

UNIVERSIDAD DE SANTIAGO DE CHILE
Facultad de Ciencia
Departamento de Matemática y Ciencia de la Computación



El número de pitágoras del cuerpo de funciones de curvas reales y racionales

Vicente Muñoz Briones

Profesor guía:
David Grimm

Tesis para optar al título de
Magister en Ciencia en la Especialidad de Matemática

Santiago, Chile
2026

Esta investigación se ha realizado
en el marco el proyecto Dicyt - 042432G

Resumen

La conjetura de Pfister, formulada en la década de los 90's, afirma que, dada una extensión finita sobre el cuerpo de fracciones del anillo de polinomios en una variable sobre los números racionales y en extensiones finitas de este cuerpo de fracciones, todo elemento totalmente positivo puede expresarse como suma de a lo más cinco cuadrados. En este trabajo presentaremos la demostración de dicha conjetura, propuesta por Olivier Benoist en 2025. La demostración original utiliza el lenguaje de secciones globales y racionales de fibrados lineales, utilizando implícitamente la equivalencia con divisores. En nuestro caso, el objetivo es reducir la prueba puramente al lenguaje de divisores y a los subespacios asociados en el cuerpo de funciones. Con esto, buscamos hacer el trabajo accesible a lectores con conocimiento previo en la teoría algebraica de cuerpos de funciones —como la desarrollada en el texto de Stichtenoth— sin la necesidad de recurrir a las diversas equivalencias de categorías que habitualmente se adquieren en cursos de geometría algebraica más avanzada.

Palabras clave: Suma de cuadrados, divisores y valuaciones.

Abstract

Pfister's conjecture, formulated in the 1990s, states that, given a finite extension over the field of fractions of the ring of polynomials in one variable over the rational numbers and finite extensions of this field of fractions, every totally positive element can be expressed as the sum of at most five squares. In this thesis, we will present the proof of this conjecture, proposed by Olivier Benoist in 2025. The original proof uses the language of global and rational sections of linear bundles, implicitly employing equivalence with divisors. In our case, the aim is to reduce the proof purely to the language of divisors and the associated subspaces in the field of functions. By doing so, we seek to make the work accessible to readers with prior knowledge of algebraic function field theory—such as that developed in Stichtenoth's text—without the need to resort to the various category equivalences typically acquired in more advanced algebraic geometry courses.

Keywords: Sums of square, valuations and divisor.

A Sofía y Martuca.

Agradecimientos

En primera instancia agradecerle a mis padres por apoyar mi decisión de estudiar matemáticas, a mi madre por su apoyo incondicional, a mi padre por siempre estar ahí, a mi hermano Franz por apoyarme a su manera. Agradecer profundamente a mi novia Sofía, por darme razones para seguir adelante, sin ella no hubiera podido completar esta etapa de ninguna manera. Agradecer la compañía desinteresada de mi gata Martuca, quien me estuvo cada día conmigo en cada día de la redacción de este documento. También a mis amigos: Cami, Basti, Toto, Mati, Saiqi, Pedro y Bruno, por ser el único lindo recuerdo que tengo de la U. de Chile. A mis amigas Macarena y Vale merino por apoyarme a la distancia.

Agradecer a quienes me recomendaron para este programa, Dr. G. Lucchini y en especial a la Doctora Alicia Labra, a quien agradeceré eternamente por confiar en mi y creer que podría realizar este Magíster sin complicaciones, gracias a sus palabras alentadoras tuve la motivación de continuar en el programa a pesar de todas las dificultades que se presentaron. Con orgullo llevaré siempre sus palabras conmigo y recordaré que una eminencia como ella creyó en mi.

Obviamente debo agradecerle a las política publicas de educación gratuita, ya que sin ellas no hubiese podido estudiar la licenciatura, también agradecer a la labor social de la USACH que me permitió estudiar este magister.

Finalmente agradecerle al profesor David Grimm, quien tuvo la disposición de ayudarme y guiarme de una manera excelente. Agradecerle por el apoyo, las reuniones y la paciencia.

