Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ciencias Matemáticas
Escuela Profesional de Matemática

Cuerpos reales

TESIS

Para optar el Título Profesional de Licenciado en Matemática

AUTOR

Michel Anthony Salvador LUNA CCORA

ASESOR

Dr. Gabriel Armando MUÑOZ MÁRQUEZ

Lima, Perú

2023

Referencia bibliográfica

Luna, M. (2023). *Cuerpos reales*. [Tesis de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ciencias Matemáticas, Escuela Profesional de Matemática]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Michel Anthony Salvador Luna Ccora
Tipo de documento de identidad	DNI
Número de documento de identidad	46464203
URL de ORCID	https://orcid.org/0009-0003-3300-4163
Datos de asesor	
Nombres y apellidos	Gabriel Armando Muñoz Márquez
Tipo de documento de identidad	DNI
Número de documento de identidad	44444774
URL de ORCID	https://orcid.org/0000-0001-5064-1250
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Leonardo Henry Alejandro Aguilar
Tipo de documento	DNI
Número de documento de identidad	43069051
Miembro del jurado 1	
Nombres y apellidos	Luis Guillermo Huamanlazo Ricci
Tipo de documento	DNI
Número de documento de identidad	09197486
Datos de investigación	
Línea de investigación	A.3.1.3. Álgebra

Grupo de investigación	No aplica.
Agencia de financiamiento	Sin financiamiento.
Ubicación geográfica de la investigación	Universidad Nacional Mayor de San Marcos País: Perú Departamento: Lima Provincia: Lima Distrito: Lima Coordenadas geográficas Latitud: -12.058333 Longitud: -77.083333
Año o rango de años en que se realizó la investigación	Mayo 2023 – octubre 2023
URL de disciplinas OCDE	Matemáticas puras https://purl.org/pe-repo/ocde/ford#1.01.01 Matemáticas aplicadas https://purl.org/pe-repo/ocde/ford#1.01.02

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. Decana de América
FACULTAD DE CIENCIAS MATEMÁTICAS
ESCUELA PROFESIONAL DE MATEMÁTICA

ACTA DE SUSTENTACIÓN DE TESIS PARA LA OBTENCIÓN DEL TÍTULO PROFESIONAL DE LICENCIADO(A) EN MATEMÁTICA (PROGRAMA DE TITULACIÓN PROFESIONAL 2023)

En la UNMSM – Ciudad Universitaria – Facultad de Ciencias Matemáticas, siendo las 09:40 horas del viernes 06 de octubre del 2023, se reunieron los docentes designados como Miembros del Jurado Evaluador (PROGRAMA DE TITULACIÓN PROFESIONAL 2023): Dr. Leonardo Henry Alejandro Aguilar (PRESIDENTE), Mg. Luis Guillermo Huamanlazo Ricci (MIEMBRO) y el Dr. Gabriel Armando Muñoz Márquez (MIEMBRO ASESOR), para la sustentación de la Tesis titulada: "**CUERPOS REALES**", presentado por el señor **Bachiller MICHEL ANTHONY SALVADOR LUNA CCORA**, para optar el Título Profesional de Licenciado en Matemática.

Luego de la exposición de la Tesis, el Presidente invitó al expositor a dar respuesta a las preguntas formuladas.

Realizada la evaluación correspondiente por los Miembros del Jurado Evaluador, el expositor mereció la aprobación Sobresaliente....., con un calificativo promedio de dieciocho (18)

A continuación, los Miembros del Jurado Evaluador dan manifiesto que el participante **Bachiller MICHEL ANTHONY SALVADOR LUNA CCORA**, en vista de haber aprobado la sustentación de su Tesis, será propuesto para que se le otorgue el Título Profesional de Licenciado en Matemática.

Siendo las 10:20 horas se levantó la sesión firmando para constancia la presente Acta.

Dr. Leonardo Henry Alejandro Aguilar
PRESIDENTE

Mg. Luis Guillermo Huamanlazo Ricci
MIEMBRO

Dr. Gabriel Armando Muñoz Márquez
MIEMBRO ASESOR

Yo Gabriel Armando Muñoz Márquez en mi condición de asesor acreditado con la Resolución Decanal N° 001544-2023-D-FCM/UNMSM de la tesis, cuyo título es CUERPOS REALES, presentado por el bachiller Michel Anthony Salvador Luna Ccora para optar el título Profesional de Licenciado en Matemática de la Facultad de Ciencias Matemáticas.

CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante el software de similitud textual, el documento evaluado cuenta con el porcentaje de 6 % de similitud, nivel **PERMITIDO** para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional.**

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del título correspondiente.

Firma del Asesor _____

DNI: 44444774

Nombres y apellidos del asesor:
Gabriel Armando Muñoz Márquez

Índice general

Agradecimientos

Agradezco primeramente a Dios por la oportunidad de poder realizar este trabajo. A mis padres, por la formación y el cariño brindado, a mis amistades por el apoyo y la confianza. Finalmente, agradezco a mi asesor el Dr. Gabriel Muñoz por sus enseñanzas, su tiempo e interés que mostró desde el inicio de este trabajo.

Resumen

En este trabajo estamos interesados en el estudio de cuerpos donde no se cumpla la relación

$$\sum a_i^2 = -1$$

con los a_i en dicho cuerpo. Consideraremos lo conceptos de cuerpo ordenado, cuerpo real, cuerpo real cerrado y cerradura real. Probaremos que todo cuerpo real admite una cerradura real, es decir, una extensión algebraica que es real cerrada. Además, probaremos que todo cuerpo real cerrado admite un único orden y que los positivos de un cuerpo ordenado están determinados por los cuadrados de una de sus cerraduras reales.

Palabras Clave: Cuerpo ordenado, cuerpo real, cerradura real, teorema de Sturm.

Abstract

In this work we are interested in the study of fields where the relation does not hold relación

$$\sum a_i^2 = -1$$

with the a_i in said field. We will consider the concepts of ordered field, real field, closed real field and real closure. We will prove that every real field admits a real closure, that is, an algebraic extension which is real closed. Also, we will prove that every closed real field admits a unique order and that the positives of an ordered field are determined by the squares of one of its real closures.

Keywords: Ordered field, real field, real closure, Sturm theorem.

Introducción

Una propiedad básica de los números reales es que la única relación de la forma

$$\sum a_i^2 = 0 \text{ con } a_i \in \mathbb{R},$$

sea la trivial:

$$0^2 + 0^2 + \cdots + 0^2 = 0.$$

De forma equivalente, podemos determinar que en los reales no tenemos la siguiente relación:

$$\sum a_i^2 = -1 \text{ con } a_i \in \mathbb{R},$$

así el objetivo de este trabajo es estudiar cuerpos donde no se cumpla dicha propiedad, a los cuales llamaremos **cuerpos reales**.

El trabajo esta estructurado de la siguiente manera: en el primer capitulo abarcaremos los conceptos preliminares como son cuerpos y extensiones de cuerpos; donde mencionaremos ejemplos y resultados que serán utilizados en el capitulo 2.

En el segundo capitulo abarcaremos nuevos conceptos, como es el de **cuerpo ordenado**: definiremos el concepto de orden en un cuerpo, el cual esta determinado por el conjunto de elementos positivos. Verificaremos propiedades que se cumplen en un cuerpo ordenado, como por ejemplo; la unidad es positiva, el inverso de un elemento positivo también es positivo, los cuadrados de elementos son positivos, etc.

También en el segundo capitulo, veremos el concepto de cuerpo real, el cual esta caracterizado porque la relación

$$\sum a_i^2 = -1$$

con los a_i en el cuerpo, no se cumple. Veremos que un cuerpo ordenado es real y bajo nuevos conceptos podremos determinar la forma de los elementos positivos. Veremos los conceptos de cuerpo real cerrado y cerradura real, donde tendremos resultados interesantes como:

- Todo cuerpo real admite una cerradura real, es decir, una extensiń algebraica que es real cerrada. Este resultado nos permitirá encontrar un orden en el cuerpo.

- Si un cuerpo es real cerrado entonces admite un único orden caracterizado por sus cuadrados.

- Versión del teorema del valor intermedio para polinomios con coeficientes en un cuerpo real cerrado.

- Existencia de cerradura real para un cuerpo ordenado, también se garantiza la unicidad mediante un isomorfismo que preserva el orden.

Capítulo 1

Preliminares

1.1. Cuerpos

Definición 1.1.1. *Un cuerpo es un conjunto K con dos operaciones binarias en K llamadas adición y multiplicación. Una operación binaria es un mapeo $K \times K \to K$, esto es, una correspondencia que asocia cada par ordenado de elementos de K a un únicamente determinado elemento de K. Es decir, para la adición;*

$$\begin{aligned} + : K \times K &\longrightarrow K \\ (a, b) &\longmapsto a + b \end{aligned}$$

y para la multplicación;

$$\begin{aligned} \cdot : K \times K &\longrightarrow K \\ (a, b) &\longmapsto a \cdot b \end{aligned}$$

se refiere a $a+b$ como la suma de a mas b y a $a \cdot b$ (también denotado ab) como el producto de a y b. Estas operaciones tienen que satisfacer las siguientes propiedades:

- ***Asociatividad*** *de la adición y multiplicación: Sean a, b y $c \in K$; $a + (b + c) = (a + b) + c$ y $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.*

- ***Conmutatividad*** *de la adición y multiplicación: Sean a y $c \in K$; $a + b = b + a$ y $a \cdot b = b \cdot a$.*

- ***Identidad*** *aditiva y multiplicativa: Existen dos elementos diferentes 0 y 1 en K tal que para cualquier $a \in K$; $a + 0 = a \quad y \quad a \cdot 1 = a$.*

- ***Inversos aditivos**: Para todo $a \in K$, existe un elemento en K, denotado $-a$, llamado inverso aditivo de a, tal que $a + (-a) = 0$.*

- ***Inversos multiplicativos**: Para todo $a \neq 0 \in K$, existe un elemento en K, denotado a^{-1} o $1/a$, llamado inverso multiplicativo de a, tal que $a \cdot a^{-1} = 1$.*

- ***Distribucion** de la multiplicación sobre la adición: Sean a, b y $c \in K$; $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.*

Observación 1.1.2. *Dado K un cuerpo:*

- *Se puede definir $K[X]$ como el conjunto de polinomios con coeficientes en K, es decir, dicho conjunto tiene elementos de la forma:*

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,\ n \in \mathbb{N} \cup \{0\}.$$

- *Si $a_n \neq 0$ decimos que n es el **grado del polinomio** f, en otras palabras, el grado de un polinomio f es el menor entero n tal que $a_r = 0$ para todo $r > n$, en dicho caso; a_n es llamado coeficiente principal. Los elementos de K son llamados **polinomios constantes o de grado cero**.*

- *No es difícil demostrar que $K[X]$ cumple con casi todas las condiciones de cuerpo ya mencionadas con la suma ($f(x) + g(x) = (f + g)(x)$) y multiplicación ($f(x) \cdot g(x) = (f \cdot g)(x) = fg(x)$) usuales, menos la de la existencia de inversos multiplicativos para todos sus elementos. A este conjunto se le conoce como **anillo de polinomios**.*

Proposición 1.1.3. *Sea K un cuerpo, $f, g \in K[X]$ polinomios donde g tiene como coeficiente principal la unidad. Entonces existen $q, r \in K[X]$ únicos, tal que*

$$f = gq + r$$

y grado de r es menor al grado de g. Como es usual q es llamado cociente y r es llamado residuo.

