*

[2]Para probar esto basta observar que $\sum F^2[-1] = F$, ya que para cualquier $x \in F$ puede escribirse que $x = [(1+x)^2 + (-1)(1-x)^2]/4$ y $\mathbb{Q}$ es un subcuerpo de $F$ por ser $F$ un cuerpo infinito.

**Cuerpos Realmente Cerrados y Clausura Real.**

A continuación veremos el otro resultado característico de la Teoría de Artin-Schreier, aquel que trata sobre cuerpos realmente cerrados y su clausura algebraica. Los cuerpos realmente cerrados son un ejemplo particular de cuerpo formalmente real que incluye al cuerpo $\mathbb{R}$ de los reales pero no a $\mathbb{Q}$. Ya señalamos que en $\mathbb{R}$ cada elemento positivo es un cuadrado y que esto no sucede así para $\mathbb{Q}$. Lo que sucede es que existe algún $a \in \mathbb{Q}$ positivo (por ejemplo $a = 2$) tal que la extensión algebraica $\mathbb{Q}[X]/(X^2 - a)/\mathbb{Q}$ es no trivial y además existe alguna ordenación de $\mathbb{Q}[X]/(X^2 - a)$ que extiende a la de $\mathbb{Q}$. La idea de cuerpo realmente cerrado se basa en llegar a una extensión del cuerpo formalmente real que incluya todas estas raíces cuadradas de elementos positivos. Dicho esto, no resultará arbitraria la definición siguiente.

Definición 37. **(Cuerpo Realmente Cerrado)**
*Se dice cuerpo realmente cerrado a todo cuerpo formalmente real que no tenga una extensión de cuerpos algebraica propia que además sea un cuerpo formalmente real.*

Nótese del ejemplo de la introducción que el cuerpo $\mathbb{Q}$ de los racionales no cumple con la definición de cuerpo realmente cerrado. Por otra parte, $\mathbb{R}$ sí que es un cuerpo realmente cerrado, ya que por el Teorema Fundamental del Álgebra se sabe que $\mathbb{C}$ es la única extensión algebraica propia de $\mathbb{R}$ y este no admite ordenación. Conviene aclarar una cuestión sobre el ejemplo de la extensión $\mathbb{Q}[X]/(X^2 - a)$ del cuerpo $\mathbb{Q}$, y es que en primer lugar, se dice que $F/H$ es una extensión de cuerpos cuando $F$ y $H$ son cuerpos y además existe un morfismo inyectivo de $H$ en $F$. Ahora bien, en el citado ejemplo queríamos decir que $\mathbb{Q}[X]/(X^2 - a)/\mathbb{Q}$ resulta ser una extensión algebraica de cuerpos ordenados, y esto quiere decir que el morfismo inyectivo de $\mathbb{Q}$ en $\mathbb{Q}[X]/(X^2 - a)$ (asumiendo una ordenación en cada uno de ellos) cumple que es además ordenado. Definimos la idea de un morfismo ordenado.

Definición 38. **(Morfismo Ordenado)**
*Sean $(F, \leq)$ y $(H, \preceq)$ un par de cuerpos ordenados de conos positivos $P$ y $Q$, respectivamente. Sea $\phi : F \to H$ un morfismo de cuerpos. El morfismo $\phi$ se dice ordenado cuando $\phi(P) \subset Q$. Si además se cumple que el morfismo $\phi$ es una aplicación biyectiva y que su inversa satisface $\phi^{-1}(Q) \subset P$, se dirá que $\phi$ es un isomorfismo ordenado y que los cuerpos ordenados $(F, \leq)$ y $(H, \preceq)$ son cuerpos ordenados isomorfos.*

Con las notaciones de la definición precedente, observemos un morfismo ordenado $\phi : F \to H$ cumple que si $x \leq y$ para un par de elementos $x, y \in F$, entonces $\phi(x) \preceq \phi(y)$. Retomando el tema principal, veamos que efectivamente los cuerpos realmente cerrados cumplen con aquella propiedad que destacábamos en $\mathbb{R}$.

Proposición A.8. *Todo cuerpo realmente cerrado admitirá una única ordenación en la que sus elementos positivos serán los cuadrados.*

En el Apéndice E se verá que esta propiedad lleva a definir la norma euclídea en el espacio afín $\mathbb{A}^n(R)$ definido sobre un cuerpo realmente cerrado $R$, y con ello una topología euclídea sobre $\mathbb{A}^n(R)$. Pasamos a ver el resultado de Artin y Schreier para cuerpos realmente cerrados.[3]

Teorema A.9. **(de Artin-Schreier para Cuerpos Realmente Cerrados)**
*Sea $K$ un cuerpo algebraicamente cerrado. Si $R$ es un subcuerpo propio de $K$ tal que $K/R$ es una extensión de cuerpos de grado $[K : R]$ finito, entonces $R$ es un cuerpo formalmente real y su clausura algebraica será el cuerpo $R[\sqrt{-1}]$ isomorfo a $K$.*

Puede enunciarse también la caracterización siguiente sacada del Teorema 1.2.2 de [**BCR, 1998**], que es también la que veremos de forma reducida durante la Sección 2.1.

Teorema A.10. *Sea $F$ un cuerpo. Entonces, son equivalentes:*

(*i*) *$F$ es un cuerpo realmente cerrado.*
(*ii*) *$F$ admite una única ordenación cuyos elementos positivos son los cuadrados de $F$, y además todo polinomio $f \in F[X]$ de grado impar tiene alguna raíz en $F$.*
(*iii*) *El anillo $F[X]/(X^2 + 1)$ es un cuerpo algebraicamente cerrado.*

[3]Puede consultarse esta presentación del resultado de Artin-Schreier junto con una prueba en el TFG de M. E. López titulado *"Cuerpos Ordenados"* con fecha de 2018.

Para concluir el apartado volvemos sobre el ejemplo del inicio, en el que dijimos que el cuerpo $\mathbb{Q}$ puede ir extendiéndose en otros cuerpos formalmente reales añadiendo las raíces cuadradas de sus elementos positivos (por raíz cuadrada de un elemento $a \in F$ entenderemos que es la raíz del polinomio $X^2 - a$ que es positiva para la extensión de cuerpos ordenados $F[a]/F$). La cuestión aquí es si para todo cuerpo formalmente real puede darse un cuerpo realmente cerrado que sea una extensión algebraica de este que respete su ordenación y que sea maximal de entre todas estas extensiones algebraicas. Primeramente nombraremos a este tipo de extensión.

Definición 39. **(Clausura Real)**
*Sea $F$ un cuerpo formalmente real junto con una ordenación $\leq$. Se dice clausura real de $F$ a toda extensión algebraica $R$ de $F$ que sea cuerpo realmente cerrado y cuya única ordenación extienda a la de $F$.*

Queda claro por el Teorema Artin-Schreier para Cuerpos Realmente Cerrados A.9 que de existir una clausura real $R$ de un cuerpo ordenado $F$, la extensión $R/F$ no puede tener grado finito. Es decir, que la idea de ir añadiendo raíces cuadradas ausentes una a una no es solvente en cuestión de dar una extensión de este tipo, pero sí que puede probarse su existencia a partir de la existencia de una clausura algebraica para un cuerpo en general. Al igual que la clausura algebraica, la clausura real de un cuerpo ordenado no será única, aunque sí lo será salvo $F$-isomorfismos. Recordemos que un $F$-isomorfismo de un par de extensiones del cuerpo $F$ es un isomorfismo entre dichos cuerpos que aplicado a elementos de $F$ (en el sentido de las inclusiones) es la identidad.

Teorema A.11. *Todo cuerpo formalmente real $F$ tiene clausura real. Además, si $R_1$ y $R_2$ son un par de clausuras reales de $F$, existirá un $F$-isomorfismo de $R_1$ en $R_2$.*

Terminemos con un ejemplo de clausura real. La clausura real del cuerpo $\mathbb{Q}$ de los racionales no es $\mathbb{R}$, sino que es el cuerpo $\mathbb{R}_{alg}$ de los números reales algebraicos sobre $\mathbb{Q}$.

**Ejemplos de Cuerpos Ordenados y Clasificación de Cuerpos Realmente Cerrados.**

En esta subsección se quiere tocar algunos temas relacionados con las nociones de cuerpo ordenado y de cuerpo realmente cerrado que siguen al trabajo de Artin y de Schreier. Comenzamos con un pequeño estudio sobre cuerpos ordenados. Si $F$ es un cuerpo que admite ordenación, o equivalentemente un cuerpo formalmente real, se denota por $\Lambda_F$ al conjunto de sus conos propios. En algún apartado previo se vio la estructura de este conjunto al considerar la relación de inclusión. Aquí veremos ejemplos sobre todo tipo de casos: cuerpos que admiten una única ordenación, una cantidad finita de ellas, o infinita, o ninguna en absoluto; y durante el proceso se verá algún resultado sobre conos que permite definir cómodamente a las distintas ordenaciones de algunos cuerpos. Comencemos por recordar los ejemplos más sencillos.

Ejemplo A.12. *Vemos algunos ejemplos muy elementales de cuerpos ordenados y de cuerpos realmente cerrados:*

(i) *El cuerpo $\mathbb{C}$ de los números complejos no admite ordenación, ya que $-1 = i^2$ es un cuadrado en $\mathbb{C}$. Este mismo razonamiento es válido cualquier cuerpo $K$ algebraicamente cerrado, entendiendo que $i$ es alguna raíz del polinomio $X^2 + 1 \in K[X]$.*

(ii) *El cuerpo $\mathbb{R}$ de los números reales es un cuerpo realmente cerrado, ya que por el Teorema Fundamental del Álgebra se sabe que $\mathbb{C}$ es su única extensión algebraica propia. En particular, $\mathbb{R} = \mathbb{R}/(X^2 - a) = \mathbb{R}[\sqrt{a}]$ para cada $a \in \mathbb{R}$ positivo ($a \in \sum \mathbb{R}^2$).*

(iii) *El cuerpo $\mathbb{Q}$ de los números racionales es un cuerpo formalmente real, dado que para todo $m/n \in \mathbb{Q}$ positivo puede escribirse que:*

$$\frac{m}{n} = \frac{mn}{n^2} = \left(\frac{1}{n}\right)^2 + \ldots + \left(\frac{1}{n}\right)^2.$$

*Además este admite una única ordenación, ya que todo elemento positivo es una suma de cuadrados. No es un cuerpo realmente cerrado porque tiene extensiones algebraicas propias, como $\mathbb{Q}[\sqrt{2}]$, que admiten alguna ordenación que extiende a la de $\mathbb{Q}$. Como $\pi \in \mathbb{R}$ es un elemento trascendente sobre $\mathbb{Q}$, $\mathbb{R}$ no es una extensión algebraica de $\mathbb{Q}$ no puede ser una clausura real de $\mathbb{Q}$, aunque la contiene.*

Para dar ejemplos de cuerpos formalmente reales con varias ordenaciones, será conveniente explotar una propiedad de los morfismos de cuerpos que se enuncia como sigue.

PROPOSICIÓN A.13. *Sean $F_1$ y $F_2$ un par de cuerpos formalmente reales y sean $\Lambda_{F_1}, \Lambda_{F_2}$ los conjuntos de los conos propios de cada uno de ellos. Supongamos que $F_1$ y $F_2$ son cuerpos isomorfos y que $\phi : F_1 \to F_2$ es un isomorfismo de cuerpos. Entonces, la aplicación de $\Lambda_{F_1}$ en $\Lambda_{F_2}$ definida por $P \mapsto \phi(P)$ para cada $P \in \Lambda_{F_1}$ es biyectiva. Además, esta aplicación preserva la relación de inclusión de los conjuntos $\Lambda_{F_1}, \Lambda_{F_2}$, y en particular se tiene que un isomorfismo de cuerpos transforma conos positivos en conos positivos.*

Hay varias cosas que comentar. Lo primero es que los isomorfismos de cuerpos preservan la estructura del conjunto de los conos positivos. Es decir, que dados un par de cuerpos isomorfos, los conjuntos de conos propios asociados guardan una relación de biyección que, con las notaciones de la proposición precedente, cumple que $\phi(P) \subset \phi(P')$ cuando $P \subset P'$ para $P, P' \in \Lambda_{F_1}$. Un hecho que se sigue de esto, es que los isomorfismos de cuerpos respetan la propiedad de que un cuerpo sea formalmente real o no, y no tiene sentido hacer una distinción hablando de morfismos de cuerpos formalmente reales. Otra cosa a señalar, es que esto es diferente del caso en el que ambos cuerpos formalmente reales vengan ya con una ordenación específica, por lo cual sí que tiene sentido hablar de morfismos ordenados como se hizo en la Definición 38. En relación con esto último se tiene el corolario siguiente.

COROLARIO A.14. *Sean $F_1$ y $F_2$ un par de cuerpos formalmente reales que son isomorfos y sea $\phi : F_1 \to F_2$ cualquier isomorfismo de cuerpos. Entonces, para cada cono positivo $P \in \Lambda_{F_1}$ se tiene que $\phi$ es un isomorfismo ordenado del cuerpo $F_1$ con la ordenación dada por $P$ en el cuerpo $F_2$ con la ordenación dada por $\phi(P)$.*

Se desea utilizar estas propiedades para obtener diferentes ordenaciones de un cuerpo formalmente real. Nos fijamos en el caso particular de un único cuerpo formalmente real $F$ y llamamos $\Gamma_F$ al conjunto de sus conos positivos. Nos damos cuenta de que el grupo $Aut(F)$ de los automorfismos de $F$ define una acción sobre $\Gamma_F$ de la forma siguiente:

$$\begin{aligned} Aut(F) \times \Gamma_F &\longrightarrow \Gamma_F \\ (\phi, P) &\longmapsto \phi(P). \end{aligned}$$

Notemos que los automorfismos de un cuerpo $F$ dejan invariantes a los elementos de su cuerpo primo, y que para cuerpos formalmente reales podemos hablar del grupo $Aut_{\mathbb{Q}}(F)$ de los $\mathbb{Q}$-automorfismos. Si se desea considerar tan solo las ordenaciones de $F$ que extienden alguna de las posibles ordenaciones de otro subcuerpo formalmente real $H$, habría que estudiar en su lugar la acción que define de forma análoga $Aut_H(F)$ sobre el subconjunto de conos positivos que incluyen algún cono positivo de $H$. La labor de hallar condiciones para hacer que esta acción sea transitiva o fiel no nos parece trivial, y lo que haremos será únicamente examinar lo que sucede para un par de ejemplos. La transitividad de esta acción implica que si se conoce el grupo de automorfismos, entonces puede encontrarse un automorfismo que transforme a un cono positivo conocido en cualquier otro; y la propiedad de ser fiel implica que, de existir, dicho automorfismo es único. Pasemos a los ejemplos.

EJEMPLO A.15. *Consideremos la extensión de cuerpos finita $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$. El cuerpo $\mathbb{Q}$ tiene una ordenación única dada por $\sum \mathbb{Q}^2$ y el grupo $Aut_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}])$ de los automorfismos de $\mathbb{Q}[\sqrt{2}]$ tiene tan solo 2 elementos. Uno de ellos es la identidad, id, y el otro, llamémosle $\sigma$, se identifica por satisfacer $\sigma(\sqrt{2}) = -\sqrt{2}$. Por otra parte, puede probarse que $\sum \mathbb{Q}^2[\sqrt{2}]$ es un cono positivo de $\mathbb{Q}[\sqrt{2}]$. Entonces, los conos positivos de esta extensión que pueden encontrarse por el grupo de automorfismos son $id(\sum \mathbb{Q}^2[\sqrt{2}]) = \sum \mathbb{Q}^2[\sqrt{2}]$ y $\sigma(\sum \mathbb{Q}^2[\sqrt{2}]) = \sum \mathbb{Q}^2[-\sqrt{2}]$. Puede probarse que estos son los únicos conos positivos de $\mathbb{Q}[\sqrt{2}]$ y que, por lo tanto, este cuerpo admite dos ordenaciones distintas.*

En este ejemplo se tiene que la acción del grupo de automorfismos en el conjunto de los conos positivos es transitiva y fiel, y por ello nos ha permitido obtener todos los conos positivos de la extensión a partir de uno solo. Insistimos en que, si se conoce unas condiciones para que dicha acción sea transitiva y se conoce el grupo de automorfismos, entonces queda resuelto el problema de conocer las posibles ordenaciones de un cuerpo bajo esas condiciones. Ahora vemos

un ejemplo clásico de un cuerpo formalmente real que admite una cantidad no numerable de ordenaciones.

EJEMPLO A.16. *Consideramos $\mathbb{R}(X)$ el cuerpo de fracciones de $\mathbb{R}[X]$. Vamos a ver la manera de definir todas las posibles ordenaciones de este cuerpo. En primer lugar, definamos una ordenación sobre $\mathbb{R}(X)$ que extienda a la de $\mathbb{R}$ y que además satisfaga $X < a$ para todo $a \in \mathbb{R}$ que sea estrictamente positivo. Si se tiene un polinomio $f \in \mathbb{R}(X)$ que sea de la forma:*

$$f(X) = a_n X^n + \ldots + a_k X^k,$$

*con $a_n, a_k \neq 0$, puede descomponerse como*

$$f(X) = a_n(X - \alpha_1) \cdot \ldots \cdot (X - \alpha_r) g_1(X) \cdot \ldots \cdot g_s(X),$$

*donde $\alpha_1, \ldots, \alpha_r \in \mathbb{R}$ son las raíces reales de $f$ y cada $g_i(X) \in \mathbb{R}(X)$ es un polinomio irreducible de grado 2 con raíces $z_i, \overline{z}_i \in \mathbb{C}$. Por un lado, cada polinomio $g_i(X) = X^2 + bX + c$ con $b^2 - 4c < 0$ puede escribirse como:*

$$g_i(X) = \left(X + \frac{b}{2}\right)^2 + \left(\frac{\sqrt{4c - b^2}}{4}\right)^2,$$

*de modo que $g_1, \ldots, g_s \geq 0$. Entonces el signo del polinomio $f$ será el signo del producto $a_n(X - \alpha_1) \cdot \ldots \cdot (X - \alpha_r)$. Se tiene que $X - \alpha_i \geq 0$ si y solo si $X \geq \alpha_i$, y esto solo ocurre cuando $-\alpha_i \geq 0$. Entonces $f \geq 0$ si y solamente si $a_n(-\alpha_1) \cdot \ldots \cdot (-\alpha_r) \geq 0$. Aplicando las Fórmulas de Cardano-Vieta (véase el Apéndice F), se tiene que $f > 0$ si y solo si $a_n > 0$. Si tomamos un cociente de polinomios $f/g \in \mathbb{R}(X)$, basta considerar que $f/g = fg/g^2$ y que entonces $f/g > 0$ si y solamente si $fg > 0$. Esto prueba que la relación dada por las condiciones anteriores está bien definida para cada elemento de $\mathbb{R}(X)$. Omitimos probar que se trata de una ordenación, que es un ejercicio sencillo. Este y el resto de ordenaciones de $\mathbb{R}(X)$ se definen extendiendo la ordenación de $\mathbb{R}$ a $\mathbb{R}(X)$ imponiendo alguna condición de entre las siguientes:*

- *(i) $X < a$ para todo $a \in \mathbb{R}$,*
- *(ii) dado un $a \in \mathbb{R}$ estrictamente positivo, $a - \varepsilon < X < a$ para todo $\varepsilon \in \mathbb{R}$ estrictamente positivo,*
- *(iii) dado un $a \in \mathbb{R}$ estrictamente positivo, $a < X < a + \varepsilon$ para todo $\varepsilon \in \mathbb{R}$ estrictamente positivo,*
- *(iv) $X > a$ para todo $a \in \mathbb{R}$.*

*Hemos probado que la Condición (i) define una ordenación sobre $\mathbb{R}(X)$. Puede probarse que el resto de condiciones definen una ordenación diferente utilizando la Proposición A.13 y planteando unos $\mathbb{R}$-automorfismos que satisfagan las condiciones siguientes:*

- *(I) $X \mapsto X$,*
- *(II) sea la misma constante $a \in \mathbb{R}$ que la dada en la Condición (ii) de más arriba, el automorfismo asociado es $X \mapsto a - X$,*
- *(III) sea la misma constante $a \in \mathbb{R}$ que la dada en la Condición (iii) de más arriba, el automorfismo asociado es $X \mapsto X - a$,*
- *(IV) $X \mapsto \dfrac{1}{X}$,*

*de manera que (i) se corresponde con (I), (ii) con (II), (iii) con (III) y (iv) con (IV). Omitimos probar que se ha dado todas las posibles ordenaciones de $\mathbb{R}(X)$, pero consideraremos que así es.*

En este caso las transformaciones del cono positivo inicial no han sido evidentes, pero de igual forma tenemos un cuerpo ordenado donde los automorfismos permiten obtener todas las ordenaciones a partir de una de ellas, es decir, que la acción del grupo de automorfismos es transitiva. Sin embargo, esta acción no es fiel y se demuestra observando que el $\mathbb{R}$-automorfismo que cumple $X \mapsto 2X$ actúa igual que la identidad sobre el conjunto de los conos positivos de $\mathbb{R}(X)$.

Este ejemplo se distingue de $\mathbb{Q}$ y de $\mathbb{R}$, aparte de la diferencia evidente por la cantidad de ordenaciones que presenta, en la Propiedad de Arquimedianidad que presentan todas las ordenaciones de $\mathbb{R}(X)$, propiedad sobre la que hablaremos en el apartado siguiente.

Ahora, pasamos a discutir brevemente sobre la clasificación de las clases de isomorfía de cuerpos realmente cerrados. En el caso de cuerpos algebraicamente cerrados, se tiene el trabajo de E. Steinitz titulado *"Algebraische Theorie der Körper"* y publicado en 1910 en que clasifica a los

cuerpos algebraicamente cerrados salvo isomorfía por medio de su característica y del grado de trascendencia (noción que introducimos en el Apéndice C). De momento, no se conoce una clasificación completa de las clases de isomorfía de cuerpos realmente cerrados.

Sin embargo, el caso de cuerpos realmente cerrados no requiere de una clasificación en el sentido siguiente. Existe el Principio de Trasferencia 1.2.5 que nos dice que cuando cierto tipo de enunciados son ciertos para algún cuerpo realmente cerrado, ya sea el arquetipo $\mathbb{R}$, entonces el enunciado será cierto para el resto de cuerpos realmente cerrados. El caso es que los cuerpos algebraicamente cerrados no disponen de un resultado que funcione de manera tan general, sino que esta transferencia se garantiza entre cuerpos algebraicamente cerrados con la misma característica. Este resultado para característica 0 se conoce como el Principio de Lefschetz.

**Análisis Real y Arquimedianidad en Cuerpos Ordenados.**

Para finalizar este apéndice hablaremos de las generalizaciones del análisis sobre el cuerpo $\mathbb{R}$ de los reales al análisis de cuerpos realmente cerrados en general. En el caso general pasa que a veces se cumplen los resultados del caso real y a veces no. La diferencia principal, como veremos, consiste en otra propiedad que posee $\mathbb{R}$ y que le caracteriza. La relacionaremos con las ideas de arquimedianidad y densidad, y mostraremos ejemplos de órdenes no arquimedianos que ya hemos visto.

Para empezar, veremos algunos de los resultados más básicos del Análisis Real pero aplicados solo a funciones polinomiales. Es necesario conocer la noción de derivada de un polinomio dada por la Definición 64 antes de seguir. También hay que detallar que dado un cuerpo ordenado $F$ y un par de elementos $a, b \in F$ con $a < b$, se definen los intervalos:

$$(a, b) = \{x \in F : a < x < b\}, \qquad [a, b] = \{x \in F : a \leq x \leq b\}.$$

A continuación se enuncia varios resultados reconocibles del Análisis Real, pero generalizados a cuerpos realmente cerrados.

Proposición A.17. **(Teorema de Bolzano)**
*Sean $R$ un cuerpo realmente cerrado, $f \in R[X]$ un polinomio y unos elementos $a, b \in R$ tales que $a < b$. Si $f(a)f(b) < 0$, entonces existirá un elemento $c \in (a, b)$ que es raíz de $f$, es decir, $f(c) = 0$.*

Proposición A.18. **(Teorema de Rolle)**
*Sean $R$ un cuerpo realmente cerrado, $f \in R[X]$ un polinomio y unos elementos $a, b \in R$ tales que $a < b$. Si $f(a) = f(b) = 0$, entonces existirá un elemento $c \in (a, b)$ que es raíz del polinomio derivada $f'$, es decir, $f'(c) = 0$.*

Proposición A.19. **(Teorema del Valor Medio)**
*Sean $R$ un cuerpo realmente cerrado, $f \in R[X]$ un polinomio y unos elementos $a, b \in R$ tales que $a < b$. Entonces existe $c \in (a, b)$ tal que $f(b) - f(a) = (b - a)f'(c)$.*

Prosigamos con algunos resultados sobre el conteo de raíces para cuerpos realmente cerrados. Mostraremos una versión más general del clásico Teorema de Sturm, que es la que se utiliza en [**BCR, 1998**] para probar el Pincipio de Tarski-Seidenberg 1.2.3. Se basa en la definición siguiente.

Definición 40. **(Sucesión de Sturm)**
*Sea $R$ un cuerpo realmente cerrado. Sean $f, g \in R[X]$. Se define la sucesión de Sturm de $f, g$ como la sucesión finita de polinomios $f_0, \ldots, f_r$ que satisface:*

- *(i)* $f_0 = f$,
- *(ii)* $f_1 = f'g$,
- *(iii)* $f_i = f_{i-1}q_i - f_{i-2}$, *donde* $q_i \in R[X]$ *y* $deg(f_i) < deg(f_{i-1}) < deg(f_{i-2})$, *para cada* $i = 2, \ldots, r$,
- *(iv)* $f_r = gcd(f, f'g)$.

Al ser $R$ un cuerpo, se observa que $R[X]$ es un dominio euclídeo junto con la función que asigna a cada polinomio su grado, y entonces puede obtenerse la sucesión de Sturm de $f, g$ aplicando el Algoritmo de Euclides a $f$ y $f'g$. Ahora, si consideramos una sucesión finita de elementos de

un cuerpo realmente cerrado $R$, sea esta $a_0, \ldots, a_r$ y con $a_0 \neq 0$, se define el número de cambios de signo de la sucesión como el cardinal del siguiente conjunto:

$$\{(a_i, a_j) \in \{a_0, \ldots, a_r\} \times \{a_0, \ldots, a_r\} : i < j,\ i < k < j \Rightarrow a_k = 0,\ a_i a_j < 0\},$$

que esencialmente son los cambios de signo pero despreciando a los ceros de la sucesión. Con las notaciones de la Definición 40, se considera $a \in R$ tal que $f(a) \neq 0$ y se denota por $v(f, g; a)$ al número de cambios de signo de la sucesión $f_0(a), \ldots, f_r(a)$. Con todo esto pasamos a enunciar sin demostrar el siguiente resultado de Sylvester que generaliza al Teorema de Sturm, y que mostramos inmediatamente después como un corolario del primero.

Teorema A.20. **(de Sturm Extendido (por Sylvester))**
*Sea $R$ un cuerpo realmente cerrado y sean $f, g \in R[X]$. Sean $a, b \in R$ tales que $a < b$ y $f(a), f(b) \neq 0$. Entonces, la diferencia entre el número de raíces de $f$ en el intervalo $(a, b)$ para las que $g$ sea positivo y el número de raíces de $f$ en el mismo intervalo para las que $g$ sea negativo es igual a $v(f, g; a) - v(f, g; b)$.*

Corolario A.21. **(Teorema de Sturm)**
*Sea $R$ un cuerpo realmente cerrado y sea $f \in R[X]$. Sean $a, b \in R$ tales que $f(a), f(b) \neq 0$ y $a < b$. Entonces el número de raíces de $f$ en el intervalo $(a, b)$ es igual a $v(f, 1; a) - v(f, 1; b)$.*

Añadimos otro resultado que es una cota al número de raíces en un cuerpo realmente cerrado $R$ que presenta un polinomio de $R[X]$.