Tabla de contenido

Introducción	1
1. Preliminares algebraicos	4
1.1. Sumas de cuadrados sobre cuerpos	4
1.2. Cuerpos Real Cerrados	5
1.3. Teoría algebraica de formas cuadráticas	7
2. Cuerpos de funciones en una variable	15
2.1. Cuerpo de funciones algebraicas F/K	15
2.2. Anillos de valuación de F/K	17
2.3. Lugares de un cuerpo de Funciones algebraicas	18
2.4. Divisores	21
2.5. Control de polos o ceros en representaciones de sumas de cuadrados . . .	25
2.6. Cambio de base	26
3. Sumas de cuadrados de funciones sobre un cuerpo real cerrado	29
3.1. Existencia de lugares reales	30
3.2. Estudio del nivel y divisores de F/R	33
3.3. Cálculo del número de Pitágoras de F/R	36
4. Preliminares aritméticos	38
4.1. Cuerpos p -ádicos	38
4.2. Lema de Hensel y sus consecuencias	42
5. Sumas de cuadrados de funciones sobre un cuerpo de números	47
5.1. Principio Local-Global Kato	49
5.2. Existencia 2-ádica de representación por sumas de 5 cuadrados	53
5.3. Variaciones 2-ádicas de sumas de 4 cuadrados	55
5.4. Existencia real de representación por sumas de 5 cuadrados	62
5.5. Variaciones reales de suma de 4 cuadrados	64
5.6. Cálculo del número de pitágoras de F/k	66

5.7. Consecuencias del Teorema de Benoist	69
5.7.1. Preguntas Finales	72
Referencias	74

Índice de figuras

2.1. Diagrama de la extensión F'/K' sobre F/K	27
---	----

Introducción

El número de Pitágoras $p(k)$ de un cuerpo k es el entero positivo más pequeño p tal que cada suma de cuadrados en k es una suma de p cuadrados. Sabemos que Euler (1760) demostró que $p(\mathbb{Q}) = 4$, mientras que Siegel (1921) extendió este resultado a un cuerpo de números k arbitrario, demostrando que $p(k) \leq 4$. Posteriormente, Pourchet (1971) consideró el caso de $\mathbb{Q}(t)$, el cuerpo de funciones racionales en una variable sobre $\mathbb{Q}$, donde demostró que $p(\mathbb{Q}(t)) \leq 5$. Basado en ese resultado, Pfister conjeturó que, si F es una extensión finita de $k(t)$ para k un cuerpo de números, entonces $p(F) \leq 5$ (véase Pfister (1995, Capítulo 7, Conjetura 1.10(1))). En julio de 2025, el matemático Olivier Benoist publicó un preprint (Benoist, 2025) con el enunciado de la afirmación de la conjetura, este preprint fue escrito en el lenguaje geométrico, usando esquemas y espacios anillados, nosotros buscaremos traducir esta demostración al lenguaje de valuaciones y divisores.

En los más de 50 años entre Pourchet (1971) y Benoist (2025) se desarrollaron muchos resultados parciales. Por ejemplo, Colliot-Thélène y Jannsen (1991) demostró que $p(F) \leq 7$. Ya en 1934, Ernst Witt demostró que $p(F) = 2$ si F es una extensión finita de $\mathbb{R}(t)$. Este trabajo inicial está escrito en un lenguaje de geometría compleja (superficies de Riemann), pero las ideas de su demostración pueden rastrearse en los trabajos posteriores. Con el objetivo de clarificar el desarrollo de estas ideas. Uno de nuestros objetivos será algebraizar los argumentos analíticos de Witt e identificar la secuencia lógica en los demás trabajos, lo que permitirá entender y evaluar la veracidad del preprint de Benoist (2025).

Para lograr este objetivo, el presente trabajo se estructura de la siguiente manera.

En el Capítulo 1, introduciremos los preliminares algebraicos necesarios, centrados principalmente en la teoría de formas cuadráticas y la introducción de los anillos de Witt los cuales serán esenciales para enunciar el Teorema de Kato.

El Capítulo 2 establecerá las bases de la teoría de cuerpos de funciones algebraicas

sobre un cuerpo k , definiendo conceptos esenciales como anillos de valuación, lugares, y divisores, sentando las bases del lenguaje algebraico en el cual se desarrollará el trabajo.