Demostración. Revisar pagina 174 de [3]. □

Observación 1.1.4. *Sea K un cuerpo:*

- *Dada la proposición anterior, se puede definir la división de polinomios, dados $f, g \in K[x]$:*

$$g|_f, \text{ es decir, } g \text{ divide a } f \iff \exists h \in K[X] \text{ tal que } f = gh.$$

- *Un polinomio $f \in K[X]$ es llamado **irreducible en** $K[X]$ si tiene grado mayor igual que uno y no se puede escribir como producto de otros dos polinomios; $f = gh$, tal que $g, h \in K[x]$ no son constantes.*

- *Dado $f \in K[X]$, $\alpha \in K$ es llamada **raiz de** f si $f(\alpha) = 0$.*

- *Se puede definir también **la derivada un de polinomio**, dado $f \in K[X]$; $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ entonces la derivada de f sera*

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1$$

Se pueden verificar las siguientes propiedades, dados $f, g \in K[X]$:

$$(f+g)' = f' + g' \ \wedge \ (fg)' = f'g + fg'$$

Ejemplo 1.1.5. *Sea $\mathbb{R}$ los números reales, sea F el conjunto de **funciones racionales**, es decir funciones de una variable que son expresadas como cociente de dos polinomios:*

$$f(x) = \frac{p(x)}{q(x)},$$

donde $p, q \in \mathbb{R}[X]$ no teniendo ningún factor en común y q no idéntico a cero. De manera general, cada función racional puede expresarse de la siguiente forma:

$$f(x) = \frac{a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0}{b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0},$$

donde $b_n \neq 0$. De hecho, sin perdida de generalidad, se puede tomar $b_n = 1$.

El dominio de una función racional consiste en todos números reales a excepción de una cantidad finita de números donde el denominador es 0, en dichos puntos el numerador es diferente de 0. Así, cuando se comparen dos funciones racionales f y g; la intersección de sus dominios consistirá también de todos los reales a excepción de una cantidad finita de números.

Definamos la suma y producto en dicho conjunto:

$$\left(\frac{p}{q} + \frac{r}{s}\right)(x) = \frac{p(x)s(x) + q(x)r(x)}{q(x)s(x)} \quad \wedge \quad \left(\frac{p}{q} \cdot \frac{r}{s}\right)(x) = \frac{p(x)r(x)}{q(x)s(x)},$$

teniendo en cuenta que los factores en común deben ser simplificados.

Para verificar que F con dicha suma y producto forma un cuerpo se deben verificar las propiedades anteriormente mencionadas. No es difícil verificar la asociatividad, conmutatividad y distribucion. Se puede ver que 0 y 1 en $\mathbb{R}$ serian la identidad aditiva y la identidad multiplicativa, respectivamente. Para los inversos; si f es una función racional, consideramos a $-f$ como inverso aditivo y para el multiplicativo; f^{-1}, el cual no es función inversa, sino el reciproco de f, es decir;

$$si \quad f = \frac{p}{q} \quad entonces \quad f^{-1} = \frac{q}{p},$$

donde el dominio de f^{-1} no tendrá los valores x donde $p(x) = 0$.

1.2. Extensiones de Cuerpos

Definición 1.2.1. *Sea E y F cuerpos tales que $E \subset F$, entonces se denomina a F como **extension** de E. También podemos llamar a E como **subcuerpo** de F. Podemos ver a F como un espacio vectorial sobre E, y decimos que F es una **extension finita** o **infinita** de E de acuerdo a su dimension como espacio vectorial.*

Definición 1.2.2. *Sea E un subcuerpo de un cuerpo F.*

- *Un elemento $\alpha \in F$ es llamado **algebraico sobre** E si existe una cantidad finita de elementos $a_0, a_1, \cdots, a_n \in E$ $(n \geq 1)$, no todos iguales a 0, tales que*

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

  En otras palabras, $\alpha \in F$ es algebraico sobre E, si existe $p \in E[X]$ tal que α es raiz de p:

$$p(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

- *Dado un $\alpha \in F$ algebraico sobre E, se define $Irr(\alpha, E, X) \in E[X]$, como el **polinomio irreducible de** α **sobre** E, dicho polinomio es el de menor grado (mayor igual a 1) en $E[X]$ tal que α sea su raíz y tiene como coeficiente principal la unidad.*

Como el nombre indica, veamos que dicho polinomio es irreducible, denotando como $f = Irr(\alpha, E, X)$*, supongamos que no lo sea;*

$$\rightarrow \exists\, p, q \in E[X],\ \textit{no constantes con coeficiente principal la unidad} \,/\, f = pq,$$

dado que α *es raíz de* f*; entonces*

$$p(\alpha) = 0 \ \vee \ q(\alpha) = 0,$$

en caso contrario; $f(\alpha) = p(\alpha)p(\alpha) \neq 0$ *lo cual es contradicción. Así* α *es raíz de* p *o* q*, ambos polinomios con la unidad como coeficiente principal y de menor grado que el de* f*, lo cual es contradicción con la definición de* f*.*

- *Una extension* F *de un cuerpo* E *se dice* ***extension algebraica de*** E *si todo elemento de* F *es algebraico sobre* E*.*

Proposición 1.2.3. *Sean* K *un cuerpo,* F *una extension y* $\alpha \in F$ *algebraico. Sea* f *irreducible en* $K[x]$ *tal que* α *es raíz de* f*. Entonces, dado* $g \in K[X]$*,* $g(\alpha) = 0$ *si y solo si* $f|_g$ *en* K*; es decir existe un* $h \in K[x]$ *tal que* $g = fh$*.*

Demostración. Revisar pagina 2 de [1]. □

Proposición 1.2.4. *Sean* E *un cuerpo,* $E \subset F$ *una extension. Entonces*

$$A = \{\alpha \in F \mid \alpha \textit{ es algebraico sobre } E\}$$

es una extension de E*.*

Demostración. Ver pagina 256 de [2]. □

Observación 1.2.5.

- *Tomando en cuenta la proposición anterior, vemos que si* $\alpha, \beta \in F$ *son algebraicos sobre* E *entonces* $\alpha + \beta$ *y* $\alpha\beta$ *son algebraicos sobre* E*, es decir, suma y producto de algebraicos son algebraicos.*

- *Dado* E *un cuerpo,* $E \subset F$ *una extension e* I *un conjunto finito o infinito de elementos de* F *que son algebraicos sobre* E*. Entonces definimos la familia de subgrupos de* F*:*

$$B = \{G \subseteq F \mid E \cup I \subset G\},$$

vemos que no es vacío, ya que $E \cup I \subset F$. No es difícil probar que

$$C = \bigcap_{G \in B} B$$

es una extension de E. Dependiendo de I, los elementos de C tendrán una forma definida, como en la proposición siguiente.

Definición 1.2.6. *Sea K un cuerpo y E una extension. Dado $\alpha \in E$, denotamos como $K(\alpha)$ al subcuerpo mas pequeño de E que contiene a K y α. Se verifica que dicho subcuerpo es una extension de K y sus elementos son de la forma $f(\alpha)/g(\alpha)$, con $f, g \in K[X]$ tal que $g(\alpha) \neq 0$.*

Proposición 1.2.7. *Sea K un cuerpo, E una extension y $\alpha \in E$ algebraico sobre K. Entonces, siendo $n \in \mathbb{N}$ el grado de $Irr(\alpha, K, X)$:*

$$K(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} / a_i \in K, \forall i = 0 : n-1\},$$

es decir, $K(\alpha)$ es una extension finita sobre K con dimension n.

Demostración. Ver pagina 225 de [3]. □

Definición 1.2.8. *Sea K un cuerpo y E una extension. Dados $\alpha_1, \alpha_2, \cdots, \alpha_n \in E$, denotamos como $K(\alpha_1, \alpha_2, \cdots, \alpha_n)$ al subcuerpo mas pequeño de E que contiene a K y $\alpha_1, \alpha_2, \cdots, \alpha_n$. Se verifica que dicho subcuerpo es una extension de K y sus elementos son de la forma*

$$\frac{f(\alpha_1, \alpha_2, \cdots, \alpha_n)}{g(\alpha_1, \alpha_2, \cdots, \alpha_n)},$$

con f, g polinomios de n variables con coeficientes en K y $g(\alpha_1, \alpha_2, \cdots, \alpha_n) \neq 0$.

Proposición 1.2.9. *Sea K un cuerpo y $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ elementos algebraicos sobre K. Entonces $K(\alpha_1, \alpha_2, \cdots, \alpha_n)$ es una extension finita sobre K.*

Demostración. Ver pagina 227 de [3]. □

Definición 1.2.10. *Sea E un cuerpo, se dice que es **algebraicamente cerrado** si todo polinomio en $E[X]$ de grado mayor o igual a 1 tiene una raíz en E.*

Proposición 1.2.11. *Sea K un cuerpo. Existe una extension de K, denotada K^a, que es algebraica sobre K y algebraicamente cerrada.*

Demostración. Ver pagina 232 de [3] . □

Definición 1.2.12. *Sean E, F dos cuerpos,*

- *Un **homomorfismo** entre E y F es una función $\phi : E \to F$ tal que preserva las operaciones del cuerpo, es decir, dados $a, b \in E$:*

$$\phi(a+b) = \phi(a) + \phi(b)$$
$$\phi(ab) = \phi(a)\phi(b)$$

- *Un **monomorfismo** es un homomorfismo inyectivo, es decir, dados $a, b \in E$ tal que*

$$\phi(a) = \phi(b) \to a = b$$

- *Si ademas un monomorfismo es sobreyectivo, es decir, $\phi(E) = F$; se le llama **isomorfismo**,*

Definición 1.2.13. *Sean E, F dos cuerpos, tal que $E \subset F$ extension:*

- *Sea $\alpha \in F$ algebraico sobre E, se dice que α **es separable sobre** E si $Irr(\alpha, E, X)$ no tiene múltiples raíces.*

- *Una extension F es **separable** si cada elemento $\alpha \in F$ es separable sobre E.*

Definición 1.2.14. *La **característica** de un cuerpo es definida como el menor numero de veces que se necesita usar la identidad multiplicativa (1) en una suma para obtener la identidad aditiva (0). Si la suma nunca alcanza la identidad aditiva, se dice que la característica es cero.*

$$\underbrace{1 + \cdots + 1}_{n \text{ sumandos}} = 0$$

si n existe; el menor n seria la característica, en caso contrario; la característica es 0.

Proposición 1.2.15. *Sean E, F dos cuerpos, tal que $E \subset F$ extension:*

- *Dado $\alpha \in F$ algebraico sobre E. Si E tiene característica 0 entonces α es separable.*

- *Si F es extension algebraica de E con característica 0 entonces F es separable.*

Demostración. Revisar pagina 247 de [3]. □

Teorema 1.2.16. ***(Teorema del Elemento Primitivo).*** *Sea F una extension finita de un cuerpo E. Si F es separable sobre E, entonces existe un elemento $\alpha \in F$ tal que $F = E(\alpha)$.*

Demostración. Revisar pagina 243 de [3]. □

Capítulo 2

Cuerpos Reales

2.1. Cuerpos Ordenados

Definición 2.1.1. *Sea K un cuerpo. Un* ***orden de*** *K es un subconjunto P de K que presenta las siguientes propiedades:*

O1. Dado $x \in K$, se tiene que $x \in P$, o $x = 0$, o $-x \in P$, y estas tres posibilidades son mutuamente exclusivas. En otras palabras, K es la unión disjunta de P,$\{0\}$ y $-P$.

O2. Si $x, y \in K$, entonces $x + y \in P$ y $xy \in P$.

Decimos tambien que K ***es ordenado por*** *P, y llamamos a P como el* ***conjunto de elementos positivos****.*

Ejemplo 2.1.2. *Recordando a F el cuerpo de* ***funciones racionales****, es decir funciones de una variable que son expresadas como cociente de dos polinomios $p, q \in \mathbb{R}[X]$:*

$$f(x) = \frac{p(x)}{q(x)} = \frac{a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0}{x^n + b_{n-1}x^{n-1} + \cdots + b_0},$$

se puede tomar a q con coeficiente principal igual a 1.