Lema A.22. **(de Descartes)**
*Sea $R$ un cuerpo realmente cerrado y sea $f \in R[X]$ un polinomio que pueda escribirse como $f(X) = a_n X^n + \ldots + a_k X^k$ y con $a_n, a_k \neq 0$. Entonces, el número de raíces de $f$ en $R$ está superiormente acotado por el número de cambios de signo en la sucesión finita $a_n, \ldots, a_k$.*

Con este pequeño recopilatorio de propiedades del Análisis Real, queda ejemplificada la utilidad de la idea de cuerpo realmente cerrado. Sin embargo, no es cierto que toda propiedad de los números reales se cumpla también para un cuerpo realmente cerrado cualquiera. Sin ir más lejos, $\mathbb{Q}$ es denso en $\mathbb{R}$, pero no se cumple que $\mathbb{Q}$ sea denso en $R$ para un cuerpo realmente cerrado cualquiera, y basta con ver el cuerpo $\mathbb{R}(X)$ del Ejemplo A.16.

Visto desde otra perspectiva, el conjunto $\mathbb{R}$ de los números reales puede definirse, salvo isomorfismo de cuerpos, como el conjunto que satisface los axiomas de cuerpo ordenado (esto es, las propiedades con las que se define a un cuerpo ordenado) y una propiedad adicional que se conoce como el Axioma de Completitud o el Axioma del Supremo. Queda enunciado a continuación para el cuerpo de los reales.

Axioma A.23. **(de Completitud en $\mathbb{R}$)**
*Para todo subconjunto de $\mathbb{R}$ acotado superiormente existe un supremo en $\mathbb{R}$. Se dice que $\mathbb{R}$ es un cuerpo ordenado completo al satisfacer esta propiedad.*

Es evidente que los números racionales no satisfacen esta propiedad, pues el conjunto $(0, \sqrt{2}) \cap \mathbb{Q}$ (entendiendo que el intervalo se define sobre $\mathbb{R}$) está acotado y no posee un supremo en $\mathbb{Q}$. El Axioma de Completitud es, junto con los axiomas de cuerpo ordenado, la base sobre la que se desarrolla el Análisis Real y que puede cumplirse o no para cuerpos realmente cerrados en general. Notemos que no estamos hablando de cuerpos ordenados sino de cuerpos realmente cerrados. Esta noción se acerca más a las propiedades de $\mathbb{R}$, ya que por ejemplo permite definir una norma y una topología euclídea (véase el Apéndice E), pero un cuerpo realmente cerrado tampoco llega a ser un cuerpo ordenado completo, en general, como sí lo es $\mathbb{R}$. Hemos visto algunos ejemplos de propiedades que no necesitan de este Axioma de Completitud, ya que sirven para cuerpos realmente cerrados en general. Veamos una propiedad que no satisfacen los cuerpos ordenados en general y que necesita del Axioma de Completitud para probarse.

Definición 41. **(Cuerpo Ordenado Arquimediano)**
*Sea $(F, \leq)$ un cuerpo ordenado. Se dice que dicho cuerpo ordenado es arquimediano y que su ordenación es arquimediana si se cumple que para cada $x \in F$ existe $k \in \mathbb{N}$ tal que $x < k1$.*

El cuerpo $\mathbb{R}$ es claramente arquimediano, mientras que en $\mathbb{R}(X)$ (véase el Ejemplo A.16) existirá alguna cota superior de $\mathbb{N}$, por ejemplo, $X > n$ escogiendo la ordenación adecuada. Este tipo de elementos de un cuerpo ordenado se nombran de cierta manera.

DEFINICIÓN 42. **(Elemento Infinito e Infinitésimo)**
*Sea $(F, \leq)$ un cuerpo ordenado y sea $x \in F$. El elemento $x$ se dice infinito si es una cota superior de $\mathbb{N}$ en $F$, es decir, si para cualquier $k \in \mathbb{N}$ se cumple que $k1 \leq x$. El elemento $x$ se dice infinitésimo si para cada $k \in \mathbb{N}$ se sigue que $0 \leq kx \leq 1$.*

Se observa que los elementos infinitos y los infinitésimos son siempre elementos no negativos y que 0 es un infinitésimo. Ocurre que los elementos infinitos aparecen cuando el cuerpo ordenado no es arquimediano. Puede hallarse las siguientes propiedades equivalentes con la arquimedianidad de un cuerpo ordenado.

PROPOSICIÓN A.24. *Sea $(F, \leq)$ un cuerpo ordenado. Entonces, son equivalentes:*

- *(i)* $\mathbb{N}$ *no está acotado en $F$, es decir, no existen elementos infinitos en $F$,*
- *(ii)* $0$ *es el único infinitésimo de $F$,*
- *(iii) para cada $x, y \in F$ tales que $x < y$ existe algún $n/m \in \mathbb{Q}$ tal que $x < (n1)/(m1) < y$,*
- *(iv) $(F, \leq)$ es un cuerpo ordenado arquimediano.*

La Propiedad *(iii)* de la proposición precedente significa que la copia isomorfa de $\mathbb{Q}$ de un cuerpo $F$ ordenado cualquiera es un conjunto denso en $F$, y resulta ser que esta propiedad es equivalente con la arquimedianidad del cuerpo ordenado. Para el caso de $\mathbb{R}$, ambas propiedades se siguen del Axioma de Completitud. Cabe preguntarse si se cumple el recíproco para un cuerpo ordenado en general, y la respuesta es negativa.

TEOREMA A.25. *Sea $(F, \leq)$ un cuerpo ordenado arquimediano. Entonces existe algún subcuerpo $H \subset \mathbb{R}$ con una ordenación $\preceq$ que respeta a la de $\mathbb{R}$ y tal que $(F, \leq)$ y $(H, \preceq)$ son cuerpos ordenados isomorfos. En particular, todo cuerpo realmente cerrado arquimediano será isomorfo a $\mathbb{R}$ y el isomorfismo entre ambos será único.*

Recapitulando, se tiene que la Propiedad de Completitud de $\mathbb{R}$ conduce a la Propiedad de Arquimedianidad, la cual dada sobre un cuerpo ordenado cualquiera equivale a que $\mathbb{Q}$ sea denso en dicho cuerpo. No sucede que, para un cuerpo ordenado cualquiera, se deduzca la Propiedad de Completitud a partir de su arquimedianidad, esto ocurre únicamente en el caso en que dicho cuerpo ordenado sea realmente cerrado. En tal caso, existirá un único isomorfismo de dicho cuerpo realmente cerrado arquimediano con $\mathbb{R}$, y por ello decimos que $\mathbb{R}$ se define como el único cuerpo realmente cerrado arquimediano, que lo es salvo isomorfismo de cuerpos.

En definitiva, los cuerpos realmente cerrados se distinguen de $\mathbb{R}$ en la Propiedad Arquimediana y por ello los resultados del Análisis Real no son siempre ciertos para cuerpos realmente cerrados. Existe una rama de las matemáticas conocida como Análisis No Normal que se inició con el texto de 1966 titulado *"Nonstandard Analysis"* y escrito por A. Robinson, el cual trata de probar los resultados del Análisis Real en cuerpos ordenados no arquimedianos y que, por ejemplo, logra dar unas nociones de continuidad y derivabilidad usando el Principio de Transferencia 1.2.5.

Apéndice B

# Anillos de Fracciones y Localización.

Este apéndice es una introducción muy elemental a los anillos de fracciones y anillos locales, al nivel que necesitaremos en el resto del texto. Fundamentalmente, se ha seguido el hilo argumental de los Capítulos 6 y 7 de [**Tabera, 2023**], y también se ha inspirado en algunas partes del Capítulo 5 de [**Sharp, 1990**] y el Capítulo 3 de [**AtMac, 1969**].

Antes de empezar, resulta conveniente aclarar la notación sobre ideales extendidos y contraídos por un morfismo de anillos. Dados un par de anillos $A$, $B$ y un morfismo $f : A \to B$, se define el contraído de un ideal $\mathfrak{b} \subset B$ por el morfismo $f$ como $f^{-1}(\mathfrak{b})$, que siempre será un ideal. También se define el ideal extendido de un ideal $\mathfrak{a} \subset A$ por el morfismo $f$ como $f(\mathfrak{a})$. Si el morfismo $f$ se sobrentiende por el contexto, simplemente se denotarán por $\mathfrak{b}^c = f^{-1}(\mathfrak{b})$ y $\mathfrak{a}^e = f(\mathfrak{a})$. Para el caso en que $A \subset B$, ocurre que $\mathfrak{b}^c = \mathfrak{b} \cap A$ y que $\mathfrak{a}^e = \mathfrak{a}B$, por lo que será habitual expresar con esta 'notación' al contraído y al extendido de los ideales $\mathfrak{b}$ y $\mathfrak{a}$, respectivamente. Incluso aunque el morfismo considerado no sea inyectivo.

**Anillos de Fracciones.**

Dado un dominio de integridad $D$, esto es, un anillo conmutativo sin divisores de cero distintos de 0, se tiene la siguiente relación de equivalencia sobre $D \times (D \setminus \{0\})$:

$$(a, s) \sim (b, t) \Leftrightarrow at - bs = 0,$$

dados $(a, s), (b, t) \in D \times (D \setminus \{0\})$. Denotemos este conjunto por $Frac(D)$ y, junto con las siguientes operaciones de suma y producto de sus clases:

$$(a, s) + (b, t) = (at + bs, st), \qquad (a, s) \cdot (b, t) = (ab, st),$$

se tiene una estructura de cuerpo conocida como el cuerpo de fracciones de $D$. Esta es la construcción por la que puede definirse el cuerpo $\mathbb{Q}$ de los números racionales a partir del dominio de los números enteros $\mathbb{Z}$, y es habitual denotar la clase de equivalencia a la que pertenece $(a, s)$ por $a/s$.

Si tratamos de generalizar esta relación a un anillo conmutativo $A$ cualquiera, aparecen problemas por la presencia de divisores de cero. En primer lugar se necesitará que las operaciones de las clases estén bien definidas, y para ello se requiere que el conjunto de los cocientes sea multiplicativamente cerrado. Esto motiva la siguiente definición.

Definición 43. **(Sistema Multiplicativamente Cerrado)**
*Sea $A$ un anillo conmutativo y sea $S$ un subconjunto de $A$. $S$ se dice sistema multiplicativamente cerrado, SMC de forma abreviada, si cumple que:*

(*i*) $1 \in S$,
(*ii*) *si* $s, t \in S$, *entonces* $st \in S$.

El siguiente paso a dar es retocar la relación para que sea de equivalencia. Un SMC no es un grupo multiplicativo y en consecuencia no se tiene la Ley de Cancelación para el producto, de la que se sigue la Propiedad Transitiva en la correspondencia dada anteriormente. Esto se soluciona considerando, en su lugar, la relación siguiente sobre $A \times S$:

$$(a, s) \sim (b, t) \Leftrightarrow \exists u \in S \text{ tales que } u(at - bs) = 0,$$

con $(a, s), (b, t) \in A \times S$. Nuevamente, se utilizará la notación $a/s = [(a, s)]_\sim$. La relación dada es de equivalencia, y sus clases de equivalencia tienen estructura de grupo respecto de las operaciones descritas, lo hemos enunciado a continuación.[1]

[1] Puede verse la prueba de estas afirmaciones en el Lema 5.1 de [**Sharp, 1990**].

PROPOSICIÓN B.1. **(Anillo de Fracciones)**
*Sea $A$ un anillo conmutativo y sea $S$ un SMC de $A$. Entonces, el conjunto de las clases de equivalencia de la relación $\sim$ definida previamente sobre $A \times S$ es un anillo para las operaciones siguientes:*

$(i)$ $\dfrac{a}{s} + \dfrac{b}{t} = \dfrac{at + sb}{st}$,

$(ii)$ $\dfrac{a}{s} \cdot \dfrac{b}{t} = \dfrac{ab}{st}$,

*para cada $(a, s), (b, t) \in A \times S$. Dicho anillo se llamará anillo de fracciones de $A$ respecto de $S$ y se denotará por $S^{-1}A$.*

OBSERVACIÓN B.2. Si $0 \in S$, el anillo de fracciones $S^{-1}A$ será el anillo trivial. También, si una pareja de divisores de cero $a, b$ no nulos tales que $ab = 0$ pertenecen al SMC con el que se define el anillo, entonces este será el anillo trivial por el mismo motivo.

Veamos algunos ejemplos de SMC y por consiguiente, distintos anillos de fracciones para anillos conmutativos.

EJEMPLO B.3. *Para un anillo conmutativo $A$, puede darse los siguientes ejemplos de SMR:*

(I) *Dado un elemento $a \in A$, se tiene el siguiente SMC:*

$$S = \{a^k : k \in \mathbb{N}\}.$$

*Se denotará $A_a = S^{-1}A$.*

(II) *Sea $\mathfrak{a}$ un ideal de $A$, se considera la clase lateral $1 + \mathfrak{a}$, es decir, la clase del $1$ que define el cociente $A/\mathfrak{a}$. Se tiene que $1 + \mathfrak{a}$ es un SMC de $A$.*

(III) *Dado un ideal primo $\mathfrak{p} \in Spec(A)$, se tiene que $A \setminus \mathfrak{p}$ es un SMC. Recíprocamente, si $S = A \setminus \mathfrak{a}$ es un SMC con $\mathfrak{a}$ un ideal de $A$, entonces $\mathfrak{a}$ será ideal primo de $A$. Se define el anillo $A$ localizado en un ideal $\mathfrak{p} \in Spec(A)$ como el anillo $A_{\mathfrak{p}} = (A \setminus \mathfrak{p})^{-1}A$.*

(IV) *El conjunto de los no divisores de cero de un anillo es un SMC.*

Ocurre que un par de SMC distintos pueden dar lugar al mismo anillo de fracciones. De entre todos los SMC que definen a un mismo anillo de fracciones, se distingue aquel que contiene una mayor cantidad de cocientes, en el sentido de que satisface el recíproco de la Propiedad $(ii)$ de la Definición 43. Le daremos un nombre especial.

DEFINICIÓN 44. **(Sistema Multiplicativamente Cerrado Saturado)**
*Sea $A$ un anillo conmutativo y sea $S$ un subconjunto de $A$. $S$ se dice saturado, SMCS de forma abreviada, si es un SMC que además satisface:*

$$st \in S \Rightarrow s, t \in S \text{ para cualesquiera } s, t \in A.$$

No todo SMC tiene como complementario a un ideal primo, ni tampoco a un ideal (ver el Ejemplo B.3, Apartado (II)). Los SMCS tampoco cumplen esta propiedad, pero pueden caracterizarse por tener un complementario que sea unión finita de ideales primos.

PROPOSICIÓN B.4. *Sea $A$ un anillo conmutativo. Un subconjunto $S \subset A$ es SMC saturado si y solamente si su complementario es unión finita de ideales primos, es decir, si:*

$$A \setminus S = \bigcup_{i=1}^{r} \mathfrak{p}_i \text{ para algunos } \mathfrak{p}_1, \ldots, \mathfrak{p}_r \in Spec(A).$$

En consecuencia, se cumple que la intersección finita de SMC saturados es también un SMC saturado, sin más que aplicar las Leyes de Morgan. En general, se tiene que la intersección arbitraria de SMC sea un SMC, y además ocurre que la intersección de todos los SMC que contengan a otro SMC, llámese $S$, tiene como resultado un SMCS que define al mismo anillo de fracciones que define $S$. Enunciemos esto último junto a la siguiente definición.

PROPOSICIÓN B.5. *Sea $A$ un anillo conmutativo y sea $S$ un SMC de $A$. Se define el siguiente conjunto:*

$$\overline{S} = \bigcap_{\substack{S \subset T \\ T \subset A \text{ es SMC}}} T.$$

*Entonces, $\overline{S}$ es un SMCS de $A$ tal que $\overline{S}^{-1}A = S^{-1}A$. Se dice saturación de $S$ a $\overline{S}$.*

De todo lo expuesto, se observa que la saturación de un SMC puede simplemente escribirse como el complementario de la unión de los ideales primos que contengan algún elemento de dicho SMC. Lo escribimos.

COROLARIO B.6. *Sea $S$ un SMC de un anillo conmutativo $A$. Entonces su saturación $\overline{S}$ es un SMCS de $A$ que puede escribirse como:*

$$\overline{S} = A \setminus \bigcup_{\substack{\mathfrak{p}\in Spec(A)\\ \mathfrak{p}\cap S=\emptyset}} \mathfrak{p}.$$

En la prueba de la Proposición B.5 resultaría conveniente contar con alguna propiedad que diga que si $S \subset T \subset A$ son un par de SMC del anillo conmutativo $A$, entonces $S^{-1}A \subset T^{-1}A$; pero esto es falso. Puede verse si construimos el morfismo natural de un anillo conmutativo $A$ en algún anillo de fracciones $S^{-1}A$, que no siempre será inyectivo. Dicho morfismo sería:

$$\begin{aligned} \phi : A &\longrightarrow S^{-1}A \\ a &\longmapsto \frac{a}{1}, \end{aligned}$$

el cual se conoce como morfismo natural o canónico de $A$ en su anillo de fracciones $S^{-1}A$. Los anillos de fracciones, al igual que los anillos cociente o los anillos de polinomios, tienen una Propiedad Universal que vemos a continuación.

TEOREMA B.7. **(Propiedad Universal del Anillo de Fracciones)**
*Sean $A$ y $B$ un par de anillos conmutativos. Sea $S$ un SMC de $A$. Consideramos un morfismo de anillos $\psi : A \to B$ y el morfismo natural $\phi$ de $A$ en el anillo de fracciones $S^{-1}A$. Si $\psi$ cumple que $\psi(x)$ es una unidad de $B$ para cada $x \in S$, entonces existe un único morfismo $\psi'$ de $S^{-1}A$ en $B$ tal que $\psi = \psi' \circ \phi$, y además viene dado por $\psi'(a/s) = \psi(a)\psi^{-1}(s)$.*

Los ideales extendidos por el morfismo natural de $A$ en $S^{-1}A$ son de la siguiente forma.

PROPOSICIÓN B.8. *Sea $A$ un anillo conmutativo y $S$ un SMC de $A$. Sea $\mathfrak{a}$ un ideal de $A$ y consideramos el ideal $\mathfrak{a}^e$ extendido por el morfismo natural de $A$ en $S^{-1}A$. Entonces:*

$$\mathfrak{a}^e = \{x \in S^{-1}A : x = \frac{a}{s}, a \in \mathfrak{a}, s \in S\}.$$

Esta propiedad permite ver que los ideales de $S^{-1}A$ son los extendidos de ideales de $A$. Puede verse además que el extendido de un ideal finitamente generado es finitamente generado y que, por lo tanto, si $A$ es un anillo noetheriano, también lo será $S^{-1}A$.

La Proposición B.8 dice que un elemento pertenece al ideal extendido cuando tiene alguna representación con el numerador en el ideal. En el caso de un ideal primo que no posea denominadores, puede verse que esto ocurre para cualquier representación.

PROPOSICIÓN B.9. *Sea $A$ un anillo conmutativo y $S$ un SMC de $A$. Sea $\mathfrak{p} \in Spec(A)$ un ideal primo tal que $\mathfrak{p} \cap S = \emptyset$. Dado $a/s \in \mathfrak{p}^e$, se tiene que $a \in \mathfrak{p}$.*

Esta propiedad de los ideales primos que no contienen denominadores, permite dar la siguiente descripción del espectro primo del anillo de fracciones.

TEOREMA B.10. *Sea $A$ un anillo conmutativo y $S \subset A$ un SMC. Entonces, se tiene la siguiente aplicación biyectiva:*

$$\begin{aligned} \left\{ \begin{array}{c} \textit{ideales primos de } A \\ \textit{sin elementos de } S \end{array} \right\} &\longrightarrow Spec(S^{-1}A) \\ \mathfrak{p} &\longmapsto \mathfrak{p}^e, \end{aligned}$$

*donde la extensión de los ideales de $A$ es la dada por el morfismo natural de $A$ en $S^{-1}A$.*

Nótese que la localización $A_{\mathfrak{p}}$ de un anillo $A$ por un ideal primo $\mathfrak{p}$ es un anillo cuyo espectro primo describe a los ideales primos de $A$ que están contenidos en $\mathfrak{p}$. En cambio, el anillo cociente $A/\mathfrak{p}$ tiene un espectro primo que describe a los ideales primos de $A$ que contienen a $\mathfrak{p}$ (véase la Proposición C.1).

**Anillos Locales y Propiedades Locales.**

En este apartado se introduce a los anillos locales, junto con varios ejemplos destacables y algunas propiedades. Se hace énfasis en la idea de propiedad local y se introduce como ejemplo a los anillos catenarios.

DEFINICIÓN 45. **(Anillo Local)**
*Un anillo conmutativo $A$ se dice local si posee un único ideal maximal $\mathfrak{m}$, y en tal caso se denota por $(A, \mathfrak{m})$ al anillo local. Se dice cuerpo residual de $(A, \mathfrak{m})$ al cuerpo $k(\mathfrak{m}) = A/\mathfrak{m}$.*

Veamos algunos ejemplos de anillos locales.

EJEMPLO B.11. *Los siguientes son ejemplos de anillos locales:*

(I) $(K, (0))$ *donde $K$ es cualquier cuerpo.*
(II) *El anillo $A$ localizado en $\mathfrak{p} \in Spec(A)$, es decir, $A_{\mathfrak{p}}$ con la notación introducida en el Apartado* (III) *del Ejemplo B.3, es un anillo local de maximal $\mathfrak{p}^e = \mathfrak{p}A_{\mathfrak{p}}$ y cuyo cuerpo residual es isomorfo al cuerpo de fracciones de $A/\mathfrak{p}$.*
(III) $(\mathbb{Z}_p, (p))$*, donde $p$ es un elemento primo de $\mathbb{Z}$ y se utiliza la notación del Apartado* (I) *del Ejemplo B.3.*
(IV) *Dado un cuerpo $K$, se tiene el anillo local $(K[X_1, \ldots, X_n]_{\mathfrak{m}_x}, \mathfrak{m}_x^e)$ donde $\mathfrak{m}_x$ se define como el ideal maximal $(X_1 - x_1, \ldots, X_n - x_n)$ de $K[X_1, \ldots, X_n]$ dado por un elemento $x = (x_1, \ldots, x_n) \in K^n$.*

Los anillos locales cumplen con la siguiente caracterización.

PROPOSICIÓN B.12. *Un anillo conmutativo $A$ es local si y solamente si el conjunto de sus no unidades es un ideal, en cuyo caso sería el ideal maximal del anillo.*

Una propiedad de los anillos de fracciones, como ya se dijo, es que se preserva la noetherianidad. En particular, la localización preserva la noetherianidad.

PROPOSICIÓN B.13. *Sea $A$ un anillo conmutativo noetheriano y sea $\mathfrak{p} \in Spec(A)$ un ideal primo. Entonces el anillo localizado $(A_{\mathfrak{p}}, \mathfrak{p}A_{\mathfrak{p}})$ es un anillo local noetheriano.*

Cabe preguntarse si el hecho de que todas las localizaciones de un anillo sean anillos noetherianos locales implica que el propio anillo sea noetheriano necesariamente. Existe un resultado clásico de Nagata que responde afirmativamente para un caso particular de anillos, y es el siguiente.[2]

PROPOSICIÓN B.14. *Sea $A$ un anillo conmutativo y supongamos que se cumple que:*

*(i) el anillo local $A_{\mathfrak{m}}$ es noetheriano para cada $\mathfrak{m} \in MaxSpec(A)$,*
*(ii) todo elemento $a \in A$ está contenido en un número finito de ideales maximales.*

*Entonces, $A$ es un anillo noetheriano.*

De los dos últimos resultados se sigue un corolario para el caso particular de anillos semilocales. Definamos primero a estos anillos y veamos seguidamente el resultado.

DEFINICIÓN 46. **(Anillo Semilocal)**
*Un anillo conmutativo $A$ se dice semilocal si posee una cantidad finita de ideales maximales. Se denota al anillo semilocal por $(A, \mathfrak{m}_1, \ldots, \mathfrak{m}_r)$, siendo que $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\} = MaxSpec(A)$.*

COROLARIO B.15. *Sea $(A, \mathfrak{m}_1, \ldots, \mathfrak{m}_r)$ un anillo semilocal. Entonces, son equivalentes:*

*(i) El anillo $(A, \mathfrak{m}_1, \ldots, \mathfrak{m}_r)$ es noetheriano.*
*(ii) Para cualquier ideal primo $\mathfrak{p} \in Spec(A)$, el anillo local $(A_{\mathfrak{p}}, \mathfrak{p}A)$ es noetheriano.*
*(iii) Para cualquier ideal maximal $\mathfrak{m} \in MaxSpec(A)$, el anillo local $(A_{\mathfrak{m}}, \mathfrak{m}A)$ es noetheriano.*

El resultado precedente es un ejemplo de propiedad local para anillos semilocales. Llamaremos propiedades locales, sobre una clase de anillos determinada, a aquellas propiedades que se preserven por localización y viceversa, es decir, una propiedad se dice local si, cuando se cumple para un anillo $A$, esta se cumple para cualquiera de sus localizaciones $A_{\mathfrak{p}}$ por un ideal primo $\mathfrak{p} \in Spec(A)$ y viceversa. Otro ejemplo de propiedad local, algo trivial quizá, es la propiedad de trivialidad de un anillo. Veamos lo que quiere decir esto.

[2]Puede verse una prueba en el *Example 1* del Apéndice 1 de [**Nagata, 1927**].

PROPOSICIÓN B.16. *Sea $A$ un anillo conmutativo. Las siguientes propiedades son equivalentes:*

(*i*) *El anillo $A$ es trivial, esto es, $A = 0$.*
(*ii*) *Para cualquier ideal primo $\mathfrak{p} \in Spec(A)$, el anillo local $(A_{\mathfrak{p}}, \mathfrak{p}A)$ es trivial.*
(*iii*) *Para cualquier ideal maximal $\mathfrak{m} \in MaxSpec(A)$, el anillo local $(A_{\mathfrak{m}}, \mathfrak{m}A)$ es trivial.*

Veamos otro ejemplo de propiedad local, como la catenaridad de anillos que utilizaremos en el Apéndice D. A continuación se define a los anillos con esta propiedad.

DEFINICIÓN 47. **(Anillo Catenario)**
*Un anillo conmutativo $A$ se dice catenario si para cada par de ideales primos $\mathfrak{p}, \mathfrak{q} \in Spec(A)$ tales que $\mathfrak{p} \subset \mathfrak{q}$ existe un entero $k \in \mathbb{N}$ tal que toda cadena de ideales primos de la forma:*

$$\mathfrak{p} = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_r = \mathfrak{q},$$

*cumple que $r \leq k$ y se da la igualdad si y solamente si la cadena es maximal, en el sentido de que no existe $\mathfrak{p}' \in Spec(A)$ tal que $\mathfrak{p}_{i-1} \subsetneq \mathfrak{p}' \subsetneq \mathfrak{p}_i$ para algún $i = 1, \ldots, r$.*

La idea de un anillo catenario está ligada a la de topología catenaria, en relación con la topología que se define sobre el espectro primo $Spec(A)$ que no comentaremos; y también guarda relación con la idea de dimensión de variedades algebraicas que se discute en los apéndices siguientes. De momento, lo relevante de la catenaridad de un anillo es que es una propiedad local, como nos muestra el siguiente enunciado.[3]

PROPOSICIÓN B.17. *Sea $A$ un anillo conmutativo. Las siguientes propiedades son equivalentes:*

(*i*) *El anillo $A$ es catenario.*
(*ii*) *Para cualquier ideal primo $\mathfrak{p} \in Spec(A)$, el anillo local $(A_{\mathfrak{p}}, \mathfrak{p}A)$ es catenario.*
(*iii*) *Para cualquier ideal maximal $\mathfrak{m} \in MaxSpec(A)$, el anillo local $(A_{\mathfrak{m}}, \mathfrak{m}A)$ es catenario.*

Otra propiedad evidente de los anillos catenarios se deduce de la biyección que existe entre los ideales primos del anillo cociente $A/\mathfrak{a}$, donde $A$ es un anillo conmutativo y $\mathfrak{a} \subset A$ un ideal, y los ideales primos de $A$ que contienen a $\mathfrak{a}$ (véase de nuevo la Proposición C.1).

