UNIVERSIDAD NACIONAL DEL CALLAO

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

ESCUELA PROFESIONAL DE MATEMÁTICA

"SOLUCIÓN DEL PROBLEMA DIECISIETE DE HILBERT"

TESIS PARA OBTAR EL TÍTULO PROFESIONAL DE

LICENCIADO EN MATEMÁTICA

PABLO FERNANDO NOEL FIGUEROA

Callao, Marzo, 2019

PERÚ

DEDICATORIA

A mi esposa Graciela Stefany Velásquez Huarcaya por haberme ayudado a alcanzar una de mis más grandes metas esta tesis. Por su invalorable ejemplo de perseverancia y optimismo para seguir adelante y alcanzar nuestros objetivos.

AGRADECIMIENTOS

Expreso mi total agradecimiento para mi asesor de esta tesis el Mg. Mario Enrique Santiago Saldaña por brindarme sus conocimientos que fueron de gran aporte para que el presente trabajo de investigación se volviera realidad.

Índice general

RESUMEN

SOLUCIÓN DEL PROBLEMA DIECISIETE DE HILBERT

PABLO FERNANDO NOEL FIGUEROA

Marzo, 2019

Asesor: Mg. Mario Enrique Santiago Saldaña

Título obtenido: Licenciado en Matemática

En esta tesis se demuestra lo siguiente:

Dados (K, P) un cuerpo ordenado y R una extensión real cerrado de K tal que $R^{(2)} \cap K = P$. Sea $f \in K[X_1, \ldots, X_n]$ tal que $f(x) \geq 0, \forall\, x \in R^n$. Entonces f se puede escribir como $f = \sum_{i=1}^{s} r_i f_i^2$; $r_i \in P$, $f_i \in K(X_1, \ldots, X_n)$.

Esta tesis tiene como objetivo específico estudiar una de las soluciones del problema diecisiete de Hilbert, el cual es:

Sea $f \in \mathbb{R}[X_1, \ldots, X_n]$ tal que $f(x) \geq 0, \forall\, x \in \mathbb{R}^n \Longrightarrow f$ se puede escribir como suma finita de cuadrados de $\mathbb{R}(X_1, \ldots, X_n)$.

Palabras Claves: Extensión, cuerpo ordenado, cuerpo real cerrado.

ABSTRACT

SOLUTION OF THE SEVENTEEN PROBLEM OF HILBERT

PABLO FERNANDO NOEL FIGUEROA

March, 2019

Adviser: Mg. Mario Enrique Santiago Saldaña

Degree Obtained: Licentiate in Mathematics

In this thesis the following is demonstrated:

Given (K, P) an ordered body and R a closed real extension of K such that $R^{(2)} \cap K = P$. Be $f \in K[X_1, \ldots, X_n]$ such that $f(x) \geq 0, \forall\, x \in R^n$. Then f can be written as $f = \sum_{i=1}^{s} r_i f_i^2$; $r_i \in P$, $f_i \in K(X_1, \ldots, X_n)$.

This thesis has as its specific objective to study one of the solutions of the seventeen problem of Hilbert, which is:

Be $f \in \mathbb{R}[X_1, \ldots, X_n]$ such that $f(x) \geq 0, \forall\, x \in \mathbb{R}^n \Longrightarrow f$ can be written as a finite sum of squares of $\mathbb{R}(X_1, \ldots, X_n)$.

Key Words: Extension, ordered field, closed real field.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

La historia del problema diecisiete de Hilbert se inicia con la defensa de la tesis doctoral de Hermann Minkowski en la Universidad de Konigsberg (en Alemania) en 1885, donde David Hilbert era un jurado en dicha defensa. Minkowski expresó: "Existen polinomios reales que no son negativos en todo $\mathbb{R}^n$ y no pueden escribirse como suma finita de cuadrados de polinomios reales". Hilbert en 1888 probó en un artículo ver [7] la existencia de un polinomio real en dos variables de grado seis que no es negativo en $\mathbb{R}^2$ pero no es una suma finita de cuadrados de polinomios reales. La prueba de Hilbert utilizó resultados básicos de la teoría de las curvas algebraicas. Aparte de esto su construcción es completamente elemental. El primer ejemplo *explícito* de este tipo fue dado por T. Motzkin [18] en 1967, es el polinomio:

$$M(X,Y) = X^4Y^2 + X^2Y^4 + 1 - 3X^2Y^2$$

es un polinomio no negativo en $\mathbb{R}^2$ pero no es una suma finita de cuadrados de polinomios reales.

Hilbert en 1893 probó en un artículo ver [6] que todo polinomio $f \in \mathbb{R}[X,Y]$ no negativo en $\mathbb{R}^2$ es una suma finita de cuadrados de $\mathbb{R}(X,Y)$. La prueba muestra incluso que f es una suma de cuatro cuadrados.

Motivado por su trabajo anterior, Hilbert planteó su famoso problema diecisiete en el Congreso Internacional de Matemáticos en París (1900) ver [5]:

El problema diecisiete de Hilbert. Sea $f \in \mathbb{R}(X_1, \ldots, X_n)$ tal que $f(x) \geq 0, \forall\, x \in \mathbb{R}^n$ donde se define $f \Longrightarrow$ ¿ f se puede escribir como suma finita de cuadrados de $\mathbb{R}(X_1, \ldots, X_n)$?.

Este problema es equivalente a:

Sea $f \in \mathbb{R}[X_1, \ldots, X_n]$ tal que $f(x) \geq 0, \forall\, x \in \mathbb{R}^n \Longrightarrow$¿ f se puede escribir como suma finita de cuadrados de $\mathbb{R}(X_1, \ldots, X_n)$?.

Emil Artin solucionó este problema en 1927 ver [8] y reemplazando $\mathbb{R}$ por un cuerpo real cerrado arbitrario.

1.2. Formulación del problema

Se quiere resolver la siguiente interrogante:

Dados (K, P) un cuerpo ordenado y R una extensión real cerrado de K tal que $R^{(2)} \cap K = P$. Sea $f \in K[X_1, \ldots, X_n]$ tal que $f(x) \geq 0, \forall\, x \epsilon R^n$. ¿Será posible que f se pueda escribir como $f = \sum_{i=1}^{s} r_i f_i^2$; $r_i \in P$, $f_i \in K(X_1, \ldots, X_n)$?.

1.3. Objetivos

1.3.1. Objetivo general

Estudiar la teoría de cuerpos ordenados, cuerpos reales y cuerpos reales cerrados.

1.3.2. Objetivo específico

Estudiar una de las soluciones del problema diecisiete de Hilbert.

1.4. Limitantes de la investigación

El problema diecisiete de Hilbert fue solucionado por Emil Artin en 1927 ver [8] y utilizó la teoría Artin-Schreier de cuerpos ordenados, estudiar esta teoría es la base para el estudio de la geometría algebraica real.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes del estudio

El problema diecisiete de Hilbert fue resuelto por Emil Artin en 1927, ver [8] el trabajo de Artin representó un gran avance. Su prueba combinó dos nuevos argumentos. El primer argumento: Una descripción de elementos positivos de un cuerpo en cualquier orden (cono positivo) esto se ha convertido en un tema más amplio conocido como el Álgebra Real ver [1]. El segundo argumento: Son ciertos "lemas de especialización" para cuerpos reales cerrados, que evolucionó con el tiempo en lo que ahora se conoce como el Principio de Transferencia de Tarski, que es un resultado importante en la teoría de modelos de cuerpos reales cerrados, ver [1].

Después de la prueba de Artin, otras demostraciones que hacen uso de la lógica han sido obtenidas, ver [11].

En esta tesis estudiaremos la solución del problema diecisiete de Hilbert utilizando el primer argumento de Artin ver [1] y el teorema del homomorfismo de Lang, ver [15].

2.2. Notaciones

En esta tesis F, K, L y R son cuerpos. También consideramos:

(1) $\mathbb{N} = \{1, 2, 3, \dots\}$ es el conjunto de los números naturales, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, $\mathbb{Z}$ es el anillo de los números enteros; $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ el cuerpo de los números racionales, reales y complejos respectivamente.

(2) $K^{(2)} = \{a^2 / a \in K\}$.

(3) $\sum K^{(2)}$ denota al conjunto que consiste de todas la sumas finitas $\sum a_i^2$, $a_i \in K$.

(4) Sea $W \subseteq K$ no vacío:

$$-W = \{-a \ / \ a \in W\} = \{b \ \in \ K \ / -b \in \ W\} \subseteq K$$

(5) Denotaremos a la *característica de K* por: $car(K)$.

(6) Denotamos a la *clausura algebraica* de K por: $\overline{K}$.

(7) Dado $\alpha = (\alpha_1, \dots, \alpha_n) \in (\mathbb{N}_0)^n$:

$\underline{X}^{\alpha} = X_1^{\alpha_1} \dots X_n^{\alpha_n}$ es un *monomio* en $X_1, \dots, X_n$ variables.

Cuando $\alpha = (0, \dots, 0)$, note que $\underline{X}^{\alpha} = 1$; denotamos y definimos el grado total (o simplemente grado) de $\underline{X}^{\alpha}$ por: $|\alpha| = \sum_{i=1}^{n} \alpha_i$.

(8) Un *polinomio* f en $X_1,\ldots,X_n$ variables, con coeficientes en el cuerpo K es una combinación lineal finita $(\text{con coeficientes en } K)$ de monomios. Escribiremos un polinomio f en la forma:

$$f = \sum_{\alpha} a_\alpha \underline{X}^\alpha \; ; \;\; a_\alpha \in K \;\; , \;\; \alpha \in (\mathbb{N}_0)^n$$

donde la suma esta sobre un número finito de $n-uplas\ \alpha = (\alpha_1,\ldots,\alpha_n\ )$. El conjunto de todos los polinomios en $X_1,\ldots,X_n$ variables, con coeficientes en el cuerpo K, es denotado por $K[X_1,\ldots,X_n]$. Bajo la suma y multiplicación usual para polinomios; $K[X_1,\ldots,X_n]$ es un anillo conmutativo con unidad y es dominio entero; llamado anillo de polinomios.

(9) Denotamos al anillo de polinomios $K[X_1,\ldots,X_n]$ por $K[\underline{X}]$.

Así, $\underline{X}$ es la escritura para la $n-upla$ de variables $(X_1,\ldots,X_n)$.

(10) Si $f \in K[\underline{X}]$, entonces $f = \sum_\alpha a_\alpha \underline{X}^\alpha \; ; \;\; a_\alpha \in K \;\; , \;\; \alpha \in (\mathbb{N}_0)^n$ es una combinación lineal finita de monomios.

Ahora,

Si $f \neq 0$ denotamos y definimos el grado total (o simplemente grado) de f por:

$$gr(f) = máx\{|\alpha| / a_\alpha \neq 0\}$$

el grado del polinomio cero es indefinido.

(11) $K(\underline{X})$ denota el cuerpo de las funciones racionales, es decir, el cuerpo de fracciones del dominio entero $K[\underline{X}]$.

(12) Para $f \in K[\underline{X}]$ y $x = (x_1, \ldots, x_n) \in K^n$, $f(x) \in K$ denota el resultado de evaluar f en x.

2.3. Extensiones de cuerpos

Definición 2.3.1. Se dice que L es una *extensión* de K, lo cual se escribe L/K si existe un homomorfismo inyectivo (monomorfismo) $\varphi: K \to L(K = \varphi(K))$. L/K se representa gráficamente como:

$$\begin{matrix} L \\ | \\ K \end{matrix}$$

Definición 2.3.2. Sean L/K y $S \subseteq L$. Denotamos por $K(S)$ al menor subcuerpo de L que contiene tanto a K como S; es decir:

$$K(S) = \bigcap_{\substack{F \text{ es un} \\ \text{subcuerpo} \\ \text{de } L \\ \text{tal que} \\ K,S \subseteq F}} F$$

Observación 2.3.1.