Definamos el siguiente conjunto:

$$P = \{f(x) \in F \mid a_m > 0\},$$

veamos que define un orden en F:

O1. Dado $f \in F$ entonces $a_m > 0$ o $a_m = 0$ o $a_m < 0$, considerando el primer caso; $f \in P$, considerando el caso del medio; sabemos que si el coeficiente principal es 0

entonces el polinomio debe ser idénticamente nulo; por lo que $f = 0$*, considerando el ultimo caso, entonces* $-a_m > 0$*;* $-f \in P$*.*

O2. Dados $f = \frac{p}{q}, g = \frac{r}{s} \in P$*. Sabemos que* $fg = \frac{pr}{qs}$ *por lo que el coeficiente principal del numerador sera mayor a cero ya que sera el producto de los coeficientes principales de* p *y* q *y dichos coeficientes son mayores que cero, así* $fg \in P$*.*

Veamos la suma:

$$\frac{p(x)}{q(x)} + \frac{r(x)}{s(x)} = \frac{p(x)s(x) + q(x)r(x)}{q(x)s(x)}.$$

Recordando que podemos tomar a q *y* s *con coeficientes principales igual a* 1*, suponemos casos dependiendo de los grados:*

C.1: Si el $grado(p) + grado(s) > grado(q) + grado(r)$*. El coeficiente principal del numerador sera el coeficiente principal de* p *y es mayor a cero.*

C.2: Si el $grado(p) + grado(s) < grado(q) + grado(r)$*. El coeficiente principal del numerador sera el coeficiente principal de* r *y es mayor a cero.*

C.3: Si el $grado(p) + grado(s) = grado(q) + grado(r)$*. El coeficiente principal del numerador sera la suma de coeficientes principales de* p *y* r*, dicha suma es mayor a cero.*

En cualquier caso; $f + g \in P$*.*

Observación 2.1.3. *Probemos algunos resultados menores que se cumplen en un cuerpo ordenado. Asumamos que* K *es ordenado por un orden* P*.*

a) $1 \in P$*. Dado que* $1 \in K$ *y* $1 \neq 0$ *entonces* $1 \in P$ *o* $-1 \in P$*, suponiendo este ultimo; sabemos que* $1 = (-1)^2 = (-1)(-1) \in P$*.*

b) K *tiene característica* 0*. Dado que* K *es unión disjunta de* P*,* 0 *y* $-P$*, y* $1+1+\cdots+1 \in P$*, es decir, las sumas de la identidad multiplicativa nunca darán la identidad aditiva. Entonces,* ***todo cuerpo ordenado tiene característica cero****.*

c) Si $x \in P$ *con* $x \neq 0$ *entonces* $x^{-1} \in P$*. Dado que* $x \neq 0$ *así* $x^{-1} \in P$ *o* $-x^{-1} \in P$*, suponiendo lo ultimo;* $(x)(-x^{-1}) = -1 \in P$*, lo cual llevaría a una contradicción, así solamente* $x^{-1} \in P$*.*

Definido un orden P en un cuerpo K, podemos usar las notaciones usuales de desigualdades; sean $x, y \in K$:

$$x < y \text{ (o } y > x) \iff y - x \in P$$

Si $x < 0$, decimos que x **es negativo**, lo cual implica que $-x$ es positivo.

Observación 2.1.4. *Podemos verificar que se cumplen algunas relaciones de desigualdades:*

a) $x < y \wedge y < z$ *entonces* $x < z$. *Tenemos que* $y - x \in P$ *y* $y - z \in P$ *por lo que* $z - x = (y - x) + (y - z) \in P$.

b) $x < y \wedge z > 0$ *entonces* $xz < yz$. *Tenemos que* $y - x \in P$ *y* $z \in P$ *por lo que* $yz - xz = (y - x)z \in P$.

c) $x < y \wedge z > 0$ *entonces* $x < y + z$. *Tenemos que* $y - x \in P$ *y* $z \in P$ *por lo que* $y - x + z = (y + z) - x \in P$.

d) $x < y \wedge x, y > 0$ *entonces* $1/y < 1/x$. *Teniendo en cuenta que* $1/x = x^{-1} \in P$, $1/y = y^{-1} \in P$ *(por observaciones anteriores) y sabemos que* $y - x \in P$, *así que* $1/x - 1/y = x^{-1} - y^{-1} = y^{-1}x^{-1}(y - x) \in P$.

e) $x > 1$ *entonces* $x^{-1} < 1$. *Se desprende de b); dado que* $1, x^{-1} > 0$. *De igual manera se puede demostrar que* $x^n > 1$, *para todo* $n \in \mathbb{N}$, *ya que* $x^2 = (x)(x) > x > 1$ *y así inductivamente.*

Observación 2.1.5. *Recordando la definición de orden en un conjunto; sea un conjunto* S, *un* ***orden (u orden parcial)*** *de* S *es una relación* R *sobre los pares de elementos de* S, *cumpliendo las siguientes propiedades; dados* $x, y, z \in S$:

i) xRx.

ii) Si xRy *y* yRx *entonces* $x = y$.

iii) Si xRy *y* yRz *entonces* xRz.

Se dice que R *es* ***orden total*** *en* S *si se cumple una cuarta propiedad:*

iv) Dado cualquier par $x, y \in S$; *se debe cumplir que* xRy *o* yRx.

Observamos que bajo la definición de orden en un cuerpo, se puede establecer un orden total en dicho cuerpo considerando " $\leq$ "; dados $x, y \in K$, decimos que

$$x \leq y \iff x < y \vee x = y,$$

verifiquemos la propiedades:

i) $x \leq x$, *ya que* $x = x$

ii) Si $x \leq y$ *y* $y \leq x$ *entonces* $x = y$. *Suponiendo que* $x \neq y$, *entonces tendríamos que* $y - x \in P$ *y* $x - y \in P$, *así* $(y - x) + (x - y) = 0 \in P$, *lo cual es una contradicción.*

iii) Si $x \leq y$ *y* $y \leq z$ *entonces* $x \leq z$. *Si se cumple al menos una igualdad, es directo. Supongamos que no se cumple ninguna igualdad, por lo que,* $y - x \in P$ *y* $z - y \in P$, *así* $(y - x) + (z - y) = z - x \in P$ *entonces* $x < z$.

iv) Dados $x, y \in K$, *así* $y - x \in K$ *por lo que* $y - x \in P$ *o* $y - x = 0$ *o* $-(y - x) = x - y \in P$, *es decir,* $x < y$ *o* $y = x$ *o* $y < x$, *lo cual también se puede escribir como* $x \leq y$ *o* $y \leq x$.

Observación 2.1.6. *Veamos algunos resultados sobre cuadrados en un cuerpo ordenado:*

a) Si $x \in K$ *y* $x \neq 0$ *entonces* $x^2 \in P$. *Se tiene que* $x \in P$ *o* $-x \in P$, *en cualquiera de los casos* $x^2 = (x)(x) = (-x)(-x) \in P$.

b) La suma de cuadrados en K *es positiva o es* 0. *Sean* $a \neq 0$, $b \neq 0 \in K$ *y supongamos que* $-(a^2 + b^2) \in P$, *así* $a^2 + b^2 - (a^2 + b^2) = 0 \in P$, *lo cual es una contradicción, se puede demostrar de la misma manera para el caso de mas de dos elementos de* K, *por lo que solo tendríamos las dos primeras opciones.*

Veamos algunos resultados sobre cuadrados en un cuerpo cualquiera, sea E *un cuerpo:*

c) El producto de sumas de cuadrados en E *es una suma de cuadrados. Sean* $a, b, c, d \in E$ *entonces* $(a^2 + b^2)(c^2 + d^2) = (ac)^2 + (ad)^2 + (bc)^2 + (bd)^2$, *para sumas con mas de dos sumandos, se puede proceder por inducción.*

d) Si $a, b \in E$ *son sumas de cuadrados y* $b \in 0$ *entonces* $a \backslash b$ *es una suma de cuadrados. Sabemos que* $a \backslash b = ab^{-1} = ab(b^{-1})^2$, *por lo queda probado por c).*

Observación 2.1.7. *Definamos el* ***valor absoluto****, sea K un cuerpo ordenado; dado $x \in K$:*

$$|x| = \begin{cases} x & , \quad x \geq 0 \\ -x & , \quad x < 0 \end{cases}$$

Podemos probar los siguientes resultados:

a) Para todo $x \in K$; $|x| \geq 0$. Si $x \geq 0$; $|x| = x \geq 0$, si $x < 0$; $|x| = -x > 0$.

b) Para todo $x \in K$; $|x| = |-x|$. Si $x \geq 0$ entonces $-x \leq 0$; $|x| = x = -(-x) = |-x|$, si $x < 0$ entonces $-x > 0$; $|x| = -x = |-x|$.

c) Dados $x, y \in K$; $|x| \leq y$ entonces $-y \leq x \leq y$. Por a) $y \geq 0$, entonces si $x \geq 0$; $-y \leq 0 \leq x \leq y$, si $x < 0$; $|x| = -x \leq y$ entonces $-y \leq x < 0 \leq y$.

d) Dados $x, y \in K$; $|x| \leq y$ entonces $-y \leq x \leq y$. Por a) $y \geq 0$, entonces si $x \geq 0$; $-y \leq 0 \leq x \leq y$, si $x < 0$; $|x| = -x \leq y$ entonces $-y \leq x < 0 \leq y$.

e) Dados $x, y \in K$; $|xy| = |x||y|$. Si $x, y \geq 0 \vee x, y \leq 0$ entonces $xy \geq 0$; $|xy| = xy = (-x)(-y) = |x||y|$. Si $x \geq 0$ y $y \leq 0$ entonces $xy \leq 0$; $|xy| = -xy = x(-y) = |x||y|$, de manera similar se demuestra si $y \geq 0$ y $x \leq 0$.

f) Dados $x, y \in K$; $|x+y| \leq |x|+|y|$. Si $x, y \geq 0$ entonces $x+y \geq 0$; $|x+y| = x+y = |x| + |y|$. Si $x, y \leq 0$ entonces $x + y \leq 0$; $|x + y| = -x - y = |x| + |y|$. Si $x \geq 0$ y $y \leq 0$ entonces $-x \leq 0$ y $-y \geq 0$, si $x+y \leq 0$; $|x+y| = -x-y \leq x-y = |x|+|y|$, si $x + y \geq 0$; $|x+y| = x+y \leq x-y = |x|+|y|$, de manera similar se demuestra si $y \geq 0$ y $x \leq 0$.

Proposición 2.1.8. *Sea K un cuerpo, P y Q dos ordenes en K. Si $P \subset Q$ entonces $P = Q$.*

Demostración. Verifiquemos que $Q \subset P$; sea $q \neq 0 \in Q \subset K$ entonces $q \in P$ o $q \in -P$, suponiendo lo ultimo; existe $p \in P$ tal que $q = -p$ entonces $-q = p \in P \subset Q$, así $q + (-q) = 0 \in Q$, lo cual es contradicción, por lo que $q \in P$. □

Ejemplo 2.1.9. *Sea $\mathbb{Q}$ el conjunto de los números racionales, entonces $\mathbb{Q}$ solo tiene un orden dado por $P = \{\alpha \in \mathbb{Q} \,|\, \alpha > 0$ en el sentido usual$\}$. Supongamos que existe $\bar{P}$ orden en $\mathbb{Q}$, verifiquemos que $P \subset \bar{P}$; sea $p \in P$ así $p = \dfrac{a}{b} > 0$ con $a, b > 0$, por lo que*

$ab > 0$, utilizando el teorema de Lagrange (ver [4]); podemos escribir ab como la suma de de cuadrados de cuatro enteros, es decir, existen $c, d, e, f \in \mathbb{Z}$ tal que

$$ab = c^2 + d^2 + e^2 + f^2$$
$$\rightarrow p = \frac{a}{b} = \left(\frac{c}{b}\right)^2 + \left(\frac{d}{b}\right)^2 + \left(\frac{e}{b}\right)^2 + \left(\frac{f}{b}\right)^2,$$

como los cuadrados de $\mathbb{Q}$ están en $\bar{P}$ entonces por p ser suma de cuadrados de dichos elementos, $p \in \bar{P}$, por la observación $P = \bar{P}$.