PROPOSICIÓN B.18. *Sea $A$ un anillo conmutativo y sea $\mathfrak{a} \subset A$ un ideal. Se cumple que si $A$ es catenario, entonces $A/\mathfrak{a}$ también es catenario.*

No entraremos en detalles sobre la teoría que hay detrás de los anillos catenarios, sobre la cual puede verse el monográfico de A. Bot.[4] Ahí se prueba el siguiente resultado.

TEOREMA B.19. *Sea $A$ un anillo conmutativo. Si $A$ es finitamente generado sobre un cuerpo $K$ o sobre el dominio $\mathbb{Z}$ de los enteros, entonces $A$ es un anillo catenario.*

De este resultado se sigue que los anillos de polinomios $K[X_1, \ldots, X_n]$ construidos sobre un cuerpo $K$ son catenarios. En el citado trabajo también se prueba un resultado sobre dimensión para anillos catenarios, el cual añadiremos como observación en el Apéndice C.

Resulta laborioso hablar de propiedades locales sin introducir la terminología de módulos. Puede consultarse la sección sobre propiedades locales en el Capítulo 3 de [**AtMac, 1969**] para ver algunos ejemplos más de propiedades locales. También puede verse la subsección de anillos locales regulares en el Apéndice D, donde se presenta el Teorema de Serre D.8 que asegura que la regularidad de los anillos locales noetherianos es una propiedad local.

[3] Puede consultarse la prueba en: https://stacks.math.columbia.edu/tag/00NH.
[4] A. Bot, *"Catenary rings"*. ETH Zürich, proyecto de fin de carrera, Octubre 2017.

Apéndice C

# Teoría de la Dimensión en Anillos.

En esta sección se desarrolla lo más básico de la Teoría de la Dimensión para anillos conmutativos. Simplemente revisaremos las nociones más básicas, y también algunas propiedades sacadas de diversos resultados como los Teoremas del Ascenso y del Descenso, el Lema de Normalización de Noether y el Teorema de Intercambio de Steinitz. Este último debe asociarse a las ideas de base y de grado de trascendencia. Dejaremos para el apéndice siguiente otros temas relacionados. Antes de empezar, resultará útil no perder de vista los resultados de localización de anillos que se encuentran en el Apéndice B y también el siguiente resultado de la Teoría de Ideales.

Si consideramos un anillo conmutativo $A$ y algún ideal $\mathfrak{a} \subset A$, se tendrá la construcción del anillo cociente $A/\mathfrak{a}$ acompañada de un morfismo $\pi : A \to A/\mathfrak{a}$ conocido como la proyección en el anillo cociente. En este contexto, se tiene la siguiente biyección que describe al espectro primo del anillo cociente.

PROPOSICIÓN C.1. *Sea $A$ un anillo conmutativo y sea $\mathfrak{a}$ un ideal. Entonces, la siguiente aplicación es biyectiva:*

$$\begin{aligned} \{\mathfrak{p} \in Spec(A) : \mathfrak{p} \supset \mathfrak{a}\} &\longrightarrow Spec(A/\mathfrak{a}) \\ \mathfrak{p} &\longmapsto \mathfrak{p}/\mathfrak{a}, \end{aligned}$$

donde la imagen de un ideal primo de $A$ por esta aplicación será el ideal extendido por el morfismo $\pi$. Otro contexto que nos interesa será el de una extensión de anillos, es decir, un par de anillos conmutativos $A$ y $B$ y un morfismo inyectivo $\tilde{\imath} : A \to B$, que es la inclusión de $A$ en $B$. Cometiendo un abuso de notación, puede denotarse a la extensión de anillos por $A \subset B$, y también al extendido $\mathfrak{a}^e$ de un ideal $\mathfrak{a} \subset A$ por $\mathfrak{a}$ (en lugar de $\tilde{\imath}(\mathfrak{a})$). En la misma línea, se denota al contraído $\mathfrak{b}^c$ de un ideal $\mathfrak{b} \in B$ por $\mathfrak{b} \cap A$.

Este apéndice se ha elaborado con base en la siguiente bibliografía. Los apartados sobre la Dimensión de Krull y el Lema de Normalización de Noether pueden encontrarse en el Capítulo 2 de [**Kunz, 1985**]. La presentación de los Teoremas del Ascenso y del Descenso se ha basado en el Capítulo 5 de [**AtMac, 1969**]. El último apartado, que introduce las bases y el grado de trascendencia, puede seguirse en el Capítulo 18 de [**Stewart, 1972**]. La breve nota sobre la Teoría de Ideales que se ha hecho durante esta introducción puede verse y ampliarse en el Capítulo 3 de [**Sharp, 1990**].

### Dimensión de Krull de un Anillo.

En este apartado se introducen los conceptos de altura y co-altura de un ideal primo y la dimensión de Krull de un anillo. Seguidamente veremos algunas propiedades básicas de estas definiciones, y al final, se extiende las nociones de altura y co-altura a ideales en general.

DEFINICIÓN 48. **(Altura y Co-Altura de un Ideal Primo)**
*Sea $A$ un anillo conmutativo y sea el ideal primo $\mathfrak{p} \in Spec(A)$. Se dice altura del ideal $\mathfrak{p}$ en $A$, y se denota por $ht(\mathfrak{p})$, al máximo $r \in \mathbb{N}$ para el que existe una cadena de ideales primos que cumpla:*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_r \subset \mathfrak{p}.$$

*Si no existe tal $r$, se define $ht(\mathfrak{p}) = +\infty$. También se define co-altura del ideal $\mathfrak{p}$ en $A$, y se denota por co-$ht(\mathfrak{p})$, al máximo $r \in \mathbb{N}$ tal que existe una cadena de ideales primos que cumpla:*

$$\mathfrak{p} \subset \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_r.$$

*Si no existe dicho $r$, se define co-$ht(\mathfrak{p}) = +\infty$.*

DEFINICIÓN 49. **(Dimensión de Krull de un Anillo)**
*Sea $A$ un anillo conmutativo. Se dice dimensión de Krull de $A$, y se denota por $dim_{Krull}(A)$, al máximo de los $r \in \mathbb{N}$ para los que existe alguna cadena de ideales primos tales que:*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_r.$$

*En caso de no existir dicho máximo, se define $dim_{Krull}(A) = +\infty$.*

De la propia definición se sigue que la altura de un ideal primo minimal es 1 y que la co-altura de un ideal maximal es 0. Una forma alternativa de definir la altura de un ideal surge de considerar que, dado $A$ un anillo conmutativo, el conjunto $Spec(A)$ tiene estructura de grafo orientado respecto a la relación de inclusión. Una cadena de ideales primos como la siguiente:

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_r,$$

es un camino de longitud $r$ del grafo orientado $(Spec(A), \subset)$. La proposición siguiente relaciona la dimensión de Krull con la longitud de un camino en el grafo.

PROPOSICIÓN C.2. *Sea el anillo conmutativo $A$. Entonces $dim_{Krull}(A)$ coincide con el máximo de las longitudes de los caminos del grafo orientado $(Spec(A), \subset)$.*

La altura de un ideal primo $\mathfrak{p}$ en un anillo conmutativo $A$ puede obtenerse como la dimensión del anillo localizado $A_{\mathfrak{p}}$, basado en la biyección del Teorema B.10 que relaciona a los ideales primos de $A$ contenidos en el ideal $\mathfrak{p}$ con el espectro primo del anillo localizado $A_{\mathfrak{p}}$.

PROPOSICIÓN C.3. *Sea $A$ un anillo conmutativo y sea $\mathfrak{p}$ un ideal primo de $A$. Entonces:*

$$ht(\mathfrak{p}) = dim_{Krull}(A_{\mathfrak{p}}).$$

Se tiene un resultado análogo para la co-altura de un ideal primo $\mathfrak{p}$ de $A$, al considerar la dimensión del anillo cociente $A/\mathfrak{p}$ y la correspondencia biyectiva de la Proposición C.1.

PROPOSICIÓN C.4. *Sea $A$ un anillo conmutativo y sea $\mathfrak{p}$ un ideal primo de $A$. Entonces:*

$$co\text{-}ht(\mathfrak{p}) = dim_{Krull}(A/\mathfrak{p}).$$

El resultado precedente puede usarse en un anillo cociente de un anillo noetheriano, de modo que la dimensión de dicho anillo vendrá dada por las co-alturas de los primos asociados al ideal por el que se cocienta (véase el Teorema de Lasker-Noether 1.3.4).

PROPOSICIÓN C.5. *Sea $\mathfrak{a}$ un ideal de un anillo noetheriano $A$, con primos asociados $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Entonces, se satisface las siguientes igualdades:*

$$dim_{Krull}(A/\mathfrak{a}) = \max_{i=1,\ldots,r}(\{dim_{Krull}(A/\mathfrak{p}_i)\}) = \max_{i=1,\ldots,r}(\{co\text{-}ht(\mathfrak{p}_i)\}).$$

Para terminar con esta lista de propiedades sobre la altura de ideales primos, añadimos el siguiente resultado para anillos locales.

PROPOSICIÓN C.6. *Sea $A$ un anillo local de maximal $\mathfrak{m}$. Entonces:*

$$dim_{Krull}(A) = ht(\mathfrak{m}) = co\text{-}ht((0)).$$

Ahora, ampliaremos la definición de altura y co-altura a un ideal cualquiera de un anillo.

DEFINICIÓN 50. **(Altura y Co-Altura de un Ideal)**
*Sea $A$ un anillo conmutativo y sea $\mathfrak{a}$ un ideal de $A$. Se define la altura de $\mathfrak{a}$ en $A$ y se denota por:*

$$ht(\mathfrak{a}) = inf\left(\{ht(\mathfrak{p}) : \mathfrak{p} \in Spec(A), \mathfrak{a} \subset \mathfrak{p}\}\right).$$

*Se define también la co-altura de $\mathfrak{a}$ en $A$ y se denota por:*

$$co\text{-}ht(\mathfrak{a}) = max\left(\{co\text{-}ht(\mathfrak{p}) : \mathfrak{p} \in Spec(A), \mathfrak{a} \subset \mathfrak{p}\}\right).$$

En este caso, $A \setminus \mathfrak{a}$ no es un sistema multiplicativamente cerrado y no puede generalizarse la Proposición C.3 a cualquier ideal. Sin embargo, sí ocurre que la co-altura del ideal $\mathfrak{a}$ en $A$ coincide con la dimensión de Krull del anillo cociente $A/\mathfrak{a}$, en analogía con la Proposición C.4. Para concluir, se añade la siguiente desigualdad.

PROPOSICIÓN C.7. *Sea $A$ un anillo conmutativo y $\mathfrak{a} \subset A$ un ideal. Entonces se cumple que:*

$$ht(\mathfrak{a}) + co\text{-}ht(\mathfrak{a}) \leq dim_{Krull}(A).$$

Nótese que la igualdad ha de darse para algún ideal del anillo, a consecuencia de la propia definición de dimensión de Krull, pero que no necesariamente viene dada por cualquier ideal. Además, debe existir algún ideal primo $\mathfrak{p} \in Spec(A)$ para el que:

$$ht(\mathfrak{p}) + co\text{-}ht(\mathfrak{p}) = dim_{Krull}(A),$$

y dicha igualdad se satisface para cualquier ideal de cualquier cadena de primos de longitud maximal a la que pertenezca $\mathfrak{p}$. Esta igualdad se satisface para cualquier ideal primo si el anillo es catenario (se introducen en el Apéndice B), y en particular se cumple que la dimensión de Krull de un anillo catenario es la altura de cualquiera de sus ideales maximales.

**Extensiones Enteras.**

Aquí vamos a introducir las extensiones enteras, que son el paso previo a ver los Teoremas del Ascenso y del Descenso. Se trata de un tipo de extensiones de anillos que recuerda a las extensiones algebraicas de cuerpos. En lugar de elementos algebraicos sobre un cuerpo, se define un elemento entero sobre un anillo.

Definición 51. **(Elemento Entero)**
*Sea $A$ un anillo conmutativo y sea $B$ una extensión del anillo $A$, es decir, $A \subset B$. Un elemento $x \in B$ se dice entero sobre $A$ si existe algún polinomio $f$ mónico, univariado, no nulo, con coeficientes en $A$, y tal que $x$ sea una raíz de $f$ en $B[X]$.*

Dado este tipo de elementos, se define una extensión entera de forma similar a como se define una extensión algebraica de cuerpos.

Definición 52. **(Extensión Entera)**
*Sea el anillo $B$ una extensión del anillo $A$. $B$ se dice extensión entera de $A$ si todo elemento de $B$ es entero sobre $A$.*

En el caso de una extensión de cuerpos $H/F$, un elemento $x \in H$ entero sobre $F$ es un elemento algebraico sobre $F$ y viceversa. Es decir, las extensiones enteras de cuerpos serán las extensiones algebraicas y solo tendrá sentido considerar esta nueva noción para el caso de una extensión de dominios de integridad o de anillos conmutativos en general.

Ahora mostraremos una caracterización clásica de un elemento entero de una extensión de anillos, pero antes revisaremos lo que es un $A$-módulo finitamente generado. Si se tiene un $A$-módulo $M$ y tomamos alguna subfamilia $\mathcal{F} \subset M$, puede definirse el submódulo de $M$ generado por $\mathcal{F}$ como la intersección de todos los submódulos de $M$ que contienen a la familia $\mathcal{F}$, y por supuesto también a $A$, y se denotaría este submódulo por $A\langle\mathcal{F}\rangle$. El resultado siguiente nos dice qué forma tienen los elementos de este submódulo.[1]

Proposición C.8. *Sean $A$ un anillo conmutativo, $M$ un $A$-módulo y $\mathcal{F} \subset M$ un subconjunto. Entonces, puede describirse el $A$-módulo generado por $\mathcal{F}$ de la siguiente manera:*

$$A\langle\mathcal{F}\rangle = \left\{ \sum_{k=1}^{r} a_k m_k : r \in \mathbb{N}, a_1, \ldots, a_r \in A, m_1, \ldots, m_r \in M \right\}.$$

Se dirá que un $A$-módulo $M$ es finitamente generado cuando pueda tomarse una subfamilia finita $\{m_1, \ldots, m_r\} \subset M$ de elementos que generen a $M$, es decir, que cumplan la igualdad $M = A\langle\{m_1, \ldots, m_r\}\rangle$. En vista de la proposición precedente, los elementos de este módulo serían las combinaciones lineales de $m_1, \ldots, m_r$ con coeficientes en $A$. Notemos que el módulo $M$ finitamente generado es una $A$-álgebra finita, en contraposición con lo que se dice una $A$-álgebra finitamente generada (véase la Definición 9) que es isomorfa a un anillo generado por la evaluación del anillo de polinomios $A[X_1, \ldots, X_n]$ en algún elemento $x \in A^n$.[2] Además, si $A = K$ es un cuerpo, un $A$-módulo $M$ finitamente generado será un $K$-espacio vectorial y los generadores de $M$ como $A$-módulo son un sistema generador (no necesariamente una base) de $M$ como $K$-espacio vectorial. Retomando el tema que nos ocupa, enunciemos la caracterización de elementos enteros que se viene advirtiendo.

[1] Puede verse en la Proposición 2.2.13 de [**Pardo, 2023**].

[2] Nótese que tal morfismo de evaluación $ev_x$ define el ideal $ker(ev_x)$ y que son isomorfos $im(ev_x)$ y $A[X_1, \ldots, X_n]/ker(ev_x)$.

PROPOSICIÓN C.9. *Sea $A \subset B$ una extensión de anillos y sea $x \in B$. Entonces, son equivalentes:*

(*i*) *$x$ es entero sobre $A$,*
(*ii*) *$A[x]$ es un $A$-módulo finitamente generado,*
(*iii*) *existe $C$ subanillo de $B$ tal que $A \subset C$, $x \in C$ y $C$ es un $A$-módulo finitamente generado.*

El subconjunto de los elementos de $B$ que son enteros sobre $A$ definen a una extensión entera de $A$, como asegura el resultado siguiente.

COROLARIO C.10. *Sea $A$ un anillo conmutativo y sea $B$ una extensión de este anillo. Se define el conjunto $\overline{A}$ de los elementos de $B$ que son enteros sobre $A$. Entonces $\overline{A}$ es un subanillo de $B$ y una extensión entera del anillo $A$. El anillo $\overline{A}$ se dice clausura entera de $A$ sobre $B$.*

Las extensiones enteras satisfacen también la siguiente propiedad de transitividad.

COROLARIO C.11. *Sea $A$ un anillo conmutativo. Sea $B$ una extensión entera de $A$ y sea $C$ una extensión entera de $B$. Entonces $C$ es una extensión entera del anillo $A$.*

Las extensiones enteras se preservan para el cociente por un ideal y para anillos de fracciones, en el sentido siguiente.

COROLARIO C.12. *Sea $B$ una extensión entera del anillo conmutativo $A$. Entonces:*

(*i*) *Para cada ideal propio $\mathfrak{b} \subsetneq B$, se cumple que $B/\mathfrak{b}$ es una extensión entera de $A/\mathfrak{b}^c$.*
(*ii*) *Para cualquier $S \subset A$ sistema multiplicativamente cerrado, $S$ es un sistema multiplicativamente cerrado de $B$ y además $S^{-1}B$ es una extensión entera de $S^{-1}A$.*

**Teorema del Ascenso.**

En este apartado veremos el Teorema del Ascenso, resultado que se atribuye a W. Krull, I. S. Cohen y A. Seidenberg, y que consiste en la ampliación de una cadena ascendente de ideales primos en una extensión entera. La prueba, que no detallaremos aquí, pasa por ver algunos de los siguientes resultados previos.

LEMA C.13. *Sean $A$ y $B$ un par de dominios de integridad tales que $B$ sea extensión entera de $A$. Entonces, $A$ es un cuerpo si y solamente si $B$ es también un cuerpo.*

El Teorema del Ascenso trabaja con la contracción de ideales que define el morfismo de inclusión de una extensión entera de anillos. En este contexto particular, se cumple la siguiente propiedad para los ideales contraídos.

PROPOSICIÓN C.14. *Sea $A$ un anillo conmutativo y sea $B$ una extensión entera de $A$. Dado el ideal primo $\mathfrak{p} \in Spec(B)$, son equivalentes:*

(*i*) *$\mathfrak{p} \in MaxSpec(B)$,*
(*ii*) *$\mathfrak{p}^c \in MaxSpec(A)$.*

El enunciado previo implica que, si dos ideales distintos de $B$ tienen el mismo ideal contraído, entonces no puede estar uno de ellos contenido en el otro.

COROLARIO C.15. *Sea $A \subset B$ una extensión entera de anillos. Dados $\mathfrak{q}_1, \mathfrak{q}_2 \in Spec(B)$ distintos y tales que $\mathfrak{q}_1^c = \mathfrak{q}_2^c$, se tendrá que $\mathfrak{q}_1 \not\subset \mathfrak{q}_2$ y que $\mathfrak{q}_2 \not\subset \mathfrak{q}_1$.*

En vista de estos dos últimos resultados, se tiene, para una extensión entera $B$ de un anillo conmutativo $A$, la siguiente aplicación sobreyectiva:

$$\begin{array}{rcl} \varphi : Spec(B) & \longrightarrow & Spec(A) \\ \mathfrak{q} & \longmapsto & \mathfrak{q}^c, \end{array}$$

y para la que además se cumple que $\varphi(MaxSpec(B)) = MaxSpec(A)$. Con todo esto, pasemos a dar el Teorema del Ascenso.

TEOREMA C.16. **(del Ascenso)**
*Sea $A \subset B$ una extensión entera de anillos. Supongamos dadas las siguientes cadenas:*

$$\mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_n, \qquad \mathfrak{q}_1 \subset \ldots \subset \mathfrak{q}_m,$$

*donde $n > m$ y se tienen $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in Spec(A)$ y $\mathfrak{q}_1, \ldots, \mathfrak{q}_m \in Spec(B)$ tales que $\mathfrak{q}_i^c = \mathfrak{p}_i$ para cada $i = 1, \ldots, m$. Entonces, existen $\mathfrak{q}_{m+1}, \ldots, \mathfrak{q}_n \in Spec(B)$ tales que $\mathfrak{q}_m \subset \ldots \subset \mathfrak{q}_n$ y se verifica $\mathfrak{q}_j^c = \mathfrak{p}_j$ para cada $j = m+1, \ldots, n$.*

A partir del Teorema del Ascenso, se deduce la siguiente relación entre la co-altura de un ideal primo y su contraído. Dado que esto ocurre para toda la colección de ideales primos, las observaciones hechas tras Proposición C.7 llevan a que un anillo conmutativo tenga la misma dimensión de Krull que cualquiera de sus extensiones enteras.

COROLARIO C.17. *Sea $A \subset B$ una extensión entera de anillos. Entonces, para cualquier ideal primo $\mathfrak{p} \in Spec(A)$ existe $\mathfrak{q} \in Spec(B)$ tal que $\mathfrak{q}^c = \mathfrak{p}$, y adicionalmente este cumple que $co\text{-}ht(\mathfrak{p}) = co\text{-}ht(\mathfrak{q})$. En particular, se tiene que $dim_{Krull}(A) = dim_{Krull}(B)$.*

**Teorema del Descenso.**

Ahora veremos el Teorema del Descenso, que es el otro de los Teoremas de Cohen-Seidenberg, y que consiste en una versión para cadenas descendentes de ideales primos del Teorema del Ascenso C.16. En este caso, no bastará con considerar una extensión de anillos conmutativos en general, sino que es preciso introducir un tipo particular de dominio de integridad.

DEFINICIÓN 53. **(Dominio Normal)**
*Sea $A$ un dominio de integridad y denotemos por $Frac(A)$ a su cuerpo de fracciones. Decimos que $A$ es un dominio normal o un dominio íntegramente cerrado cuando la clausura entera de la extensión de anillos $A \subset Frac(A)$ es $A$.*

Veamos detalladamente que los dominios de factorización única, abreviadamente DFU, son un ejemplo de dominio normal.

EJEMPLO C.18. *Llamemos $D$ a un dominio de factorización única y $K$ a su cuerpo de fracciones. Sea $z \in K$ un elemento entero sobre $D$. Sean $x, y \in D$ con $y \neq 0$ y tales que $z = x/y$. Sin pérdida de generalidad, porque estamos tratando con un DFU, puede suponerse que $x, y$ no tengan factores primos comunes. Probaremos que $D$ es normal si el elemento $z$ pertenece necesariamente a $D$, es decir, si se tiene que $y$ es una unidad de $D$. Se considera el polinomio $f = X^d + a_{d-1}X^{d-1} + \ldots + a_1X + a_0 \in D[X]_{mon}$ que satisface la ecuación de dependencia entera de $z$ sobre $D$, es decir, $f(z) = 0$. Sustituyendo $z$ por $x/y$ en dicha ecuación, multiplicando por $y^d$ y despejando $x^d$, se obtiene que:*

$$x^d = -y\left(a_{d-1}x^{d-1} + a_{d-2}x^{d-2}y + \ldots + a_1xy^{d-2} + a_0y^{d-1}\right).$$

*Supongamos que $y$ no es unidad de $D$ y que existe algún primo $p \in D$ que divide a $y$. De la igualdad se sigue que $p$ divide a $x^d$ y como es primo, dividirá también a $x$. Esto es una contradicción dado que $x$ e $y$ se han escogido sin factores primos comunes. En definitiva, $y$ debe ser una unidad de $D$ y se tiene que $D$ es un dominio normal.*

A continuación, se añade algunos ejemplos más de dominios conocidos que son normales.

EJEMPLO C.19. *Los siguientes son ejemplos de dominios normales:*

(I) *Cualquier dominio de ideales principales, abreviadamente DIP, es normal dado que es un DFU. En particular, $\mathbb{Z}$ es un dominio de integridad normal.*
(II) *Los anillos de polinomios $D[X_1, \ldots, X_n]$ con $D$ un DFU son dominios normales por el Lema de Gauss.*
(III) *Los anillos de series de potencias formales $K[[X_1, \ldots, X_n]]$ con $K$ un cuerpo son dominios normales por los Teoremas de Weierstrass.*

También se requiere esta propiedad que amplía a la Afirmación $(ii)$ del Corolario C.12.

PROPOSICIÓN C.20. *Sea $A \subset B$ una extensión de anillos y sea $\overline{A}$ la clausura entera de $A$ en $B$. Entonces, para cualquier sistema multiplicativamente cerrado $S \subset A$, $S^{-1}\overline{A}$ es la clausura entera de $S^{-1}A$ en $S^{-1}B$.*

Tras esto, ya puede enunciarse el Teorema del Descenso, cuya prueba no se incluye.

TEOREMA C.21. **(del Descenso)**
*Sea $A \subset B$ una extensión entera de dominios de integridad, es decir, $B$ es una extensión entera de $A$ y ambos son dominios de integridad. Supongamos que $A$ es además un dominio normal, y que se tiene las siguientes cadenas de ideales primos:*

$$\mathfrak{p}_1 \supset \ldots \supset \mathfrak{p}_n, \qquad \mathfrak{q}_1 \supset \ldots \supset \mathfrak{q}_m,$$

*donde $n > m$ y se tienen $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in Spec(A)$ y $\mathfrak{q}_1, \ldots, \mathfrak{q}_m \in Spec(B)$ tales que $\mathfrak{q}_i^c = \mathfrak{p}_i$ para cada $i = 1, \ldots, m$. Entonces, existen unos $\mathfrak{q}_{m+1} \ldots \mathfrak{q}_n \in Spec(B)$ tales que $\mathfrak{q}_m \supset \ldots \supset \mathfrak{q}_n$ y que $\mathfrak{q}_j^c = \mathfrak{p}_j$ para cada $j = m+1, \ldots, n$.*

El Teorema del Descenso tiene consecuencias para la altura de un ideal y de su contraído, en el caso de una extensión de dominios de integridad que cumpla con las condiciones del enunciado.

COROLARIO C.22. *Sea $A \subset B$ una extensión entera de dominios de integridad. Supongamos que $A$ es un dominio normal y que $B$ es entero sobre $A$. Entonces, para cada $\mathfrak{q} \in Spec(B)$, se cumple:*

$$ht(\mathfrak{q}) = ht(\mathfrak{q}^c).$$

Nótese que el Corolario C.17 es aplicable a este caso particular de extensión de dominios de integridad y que complementa al resultado.

**Lema de Normalización de Noether.**

Aquí presentaremos el Lema de Normalización de Noether, en la forma en que se expone en [**Kunz, 1985**]. Particularizando al caso que nos ocupa, que es el de un anillo de polinomios sobre un cuerpo realmente cerrado, veremos algunas propiedades sobre la dimensión de estos anillos de polinomio. En primer lugar, se enuncia el Lema de Normalización sin demostración.

TEOREMA C.23. **(Lema de Normalización de Noether)**
*Sean $F$ un cuerpo, $A$ una $F$-álgebra finitamente generada y $\mathfrak{a}$ un ideal propio de $A$. Entonces, existirán $s, d \in \mathbb{N}$ y $Y_1, \ldots, Y_d \in A$ tales que:*

- *(i) la familia $Y_1, \ldots, Y_d$ es algebraicamente independiente sobre $K$ (ver Definición 54),*
- *(ii) $A$ es un $F[Y_1, \ldots, Y_d]$-módulo finitamente generado,*
- *(iii) $\mathfrak{a} \cap F[Y_1, \ldots, Y_d] = (Y_{s+1}, \ldots, Y_d)$ para algún $s = 1, \ldots, d$.*

*Si además $F$ es un cuerpo infinito y $A = K[X_1, \ldots, X_n]$ es un anillo de polinomios, se cumple adicionalmente que los $Y_1, \ldots, Y_d$ son combinaciones lineales de $X_1, \ldots, X_n$.*

Ahora si, consideremos el caso de un anillo de polinomios $R[X_1, \ldots, X_n]$ definido sobre algún cuerpo realmente cerrado $R$ que siempre será infinito. La primera propiedad se basa en que los cuerpos realmente cerrados tienen dimensión de Krull igual a 0.

COROLARIO C.24. *Si $R$ es cuerpo realmente cerrado, $dim_{Krull}(R[X_1, \ldots, X_n]) = n$.*

Para este mismo caso de $R[X_1, \ldots, X_n]$, se tendrá que todo ideal primo cumple la igualdad para la desigualdad de la Proposición C.7. Es decir, cualquier cadena de ideales primos a la que no se pueda añadir más ideales primos intermedios tendrá la misma cantidad de ideales.