(1) $K(S)$ es una extensión de K y se dice que se obtiene al adjuntar S a K.

(2) Si S es un conjunto finito no vacío; es decir; $S = \{a_1, \ldots, a_n\}$, denotaremos a $K(S)$ por $K(a_1, \ldots, a_n)$.

(3) Si L/K ($\exists\ \varphi: K \to L$ monomorfismo) entonces L es un espacio vectorial sobre K, donde:

- **Adición:** Es la adición sobre L.
- **Multiplicación por un escalar:**

$$\cdot : K \times L \ \to \ L$$

$$(\alpha, a) \longmapsto \cdot(\alpha, a) = \alpha.a = \alpha a = \varphi(\alpha)a$$

como tal; L tiene una dimensión sobre K, que puede ser infinita. Esta dimensión se llama el grado de L sobre K y se denota por $[L/K]$.

Teorema 2.3.1. Si K es una extensión de F y L es una extensión de K entonces $[L/F] = [L/K][K/F]$.

Demostración. Ver [16], página 1.

Definición 2.3.3. Una extensión L de K es llamada una *extensión finita* de K si $[L/K]$ es finito.

Definición 2.3.4. Una extensión L de K es llamada *extensión simple* de K si $L = K(a)$, para algún $a \in L$.

Definición 2.3.5. Sean L/K y $S \subseteq L$, asumamos que $L = K(S)$. Sea w el número cardinal del conjunto S y $f(X_1, \ldots, X_n)$ un polinomio en n variables; donde $n \leq w$, con coeficientes en K. Si $a_1, \ldots, a_n \in S$ entonces $f(a_1, \ldots, a_n) \in L$. El conjunto de todos esos elementos de L forman un subanillo de L que contiene tanto a K como S, y que denotamos por $K[S]$; es decir:

$$K[S] = \{f(a_1, \ldots, a_n)/f \in K[X_1, \ldots, X_n], n \leq w \; y \; a_1, \ldots, a_n \in S \} \subseteq L$$

Observación 2.3.2.

(1) $K[S]$ es un dominio entero con unidad, que contiene a K y S.

(2) Si S es un conjunto finito no vacío; es decir; $S = \{a_1, \ldots, a_n\}$, denotaremos a $K[S]$ por $K[a_1, \ldots, a_n]$; por lo tanto:

$$K[a_1, \ldots, a_n] = \{f(a_1, \ldots, a_n)/f \in K[X_1, \ldots, X_n]\} \subseteq L$$

Definición 2.3.6. Sea L una extensión de K y $a \in L$. Decimos que a es *algebraico* sobre K si existe un polinomio no constante $f \in K[X]$ tal que $f(a) = 0$. Si a no es algebraico sobre K, decimos que es *trascendental* sobre K. La extensión L de K es llamada una *extensión algebraica* de K si cada elemento de L es algebraico sobre K. Por otro lado, si al menos un elemento de L es trascendental sobre K, entonces L es llamada una *extensión trascendental* de K.

Teorema 2.3.2. Si L es una extensión finita de K entonces L es una extensión algebraica de K.

Demostración. Ver [16], página 3.

Definición 2.3.7. Un cuerpo K es *algebraicamente cerrado* si para todo $f \epsilon\, K[X]$ de grado mayor que uno, existe $\alpha = \alpha(f) \epsilon\, K$ tal que $f(\alpha) = 0$.

Equivalentemente, todo polinomio de grado mayor que uno en $K[X]$ se descompone en factores lineales en $K[X]$; es decir; sea $f \,\epsilon\, K[X]$ de grado mayor que uno, entonces existen $\alpha_1, \ldots, \alpha_{gr(f)} \,\epsilon\, K$ (se llaman raíces de f, contado con multiplicidades; es decir; puede darse el caso de que dos o más raíces sean iguales) y $a \,\epsilon\, K$ tal que:

$$f(X) = a \,.\, \prod_{i=1}^{gr(f)} (X - \alpha_i)$$

Definición 2.3.8. Sea K un cuerpo. Una *clausura algebraica* de K es una extensión L/K tal que:

(a) L/K es algebraica,

(b) L algebraicamente cerrado.

Teorema 2.3.3. Sea K un cuerpo. Entonces, existe y es única (salvo isomorfismo) una clausura algebraica $\overline{K}/K$.

Demostración. Ver [9], página 72.

2.4. Cuerpos ordenados

Decimos que una relación binaria $a \leq b$ (se lee: a menor ó igual que b) ordena linealmente un conjunto no vacío si:

$$a \leq a,$$

$$a \leq b\ , b \leq c \implies a \leq c,$$

$$a \leq b\ , b \leq a \implies a = b,$$

$$a \leq b \ \vee \ b \leq a$$

$\forall\ a, b, c$ en el conjunto.

Definición 2.4.1. Si $\leq$ ordena linealmente K. Decimos que $\leq$ es un *ordenamiento* de K si, adicionamos:

$$a \leq b \Longrightarrow a + c \leq b + c,$$
$$0 \leq a\ , 0 \leq b \Longrightarrow 0 \leq ab$$

$\forall\ a, b, c\ \in\ K$.

Si $\leq$ es un ordenamiento de K, llamamos al par $(K, \leq)$ un cuerpo ordenado, en caso que el ordenamiento $\leq$ es sobreentendido, nos referimos a K como un cuerpo ordenado.

Proposición 2.4.1. $0 \leq 1$.

Demostración. Inmediata de la definición.

Ejemplo 2.4.1. $\mathbb{R}$ es un cuerpo ordenado con respecto a su ordenamiento usual.

Definición 2.4.2. Sea $(K, \leq)$ un cuerpo ordenado, definimos $\forall\, a, b, c \in K$:

(1) $a \geq b$ (se lee: a mayor ó igual que b) $\Leftrightarrow b \leq a$,

(2) $a < b$ (se lee: a menor que b) $\Leftrightarrow a \leq b\ ,\ a \neq b$,

(3) $a > b$ ($se\ lee$: a mayor que b) $\Leftrightarrow b < a$,

(4) $a < b < c \ \Leftrightarrow\ a < b\ ,\ b < c$,

(5) $a \leq b < c \ \Leftrightarrow\ a \leq b\ ,\ b < c$,

(6) $a < b \leq c \ \Leftrightarrow\ a < b\ ,\ b \leq c$,

(7) $a \leq b \leq c \ \Leftrightarrow\ a \leq b\ ,\ b \leq c$.

Definición 2.4.3. Sean $(K, \leq)$ un cuerpo ordenado, $a \in K$. Entonces:

(1) Se dice que a es positivo (negativo) si $0 < a$ $(a < 0)$,

(2) Se dice que a es no negativo (no positivo) si $0 \leq a$ $(a \leq 0)$

Proposición 2.4.2. Sea $(K, \leq)$ un cuerpo ordenado, entonces:

(1)$a < b \Longrightarrow a \leq b\ ;\ \forall\, a, b \in\ K$,

(2) $a \leq b \Leftrightarrow a < b$ ó $a = b$; $\forall\, a, b \in K$,

(3) $a < b$ ó $a = b$ ó $b < a$; $\forall\, a, b \in K$

Demostración: Inmediato de la definición.

Proposición 2.4.3. Sea $(K, \leq)$ un cuerpo ordenado, tenemos las siguientes consecuencias:

(1) $0 \leq a^2$; $\forall\, a \in K$,

(2) $a \leq b$, $0 \leq c \implies ac \leq bc$; $\forall\, a, b, c \in K$,

(3) $0 < a < b \implies 0 < \frac{1}{b} < \frac{1}{a}$; $\forall\, a, b \in K$,

(4) $0 \leq ab \iff 0 \leq \frac{a}{b}$ (si $b \neq 0$) ; $\forall\, a, b \in K$,

(5) $0 < n$; $\forall\, n \in \mathbb{N}$ (así, en particular, $car(K) = 0$).

Demostración.

(1) Sea $a \in K$:

$0 \leq a \ \vee \ a \leq 0$

- $0 \leq a$

  Tenemos: $0 \leq a$, $0 \leq a \implies 0 \leq a^2$

- $a \leq 0$

  $\Longrightarrow 0 \leq -a$

  Tenemos: $0 \leq -a \ , \ 0 \leq -a \ \Rightarrow \ 0 \leq a^2$

  $$\therefore \ 0 \leq a^2 \ ; \ \forall \ a \ \in \ K$$

(2) $a \leq b \ \Longrightarrow \ 0 \leq b - a$

Tenemos: $0 \leq b - a \ , \ 0 \leq c \ \Longrightarrow \ 0 \leq (b - a)c$

$\Longrightarrow 0 \leq bc - ac \ \Longrightarrow ac \leq bc$

(3) $0 < a < b \Longrightarrow 0 < a \ , \ a < b$

$\Longrightarrow 0 < b \ \Rightarrow \ \exists \frac{1}{b} \ \epsilon \ K \backslash \{0\}$

Tenemos: $0 \leq \left(\frac{1}{b}\right)^2$ y $0 \leq b, b \neq 0$

$\Longrightarrow 0 \leq \frac{1}{b}$; como $\frac{1}{b} \neq 0$

$\Longrightarrow 0 < \frac{1}{b}$, análogamente $0 < \frac{1}{a} \ \Rightarrow 0 \leq \frac{1}{ab} \ , \ \frac{1}{ab} \neq 0$

$a < b \ \Leftrightarrow a \leq b \, , a \neq b$

$\Longrightarrow \ a\frac{1}{ab} \leq b\frac{1}{ab}$

$\Longrightarrow \frac{1}{b} \leq \frac{1}{a}$

Como $\frac{1}{b} \neq \frac{1}{a}$

$\Longrightarrow \frac{1}{b} < \frac{1}{a}$

$$\therefore 0 < \frac{1}{b} < \frac{1}{a}$$

(4)

$(\Longrightarrow)$

Tenemos: $0 \leq ab$, $0 \leq \left(\frac{1}{b}\right)^2$

$\Longrightarrow 0 \leq ab\left(\frac{1}{b}\right)^2 = \frac{a}{b}$

$\Longrightarrow 0 \leq \frac{a}{b}$ (si $b \neq 0$)

$(\Longleftarrow)$

Tenemos: $0 \leq \frac{a}{b}$, $0 \leq b^2$

$\Longrightarrow 0 \leq \frac{a}{b}\, b^2 = ab$

$\Longrightarrow 0 \leq ab$

(5) Inmediato, por inducción y definición.

Observación 2.4.1. Sea $(K, \leq)$ un cuerpo ordenado, entonces $\mathbb{Q} \subseteq K$.

Definición 2.4.4. Sea $(K, \leq)$ un cuerpo ordenado. Definimos la aplicación llamada *valor absoluto* denotada por $|\cdot|$, como:

$$\begin{array}{rcl} |\cdot| : K & \longrightarrow & K \\ a & \longmapsto & |a| = \begin{cases} -a \; si \; a < 0, \\ a \; si \; 0 \leq a. \end{cases} \end{array}$$

$|a|$: se lee valor absoluto de a.

Proposición 2.4.4. Sea $(K, \leq)$ un cuerpo ordenado, entonces:

(1) $0 \leq |a| \, , \forall \, a \in K$,

(2) $|ab| = |a||b| \; ; \; \forall \, a, b \in K$,

(3) $|-a| = |a| \; ; \; \forall \, a \in K$,

(4) $a \leq |a| \;\; ; \;\; \forall \, a \in K$,

(5) Sean $r \in K, 0 \leq r, a \in K$:

$$|a| \leq r \Leftrightarrow -r \leq a \leq r$$

(6) Sean $a, r \in K$:

$$|a| \geq r \Leftrightarrow a \geq r \; \vee \; a \leq -r$$

(7) $\left|\sqrt{a^2 + b^2}\right| \geq |a| \;\; ; \;\; \forall \, a, b \in K$

Demostración. Inmediata de la definición.