Definición 2.1.10. *Dado K un cuerpo con orden P, y $F \subset K$ es un subcuerpo (cuerpo dentro de K), entonces $P \cap F$ define un orden de F, el cual es llamado* ***orden inducido****.*

2.2. Cuerpos Reales

Definición 2.2.1. *Sea K un cuerpo:*

- *K es llamado* ***real*** *si -1* ***no es una suma de cuadrados en*** *K.*
- *K es llamado* ***real cerrado*** *si* ***es real y cualquier extension algebraica de K, que sea real, debe ser el mismo K****. En otras palabras, K es maximal con respecto a la propiedad de realidad en una cerradura algebraica.*

Observación 2.2.2. *Vemos que todo cuerpo K ordenado es real, ya que la suma de cuadrados es 0 o positiva, así nunca podrá ser igual a -1.*

Proposición 2.2.3. *Sea K un cuerpo real:*

i. Dado $a \in K$, si $K(\sqrt{a})$ no es real, entonces $-a$ es una suma de cuadrados en K.

ii. Dado $a \in K$, una suma de cuadrados en K entonces $K(\sqrt{a})$ es real.

iii. Dado $a \in K$, entonces $K(\sqrt{a})$ o $K(\sqrt{-a})$ es real.

iv. Sea $f \in K[X]$ un polinomio irreductible de grado impar n y α es una raíz de f, entonces $K(\alpha)$ es real.

Demostración. i. Vemos que $\sqrt{a} \notin K$; en caso contrario $K = K(\sqrt{a})$ no es real; contradicción, así aplicando la proposición 1.2.7; $K(\sqrt{a}) = \{b + c\sqrt{a} | b, c \in K\}$.

Entonces, como $K(\sqrt{a})$ no es real; existen $b_i, c_i \in K$ tal que

$$-1 = \sum (b_i + c_i\sqrt{a})^2 = \sum b_i^2 + 2\sqrt{a}\sum b_i c_i + a\sum c_i^2$$
$$\rightarrow \sqrt{a}\left(2\sum b_i c_i\right) = -1 - \sum b_i^2 - a\sum c_i^2$$

si $\sum b_i c_i \neq 0$ entonces tiene inversa, por lo que $\sqrt{a} \in K$, por lo tanto $K(\sqrt{a}) \subset K$, así $K(\sqrt{a}) = K$ real, lo cual es contradicción, por lo que $\sum b_i c_i = 0$, así

$$-1 = \sum b_i^2 + a\sum c_i^2 \tag{2.1}$$

$$\rightarrow -a = \frac{1 + \sum b_i^2}{\sum c_i^2} \tag{2.2}$$

así $-a$ es un cociente de sumas de cuadrados lo cual, por la observación 2.1.6 ; es una suma de cuadrados en K.

ii. Suponiendo que $K(\sqrt{a})$ no es real; como en (2.1), existen $b_i, c_i \in K$ tal que

$$-1 = \sum b_i^2 + a\sum c_i^2$$

como a es suma de cuadrados en K entonces -1 , escrito como suma de cuadrados mas un producto de sumas de cuadrados, es suma de cuadrados en K, lo cual es contradicción con K ser real.

iii. Si suponemos que $K(\sqrt{a})$ no es real y $K(\sqrt{-a})$ no es real, como en (2.1) y (2.2), tenemos que existen $b_i, c_i, d_i, e_i \in K$tal que

$$-a = \frac{1 + \sum b_i^2}{\sum c_i^2}$$

y

$$-1 = \sum d_i^2 - a\sum e_i^2$$

Entonces reemplazando el primero en el segundo llegaríamos a que -1 es suma de cuadrados en K, lo cual es contradicción por K ser real.

iv. Suponiendo que $K(\alpha)$ no es real, por proposición 1.2.7; existen polinomios $g_i \in K[X]$ de grado $\leq n-1$ tal que

$$-1 = \sum (g_i(\alpha))^2$$
$$\rightarrow -1 - \sum (g_i(\alpha))^2 = 0$$

así α es una raíz de dicho nuevo polinomio y como f es irreductible, existe $h \in K[X]$ tal que

$$-1 - \sum g_i(X)^2 = h(X)f(X) \tag{2.3}$$

$$\rightarrow -1 = -\sum g_i(X)^2 + h(X)f(X) \tag{2.4}$$

La suma de $g_i^2(X)$ debe tener grado par diferente de 0 ya que si es 0; -1 es suma de cuadrados en K real, este grado debe ser menor o igual a $2n-2$. Ya que f tiene grado impar n, por (2.3) sigue que el grado de h debe ser impar y menor o igual a $n-2$. Sea β raíz h entonces evaluando en (2.4), -1 se escribe como suma de cuadrados, por lo que $K(\beta)$ no es real. Ya que grado de h es menor al grado de f, la prueba es terminada por inducción, para aplicarla volvemos al comienzo sin ninguna suposición:

- n=1: $f(x) = x - \alpha \in K[X]$ por lo que $\alpha \in K$, así $K(\alpha) = K$ real.
- n=2k+1: Suponemos que este caso se cumple para polinomios irreductibles de grado impar hasta $2k+1$ con $k \geq 0$.
- n=2(k+1)+1: Si suponemos que dado α, una raíz de f, tal que $K(\alpha)$ no es real; llegamos a que existe $h \in K[X]$ con grado impar menor o igual a $n-2 = 2(k+1)+1-2 = 2k+1$, si suponemos que h es irreductible y tomamos una raíz β entonces llegamos a que $K(\beta)$ no es real; lo cual contradice la hipótesis inductiva, si h es reductible, tiene un factor irreductible h_1 con grado impar (ya que h tiene grado impar) menor a $2k+1$, y de igual manera llegamos a una contradicción.

□

Definición 2.2.4. *Sea K un cuerpo real. Llamamos como **cerradura real de** K a un cuerpo L si es real cerrado y extension algebraica de K.*

Teorema 2.2.5. *Sea K un cuerpo real. Entonces existe una cerradura real de K. Si R es real cerrado,entonces R tiene un único orden. Los elementos positivos son los cuadrados de R. Cada elemento positivo es un cuadrado, y cada polinomio de grado impar es $R[X]$ tiene una raíz en R. Se tiene que $R^a = R(\sqrt{-1})$.*

Demostración. Vamos a dividir la demostración por partes:

- **Existencia de la cerradura real.** Sabiendo que toda extension algébraica E de K; $E \subset K^a$ cerradura algebraica de K, definimos

$$S = \{E \text{ extension algebraica y real de } K\}$$

Ahora verifiquemos las condiciones necesarias para utilizar el lema de Zorn:

i) $S \neq \emptyset$, ya que $K \in S$.

ii) La inclusión ($\subseteq$) define un orden en S. Dado que

- Para todo $E \in S$; $E \subseteq E$.
- Si $E \subseteq F$ y $F \subseteq G$ entonces $E \subseteq G$.
- Si $E \subseteq F$ y $F \subseteq E$ entonces $E = F$.

iii) S es inductivamente ordenado. Sea $T \subset S$ totalmente ordenado, definimos

$$M = \cup_{E \in T} E$$

es una cota superior de T. Probemos, $E \subseteq M$ para todo $E \in T$, M es una extension algebraica de K, falta probar que es real; supongamos que no lo sea, entonces existen $n \in \mathbb{Z}$ y $a_i \in M, \forall i = 1 : n$ tal que

$$-1 = \sum a_i^2,$$

sabemos que existen $E_i \in S$ tal que $a_i \in E_i$ y como T es totalmente ordenado, podemos suponer que $E_i \subseteq E_{i+1}, \forall i = 1 : n-1$, así $a_i \in E_n, \forall i$ y por la igualdad anterior tendríamos que E_n no es real, lo cual es una contradicción.

Por lema de Zorn, existe un elemento maximal de S, el cual es una extension algebraica y real de K y por ser maximal es real cerrado.

- **Existencia y unicidad del orden.** Ahora sea R un cuerpo real cerrado, definamos como P el conjunto de elementos diferentes de cero de R tales que son sumas de cuadrados. Probemos que P es un orden:

O1. Dado $a \in R$ real, con $a \neq 0$, por la Proposición 1.2.1 iii;

$$R(\sqrt{a}) \text{ es real } \vee \ R(\sqrt{-a}) \text{ es real}$$

y como R es cerrado

$$\sqrt{a} \in R(\sqrt{a}) = R \vee \sqrt{-a} \in R(\sqrt{-a}) = R$$

asi

$$a = (\sqrt{a})^2 \in P \vee -a = (\sqrt{-a})^2 \in P$$

De esto también se desprende que todo elementos positivo es un cuadrado; dado $a \in P$; $\sqrt{a} \in R(\sqrt{a}) = R$ así $a = (\sqrt{a})^2 \in P$.

O2. Por la observación 2.1.6, se puede verificar que la suma y producto de sumas de cuadrados, son sumas de cuadrados.

El orden definido es único; supongamos que existe un orden Q de R, debemos demostrar que $P = Q$:

$\subseteq$: Sea $p \in P$, entonces existe $a \in R$ tal que $p = a^2$, si $a \neq 0$, entonces $a \in Q$ o $-a \in Q$ así $p = (a)(a) = (-a)(-a) = a^2 \in Q$

$\supseteq$: Sea $q \in Q$, entonces $q \in P$ o $-q \in P$, si suponemos lo ultimo entonces existe $a \in P$ tal que $-q = a^2$ así $(-a)(a) = q \in Q$, si suponemos que $a \in Q$ entonces $-a \in Q$, lo cual es contradicción, lo mismo sucede si $-a \in Q$, por lo que $q \in P$.

- **Existencia de una raíz en** R**.** Sea f un polinomio de grado impar en $R[X]$. Si suponemos que es irreductible, dada una raíz α; $R(\alpha) = R$ por proposición 2.2.3 y dado que R es real cerrado, así $\alpha \in R$. Si f es reductible, podemos encontrar un factor $h \in R[X]$ irreductible de grado impar (ya que f tiene grado impar), tomamos una raíz β de h, la cual también seria raíz de f y procedemos como en el caso anterior con h, así $\beta \in R$.

- $R^a = R(\sqrt{-1})$. Bajo las propiedades ya demostradas de R; ser un cuerpo ordenado, los positivos ser cuadrados y que todo polinomio de grado impar tiene una raíz en R, siguiendo el ejemplo 5 de la sección 2 del capitulo 6 de [3]; se demuestra que $R(\sqrt{-1})$ es algebraicamente cerrado, por lo tanto $R(\sqrt{-1}) = R^a$.

□

Corolario 2.2.6. *Sea K un cuerpo real y dado $a \in K$, tal que no es una suma de cuadrados, entonces existe un orden en K tal que a es negativo.*

Demostración. Afirmamos que $K(\sqrt{-a})$ es real, si no fuese real; por la proposición 1.2.1.; $a = -(-a)$ es una suma de cuadrados. Aplicando el teorema 2.2.5, existe un orden (como fue definido en el teorema 2.2.5) en $K(\sqrt{-a})$, así $-a = (\sqrt{-a})^2 > 0$, por lo que a es negativo. □

Proposición 2.2.7. *Sea R un cuerpo tal que $R \neq R^a$ pero $R^a = R(\sqrt{-1})$, entonces R es real y por lo tanto real cerrado.*

Demostración. Primero demostremos que se puede definir un orden en R, sea P el conjunto de cuadrados diferentes de cero en R.