COROLARIO C.25. *Sea $R$ cuerpo realmente cerrado. Dado $\mathfrak{p} \in Spec(R[X_1, \ldots, X_n])$, entonces $ht(\mathfrak{p}) + cp\text{-}ht(\mathfrak{p}) = n$.*

Del Lema de Normalización también se deduce que una $R$-álgebra finitamente generada con $R$ un cuerpo realmente cerrado tiene dimensión finita.

COROLARIO C.26. *Sea $R$ cuerpo realmente cerrado. Si $A$ es una $R$-álgebra finitamente generada, entonces $dim_{Krull}(A) < +\infty$.*

Si además se trata de una $R$-álgebra finitamente generada isomorfa a un anillo de la forma $R[X_1, \ldots, X_n]/\mathfrak{p}$ con $\mathfrak{p}$ primo, entonces se tiene la siguiente relación entre la altura de los ideales primos de la $R$-álgebra en cuestión con los ideales primos de $R[X_1, \ldots, X_n]$ que contengan a $\mathfrak{p}$.

COROLARIO C.27. *Sea $R$ es cuerpo realmente cerrado. Sean $\mathfrak{p}, \mathfrak{q} \in Spec(R[X_1, \ldots, X_n])$ tales que $\mathfrak{p} \subset \mathfrak{q}$. Entonces:*

$$ht(\mathfrak{q}/\mathfrak{p}) = ht(\mathfrak{q}) - ht(\mathfrak{p}) = co\text{-}ht(\mathfrak{q}) - co\text{-}ht(\mathfrak{p}).$$

En particular, estos dos últimos resultados servirán para el estudio de cualquier anillo de polinomios $\mathcal{P}(V)$, introducidos en la Sección 1.1, el cual es isomorfo al anillo cociente $R[X_1,\ldots,X_n]/\mathfrak{a}$ donde $\mathfrak{a}=\mathcal{I}_{R[X_1,\ldots,X_n]}(V)$ es el ideal generado por un conjunto algebraico $V$ y es primo.

**Base y Grado de Trascendencia.**

En esta subsección se introduce las nociones de base y grado de trascendencia, que como se verá al final, guardan cierta relación con la dimensión de Krull. Las demostraciones de los resultados de este apartado pueden encontrarse en [**Stewart, 1972**], y en particular se ha adaptado el corolario sobre dimensión al caso de un cuerpo realmente cerrado, que es de característica 0.

En primer lugar, diferenciemos entre lo que es una extensión de cuerpos finita y una extensión de cuerpos finitamente generada. Si llamamos $L/K$ a una extensión de cuerpos, esta se dirá finita cuando $L$ sea un $K$-espacio vectorial de dimensión finita, o equivalentemente si $L$ es un $K$-módulo finitamente generado. Se denotará por $[L:K]$ a la dimensión de $L$ como $K$-espacio vectorial. Por otra parte, la extensión $L/K$ se dirá finitamente generada si $L$ es el menor cuerpo que contiene al cuerpo $K$ y a alguna familia finita de $L$. Es decir, si existen $\alpha_1,\ldots,\alpha_r\in L$ tales que el cuerpo generado $K(\alpha_1,\ldots,\alpha_r)$ sea igual a $L$. Obsérvese que, dada la extensión de cuerpos $L/K$ y dados $\alpha_1,\ldots,\alpha_r\in L$, la $K$-álgebra generada $K[\alpha_1,\ldots,\alpha_r]$[3] será un dominio de integridad cuyo cuerpo de fracciones es precisamente $K(\alpha_1,\ldots,\alpha_r)$. Ahora, se define la idea de independencia algebraica que ya utilizamos en el apartado previo. Se escoge introducirla aquí para poder discutirla en términos de las extensiones de cuerpos que acabamos de ver.

Definición 54. **(Familia Algebraicamente Independiente)**
*Sea $K$ un cuerpo y sea $A$ una $K$-álgebra. Una familia finita $\{\alpha_1,\ldots,\alpha_r\}$ de elementos de $A$ se dice algebraicamente independiente sobre $K$ si se cumple:*

$$f(\alpha_1,\ldots,\alpha_r)=0\Rightarrow f=0,\ \textit{para cada } f\in K[X_1,\ldots,X_r].$$

*En caso contrario, se dirá que la familia es algebraicamente dependiente sobre $K$.*

Observación C.28. Para el caso de una extensión de cuerpos $L/K$, que la familia $\{\alpha_1\}\subset L$ sea algebraicamente independiente sobre $K$ equivale a que $\alpha_1$ sea un elemento de $L$ trascendente sobre $K$. Más aún, si una familia de elementos de $L$ contiene algún elemento algebraico sobre $K$, esta será algebraicamente dependiente sobre $K$.

La noción de independencia algebraica puede entenderse por medio de la propiedad siguiente. Dada una extensión de cuerpos $L/K$ y una familia $\{\alpha_1,\ldots,\alpha_r\}\subset L$, se tiene que esta es algebraicamente independiente sobre $K$ si y solamente si la aplicación:

$$\begin{aligned}K[X_1,\ldots,X_r]&\longrightarrow \quad L\\ f(X_1,\ldots,X_r)&\longmapsto f(\alpha_1,\ldots,\alpha_r),\end{aligned}$$

es un monomorfismo de $K$-álgebras. Más aún, $K[\alpha_1,\ldots,\alpha_r]$ es la imagen de este monomorfismo y por lo tanto, $K[\alpha_1,\ldots,\alpha_r]$ será isomorfo a $K[X_1,\ldots,X_r]$. En particular, una extensión trascendente $K[\alpha]$ del cuerpo $K$ dada por un elemento $\alpha\in L$ trascendente sobre $K$ será isomorfa al anillo de polinomios univariados $K[X]$. Otro ejemplo evidente viene dado por la extensión $K[X_1,\ldots,X_n]/K$ para un cuerpo $K$, donde $\{X_1,\ldots,X_n\}$ es una familia de elementos algebraicamente independientes sobre $K$.

Vamos a seguir con una herramienta que, por un lado, nos permite definir unas nociones de base y de grado para las extensiones de cuerpos trascendentes, y por otro lado, lleva junto con el Lema de Normalización de Noether C.23, a un resultado útil sobre la dimensión de anillos de polinomios definidos sobre una variedad algebraica irreducible. En primer lugar, se tiene este lema previo.

Lema C.29. *Sea $L/K$ una extensión de cuerpos finitamente generada. Entonces, existe un conjunto $\{\alpha_1,\ldots,\alpha_r\}\subset L$ algebraicamente independiente sobre $K$ tal que la extensión de cuerpos $L/K(\alpha_1,\ldots,\alpha_r)$ es finita.*

[3]Con las notaciones expuestas, $K[\alpha_1,\ldots,\alpha_r]$ se definiría como el menor subanillo de $L$ que contiene a $\alpha_1,\ldots,\alpha_r$ y a $K$, aquel cuyos elementos son de la forma $ev_{\alpha_1,\ldots,\alpha_r}(f)$ para algún polinomio $f\in K[X_1,\ldots,X_n]$.

Este lema sirve para probar el llamado Teorema de Intercambio de Steinitz, que esencialmente nos dice que, dada una extensión de cuerpos $L/K$ finitamente generada, si bien la familia $\{\alpha_1, \ldots, \alpha_r\} \subset L$ algebraicamente independiente sobre $K$ que genera a $L$ como $K(\alpha_1, \ldots, \alpha_r)$ no es única, sí que será único el cardinal de dicha familia.

TEOREMA C.30. **(de Intercambio de Steinitz)**
*Sea $L/K$ una extensión finitamente generada. Sean $\{\alpha_1, \ldots, \alpha_r\}$ y $\{\beta_1, \ldots, \beta_s\}$ dos familias finitas de elementos de $L$ que son algebraicamente independientes sobre $K$ y tales que las extensiones de cuerpos $L/K(\alpha_1, \ldots, \alpha_r)$ y $L/K(\beta_1, \ldots, \beta_s)$ sean finitas. Entonces $r = s$.*

La idea de este resultado recuerda al Teorema del Reemplazamiento para espacios vectoriales, pero sustituyendo la noción de independencia lineal por la de independencia algebraica. Todo esto conduce a las siguientes definiciones.

DEFINICIÓN 55. **(Base y Grado de Trascendencia)**
*Sea $L/K$ una extensión de cuerpos finitamente generada. Se dice base de trascendencia de $L$ sobre $K$ a cualquier conjunto finito $\mathcal{B} \subset L$ algebraico sobre $K$ y tal que $L/K(\mathcal{B})$ es una extensión de cuerpos finita. Se dice grado de trascendencia de la extensión al cardinal de cualquiera de sus bases de trascendencia, y denota por $grTr_K(L)$.*

En vista de la Observación C.28, se tiene que una extensión de cuerpos $L/K$ algebraica no admite una subfamilia no vacía de $L$ que sea algebraicamente independiente sobre $K$. Es decir, la idea de una base de trascendencia solo tiene sentido para extensiones de cuerpos finitamente generadas y trascendentes.

Para concluir con el apartado, veremos un resultado particularizado a cuerpos realmente cerrados que relaciona la dimensión de un anillo de polinomios $\mathcal{P}(V)$ definido sobre una variedad algebraica irreducible $V \subset \mathbb{A}^n(R)$ con el grado de trascendencia de la extensión de cuerpos $\mathcal{K}(V)/R$. Se incuye la prueba como un ejemplo de uso del Lema de Normalización de Noether C.23. Las notaciones del anillo de polinomios $\mathcal{P}(V)$ y de su cuerpo de fracciones $\mathcal{K}(V)$ que se utilizan se han introducido en la Sección 1.1 y en la Sección 2.4, respectivamente.

COROLARIO C.31. *Sea $R$ un cuerpo realmente cerrado y $V \subset \mathbb{A}^n(R)$ una variedad algebraica irreducible. Sea $\mathcal{P}(V)$ el dominio de las funciones polinomiales de $V$ en $R$. Sea $\mathcal{K}(V)$ el cuerpo de fracciones de $\mathcal{P}(V)$ (es decir, el cuerpo de funciones racionales definidas en algún cerrado Zariski de $V$, con coeficientes en $R$), se tiene:*

$$dim_{Krull}(\mathcal{P}(V)) = grTr_R(\mathcal{K}(V)).$$

DEMOSTRACIÓN. El anillo $\mathcal{P}(V)$ es una $R$-álgebra, y entonces podemos aplicar el Lema de Normalización C.23 tomando este anillo y cualquier ideal propio, por ejemplo (0). Entonces, para algún $d \in \mathbb{N}$ existe una familia $\{Y_1, \ldots, Y_d\}$ de $\mathcal{P}(V)$ que es algebraicamente independiente sobre $R$ y cuyos elementos definen a un anillo de polinomios $R[Y_1, \ldots, Y_d]$ tal que $\mathcal{P}(V)$ es una $R[Y_1, \ldots, Y_d]$-álgebra finita. Como $R$ es un cuerpo, $R[Y_1, \ldots, Y_d]$ es además un dominio de integridad y $R(Y_1, \ldots, Y_d)$ será su cuerpo de fracciones. Veamos entonces que $\mathcal{K}(V)$ es una $R(Y_1, \ldots, Y_d)$-álgebra finita. Dada la inclusión de $R[Y_1, \ldots, Y_d]$ en $\mathcal{P}(V)$, es claro que $R(Y_1, \ldots, Y_d) \subset \mathcal{K}(V)$ y tomando el morfismo de inclusión se tendrá que $\mathcal{K}(V)$ es una $R(Y_1, \ldots, Y_d)$-álgebra. Para ver que es finita, tomemos un elemento $f/g \in \mathcal{K}(V)$ dado por unas funciones polinomiales $f, g \in \mathcal{P}(V)$ con $g \neq 0$. Como $\mathcal{P}(V)$ es una $R[Y_1, \ldots, Y_d]$-álgebra finita, existe una lista finita de elementos $h_1, \ldots, h_r \in \mathcal{P}(V)$ tales que puede escribirse $f = f_1 h_1 + \ldots + f_r h_r$ para algunos $f_1, \ldots, f_d \in R[Y_1, \ldots, Y_d]$. Entonces:

$$\frac{f}{g} = \frac{f_1}{g} h_1 + \ldots + \frac{f_r}{g} h_r,$$

y acabamos de probar que todo elemento no nulo de $\mathcal{K}(V)$ es una combinación lineal de unos elementos $h_1, \ldots, h_r$ con coeficientes en $R(Y_1, \ldots, Y_d)$ y por ende, $\mathcal{K}(V)$ es una $R(Y_1, \ldots, Y_d)$-álgebra finita. Es decir, $\mathcal{K}(V)/R(Y_1, \ldots, Y_d)$ es una extensión finita de cuerpos, luego $\{Y_1, \ldots, Y_d\}$ es una base de trascendencia de la extensión $\mathcal{K}(V)/R$ y su grado de trascendencia es $d$. Por otra parte, que $\mathcal{P}(V)$ sea una $R[Y_1, \ldots, Y_d]$-álgebra finita implica que la extensión de anillos $R[Y_1, \ldots, Y_d] \subset \mathcal{P}(V)$ es entera. Aplicando el Corolario C.17 y el Corolario C.24 se sigue las siguientes igualdades:

$$dim(\mathcal{P}(V)) = dim(R[Y_1, \ldots, Y_d]) = d = grTr_R(V). \qquad \square$$

Apéndice D

# Teorema de la Dimensión Local y Regularidad.

Este apartado tiene como fin el estudio de los puntos regulares de una variedad. Para llegar a esto, previamente se verá el Teorema de la Dimensión Local y se introducirá a los anillos locales regulares. Después veremos el Criterio del Jacobiano, que se utiliza para caracterizar a los puntos regulares de una variedad algebraica definida sobre un cuerpo realmente cerrado en nuestro caso. También se añade un breve apartado final sobre el producto cartesiano de semi-algebraicos y su dimensión.

En cuanto a la bibliografía empleada en esta sección, nos apoyaremos en [**González, 2022**] para mostrar, de manera sucinta, el Teorema de la Dimensión Local. También se inspira en esta cita la presentación de anillos locales regulares, que se completa con la Sección $V$,5 de [**Kunz, 1985**]. El Criterio de Jacobiano se saca de la Sección $VI$,1 de esta última referencia bib-liográfica. Por último, el apartado sobre puntos regulares sigue el hilo argumental de la Sección 3.3 de [**BCR, 1998**].

**Teorema de la Dimensión Local.**

A primera vista, uno podría esperar que la dimensión de Krull de un anillo noetheriano es siempre finita dado que la altura de cada uno de sus ideales es finita. Sin embargo, Nagata nos muestra con el *"Example 1"* de su apéndice sobre *"Examples of bad Noetherian rings"* de [**Nagata, 1927**], un ejemplo de un anillo noetheriano con dimensión de Krull no finita.

Ejemplo D.1. *Reproducimos el ejemplo de un 'mal anillo noetheriano' de Nagata. Consideremos un cuerpo $K$ y una familia $\{X_1, X_2, \dots\} = \{X_{k+1}\}_{k\in\mathbb{N}}$ de indeterminadas, o dicho de otra forma, de elementos algebraicamente independientes sobre $K$ en el sentido de que toda subfamilia finita sea una familia algebraicamente independiente sobre $K$ (véase la Definición 54). Se define el conjunto:*

$$K[X_1, X_2, \dots] = \bigcup_{k=1}^{\infty} K[X_1, \dots, X_k],$$

*que resulta ser un anillo con las operaciones suma y producto definidas para cada par de elementos $f \in K[X_1, \dots, X_r]$ y $g \in K[X_1, \dots, X_s]$, pertenecientes ambos a $K[X_1, X_2, \dots]$, como la suma y producto de $f$ y $g$ como elementos de $K[X_1, \dots, X_{rs}]$. Ahora se considera una sucesión no finita $(m_1, m_2, \dots)$ de números naturales que cumpla que $0 < m_k - m_{k-1} < m_{k+1} - m_k$ para cada $k \geq 2$. Con esto se define a los ideales $\mathfrak{p}_k = (X_{m_k}, \dots, X_{m_{k+1}-1})$ para cada $k \geq 1$. Cada uno de estos ideales es primo y tiene asociada la siguiente cadena de ideales primos:*

$$(0) \subsetneq (X_{m_k}) \subsetneq \dots \subsetneq (X_{m_k}, \dots, X_{m_{k+1}-1}) = \mathfrak{p}_k,$$

*que como veremos más adelante por el Teorema del Ideal Principal de Krull D.5, esta será de longitud máxima y entonces $ht(\mathfrak{p}_k) = m_{k+1} - m_k$. Por otro lado se tiene la Proposición B.4, que nos dice que el conjunto $S$ definido como la intersección de los complementarios en $K[X_1, X_2, \dots]$ de los $\mathfrak{p}_k$ será un sistema multiplicativamente cerrado, y entonces puede definirse el anillo $A = S^{-1}K[X_1, X_2, \dots]$. La prueba de que este anillo es noetheriano se debe a la Proposición B.14, la cual puede verse probada en* [**Nagata, 1927**]. *Aquí tan solo añadiremos que la dimensión de Krull de este anillo es no finita como consecuencia de la Proposición C.7 y de que el conjunto de las alturas de los ideales no está acotado.*

En conclusión, no puede seguirse de la condición de noetherianidad de un anillo que su dimensión sea finita. Afortunadamente, puede utilizarse una noción de dimensión para anillos locales noetherianos que cumple varias cosas. Por un lado, es equivalente a la dimensión de Krull para

esta clase de anillos, por un resultado que se conoce como el Teorema de la Dimensión Local. Por otra parte, permite deducir que la dimensión de un anillo local noetheriano es siempre finita. Este hecho da cuenta de por qué la localización es un tema relevante en Geometría Algebraica.

En primer lugar, ha de enunciarse un resultado de Hilbert y Samuel que motiva una definición de dimensión para anillos locales noetherianos. Recuérdese la definición de anillo local $(A, \mathfrak{m})$ introducida en el Apéndice B, y también la del cuerpo residual $k(\mathfrak{m}) = A/\mathfrak{m}$ asociado a este anillo local. A continuación, el resultado junto con la definición del polinomio de Hilbert-Samuel de un anillo local noetheriano.

TEOREMA D.2. **(de Hilbert-Samuel)**
*Sea $(A, \mathfrak{m})$ un anillo local noetheriano y sea $k(\mathfrak{m})$ su cuerpo residual. Entonces:*

(*i*) *Dado $n \geq 1$, $A/\mathfrak{m}^n$ es un $k(\mathfrak{m})$-espacio vectorial de dimensión finita $dim_{k(\mathfrak{m})}(A/\mathfrak{m}^n)$.*
(*ii*) *Se define la función siguiente:*

$$\begin{aligned} \mathcal{P}_{\mathfrak{m}} : \mathbb{N} &\longrightarrow \quad \mathbb{N} \\ n &\longmapsto dim_{k(\mathfrak{m})}(A/\mathfrak{m}^n). \end{aligned}$$

*Entonces existe un único polinomio $f \in \mathbb{Z}[X]$ y un $n_0 \in \mathbb{N}$ de tal modo que*

$$\mathcal{P}_{\mathfrak{m}}(n) = f(n), \text{ para cada } n \geq n_0.$$

*La función $\mathcal{P}_{\mathfrak{m}}$ se denomina función polinomial (o polinomio) de Hilbert-Samuel del anillo local $(A, \mathfrak{m})$, y se dice grado de $\mathcal{P}_{\mathfrak{m}}$, que se denota por $deg(\mathcal{P}_{\mathfrak{m}})$, al grado del polinomio $f$.*

El teorema precedente asocia un polinomio a cada anillo local noetheriano. La unicidad de este polinomio y en particular la de su grado, permite definir una nueva noción de dimensión.

DEFINICIÓN 56. **(Dimensión de Hilbert-Samuel)**
*Sea $(A, \mathfrak{m})$ un anillo local noetheriano. Se llama dimensión de Hilbert-Samuel de $(A, \mathfrak{m})$, abreviadamente HS, al grado de su polinomio de Hilbert:*

$$dim_{HS}(A) = deg(\mathcal{P}_{\mathfrak{m}}).$$

Existe otra idea para definir a la dimensión de un anillo local noetheriano, también equivalente a la dimensión de Krull. Se basa en el siguiente tipo de ideales de un anillo local noetheriano.

DEFINICIÓN 57. **(Ideal de Definición)**
*Sea $(A, \mathfrak{m})$ un anillo local noetheriano. Sea un ideal $\mathfrak{a} = (a_1, \ldots, a_r)$ de $A$. El ideal $\mathfrak{a}$ se dice ideal de definición de $(A, \mathfrak{m})$ cuando $\sqrt{\mathfrak{a}} = \mathfrak{m}$.*

Otras maneras equivalentes de definir a un ideal $\mathfrak{a}$ de definición de un anillo local noetheriano $(A, \mathfrak{m})$ son:

(*i*) si existe algún $t \in \mathbb{N}$ tal que $\mathfrak{m}^t \subset \mathfrak{a}$,
(*ii*) o si $A/\mathfrak{a}$ es un anillo con un único ideal primo, es decir, si $A/\mathfrak{a}$ es un anillo local artiniano.

Con esto, se define la dimensión de Chevalley de un anillo local noetheriano.

DEFINICIÓN 58. **(Dimensión de Chevalley)**
*Sea $(A, \mathfrak{m})$ un anillo local noetheriano. Llamaremos dimensión de Chevalley de $A$ a*

$$dim_{Ch}(A) = min\{r \in \mathbb{N} : \exists \{a_1, \ldots, a_r\} \subset A, \sqrt{(a_1, \ldots, a_r)} = \mathfrak{m}\}.$$

Ahora viene el resultado que nos dice que todas estas definiciones de dimensión son equivalentes para el caso de un anillo local noetheriano. Se conoce como el Teorema de la Dimensión Local y se atribuye a Samuel y a Chevalley.

TEOREMA D.3. **(de la Dimensión Local)**
*Sea $(A, \mathfrak{m})$ un anillo local noetheriano. Entonces,*

$$dim_{Krull}(A) = dim_{HS}(A) = dim_{Ch}(A).$$

A partir de aquí, cuando se hable de dimensión de un anillo local regular se estará hablando de cualquiera de estas tres definiciones de dimensión, ya que son equivalentes. Dado un anillo noetheriano $A$, se deduce del Teorema de la Dimensión Local que todo ideal primo $\mathfrak{p} \in Spec(A)$ tiene altura finita. Esto equivale a decir que el anillo local noetheriano $A_{\mathfrak{p}}$ tiene dimensión

finita, ya que por la Proposición C.3 se tiene que $ht(\mathfrak{p}) = dim_{Krull}(A_{\mathfrak{p}})$ y $\mathfrak{p} = (a_1, \ldots, a_r)$ al ser $A$ un anillo noetheriano. De esto último se sigue que $\mathfrak{p}$ como ideal maximal de $A_{\mathfrak{p}}$ satisface $\mathfrak{p} = \sqrt{(a_1, \ldots, a_r)}$ por ser un ideal primo, y en definitiva ocurre que:

$$ht(\mathfrak{p}) = dim_{Krull}(A_{\mathfrak{p}}) = dim_{Ch}(A_{\mathfrak{p}}) \leq r < +\infty.$$

Obviamente, el ejemplo de Nagata (Ejemplo D.1) muestra que, aunque las alturas de los ideales primos sean finitas, estas pueden ser arbitrariamente grandes. Otra clásica aplicación del Teorema de la Dimensión Local es el conocido Teorema del Ideal Principal de Krull. Se requiere la siguiente definición previa.

Definición 59. **(Sucesión Regular)**
*Sea $A$ un anillo conmutativo y sean $a_1, \ldots, a_r$ elementos de $A$. Se dice que $a_1, \ldots, a_r$ es una sucesión regular en $A$ si se verifica:*

(*i*) $(a_1, \ldots, a_r) \neq A$,
(*ii*) *$a_1$ no es divisor de cero en $A$ y tampoco es divisor de cero la clase de $a_i$ en el anillo cociente $A/(a_1, \ldots, a_{i-1})$ para cualquier $i = 2, \ldots, r$.*

Nótese que para cualquier el anillo de polinomios $A[X_1, \ldots, X_n]$, la sucesión $(X_1, \ldots, X_n)$ es regular. El hecho de definir las sucesiones regulares como conjuntos ordenados se debe a que las sucesiones finitas no mantienen, en general, la propiedad de ser regular ante una permutación de elementos.[1] No obstante, esto sí que sucede para el caso de un anillo local noetheriano.[2]

Proposición D.4. *Sea $(A, \mathfrak{m})$ un anillo local noetheriano y sea $a_1, \ldots, a_r$ una sucesión regular en $A$. Entonces, $a_{\tau(1)}, \ldots, a_{\tau(r)}$ es una sucesión regular en $A$ para toda permutación $\tau \in \Sigma_n$.*

Ahora, veamos el enunciado del Teorema del Ideal Principal de Krull. Se trata de una cota a la altura de los ideales de un anillo noetheriano y de una condición que asegura la igualdad entre la altura del ideal y dicha cota.

Teorema D.5. **(del Ideal Principal de Krull)**
*Sea $A$ un anillo noetheriano. Sean $a_1, \ldots, a_r$ elementos de $A$ y sea $\mathfrak{a} = (a_1, \ldots, a_r)$. Entonces, para cada ideal primo $\mathfrak{p} \in Spec(A)$ minimal entre los ideales primos que contienen a $\mathfrak{a}$, se tiene que $ht(\mathfrak{p}) \leq r$. Si además $a_1, \ldots, a_r$ es una sucesión regular en $A$, se verifica la igualdad.*

Volviendo al caso de un anillo local noetheriano $(A, \mathfrak{m})$, tenemos que si el ideal maximal $\mathfrak{m}$ está generado por los elementos de una sucesión regular en $A$, aplicando el resultado precedente se tiene que $ht(\mathfrak{m})$ será la cantidad de elementos en dicha sucesión regular y por la Proposición C.6, esta coincidirá con la dimensión del anillo. Como conclusión, la dimensión de un anillo local noetheriano es necesariamente finita. Todas estas consideraciones motivan la siguiente redefinición del concepto de sucesión regular para el caso de un anillo local noetheriano.

Definición 60. **(Sistema Regular de Parámetros de un Anillo Local Noetheriano)**
*Sea $(A, \mathfrak{m})$ un anillo local noetheriano. Se dice sistema regular de parámetros del anillo $(A, \mathfrak{m})$ a cualquier conjunto $\{a_1, \ldots, a_d\} \subset A$ que genere al ideal $\mathfrak{m}$ y que cumpla que $d = dim_{Krull}(A)$.*

Nótese que aquí hablamos de un conjunto no ordenado dado que se tiene la Proposición D.4 en el caso de anillos locales noetherianos. Para finalizar, veamos un resultado de Nagata que utiliza el Teorema de Lasker-Noether 1.3.4 para probar esta caracterización de los dominios de factorización única noetherianos.

Corolario D.6. *Sea $A$ un dominio de integridad noetheriano. Entonces, son equivalentes:*

(*i*) *$A$ es un dominio de factorización única,*
(*ii*) *todo ideal primo $\mathfrak{p} \in Spec(A)$ con $ht(\mathfrak{p}) = 1$ es un ideal principal.*

### Anillos Locales Regulares.

En este apartado se introduce a los anillos locales regulares. Estos son, esencialmente, los anillos locales noetherianos para los que se tiene alguna sucesión regular, es decir, unos generadores

[1] Puede verse un ejemplo en: https://stacks.math.columbia.edu/tag/0AUH.
[2] También en https://stacks.math.columbia.edu/tag/0AUH puede verse este resultado adaptándolo de la terminología de módulos.

de su ideal maximal que cumplan con la igualdad del Teorema del Ideal Principal de Krull D.5. En primer lugar, se verá cómo definirlos mediante tres propiedades equivalentes, introduciendo los conceptos de filtración y de graduación de un anillo. Después, se añade algunas de las propiedades de estos anillos, destacando el Criterio del Jacobiano. Dicho resultado se estudiará en el apartado siguiente y servirá para definir las ideas de regularidad y singularidad de los puntos de una variedad en el sentido algebraico.