Definición 2.4.5. Sea $(K, \leq)$ un cuerpo ordenado. Definimos la aplicación llamada *signo* denotada por $sign$, como:

$$\begin{array}{rcl} sign : K & \longrightarrow & \{-1, 0, 1\} \\ a & \longmapsto & sign(a) = \begin{cases} -1 \; si \; a < 0, \\ 0 \; si \; a = 0, \\ 1 \; si \; 0 < a. \end{cases} \end{array}$$

$sign(a)$: se lee el signo de a.

Proposición 2.4.5. $sign(ab) = sign(a)sign(b)\ ;\ \forall\, a, b \in K.$

Demostración. Inmediata de la definición.

Definición 2.4.6. Sea $T \subseteq K$. Entonces decimos que T es un *cono prepositivo* de K, o un preordenamiento de K, si:

$$T + T \subseteq T, T \cdot T \subseteq T, K^{(2)} \subseteq T, \text{y } -1 \notin \text{T}.$$

Si, además,

$$T \cup -T = K,$$

entonces decimos que T es un *cono positivo* de K.

Proposición 2.4.6. Sea $T \subseteq K$. T es un cono prepositivo de $K \Leftrightarrow T + T\,, T \cdot T, K^{(2)} \subseteq T, \text{y } T \cap -T = \{0\}$.

Demostración.

($\Longrightarrow$) Faltaría demostrar que $T \cap -T = \{0\}$:

- $\{0\} \subseteq T \cap -T$, inmediato.
- Supongamos que $T \cap -T \nsubseteq \{0\}$

  $\Longrightarrow \exists\, x \in T \cap -T\ ,\ x \neq 0$

  $\Longrightarrow x \in T\ , -x \in T\ ,\ x \neq 0$

  Ahora:

  $$T \ni \underbrace{x}_{\in T}\ \underbrace{(-x)}_{\in T}\ \underbrace{(x^{-1})^2}_{\in T} = -1$$

$\Longrightarrow -1 \in T\ (\longrightarrow\longleftarrow) - 1 \notin T$

$\Longrightarrow T \cap -T \subseteq \{0\}$

Por lo tanto:

$T \cap -T = \{0\}$

($\Longleftarrow$) Faltaría demostrar que $-1 \notin T$:

Supongamos que $-1 \in T$:

$\Longrightarrow 1 \in T \cap -T = \{0\}$

$\Longrightarrow 1 = 0 (\longrightarrow\longleftarrow) 1 \neq 0$

Por lo tanto:

$-1 \notin T$

Teorema 2.4.1. Si $\sum K^{(2)}$ es un cono positivo de K entonces $\sum K^{(2)}$ es el único cono positivo.

Demostración.

Sea P un cono positivo de K:

Afirmación 2.4.1. $P = \sum K^{(2)}$.

Demostración.

- $\sum K^{(2)} \subseteq P$ inmediato.

- $x \in P \Longrightarrow x \in K = \sum K^{(2)} \cup -\sum K^{(2)}$
  - $x \in \sum K^{(2)} \Longrightarrow P \subseteq \sum K^{(2)}$
  - $x \in -\sum K^{(2)} \Longrightarrow -x \in \sum K^{(2)} \subseteq P \Longrightarrow x \in -P$

    $\Longrightarrow x = 0$

    $\Longrightarrow\ P \subseteq \sum K^{(2)}$

$$\therefore P = \sum K^{(2)}$$

Proposición 2.4.7. Sea $P \subseteq K$. P es un cono positivo de $K \Leftrightarrow P + P\ , P \cdot P \subseteq P, -1\ \notin P,$ y $K \subseteq P \cup -P\ ;\ P \cup -P \subseteq K$ es obvio.

Demostración.

($\Longrightarrow$) Por definición.

($\Longleftarrow$) Faltaría demostrar que $K^{(2)} \subseteq P$:

Sea $x\ \in\ K^{(2)}$:

$\Longrightarrow x = a^2\ ;\ a \in\ K$

$a\ \in\ K \subseteq P \cup -P$

$\Longrightarrow a\ \in\ P\ o\ a\ \in -P$

$\Leftrightarrow a\ \in\ P\ o\ -a\ \in\ P$

- $a\ \in\ P$

  $\Longrightarrow\ x = a^2 = a \cdot a\ \in\ P$

$\Longrightarrow x \in P$

- $-a \in P$

  $\Longrightarrow x = a^2 = (-a) \cdot (-a) \in P$

  $\Longrightarrow x \in P$

Lema 2.4.1. Si $\leq$ es un ordenamiento de K, entonces el conjunto $P_{\leq} = \{a \in K \ / \ 0 \leq a\}$ es un cono positivo de K; si P es un cono positivo de K, entonces la relación $\leq_P$ definida por:

$$a \leq_P b \Leftrightarrow b - a \in P \ ; \ \forall a, b \in P$$

es un ordenamiento de K.

Demostración.

Afirmación 2.4.2. $P_{\leq}$ es un cono positivo de K.

Demostración.

- Sean $a, b \in P_{\leq}$:

  $\Longrightarrow a, b \in K \ / \ 0 \leq a, 0 \leq b$

  $\Longrightarrow b \leq a + b$

  $\Longrightarrow 0 \leq a + b$

  $\Longrightarrow a + b \in P_{\leq}$

y

$0 \leq ab \implies ab \in P_{\leq}$

Por lo tanto:

$P_{\leq} + P_{\leq}, P_{\leq} \cdot P_{\leq} \subseteq P_{\leq}$

- $-1 \in K$, $-1 < 0 \implies -1 \notin P_{\leq}$
- Sea $a \in K$:

  $\implies 0 \leq a \ \vee \ a \leq 0$

  - $0 \leq a \implies a \in P_{\leq}$

    $\vee$

  - $a \leq 0 \implies 0 \leq -a \implies -a \in P_{\leq} \implies a \in -P_{\leq}$

    $\implies a \in P_{\leq} \cup -P_{\leq}$

    Por lo tanto:

    $K \subseteq P_{\leq} \cup -P_{\leq}$

Por Proposición 2.4.7:

$\therefore P_{\leq}$ es un cono positivo de K.

Afirmación 2.4.3. $\leq_P$ es un ordenamiento de K.

Demostración.

Sean $a, b, c \in K$:

- $a - a = 0 \in P \implies a \leq_P a$
- $a \leq_P b \ , \ b \leq_P c$

  $\implies b - a, c - b \in P$

  $\implies \underbrace{(c - b) + (b - a)}_{= c - a} \in P$

  $\implies c - a \in P$

  $\implies a \leq_P c$
- $a \leq_P b \ , \ b \leq_P a$

  $\implies \underbrace{b - a}_{= -(a - b)} \ , \ a - b \in P$

  $\implies a - b \in -P \ , \ a - b \in P$

  $\implies a - b \in P \cap -P = \{0\}$ por Proposición 2.4.6

  $\implies a - b = 0$

  $\iff a = b$
- $b - a \in K = P \cup -P$

  $\implies b - a \in P \ o \ b - a \in -P$

  - $b - a \in P \implies a \leq_P b$

    o
  - $b - a \in -P \implies \underbrace{-(b - a)}_{= a - b} \in P \implies b \leq_P a$

$\Longrightarrow a \leq_P b \quad o \quad b \leq_P a$

- $a \leq_P b \Rightarrow \underbrace{b-a}_{=(b+c)-(a+c)} \in P$

  $\Longrightarrow a+c \leq_P b+c$

- $0 \leq_P a \ , \ 0 \leq_P b \Leftrightarrow a \in P \ , \ b \in P \Longrightarrow ab \in P \Leftrightarrow 0 \leq_P ab$

$\therefore \leq_P$ es un ordenamiento de K.

En vista del Lema 2.4.1:

Con frecuencia identificaremos un ordenamiento $\leq$ con su cono positivo $P_{\leq}$, y un cono positivo P con su ordenamiento asociado $\leq_P$. Si P es un cono positivo de K, llamamos a (K, P) un cuerpo ordenado.

Lema 2.4.2. Si T es un cono prepositivo de K, y sea $x \in K - T$, entonces, $T' = T - xT = \{t_1 - xt_2 \ / t_1, t_2 \epsilon T\}$ es un cono prepositivo de K.

Demostración.

- Sean $a, b \in T'$:

  $\Longrightarrow a = t_1 - xt_1' \quad , \quad b = t_2 - xt_2' \quad ; \quad t_1, t_1', t_2, t_2' \in T$

  $\Longrightarrow a+b = \underbrace{(t_1+t_2)}_{\in T} - x\underbrace{(t_1'+t_2')}_{\in T} \in T'$ y

  $ab = \underbrace{(t_1t_2 + x^2t_1't_2')}_{\in T} - x\underbrace{(t_1't_2 + t_1t_2')}_{\in T} \in T'$

  $\Longrightarrow T'+T', T' \cdot T' \subseteq T'$

- Sea $a \in K$:

$\Longrightarrow a^2 \in T$

$a^2 = a^2 - x0 \in T'$

$\Longrightarrow K^{(2)} \subseteq T'$

- Supongamos que, $-1 \in T'$:

  $\Longrightarrow -1 = t_1 - xt_2 \;\; ; \;\; t_1, t_2 \in T \;\; \ldots(*)$

Afirmación 2.4.4. $t_2 \neq 0$.

Demostración.

Supongamos que, $t_2 = 0$:

$\Longrightarrow -1 = t_1 \in T$

$\Longrightarrow -1 \in T \;\; (\longrightarrow\longleftarrow) -1 \notin T$

Por lo tanto:

$t_2 \neq 0$

En $(*)$:

$$-1 = t_1 - xt_2$$

$$\Longrightarrow x = (1 + t_1)(t_2^{-1})^2 t_2 \in T$$

$$\Longrightarrow x \in T \; (\longrightarrow\longleftarrow) \; x \notin T$$

$$\Longrightarrow -1 \notin T'$$

Por lo tanto:

T' es un cono prepositivo de K.

Teorema 2.4.2. Si T es un cono prepositivo de K y sea $x \in K - T$, entonces, existe un cono positivo P de K con $T \subseteq P, x \notin P$.

Demostración.

Por Lema 2.4.2 tenemos $T' = T - xT$ es un cono prepositivo de K.

Consideremos la familia:

$$\mathfrak{F} = \{S \text{ un cono prepositivo de } K \ / \ S \supseteq T'\}$$

- $T' \in \mathfrak{F}$ así $\mathfrak{F} \neq \emptyset$.
- En $\mathfrak{F}$ consideramos el preorden inclusión " $\subseteq$ " así $(\mathfrak{F}, \subseteq)$ es un conjunto parcialmente ordenado (c.p.o).

Por Lema de Zorn, $(\mathfrak{F}, \subseteq)$ posee un elemento maximal, digamos P.

Como $P \in \mathfrak{F} \Longrightarrow P$ es un cono prepositivo de K tal que $P \supseteq T'$.

$T \subseteq T - xT = T' \subseteq P \Longrightarrow T \subseteq P$.

Afirmación 2.4.5. P es un cono positivo de K.

Demostración.