O1. Dado $a \in R$ real, con $a \neq 0$, entonces $a \in P$ o $a \notin P$; supongamos lo ultimo, sea α raíz de $x^2 - a = 0$, entonces $\alpha \in R(\alpha) = R(\sqrt{-1})$ ya que $R(\alpha) \subset R^a = R(\sqrt{-1})$ y los dos tienen dimension 2, ya que α y $\sqrt{-1}$ son raíces de polinomios irreductibles de grado 2 en R (proposición 1.2.7) , así existen $c, d \in R$ tal que

$$\alpha = c + d\sqrt{-1}$$
$$\rightarrow \alpha^2 = (c^2 - d^2)(1) + (2cd)(\sqrt{-1}),$$

como $1, \sqrt{-1}$ son linealmente independiente sobre R; $cd = 0$, si $d = 0$ entonces $\alpha \in R$ contradicción, por lo que $c = 0$:

$$\alpha^2 = -d^2$$
$$\rightarrow -a = d^2 \in P$$

O2. Sabemos que el producto de cuadrados es un cuadrado por lo que resta probar que la suma de cuadrados es un cuadrado. Sean $a, b \in R$ y escribiendo a $\sqrt{-1} = i$, tomamos en cuenta $x^2 - (a + bi) \in R(i)[X]$ existen $c, d \in R$ tal que $c + di$ es una raíz, ya que $R(i)$ es algebraicamente cerrado. Así

$$a + bi = (c + di)^2 = (c^2 - d^2) + 2cdi$$
$$\rightarrow a = c^2 - d^2 \wedge b = 2cd,$$

así

$$\begin{aligned} a^2 + b^2 &= (c^2 - d^2)^2 + (2cd)^2 \\ &= c^4 + d^4 - 2c^2d^2 + 4c^2d^2 \\ &= (c^2 + d^2)^2 \end{aligned}$$

Ahora supongamos que R no es real, entonces existen $a_i \in R$ tal que

$$-1 = \sum a_i^2,$$

sabemos que por Ord. 2, existe $a \in R$ tal que $\sum a_i^2 = a^2 = -1$ por lo que $a = \sqrt{-1} \in R$ lo que lleva a $R = R(\sqrt{-1}) = R^a$ contradicción. □

Teorema 2.2.8. *Sea R un cuerpo real cerrado, y $f(x)$ un polinomio en $R[X]$. Dados $a, b \in R$ y asuma que $f(a) < 0$ y $f(b) > 0$. Entonces existe c entre a y b tal que $f(c) = 0$.*

Demostración. Probemos primero que todo polinomio irreductible en $R[X]$, solo puede tener grado 1 o 2. Sea f irreductible con grado n, tomemos α raíz de f; así $R(\alpha)$ el cual tiene dimension n (como espacio vectorial sobre R) es una extension algebraica de R, por lo que $R(\alpha) \subset R^a = R(\sqrt{-1})$ **ya que $R(\sqrt{-1})$ es algebraicamente cerrado**, así $n \leq 2 =$ dimension de $R(\sqrt{-1})$ (ya que $\sqrt{-1}$ es raíz de un polinomio cuadrático de $R[X]$).

Dado $f \in R[X]$, lo podemos escribir como producto de factores irreductibles de grado 1 y 2, es decir

$$f(x) = \prod_i g_i(x)$$

donde

$$g_i(x) = x - \theta_i \text{ o } g_i(x) = x^2 - \alpha_i x + \beta_i^2 \text{ donde } \theta_i, \beta_i, \alpha_i \in R$$

supongamos que $x^2 + \alpha x + \beta^2$ es un factor cuadrático irreductible entonces

$$x^2 + \alpha x + \beta^2 = (x + \tfrac{\alpha}{2})^2 + (\beta - \tfrac{\alpha^2}{4}),$$

se debe cumplir que $\beta > \frac{\alpha^2}{4}$, en caso contrario el factor seria una diferencia de cuadrados y se podría factorizar, así vemos que los factores cuadráticos siempre serán positivos. Ahora, solo consideremos al producto de factores lineales:

$$\prod_i (x - \theta_i) \text{ donde } \theta_i \text{ son raíces de } f,$$

el signo de f dependerá del signo dicho producto. Supongamos que $a < b$; si

$$\forall \theta_i : \theta_i < a \vee b < \theta_i$$

$$\to \forall \theta_i : (0 < a - \theta_i \wedge 0 < b - \theta_i) \vee (b - \alpha_i < 0 \wedge a - \theta_i < 0)$$

así, suponiendo que existen $\theta_j < a$ y $b < \theta_k$, podemos separar el producto en dos factores; uno negativo y otro positivo:

$$\prod_i (a - \theta_i) = (factor+)(factor-) < 0$$

$$\rightarrow f(a) < 0$$

pero

$$\prod_i (b - \theta_i) = (factor+)(factor-) < 0$$

$$\rightarrow f(b) < 0 \,(\text{contradicción})$$

De manera similar llegaríamos a una contradicción en el caso que todos los $\theta_i < a$ o todos los $\theta_i > b$. Así existe $c = \theta \in R$ raíz de f tal que $a < c < b$. □

Lema 2.2.9. *Sea K un subcuerpo de un cuerpo ordenado E y $\alpha \in E$ algebraico sobre K, raíz del polinomio*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

con coeficientes en K, entonces $|\alpha| \leq 1 + |a_{n-1}| + \cdots + |a_0|$.

Demostración. Si $|\alpha| \leq 1$, la demostración es inmediata. Si $|\alpha| > 1$, entonces

$$|\alpha|^{-1} < 1 \rightarrow |\alpha|^{-i} < 1, \forall i \geq 1.$$

Como α es raíz de f, entonces:

$$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + a_0 = 0$$

$$\rightarrow -\alpha^n = a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + a_0$$

$$\rightarrow |\alpha|^n = |-\alpha^n| = |a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + a_0|$$

$$\rightarrow |\alpha|^n \leq |a_{n-1}||\alpha|^{n-1} + |a_{n-2}||\alpha|^{n-2} + \cdots + |a_0|$$

dividiendo entre $|\alpha|^{n-1} \neq 0$ y como $|\alpha|^{-i} < 1$, $\forall i \geq 1$:

$$\rightarrow |\alpha| \leq |a_{n-1}| + |a_{n-2}||\alpha|^{-1} + \cdots + |a_0||\alpha|^{-(n-1)}$$

$$\rightarrow |\alpha| < 1 + |a_{n-1}| + |a_{n-2}| + \cdots + |a_0|$$

□

Definición 2.2.10. ***(Sucesión de Sturm)***

- *Sea f un polinomio con coeficientes en un cuerpo R real cerrado ($f \in R[X]$), y asuma que f no tiene raíces múltiples (en su cerradura algebraica). Sea $u < v$ elementos de R. Definimos como una* ***sucesión de Sturm*** *de f sobre un intervalo $[u, v]$ a una sucesión de polinomios*

$$S = \{f = f_0, f' = f_1, f_2, \cdots, f_m\}$$

con las siguientes propiedades:

ST_1. *El ultimo polinomio f_m es una constante diferente de cero.*

ST_2. *No existe $x \in [u, v]$ tal que $f_j(x) = f_{j+1}(x) = 0$ para cualquier $0 \leq j \leq m-1$.*

ST_3. *Si $x \in [u, v]$ y $f_j(x) = 0$ para algún $j = 1, \cdots, m-1$, entonces $f_{j-1}(x)$ y $f_{j+1}(x)$ tienen signos opuestos.*

ST_4. *Se debe cumplir que $f_j(u) \neq 0$ y $f_j(v) \neq 0$ para todo $j = 0, \cdots, m$.*

- *Para cualquier $x \in [u, v]$, que no es una raíz de cualquier f_j, denotamos por $W_S(x)$ el numero de cambios de signo en la sucesión*

$$S = \{f(x), f_1(x), \cdots, f_m(x)\},$$

y llamamos a $W_S(x)$ como ***variacíon de signos en la sucesión****.*

Teorema 2.2.11. ***Teorema de Sturm.*** *El numero de raíces de f entre u y v es igual a $W_S(u) - W_S(v)$ para cualquier S, sucesión de Sturm .*

Demostración. Tomando en cuenta las raíces de los polinomios f_j en $[u, v]$ ($j = 0, \cdots, m-1$); las ordenamos $\alpha_1 < \alpha_2 < \cdots < \alpha_r$, se prueba que $W_S(x)$ es constante en los intervalos abiertos entre raíces, supongamos que no lo sea; entonces existen $x, y \in (\alpha_i, \alpha_{i+1})$, tal que $W_S(x) < W_S(y)$, así existe j_0 tal que

$$f_j(x) > 0, \forall j \leq j_0 \ \vee \ \ f_j(x) < 0, \forall j \leq j_0$$

Tomando el primer caso y suponemos que $f_{j_0}(y) > 0$, dado que $W_S(x) < W_S(y)$, existe j_1 tal que $f_{j_0+j_1}(y) < 0$ y $f_{j_0+j_1}(x) > 0$, así por teorema 2.2.8; existe una raíz de $f_{j_0+j_1}$ entre x y y, lo cual es contradicción. De manera similar llegaríamos a una contradicción

si suponemos que $f_{j_0}(y) < 0$ o, $f_j(x) < 0, \forall j \leq j_0$ con cualquier signo de $f_{j_0}(y)$.

Dado el resultado anterior, sera suficiente probar que si existe solo un elemento α tal que $u < \alpha < v$:

$$W_S(u) - W_S(v) = \begin{cases} 0 & \text{si } \alpha \text{ es raiz de algun } f_j \text{ con } j > 0 \\ \\ 1 & \text{si } \alpha \text{ es raiz de } f_0 = f \end{cases}$$

a) Supongamos que α es raíz de algún f_j, para $1 \leq j \leq m-1$. Por ST 3.; $f_{j-1}(\alpha), f_{j+1}(\alpha)$ tienen signos opuestos, veamos que estos signos no cambian al reemplazar α por u o v. Suponiendo lo contrario; $Signo(f_{j-1}(\alpha)) \neq Signo(f_{j-1}(u))$, por teorema 2.2.8; existe una raíz entre u y α, lo cual es contradicción, lo mismo sucede con v, por lo tanto $Signo(f_{j-1}(u)) = Signo(f_{j-1}(v))$ y $Signo(f_{j+1}(u)) = Signo(f_{j+1}(v))$. Así considerando la variación de signos en

$$\{f_{j-1}(u), f_j(u), f_{j+1}(u)\} \text{ y } \{f_{j-1}(v), f_j(v), f_{j+1}(v)\},$$

verificamos que es la misma en ambas. Si α fuese raíz de otro f_{j_1}, con $j_1 \neq j$ (diferente a $j-1$ y $j+1$), se daría lo mismo que en el caso anterior. Para un f_{j_2} que no tiene como raíz a α, vemos que $Signo(f_{j_2}(u)) = Signo(f_{j_2}(v))$ ya que en caso contrario existiría una raíz de f_{j_2} entre u y v, lo cual no puede darse ya que α es la única raíz de los $\{f_j\}_j$. Por lo tanto, la variación de signos en las sucesiones $\{f_i(u)\}_{i=0:m}$ y $\{f_i(v)\}_{i=0:m}$ es la misma, así se concluye que

$$W_S(u) = W_S(v)$$
$$\rightarrow W_S(u) - W_S(v) = 0$$

b) Supongamos que α es raíz de $f = f_0$. Probemos que $f(u)$ y $f(v)$ tienen diferente signo; dado que sabemos que existe $g \in R[X]$ tal que

$$f(x) = (x - \alpha)g(x),$$

así $g(u)$ y $g(v)$ tienen igual signo, de lo contrario existiría una raíz de g entre u y v;

la cual seria también raíz de f diferente a α, lo cual es contradicción. Como

$$u < \alpha < v$$
$$\rightarrow (0 < \alpha - u) \wedge (\alpha - v < 0)$$
$$\rightarrow Signo(f(u)) \neq Signo(f(v))$$

De hecho, con la misma idea se muestra que $Signo(g(u)) = Signo(g(\alpha)) = Signo(g(v))$. Considerando la relación entre f y g; se puede verificar que $f(u)$ y $g(u)$ tienen signos diferentes. Consideremos:

$$f'(x) = ((x-\alpha)g(x))' = g(x) + (x-\alpha)g'(x)$$
$$\rightarrow f'(\alpha) = g(\alpha)$$

Ahora, por ST2; α no es raíz de $f_1 = f'$ entonces $Signo(f'(u)) = Signo(f'(\alpha)) = Signo(f'(v))$, en caso contrario, existiría una raíz ya sea entre u y α, α y v o u y v lo cual no se puede dar.