Comencemos por definir lo que es una graduación de un anillo, que no es otra cosa que una forma de separarlo en componentes que sean subgrupos aditivos y que tengan asociado un tamaño entero de manera que el producto de elementos de tamaños $n$ y $m$ sea un elemento de tamaño $nm$. Esta idea recuerda a la descomposición de un anillo de polinomios en componentes que son polinomios homogéneos (se desarrolla un poco este ejemplo al inicio del Apéndice E).

Definición 61. **(Graduación de un Anillo)**
*Sea $A$ un anillo conmutativo. Supongamos que existe una familia $\{A_n\}_{n\in\mathbb{N}}$ de subgrupos aditivos de $A$ tales que:*

(*i*) $A = \bigoplus_{n\in\mathbb{N}} A_n$,
(*ii*) $A_n A_m \subset A_{nm}$ *para cualesquiera* $n, m \in \mathbb{N}$.

*En tal caso se dirá que $\{A_n\}_{n\in\mathbb{N}}$ es una graduación sobre $A$ y que $A$ es un anillo graduado. Se dice elementos homogéneos de grado $n$ a los elementos de $A_n$ distintos de $0$.*

En este caso, nos interesa estudiar la graduación de un anillo local noetheriano $(A, \mathfrak{m})$ y para ello introducimos el concepto de filtración de un anillo. Este nos permitirá definir una filtración del anillo, pero primero definámoslo.

Definición 62. **(Filtración de un Anillo)**
*Sea $A$ un anillo conmutativo. Se dice filtración del anillo $A$ a una cadena descendente de ideales:*

$$A = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \ldots \supset \mathfrak{a}_k \supset \ldots,$$

*que denotaremos por $\Sigma$, y que cumpla que $\mathfrak{a}_k\mathfrak{a}_l \subset \mathfrak{a}_{kl}$ para cada par $k, l \in \mathbb{N}$. En tales condiciones, $(A, \Sigma)$ se dice anillo filtrado.*

Ahora, si disponemos de un anillo conmutativo $A$ y de una filtración $\Sigma \equiv A = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \ldots$, puede definirse el conjunto siguiente:

$$G_\Sigma(A) = \bigoplus_{n\in\mathbb{N}} (\mathfrak{a}_n/\mathfrak{a}_{n+1}),$$

al que dotaremos con una estructura de anillo graduado. Un par de elementos $a, b \in G_\Sigma(A)$ pueden escribirse, al ser elementos de una suma directa, como sumas finitas de elementos:

$$a = \sum_{i\in I} a_i + \mathfrak{a}_{i+1}, \qquad\qquad b = \sum_{j\in J} b_j + \mathfrak{a}_{j+1},$$

donde $I$ y $J$ son un par de subconjuntos finitos de $\mathbb{N}$. Se define la siguiente operación de suma sobre el conjunto $G_\Sigma(A)$:

$$a + b = \sum_{k\in I\cup J} (a_k + b_k) + \mathfrak{a}_{k+1},$$

donde se entiende que $a_k = 0$ para $k \notin I$ y que $b_k = 0$ para $k \notin J$. También se define una operación producto de la manera siguiente:

$$a \cdot b = \sum_{i\in I}\sum_{j\in J} (a_i b_j) + \mathfrak{a}_{i+j+1}.$$

Puede comprobarse que la definición del producto no depende de los representantes escogidos para las clases, y también que $(G_\Sigma(A), +, \cdot)$ tiene estructura de anillo graduado. Este se dice el anillo graduado asociado al anillo filtrado $(A, \Sigma)$.

Ahora definimos el anillo graduado asociado a la siguiente filtración de un anillo local noetheriano $(A, \mathfrak{m})$:

$$A \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \ldots \supset \mathfrak{m}^k \supset \ldots,$$

el cual se denotará por $G_\mathfrak{m}(A)$. Además de este anillo graduado, puede considerarse el $k(\mathfrak{m})$-espacio vectorial $(\mathfrak{m}/\mathfrak{m}^2, +, \cdot_{k(\mathfrak{m})})$ asociado al anillo local noetheriano $(A, \mathfrak{m})$, donde $k(\mathfrak{m})$ es el

cuerpo residual de $(A, \mathfrak{m})$ y $\cdot_{k(\mathfrak{m})}$ es la acción evidente definida para los elementos homogéneos de $G_{\mathfrak{m}}(A)$ de grado 1 según el producto en $A$ como sigue:

$$x \cdot_{k(\mathfrak{m})} (a + \mathfrak{m}^2) = xa + \mathfrak{m}^2,$$

para cualesquiera $x \in k(\mathfrak{m})$, $a \in \mathfrak{m}$. En adición a estas dos cosas, también se tiene la idea de un sistema regular de parámetros, introducida en la sección previa (véase la Definición 60). Estos tres conceptos están relacionados de la siguiente manera.

Teorema D.7. *Sea $(A, \mathfrak{m})$ un anillo local noetheriano con cuerpo residual $k(\mathfrak{m}) = A/\mathfrak{m}$ y dimensión $d = dim_{Krull}(A)$. Sean el $k(\mathfrak{m})$-espacio vectorial $(\mathfrak{m}/\mathfrak{m}^2, +, \cdot_{k(\mathfrak{m})})$ y el anillo graduado $G_{\mathfrak{m}}(A)$ descritos en los párrafos previos. Entonces, son equivalentes:*

- *(i) Existe algún sistema regular de parámetros de $A$, es decir, una familia de $d$ elementos de $A$ que generen al ideal $\mathfrak{m}$.*
- *(ii) Se cumple que $dim_{k(\mathfrak{m})}(\mathfrak{m}/\mathfrak{m}^2) = dim_{Krull}(A)$.*
- *(iii) El anillo $G_{\mathfrak{m}}(A)$ es isomorfo al anillo de polinomios $k(\mathfrak{m})[X_1, \ldots, X_d]$.*

Definición 63. **(Anillo Local Regular)**
*En el contexto del teorema precedente, el anillo $(A, \mathfrak{m})$ se dice regular si cumple alguna de las tres propiedades equivalentes.*

Ahora veremos varias propiedades notables de esta clase de anillos. La motivación del estudio de estos anillos se debe a su papel dentro de la Geometría Algebraica, pero esto se discutirá más adelante. Por el momento, dejamos sin demostración un par resultados sobre anillos locales regulares. Puede consultarse una prueba en [**González, 2022**] y también sus implicaciones dentro del álgebra homológica.

El primero de tales resultados, como ya se dijo en el Apéndice B, consiste en que la propiedad de ser regular es una propiedad local de los anillos locales noetherianos.

Teorema D.8. **(de Serre)**
*Sea $(A, \mathfrak{m})$ un anillo local noetheriano. Entonces, $(A, \mathfrak{m})$ es regular si y solamente si el anillo local noetheriano $(A_{\mathfrak{p}}, \mathfrak{p}A)$ es regular para cada ideal primo $\mathfrak{p} \in Spec(A)$.*

Este otro resultado asegura que todo anillo local regular es un DFU y que puede aplicarse otros resultados como el Corolario D.6, o también los Teoremas del Ascenso C.16 y del Descenso C.21 dado que, en particular, los DFU son dominios de integridad normales (véase el Ejemplo C.18).

Teorema D.9. **(de Auslander-Buchsbaum)**
*Sea $(A, \mathfrak{m})$ un anillo local regular. Entonces, $(A, \mathfrak{m})$ es un dominio de factorización única.*

Lo que resta por hacer en este apartado es presentar el Criterio del Jacobiano. Para ello, vemos antes una caracterización de los anillos cociente de anillos locales regulares que son a su vez anillos locales regulares. Inmediatamente después definiremos la derivada de un polinomio en un anillo respecto de alguna de sus variables.

Proposición D.10. *Sea $(A, \mathfrak{m})$ un anillo local regular de dimensión $d$. Para $r \leq d$, sea un subconjunto $\{a_1, \ldots, a_r\}$ del ideal $\mathfrak{m}$. Entonces, las siguientes propiedades son equivalentes:*

- *(i) El conjunto $\{a_1, \ldots, a_r\}$ está incluido en algún sistema regular de parámetros del anillo local regular $(A, \mathfrak{m})$.*
- *(ii) Las clases $a_1 + \mathfrak{m}^2, \ldots, a_r + \mathfrak{m}^2$ de $\mathfrak{m}/\mathfrak{m}^2$ son linealmente independientes sobre $A/\mathfrak{m}$.*
- *(iii) $A/(a_1, \ldots, a_r)$ es un anillo local regular de dimensión $n - r$.*

*Si se satisface alguna de estas propiedades, entonces $(a_1, \ldots, a_r)$ es un ideal primo de $A$.*

Definición 64. **(Derivada de un Polinomio en un Anillo)**
*Sea $A$ un anillo conmutativo y sea $f \in A[X_1, \ldots, X_n]$. Supongamos que existen $d_i \in \mathbb{N}$ y unos polinomios $\hat{f}_0, \ldots, \hat{f}_{d_i} \in A[X_1, \ldots, X_n]$ que no dependen de la variable $X_i$, de tal modo que:*

$$f = \sum_{k=0}^{d_i} \hat{f}_k X^k.$$

*Entonces, se define la derivada de $f$ respecto de $X_i$ como el polinomio siguiente:*

$$\frac{\partial f}{\partial X_i}(X_1, \ldots, X_n) = \sum_{k=0}^{d_i - 1} (k+1) \hat{f}_{k+1} X^k.$$

Con esto, pasemos a ver el Criterio del Jacobiano dentro de un contexto particular. Sea $R$ un cuerpo realmente cerrado. Consideremos algún punto del espacio afín $p = (p_1, \ldots, p_n) \in \mathbb{A}^n(R)$ y también el ideal maximal asociado a dicho punto $\mathfrak{m}_p = (X_1 - p_1, \ldots, X_n - p_n) \subset R[X_1, \ldots, X_n]$. Dados unos polinomios $f_1, \ldots, f_r \in R[X_1, \ldots, X_n]$, se define la siguiente matriz:

$$\mathcal{J}(f_1, \ldots, f_r)(p) = \left( \frac{\partial f_i}{\partial X_j}(p) \right)_{\substack{i=1,\ldots,r \\ j=1,\ldots,n.}}$$

que se dice matriz jacobiana. El Criterio del Jacobiano es un resultado que permite reducir el estudio de la variedad algebraica definida por los polinomios $f_1, \ldots, f_r$ en un punto de dicha variedad $p \in \mathcal{Z}_{\mathbb{A}^n(R)}(f_1, \ldots, f_r)$ (relacionado con la localización $R[X_1, \ldots, X_n]_{\mathfrak{m}_p}$) al estudio de la matriz jacobiana definida en tales circunstancias.

Teorema D.11. **(Criterio del Jacobiano)**
*Sea $R$ un cuerpo realmente cerrado. Consideremos el punto $p \in \mathcal{Z}_{\mathbb{A}^n(R)}(f_1, \ldots, f_r)$ de la variedad algebraica definida por unos polinomios $f_1, \ldots, f_r \in R[X_1, \ldots, X_n]$. Denotemos por $(A, \mathfrak{m})$ al anillo local regular asociado a dicho punto, es decir, $A = R[X_1, \ldots, X_n]_{\mathfrak{m}_p}$ y $\mathfrak{m} = \mathfrak{m}_p A$. Supongamos que $r \leq n$. Entonces, son equivalentes:*

- *(i) El conjunto $\{f_1, \ldots, f_r\}$ es una subfamilia de algún sistema regular de parámetros del anillo local regular $(A, \mathfrak{m})$.*
- *(ii) La matriz jacobiana $\mathcal{J}(f_1, \ldots, f_r)(p)$ tiene rango $n - r$.*
- *(iii) El anillo cociente $A/(f_1, \ldots, f_r)$ es un anillo local regular de dimensión $n - r$.*

*En particular, si se da cualquiera de las Propiedades (i), (ii) o (iii), el ideal $(f_1, \ldots, f_r)$ es un ideal primo en $A$ y en $R[X_1, \ldots, X_n]$, y con altura $r$.*

Observación D.12. Nótese que cualquier variedad algebraica de $\mathbb{A}^n(R)$ puede definirse por un ideal generado por los polinomios $f_1, \ldots, f_r \in R[X_1, \ldots, X_n]$ con $r \leq n$ y que, por lo tanto, esta suposición no implica una pérdida de generalidad a la hora de poder estudiar una variedad algebraica de $\mathbb{A}^n(R)$ cualquiera.

### Puntos Regulares de una Variedad Algebraica Real.

En esta subsección se habla de regularidad y singularidad de los puntos de una variedad algebraica definida en algún espacio afín sobre un cuerpo realmente cerrado. Se presenta varias formas equivalentes de definir a los puntos regulares de una variedad. Para empezar, veamos un resultado sobre el rango de la matriz jacobiana que puede aplicarse a cualquier anillo de la forma $\mathcal{P}(V)$ definido por una variedad algebraica $V \subset \mathbb{A}^n(R)$ irreducible. La razón de escoger una variedad irreducible es que su ideal asociado $\mathcal{I}_{R[X_1,\ldots,X_n]}(V)$ es primo y puede aplicarse el siguiente resultado.

Proposición D.13. *Sea $R$ un cuerpo realmente cerrado. Sea $\mathfrak{p}$ un ideal primo de $R[X_1, \ldots, X_n]$ y sea $\{f_1, \ldots, f_r\} \subset R[X_1, \ldots, X_n]$ una familia de generadores del ideal $\mathfrak{p}$. Se considera el anillo cociente $R[X_1, \ldots, X_n]/\mathfrak{p}$ con dimensión $d = dim_{Krull}(R[X_1, \ldots, X_n]/\mathfrak{p})$ y a su cuerpo de fracciones $k(\mathfrak{p}) = Frac(R[X_1, \ldots, X_n]/\mathfrak{p})$. Se define esta matriz con coordenadas en $k(\mathfrak{p})$:*

$$DF = \left( \frac{\partial f_i}{\partial X_j} + \mathfrak{p} \right)_{\substack{i=1,\ldots,r \\ j=1,\ldots,n}} \in \mathcal{M}_{r \times n}(k(\mathfrak{p})).$$

*Entonces, $DF$ es una matriz de $\mathcal{M}_{r \times n}(k(\mathfrak{p}))$ con rango $n - d$.*

Observemos que la matriz $DF$ que acabamos de definir es parecida a la matriz jacobiana que definimos en la subsección anterior, se distinguen porque en $DF$ no hemos evaluado los polinomios en un punto.

Ahora vemos la definición de Zariski del espacio tangente a un punto $p$ de una variedad algebraica $V \subset \mathbb{A}^n(R)$. Antes de esto, es preciso definir el gradiente de un polinomio $f$ de $R[X_1, \ldots, X_n]$ en un punto $p \in \mathbb{A}^n(R)$ del espacio afín:

$$\nabla_p f = \left( \frac{\partial f}{\partial X_1}(p), \ldots, \frac{\partial f}{\partial X_n}(p) \right).$$

DEFINICIÓN 65. **(Espacio Tangente)**
*Sea $R$ un cuerpo realmente cerrado y sea $V \subset \mathbb{A}^n(R)$ una variedad algebraica irreducible. Sea el punto $p \in V$ y supongamos que $\mathcal{I}_{R[X_1,\ldots,X_n]}(V) = (f_1, \ldots, f_r)$. Se define el espacio tangente a $V$ en el punto $p$ como el siguiente $R$-espacio vectorial:*

$$T_pV = \{v = (v_1, \ldots, v_n) \in \mathbb{A}^n(R) : \nabla_p f_i(v) = \sum_{j=1}^{n} \frac{\partial f_i}{\partial X_j}(p) v_j = 0\}.$$

Es sencillo verificar que esta definición del espacio tangente no depende del conjunto de generadores de $\mathcal{I}_{R[X_1,\ldots,X_n]}(V)$ escogido, y también que se trata de un $R$-espacio vectorial.

Ahora, con las notaciones de la definición precedente, volvamos a la matriz $DF$ de la Proposición D.13 definida para los generadores $f_1, \ldots, f_r$ del ideal pero evaluada en el punto $p$. La denotamos por $DF(p)$ y se trata de una matriz de $\mathcal{M}_{r\times n}(R)$ cuyas filas son los gradientes $\nabla_p f_1, \ldots, \nabla_p f_r$ de los generadores del ideal. Podemos considerar la aplicación lineal que define $DF(p)$:

$$\begin{aligned} DF(p) : \mathbb{A}^n(R) &\longrightarrow \quad \mathbb{A}^r(R) \\ v \quad &\longmapsto DF(p) \cdot v, \end{aligned}$$

y el núcleo de esta aplicación lineal será el espacio tangente a $V$ en $p$, es decir, se tendrá que $T_pV = ker(DF(p))$. La dimensión de $T_pV$ como $R$-espacio vectorial viene dada por el rango de la matriz $DF(p)$ y es:

$$dim_R(T_pV) = n - rank(DF(p)).$$

Volvamos a la Proposición D.13. El rango de la matriz $DF$ para un sistema de generadores del ideal $\mathcal{I}_{R[X_1,\ldots,X_n]}(V)$ será igual que la dimensión de Krull del anillo $\mathcal{P}(V)$. Para la matriz evaluada en un punto $p$, $DF(p)$, se sabe que si un menor de $DF$ es nulo, entonces también lo será en $DF(p)$, pero no necesariamente a la inversa y entonces se sigue la desigualdad siguiente.

COROLARIO D.14. *Sea $R$ un cuerpo realmente cerrado y sea $V \subset \mathbb{A}^n(R)$ una variedad algebraica irreducible. Se considera el anillo $\mathcal{P}(v)$ de funciones polinomiales de $V$ en $R$. Entonces, para cada $p \in V$ se verifica:*

$$dim_R(T_pV) \geq dim_{Krull}(\mathcal{P}(V)).$$

Los puntos para los que se satisface la igualdad se dicen puntos regulares de la variedad. Damos la definición a continuación.

DEFINICIÓN 66. **(Puntos Regulares y Singulares)**
*Sea $R$ un cuerpo realmente cerrado. Dado un punto $p$ perteneciente a la variedad algebraica irreducible $V$ de $\mathbb{A}^n(R)$, este se dice punto regular si se satisface:*

$$dim(T_pV) = dim_{Krull}(\mathcal{P}(V)),$$

*y se dirá punto singular en caso contrario. Se denota por $Reg(V)$ al conjunto de los puntos regulares de una variedad, y por $Sing(V)$ al conjunto de puntos singulares.*

En el Capítulo 3 de [**BCR, 1998**] se prueba el resultado siguiente, que trata la dimensión de $Reg(V)$ y $Sing(V)$, así como su relación con la topología de Zariski.

TEOREMA D.15. *Sean $R$ un cuerpo realmente cerrado y $V$ una variedad algebraica irreducible de $\mathbb{A}^n(R)$. Entonces $Reg(V)$ es un abierto no vacío para la topología de Zariski y $Sing(V) \subset V$ es una subvariedad algebraica real, es decir, un cerrado Zariski de $V$ con la topología heredada de $\mathbb{A}^n(R)$, y cuyas dimensiones de Krull satisfacen:*

$$dim_{Krull}(\mathcal{P}(clau_{\mathcal{Z}}(Sing(V)))) < dim_{Krull}(\mathcal{P}(clau_{\mathcal{Z}}(Reg(V)))) = dim_{Krull}(\mathcal{P}(V)).$$

Para probar esto, basta con observar que los puntos de $Reg(V)$ son aquellos en los que no se anula ningún menor $(n-d)\times(n-d)$ de la matriz $DF$ evaluada en cada uno de dichos puntos.

Pasemos a considerar anillos notherianos locales. Dado un punto $p$ de una variedad algebraica irreducible $V$ de $\mathbb{A}^n(R)$, se considera el ideal maximal de $\mathcal{P}(V)$:

$$\mathfrak{m}_p = \{f \in \mathcal{P}(V) : f(p) = 0\}.$$

Con esto, se toma la localización de $\mathcal{P}(V)$ en el ideal maximal $\mathfrak{m}_p$ y se denota por $(\mathcal{R}(V)_p, \overline{\mathfrak{m}}_p)$ al anillo local noetheriano que define la localización, siendo el ideal maximal $\overline{\mathfrak{m}}_p = \mathfrak{m}_p\mathcal{R}(V)_p$. Como el anillo $R[X_1, \ldots, X_n]$ es catenario,[3] se cumple las siguientes igualdades:

$$ht(\mathfrak{m}_p) = dim_{Krull}(\mathcal{R}(V)_p) = dim_{Krull}(\mathcal{P}(V)).$$

También se tiene los siguientes $R$-espacios vectoriales isomorfos. Los dos primeros son isomorfos porque la localización respeta al ideal que queda como maximal, y el otro es el dual del espacio tangente al punto $p$ que, recordemos, define al ideal $\mathfrak{m}_p$. La relación de isomorfía es la siguiente:

$$\mathfrak{m}_p/\mathfrak{m}_p^2 \cong \overline{\mathfrak{m}}_p/\overline{\mathfrak{m}}_p^2 \cong (T_pV)^* = Hom_R(T_pV, R),$$

donde la última relación de isomorfía se tiene porque los elementos de $\mathfrak{m}_p/\mathfrak{m}_p^2$ son clases de polinomios que se anulan en $p$ y que además tienen como representante a un único polinomio homogéneo de grado 1 que se anula en $p$. De manera obvia, los polinomios homogéneos de grado 1 se relacionan con aplicaciones lineales. De las relaciones de isomorfía de anillos dadas se concluye que si $p \in Reg(V)$ es un punto regular de la variedad, entonces:

$$dim_R(\overline{\mathfrak{m}}_p/\overline{\mathfrak{m}}_p^2) = dim_R(T_pV) = dim_{Krull}(\mathcal{P}(V)).$$

A modo de recopilación de todo lo que hemos visto hasta ahora, se tiene el siguiente resultado que nos dice las propiedades equivalentes que satisfacen los puntos regulares.

Corolario D.16. *Sea $R$ un cuerpo realmente cerrado. Sea $V$ una variedad algebraica irreducible de $\mathbb{A}^n(R)$. Entonces, dado un punto $p \in V$, se verifican las siguientes propiedades equivalentes:*

- *(i)* $p \in Reg(V)$,
- *(ii)* $\mathcal{R}(V)_p$ *es un anillo local regular de dimensión igual a* $dim_{Krull}(\mathcal{P}(V))$,
- *(iii)* $dim_R(T_pV) = dim_{Krull}(\mathcal{P}(V))$,
- *(iv)* $rank(DF(p)) = n - dim_{Krull}(\mathcal{P}(V))$,
- *(v)* $dim_R(\mathfrak{m}_p/\mathfrak{m}_p^2) = dim_{Krull}(\mathcal{P}(V)) = dim_{Krull}(\mathcal{R}(V)_p)$.

En particular, observemos tanto la presencia del Criterio del Jacobiano D.11 como del concepto de anillo local regular a la hora de definir a los puntos regulares de una variedad.

[3] Véase la Definición 47 y propiedades en el Apéndice B.

Apéndice E

# Dimensión y Topologías sobre $\mathbb{A}^n(R)$.

La finalidad de este apéndice es introducir las ideas dimensión de un conjunto semi-algebraico y de dimensión puntual en un semi-algebraico utilizando de manera razonada todo lo que se ha visto durante los Apéndices C y D. Antes de dar las definiciones de estos conceptos, es necesario hablar de ciertos temas. Comenzaremos introduciendo una topología en $\mathbb{A}^n(R)$ definida a partir de una norma que recuerda a la norma euclídea de $\mathbb{A}^n(\mathbb{R})$. Después, hablaremos de un tipo especial de funciones y de cómo estas llevan a una descomposición de conjuntos semi-algebraicos en componentes semi-algebraicas con una dimensión topológica clara. Finalmente, trataremos de aplicar las ideas de dimensión de los apéndices previos para dar una definición de dimensión 'algebraica' que coincida con esta idea de dimensión topológica.

Para la elaboración de esta presentación se ha utilizado el Capítulo 2 de [**BCR, 1998**], al que puede remitirse el lector para consultar las pruebas de los enunciados que aquí presentaremos.

**Norma y Topología Euclídea para $\mathbb{A}^n(R)$.**

Comencemos por introducir una generalización de la topología euclídea de $\mathbb{A}^n(\mathbb{R})$ para los espacios afines $\mathbb{A}^n(R)$ con $R$ un cuerpo realmente cerrado. Al contrario que en un cuerpo ordenado, se tiene para cualquier cuerpo realmente cerrado $R$ que la raíz de todo elemento positivo del cuerpo pertenece a $R$, por el Lema 2.1.12, y en particular pertenecen a $R$ las raíces de las sumas de cuadrados de $R$. Por lo tanto, la siguiente aplicación está bien definida:

$$\begin{aligned} ||\cdot|| : \quad \mathbb{A}^n(R) \quad &\longrightarrow \quad R \\ x = (x_1, \ldots, x_n) &\longmapsto ||x|| = \sqrt{x_1^2 + \cdots + x_n^2}, \end{aligned}$$

y es una norma sobre $\mathbb{A}^n(R)$ como $R$-espacio vectorial. Esta norma induce una distancia, y a su vez esta define una topología a la que llamaremos topología euclídea sobre $\mathbb{A}^n(R)$, ya que para el caso real $R = \mathbb{R}$ esta coincide con la topología euclídea sobre $\mathbb{A}^n(\mathbb{R})$. La distancia entre dos puntos $x, y \in \mathbb{A}^n(R)$ viene dada por esta norma y es $||x - y||$. Utilizando esta distancia puede definirse la base de una topología. Tomamos $x \in \mathbb{A}^n(R)$ y $r \in R$ positivo, y con esto se define los conjuntos:

$$\begin{aligned} B_n(x, r) &= \{y \in \mathbb{A}^n(R) : ||y - x|| < r\}, \\ \overline{B}_n(x, r) &= \{y \in \mathbb{A}^n(R) : ||y - x|| \leq r\}, \\ S^{n-1}(x, r) &= \{y \in \mathbb{A}^n(R) : ||y - x|| = r\}, \end{aligned}$$

que se conocen como bola abierta, bola cerrada y $(n-1)$-esfera, respectivamente, de centro $x$ y radio $r$. El conjunto de las bolas abiertas de centro $x \in \mathbb{A}^n(R)$ y radio $r \in R$ positivo son una base para la topología de $\mathbb{A}^n(R)$ que definiremos como la topología euclídea sobre dicho espacio afín. Las bolas cerradas son conjuntos cerrados para esta topología.

Con esta topología en $\mathbb{A}^n(R)$, las funciones polinomiales definidas por cualquier polinomio de $R[X_1, \ldots, X_n]$ son continuas. En particular como $\mathbb{A}^n(R)$ es a la vez un abierto y un cerrado, se tiene que cualquier conjunto definido por una igualdad de la forma $f(X_1, \ldots, X_n) = 0$ con $f \in R[X_1, \ldots, X_n]$ es un cerrado para la topología euclídea. Por lo tanto, también son cerrados en esta topología las uniones finitas de este tipo de conjuntos, es decir, los cerrados para la topología de Zariski son cerrados en la topología euclídea y en conclusión, la topología euclídea es más fina que la topología de Zariski.

Consideremos ahora un conjunto de la forma:

$$\{x \in \mathbb{A}^n(R) : f(x) \geq 0\} = f^{-1}([0, \infty)^n),$$

dado el polinomio $f \in R[X_1, \dots X_n]$. Como este conjunto puede escribirse como la anti imagen del cerrado $[0, \infty)^n$ de $\mathbb{A}^n(R)$ por una aplicación $f$ continua para la topología euclídea, entonces es un conjunto semi-algebraico cerrado. De hecho, las uniones finitas de cerrados son a su vez cerrados, por lo que los conjuntos cerrados básicos son semi-algebraicos cerrados para la topología euclídea sobre $\mathbb{A}^n(R)$. Más aún, T. Recio prueba que los conjuntos semi-algebraicos cerrados para la topología euclídea son de hecho cerrados básicos (puede verse en [**Recio, 1978**]). Teniendo en cuenta que cada conjunto abierto básico es el complementario en $\mathbb{A}^n(R)$ de otro cerrado básico, se tiene que los abiertos básicos son los conjuntos semi-algebraicos abiertos para la topología euclídea sobre $\mathbb{A}^n(R)$.