Tenemos:

- P es un cono prepositivo de K.
- Sea $b \in K \Longrightarrow b \in P$ o $b \notin P$
  - $b \in P$:

    $\Longrightarrow K \subseteq P \cup -P$
  - $b \notin P$:

    Por Lema 2.4.2:

$\Longrightarrow P - bP$ es un cono prepositivo de K tal que:

$$T' \subseteq P \subseteq P - bP \Longrightarrow P - bP \supseteq T'$$

$$\Longrightarrow P - bP \in \mathfrak{F}$$

Ahora: $P \subseteq P - bP$

Pero como P es maximal en $(\mathfrak{F}, \subseteq) \Longrightarrow P = P - bP \Longrightarrow -b \in P \Longrightarrow b \in -P$

$\Longrightarrow K \subseteq P \cup -P$

$\therefore P$ es un cono positivo de K.

Afirmación 2.4.6. $x \notin P$.

Demostración.

$x \notin T \Longrightarrow x \neq 0$

Como $T' \subseteq P \Longrightarrow -x \in P \Longrightarrow x \in -P \Longrightarrow x \notin P$

Por lo tanto:

$\exists\ P$ un cono positivo de K con $T \subseteq P, x \notin P$.

Corolario 2.4.1. K tiene un cono positivo sí, y sólo sí, $-1 \notin \sum K^{(2)}$ $\left(\text{es decir: } \sum K^{(2)} \text{ es un cono prepositivo de } K\right)$.

Demostración. Inmediato por Teorema 2.4.1.

2.5. Cuerpos reales

Teorema 2.5.1. Las siguientes propiedades son equivalentes:

(a) K tiene un ordenamiento,

(b) K tiene un cono positivo,

$(c)\ -1\ \notin\ \sum K^{(2)}$,

(d) Para cada $x_1, \ldots, x_n \in\ K$ tal que

$$\sum_{i=1}^{n} x_i^2 \Longrightarrow x_i = 0, \forall\ i \in \{1, \ldots, n\}$$

Demostración.

$(a) \Leftrightarrow (b)$: Por Lema 2.4.1.

$(b) \Leftrightarrow (c)$: Por Corolario 2.4.1.

$(c) \Longrightarrow (d)$: Demostraremos por contradicción:

Supongamos que: $\exists\ x_1, \ldots, x_n \in\ K$ no todos ceros; es decir $\exists\ i_0 \in\ \{1, \ldots, n\}$ tal que $x_{i_0} \neq 0$, tenemos:

$$\sum_{i=1}^{n} x_i^2 = 0$$

$$\Longrightarrow \left(\frac{1}{x_{i_0}}\right)^2 \left(\sum_{i=1}^{n} x_i^2\right) = 0 \Leftrightarrow 1 + \sum_{\substack{i=1 \\ i \neq i_0}}^{n} \left(\frac{x_i}{x_{i_0}}\right)^2 = 0 \Longrightarrow -1 \in \sum K^{(2)}\ (\longrightarrow\longleftarrow)(c)$$

$\therefore$ Tenemos (d).

$(d) \Longrightarrow (c)$: Demostraremos por contradicción:

Supongamos que: $-1 \in \sum K^{(2)}$.

$$\Longrightarrow -1 = \sum_{i=1}^{n} x_i^2 \Leftrightarrow 1^2 + \sum_{i=1}^{n} x_i^2 = 0 \Longrightarrow 1 = 0\ (\longrightarrow\longleftarrow)\ 1 \neq 0$$

$\therefore$ Tenemos (c).

$(d) \Longrightarrow (a)$: $(d) \Longrightarrow (c) \Longrightarrow (b) \Longrightarrow (a)$.

Definición 2.5.1. Un cuerpo que satisface alguna, y por lo tanto todas las propiedades anteriores se llama *cuerpo real*.

Ejemplo 2.5.1. $\mathbb{R}$ es un cuerpo real, ya que tiene un ordenamiento.

2.6. Resultados importantes

Recordemos que una permutación del conjunto $\{1,\ldots,n\}$ es cualquier biyección:

$$\sigma\colon\{1,\ldots,n\} \longrightarrow \{1,\ldots,n\}$$

Definición 2.6.1. Sea $f \in K[X_1,\ldots,X_n]$ es simétrico si para toda permutación σ de $\{1,\ldots,n\}$, se cumple:

$$f\left(X_{\sigma(1)},\ldots,X_{\sigma(n)}\right) = f(X_1,\ldots,X_n)$$

Para $i = 1,\ldots,n$; la i −ésima función simétrica elemental en las variables $X_1,\ldots,X_n$ es:

$$E_i(X_1,\ldots,X_n) = \sum_{1 \le j_1 < \ldots < j_i \le n} X_{j_1} \ldots X_{j_i}$$

Las funciones simétricas elementales están relacionadas con coeficientes de polinomios de la siguiente manera:

Lema 2.6.1. Sean $x_1,\ldots,x_n$ elementos de K, y $f(X) = (X - x_1)\ldots(X - x_n) = X^n + C_1X^{n-1} + \ldots + C_n$, entonces $C_i = (-1)^i E_i(x_1,\ldots,x_n)$; $\forall\, i \in \{1,\ldots,n\}$.

Demostración. Ver [2], página 46.

Proposición 2.6.1. Sea $f \in K[X]$ de grado n, y $x_1, \ldots, x_n$ son raíces de f (contado con multiplicidades) en un cuerpo algebraicamente cerrado F extensión de K. Si un polinomio $g \in K[X_1, \ldots, X_n]$ es simétrico, entonces $g(x_1, \ldots, x_n) \in K$.

Demostración. Ver [2], página 47.

Teorema 2.6.1 (Teorema de las Bases de Hilbert). Cada ideal $I \subseteq K[X_1, \ldots, X_n]$ tiene un conjunto generador finito. En otras palabras $I = \langle g_1, \ldots, g_t \rangle$ para algunos $g_1, \ldots, g_t \in I$.

Demostración. Ver [4], página 77.

2.7. Cuerpos reales cerrados

Definición 2.7.1. Un *cuerpo real cerrado* es un cuerpo real K que no admite una extensión real algebraica no trivial.

Los cuerpos reales cerrados se caracterizan de la siguiente manera:

Teorema 2.7.1. Las siguientes propiedades son equivalentes:

(a) K es un cuerpo real cerrado,

(b) $K^{(2)}$ es un cono positivo de K, y cualquier $f \in K[X]$ de grado impar tiene una raíz en K, y

(c) $K \neq K(\sqrt{-1})$ y $K(\sqrt{-1})$ es algebraicamente cerrado.

Demostración.

$(a) \Longrightarrow (b)$:

Tenemos:

$K^{(2)} \cdot K^{(2)} \subseteq K^{(2)}, -1 \notin K^{(2)}$.

Afirmación 2.7.1. $K = K^{(2)} \cup -\sum K^{(2)}$.

Demostración.

- $\supseteq$ inmediato.
- $a \in K \Longrightarrow a \in K^{(2)} \ \vee \ a \notin K^{(2)}$
  - $a \in K^{(2)}$

    $\Longrightarrow K \subseteq K^{(2)} \cup -\sum K^{(2)}$
  - $a \notin K^{(2)}$

    $\Longrightarrow K\left(\sqrt{a}\right)$ es una extensión algebraica de K no trivial.

    Como K es real cerrado:

    $\Longrightarrow -1 + 0\sqrt{a} \ \in \sum K\left(\sqrt{a}\right)^{(2)}$

    $\Leftrightarrow \ -1 + 0\sqrt{a} = \sum_{i=1}^{n}\left(x_i + y_i\sqrt{a}\right)^2$

    $\Leftrightarrow \ (-a)\sum_{i=1}^{n} y_i^2 = 1 + \sum_{i=1}^{n} x_i^2 \ \wedge \ \sum_{i=1}^{n} x_i y_i = 0$

    Como K es real:

    $y = \sum_{i=1}^{n} y_i^2 \neq 0$

    $\Longrightarrow -a = (1 + \sum_{i=1}^{n} x_i^2)(\sum_{i=1}^{n} y_i^2)^{-1}$

    $\Leftrightarrow -a = (1 + \sum_{i=1}^{n} x_i^2)(\sum_{i=1}^{n} y_i^2)(y^2)^{-1}$

    $\Leftrightarrow -a = (1 + \sum_{i=1}^{n} x_i^2)\left(\sum_{i=1}^{n}\left(\frac{y_i}{y}\right)^2\right) \in \sum K^{(2)}$

    $\Longrightarrow a \in -\sum K^{(2)}$

    $\Longrightarrow K \subseteq K^{(2)} \cup -\sum K^{(2)}$

$$\therefore K = K^{(2)} \cup -\sum K^{(2)}$$

Afirmación 2.7.2. $K^{(2)} = K^{(2)} + K^{(2)}$ (entonces: $K^{(2)} + K^{(2)} \subseteq K^{(2)}$, por lo tanto $\sum K^{(2)} = K^{(2)}$).

Demostración.

- $\subseteq$ inmediato.
- $x \in K^{(2)} + K^{(2)} \Longrightarrow x = a^2 + b^2 \; ; \; a, b \in K$

  Ahora:

  $x \in K = K^{(2)} \cup -\sum K^{(2)}$

  $\Longrightarrow x \in K^{(2)} \vee x \in -\sum K^{(2)}$

  - $x \in K^{(2)}$

    $\Longrightarrow K^{(2)} + K^{(2)} \subseteq K^{(2)}$

  - $x \in -\sum K^{(2)}$

    $\Longrightarrow -x \in \sum K^{(2)}$

    $\Longrightarrow -x = \sum_{i=1}^{n} x_i^2$

    $\Leftrightarrow \sum_{i=1}^{n} x_i^2 + a^2 + b^2 = 0$

    Como K es real:

    $\Longrightarrow a = 0 = b$

    $\Longrightarrow x = 0$

    $\Longrightarrow x \in K^{(2)}$

$$\Longrightarrow K^{(2)} + K^{(2)} \subseteq K^{(2)}$$

$$\therefore K^{(2)} = K^{(2)} + K^{(2)}$$

Por lo tanto:

$K^{(2)}$ es un cono positivo de K.

Afirmación 2.7.3. Cualquier $f \in K[X]$ de grado impar tiene una raíz en K.

Demostración. Por contradicción:

Supongamos que: $\exists\ \tilde{f} \in K[X]$ de grado impar que no admite una raíz en K.

Sea $r = gr(\tilde{f})$:

Tenemos que:

$\exists\ \tilde{f} \in K[X]$ de grado impar $r > 1$ que no admite una raíz en K.

$\Longrightarrow \exists\ f \in K[X]$ de menor grado impar $d > 1$ que no admite una raíz en K.

Afirmación 2.7.4. f es irreducible en $K[X]$.

Demostración. Por contradicción:

Supongamos que: f es reducible en $K[X]$.

$\Longrightarrow f = f_1 f_2 \ \ ; \quad f_1, f_2 \in K[X] \ \ , \ \ 1 \leq gr(f_1), gr(f_2) < d$

$\Longrightarrow \underbrace{gr(f)}_{\text{impar}} = gr(f_1) + gr(f_2)$

$\Longrightarrow$ o $gr(f_1) = \text{impar}$ o $gr(f_2) = \text{impar}$

$\Longrightarrow f$ admite una raíz en K $(\longrightarrow\longleftarrow)$ f no admite una raíz en K

$$\therefore f \text{ es irreducible en } K[X]$$

Afirmación 2.7.5. $K[X]/\langle f\rangle$ es una extensión no trivial de K.

Demostración.

Definimos:

$$\begin{array}{rccc} \phi: & K & \longrightarrow & K[X]/\langle f\rangle \\ & a & \longmapsto & \phi(a) := a + \langle f\rangle \end{array}$$

es un monomorfismo.

$\therefore$ $K[X]/\langle f\rangle$ es una extensión no trivial de K.

Como $K[X]/\langle f\rangle$ es una extensión K:

$\Longrightarrow$ $K[X]/\langle f\rangle$ es un $K-$ espacio vectorial.

Sabemos que $gr(f) = d > 1$ e impar.