Tomando en cuenta todo lo anterior y analizando por casos, si $f(u)$ fuese positivo:

$$\begin{array}{lcl} f_0(u) = f(u)\ (+) & & (-)\quad g(u) \qquad f'(u) = f_1(u)\ (-) \\ f_0(\alpha) = f(\alpha) = 0 & \rightarrow & (-)\quad g(\alpha) \quad = \quad f'(\alpha) = f_1(\alpha)\ (-) \\ f_0(v) = f(v)\ (-) & & (-)\quad g(v) \qquad f'(v) = f_1(v)\ (-) \end{array}$$

En el caso que $f(u)$ fuese negativo:

$$\begin{array}{lcl} f_0(u) = f(u)\ (-) & & (+)\quad g(u) \qquad f'(u) = f_1(u)\ (+) \\ f_0(\alpha) = f(\alpha) = 0 & \rightarrow & (+)\quad g(\alpha) \quad = \quad f'(\alpha) = f_1(\alpha)\ (+) \\ f_0(v) = f(v)\ (+) & & (+)\quad g(v) \qquad f'(v) = f_1(v)\ (+) \end{array}$$

En cualquier caso la variación de signos en $\{f_0(u), f_1(u)\}$ es uno y en $\{f_0(v), f_1(v)\}$ es cero. Si α fuese o no raíz de un f_j $(j \geq 2)$, se cumpliría lo mismo que en el item a), por lo tanto la variación de signo en $\{f_i(u)\}_{i=0:m}$ siempre sera mayor por uno de

la variación de signos de $\{f_i(v)\}_{i=0:m}$, y se cumple

$$W_S(u) = W_S(v) + 1$$
$$\rightarrow W_S(u) - W_S(v) = 1$$

Así, como al inicio, se puede considerar a las raíces de los polinomios f_j en $[u, v]$ ($j = 0, \cdots, m-1$); las ordenamos $\alpha_1 < \alpha_2 < \cdots < \alpha_r$ y tomando valores w_i tales que $\alpha_i < w_i < \alpha_{i+1}$ con $i = 1 : r-1$ y w_i no es raíz para ningún f_j (podemos tomar $w_i = (\alpha_i + \alpha_{i+1})/2$), considerando $w_0 = u$ y $w_r = v$, así cada raíz estará en un tramo; $\alpha_i \in [w_{i-1}, w_i]$ y podemos aplicar los resultados encontrados a cada tramo obteniendo:

$$W_S(w_{i-1}) - W_S(w_i) = \begin{cases} 0 & \text{si } \alpha_i \text{ no es raiz de } f \\ & \\ 1 & \text{si } \alpha_i \text{ es raiz de } f \end{cases}, \ \forall i = 1 : r$$

Así

$$W_S(u) - W_S(v) = \sum_{i=1}^{r}(W_S(w_{i-1}) - W_S(w_i)) = \text{Numero de raices de } f \text{ en } [u, v]$$

□

Observación 2.2.12. *Para la construcción de una sucesión de Sturm para un polinomio sin raíces múltiples, se puede considerar el siguiente algoritmo:*

$$f = g_1 f' - f_2,$$
$$f_1 = g_2 f_2 - f_3,$$
$$\vdots$$
$$f_{m-2} = g_{m-1} f_{m-1} - f_m,$$

usando $f_0 = f$, $f_1 = f'$ y $f_i = -Res(f_{i-2}, f_{i-1}) = -$(Residuo de la división de f_{i-2} entre f_{i-1}) para $i = 2 : m$, el algoritmo para cuando $Res(f_{m-1}, f_m) = 0$ y $f_m \neq 0$. Verificando las condiciones para ser sucesión de Sturm, empezamos de la ultima:

ST_4. Ya que $\{f_i\}_{i=0:m}$ es una sucesión finita, las cantidad raíces de los polinomios es finita, por lo tanto deben existir $u, v \in R$ $(u < v)$ tal que $f_j(u) \neq 0$ y $f_j(v) \neq 0$ para todo $j = 0 : m$.

ST_3. *Suponiendo que existe* $x \in [u, v]$ *tal que* $f_j(x) = 0$ *para un* j*, considerando el algoritmo y evaluando en dicho* x*:*

$$f_{j-1} = g_j f_j - f_{j+1}$$
$$\rightarrow f_{j-1}(x) = g_j(x) f_j(x) - f_{j+1}(x)$$
$$\rightarrow f_{j-1}(x) = -f_{j+1}(x),$$

así, $f_{j-1}(x)$ *y* $f_{j+1}(x)$ *tienen signos opuestos.*

ST_2. *Primero probemos que* $f_0 = f$ *y* $f_1 = f'$ *no tienen raíces en común. Suponiendo que existe* $x_0 \in [u.v]$ *raíz de* f *y* f' *entonces*

$$f(x) = (x - x_0) q(x)$$
$$\rightarrow f'(x) = q(x) + (x - x_0) q'(x)$$
$$\rightarrow f'(x_0) = q(x_0) + (x_0 - x_0) q'(x_0) = 0$$
$$\rightarrow f'(x_0) = q(x_0) = 0$$

por lo que x_0 *seria raíz de* q*; lo significaría que* x_0 *es raíz múltiple de* f*, lo cual no se puede dar ya que* f *no tiene raícez múltiples. Ahora, si suponemos que* f_1 *y* f_2 *tienen una raíz* x_1 *en común; por el algoritmo:*

$$f_0 = g_1 f_1 - f_2$$
$$\rightarrow f_0(x_1) = g_1(x_1) f_1(x_1) - f_2(x_1) = g_1(x_1)(0) - 0$$
$$\rightarrow f_0(x_1) = 0,$$

entonces x_1 *también seria raíz de* f_0*, lo cual es contradicción. Podemos utilizar el mismo proceso para los demás* f_j *y* f_{j+1} *en la sucesión.*

ST_1. *Si suponemos que* f_m *no es contante. Primero vemos que el proceso termina si* $Res(f_{m-1}, f_m) = 0$ *y* $f_m \neq 0$*, por lo tanto:*

$$f_{m-1} = g_m f_m$$

Considerando el algoritmo y haciendo el reemplazo:

$$f_{m-2} = g_{m-1} f_{m-1} - f_m = g_{m-1} g_m f_m - f_m$$
$$\rightarrow f_{m-2} = (g_{m-1} g_m - 1) f_m,$$

es decir, f_m es factor de f_{m-2}, y así sucesivamente llegamos que f_m es factor de f_0 y f_1, por lo que existen $q, \bar{q}$ polinomios tal que

$$f_0 = f = qf_m \, y \;\; f_1 = f' = \bar{q}f_m,$$

entonces si f_m no es constante, tiene raíz en la cerradura algebraica; por lo que f_0 y f_1 tendrían una raíz en común, lo cual es contradicción.

Ejemplo 2.2.13. *Sea $f(x) = x^6 - 4x^3 + x - 2$ polinomio en $\mathbb{R}[X]$, hallemos la sucesión de Sturm asociada:*

- $f_0(x) = x^6 - 4x^3 + x - 2$.
- $f_1(x) = 6x^5 - 12x^2 + 1$.
- $f_2(x) = -Res(x^6 - 4x^3 + x - 2, 6x^5 - 12x^2 + 1) = 2x^3 - \frac{5}{6}x + 2$.
- $f_3(x) = -Res(6x^5 - 12x^2 + 1, 2x^3 - \frac{5}{6}x + 2) = 18x^2 - \frac{25}{24}x + \frac{3}{2}$.
- $f_4(x) = -Res(2x^3 - \frac{5}{6}x + 2, 18x^2 - \frac{25}{24}x + \frac{3}{2}) = \frac{92687}{93312}x - \frac{5159}{2592}$.
- $f_5(x) = -Res(18x^2 - \frac{25}{24}x + \frac{3}{2}, \frac{92687}{93312}x - \frac{5159}{2592}) = -\frac{12568084416}{175324081}$.

Se puede verificar que si $|x| \geq 2$, $|x|^6 > 4|x|^3 + |x| + |2|$, de lo cual se concluye que las raíces de f estarán en $(-2, 2)$. Procedemos a evaluar la sucesión en $x = -2$ y $x = 2$:

$f_0(-2)$	$f_1(-2)$	$f_2(-2)$	$f_3(-2)$	$f_4(-2)$	$f_5(-2)$
92	-239	$-12{,}33$	$75{,}58$	$-3{,}98$	$-71{,}68$

$f_0(2)$	$f_1(2)$	$f_2(2)$	$f_3(2)$	$f_4(2)$	$f_5(2)$
32	145	$16{,}33$	$71{,}42$	$-3{,}8 \cdot 10^{-3}$	$-71{,}68$

Así, tendremos que la cantidad de raíces de f en $(-2, 2)$ es $W_s(-2) - W_s(2) = 3 - 1 = 2$, graficando f se puede verificar que las raíces son aproximadamente $1{,}5625$ y $-0{,}8125$.

Corolario 2.2.14. *Sea K un cuerpo ordenado, f un polinomio irreducible de grado ≥ 1 sobre K. El numero de raíces de f en dos cerraduras reales de K, que inducen el orden en K, es el mismo.*

Demostración. Supongamos que $f(x) = x^n + a_{n-1}x^{n-1} + \cdots a_0$ $(a_i \in K)$ y sea α raíz de f; por lemma 2.2.9;

$$|\alpha| \leq 1 + |a_{n-1}| + \cdots + |a_0|$$
$$\rightarrow -(1 + |a_{n-1}| + \cdots + |a_0|) \leq \alpha \leq 1 + |a_{n-1}| + \cdots + |a_0|,$$

haciendo $u = -(1 + |a_{n-1}| + \cdots + |a_0|)$ y $v = 1 + |a_{n-1}| + \cdots + |a_0|$, todas las raíces f se encuentran en $[u, v]$ y como $u, v \in K \subset R$ cerrado real, por teorema 2.2.11, la cantidad de raíces de f en R es igual a $W_S(u) - W_S(v)$, de igual manera para R'. Observamos que para cualquier cerradura real de K que le induzca el orden se cumplirá lo anterior, ya que $W_S(u) - W_S(v)$ no depende de la extension sino de K y el orden en K. □

Teorema 2.2.15. *Sea K un cuerpo ordenado,y sean R, R' cerraduras reales de K, cuyos ordenes inducen el orden en K. Entonces existe un único isomorfismo $\sigma : R \rightarrow R'$ sobre K, y preserva el orden.*

Demostración. Dividamos la demostración por partes:

a) Demostremos primero que dada una subextension de la forma $E = K(\alpha)$ de R, donde $\alpha \in R$, existe un monomorfismo de E en R' sobre K. Sea $\alpha \in R$, consideramos $E = K(\alpha)$, y sea

$$p(x) = Irr(\alpha, K, x),$$

dado que $p(\alpha) = 0$, por corolario 2.2.13 , existe una raíz $\beta \in R'$ y $p(x) = Irr(\beta, K, x)$. Recordando que los elementos de $K(\alpha)$ son de la forma $f(\alpha)$ donde $f \in K[X]$, definimos

$$\sigma : K(\alpha) \longrightarrow R'$$
$$f(\alpha) \longmapsto f(\beta)$$

se puede verificar que es un homomorfismo, la buena definición y la inyectividad se pueden demostrar de manera similar; dados $f(\alpha), g(\alpha) \in K(\alpha)$ donde $f, g \in K[X]$, tal que:

$$\sigma(f(\alpha)) = \sigma(g(\alpha))$$
$$\rightarrow f(\beta) = g(\beta)$$
$$\rightarrow ((f - g)(\beta) = 0,$$

por lo que β es raíz de $(f-g)(x)$ así:

$$\begin{aligned} & p|_{f-g} \\ \rightarrow & (f-g)(\alpha)=0 \\ \rightarrow & f(\alpha)=g(\alpha), \end{aligned}$$

Por lo que σ es un monomorfismo y se cumple que $\sigma|_K = Id(K)$ y $\sigma(\alpha)=\beta$.

b) Sabiendo que la cantidad de raíces diferentes de p en R es la misma que en R', consideramos dichas raíces:

$$\alpha_1 < \cdots < \alpha_n \text{ ordenadas en } R \tag{2.5}$$

$$\beta_1 < \cdots < \beta_n \text{ ordenadas en } R' \tag{2.6}$$

Verifiquemos que existe un isomorfismo $\sigma : K(\alpha_1, \cdots, \alpha_n) \rightarrow K(\beta_1, \cdots, \beta_n)$ tal que $\sigma(\alpha_i)=\beta_i$, $\forall i = 1:n$ y que conserva el orden. Tomando en cuenta las desigualdades de las raíces en (2.5), sean $w_i \in R$ tales que

$$w_i^2 = \alpha_{i+1} - \alpha_i, \ \forall i = 1 : n-1,$$

y $E_1 = K(\alpha_1, \cdots, \alpha_n, w_1, \cdots, w_{n-1})$, dado que K es ordenado entonces tiene característica 0, w_i es algebraico sobre K dado que w_i^2 es diferencia de algebraicos para todo $i = 1 : n-1$ (α_i es algebraico sobre K para todo $i = 1 : n$ y se aplica la proposición 1.2.4) entonces E_1 es extension finita de K (proposición 1.2.9), aplicando el Teorema del Elemento Primitivo (teorema 1.2.16); E_1 se puede escribir como en a), por lo que existe un monomorfismo $\sigma_1 : E_1 \rightarrow R'$ tal que $\sigma_1|_K = Id(K)$, consideremos $\sigma = \sigma_1|_{K(\alpha_1,\cdots,\alpha_n)}$ y evaluamos

$$\begin{aligned} \sigma(\alpha_{i+1}) - \sigma(\alpha_i) &= \sigma_1(\alpha_{i+1}) - \sigma_1(\alpha_i) \\ &= \sigma_1(\alpha_{i+1} - \alpha_i) \\ &= \sigma_1(w_i^2) \\ &= (\sigma_1(w_i))^2, \ \forall i = 1 : n-1, \end{aligned}$$

por lo que

$$\sigma(\alpha_1) < \cdots < \sigma(\alpha_n) \quad \text{ordenadas en } R',$$

ademas como $p(\sigma(\alpha_i)) = \sigma(p(\alpha_i)) = \sigma(0) = 0$; $\sigma(\alpha_i)$ es raíz de f en R' y como solo hay n raíces en R', considerando las desigualdades en (2.5) y (2.6), se cumple que $\sigma(\alpha_i) = \beta_i$, $\forall i = 1 : n$.