Sin embargo, no todo cerrado para la topología euclídea es un conjunto semi-algebraico. Veamos un ejemplo. Utilizaremos la función exponencial, que se define puntualmente como la evaluación de la siguiente serie de potencias formal univariada sobre un cuerpo realmente cerrado $R$:

$$exp(X) = \sum_{i=0}^{\infty} \frac{X^i}{i!}.$$

Definimos para cada $k \in \mathbb{N}$ el polinomio univariado $g_k(X) = 1 + X + \ldots + X^k/(k!)$ y nos damos cuenta de que $ev_x(exp) \geq ev_x(g_k)$ para todo $x \in R$ no negativo y para cada $k \in \mathbb{N}$. Entonces, podemos considerar los conjuntos semi-algebraicos cerrados para la topología euclídea de $\mathbb{A}^2(R)$:

$$S_k = \{(x_1, x_2) \in \mathbb{A}^n(R) : x_1 \geq 0, x_2 - g_k(x_1) \geq 0\},$$

definidos para cada $k \in \mathbb{N}$. Definimos también el conjunto:

$$S = \{(x_1, x_2) \in \mathbb{A}^n(R) : x_1 \geq 0, x_2 - exp(x_1) \geq 0\}.$$

Dado que $S_k \subset S_{k+1} \subset S$ para todo $k \in \mathbb{N}$, es fácil argumentar que $S$ coincide con la intersección de todos los $S_k$, y como es una intersección numerable de cerrados, ha de ser también un cerrado, pero que claramente no es un semi-algebraico. Para finalizar este apartado, diremos que sí se cumple que el interior y la clausura de un semi-algebraico de $\mathbb{A}^n(R)$ sean semi-algebraicos (Véase la Proposición 2.2.2 de [**BCR, 1998**]).

**Aplicaciones Semi-Algebraicas.**

A continuación, introducimos un tipo de aplicaciones que sirven para dar una descomposición de los conjuntos semi-algebraicos, la permite ver la equivalencia entre la dimensión topológica de los semi-algebraicos y la dimensión con base en la dimensión de anillos que se define en subsecciones posteriores. En primer lugar, definimos este otro tipo de aplicaciones.

DEFINICIÓN 67. **(Aplicación Semi-Algebraica)**
*Sea $R$ un cuerpo realmente cerrado. Sean $A$ y $B$ conjuntos semi-algebraicos de $\mathbb{A}^n(R)$ y $\mathbb{A}^m(R)$, respectivamente. Una aplicación $f : A \longrightarrow B$ se dice semi-algebraica si su grafo, es decir:*

$$Graf(f) = \{(x, y) \in \mathbb{A}^{n+m}(R) : f(x) = y\}$$

*es un conjunto semi-algebraico de $\mathbb{A}^{n+m}(R)$.*

Lo primero que nos dice la definición es que la imagen de una aplicación semi-algebraica es un conjunto semi-algebraico, sin más que considerar la proyección que olvida a las $n$ primeras coordenadas y el Corolario 1.2.4. Veamos algunos ejemplos de aplicaciones semi-algebraicas.

EJEMPLO E.1. *Los siguientes son ejemplos de aplicaciones semi-algebraicas:*

(I) *La función distancia a un conjunto semi algebraico $S \subset \mathbb{A}^n(R)$, se define como sigue:*

$$\begin{aligned} dist(\cdot, S) : \mathbb{A}^n(R) &\longrightarrow \mathbb{A}(R) \\ x &\longmapsto dist(x, S) = inf\{||x - y|| : y \in S\}. \end{aligned}$$

*Esta aplicación es semi-algebraica, y también continua si se considera a la topología euclídea en ambos espacios.*

(II) *Las operaciones de suma y producto en $R$ llevan a definir las siguientes aplicaciones semi-algebraicas:*

$$\begin{aligned} \mathbb{A}^2(R) &\longrightarrow \mathbb{A}(R) \\ (x_1, x_2) &\longmapsto x_1 + x_2, \end{aligned} \qquad \begin{aligned} \mathbb{A}^2(R) &\longrightarrow \mathbb{A}(R) \\ (x_1, x_2) &\longmapsto x_1 x_2. \end{aligned}$$

La composición de aplicaciones semi-algebraicas es, a su vez, otra aplicación semi-algebraica. Más aún, las aplicaciones semi-algebraicas que van de un conjunto semi-algebraico $S \subset \mathbb{A}^n(R)$ en $\mathbb{A}(R)$ constituyen un anillo con las operaciones de suma y producto de funciones descritas en el ejemplo anterior. Dejamos esto enunciado como una propiedad.

PROPOSICIÓN E.2. *Sea $R$ un cuerpo realmente cerrado y sea $S \subset \mathbb{A}^n(R)$ un conjunto semi-algebraico. Entonces, el conjunto de aplicaciones semi-algebraicas de $S$ en $\mathbb{A}(R)$ es un anillo respecto de la suma y el producto de aplicaciones descritas en el Apartado* (II) *del Ejemplo E.1.*

Lo que hace especial a las aplicaciones semi-algebraicas es la propiedad de transformar conjuntos semi-algebraicos en otros conjuntos semi-algebraicos. Queda escrito a continuación.

PROPOSICIÓN E.3. *Sea $R$ un cuerpo realmente cerrado. Sea $f : S \subset \mathbb{A}^n(R) \longrightarrow T \subset \mathbb{A}^m(R)$ una aplicación semi-algebraica. En ese caso:*

(i) *si $S' \subset S$ es semi-algebraico, se tiene que $f(S')$ es semi-algebraico,*
(ii) *y si $T' \subset T$ es semi-algebraico, entonces $f^{-1}(T')$ es también semi-algebraico.*

Las aplicaciones semi-algebraicas definidas de $\mathbb{A}^n(R)$ en $\mathbb{A}^m(R)$ no siempre son aplicaciones continuas para la topología euclídea en ambos espacios. El tipo de aplicaciones que mencionábamos al principio de este apartado, son aquellas aplicaciones semi-algebraicas que además son homeomorfismos, es decir, biyectivas, continuas para la topología euclídea en ambos espacios y con inversa también continua. Este tipo de aplicaciones se dicen homeomorfismos semi-algebraicos, y también se dice que un par de subconjuntos de $\mathbb{A}^n(R)$ y $\mathbb{A}^m(R)$ son semi-algebraicamente homeomorfos si existe algún homeomorfismo semi-algebraico entre ellos.

**Loncheado de un Conjunto Semi-Algebraico.**

En esta subsección veremos la descomposición de un conjunto semi-algebraico de $\mathbb{A}^n(R)$ en una unión de conjuntos semi-algebraicos tales que cada uno sea semi-algebraicamente homeomorfo a un hipercubo de dimensión $d \leq n$, es decir, el conjunto $(0,1)^d \subset \mathbb{A}^d(R)$ definido como el producto cartesiano del intervalo abierto $(0,1) = \{x \in R : 0 \leq x \leq 1\}$.

No nos centraremos en la parte técnica necesaria para llegar a dar esta descomposición, que puede verse en las Secciones 1.4 y 2.3 de [**BCR, 1998**], sino más bien en entender qué es esta descomposición de los semi-algebraicos. La siguiente definición viene motivada por el Teorema 2.3.1 de [**BCR, 1998**], y consiste en una técnica que resulta en una partición del espacio $\mathbb{A}^n(R)$ en una familia finita de conjuntos semi-algebraicos, conocida coloquialmente como loncheado.

DEFINICIÓN 68. **(Loncheado del Espacio Afín)**
*Sea $R$ un cuerpo realmente cerrado. Sean $f_1, \ldots, f_r \in R[X_1, \ldots, X_n, Y]$. Se tiene una partición de $\mathbb{A}^n(R)$ en conjuntos semi-algebraicos $S_1, \ldots, S_k$ junto a las aplicaciones:*

$$\zeta_{i,j} : S_i \longrightarrow \mathbb{A}(R), \text{ con } i = 1, \ldots, k, \ j = 1, \ldots, s_i,$$

*semi-algebraicas y continuas para la topología euclídea en $\mathbb{A}^n(R)$, de modo que se cumple para cada $i = 1, \ldots, k$ y dado $x \in S_i$:*

(i) *que $\{\zeta_{i,1}(x), \ldots, \zeta_{i,s_i}(x)\}$ es el conjunto de las raíces de los polinomios univariados $f_1(x,Y), \ldots, f_r(x,Y)$ que sean no nulos,*
(ii) *y que dado $y \in \mathbb{A}(R)$, el signo de cada $f_1(x,y), \ldots, f_r(x,y)$ depende únicamente de los signos de $y - \zeta_{i,1}(x), \ldots, y - \zeta_{i,s_i}(x)$.*

*En tal caso, se dirá que es el loncheado de $\mathbb{A}^n(R)$ dado por $f_1, \ldots, f_r$ a la partición $S_1, \ldots, S_k$ de $\mathbb{A}^n(R)$ junto con las aplicaciones $\zeta_{i,j}$. Se denotará el loncheado por $(S_i, (\zeta_{i,1}, \ldots, \zeta_{i,s_i}))_{i=1,\ldots,k}$.*

La descomposición de un semi-algebraico que se mencionaba al principio puede hallarse con este resultado, haciendo un argumento de inducción en $n$ y construyendo cierta aplicación semi-algebraica. No nos ocuparemos de reproducir aquí la prueba, pero sí se va a enunciar el resultado.

TEOREMA E.4. *Dado un cuerpo realmente cerrado $R$, todo conjunto semi-algebraico de $\mathbb{A}^n(R)$ es la unión disjunta de un número finito de conjuntos semi-algebraicos tales que cada uno de ellos es semi-algebraicamente homeomorfo a un hipercubo $(0,1)^d \subset \mathbb{A}^d(R)$ para algún $d \in \mathbb{N}$.*

Se introduce algo de notación para esta descomposición de un conjunto semi-algebraico $S$ de $\mathbb{A}^n(R)$. Nos referiremos a ella como loncheado de $S$ y la denotaremos por $(S_1, \phi_1), \ldots, (S_r, \phi_r)$, siendo $S_1, \ldots, S_r$ la partición de $S$ en conjuntos semi-algebraicos y $\phi_i$ el homeomorfismo semi-algebraico que aplica a $S_i$ en $(0,1)^{d_i}$ para algún $d_i \leq n$ y para todo $i = 1, \ldots, r$. También llamaremos componente semi-algebraica de $S$ a cada uno de los $S_i$.

**Dimensión de Conjuntos Semi-Algebraicos.**

Este apartado se dedica a dar una definición de dimensión para los conjuntos semi-algebraicos y a ver que se cumple la siguiente observación sobre el loncheado de un conjunto semi-algebraico. Dado el hipercubo $(0,1)^d$, se tiene que $d$ es su dimensión como variedad topológica de $\mathbb{A}^n(R)$. Entonces, si se tiene un conjunto semi-algebraico $S$ de $\mathbb{A}^n(R)$, damos un loncheado de $\mathbb{A}^n(R)$ que defina a $(S_1, \phi_1), \ldots, (S_r, \phi_r)$ como un loncheado de $S$ y llamamos $d_i$ a la dimensión topológica de cada hipercubo $\phi_i(S_i)$, es de esperar que la dimensión que definamos para $S$ coincida con el máximo de las dimensiones topológicas de los $S_1, \ldots, S_r$, que por la relación de homeomorfía serán $d_1, \ldots, d_r$.

Nos aventuramos a dar una definición puramente algebraica de dimensión para los conjuntos semi-algebraicos, con la condición de que se respete esta propiedad. Será útil considerar el resultado siguiente, cuya prueba se basa en las propiedades del ideal generado y en que la topología euclídea sobre $\mathbb{A}^n(R)$ es más fina que la de Zariski. Esto último lleva a que $clau_{Euc}(S) \subset clau_{\mathcal{Z}}(S)$ para todo semi-algebraico $S \subset \mathbb{A}^n(R)$, donde $clau_{Euc}(S)$ denota a la clausura de $S$ por la topología euclídea sobre $\mathbb{A}^n(R)$ y $clau_{\mathcal{Z}}(S)$ es la clausura Zariski de $S$.

Proposición E.5. *Sea $R$ un cuerpo realmente cerrado y sea $S \subset \mathbb{A}^n(R)$ un conjunto semi-algebraico. Entonces se tiene las siguientes igualdades:*

$$\mathcal{I}_{R[X_1,\ldots,X_n]}(S) = \mathcal{I}_{R[X_1,\ldots,X_n]}(clau_{Euc}(S)) = \mathcal{I}_{R[X_1,\ldots,X_n]}(clau_{\mathcal{Z}}(S)).$$

Este resultado nos asegura que el ideal asociado a un conjunto semi-algebraico $S \subset \mathbb{A}^n(R)$ es el mismo que el de sus clausuras para la topología euclídea y la de Zariski sobre $\mathbb{A}^n(R)$ y, por lo tanto, puede asociarse a $S$ el anillo de polinomios $\mathcal{P}(clau_{\mathcal{Z}}(S))$. De este modo, la dimensión de un semi-algebraico será la dimensión de Krull del anillo de polinomios descrito.

Definición 69. **(Dimensión de un Conjunto Semi-Algebraico)**
*Sea $R$ un cuerpo realmente cerrado y sea $S$ un conjunto semi-algebraico de $\mathbb{A}^n(R)$. Se define la dimensión de $S$ como:*

$$dim(S) = dim_{Krull}(\mathcal{P}(clau_{\mathcal{Z}}(S))).$$

Observación E.6. En vista de la definición precedente y la Proposición E.5, se tiene que:

$$dim(S) = dim(clau_{Euc}(S)) = dim(clau_{\mathcal{Z}}(S)).$$

Veamos una primera consecuencia de esta definición de dimensión. Nótese que la primera afirmación es consecuencia directa del Corolario C.24.

Proposición E.7. *Sea $R$ un cuerpo realmente cerrado. Se cumple las siguientes propiedades:*

(*i*) $dim(\mathbb{A}^n(R)) = n$.

(*ii*) *Sean $S_1, S_2 \subset \mathbb{A}^n(R)$ unos conjuntos semi-algebraicos tales que $S_1 \subset S_2$. Entonces:*

$$dim(S_1) \leq dim(S_2).$$

Otras propiedades sobre la dimensión que se prueban en [**BCR, 1998**] son las siguientes.

Proposición E.8. *Sea $R$ un cuerpo realmente cerrado. Entonces, se cumple que:*

(*i*) *Si $U \subset \mathbb{A}^n(R)$ es un abierto no vacío para la topología euclídea sobre $\mathbb{A}^n(R)$, entonces:*

$$dim(U) = n.$$

(*ii*) *Si $S \subset \mathbb{A}^n(R)$ es un conjunto semi-algebraico, se tendrá que:*

$$dim(clau_{\mathcal{Z}}(S) \setminus S) < dim(S).$$

(*iii*) *Si $V_1, V_2 \subset \mathbb{A}^n(R)$ son un par de conjuntos algebraicos tales que $V_1 \subsetneq V_2$, se sigue que:*

$$dim(V_1) < dim(V_2).$$

Sigamos con un surtido de propiedades de la dimensión de semi-algebraicos acerca de las operaciones con semi-algebraicos que conocemos: uniones e intersecciones finitas, proyección y producto cartesiano.

PROPOSICIÓN E.9. *Sea $R$ un cuerpo realmente cerrado. Se tienen las siguientes propiedades para la dimensión de semi-algebraicos:*

(*i*) *Si $S_1, \ldots, S_r$ son conjuntos semi-algebraicos de $\mathbb{A}^n(R)$, entonces:*
$$dim(S_1 \cup \cdots \cup S_r) = \max_{i=1,\ldots,r}(\{dim(S_i)\}).$$

(*ii*) *Si $S_1, \ldots, S_r$ son conjuntos semi-algebraicos de $\mathbb{A}^n(R)$, entonces:*
$$dim(S_1 \cap \cdots \cap S_r) \leq \min_{i=1,\ldots,r}(\{dim(S_i)\}).$$

(*iii*) *Si $S \subset \mathbb{A}^{n+m}(R)$ es un conjunto semi-algebraico y $\pi$ es la proyección de $\mathbb{A}^{n+m}(R)$ en $\mathbb{A}^n(R)$ que olvida las $m$ últimas coordenadas, entonces:*
$$dim(\pi(S)) \leq dim(S).$$

(*iv*) *Si $S \subset \mathbb{A}^n(R)$ y $T \subset \mathbb{A}^m(R)$ son conjuntos semi-algebraicos, entonces:*
$$dim(S \times T) = dim(S) + dim(T),$$
*entendiendo la dimensión de $S \times T$ como la de un semi-algebraico de $\mathbb{A}^{n+m}(R)$.*

OBSERVACIÓN E.10. De la Afirmación $(i)$ de la proposición precedente se sigue que la dimensión de un conjunto algebraico $V \subset \mathbb{A}^n(R)$ es el máximo de las dimensiones de las componentes de su descomposición en irreducibles. Por el mismo motivo, dado un conjunto $S \subset \mathbb{A}^n(R)$ semi-algebraico, se tiene que su dimensión coincide con el máximo de las dimensiones de las componentes de cualquier loncheado de $S$.

Llegados a este punto, tan solo nos falta por ver que cada componente semi-algebraica $S_i$ del loncheado $(S_1, \phi_1), \ldots, (S_r, \phi_r)$ de un conjunto semi-algebraico $S \subset \mathbb{A}^n(R)$ cumpla que su dimensión topológica, heredada de los hipercubos $\phi_i(S_i)$ por su relación de homeomorfía con cada $S_i$, coincida con la dimensión 'algebraica' del conjunto semi-algebraico $S$ en cuestión. Para ver esto, será necesario dar el siguiente resultado sobre aplicaciones semi-algebraicas.

TEOREMA E.11. *Sea $R$ un cuerpo realmente cerrado. Sea $S$ un conjunto semi-algebraico de $\mathbb{A}^n(R)$ y sea $f : S \to \mathbb{A}^m(R)$ una aplicación semi-algebraica. En ese caso:*
$$dim(S) = dim(Graf(f)).$$
*Además, para cualquier subconjunto $S' \subset S$ semi-algebraico en $\mathbb{A}^n(R)$ se tiene que:*
$$dim(S') \geq dim(f(S')).$$
*Adicionalmente, si $f$ es biyectiva se tendrá la igualdad.*

Utilizando varias de las propiedades sobre dimensión que hemos visto previamente y en especial este último resultado, puede probarse finalmente que la noción de dimensión que se utiliza es coherente con la observación del principio sobre el loncheado de un conjunto semi-algebraico y la dimensión topológica de sus componentes semi-algebraicas.

COROLARIO E.12. *Sea $R$ un cuerpo realmente cerrado y sea $S$ un conjunto semi-algebraico de $\mathbb{A}^n(R)$. Sea $(S_1, \phi_1), \ldots, (S_r, \phi_r)$ un loncheado de $S$ y sea $d_i$ la dimensión topológica de cada hipercubo $\phi_i(S_i)$. Entonces, se cumple la igualdad:*
$$dim(S) = max(\{d_1, \ldots, d_r\}).$$

En vista de la Observación E.10, deducimos que lo relevante que se debe probar en este resultado no es el hecho de que la dimensión de $S$ sea el máximo de las dimensiones que deberían tener los $S_i$, sino que la dimensión de cada $S_i$ efectivamente coincida con la dimensión topológica que hereda de $\phi_i(S_i)$ por homeomorfía.

**Dimensión Puntual de una Variedad Algebraica.**

Finalizamos esta sección viendo la noción puntual de dimensión de una variedad. Trataremos de relacionar esta idea con la del espacio tangente, introducida para el estudio de la regularidad de los puntos de una variedad. También enunciamos algunas propiedades relacionadas con la dimensión puntual.

Para comenzar, veamos la propiedad que motiva la definición de dimensión local. Se considera un conjunto semi-algebraico $S \subset \mathbb{A}^n(R)$ y algún punto $p \in S$. Llamaremos entorno semi-algebraico de $p$ en $S$ a un subconjunto $U \subset \mathbb{A}^n(R)$ que sea semi-algebraico y tal que $p \in U \subset S$, y nos fijamos en que una cadena descendente $U_1 \supset U_2 \supset \ldots$ de entornos semi-algebraicos del punto $p$ en $S$ cumplirá que sus ideales asociados formen una cadena ascendente de ideales:

$$\mathcal{I}_{R[X_1,\ldots,X_n]}(U_1) \subset \mathcal{I}_{R[X_1,\ldots,X_n]}(U_2) \subset \ldots \subset \mathcal{I}_{R[X_1,\ldots,X_n]}(U_k) \subset \ldots,$$

la cual se estabiliza en algún elemento porque $R[X_1, \ldots, X_n]$ es noetheriano. Como la dimensión de un semi-algebraico depende exclusivamente del ideal asociado, existe algún entorno semi-algebraico $U$ de $p$ en $S$ para el que todo otro entorno semi-algebraico $U'$ de $p$ en $S$ contenido en $U$ satisface $dim(U') = dim(U)$. Con esto, definimos la dimensión puntual en un semi-algebraico.

Definición 70. **(Dimensión Puntual en un Conjunto Semi-Algebraico)** *Sea $R$ un cuerpo realmente cerrado. Sea $S$ un conjunto semi-algebraico de $\mathbb{A}^n(R)$ y sea $p$ un punto de $S$. Se dice dimensión de $S$ en el punto $p$ a la dimensión de un entorno algebraico $U$ de $p$ en $S$ tal que cada $U' \subset U$ entorno algebraico de $p$ en $S$ cumpla $dim(U') = dim(U)$. La dimensión de $S$ en el punto $p$ se denota por $dim(S_p)$.*

La primera propiedad deseable para una definición puntual de dimensión es que coincida con la dimensión global en el sentido siguiente.

Proposición E.13. *Sea $R$ un cuerpo realmente cerrado y sea $S \subset \mathbb{A}^n(R)$ un conjunto semi-algebraico. Entonces se cumple que:*

$$dim(S) = max(\{dim(S_p) : p \in S\}).$$

Una propiedad destacable de la idea de dimensión puntual es que los puntos de un semi-algebraico con dimensión máxima forman un cerrado Zariski no vacío.

Proposición E.14. *Sea $R$ un cuerpo realmente cerrado. Sea $S$ un conjunto semi-algebraico de $\mathbb{A}^n(R)$ con dimensión $d$. Entonces, el siguiente conjunto es un cerrado Zariski no vacío de dimensión $d$:*

$$S^{(d)} = \{p \in S : dim(S_p) = d\}.$$

En el Apéndice D se introdujo la definición de punto regular de una variedad algebraica de varias formas equivalentes. Cabe preguntarse cuál es la relación entre la dimensión de la variedad en un punto y su regularidad. La respuesta es que los puntos regulares tienen siempre dimensión puntual máxima y que la clausura Zariski de estos puntos es, de hecho, el conjunto de los puntos de la variedad con dimensión puntual máxima.

Proposición E.15. *Sea $R$ un cuerpo realmente cerrado y sea $V$ un conjunto algebraico de $\mathbb{A}^n(R)$ de dimensión $d$. Entonces, se cumple que:*

$$clau_{\mathcal{Z}}(Reg(V)) = V^{(d)},$$

*y en particular, se tiene la inclusión:*

$$Reg(V) \subset V^{(d)}.$$

Si se aplica la Afirmación $(ii)$ de la Proposición E.14 al resultado precedente, se encuentra la siguiente propiedad para las dimensiones de los conjuntos de puntos regulares y singulares de una variedad algebraica.

Corolario E.16. *Sea $R$ un cuerpo realmente cerrado y sea $V$ un conjunto algebraico de $\mathbb{A}^n(R)$. Se satisface que:*

$$dim(Sing(V)) < dim(Reg(V)) = dim(V),$$

*y en particular, se tiene que $Reg(V)$ es un abierto de $\mathbb{A}^n(R)$ para la topología euclídea y también para la topología de Zariski.*

Nótese que este resultado es prácticamente igual al Teorema D.15.

Apéndice F

# Polinomios Homogéneos y Formas Cuadráticas.

En este apartado se desarrolla parte de la teoría básica sobre polinomios simétricos y formas cuadráticas, como apoyo a la Sección 3.4 y la Sección 3.5. En primer lugar, se introduce al anillo de los polinomios simétricos definidos sobre otro anillo conmutativo $A$. Ahí veremos cómo se relaciona con las familias de polinomios simétricos elementales y con las sumas de Newton. Seguidamente, se verá una presentación sobre formas cuadráticas y sus propiedades más elementales. Hablaremos aquí del concepto de espacio cuadrático y de las operaciones de suma directa y producto tensorial de estos espacios y de cómo estas ideas sirven también para formas cuadráticas. Después, comentaremos la diagonalización de las formas cuadráticas y la caracterización de formas cuadráticas equivalentes en cuerpos algebraicamente cerrados y cuerpos realmente cerrados, destacando para este último el conocido Teorema de Inercia de Sylvester. Luego se verá la Descomposición de Witt para formas cuadráticas y finalmente, los Teoremas de Representación. Una representación de un elemento por una forma cuadrática consiste en la existencia de un punto en el cual la evaluación de dicha forma en el punto es el elemento. Esta idea sirve para hablar del número de cuadrados necesarios para representar a un elemento positivo. Antes de empezar, debe definirse al anillo de los polinomios homogéneos.

Definición 71. **(Polinomio Homogéneo)**
*Sea $A$ un anillo conmutativo, y sea un polinomio $f \in A[X_1, \ldots, X_n]$. El polinomio $f$ se dice homogéneo de grado $d$ si puede escribirse de la manera siguiente:*

$$\sum_{\mu_1+\ldots+\mu_n=d} a_{\mu_1,\ldots,\mu_n} X_1^{\mu_1} \cdot \ldots \cdot X_n^{\mu_n},$$

*donde todos los $a_{\mu_1,\ldots,\mu_n}$ son elementos de $A$ con alguno de ellos no nulo.*

Se denota por $A[X_1, \ldots, X_n]_{hom}$ el conjunto de los polinomios homogéneos, y también se denota por $A[X_1, \ldots, X_n]_{hom}^{(d)}$ al subconjunto de los polinomios homogéneos de grado $d$ junto con el polinomio nulo 0. El producto de un polinomio homogéneo de grado $d_1$ con otro de grado $d_2$ será siempre un polinomio homogéneo de grado $d_1 d_2$, por lo que $A[X_1, \ldots, X_n]_{hom}$ será un anillo graduado dado por la graduación:

$$A[X_1, \ldots, X_n]_{hom}^{(1)}, A[X_1, \ldots, X_n]_{hom}^{(2)}, \ldots, A[X_1, \ldots, X_n]_{hom}^{(k)}, \ldots$$

Es decir, estos conjuntos satisfacen las hipótesis de la Definición 61. De aquí en adelante nos interesaremos principalmente por el caso en que $A$ sea un cuerpo $K$. La elaboración de esta sección se ha basado fundamentalmente en el Capítulo 10 de [**Gantmacher, 1959**] y en los Capítulos 1 y 9 de [**Lam, 1973**].

### Polinomios Simétricos y Sumas de Newton.

Comencemos definiendo a los polinomios simétricos. Denotaremos por $\Sigma_n$ al grupo de permutaciones de $n$ elementos.