Afirmación 2.7.6. $A = \{1 + \langle f\rangle,\ X + \langle f\rangle,\ \ldots, X^{d-1} + \langle f\rangle\} \subseteq K[X]/\langle f\rangle$ es una $K-$ base de $K[X]/\langle f\rangle$ (así $K[X]/\langle f\rangle$ es una extensión finita de K).

Demostración.

$(a)\ p \in K[X]/\langle f\rangle \Longrightarrow p = r + \langle f\rangle \ \ ; \ \ r = 0 \quad \vee \quad gr(r) < gr(f)$

- $r = 0$

  $\Longrightarrow p = 0(1 + \langle f\rangle) + 0(X + \langle f\rangle) + \ldots + 0(X^{d-1} + \langle f\rangle)$

- $s = gr(r) < gr(f) = d$

  $\Longrightarrow s \leq d - 1$

$$\Longrightarrow p = a_0 + a_1X + \ldots + a_sX^s + \langle f \rangle$$

$$\Leftrightarrow p = a_0 + a_1X + \ldots + a_sX^s + 0X^{s+1} + \ldots + 0X^{d-1} + \langle f \rangle$$

$$\Leftrightarrow\ p = a_0(1 + \langle f \rangle) + a_1(X + \langle f \rangle) + \ldots + 0(X^{d-1} + \langle f \rangle)$$

$$\therefore\ A \text{ genera } {}^{K[X]}\!/_{\langle f \rangle}.$$

(b) Sean $\lambda_0, \ldots, \lambda_{d-1} \in K$ tal que $\lambda_0(1 + \langle f \rangle) + \ldots + \lambda_{d-1}(X^{d-1} + \langle f \rangle) = \langle f \rangle$

$\Longrightarrow \lambda_0 + \ldots + \lambda_{d-1}X^{d-1} = gf \quad , \quad g \in K[X]$

La única posibilidad para tener la igualdad es que $g = 0$

$\Longrightarrow \lambda_0 + \ldots + \lambda_{d-1}X^{d-1} = 0$

$\Leftrightarrow \lambda_0 = \ldots = \lambda_{d-1} = 0$

$\therefore A$ es $K -$ linealmente independiente

Por lo tanto:

$$A \subseteq {}^{K[X]}\!/_{\langle f \rangle} \text{ es una } K - \text{ base de } {}^{K[X]}\!/_{\langle f \rangle}$$

$\Longrightarrow {}^{K[X]}\!/_{\langle f \rangle}$ es una extensión algebraica de K no trivial.

Como K es un cuerpo real cerrado:

$$\Longrightarrow -1 + \langle f \rangle \in \sum {}^{K[X]}\!/_{\langle f \rangle}^{(2)}$$

$$\Longrightarrow -1 + \langle f \rangle = \sum h_i^2 + \langle f \rangle \quad , \quad gr(h_i) < d \Longrightarrow gr(h_i) \leq d - 1$$

$$\Leftrightarrow -1 = \sum h_i^2 + gf \quad , \quad g \in K[X]$$

$\Longrightarrow g \neq 0 \quad \wedge \quad gr\left(\sum h_i^2\right) \leq 2d - 2$

Como K es real:

$\Longrightarrow gr\left(\sum h_i^2\right) = \text{par}$

$\Longrightarrow r = gr(g) > 1 \text{ impar}$

Como:

$-1 - \sum h_i^2 = gf$

$\Longrightarrow gr(g) < d$

Tenemos:

$g \in K[X]$ de grado r donde $1 < r < d$ impar

Sabemos que: $f \in K[X]$ tiene menor grado impar $d > 1$ que no admite raíz en K.

$\Longrightarrow g$ admite una raíz en K.

$\Longrightarrow \exists\, x \in K \,/\, g(x) = 0$

Como:

$-1 - \sum h_i^2 = gf$

$\Longrightarrow -1 \in \sum K^{(2)}$ $(\longrightarrow\longleftarrow)$ K es real.

$\therefore$ Cualquier $f \in K[X]$ de grado impar tiene una raíz en K.

$(b) \Longrightarrow (c)$:

Como $K^{(2)}$ es un cono positivo K:

$\Longrightarrow -1 \notin K^{(2)}$

Por lo tanto:

$K \neq K(\sqrt{-1})$

Afirmación 2.7.7. Todo $f \in K[X]$ admite una raíz en $K(\sqrt{-1})$.

Demostración.

Sea $f \in K[X]$ no constante, $d = gr(f) \geq 1$:

$\Longrightarrow d = 2^m n$; donde m es un entero no negativo y n un número impar (positivo).

Lo probaremos por inducción en m:

Si $m = 0$, el grado de f es n impar y por hipótesis admite una raíz en K.

$\Longrightarrow f$ admite una raíz en $K(\sqrt{-1})$.

Sea $m \in \mathbb{N}_0$:

Supongamos que el resultado vale para polinomios de grado $2^m n$, con n impar (Hipótesis Inductiva).

Sea $f \in K[X]$ de grado $d = 2^{m+1} n$, con n impar:

Sean $x_1, \ldots, x_d$ las raíces de f (contado con multiplicidades) en la clausura algebraica $\overline{K}$ de K; sabemos que $\overline{K}/K(\sqrt{-1})$.

Sea $h \in \mathbb{Z}$, definimos:

$$g_h(X_1, \ldots, X_d, X) = \prod_{\lambda<\mu} \left[X - \left(X_\lambda + X_\mu + hX_\lambda X_\mu\right)\right]$$

Consideremos:

$\xi_1 = Y_{(1,2)} = X_1 + X_2 + hX_1X_2$
$\xi_2 = Y_{(1,3)} = X_1 + X_3 + hX_1X_3$ $\xi_3 = Y_{(2,3)} = X_2 + X_3 + hX_2X_3$
. . .
$Y_{(1,d)} = X_1 + X_d + hX_1X_d$ $Y_{(2,d)} = X_2 + X_d + hX_2X_d$ . . . $\xi_s = Y_{(d-1,d)} = X_{d-1} + X_d + hX_{d-1}X_d$

Tabla 2.7.1

donde:

$$s = \frac{(d-1)d}{2} = \frac{(2^{m+1}n-1)2^{m+1}n}{2} = 2^m \underbrace{n(2^{m+1}n-1)}_{=n_1} \ , \ n_1\text{: Impar}$$

$$\Longrightarrow s = 2^m n_1 \ , \ n_1\text{: Impar}$$

$$\Longrightarrow g_h(X_1,\ldots,X_d,X) = (X-\xi_1)(X-\xi_2)\ldots(X-\xi_S)$$

$$\Leftrightarrow g_h(X_1,\ldots,X_d,X) = X^s + C_1X^{s-1} + C_2X^{s-2} + \ldots + C_s$$

Por Lema 2.6.1:

$$\Longrightarrow C_i(X_1,\ldots,X_d) = C_i = (-1)^i E_i(\xi_1,\ldots,\xi_s) = (-1)^i \sum_{1 \le j_1 < \ldots < j_i \le s} \xi_{j_1} \ldots \xi_{j_i};$$

$\forall\, i \in \{1,\ldots,s\}$.

Sea σ una permutación de $\{1,\ldots,d\}$:

$$\Longrightarrow C_i\left(X_{\sigma(1)},\ldots,X_{\sigma(d)}\right) = (-1)^i E_i(\xi_1,\ldots,\xi_s) = C_i(X_1,\ldots,X_d)$$

$\Longrightarrow C_i(X_1,\ldots,X_d) \in K[X_1,\ldots,X_d]$ es simétrica.

Por Proposición 2.6.1:

$$\Longrightarrow C_i(x_1,\ldots,x_d) \in K$$

$g_h(x_1,\ldots,x_d,X) = X^s + C_1X^{s-1} + \ldots + C_s \in K[X]$ de grado $s = 2^m n_1$; n_1: impar

Por Hipótesis Inductiva admite una raíz $x \in K\left(\sqrt{-1}\right)$

$$\Longrightarrow g_h(x_1,\ldots,x_d,x) = x^s + C_1x^{s-1} + \ldots + C_s = 0$$

$$\Leftrightarrow \prod_{\lambda<\mu}\left(x - \left(x_\lambda + x_\mu + hx_\lambda x_\mu\right)\right) = 0$$

$\Leftrightarrow \exists\, \lambda = \lambda(h)\,, \mu = \mu(h) \in \{1,\ldots,d\}$ tal que

$x_\lambda + x_\mu + hx_\lambda x_\mu \in K\left(\sqrt{-1}\right)$

Sea $A = \{1,\ldots,d\}$:

Definimos la aplicación:

$$\begin{array}{rccc} \psi: & \mathbb{Z} & \longrightarrow & A \times A \\ & h & \longmapsto & \psi(h) = (\lambda_h, \mu_h) \end{array} \quad \text{donde}$$

$$\lambda_h = máx\{1,\ldots,d\}\,, \mu_h = máx\{1,\ldots,d\}$$

tal que

$$x_{\lambda_h} + x_{\mu_h} + h x_{\lambda_h} x_{\mu_h} \in K(\sqrt{-1})$$

Como $\mathbb{Z}$ es infinito y $A \times A$ es finito

$\Longrightarrow \psi$ no es inyectiva

$\Longrightarrow \exists_n\, h, h' \epsilon\, \mathbb{Z} / h \neq h',\ \psi(h) = \psi(h') = (\lambda, \mu)$

$$\Longrightarrow \begin{matrix} x_\lambda + x_\mu + h x_\lambda x_\mu \in K(\sqrt{-1}) \\ x_\lambda + x_\mu + h' x_\lambda x_\mu \in K(\sqrt{-1}) \end{matrix}$$

Restando:

$(h - h') x_\lambda x_\mu \in K(\sqrt{-1})$

como $h - h' \neq 0$

$\Longrightarrow x_\lambda x_\mu \in K(\sqrt{-1})$

Así:

$x_\lambda x_\mu\ ,\ x_\lambda + x_\mu \in K(\sqrt{-1})$

Denotamos:

$$x_\lambda x_\mu = r\ \ ,\ \ x_\lambda + x_\mu = s\ ;\ r, s \epsilon\, K(\sqrt{-1})$$

Afirmación 2.7.8. Todo elemento de $K(\sqrt{-1})$ es un cuadrado.

Demostración.

Sea $z \epsilon\, K(\sqrt{-1})$:

$\Longrightarrow z = a + b\sqrt{-1}\ ;\ a, b \in K$

$\Longrightarrow \exists \sqrt{a^2 + b^2} \in K$

Sabemos que: $\left|\sqrt{a^2 + b^2}\right| \geq |a|$

$$\Leftrightarrow -\left|\sqrt{a^2+b^2}\right| \leq a \ , \ a \leq \left|\sqrt{a^2+b^2}\right|$$

$$\Leftrightarrow 0 \leq \frac{a+\left|\sqrt{a^2+b^2}\right|}{2} \quad , \quad 0 \leq \frac{-a+\left|\sqrt{a^2+b^2}\right|}{2}$$

Denotamos:

$$c_1 = \sqrt{\frac{a+\left|\sqrt{a^2+b^2}\right|}{2}} \in K \qquad , \qquad c_2 = \sqrt{\frac{-a+\left|\sqrt{a^2+b^2}\right|}{2}} \in K$$

Ahora: $b \neq 0$ ó $b = 0$

- $b \neq 0$

$$\left(\underbrace{|c_1| + |c_2|\big(sign(b)\big)\sqrt{-1}}_{\in K\left(\sqrt{-1}\right)}\right)^2 = z$$

- $b = 0$

$$\left(\underbrace{|c_1| + |c_2|\sqrt{-1}}_{\in K\left(\sqrt{-1}\right)}\right)^2 = z$$

$\therefore$ Todo elemento de $K\left(\sqrt{-1}\right)$ es un cuadrado.