Verifiquemos que conserva el orden, para esto sera suficiente demostrar que lleva cuadrados en cuadrados. Dado $y \in K(\alpha_1, \cdots, \alpha_n)$ (existen $h, g \in K[X_1, \cdots, X_n]$ tal que $y = h(\alpha_1, \cdots, \alpha_n)/g(\alpha_1, \cdots, \alpha_n))$ con $y > 0$ así, existe $w \in R$:

$$y = w^2, \tag{2.7}$$

considerando $E_2 = K(\alpha_1, \cdots, \alpha_n, w_1, \cdots, w_{n-1}, w)$, existe $\sigma_2 : E_1 \to R'$ monomorfismo y de la misma manera que se hizo con σ; $\sigma_2(\alpha_i) = \beta_i = \sigma(\alpha_i)$, $\forall i = 1 : n$, entonces

$$\begin{aligned}
\sigma(y) &= \sigma(h(\alpha_1, \cdots, \alpha_n)/g(\alpha_1, \cdots, \alpha_n)) \\
&= h(\sigma(\alpha_1), \cdots, \sigma(\alpha_n))/g(\sigma(\alpha_1), \cdots, \sigma(\alpha_n)) \\
&= h(\sigma_2(\alpha_1), \cdots, \sigma_2(\alpha_n))/g(\sigma_2(\alpha_1), \cdots, \sigma_2(\alpha_n)) \\
&= \sigma_2(h(\alpha_1, \cdots, \alpha_n)/g(\alpha_1, \cdots, \alpha_n)) = \sigma_2(y)
\end{aligned}$$

así en (2.7):

$$\sigma(y) = \sigma_2(y) = \sigma_2(w^2) = (\sigma_2(w))^2,$$

por lo que σ lleva cuadrados en cuadrados.

c) Considerando el conjunto

$$S = \{(E, \phi)/E \text{ extension algebraica de } K \text{ en } R \text{ y } \phi : E \to F \text{ monomorfismo que preserva el orden en } E \text{ tal que } \phi|_K = Id(K)\}$$

Ahora verifiquemos las condiciones necesarias para utilizar el lema de Zorn:

i) $S \neq \emptyset$, ya que (E_1, σ), definidos en b), pertenece a S.

ii) Definimos en en S:

$$(E,\phi) \leq (F,\sigma) \iff E \subseteq F \text{ y } \sigma|_E = \phi$$

- Para todo $(E,\phi) \in S$; $E \subseteq E$ y $\phi|_E = \phi$, entonces $(E,\phi) \leq (E,\phi)$.
- Si $(E,\phi) \leq (F,\sigma)$ y $(F,\sigma) \leq (G,\psi)$, entonces $E \subseteq F \subseteq G$ y $\psi|_E = \sigma|_E = \phi$, asi $(E,\phi) \leq (G,\psi)$.
- Si $(E,\phi) \leq (F,\sigma)$ y $(F,\sigma) \leq (E,\phi)$, entonces

$$E \subseteq F \subseteq E \to E = F$$

$$\phi|_E = \sigma \,\text{y}\, \sigma|_E = \phi \to \phi = \sigma.$$

asi $(E,\phi) = (F,\sigma)$.

iii) S es inductivamente ordenado. Sea $T \subset S$ totalmente ordenado, definimos

$$\bar{M} = \cup_{(E,\phi)\in T} E \text{ y } \bar{\sigma} : M \to R' \text{ tal que } \bar{\sigma}|_E = \phi,$$

se ve que $\bar{M}$, es extension algebraica de K en R y que $E \subset \bar{M}$ para todo E tal que $(E,\sigma) \in T$. Por su definición $\bar{\sigma}$ es un homomorfismo, veamos que también sea **inyectivo**, sean $w_1, w_2 \in \bar{M}$ tales que $\bar{\sigma}(w_1) = \bar{\sigma}(w_2)$, donde $w_1 \in E_1$ y $w_2 \in E_2$ tal que $(E_1,\phi_1),(E_2,\phi_2) \in T$ y podemos suponer que $(E_1,\phi_1) \leq (E_2,\phi_2)$, así $w_1, w_2 \in E_2$ y $\bar{\sigma}(w_1) = \phi_2(w_1) = \phi_2(w_2) = \bar{\sigma}(w_2)$, por la inyectividad de ϕ_2; $w_1 = w_2$. Veamos que $\bar{\sigma}$ **conserve el orden**, sea $y \in \bar{M}$ positivo, entonces existe $(E,\phi) \in T$ tal que $y \in E$ y $\bar{\sigma}|_E = \phi$ conserva el orden en E; por lo tanto $\bar{\sigma}(y) = \phi(y)$ es positivo. Así $(\bar{M},\bar{\sigma}) \in S$ es una **cota superior de** T .

Por lema de Zorn, existe un elemento maximal de S; (M,σ), es decir, existe $\sigma : M \to R'$ monomorfismo que preserva el orden en M y $\sigma|_K = Id(K)$. Ahora, verifiquemos:

- $M = R$, esta demostración sera parecida a los items a) y b) por lo cual también lo dividiremos en partes pero primero; suponiendo lo contrario, existe $w \in R$ tal $w \notin M$:

  I) Sea $f(x) = \sum a_i x^i \in M[X]$, así denotamos $f^\sigma(x) = \sum \sigma(a_i)x^i \in \sigma(M)[X]$, y consideramos $q = Irr(w,M,X)$ y tomamos una raíz v de q^σ en R', recordando que los elementos de $M(w)$ son de la forma $f(w)$ con $f \in M[X]$,

definimos

$$\psi : M(w) \longrightarrow \sigma(M)(v) \subset R'$$
$$f(w) \longmapsto f^{\sigma}(v)$$

se puede verificar que ψ es un homomorfismo, dado que σ es homomorfismo. Veamos que este **bien definido**; sean $g, f \in M[X]$ tales que $f(w) = g(w)$, así $(f-g)(w) = 0$ entonces $q|_{f-g}$, por lo que existe $h \in M[X]$ y tomando en cuenta que σ es homomorfismo:

$$f - g = qh$$
$$\rightarrow f - g - qh = 0$$
$$\rightarrow (f - g - qh)^{\sigma} = 0$$
$$\rightarrow (f - g)^{\sigma} = (qh)^{\sigma}$$
$$\rightarrow f^{\sigma} - g^{\sigma} = q^{\sigma}h^{\sigma},$$

así $q^{\sigma}|_{(f^{\sigma}-g^{\sigma})}$, por lo tanto v es raíz de $(f^{\sigma} - g^{\sigma})$:

$$\rightarrow (f^{\sigma} - g^{\sigma})(v) = 0$$
$$\rightarrow f^{\sigma}(v) = g^{\sigma}(v).$$

Ahora veamos la **inyectividad**, antes afirmamos que $q^{\sigma} = Irr(v, \sigma(M), X)$, observamos que q^{σ} y q tienen el mismo grado, supongamos que existe $p \in M[X]$, con menor grado que q^{σ} y diferente a una constante, tal que $p^{\sigma}|_{q\sigma}$, por lo tanto

$$\exists\, h \in M[X] \,/\, q^{\sigma} = p^{\sigma}h^{\sigma}$$
$$\rightarrow (q - ph)^{\sigma} = 0$$

considerando $(q-ph)(x) = \sum c_i x^i \in M[X]$ entonces, como σ es monomorfismo

$$(q - ph)^{\sigma}(x) = \sum \sigma(c_i)x^i = 0$$
$$\rightarrow \sigma(c_i) = 0$$
$$\rightarrow c_i = 0, \forall i,$$

por lo tanto

$$q - ph = 0$$
$$\rightarrow p|_q \ (\Rightarrow\Leftarrow)$$

Ahora, dado $f(w) \in M(w)$ tal que $\psi(f(w)) = 0 = f^\sigma(v)$, entonces $q^\sigma|_{f^\sigma}$; por lo que existe $h \in M[X]$ tal que

$$f^\sigma = q^\sigma h^\sigma$$
$$\rightarrow (f - qh)^\sigma = 0$$
$$\rightarrow f - qh = 0$$
$$\rightarrow f(w) = q(w)h(w) = (0)h(w)$$
$$\rightarrow f(w) = 0,$$

Así, dado $w \in R$, hemos definido un monomorfismo $\psi : M(w) \rightarrow R'$ y $\psi|_M = \sigma$.

II) Bajo la misma idea de I), considerando todas las raíces diferentes de q en R y las raíces de q^σ en R':

$$w_1 < \cdots < w_n \ \text{ ordenadas en } R \tag{2.8}$$

$$v_1 < \cdots < v_m \ \text{ ordenadas en } R' \tag{2.9}$$

Verifiquemos que existe un monomorfismo $\bar{\psi} : M(w_1, \cdots, w_n) \rightarrow R'$ tal que $\bar{\psi}(w_i) = v_i$, $\forall i = 1 : n$ y que conserva el orden. Tomando en cuenta las desigualdades de las raíces en (2.8), sean $r_i \in R$ tales que

$$r_i^2 = w_{i+1} - w_i, \forall i = 1 : n - 1,$$

y $E_1 = M(w_1, \cdots, w_n, r_1, \cdots, r_{n-1})$, por el teorema del elemento primitivo; E_1 se puede escribir como en I), por lo que existe un monomorfismo $\bar{\phi} : E_1 \rightarrow R'$ tal que $\bar{\phi}|_M = \sigma$, consideremos $\bar{\psi} = \bar{\phi}|_{M(w_1,\cdots,w_n)}$ y evaluamos

$$\begin{aligned}\bar{\psi}(w_{i+1}) - \bar{\psi}(w_i) &= \bar{\phi}(w_{i+1}) - \bar{\phi}(w_i) \\ &= \bar{\phi}(w_{i+1} - w_i) \\ &= \bar{\phi}(w_i^2) = (\bar{\phi}(r_i))^2, \ \forall i = 1 : n - 1,\end{aligned}$$

por lo que

$$\bar{\psi}(w_1) < \cdots < \bar{\psi}(w_n) \text{ ordenadas en } R' \tag{2.10}$$

Considerando $q(x) = \sum c_j x^j$ con $c_j \in M$ y recordando que $\bar{\psi}|_M = \bar{\phi}|_M = \sigma$, vemos que

$$\begin{aligned} q^\sigma(\bar{\psi}(w_i)) &= \sum \sigma(c_j)(\bar{\psi}(w_i))^j \\ &= \sum \bar{\psi}(c_j)\bar{\psi}((w_i)^j) \\ &= \bar{\psi}(\sum c_j (w_i)^j) = \bar{\psi}(q(w_i)) \end{aligned}$$

y como $q(w_i) = 0$ entonces $q^\sigma(\bar{\psi}(w_i)) = 0$, así todas las $\bar{\psi}(w_i)$ son raíces de q^σ en R' por lo que $n \leq m$, cambiando R por R' de igual manera podemos llegar a que $m \leq n$, por lo tanto $n = m$, considerando las desigualdades en (2.9) y (2.10), se cumple que $\bar{\psi}(w_i) = v_i$, $\forall i = 1 : n$.