Definición 72. **(Polinomio Simétrico)**
*Sea $A$ un anillo conmutativo, y sea un polinomio $f \in A[X_1, \ldots, X_n]$. Este polinomio se dice simétrico si para cualquier permutación $\tau \in \Sigma_n$ se cumple que:*

$$f(X_1, \ldots, X_n) = f(X_{\tau(1)}, \ldots, X_{\tau(n)}).$$

Ocurre que el conjunto de los polinomios simétricos es de hecho un anillo. Más aún, este puede darse como una estructura de $A$-álgebra finita. Sea el anillo de los polinomios simétricos definidos sobre un anillo conmutativo $A$ y unas variables $X_1, \ldots, X_n$ algebraicamente independientes

sobre $A$. Se define para cada $k = 1, \ldots, n$ el polinomio simétrico siguiente:

$$\sigma_k(X_1, \ldots, X_n) = \sum_{1 \leq i_1 < \ldots < i_k \leq n} X_{i_1} \cdot \ldots \cdot X_{i_k}.$$

Llamamos polinomios simétricos elementales a los polinomios $\sigma_1, \ldots, \sigma_n$, y sucede que el anillo de polinomios simétricos definidos sobre $A$ y en las variables $X_1, \ldots, X_n$ es la $A$-álgebra finita $A[\sigma_1, \ldots, \sigma_n]$. Es decir, que un polinomio simétrico definido sobre $A$ y en las variables $X_1, \ldots, X_n$ puede escribirse como una combinación lineal con coeficientes en $A$ de polinomios simétricos. Los polinomios simétricos aparecen en el estudio de las raíces de polinomios univariados. Dado un cuerpo $K$, supongamos que $f \in K[X]$ es un polinomio univariado que escinde completamente en $K[X]$ (como sería el caso de cualquier polinomio de $K[X]$ para $K$ un cuerpo algebraicamente cerrado). Entonces $f$ puede escribirse de la forma siguiente:

$$f(X) = a_n X^n + \ldots + a_1 X + a_0 = a_n(X - \lambda_1) \cdot \ldots \cdot (X - \lambda_n),$$

donde los coeficientes $a_0, \ldots, a_n$ pertenecen a $K$, $a_n$ es no nulo y $\lambda_1, \ldots, \lambda_n \in K$ son todas las raíces de $f$, no necesariamente distintas. Desarrollando los productos de polinomios irreducibles a la derecha, se obtiene las siguientes relaciones entre los coeficientes de $f$ y sus raíces:

$$\sum_{1 \leq i_1 < \ldots < i_k \leq n} \lambda_{i_1} \cdot \ldots \cdot \lambda_{i_k} = (-1)^k \frac{a_{n-k}}{a_n},$$

para cada $k = 1, \ldots, n$. Estas ecuaciones se conocen como las Fórmulas de Cardano-Vieta, y relacionan a las raíces de un polinomio con sus coeficientes. Más aún, se observa que la parte a la izquierda de estas igualdades puede escribirse como la evaluación de un polinomio simétrico en algún punto $(\lambda_1, \ldots, \lambda_n) \in K^n$:

$$\sigma_k(\lambda_1, \ldots, \lambda_n) = (-1)^k \frac{a_{n-k}}{a_n},$$

para $k = 1, \ldots, n$. Puede plantearse el descomponer a un polinomio simétrico en componentes homogéneas. Los polinomios simétricos homogéneos resultan ser la siguiente familia de polinomios, conocidos como sumas de Newton y que se definen para cada $k = 1, \ldots, n$ como:

$$N_k(X_1, \ldots, X_n) = X_1^k + \ldots + X_n^k.$$

Las familias de polinomios simétricos $\sigma_1, \ldots, \sigma_n$ y $N_1, \ldots, N_n$ se relacionan por medio de las Identidades de Newton-Girard:

$$k\sigma_k = \sum_{i=1}^{k} (-1)^{i-1} \sigma_{i-1} N_i,$$

definidas para cada $k = 1, \ldots, n$ y donde se emplea la constante $\sigma_0 = 1$. En conclusión, el anillo de los polinomios simétricos también puede describirse como la $A$-álgebra finita $A[N_1, \ldots, N_n]$, donde los generadores $N_1, \ldots, N_n$ además de ser polinomios simétricos son homogéneos.

**Formas Cuadráticas y Espacios Cuadráticos.**

En este apartado introducimos a las formas cuadráticas y su relación con las matrices simétricas, definiendo la equivalencia de formas cuadráticas. Después, veremos cómo se relaciona esto con las formas bilineales simétricas definidas sobre un espacio vectorial y hablaremos del concepto de espacio cuadrático y de isometría de espacios cuadráticos. Comencemos por definir a una forma cuadrática.

DEFINICIÓN 73. **(Forma Cuadrática)**
*Sea $K$ un cuerpo y sea un entero $n \geq 1$. Se dice forma cuadrática a cualquier polinomio $Q \in K[X_1, \ldots, X_n]$ homogéneo y de grado 2. En estas circunstancias, se dice que $Q$ es una forma cuadrática en $n$ variables.*

Una forma cuadrática $Q \in K[X_1, \ldots, X_n]$ puede escribirse en la forma:

$$Q(X_1, \ldots, X_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{i,j} X_i X_j = \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{a_{i,j} + a_{j,i}}{2} X_i X_j,$$

de modo que admite una representación como producto matricial dado por una matriz simétrica. Si se denota dicha matriz por $M_Q$, entonces:

$$Q(X_1, \ldots, X_n) = X^T M_Q X,$$

donde $X$ denota al vector columna $(X_1 \ldots X_n)$. Es importante resaltar que si el cuerpo $K$ tiene característica 2, entonces puede encontrarse que alguna forma cuadrática admita más de una representación matricial. Por ejemplo, la forma $X_1^2 \in \mathbb{F}_2[X_1, X_2]$ definida sobre el cuerpo primo con característica 2 puede describirse con dos matrices simétricas distintas de $\mathcal{M}_{2\times 2}(\mathbb{F}_2)$:

$$Q(X_1, X_2) = X^T \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} X = X_1^2 = X_1^2 + 2X_1X_2 = X^T \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} X,$$

donde $X = (X_1\ X_2)$. En lo que sigue trabajaremos únicamente con cuerpos con característica distinta de 2, de manera que la representación matricial de toda forma cuadrática será única. Esto implica que la relación de congruencia para matrices simétricas define una relación de equivalencia para las formas cuadráticas de $K[X_1, \ldots, X_n]$. Un par de matrices $M_1, M_2 \in \mathcal{M}_{n\times n}(K)$ se dicen congruentes si existe una matriz regular $P \in \mathcal{M}_{n\times n}(K)$ tal que $M_1 = P^T M_2 P$. En definitiva, un par de formas cuadráticas $Q_1, Q_2 \in K[X_1, \ldots, X_n]$ se dirán equivalentes cuando sus matrices simétricas asociadas $M_{Q_1}$ y $M_{Q_2}$ sean congruentes. En tal caso, se tiene una transformación lineal de las variables $X_1, \ldots, X_n$ algebraicamente independientes sobre $K$ en otras variables $Y_1, \ldots, Y_n$ algebraicamente independientes sobre $K$ de modo que $Q_1(X_1, \ldots, X_n) = Q_2(Y_1, \ldots, Y_n)$. Nótese que en notación matricial, si $P \in \mathcal{M}_{n\times n}(K)$ es una matriz regular tal que $M_{Q_1} = P^T M_{Q_2} P$, entonces:

$$Q_1(X) = X^T M_{Q_1} X = X^T (P^T M_{Q_2} P) X = (PX)^T M_{Q_1} (PX) = Q_2(PX) = Q_2(Y),$$

donde se denota por $Y$ al vector columna $(Y_1 \ldots Y_n)$.

Las matrices simétricas de $\mathcal{M}_{n\times n}(K)$ están relacionadas con las formas bilineales simétricas definidas sobre algún $K$-espacio vectorial de dimensión $n$. Definimos este tipo de aplicaciones.

DEFINICIÓN 74. **(Forma Bilineal Simétrica)**
*Sea $K$ un cuerpo y $V$ un $K$-espacio vectorial de dimensión $n$. Se dice forma bilineal a toda aplicación $\phi : V \times V \to K$ tal que:*

*(i)* $\phi(\lambda_1 x_1 + \lambda_2 x_2, y) = \lambda_1 \phi(x_1, y) + \lambda_2 \phi(x_2, y)$ *para cada* $x_1, x_2, y \in V$ *y cada* $\lambda_1, \lambda_2 \in K$.

*(ii)* $\phi(x, \mu_1 y_1 + \mu_2 y_2) = \mu_1 \phi(x, y_1) + \mu_2 \phi(x, y_2)$ *para cada* $x, y_1, y_2 \in V$ *y cada* $\mu_1, \mu_2 \in K$.

*Si además se tiene que $\phi(x, y) = \phi(y, x)$ para cualesquiera $x, y \in V$, entonces $\phi$ se dice simétrica.*

Expliquemos la relación entre matrices simétricas y formas bilineales simétricas. Se tiene un espacio vectorial $V$ de dimensión $n$ y definido sobre un cuerpo $K$ con característica distinta de 2. Dada una base del $K$-espacio vectorial $V$, se tendrá un isomorfismo lineal $T$ que asocie cada vector de $V$ con unas coordenadas en el espacio $K^n$ dadas respecto de esa base. Si $\phi$ es una forma bilineal simétrica definida sobre $V$, entonces existirá una única matriz simétrica $M_\phi$ de $\mathcal{M}_{n\times n}(K)$ que cumpla:

$$\phi(v, w) = T(v)^T M_\phi T(w),$$

para cada par de vectores $v, w \in V$. Diremos que $M_\phi$ es la matriz asociada a la forma bilineal simétrica $\phi$ respecto de la base dada. En general omitiremos mencionar a la base asociada, pero debe tenerse en cuenta que la relación biunívoca entre matrices simétricas y formas bilineales simétricas ocurre cuando se especifica una base del espacio vectorial, ya que de lo contrario no tiene sentido pensar en una representación matricial para la forma cuadrática. Si únicamente se tiene una forma bilineal simétrica $\phi$ definida sobre un espacio vectorial $V$, puede decirse que $\phi$ tiene asociada una clase de matrices simétricas congruentes donde cada elemento de esta clase estará asociado con una base del espacio vectorial.[1]

Dada la correspondencia biyectiva entre formas cuadráticas y matrices simétricas, queda claro que toda esta discusión sobre la relación entre formas bilineales simétricas y matrices simétricas es válida también para formas cuadráticas. Veamos las relaciones explícitas entre una forma cuadrática $Q \in K[X_1, \ldots, X_n]$ que viene representada por la misma matriz simétrica que se

[1] A primera vista puede parecer que las matrices deban ser semejantes, pero ocurre que un par de matrices simétricas son semejantes si y solamente si son congruentes.

asocia a una forma bilineal simétrica $\phi$ definida sobre el $K$-espacio vectorial $V$ y respecto de una base en la que el isomorfismo lineal $T$ lleve a cada vector de $V$ a sus coordenadas en $K^n$. En tales condiciones se cumple que:

$$\phi(v,w) = \frac{1}{2}(Q(T(v)+T(w)) - Q(T(v)) - Q(T(w))),$$

para cada $v, w \in V$, y también se cumple que:

$$Q(x) = \phi(T^{-1}(x), T^{-1}(x)),$$

para cada $x \in K^n$. Estas relaciones sirven para encontrar una forma cuadrática asociada a una forma bilineal simétrica y viceversa. Las formas cuadráticas se definen, en algún sentido, sobre el $K$-espacio vectorial modelo de dimensión $n$, $K^n$. La definición siguiente, digamos, es la generalización de una forma cuadrática definida sobre $K^n$ a una noción que se puede definir sobre cualquier espacio vectorial isomorfo a $K^n$.

DEFINICIÓN 75. **(Espacio Cuadrático)**
*Sea $K$ un cuerpo con característica distinta de 2 y sea $V$ un $K$-espacio vectorial de dimensión $n$. Sea $\phi$ una forma bilineal simétrica definida sobre $V$. Se dice espacio cuadrático al par $(V, \phi)$.*

De forma totalmente análoga al caso de una forma bilineal simétrica, un espacio cuadrático tendrá asociadas una clase de matrices simétricas congruentes y también una clase de formas cuadráticas equivalentes. Esto lleva a definir una relación de equivalencia de espacios cuadráticos. Un par de espacios cuadráticos definidos sobre sendos $K$-espacios vectoriales de dimensión $n$ se dicen isométricos si las clases de formas cuadráticas equivalentes asociadas a ambos coinciden. La siguiente propiedad caracteriza a los espacios cuadráticos isométricos.

PROPOSICIÓN F.1. *Sean $V_1$ y $V_2$ un par de $K$-espacios vectoriales de dimensión finita $n$ y con $K$ un cuerpo con característica distinta de 2. Un par de espacios cuadráticos $(V_1, \phi_1)$ y $(V_2, \phi_2)$ serán isométricos si y solamente si existe algún isomorfismo lineal $T : V_1 \to V_2$ tal que para todo $v, w \in V_1$ se cumpla que $\phi_1(v,w) = \phi_2(T(v), T(w))$.*

Diremos que una forma cuadrática $Q \in K[X_1, \ldots, X_n]$ es regular si su matriz simétrica asociada es regular (esto es, si su determinante es no nulo), y se dice singular en caso contrario. También diremos que un espacio cuadrático es regular si alguna de sus formas cuadráticas asociadas es regular, y se dirá que es singular en caso contrario. Con esta idea enunciamos otra propiedad de los espacios cuadráticos.

PROPOSICIÓN F.2. *Sea $K$ un cuerpo con característica distinta de 2 y sea $V$ un $K$-espacio vectorial de dimensión $n$. Sea $(V, \phi)$ un espacio cuadrático. Entonces, son equivalentes:*

- *(i) La matriz asociada a cualquiera de las formas cuadráticas asociadas al espacio $(V, \phi)$ es no singular.*
- *(ii) Se tiene un isomorfismo entre $V$ con su espacio dual $V^* = Hom_K(V, V)$ dado por $x \mapsto \phi(\cdot, x)$.*
- *(iii) No existe $x \in V$ distinto de 0 y tal que $\phi(x, y) = 0$ para todo $y \in V$.*

En [**Lam, 1973**] se encuentra utilidad a estas propiedades y también a la noción de espacio cuadrático para probar resultados sobre formas cuadráticas.

**Operaciones con Espacios Cuadráticos y Diagonalización.**

En este apartado veremos que las clases de formas cuadráticas equivalentes poseen siempre algún representante cuya matriz asociada es diagonal. Por el camino también definiremos algunas operaciones para espacios cuadráticos, que también pueden entenderse como operaciones de formas cuadráticas. El primer paso será definir la representación de unidades.

DEFINICIÓN 76. **(Representación de Unidades por una Forma Cuadrática)**
*Sea $K$ un cuerpo con característica distinta de 2 y sea $Q \in K[X_1, \ldots, X_n]$ una forma cuadrática. Sea $K_1$ una $K$-álgebra y sea $u$ una unidad de $K_1$. Se dice que $Q$ representa a $u$ sobre $K_1$ cuando existe $x \in K_1^n$ tal que $Q(x) = u$. Se denota por $D_{K_1}(Q)$ al conjunto de unidades de $K_1$ que vienen representadas por $Q$ sobre $K_1$. La forma $Q$ se dirá universal sobre $K_1$ si $D_{K_1}(Q)$ contiene a todas las unidades de $K_1$.*

Se observa que si $Q_1, Q_2 \in F[X_1, \ldots, X_n]$ son formas cuadráticas equivalentes, entonces coincide $D_F(Q_1)$ con $D_F(Q_2)$ y puede decirse que una unidad viene representada por un espacio cuadrático si viene representada por alguna de sus formas cuadráticas asociadas. Otra propiedad es que dadas unas unidades $u$ y $a$ de $K$ y una forma cuadrática $Q \in K[X_1, \ldots, X_n]$, se tiene que $u \in D_K(Q)$ si y solo si $a^2u \in D_K(Q)$.

Ahora definimos un par de operaciones de espacios cuadráticos. Comenzamos por definir la suma ortogonal. Dados un par de espacios cuadráticos $(V_1, \phi_1)$ y $(V_2, \phi_2)$ definidos sobre un mismo cuerpo $K$ de característica distinta de 2, se define el $K$-espacio vectorial $V = V_1 \oplus V_2$ y también la aplicación:

$$\begin{array}{rccc} \phi: & V \times V & \longrightarrow & F \\ & ((v_1, v_2), (w_1, w_2)) & \longmapsto & \phi_1(v_1, w_1) + \phi_2(v_2, w_2), \end{array}$$

de modo que $(V, \phi)$ es un espacio cuadrático que se denomina el espacio suma ortogonal de $(V_1, \phi_1)$ y $(V_2, \phi_2)$. Esta operación de espacios cuadráticos se denota por $V = V_1 \perp V_2$. Damos sentido a esta operación sobre las formas cuadráticas de la manera siguiente. Dadas un par de formas cuadráticas $Q_1 \in K[X_1, \ldots, X_n]$ y $Q_2 \in K[Y_1, \ldots, Y_m]$ definidas sobre un mismo cuerpo $K$, se define la forma suma ortogonal $Q = Q_1 \oplus Q_2$ como aquella forma cuadrática de $K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ que satisface:

$$Q((x, y)) = Q_1(x) + Q_2(y),$$

para cualesquiera $x \in K^n$, $y \in K^m$. Obviamente, si $Q_1$ y $Q_2$ son formas cuadráticas asociadas a los espacios cuadráticos $(V_1, \phi_1)$ y $(V_2, \phi_2)$ respectivamente, entonces $Q_1 \oplus Q_2$ es una forma cuadrática asociada al espacio cuadrático $V_1 \perp V_2$.

Veamos la otra operación de espacios cuadráticos. Esta se conoce como producto tensorial o producto de Kronecker, y se define de la manera siguiente. Sea $K$ un cuerpo con característica distinta de 2 y sean los espacios cuadráticos $(V_1, \phi_1)$ y $(V_2, \phi_2)$ definidos sobre el mismo cuerpo $K$. Se define el $K$-espacio vectorial $V = V_1 \otimes V_2$, que tiene dimensión $dim_K(V) = dim_K(V_1)dim_K(V_2)$. Se define también la forma bilineal simétrica $\phi$ sobre $V$ que satisface:

$$\phi(v_1 \otimes v_2, w_1 \otimes w_2) = \phi_1(v_1, w_1)\phi_2(v_2, w_2),$$

para cada $v_1, w_1 \in V_1$ y cada $v_2, w_2 \in V_2$. Se define el espacio producto tensorial como $(V, \phi)$ y se denota por $(V_1, \phi_1) \otimes (V_2, \phi_2)$. Se consideran un par de formas cuadráticas $Q_1 \in K[X_1, \ldots, X_n]$ y $Q_2 \in K[Y_1, \ldots, Y_m]$ definidas sobre el mismo cuerpo $K$. Se define la forma producto tensorial $Q = Q_1 \otimes Q_2$ como aquella forma cuadrática definida sobre $K$ en $nm$ variables que cumple que:

$$Q(x \otimes y) = Q_1(x)Q_2(y),$$

para todo $x \in K^n$ y todo $y \in K^m$. Nótese que si tenemos un par de formas cuadráticas $Q_1 \in K[X_1, \ldots, X_n]$ y $Q_2 \in K[Y_1, \ldots, Y_m]$ definidas sobre $K$ con matrices asociadas $M_{Q_1}$ y $M_{Q_2}$ respectivamente, la matriz $M_Q$ asociada a la forma producto tensorial $Q = Q_1 \otimes Q_2$ es la dada por el producto de Kronecker de matrices $M_Q = M_{Q_1} \otimes M_{Q_2}$, y por eso esta operación también se conoce como producto de Kronecker. Como la suma ortogonal de formas cuadráticas cumple que su matriz asociada es la suma de las matrices asociadas a cada forma de la suma ortogonal, se tiene las siguientes propiedades conmutativa, asociativa y distributiva en términos de equivalencia de formas.

PROPOSICIÓN F.3. *Sea $K$ un cuerpo con característica distinta de 2. Sean $Q_1, Q_2, Q_3$ y $Q$ unas formas cuadráticas definidas sobre $K$. Entonces:*

- *(i)* $Q_1 \otimes Q_2$ *es equivalente a* $Q_2 \otimes Q_1$,
- *(ii)* $(Q_1 \otimes Q_2) \otimes Q_3$ *es equivalente a* $Q_1 \otimes (Q_2 \otimes Q_3)$,
- *(iii)* $Q \otimes (Q_1 \perp Q_2)$ *es equivalente a* $(Q \perp Q_1) \otimes (Q \perp Q_2)$.

Recordemos que el objetivo es encontrar a un representante de la clase de formas cuadráticas equivalentes que tenga asociada una matriz diagonal. Denotemos por $\langle u \rangle$ a la forma diagonal $Q(X_1) = uX_1^2$, dada una unidad $u \in F$. El siguiente resultado es el primer paso para encontrar ese representante con matriz asociada diagonal.

PROPOSICIÓN F.4. *Sea $K$ un cuerpo con característica distinta de 2 y sea $(V,\phi)$ un espacio cuadrático donde $V$ es un $K$-espacio vectorial. Sea $u \in K$ una unidad. Entonces, $u \in D_K(Q_\phi)$ si y solamente si existe otro espacio cuadrático $(V',\phi')$ tal que $(V,\phi)$ es un espacio cuadrático isométrico a $\langle u\rangle \perp V'$.*

En este resultado se ha mezclado los conceptos de forma cuadrática y de espacio cuadrático en una suma ortogonal. Entenderemos esto como que una forma cuadrática definida sobre el cuerpo $K$ en $n$ variables define un espacio cuadrático $(K^n,\phi_Q)$ donde $\phi_Q$ es la forma bilineal con la misma matriz asociada que $Q$ si consideramos la base canónica en $K^n$. En lo que sigue, deberá entenderse esta misma aclaración.

El resultado anterior aplicado $n$ veces sobre un espacio cuadrático donde el espacio vectorial asociado es de dimensión $n$ lleva a escoger una forma cuadrática equivalente que sea una suma ortogonal de espacios cuadráticos (o formas) $\langle u_i\rangle$. Nótese que, si durante el proceso se obtiene algún espacio cuadrático $(V',\phi')$ para el que $D_K(Q_{\phi'})$ sea vacío, entonces $\phi' = 0$ y basta con completar la suma ortogonal con $\langle 0\rangle$.

COROLARIO F.5. *Sea $K$ un cuerpo con característica distinta de 2 y sea $(V,\phi)$ un espacio cuadrático donde $V$ es un $K$-espacio vectorial de dimensión $n$. Entonces, existen $u_1,\ldots,u_n \in K$ tales que $(V,\phi)$ sea un espacio isométrico a $\langle u_1\rangle \perp \ldots \perp \langle u_n\rangle$.*

NOTACIÓN F.6. En las condiciones del corolario precedente, se introduce la notación:

$$\langle u_1,\ldots,u_n\rangle = \langle u_1\rangle \perp \ldots \perp \langle u_n\rangle.$$

También se utilizará la notación $n\langle x\rangle = \langle x\rangle + \ldots + \langle x\rangle$ para cualquier $x \in K$ y cualquier $n \geq 1$.

En vista de este resultado, si se tiene una forma cuadrática $Q \in K[X_1,\ldots,X_n]$ y definimos el espacio cuadrático $(K^n,\phi_Q)$ respecto de la base canónica, entonces existirá un espacio cuadrático dado por la suma ortogonal $\langle u_1,\ldots,u_n\rangle$ que sea isométrico a $(K^n,\phi_Q)$. Como los espacios isométricos comparten la misma clase de formas cuadráticas equivalentes, entonces la forma $u_1X_1^2 + \ldots + u_nX_n^2$ será equivalente a $Q$ y su matriz asociada será la matriz diagonal $diag(u_1,\ldots,u_n)$. En el Apartado 3 del Capítulo 10 de [**Gantmacher, 1959**] puede verse el Método de Jacobi para encontrar una forma cuadrática equivalente diagonal $\langle u_1,\ldots,u_n\rangle$.

**Clasificación de Formas Cuadráticas.**

En esta subsección lidiaremos con el problema de clasificar a las formas cuadráticas definidas sobre $R[X_1,\ldots,X_n]$ donde $R$ es un cuerpo realmente cerrado. Se trata de encontrar algún representante distinguido para cada clase de formas cuadráticas equivalentes. El caso que trataremos queda resuelto por el conocido Teorema de Inercia de Sylvester, que mostraremos sin demostración. Adicionalmente, se comentará el caso de las formas cuadráticas definidas sobre $K[X_1,\ldots,X_n]$ donde $K$ es un cuerpo algebraicamente cerrado.

Sea $K$ un cuerpo con característica distinta de 2. De algún modo, estamos trabajando con la relación de congruencia de matrices. Recordemos la relación de semejanza de matrices. Un par de matrices $M_1, M_2 \in \mathcal{M}_{n\times n}(K)$ se dicen semejantes si existe una matriz regular $P \in \mathcal{M}_{n\times n}(K)$ tal que $M_1 = P^{-1}M_2P$. Se tiene que todo par de matrices semejantes tienen el mismo determinante, de hecho tienen los mismos valores propios. Esto será diferente para el caso de matrices congruentes, pues si $M_1, M_2 \in \mathcal{M}_{n\times n}(K)$ son congruentes y si $P \in \mathcal{M}_{n\times n}(K)$ es una matriz regular tal que $M_1 = P^TM_2P$, entonces sus determinantes satisfacen la igualdad $det(M_1) = det(M_2)(det(P))^2$ y no será, en general, una cantidad invariante dentro de las matrices asociadas a las formas cuadráticas equivalentes de una clase. En algunos contextos puede distinguirse clases de determinantes módulo $K^2$, pero para el caso en que $K$ sea cuerpo realmente cerrado se tiene que todo elemento positivo es un cuadrado (o si $K$ es algebraicamente cerrado, directamente todo elemento es un cuadrado), y entonces no se puede diferenciar entre clases de formas equivalentes por la clase de determinantes asociada.

En el apartado previo se vio que toda clase de formas cuadráticas equivalentes tiene algún representante $Q \in [X_1,\ldots,X_n]$, no necesariamente único, de la forma:

$$Q(X_1,\ldots,X_n) = a_1X_1^2 + \cdots + a_nX_n^2 = \langle a_1,\ldots,a_n\rangle,$$

para algunos $a_1, \ldots, a_n \in K$. Lo que si se cumple es que la misma cantidad de coeficientes $a_i$ serán nulos para todas las formas cuadráticas de una misma clase de formas equivalentes.

PROPOSICIÓN F.7. *Sea $K$ un cuerpo con característica distinta de 2. Si se tiene una forma cuadrática $Q_1 = \langle a_1, \ldots, a_n \rangle$ definida sobre el cuerpo $K$ que es equivalente a otra forma cuadrática $Q_2 = \langle b_1, \ldots, b_n \rangle$ definida sobre el mismo cuerpo, entonces se tiene la misma cantidad de coeficientes $a_i$ nulos que de coeficientes $b_i$ nulos, y dicha cantidad se corresponde con el rango de sus matrices $M_{Q_1}, M_{Q_2}$ asociadas.*

Entonces el rango de la matriz asociada a una forma cuadrática será invariante por la clase de equivalencia de la forma cuadrática en cuestión. Esto motiva la siguiente definición.

DEFINICIÓN 77. **(Rango de una Forma Cuadrática)**
*Sea $K$ un cuerpo con característica distinta de 2 y sea $Q \in K[X_1, \ldots, X_n]$ una forma cuadrática con matriz simétrica asociada $M_Q$. Se dice rango de $Q$ a $rank(M_Q)$ y se denota por $rank(Q)$.*

Las formas cuadráticas regulares $Q \in K[X_1, \ldots, X_n]$ cumplen que $rank(Q) = n$, mientras que si $rank(Q) < n$, la forma $Q$ será singular. Precisamente, el rango de una forma cuadrática $Q \in K[X_1, \ldots, X_n]$ es suficiente para caracterizar a las clases de formas equivalentes para el caso en que $K$ sea un cuerpo algebraicamente cerrado. Si tomamos un par de formas cuadráticas equivalentes $Q_1(X_1, \ldots, X_n) = a_1X_1^2 + \cdots + a_rX_r^2$ y $Q_2(X_1, \ldots, X_n) = b_1X_1^2 + \cdots + b_sX_s^2$ donde los $a_1, \ldots, a_r, b_1, \ldots, b_s$ sean todos no nulos y queremos dar una matriz regular $P$ tal que $M_{Q_1} = P^T M_{Q_2} P$, entonces se necesita tomar una matriz $P$ diagonal como la siguiente:

$$P = diag\left(\frac{\sqrt{a_1}}{\sqrt{b_1}}, \ldots, \frac{\sqrt{a_r}}{\sqrt{b_r}}, 1, \ldots, 1\right),$$

que está bien definida y es regular solo para el caso $r = s$. Nótese que las cantidades $\sqrt{a_i}, \sqrt{b_i}$ están bien definidas por ser $K$ un cuerpo algebraicamente cerrado. El caso de un cuerpo realmente cerrado será distinto porque solo se tiene las raíces de los elementos positivos. Dejamos por escrito el resultado sobre la clasificación de formas cuadráticas definidas sobre un cuerpo algebraicamente cerrado.