Afirmación 2.7.9. Todo polinomio en $K\left(\sqrt{-1}\right)[X]$ de grado dos, tiene sus raíces en $K\left(\sqrt{-1}\right)$.

Demostración.

Sea $p \in K\left(\sqrt{-1}\right)[X]$ de grado dos:

$$\Longrightarrow p(X) = aX^2 + bX + c \ \ ; \ \ a, b, c \in K\left(\sqrt{-1}\right) \ , \ a \neq 0$$

Para encontrar sus raíces, resolvemos la ecuación:

$p(X) = 0$

$\Leftrightarrow aX^2 + bX + c = 0$

$\Leftrightarrow X_{1,2} = \dfrac{-b \pm q}{2a} \in K(\sqrt{-1})\ ;\ q^2 = b^2 - 4ac\ ,\ q \in K(\sqrt{-1})$

$\therefore$ Todo polinomio en $K(\sqrt{-1})[X]$ de grado dos, tiene sus raíces en $K(\sqrt{-1})$.

El polinomio cuadrático cuyas raíces son $x_\lambda\ ,\ x_\mu$ se construye de la siguiente manera:

$$p(X) = X^2 - sX + r \in K(\sqrt{-1})[X]$$

entonces por Afirmación 2.7.9 sus raíces $x_\lambda\ ,\ x_\mu \in K(\sqrt{-1})$.

$\Longrightarrow f$ admite una raíz en $K(\sqrt{-1})$.

$\therefore$ Todo $f \in K[X]$ admite una raíz en $K(\sqrt{-1})$.

Sean $f \in K(\sqrt{-1})[X]$, $\overline{f}$ es el polinomio obtenido por remplazar los coeficientes de f por sus conjugadas:

$\Longrightarrow f\overline{f} \in K[X]$

Por la Afirmación 2.7.7 $f\overline{f}$ admite una raíz x en $K(\sqrt{-1})$

$\Longrightarrow f\overline{f}(x) = 0 \Leftrightarrow f(x) = 0 \ \vee\ \overline{f}(x) = 0 \Leftrightarrow f(x) = 0 \ \vee\ f(\overline{x}) = 0$

$\Longrightarrow f$ admite una raíz en $K(\sqrt{-1})$

$\therefore\ K(\sqrt{-1})$ es algebraicamente cerrado.

$(c) \Longrightarrow (a)$:

Afirmación 2.7.10. $K^{(2)} + K^{(2)} = K^{(2)}$

Demostración.

Sean $a, b \in K$:

Por hipótesis tenemos:

$a + b\sqrt{-1} = \left(x + y\sqrt{-1}\right)^2 \ ; \ x, y \in K$

$\Longrightarrow a = x^2 - y^2 \ \ , \ \ b = 2xy \ ;$ ya que $\sqrt{-1} \notin K$

Así que:

$a^2 + b^2 = x^4 - 2x^2y^2 + y^4 + 4x^2y^2 = (x^2 + y^2)^2 \in K^{(2)}$

$$\therefore K^{(2)} + K^{(2)} = K^{(2)}$$

$\Longrightarrow \sum K^{(2)} = K^{(2)}$

Por hipótesis tenemos:

$-1 \notin K^{(2)}$

$\Longrightarrow -1 \notin \sum K^{(2)}$

$\Longrightarrow K$ es real

Afirmación 2.7.11. La única extensión algebraica no trivial de K es $K\left(\sqrt{-1}\right)$.

Demostración.

Sea L una extensión algebraica no trivial de K, entonces:

$$\begin{array}{l} \bar{L} = K\left(\sqrt{-1}\right) \\ | \\ L \\ | \\ K \end{array}$$

Por Teorema 2.3.1 tenemos:

$$\Longrightarrow \underbrace{\left[K\left(\sqrt{-1}\right)/K\right]}_{=2} = [L/K]\left[K\left(\sqrt{-1}\right)/L\right]$$

$$\Longrightarrow [L/K] = 1 \quad \vee \quad \left[K\left(\sqrt{-1}\right)/L\right] = 1$$

$$\Longrightarrow K = L \quad \vee \quad L = K\left(\sqrt{-1}\right)$$

Como L es una extensión no trivial entonces:

$L = K\left(\sqrt{-1}\right)$ no real

$$\therefore K \text{ es real cerrado}$$

Observación 2.7.1. Si K es un cuerpo real cerrado entonces $K^{(2)}$ es un cono positivo de K y es único.

Ejemplo 2.7.1. $\mathbb{R}$ es un cuerpo real cerrado.

2.8. Clausura real de un cuerpo ordenado

Definición 2.8.1 (Extensiones de ordenamientos). Sea L/K. Si $\leq_1, \leq_2$ son ordenamientos de K y L respectivamente. Decimos que $\leq_2$ *extiende* a $\leq_1$ si $\forall\, a \in K/0 \leq_1 a \Leftrightarrow 0 \leq_2 a$; y se escribe $K \hookrightarrow L$. Esto es equivalente a $P_2 \cap K = P_1$, donde P_i es el cono positivo correspondiente a $\leq_i$.

Definición 2.8.2. Una extensión algebraica R de un cuerpo ordenado (F, P) es llamada *una clausura real* de F si R es real cerrado y su único ordenamiento extiende al ordenamiento de F.

Teorema 2.8.1. Cada cuerpo ordenando (F, P) tiene una clausura real.

Demostración.

Consideremos la familia:

$$E = \{(K, Q) \text{ cuerpo ordenado} / F \hookrightarrow K \text{ y } K \text{ subcuerpo de } \overline{F}\}$$

Tenemos:

$F \in E$ así $E \neq \emptyset$

Vemos que todo elemento de E es una extensión algebraica de F.

La familia E es un conjunto parcialmente ordenado $(c.p.o)$ por la relación $(K, Q) \prec (K', Q')$ definida por K subcuerpo de K' y $K \hookrightarrow K'$.

Por el Lema de Zorn, $(E, \prec)$ posee un elemento maximal, digamos (R, P').

Sabemos R es una extensión algebraica de F.

Afirmación 2.8.1. Todo elemento positivo de (R, P') es un cuadrado.

Demostración.

Sea $a \in R$ positivo:

Tenemos:

$a \notin R^{(2)} \ \vee \ a \in R^{(2)}$

Supongamos que: $a \notin R^{(2)}$

$\Longrightarrow R \neq R(\sqrt{a})$

Definimos:

$P'' = \left\{ \sum_{i=1}^{n} b_i (c_i + d_i \sqrt{a})^2 / n \in \mathbb{N} \, ; \, c_i, d_i \in R \text{ y } b_i \in P' \right\} \subseteq R(\sqrt{a})$ subcuerpo de $\overline{F}$.

Afirmación 2.8.2. P'' es un cono prepositivo de $R(\sqrt{a})$.

Demostración.

- $P'' + P'', P'' \cdot P'', R(\sqrt{a})^{(2)} \subseteq P''$

- Supongamos que: $-1+0\sqrt{a} \in P''$

$$\Leftrightarrow -1+0\sqrt{a} = \sum_{i=1}^{n} b_i\left(c_i + d_i\sqrt{a}\right)^2 \Big/ n \in \mathbb{N}\ ;\ c_i, d_i \in R \text{ y } b_i \in P'$$

$$\Longrightarrow -1 = \underbrace{\sum_{i=1}^{n} b_i(c_i^2 + d_i^2 a)}_{\geq 0} \quad \text{en } R$$

$$\Longrightarrow -1 \geq 0 \ (\longrightarrow\longleftarrow)\ -1 < 0$$

$$\Longrightarrow -1+0\sqrt{a} \notin P''$$

$\therefore P''$ es un cono prepositivo de $R\left(\sqrt{a}\right)$.

Por Teorema 2.4.2:

$\exists\ Q$ un cono positivo de $R\left(\sqrt{a}\right)$ con $P'' \subseteq Q$.

$P \subseteq P' \subseteq P'' \subseteq Q \Longrightarrow P \subseteq Q\ ,\ P' \subseteq Q$

$Q \cap F = Q \cap (P \cup -P) = (Q \cap P) \cup (Q \cap -P) = P \cup \{0\} = P$

$\Longrightarrow Q \cap F = P$

$\Longrightarrow Q$ extiende a P

Análogamente:

$Q \cap R = P' \Longrightarrow Q$ extiende a P'

Tenemos:

$\left(R\left(\sqrt{a}\right), Q\right)$ cuerpo ordenado tal que $F \hookrightarrow R\left(\sqrt{a}\right)$ y $R\left(\sqrt{a}\right)$ subcuerpo de $\overline{F}$

$\Longrightarrow \left(R\left(\sqrt{a}\right), Q\right) \in E$

y $(R, P') \prec \left(R\left(\sqrt{a}\right), Q\right)$.

Por la maximalidad de R:

$R = R(\sqrt{a})\ (\longrightarrow\longleftarrow)\ R \neq R(\sqrt{a})$

$\Longrightarrow a \in R^{(2)}$

$\therefore$ Todo elemento positivo de (R, P') es un cuadrado.

Afirmación 2.8.3. R es real cerrado.

Demostración. Por contradicción

Supongamos que: R no es real cerrado

$\Longrightarrow R$ admite una extensión algebraica real no trivial L.

Además:

$$\begin{array}{c} \overline{L} = \overline{F} \\ | \\ L \\ | \\ F \end{array}$$

Sea Q' un cono positivo de L:

$P \subseteq P' \subseteq Q' \Longrightarrow Q' \cap R = P\ ,\ Q' \cap R = P'$

$\Longrightarrow Q'$ extiende a P' y Q' extiende a P

$\Longrightarrow (L, Q')$ cuerpo ordenado$/F \hookrightarrow L$ y L subcuerpo de $\overline{F}$

$\Longrightarrow\ (L, Q') \in E$

Tenemos:

$(R, P') \prec (L, Q')$

Por maximalidad de R:

$R = L\ (\longrightarrow\longleftarrow)\ R \neq L$

$\therefore R$ es real cerrado

Por lo tanto:

R es una clausura real de (F, P).

Proposición 2.8.1. Sea (F, P) un cuerpo ordenado, R una clausura real de (F, P), y R', una extensión real cerrada de F cuyo ordenamiento extiende al de F. Entonces existe un único homomorfismo de $F - álgebras\ \phi: R \longrightarrow R'$.

Demostración. Ver [3], página 16.

Observación 2.8.1. De la proposición anterior notamos que $R \hookrightarrow R'$.

Teorema 2.8.2. Si R y R' son dos clausuras reales del cuerpo ordenado (F, P), entonces existe un único isomorfismo de $F - álgebras\ \phi: R \longrightarrow R'$.

Demostración. Inmediato por la Proposición 2.8.1.

Por abuso del lenguaje hablaremos, de ahora en adelante, de la *clausura real* de un cuerpo ordenado.

2.9. Teorema de Tarski-Seidenberg (Versión Básica)

Teorema 2.9.1 (Teorema de Tarski-Seidenberg (Versión Básica)). Dado un sistema de ecuaciones e inecuaciones polinómicas $S(\underline{T}, \underline{X})$ en $m + n$ variables $T_1, \ldots, T_m, X_1, \ldots, X_n$ con coeficiente en $\mathbb{Q}$, entonces, existe un número finito de sistemas de ecuaciones e inecuaciones polinómicas $S_1(\underline{T}), \ldots, S_l(\underline{T})$ con coeficientes en $\mathbb{Q}$ tal que, para cada cuerpo real cerrado R y cada $t \in R^m$, el sistema $S(t, \underline{X})$ tiene una solución $x \in R^n \Leftrightarrow t$ es solución de algún $S_i(\underline{T})$.