En el Capítulo 3, abordaremos la generalización del teorema clásico de Witt, reemplazando el cuerpo $\mathbb{R}$ por un cuerpo real cerrado R . Esto lo haremos dando una demostración puramente algebraica del Teorema de Witt para cuerpos de funciones algebraicas F/R . Dada una función $f \in F/R$ positiva definida, el argumento central radicarà en estudiar su divisor principal en la extensión $F(i)/R(i)$. Utilizando la divisibilidad del grupo de clases de esta extensión, demostraremos que es posible descomponer el divisor de f como

$$\text{div}^R(f) = \text{div}^{R(i)}(A) + \overline{\text{div}^{R(i)}(A)}$$

para alguna función compleja $A = a+bi \in F(i)$ (Proposición 3.6). Esto nos permitirá deducir algebraicamente que f difiere de una suma de dos cuadrados solo por una constante $l \in R$, es decir, $f = l(a^2 + b^2)$.

La prueba concluirà dicotomizando el problema según la existencia de lugares R -racionales. si $F(R) \neq \emptyset$, la hipótesis de positividad definida sobre f fuerza a que $l > 0$ (Teorema 3.10), siendo trivialmente un cuadrado en R .

Por otro lado, si $F(R) = \emptyset$, el cuerpo no es formalmente real y -1 es suma de dos cuadrados (Corolario 3.9), lo que, mediante la identidad de Euler, permitirá absorber un eventual signo negativo de l .

En todos los casos, se garantizarà la existencia de $g, h \in F$ tales que $f = g^2 + h^2$ (Teorema 3.11). Esto nos permitirá comprender qué hipótesis reales son estrictamente necesarias en la demostración original.

El Capítulo 4 proporcionará los preliminares aritméticos, introduciendo los cuerpos p -ádicos, el Lema de Hensel y sus consecuencias, las cuales serán relevantes para el desarrollo de este trabajo.

Finalmente, el Capítulo 5. Dado un elemento $f \in F/k$ positiva definida, siempre podremos escribir su divisor de la forma $\text{div}(f) = E - 2D$. Con esto vamos a justificar la existencia de secciones $\alpha_v \in \mathcal{L}_v(lA)$ y $\beta_{i,v} \in \mathcal{L}_v(D + lA)$ para algún divisor A de F/k amplio y un $l \in \mathbb{Z}$ lo

suficientemente grande, tal que para todo lugar v de k satisfagan la siguiente ecuación

$$f\alpha_v^2 = \sum_{i=1}^5 \beta_{i,v}^2$$

en cada completación k_v respectivamente (véase Teorema 5.10 y Teorema 5.20).

Luego se probará que la propiedad de ser suma de cuatro cuadrados se preserva bajo pequeñas perturbaciones en vecindades 2-ádicas (véase Proposición 5.16), lo mismo ocurrirá para completaciones reales. De este modo se podrá argumentar que las secciones $\alpha \in \mathcal{L}(lA)$ y $\beta_5 \in \mathcal{L}(D + lA)$ en F/k que aproximan simultáneamente a α_v con α y $\beta_{5,v}$ con β_5 , cuando v es una completación diádica y real, dadas por el Teorema de aproximación débil de Artin-Whaples, cumplirán que la función positiva definida

$$f - \left(\frac{\beta_5}{\alpha} \right)^2$$

es suma de 4 cuadrados en todas las completaciones F_v/k_v (siendo este el resultado principal, véase Teorema 5.25). Finalmente se aplicará un principio local global deducido del Teorema de Kato, 1986 (Véase Teorema 5.5). Concluyendo así la prueba de la conjetura de Pfister.

Paralelamente, compararemos el proceso lógico del Trabajo de Benoist con la demostración de Pourchet para el caso particular cuando $F = \mathbb{Q}(t)$.

Capítulo 1

Preliminares algebraicos

En este primer capítulo buscaremos dar las definiciones más básicas pero sumamente relevantes para el desarrollo de este trabajo.

Este capítulo se centrará principalmente en formas cuadráticas.

1.1. Sumas de cuadrados sobre cuerpos

Como bien adelanté en la introducción y como se puede ver en el título de la tesis, el objetivo será calcular el número de Pitágoras de cuerpos de funciones algebraicas en diversos cuerpos.

Para ello, vamos con la primera definición:

Definición 1.1. El número de Pitágoras $p(K)$ de un cuerpo cualquiera K es el entero positivo p más pequeño tal que cada suma de cuadrados en K es una suma de p cuadrados.