Verifiquemos que conserva el orden, para esto sera suficiente demostrar que lleva cuadrados en cuadrados. Dado $y \in M(w_1, \cdots, w_n)$ (existen $h, g \in M[X_1, \cdots, X_n]$ tal que $y = h(w_1, \cdots, w_n)/g(w_1, \cdots, w_n))$ con $y > 0$ así, existe $z \in R$:

$$y = z^2, \tag{2.11}$$

considerando $E_2 = M(w_1, \cdots, w_n, r_1, \cdots, r_{n-1}, z)$, existe $\bar{\phi}_2 : E_2 \to R'$ monomorfismo y de la misma manera que se hizo con $\bar{\psi}$; $\bar{\phi}_2(w_i) = v_i = \bar{\psi}(w_i)$, $\forall i = 1 : n$, entonces

$$\begin{aligned} \bar{\psi}(y) &= \bar{\psi}(h(w_1, \cdots, w_n)/g(w_1, \cdots, w_n)) \\ &= h(\bar{\psi}(w_1), \cdots, \bar{\psi}(w_n))/g(\bar{\psi}(w_1), \cdots, \bar{\psi}(w_n)) \\ &= h(\bar{\phi}_2(w_1), \cdots, \bar{\phi}_2(w_n))/g(\bar{\phi}_2(w_1), \cdots, \bar{\phi}_2(w_n)) \\ &= \bar{\phi}_2(h(w_1, \cdots, w_n)/g(w_1, \cdots, w_n)) = \bar{\phi}_2(y) \end{aligned}$$

así en (2.11):

$$\bar{\psi}(y) = \bar{\phi}_2(y) = \bar{\phi}_2(r^2) = (\bar{\phi}_2(r))^2,$$

por lo que $\bar{\psi}$ lleva cuadrados en cuadrados.

Considerando $\bar{\sigma} = \bar{\psi}|_{M(w)}$ monomorfismo que preserva el orden, por lo tanto $(M(w), \bar{\sigma}) \in S$ pero $(M, \sigma) \leq (M(w), \bar{\sigma})$ contradiccion, por lo que $M = R$.

- Verifiquemos que $\sigma(R) = R'$. Sea $v \in R'$, consideremos a

$$q = Irr(v, K, X)$$

Sabemos que q tiene al menos una raíz en R, de hecho, la cantidad de raíces de q en R es la misma que la cantidad de raíces en R' (corolario 2.2.14), denotando:

$$w_1 < \cdots < w_n \text{ raices de } q \text{ ordenadas en } R,$$
$$v_1 < \cdots < v_n \text{ raices de } q \text{ ordenadas en } R'.$$

Dado que σ conserva el orden:

$$\sigma(w_1) < \cdots < \sigma(w_n) \text{ ordenadas en } R'$$

y tomando en cuenta que σ es homomorfismo tal que $\sigma|_K = Id(K)$; $q(\sigma(w_i)) = \sigma(q(w_i)) = \sigma(0) = 0$, es decir, $\sigma(w_i)$ es raíz para todo $i = 1 : n$, por lo tanto, considerando las desigualdades; $\sigma(w_i) = v_i$ para todo $i = 1 : n$, esto nos indica que debe existir un $w \in R$ (raíz de q) tal que $\sigma(w) = v$.

- Verifiquemos que el isomorofismo es único. Supongamos que existe $\psi : R \to R'$ isomorfismo que conserva el orden, sera suficiente probar que dado cualquier $w \in R$; $\sigma(w) = \psi(w)$. Consideramos

$$p = Irr(w, K, X)$$

Tomando en cuenta todas las raíces de p en R:

$$w_1 < \cdots < w_n \text{ ordenadas en } R,$$

como σ y ψ conservan el orden:

$$\sigma(w_1) < \cdots < \sigma(w_n) \text{ ordenadas en } R'$$
$$\psi(w_1) < \cdots < \psi(w_n) \text{ ordenadas en } R',$$

por lo tanto se debe cumplir que $\sigma(w_i) = \psi(w_i)$ para todo $i = 0 : n$ ya que p tiene la misma cantidad de raíces en R' y en R, así como w es raíz; $\sigma(w) = \psi(w)$.

□

Proposición 2.2.16. *Sea K un cuerpo ordenado, K' una extension tal que no existe la relación*

$$-1 = \sum_{i=1}^{n} a_i \alpha_i^2$$

con $a_i \in K$, $a_i > 0$, y $\alpha_i \in K'$. Sea L un cuerpo obtenido de K' adjuntando las raíces de todos los elementos positivos de K. Entonces L es real.

Demostración. Supongamos que L no sea real, entonces se da la relación

$$-1 = \sum_{i=1}^{n} a_i \alpha_i^2 \tag{2.12}$$

con $a_i \in K$, $a_i > 0$, y $\alpha_i \in L$ (podemos tomar $a_i = 1$). Sea r el mínimo entero tal que podemos escribir (2.12) con α_i en un subcuerpo de L de la forma

$$K'(\sqrt{b_1}, \cdots, \sqrt{b_r})$$

con $b_j \in K$, $b_j > 0$. Escribimos

$$\alpha_i = x_i + y_i\sqrt{b_r} \in K'(\sqrt{b_1}, \cdots, \sqrt{b_r})$$

con $x_i, y_i \in K'(\sqrt{b_1}, \cdots, \sqrt{b_{r-1}})$, luego

$$-1 = \sum a_i (x_i + y_i\sqrt{b_r})^2 = \sum a_i (x_i^2 + 2x_i y_i \sqrt{b_r} + y_i^2 b_r)$$
$$\to -1 - \sum a_i (x_i^2 + y_i^2 b_r) = 2(\sum x_i y_i)\sqrt{b_r} \in K'(\sqrt{b_1}, \cdots, \sqrt{b_{r-1}}),$$

ya que $b_r \in K$ pero $\sqrt{b_r} \notin K'(\sqrt{b_1}, \cdots, \sqrt{b_{r-1}})$ no, por lo tanto $2(\sum x_i y_i)\sqrt{b_r} = 0$, así

$$-1 = \sum a_i x_i^2 + \sum y_i^2 b_r,$$

lo cual contradice la minimalidad de r. □

Teorema 2.2.17. *Sea K un cuerpo ordenado, existe una cerradura real R de K induciendo el orden en K.*

Demostración. Tomando $K' = K$ y verificando las condiciones para aplicar la Proposición 2.2.16., en caso la relación

$$-1 = \sum_{i=1}^{n} a_i \alpha_i^2$$

con $a_i, \alpha_i \in K$, $a_i > 0$, se de; -1 seria positivo en K, lo cual es seria contradicción con K ser ordenado, por lo tanto existe L extension real de K (L es la extension de K que contiene a K y todas las raíces cuadradas de los elementos positivos en K), por el teorema 2.2.5., L tiene una cerradura real R, la cual seria cerradura real de K también.

Toca verificar que el orden en R, $P = \{r^2 \,|\, r \in R\}$, induce el orden de K. Denotando a Q como orden de K, debemos verificar que $Q = K \cap P$:

($\subseteq$) : Sea $q \in Q$ y $q \neq 0$;

$$q \in Q \subset K \subset R$$
$$\rightarrow\ q \in P\ \vee\ -q \in P$$

supongamos que $-q \in P$ entonces existe $r \in R$ tal que $-q = r^2$. Como q es positivo en K entonces existe $l \in L \subset R$ tal que $q = l^2$, así;

$$-l^2 = r^2$$
$$\rightarrow\ l^2 + r^2 = 0,$$

lo que indica que $0 \in P$, lo cual es contradicción, por lo que $q \in K \cap P$.

($\supseteq$) : Sea $p \in K \cap P$ y $p \neq 0$;

$$p \in P\ \wedge\ p \in K$$
$$\rightarrow \exists r \in R\ /\ p = r^2\ \wedge\ (p \in Q\ \vee\ -p \in Q),$$

supongamos que $-p \in Q$, es decir, es positivo en K entonces existe $l \in L \subset R$ tal que $-p = l^2$, así;

$$-r^2 = l^2$$
$$\rightarrow r^2 + l^2 = 0,$$

lo que indica que $0 \in P$, lo cual es contradicción, por lo que $p \in Q$.

□

Proposición 2.2.18. *Sea K un cuerpo ordenado y K' una extension. Así para que exista un orden en K' induciendo el orden en K, es necesario y suficiente que no se de la relación*

$$-1 = \sum_{i=1}^{n} a_i \alpha_i^2$$

con $a_i \in K$, $a_i > 0$, *y* $\alpha_i \in K'$.

Demostración. Es suficiente, si la relación no se cumple, utilizando la Proposición 2.2.15; existe L extension real, la cual a su vez tiene una cerradura real R induciendo el orden en K', y el orden dado en K también.

Es necesario, si la relación se cumple para algunos $a_i \in K \subset K'$, $a_i > 0$, y $\alpha_i \in K'$., entonces $-1 \in K'$ seria positivo; lo cual contradice el orden en K'. □

Observación 2.2.19. *Sea* $\mathbb{Q}$ *el cuerpo de números racionales, sea* $\mathbb{Q}^a$ *el cuerpo de números algebraicos. Sabemos que* $\mathbb{Q}$ *solo admite un orden, así por lo visto; cualquier par de cerraduras reales de* $\mathbb{Q}$ *en* $\mathbb{Q}^a$ *deben ser isomorficas.*

Conclusiones

En el presente trabajo se han estudiado a los cuerpos reales. Recordando que un cuerpo es real cuando no se cumple

$$\sum a_i^2 = -1$$

con a_i en dicho cuerpo. A continuación mencionaremos los resultados mas importantes:

i) Todo cuerpo real K; tiene una cerradura real R. Dicha cerradura R solo admite un orden; el cual esta determinado por sus cuadrados, es decir, los elementos positivos son los cuadrados de R. Con lo anterior se dan las condiciones para que se verifique que la cerradura algebraica de R esta dada por su extension generada por $\sqrt{-1}$; $R^a = R(\sqrt{-1})$, lo cual emula a lo que sucede en los números reales; donde su cerradura esta dada por lo números complejos.

ii) Hemos probado una version del teorema de valor intermedio; sea R un cuerpo real cerrado y f un polinomio en $R[X]$ tal que dados $a, b \in R$, asumiendo que $f(a) < 0$ y $f(b) > 0$, entonces existe $c \in R$ entre a y b tal que $f(c) = 0$.

iii) Se ha demostrado el teorema de Sturm. Para tal demostración se ha definido la sucesión de Sturm; dada por un polinomio $f \in R[X]$ sin raíces múltiples donde R es real cerrado. El teorema de Sturm nos indica que podemos contar la cantidad de raíces de f en un intervalo $[u, v]$, dicha cantidad estará dada por $W_S(u) - W_S(v)$ donde W_S denota la variación de signos de la sucesión de Sturn evaluada en el punto dado.

iv) Se ha visto que si existen dos cerraduras reales de un cuerpo K ordenado (orden de K inducido por el orden de las cerraduras), estas deben son isomorficas por un único isomorfismo que preserva el orden.

v) Y por ultimo se ha demostrado que todo cuerpo K ordenado admite una cerradura real induciendo el orden en K.

Un proyecto a futuro para extender la teoría vista, es dar prueba a los resultados encontrados en la sección 3 de [3], en la cual aplican los resultados vistos en el trabajo.

Bibliografía

[1] Conrad, K. (2023). *Roots and Irreducibles*. [Archivo PDF]. https://kconrad.math.uconn.edu/blurbs/galoistheory/rootirred.pdf. 5

[2] Martin I. (1994). *Algebra: A Graduate Course*. Brooks/Cole 5

[3] Lang, S. (2002). *Algebra*. Springer. 2, 6, 7, 8, 18, 39

[4] Lagrange's four-square theorem. (11 de julio del 2023). En *Wikipedia*. https://en.wikipedia.org/wiki/Lagrange%27s_four-square_theorem. 14