Demostración. Ver [14], página 161.

Ejemplo 2.9.1. Determine los $S_i(\underline{T})$ en el caso $m = 3$, $n = 1$ donde el sistema $S(\underline{T}, X)$ consiste de una sola ecuación $T_1X^2 + T_2X + T_3 = 0$.

Solución.

Sean R un cuerpo real cerrado y $t = (t_1, t_2, t_3) \in R^3$:

$t_1X^2 + t_2X + t_3 = 0$ tiene una solución $x \in R$

$\Leftrightarrow t_1 \neq 0$, $t_2^2 - 4t_1t_3 \geq 0$

Tenemos el sistema:

$$S_i(\underline{T}) = \begin{cases} T_1 \neq 0, \\ T_2^2 - 4T_1T_3 \geq 0. \end{cases}$$

Vemos que cumple el Teorema de Tarski-Seidenberg (Versión Básica).

2.10. Principio de Trasferencia de Tarski

En esta sección aplicaremos el Teorema de Tarski-Seidenberg (Versión Básica), para establecer dos versiones del Principio de Transferencia de Tarski.

Teorema 2.10.1 (Principio de Transferencia de Tarski). Dados un sistema de ecuaciones e inecuaciones polinómicas $S(\underline{T}, \underline{X})$ en $m + n$ variables $T_1, \ldots, T_m, X_1, \ldots, X_n$ con coeficiente en $\mathbb{Q}$, (K, P) un cuerpo ordenado, R_1 y R_2 extensiones reales cerrados de K tal que $K \hookrightarrow R_1$, $K \hookrightarrow R_2$ y $t \in K^m$. Entonces el sistema $S(t, \underline{X})$ tiene una solución $x \in R_1^n \Leftrightarrow$ este tiene una solución $x \in R_2^n$.

Demostración.

Por el Teorema de Tarski-Seidenberg (Versión Básica): $\exists_n\ S_1(\underline{T}),\ldots,S_l(\underline{T})$ con coeficiente en $\mathbb{Q}$.

$S(t,\underline{X})$ tiene una solución $x \in R_1^n$

$t \in K^m \subseteq R_1^m$

$\Leftrightarrow$ t es solución de algún $S_i(\underline{T})$

$t \in K^m \subseteq R_2^m$

$\Leftrightarrow$ $S(t,\underline{X})$ tiene una solución $x \in R_2^n$

Teorema 2.10.2 (Principio de Transferencia de Tarski). Dados (K,P) un cuerpo ordenado, R_1 y R_2 extensiones reales cerrados de K tal que $K \hookrightarrow R_1$, $K \hookrightarrow R_2$. Entonces un sistema de ecuaciones e inecuaciones polinómicas de la forma:

$$S(\underline{X}) = \begin{cases} f_1(\underline{X}) \rhd_1 0 \\ \vdots \\ f_k(\underline{X}) \rhd_k 0 \end{cases}$$

donde $\rhd_i \in \{\geq, >, =, \neq\}$ y cada f_i es un polinomio en n variables con coeficientes en K, tiene solución $x \in R_1^n \Leftrightarrow$ este tiene una solución $x \in R_2^n$.

Demostración.

$$f_i(\underline{X}) = \sum_{\alpha_i} a_{\alpha_i} \underline{X}^{\alpha_i}$$

Sean $t_1,\ldots,t_m$ los coeficientes de los polinomios $f_1,\ldots,f_k$, listados de menor a mayor; sustituyendo los coeficientes $t_1,\ldots,t_m$ por las variables $T_1,\ldots,T_m$ produce un sistema $S'(\underline{T},\underline{X})$.

$t=(t_1,\ldots,t_m)\in K^m$, entonces, $S'(t,\underline{X})=S(\underline{X})$

$S(\underline{X})$ tiene una solución $x\in R_1^n$

$\Leftrightarrow S'(t,\underline{X})$ tiene una solución $x\in R_1^n$

Aplicando el Teorema 2.10.1:

$\Leftrightarrow S'(t,\underline{X})$ tiene una solución $x\in R_2^n$

$\Leftrightarrow S(\underline{X})$ tiene una solución $x\in R_2^n$

2.11. Teorema de Homomorfismo de Lang

Teorema 2.11.1 (Teorema de Homomorfismo de Lang). Dados (K,P) un cuerpo ordenado con clausura real R, D un dominio entero que es una $K-álgebra$ finitamente generada y que el ordenamiento P se extiende a un ordenamiento en el cuerpo de cocientes de D. Entonces:

(a) Existe un homomorfismo de $K-álgebras\ \phi: D\longrightarrow R$,

(b) En términos más generales: Si $a_1,\ldots,a_m\in D$ son positivos en este orden extendido entonces existe un homomorfismo de $K-álgebras\ \phi: D\longrightarrow R$ tal que $\phi(a_i)>0,\ i=1,\ldots,m$.

Demostración.

(a):

Sean F el cuerpo de cocientes de D, Q la extensión de P a F y R_1 es la clausura real del cuerpo ordenado (F, Q).

Puesto que D es un dominio entero que es una $K-álgebra$ finitamente generada, entonces existe $\varphi: K[X_1, \ldots, X_n] \longrightarrow D$ un epimorfismo de $K-álgebras$.

Por lo tanto:

$$\frac{K[X_1,\ldots,X_n]}{p} = D \text{ ; donde } p = Ker(\varphi) \subseteq K[X_1, \ldots, X_n]$$

Por Teorema 2.6.1 (Teorema de las Bases de Hilbert), p es finitamente generado; es decir:

$$p = \langle g_1, \ldots, g_s \rangle \text{ ; } g_i \in p$$

Tenemos:

$$K \subseteq \frac{K[X_1, \ldots, X_n]}{p} = D \subseteq F \subseteq R_1$$

Así que:

(K, P) un cuerpo ordenado, R y R_1 extensiones reales cerrados de K tal que $K \hookrightarrow R$, $K \hookrightarrow R_1$. Dado el sistema de ecuaciones de la forma:

$$S(\underline{X}) = \begin{cases} g_1(\underline{X}) = 0 \\ \quad . \\ \quad . \\ \quad . \\ g_s(\underline{X}) = 0 \end{cases}$$

cada $g_i \in K[X_1, \ldots, X_n]$.

Afirmación 2.11.1. $x = (X_1 + p\ ,\ \ldots\ ,\ X_n + p) \in R_1^n$ es una solución del sistema $S(\underline{X})$.

Demostración.

$$g_i(x) = \sum_{\alpha_i} a_{\alpha_i} \underline{x}^{\alpha_i}$$

$$\Longrightarrow g_i(x) = \sum_{\alpha_i} a_{\alpha_i} \underline{X}^{\alpha_i} + p$$

$$\Leftrightarrow g_i(x) = g_i\left(\underline{X}\right) + p$$

$$\Leftrightarrow g_i(x) = 0$$

$$\therefore x \in R_1^n \text{ es una solución del sistema } S\left(\underline{X}\right).$$

Entonces, por el Teorema 2.10.2 (Principio de Transferencia de Tarski):

$S\left(\underline{X}\right)$ tiene una solución $r = (r_1, \ldots, r_n) \in R^n$.

Como D es una $K - \acute{a}lgebras$ finitamente generada, entonces $D = K[d_1, \ldots, d_n]$; $d_i \in D$.

Definimos:

$$\begin{array}{rccc} \phi : & D & \longrightarrow & R \\ & \sum_{\alpha_i} a_{\alpha_i} \underline{d}^{\alpha_i} & \mapsto & \phi\left(\sum_{\alpha_i} a_{\alpha_i} \underline{d}^{\alpha_i}\right) = \sum_{\alpha_i} a_{\alpha_i} \underline{r}^{\alpha_i} \end{array} \text{ ; donde}$$

$$\alpha_i = \left(\alpha_{1_i}, \ldots, \alpha_{n_i}\right) \in (\mathbb{N}_0)^n, \ a_{\alpha_i} \in K \ ; \ \underline{d}^{\alpha_i} = d_1^{\alpha_{1_i}} \ldots d_n^{\alpha_{n_i}}, \ \underline{r}^{\alpha_i} = r_1^{\alpha_{1_i}} \ldots r_n^{\alpha_{n_i}}$$

es un homomorfismo de $K - \acute{a}lgebras$

(b):

Tenemos: $a_i > 0$, $\sqrt{a_i} \in R_1$; $i = 1, \ldots, m$.

Sabemos que:

$D = K[d_1, \ldots, d_n]$, $d_i \in D$.

Definimos:

$D' = D\left[\frac{1}{\sqrt{a_1}}, \ldots, \frac{1}{\sqrt{a_m}}\right] = K\left[d_1, \ldots, d_n, \frac{1}{\sqrt{a_1}}, \ldots, \frac{1}{\sqrt{a_m}}\right] \subseteq R_1$ es un dominio entero

que es una $K - \acute{a}lgebra$ finitamente generada.

Sea F' el cuerpo de cocientes de D':

$D \subseteq D'$

$\Longrightarrow F \subseteq F' \subseteq R_1$

$\Longrightarrow \underbrace{R_1^{(2)} \cap F}_{=Q} \subseteq R_1^{(2)} \cap F'$

Sea $R_1^{(2)} \cap F'$ un ordenamiento de F':

$P \subseteq Q \subseteq R_1^{(2)} \cap F' \Longrightarrow P \subseteq R_1^{(2)} \cap F'$

Es decir: $R_1^{(2)} \cap F'$ extiende a P

Aplicando (a), obtenemos un homomorfismo de $K - \acute{a}lgebras$ $\phi: D' \longrightarrow R$.

Así:

$\sqrt{a_i} = a_i \frac{1}{\sqrt{a_i}} \in D'$ y $\phi\left(\sqrt{a_i}\right)\phi\left(\frac{1}{\sqrt{a_i}}\right) = \phi(1) = 1$

$\Longrightarrow \phi\left(\sqrt{a_i}\right) \neq 0$

$\phi: D \longrightarrow R$ es un homomorfismo de $K - \acute{a}lgebras$

$\phi(a_i) = \phi\left(\sqrt{a_i}^2\right) = \phi\left(\sqrt{a_i}\right)^2 > 0$

Por lo tanto:

$\exists\, \phi: D \longrightarrow R$ un homomorfismo de $K - \acute{a}lgebras$ tal que $\phi(a_i) > 0\,, i = 1, \ldots, m$.

CAPÍTULO III

VARIABLES E HIPÓTESIS

3.1. Variables de la investigación

Son los polinomios $f \in K[\underline{X}]$ donde K es un cuerpo ordenado.

3.2. Operacionalización de las variables

Variables	Dimensiones	Indicadores
$f \in K[\underline{X}]$ donde K es un cuerpo ordenado.	$f \in K[\underline{X}]$ donde K es un cuerpo ordenado tal que $f(x) \geq 0,\ \forall x \in R^n\ (R/K)$.	Mediante la teoría de cuerpos ordenados, $f \in K[\underline{X}]$ donde K es un cuerpo ordenado tal que $f(x) \geq 0,\ \forall x \in R^n\ (R/K)$ podrá expresarse como suma finita de cuadrados de $K(\underline{X})$.

3.3. Hipótesis general e hipótesis específica

3.3.1. Hipótesis general

El problema diecisiete de Hilbert tiene solución positiva.

3.3.2. Hipótesis específica

Usando el Teorema del Homomorfismo de Lang podemos dar solución al problema diecisiete de Hilbert.

CAPÍTULO IV

METODOLOGÍA DE LA INVESTIGACIÓN

4.1. Tipo y diseño de la investigación

4.1.1. Tipo de investigación

La investigación es de tipo científico-teórico y la metodología es de tipo inductivo-deductivo.