Resultados conocidos de este valor son, se mencionaron en la introducción, por ejemplo: Euler (1760) demostró que $p(\mathbb{Q}) = 4$, también, Pourchet (1971) demostró que $p(k(t)) \leq 5$ para cualquier cuerpo de números k . Otro ejemplo importante es el siguiente:

Ejemplo 1.2 (Pfister, 1995 Chapter 7, §1, Example 1.4 (3)). Si k es un cuerpo de números, entonces

$$p(k) = \begin{cases} 4 & \text{Si } k \text{ tiene un lugar dyadico } \mathfrak{p} \text{ con } [k_{\mathfrak{p}} : \mathbb{Q}_2] \text{ impar} \\ 3 & \text{En otro caso.} \end{cases}$$

Más adelante entraremos en detalles sobre que es $k_{\mathfrak{p}}$, por ahora podemos notar que $p(\mathbb{Q}) = 4$ ya que $[\mathbb{Q}_2 : \mathbb{Q}_2] = 1$. Dado un cuerpo k , diremos que este es *no real* si y solo si

-1 es suma de cuadrados en k . podemos desprender la siguiente definición:

Definición 1.3. Sea k un cuerpo no real, definimos el *nivel del cuerpo k* como el menor entero tal que -1 es suma de cuadrados. Lo denotamos como $s(k)$.

1.2. Cuerpos Real Cerrados

En este capítulo vamos a definir lo que es un cuerpo real cerrado, al igual que la noción de la clausura real de un cuerpo ordenado. Dado que las sumas de cuadrados son fuertemente relacionados con la noción de ordenes en un cuerpo, empezaremos con recordar algunas definiciones básicas.

Definición 1.4. Sea C un conjunto cualquiera. Una *relación de orden* $\leq$ en C es una relación binaria $\leq \subseteq C \times C$ que satisface los siguientes axiomas:

- a) Reflexiva: $\forall x \in C, x \leq x$.
- b) Antisimetría: $\forall x, y \in C, (x \leq y \wedge y \leq x) \Rightarrow x = y$.
- c) Transitividad: $\forall x, y, z \in C, (x \leq y \wedge y \leq z) \Rightarrow x \leq z$

Si además cumple que $\forall x, y \in C$ se tiene que $x \leq y$ o $y \leq x$, diremos que $\leq$ es una relación de *orden total*.

Definición 1.5. Sea $(K, +, \cdot)$ un cuerpo cualquiera. Diremos que $\leq$ es un *orden* del cuerpo K , si satisface las siguientes propiedades para todo $a, b, c \in K$:

- Si $a \leq b$ entonces $a + c \leq b + c$, y
- Si $0 \leq a$ y $0 \leq b$, entonces $0 \leq a \cdot b$.

Como es usual, escribiremos $a < b$ para $a \leq b$ y $a \neq b$. Las notaciones $b \geq a$ y $b > a$ representan $a \leq b$ y $a < b$ respectivamente. Los elementos en $0 < a$ se llaman *positivos*.

Definición 1.6. Un cuerpo ordenado es un par $(K, \leq)$ donde K es un cuerpo y $\leq$ un orden del cuerpo en K . Un cuerpo ordenado $(K, \leq)$ se denomina *maximalmente ordenado* si y solo si no existe ninguna extensión algebraica de cuerpos propia $K \subsetneq K_1$ que admita un orden $\leq_1$ que extienda el orden $\leq$ de K .

Proposición 1.7 (Prestel, 2007, Proposition 3.1). Sea $(K, \leq)$ un cuerpo maximalmente ordenado. Entonces cada elemento de K positivo con respecto $\leq$ es un cuadrado. En particular, $\leq$ es el unico orden de cuerpo en K .

Definición 1.8. Diremos que un cuerpo cualquiera K es *formalmente real* si -1 no es suma de cuadrados en K .

En algunos textos llaman a los cuerpos formalmente reales, solo reales. Nosotros reservaremos el adjetivo "real" en el caso en el que el cuerpo pueda ser incrustado en $\mathbb{R}$.

Definición 1.9. Un cuerpo R se dice *real cerrado* si R es formalmente real y que no tiene ninguna extensión algebraica de cuerpos propia formalmente real.