PROPOSICIÓN F.8. *Sea $K$ un cuerpo algebraicamente cerrado y con característica distinta de 2. Sea $Q \in K[X_1, \ldots, X_n]$ una forma cuadrática de rango $d$. Entonces, existirá otra forma cuadrática $\tilde{Q} \in K[X_1, \ldots, X_n]$ equivalente a $Q$ y tal que:*

$$\tilde{Q}(X_1, \ldots, X_n) = X_1^2 + \ldots + X_d^2.$$

OBSERVACIÓN F.9. Nótese que las matrices de permutación son regulares y por ello es que una forma cuadrática $Q = \langle a_1, \ldots, a_n \rangle$ definida sobre un cuerpo $K$ con característica distinta de 2 es equivalente a la forma $Q_\tau = \langle a_{\tau(1)}, \ldots, a_{\tau(n)} \rangle$ definida a partir de una permutación $\tau \in \Sigma_n$.

Pasamos al caso de un cuerpo realmente cerrado $R$, que será algo más complicado. Se dirá que una forma cuadrática es real cuando esta esté definida sobre algún anillo de polinomios con coeficientes en un cuerpo real. Como en este caso ya no se tiene a las raíces de los elementos negativos, el par de formas cuadráticas reales $Q_1(X_1, \ldots, X_n) = X_1^2$ y $Q_2(X_1, \ldots, X_n) = -X_1^2$ no son equivalentes. El problema de la identificación de las clases de formas cuadráticas reales equivalentes se resuelve con el Teorema de Inercia de Sylvester, que enunciamos sin demostración.

TEOREMA F.10. **(de Inercia de Sylvester)**
*Sea $R$ un cuerpo realmente cerrado y sea $Q \in R[X_1, \ldots, X_n]$ una forma cuadrática real. Sea $Y_1, \ldots, Y_n$ una familia de variables algebraicamente independientes sobre $R$ y sea $T$ un cambio lineal de coordenadas tal que $(Y_1, \ldots, Y_n) = T(X_1, \ldots, X_n)$ y:*

$$Q(T(X_1, \ldots, X_n)) = Q(Y_1, \ldots, Y_n) = a_1Y_1^2 + \ldots + a_rY_r^2,$$

*donde $r = rank(Q)$. Se define los índices de inercia $\nu^+$ y $\nu^-$ como la cantidad de coeficientes positivos y de coeficientes negativos, respectivamente, de entre los $a_1, \ldots, a_r$ no nulos. Entonces, $\nu^+$ y $\nu^-$ son iguales para cualquier transformación lineal $T$ con la propiedad de mantener algebraicamente independientes sobre $R$ a las variables.*

Observación F.11. En vista del resultado anterior, puede hablarse de los índices de inercia $\nu^+$ y $\nu^-$ asociados a una forma cuadrática real. Más aún, dado que se preservan por transformaciones lineales, puede hablarse de los índices de inercia de una clase de formas cuadráticas equivalentes.

Del Teorema de Inercia de Sylvester se sigue que el rango asociado a una clase de formas cuadráticas reales equivalentes y los índices de inercia $\nu^+$ y $\nu^-$ asociados a dicha clase permiten identificar completamente a las clases de equivalencia. Sin embargo, tan solo es necesario uno de los índices $\nu^+, \nu^-$ y puede usarse en su lugar la siguiente noción.

Definición 78. **(Signatura de una Forma Cuadrática Real)**
*Sea $R$ un cuerpo realmente cerrado y sea $Q \in R[X_1, \ldots, X_n]$ una forma cuadrática real. Se dice signatura de $Q$ y se denota por $sign(Q)$ a la suma de sus índices de inercia $\nu^+ + \nu^-$.*

Observación F.12. Para calcular la signatura o los índices de inercia de una forma cuadrática real, basta con conocer los signos de los valores propios de la matriz simétrica asociada, que por ser simétrica pertenecerán todos al cuerpo realmente cerrado en cuestión. Esta afirmación se basa en que la matriz diagonal $M = diag(\lambda_1, \ldots, \lambda_n)$ donde $\lambda_1 \geq \ldots \geq \lambda_n$ es congruente con otra matriz $M' = diag(1, \ldots, 1, 0, \ldots, 0, -1, \ldots, -1)$ por la matriz regular siguiente:

$$P = diag\left(\frac{1}{\sqrt{\lambda_1}}, \ldots, \frac{1}{\sqrt{\lambda_r}}, 1, \ldots, 1, \frac{1}{\sqrt{-\lambda_s}}, \ldots, \frac{1}{\sqrt{-\lambda_n}}\right),$$

donde se asume que $\lambda_{r+1}, \ldots, \lambda_{s-1}$ son los únicos valores propios nulos y la relación de congruencia se tiene por $M' = P^T M P$. Obsérvese que al no tener las raíces de elementos negativos, no puede transformarse ningún valor positivo en negativo y viceversa.

Nótese que el rango y la signatura de una forma cuadrática definida sobre un cuerpo realmente cerrado identifica a la clase de formas equivalentes que le corresponde. También se tiene las siguientes relaciones del rango y la signatura con los índices de inercia:

$$\nu^+ = \frac{rank(Q) + sign(Q)}{2}, \qquad \nu^- = \frac{rank(Q) - sign(Q)}{2}.$$

Corolario F.13. *Sea $R$ un cuerpo realmente cerrado y sean $Q_1, Q_2 \in R[X_1, \ldots, X_n]$ un par de formas cuadráticas reales. Entonces, las formas cuadráticas $Q_1$ y $Q_2$ serán equivalentes si y solamente si $rank(Q_1) = rank(Q_2)$ y $sign(Q_1) = sign(Q_2)$.*

Con las clases de las formas cuadráticas reales equivalentes ya caracterizadas, pasemos a ver una clasificación de estas formas. Se tiene la siguiente definición.

Definición 79. **(Forma Cuadrática Real Definida Positiva y Definida Negativa)**
*Sea $R$ un cuerpo realmente cerrado y sea $Q \in R[X_1, \ldots, X_n]$ una forma cuadrática real. La forma $Q$ se dice definida positiva cuando $Q(x) > 0$ para cada $x \in R^n$ no nulo, y semidefinida positiva si para cualquier $x \in R^n$ se tiene que $Q(x) \geq 0$. En cambio, $Q$ se dice definida negativa si $Q(x) < 0$ para cada $x \in R^n$ distinto de $0$ y se dice semidefinida negativa si $Q(x) \leq 0$ para todo $x \in R^n$.*

Todas estos tipos de formas cuadráticas reales se preservan dentro una misma clase de formas equivalentes, y precisamente se tiene el siguiente resultado que las caracteriza por medio de la signatura y del rango.

Proposición F.14. *Sea $R$ un cuerpo realmente cerrado. Sea $Q \in R[X_1, \ldots, X_n]$ una forma cuadrática real. Entonces, se tiene que:*

- *(i) $Q$ es definida positiva si y solamente si $rank(Q) = sign(Q) = n$,*
- *(ii) $Q$ es semidefinida positiva si y solamente si $rank(Q) = sign(Q)$,*
- *(iii) $Q$ es definida negativa si y solamente si $rank(Q) = -sign(Q) = n$,*
- *(iv) $Q$ es semidefinida negativa si y solamente si $rank(Q) = -sign(Q)$.*

Esta clasificación de las formas cuadráticas reales puede hacerse también por medio de los menores principales de la matriz asociada a dicha forma. Tomemos una forma cuadrática real $Q \in R[X_1, \ldots, X_n]$ con matriz simétrica asociada $M_Q$. Se denotarán por $\Delta_1, \ldots, \Delta_n$ los menores principales de la matriz $M_Q = (a_{i,j})_{i,j=1,\ldots,n}$, que son los determinantes de las submatrices $A_k = (a_{i,j})_{i,j=1,\ldots,k}$. Con esta notación puede darse el siguiente resultado.

PROPOSICIÓN F.15. *Sea $R$ un cuerpo realmente cerrado. Sea $Q \in R[X_1, \ldots, X_n]$ una forma cuadrática real con matriz simétrica asociada $M_Q$ cuyos menores principales sean $\Delta_1, \ldots, \Delta_n$. Entonces, se cumple que:*

- *(i) $Q$ es definida positiva si y solamente si $\Delta_1 > 0, \ldots, \Delta_n > 0$,*
- *(ii) $Q$ es semidefinida positiva si y solamente si $\Delta_1 \geq 0, \ldots, \Delta_n \geq 0$,*
- *(iii) $Q$ es definida negativa si y solamente si $(-1)^i \Delta_i > 0$ para cada $i = 1, \ldots, n$,*
- *(iv) $Q$ es semidefinida negativa si y solamente si $(-1)^i \Delta_i \geq 0$ para todo $i = 1, \ldots, n$.*

**Descomposición de Formas Cuadráticas.**

En este apartado veremos una descomposición de los espacios cuadráticos en componentes que sean sencillas, en algún sentido. Para ello, el primer paso es definir la propiedad de isotropía de un espacio cuadrático.

DEFINICIÓN 80. **Espacio Cuadrático Isótropo y Anisótropo)**
*Sea $(V, \phi)$ un espacio cuadrático. Un vector $v \in V$ no nulo se dice isótropo si $\phi(v, v) = 0$. En caso contrario, $v$ se dice anisótropo. El espacio cuadrático $(V, \phi)$ se dice isótropo cuando existe $v \in V$ isótropo, y se dice anisótropo en caso contrario. El espacio cuadrático $(V, \phi)$ se dice totalmente isótropo cuando todo vector no nulo sea isótropo, y en tal caso se tendrá que $\phi = 0$.*

Esta definición puede llevarse al caso de una forma cuadrática considerando el espacio cuadrático asociado $K^n$ con la base canónica (véase la Definición 31). Existe dos casos extremos de formas cuadráticas isótropas que ejemplifican las causas de que una forma cuadrática sea isótropa. Una de ellas es la forma $\langle 0 \rangle$ (o cualquier suma directa $n\langle 0 \rangle$), la cual es totalmente isótropa y tiene asociada la forma cuadrática nula. La otra forma de la que hablamos es aquella que viene dada por $\langle 1, -1 \rangle$, que es regular y universal. Esta forma cuadrática puede escribirse como $X_1^2 - X_2^2$ y es equivalente a la otra forma $X_1 X_2$, que es claramente universal. Se conoce a la forma cuadrática $\langle 1, -1 \rangle$ como el plano hiperbólico, ya que dicha forma tiene asociada el plano hiperbólico, definido como variedad algebraica. A continuación vemos un resultado que caracteriza al plano hiperbólico como espacio cuadrático salvo isometría.

TEOREMA F.16. *Sea $K$ cuerpo con característica distinta de 2. Sea $(V, \phi)$ un espacio cuadrático con $V$ un $K$-espacio vectorial de dimensión 2. Sea $Q \in K[X_1, X_2]$ alguna forma cuadrática asociada a $\phi$ y sea $M_Q$ la matriz simétrica asociada a $Q$. Entonces, son equivalentes:*

- *(i) $(V, \phi)$ es regular e isótropo,*
- *(ii) $(V, \phi)$ es regular y $det(M_Q)$ pertenece a la clase $(-1)K^{*2}$ siendo $K^*$ el conjunto de unidades del cuerpo $K$,*
- *(iii) $(V, \phi)$ es isométrico al espacio $\langle 1, -1 \rangle$.*

Más allá del plano hiperbólico, puede definirse las sumas directas finitas de planos hiperbólicos, que llamaremos espacios cuadráticos hiperbólicos. Estos espacios cuadráticos son también regulares, isótropos y universales; pero no se tendrá en general la Afirmación $(ii)$ del Teorema F.16, sino que más bien la clase de determinantes asociada al espacio hiperbólico $m\langle 1, -1 \rangle$ será $(-1)^m K^{*2}$. Lo interesante aquí es que se tiene un ejemplo de espacio cuadrático isótropo que, al contrario que $\langle 0, \ldots, 0 \rangle$ es regular y universal. Veamos primero que los espacios cuadráticos regulares que son isótropos pueden caracterizarse por la presencia del plano hiperbólico como subespacio vectorial, y luego, que los espacios cuadráticos regulares e isótropos son siempre universales.

TEOREMA F.17. *Sea $(V, \phi)$ un espacio cuadrático. Dicho espacio es regular e isótropo si y solamente si contiene algún plano hiperbólico, en el sentido de que existe otro espacio cuadrático $(V', \phi')$ tal que $V = V' \perp \langle 1, -1 \rangle$.*

PROPOSICIÓN F.18. *Sea $(V, \phi)$ un espacio cuadrático. Si dicho espacio es regular e isótropo, entonces es universal.*

Retomando el tema principal de este apartado, se quiere dar una descomposición de los espacios cuadráticos como suma directa de espacios cuadráticos en algún sentido elementales. Recordemos que una forma cuadrática o un espacio cuadrático definido sobre un cuerpo $K$ puede expresarse como una suma directa $\langle a_1 \rangle \perp \ldots \perp \langle a_n \rangle$ donde $a_1, \ldots, a_r$. Veamos un resultado

que nos dice que cada componente $\langle a_i \rangle$ es única salvo equivalencia de formas cuadráticas o isometría de espacios cuadráticos.

TEOREMA F.19. **(de Cancelación de Witt)**
*Sean $K$ y $K'$ un par de cuerpos con característica distinta de 2, y sean $Q \in K[X_1, \ldots, X_n]$ y $Q_1, Q_2 \in K'[X_1, \ldots, X_m]$ formas cuadráticas. Si $Q \perp Q_1$ y $Q \perp Q_2$ son formas equivalentes, entonces $Q_1$ y $Q_2$ serán formas cuadráticas equivalentes.*

Con este resultado en mente y recapitulando todo lo que hemos hecho hasta ahora, puede darse una descomposición atendiendo a cierto criterio. Si una forma $\langle a_1 \rangle \perp \ldots \perp \langle a_n \rangle$ no es regular, entonces puede quitarse las componentes $\langle 0 \rangle$ para quedarnos con una forma regular. Si tenemos una forma regular que además es isótropa, puede utilizarse el Teorema F.17 para quitar un plano hiperbólico. Esto puede hacerse sucesivas veces hasta obtener una forma anisótropa. Este proceso describe la descomposición de Witt de un espacio cuadrático. Lo escribimos.

TEOREMA F.20. **(de la Descomposición de Witt)**
*Dado $(V, \phi)$ un espacio cuadrático cualquiera, existen $(V_t, \phi_t)$ espacio cuadrático totalmente isótropo, $(V_h, \phi_h)$ espacio cuadrático hiperbólico y $(V_a, \phi_a)$ espacio cuadrático anisótropo tales que $(V_t, \phi_t) = (V_t, \phi_t) \perp (V_h, \phi_h) \perp (V_a, \phi_a)$. Además, los espacios cuadráticos $(V_t, \phi_t)$, $(V_h, \phi_h)$ y $(V_a, \phi_a)$ serán únicos salvo relación de isometría de espacios cuadráticos. Esta descomposición se dirá descomposición de Witt del espacio cuadrático $(V, \phi)$.*

Nótese que el Teorema de Cancelación de Witt F.19 permite establecer la unicidad salvo isometría de la descomposición. Esta unicidad lleva a definir la siguiente cantidad que permanece invariante por descomposiciones de Witt diferentes.

DEFINICIÓN 81. **(Índice de Witt)**
*En las condiciones del Teorema F.20, se dice índice de Witt del espacio cuadrático $(V, \phi)$ a la cantidad:*

$$I_{Witt}(V) = \frac{1}{2} dim_K(V_h).$$

El índice de Witt de un espacio cuadrático regular nos dice cuantas sumas directas de planos hiperbólicos contiene dicho espacio en cualquier descomposición de Witt. Si se tiene una forma cuadrática $Q = \langle u_1, \ldots, u_n \rangle \in K[X_1, \ldots, X_n]$ regular, entonces el producto tensorial:

$$\langle u_1, \ldots, u_n \rangle \otimes \langle 1, -1 \rangle = \langle u_1, -u_1 \ldots, u_n, -u_n \rangle,$$

es una forma equivalente al espacio hiperbólico $n\langle 1, -1 \rangle$ con índice de Witt $n$.

**Teoremas de Representación.**

En esta subsección veremos una serie de resultados conocidos como los Teoremas de Representación, que se trata de varias caracterizaciones de las unidades que pueden ser representadas por cierta forma cuadrática. El primero de ellos puede probarse de manera simple con uno de los resultados vistos en la subsección previa. Para los otros dos, se introduce un resultado probado por J. W. Cassels en 1963 para el caso de sumas de cuadrados de $F[X_1]$ y generalizado para todo elemento no nulo de $F[X_1]$ por A. Pfister poco después.

Comencemos viendo el Primer Teorema de Representación. Su prueba se basa en la Proposición F.18 y por ello es que puede enunciarse directamente.

COROLARIO F.21. **(Primer Teorema de Representación)**
*Sea $K$ un cuerpo con característica distinta de 2. Sea $Q$ una forma cuadrática de $K[X_1, \ldots, X_n]$ y sea $u \in K$ una unidad. Entonces, $u \in D_K(Q)$ si y solamente si $Q \perp \langle -u \rangle$ es isótropo.*

Pasemos a ver el Teorema de Cassels-Pfister, pero antes de eso, veamos este resultado previo.

LEMA F.22. *Sean $K$ un cuerpo con característica distinta de 2 y $Q$ una forma cuadrática de $K[X_1, \ldots, X_n]$. Si $Q$ es anisótropa sobre $K$, es decir si $D_K(Q) = \emptyset$, entonces $Q$ es también anisótropa sobre $K(Y_1)$ ($D_{K(Y_1)}(Q) = \emptyset$).*

Este resultado junto con el Primer Teorema de Representación F.21 permiten concluir el resultado siguiente.

COROLARIO F.23. *Sea $K$ un cuerpo con característica distinta de 2 y sea $Q \in K[X_1, \ldots, X_n]$ una forma cuadrática. Entonces, se cumple que:*

(*i*) $D_{K(Y_1)}(Q) \cap K^* = D_K(Q)$ *donde $K^*$ denota al conjunto de unidades de $K$,*
(*ii*) $-1$ *es suma de $n$ cuadrados de $K$ si y solamente si $-1$ es suma de $n$ cuadrados de $K(Y_1)$.*

La Afirmación (*ii*) del resultado precedente se sigue de tomar la forma $Q = \langle 1, \ldots, 1\rangle$ en la Afirmación (*i*) del mismo corolario, y pone de manifiesto la forma en que puede utilizarse la idea de representación de unidades para conseguir resultados sobre el número de sumas de cuadrados, que se plantea de cara a la Versión Cuantitativa del Problema XVII de Hilbert que se discute en la Sección 3.5. A continuación dejamos enunciado sin demostración el citado resultado de Cassels y Pfister.

TEOREMA F.24. **(de Cassels-Pfister)**
*Sea $K$ un cuerpo con característica distinta de 2 y sea $Q \in K[X_1, \ldots, X_n]$ una forma cuadrática. Tómese un polinomio no nulo $f \in K[Y_1]$ que sea representado por $Q$ en $K(Y_1)$, es decir tal que $f \in D_{K(Y_1)}(Q) \cap K[Y_1]$, y entonces se cumple las siguientes propiedades:*

(*i*) *El polinomio $f$ viene representado por $Q$ sobre $F[Y_1]$, es decir $f \in D_{K[Y_1]}(Q)$.*
(*ii*) *Para todo $a \in K$ que no sea una raíz de $f(Y_1)$, ocurre que $f(a) \in D_K(Q)$.*

Con esto, ya puede darse el Segundo Teorema de Representación.

TEOREMA F.25. **(Segundo Teorema de Representación)**
*Sea $K$ un cuerpo con característica distinta de 2 y sean $a_1, \ldots, a_n \in K$, con $n > 1$, tales que la forma cuadrática $Q = \langle a_1, \ldots, a_n\rangle$ sea anisótropa. También se define otra forma cuadrática $Q' = \langle a_2, \ldots, a_n\rangle$ y una unidad $u \in K$. Entonces:*

$$u \in D_K(Q') \Leftrightarrow u + a_1 Y_1^2 \in D_{K(Y_1)}(Q).$$

OBSERVACIÓN F.26. Nótese que en el resultado precedente es necesario suponer que la forma $Q$ sea anisótropa, ya que si fuese isótropa no hay garantía de $Q'$ también lo sea, luego puede darse que $D_{K(Y_1)}(Q) = K(Y_1) \setminus \{0\}$ pero que $D_K(Q') \neq K^*$ y no se cumpliría el resultado.

La motivación de este Segundo Teorema de Representación viene dada, en parte, por la Versión Cuantitativa del Problema XVII de Hilbert, ya que puede deducirse las siguientes consecuencias.

COROLARIO F.27. *Sea $F$ un cuerpo con característica distinta de 2 y tal que $-1$ no sea una suma de $n-1$ cuadrados de $F$. Se cumple las siguientes propiedades:*

(*i*) *Sea la unidad $u \in K^*$. Si $u + X_1^2$ es una suma de $n$ cuadrados en $F(X_1)$, entonces $u$ será una suma de $n-1$ cuadrados en $F$.*
(*ii*) $1 + X_1^2 + \ldots + X_n^2$ *no puede escribirse como suma de $n$ cuadrados de $F(X_1, \ldots, X_n)$.*

Nos queda por ver el Tercer Teorema de Representación. Este trabaja con la siguiente definición.

DEFINICIÓN 82. **(Dominación entre Formas Cuadráticas)**
*Sea $K$ un cuerpo con característica distinta de 2. Sean $Q_1 \in K[X_1, \ldots, X_n]$ y $Q_2 \in K[Y_1, \ldots, Y_m]$ un par de formas cuadráticas. Se dice que $Q_1$ domina a $Q_2$, y se denota por $Q_1 \succ Q_2$, cuando $Q_2$ está representado por $Q_1$ sobre $K(Y_1, \ldots, Y_m)$, es decir, cuando $Q_2 \in D_{K(Y_1,\ldots,Y_m)}(Q_1)$.*

Notemos que si $Q_1$ de la definición anterior es isótropa sobre $K$, entonces $D_{K(Y_1,\ldots,Y_m)}(Q_1)$ es igual a $K(Y_1, \ldots, Y_m) \setminus \{0\}$, y entonces cualquier forma $Q_2 \in K[Y_1, \ldots, Y_m]$ cumplirá que $Q_1 \succ Q_2$. La idea de dominación es no trivial solo para formas anisótropas, y el resultado siguiente es una caracterización de cuándo una forma anisótropa domina o no a otra.

TEOREMA F.28. **(Tercer Teorema de Representación)**
*Sea $K$ un cuerpo con característica distinta de 2. Sean $Q_1 \in K[X_1, \ldots, X_n]$ y $Q_2 \in K[Y_1, \ldots, Y_m]$ un par de formas cuadráticas. Supongamos que la forma $Q_1$ es anisótropa sobre $K$. Entonces, $Q_1$ domina a $Q_2$ si y solamente si $Q_2$ es equivalente con alguna subforma de $Q_1$.*

OBSERVACIÓN F.29. Con las notaciones del teorema anterior, si $Q_1 \succ Q_2$ entonces $n > m$.

Este resultado puede utilizarse para descomponer en elementos de la forma $\langle a\rangle$ con $a \in K$ el cuerpo con característica distinta de 2 a la parte anisótropa de la descomposición de una forma

cualquiera. Si se tiene la forma $Q \in K[X_1, \ldots, X_n]$ anisótropa y un elemento $a \in K^*$, se tendrá por la Afirmación $(i)$ del Corolario F.23 la siguiente cadena de equivalencias:

$$Q \succ \langle a \rangle \Leftrightarrow aY_1^2 \in D_{K(Y_1)}(Q) \Leftrightarrow a \in D_{K(Y_1)}(Q) \Leftrightarrow a \in D_K(Q),$$

de modo que por el Tercer Teorema de Representación F.28 se sigue que:

$$\langle a \rangle \text{ es una subforma de } Q \Leftrightarrow a \in D_K(Q).$$

En particular, si $Q$ representa a $\langle a \rangle$ sobre $K$ existirá otra forma anisótropa $Q' \in K[X_1, \ldots, X_{n-1}]$ tal que $Q$ sea equivalente a $Q' \perp \langle a \rangle$.

# Glosario de Términos

# Glosario de Teoremas y Resultados

# Bibliografía


[AtMac, 1969] M. F. Atiyah, I. G. Macdonald, *"Introduction to Commutative Algebra"*. Addison-Wesley Publishing Company, 1969.

[BaSh, 2000] R. G. Bartle, D. R. Sherbert, *"Introduction to Real Analysis"*. John Wiley & Sons, 3ra Edición, 2000.

[BCR, 1998] J. Bochnak, M. Coste, M. F. Roy, *"Real Algebraic Geometry"*. Springer-Verlag Berlin Heidelberg New York, 1998.

[CDLR, 1982] M. D. Choi, Z. D. Dai, T. Y. Lam, B. Reznick, *"The Pythagoras number of some affine algebras and local algebras"*. J. Reine Angew Math., 336, pp. 45-82, 1982.

[Gantmacher, 1959] F. M. Gantmacher, *"The Theory of Matrices"*. Traducido del ruso por Chealsea Publishing Company, 1959.

[Gentile, 1992] E. R. Gentile, *"Notas sobre Cuerpos Ordenados"*. Revista de Educación Matemática, Vol. 7, Núm. 3, Noviembre 1992.

[González, 2022] I. González, *"El Teorema de Serre-Auslander-Buchsbaum"*. Facultad de Ciencias de la Universidad de Cantabria, Trabajo de Fin de Grado, Abril 2022.

[Guangxin, 1988] Zeung Guangxin, *"A Characterization of Preordered Fields with the Weak Hilbert Property"*. Proceedings of the American Mathematical Society, Vol. 104 num. 2, October 1988.

[Hilbert, 1900] D. Hilbert, *"Matematische Probleme"*. International Congress of Mathematicians, París 1900. traducción al inglés: http://aleph0.clarku.edu/~djoyce/hilbert/problems.html

[Kunz, 1985] Ernst Kunz, *"Introduction to Commutative Algebra and Algebraic Geometry"*, Modern Birkhaüser Classics, 1985.

[Lam, 1973] T. Y. Lam, *"The Algebraic Theory of Quadratic Forms"*, Mathematics Lecture Note Series, The Benjamin/Cummings Publishing Company, 1973.

[Nagata, 1927] Masayoshi Nagata, *"Local Rings"*, R. E. Krieger Pub. Co., edición de 1975, primera edición 1927.

[Pardo, 1987] Luis M. Pardo, *"Notas de una Conferencia de Max Dickmann, Université Paris VII, Séminaire Estructures Algébriques Ordenés"*. Manuscrito, 1987.

[Pardo, 2023] Luis M. Pardo, *"Algunas notas para un curso elemental de Álgebra Conmutativa, Parte I"*, notas de clase, 2023.

[Recio, 1978] T. J. Recio, *"Una descomposición de un conjunto semialgebraico"*, Actas del V Congreso de la Agrupación de Matemáticos de Expresión Latina (Mallorca, 1977), editado en Madrid: Consejo Superior de Investigaciones Científicas, Instituto "Jorge Juan"de Matemáticas, pp. 217-221, 1978.

[Seidenberg, 1952] A. Seidenberg, *"A New Decision Method for Elementary Algebra"*. Annals of Mathematics, Vol. 60, No. 2, (publicado en) Septiembre 1954.

[Sharp, 1990] R. Y. Sharp, *"Steps in Commutative Algebra"*. London Mathematical Society, Student Texts 19.

[Stewart, 1972] Ian Stewart, *"Galois Theory"*, CRC Press, 4ta Edición, 2014.

[Tabera, 2023] Luis F. Tabera, *"Ampliación de Álgebra"*, notas de clase, 2023.

[Wikipedia] Wikipedia, *"Hilbert's seventeenth problem"*. traducción al inglés: https://en.wikipedia.org/wiki/Hilbert%27s_seventeenth_problem