4.1.2. Diseño de la investigación

El procedimiento para la demostración de los resultados es el siguiente:

(1) Se comienza estudiando la teoría de cuerpos ordenados y cuerpos reales cerrados.

(2) Presentamos el Teorema de Tarski-Seidenberg (versión básica).

(3) Utilizando el Teorema de Tarski-Seidenberg (versión básica), demostramos el Principio de Transferencia de Tarski.

(4) Teniendo el Principio de Transferencia de Tarski demostramos el Teorema de homomorfismo de Lang.

(5) Finalmente obtenemos la solución del problema diecisiete de Hilbert utilizando el Teorema de Homomorfismo de Lang.

4.2. Población y muestra

Nuestra población son los cuerpos ordenados y nuestra muestra son los cuerpos reales cerrados.

4.3. Técnicas e instrumentos de recolección de datos

Para la realización de la tesis se ha revisado bibliografía especializada y artículos en internet.

4.4: Plan de análisis estadístico de datos

Por ser nuestra tesis netamente abstracto, no se necesitó procedimientos de recolección de datos.

CAPÍTULO V

RESULTADOS

5.1. Solución del problema diecisiete de Hilbert

Teorema 5.1.1 (El problema diecisiete de Hilbert de Artin). Sean (K, P) un cuerpo ordenado y R una extensión real cerrado de (K, P) tal que $R^{(2)} \cap K = P$. Sea $f \in K[\underline{X}]$ tal que $f(x) \geq 0, \forall\, x \in R^n$. Entonces f se puede escribir como $f = \sum_{i=1}^{s} r_i f_i^2$ para algunos $f_1, \ldots, f_s \in K(\underline{X})$; $r_1, \ldots, r_s \in P$.

Demostración:

Denotamos:

$$T = \left\{ \sum_{i=1}^{s} r_i f_i^2 \,/ s \in \mathbb{N}, f_i \in K(\underline{X}) \text{ y } r_i \in P \right\} \subseteq K(\underline{X}) \text{ no vacío}$$

$\Longrightarrow T + T, T \cdot T \subseteq T$ y $K(\underline{X})^{(2)} \subseteq T$.

Afirmación 5.1.1. $-1 \notin T$

Demostración. Por contradicción

Supongamos que: $-1 \in T$

$-1/1 = \sum_{i=1}^{s} \left(r_i g_i^2 / h_i^2 \right); s \in \mathbb{N}, r_i \in P, g_i, h_i \in K[\underline{X}]$ con $h_i \neq 0 \Longrightarrow \prod_{i=1}^{s} h_i \neq 0$ es decir: $\exists\, x_1 \in K^n \,/\, \prod_{i=1}^{s} h_i\,(x_1) \neq 0$.

$$\Longrightarrow -1/1 = \left.\sum_{i=1}^{s} r_i \left[g_i \left(\prod_{\substack{j=1 \\ j\neq i}}^{s} h_j \right) \right]^2 \right/ \left(\prod_{i=1}^{s} h_i \right)^2$$

$$\Leftrightarrow \sum_{i=1}^{s} r_i \left[g_i \left(\prod_{\substack{j=1 \\ j\neq i}}^{s} h_j \right) \right]^2 + \left(\prod_{i=1}^{s} h_i \right)^2 = 0$$

Evaluando en x_1:

$$\Longrightarrow \sum_{i=1}^{s} r_i \left[g_i(x_1) \left(\prod_{\substack{j=1 \\ j\neq i}}^{s} h_j\,(x_1) \right) \right]^2 + \left(\prod_{i=1}^{s} h_i(x_1) \right)^2 = 0$$

$K \subseteq R$, $R^{(2)} \cap K = P$ entonces $r_i = a_i^2$, $a_i \in R$:

$$\Leftrightarrow \sum_{i=1}^{s} \left[a_i g_i(x_1) \left(\prod_{\substack{j=1 \\ j\neq i}}^{s} h_j\,(x_1) \right) \right]^2 + \left(\prod_{i=1}^{s} h_i(x_1) \right)^2 = 0$$

Como R es real, tenemos:

$$\prod_{i=1}^{s} h_i(x_1) = 0 (\longrightarrow\longleftarrow) \prod_{i=1}^{s} h_i(x_1) \neq 0$$

$$\therefore -1 \notin T$$

Por lo tanto:

T es un cono prepositivo de $K(\underline{X})$.

Si $f \notin T$ entonces, por Teorema 2.4.2, existe un cono positivo Q de $K(\underline{X})$ con $T \subseteq Q, f \notin Q$.

Claramente $P \subseteq Q$ así que $Q \cap K = P$, es decir, Q extiende a P.

Tenemos:

(K, P) un cuerpo ordenado, sea R' la clausura real de (K, P), $K[\underline{X}]$ es un dominio entero que es una $K - álgebra$ finitamente generada y que el ordenamiento P se extiende a Q en $K(\underline{X})$, además $-f \in Q$ $(-f > 0)$.

Aplicando el Teorema de Homomorfismo de Lang, Teorema 2.11.1 parte (b) tenemos:

$\exists\, \phi : K[\underline{X}] \longrightarrow R' \subseteq R$ un homomorfismo de $K -$ álgebras tal que $\phi(f) < 0$.

Tomando:

$a_i = \phi(X_i) \in R \;;\; i = 1, \ldots, n$

Vemos que:

$$\phi(f) = \phi\left(\sum_\alpha a_\alpha \underline{X}^\alpha\right) = \underbrace{\sum_\alpha a_\alpha \underline{\phi(X)^\alpha}}_{\underline{\phi(X)} = (\phi(X_1), \ldots, \phi(X_n))} = \underbrace{\sum_\alpha a_\alpha \underline{a}^\alpha}_{\underline{a} = (a_1, \ldots, a_n)} = f(a_1, \ldots, a_n)$$

$$< 0 \; (\longrightarrow\longleftarrow) \; f(a_1, \ldots, a_n) \geq 0$$

$\Longrightarrow f \in T$

$$\therefore f = \sum_{i=1}^{s} r_i f_i^2 \text{ para algunos } f_1, \ldots, f_s \in K(\underline{X}) \ ; \ \ r_1, \ldots, r_s \in P.$$

Observación 5.1.1. Del Teorema anterior, $f \in K[\underline{X}] \subseteq R[\underline{X}] \left(K(\underline{X}) \subseteq R(\underline{X})\right)$ se puede escribir como $f = \sum_{i=1}^{s} r_i f_i^2 \ = \sum_{i=1}^{s} (s_i f_i)^2$ para algunos $f_1, \ldots, f_s \in K(\underline{X}) \subseteq R(\underline{X})$; $r_i = s_i^2$, $s_i \in R$; es decir: f se puede escribir como suma finita de cuadrados de $R(\underline{X})$.

Corolario 5.1.1 (El problema diecisiete de Hilbert). Todo $f \in \mathbb{R}[\underline{X}]$, si $f \geq 0$ sobre $\mathbb{R}^n \Longrightarrow f$ se puede escribir como suma finita de cuadrados de $\mathbb{R}(\underline{X})$.

Demostración.

Tenemos:

$\left(\mathbb{R}, \mathbb{R}^{(2)}\right)$ un cuerpo ordenado y $\mathbb{R}$ una extensión real cerrado de $\left(\mathbb{R}, \mathbb{R}^{(2)}\right)$ tal que $\mathbb{R}^{(2)} \cap \mathbb{R} = \mathbb{R}^{(2)}$. Sea $f \in \mathbb{R}[\underline{X}]$, $f \geq 0$ sobre $\mathbb{R}^n$, entonces:

Por Teorema 5.1.1 y Observación 5.1.1, tenemos:

$$\therefore f \text{ se puede escribir como suma finita de cuadrados de } \mathbb{R}(\underline{X}).$$

CAPÍTULO VI

DISCUSIÓN DE RESULTADOS

(1) También podemos tener la solución del problema diecisiete de Hilbert sin utilizar el teorema de homomorfismo de Lang, sólo utilizando el principio de transferencia de Tarski con los argumentos de la Teoría de Modelos ver [1], página 36.

(2) Tenemos entonces el resultado, según el cual, $f \in \mathbb{R}(X_1, \ldots, X_n)$ tal que $f(x) \geq 0, \forall\, x \in \mathbb{R}^n$ donde se define f es suma de un número finito m de cuadrados de elementos de $\mathbb{R}(X_1, \ldots, X_n)$; este $m = m(n, f)$ depende de f y de n. ¿Es posible encontrar una cota superior de los $m(n, f)$?. Albrecht Pfister en 1965 contestó esta pregunta y demostró que $m(n, f) \leq 2^n$ ver [1], página 69.

CAPÍTULO VII

CONCLUSIONES

(1) El cuerpo de los números reales ($\mathbb{R}$) es un cuerpo real cerrado.

(2) El Principio de Transferencia de Tarski se puede demostrar usando Teorema de Tarski-Seidenberg (Versión Básica).

(3) El Problema diecisiete de Hilbert se puede solucionar utilizando el Teorema de Homomorfismo de Lang.

CAPÍTULO VIII

RECOMENDACIONES

(1) En esta tesis usamos mucho la teoría de cuerpos, para este tema los libros que recomiendo son [13] y [16], por lo cual es recomendable su lectura para el mejor entendimiento de la tesis.

(2) Para un estudio más amplio de la teoría de cuerpos ordenados, cuerpos reales y cuerpos reales cerrados recomiendo los libros [1], [2] y [3].

REFERENCIAS BIBLIOGRÁFICAS

[1] Alexander Prestel ; Charles Delzell. “Positive Polynomials: From Hilbert’s 17th Problem to Real Algebra”. Springer, 2004.

[2] Basu, S. ; Pollack, R. ; Roy, M.-F. “Algorithms in Real Algebraic Geometry”. Springer, 2016.

[3] Bochnak, J. ; Coste, M. ; Roy M.-F. “Real Algebraic Geometry”. Springer, 1998.

[4] David A. Cox ; John Little ; Donal O’Shea. “Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra”. Springer International Publishing, 2015.

[5] David Hilbert. “Mathematsche Probleme”. Gottinger Nach. (1900), p. 284-285.

[6] David Hilbert. “Uber terniire definite Formen”. Acta. Math. 17 (1893), p. 169-197.

[7] David Hilbert. “Uber die Darstellung definiter Formen als Summe von Formen-quadraten”. Math. Ann. 32 (1888), p. 342-350.

[8] Emil Artin. “Uber die Zerlegung definiter Funktionen in Quadrate”. Ann. Math. Sem. Hamburg 5 (1927), p. 100-115.

[9] Felipe Zaldívar. “Teoría de Galois”. Anthropos, 1996.

[10] G. H. Hardy y E. M. Wright. “An Introduction to the Theory of Numbers”. Fourth edition. Oxford at the Clarendon Press, 1968.

[11] G. Kreisel et J. L. Krivine. “Eléments de logique mathématique-Théorie des modeles”. Dunod-París, 1967.

[12] I. N. Herstein. “Álgebra Abstracta”. Grupo Editorial Iberoamérica, 1988.

[13] Iain T. Adamson. “Introduction to Field Theory”. Oliver and Boyd Ltd, 1964.

[14] Murray A. Marshall. “Positive polynomials and sums of squares”. American Mathematical Society, 2008.

[15] Murray A. Marshall. “Spaces of Ordering and Abstract Real Spectra”. Springer-Verlag Berlin Heidelberg, 1996.

[16] Paul J. McCarthy. “Algebraic Extensions of Fields”. Dover, 1991.

[17] Serge Lang. “Álgebra”. Springer-Verlag New York, 2002.

[18] T.S. Motzkin. “The arithmetic-geometric inequality”. In: Proc. Symposium on Inequalities, edited by O. Shisha. Academic Press, New York, 1967, p. 205-224.