Observación 1.10. 1. Un cuerpo R es real cerrado si y solo si tiene un único orden y $(R, \leq)$ es maximalmente ordenado (Véase Prestel, 2007, Lemma 3.2).

2. Un cuerpo R es real cerrado si y solo si $R(\sqrt{-1})$ es algebraicamente cerrado y $R \neq R(\sqrt{-1})$. (Véase Prestel, 2007, Theorem 3.3).

Si recordemos que la propiedad arquimediana en un conjunto ordenado C nos dice que: dados dos elementos $x, y \in C$ con $x > 0$, existe un $n \in \mathbb{N}$ tal que $nx > y$. Esto nos motiva a definir esta propiedad respecto a las extensiones de un cuerpo real cerrado R .

Definición 1.11. Sea $(L, \leq)$ un cuerpo ordenado y sea $R \subseteq L$ un subcuerpo que es un cuerpo real cerrado. Se dice que el cuerpo $(L, \leq)$ es *R -arquimediano* (o que la extensión ordenada L/R es *arquimediana*) si y solo si, para todo elemento $x \in L$, existe un elemento $r \in R$ tal que $x \leq r$.

Definición 1.12. Una *clausura real* de un cuerpo formalmente real K con respecto a un orden fijo es una extensión algebraica real cerrada R/K , tal que el orden de R se restringe al orden fijado en K .

Observación 1.13. Para cualquier cuerpo formalmente real K , para cualquier orden de K , existe una unica clausura real con respecto a este orden, salvo K -isomorfismo (Véase, Prestel,

2007, Lema 3.6).

1.3. Teoría algebraica de formas cuadráticas

Otro de los componentes esenciales para el desarrollo de este trabajo son las formas cuadráticas y toda la teoría que estas conllevan. La mayoría de definiciones de esta sección son extraídas del libro Lam, 2005.

Definición 1.14. Una n -forma cuadrática sobre un cuerpo K es un polinomio q homogéneo de n variables de grado dos, más precisamente

$$q(X_1, \dots, X_n) = \sum_{i,j=1}^n a_{ij} X_i X_j \in K[X_1, \dots, X_n]$$

En términos matriciales, definamos la matriz M_f como la matriz de coeficientes (a'_{ij}) , donde $a'_{ij} = \frac{1}{2}(a_{ij} + a_{ji})$ (para que la matriz sea simétrica) esto nos dice que podemos escribir el polinomio q como

$$q(X) = (X_1, \dots, X_n) \cdot M_q \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} = X^t \cdot M_f \cdot X$$

Diremos que dos formas cuadráticas f y g son *equivalentes* ($f \cong g$) si existe un cambio de coordenadas lineal, no singular y homogéneo de las coordenadas $X_1, \dots, X_n$ que envía la forma g a la forma f , en el sentido de matrices, será cuando exista una matriz $C \in GL_n(k)$ tal que $f(X) = g(C \cdot X)$ es decir que

$$\begin{aligned} f(X) &= g(C \cdot X) \\ \Rightarrow X^t \cdot M_f \cdot X &= (CX)^t \cdot M_g \cdot CX \\ \Rightarrow X^t \cdot M_f \cdot X &= (X)^t \cdot (C^t \cdot M_g \cdot C) \cdot X \\ \Rightarrow M_f &= C^t \cdot M_g \cdot C \end{aligned}$$

Esto ultimo nos dice que podemos reducir la equivalencia de formas cuadráticas de un cuerpo K , a equivalencia de matrices simétricas del grupo $GL_n(K)$.

Ahora un ejemplo de equivalencia de formas cuadráticas.

Ejemplo 1.15. Si usamos el cambio lineal ϕ que cumple que $X_1 \rightarrow X_1 + X_2, X_2 \rightarrow X_1 - X_2$, la forma binaria $g(X_1, X_2) = X_1X_2$ cambia de la siguiente manera

$$\begin{aligned} g(\phi(X)) &= g(X_1 + X_2, X_1 - X_2) = (X_1 + X_2)(X_1 - X_2) \\ &= X_1^2 - X_2^2 \end{aligned}$$

Es decir, g es equivalente a la forma $q(X_1, X_2) = X_1^2 - X_2^2$

Por tradición, definiremos la siguiente notación. Sea la forma cuadrática $q = \sum_{i=1}^n a_i X_i^2$ en K , entonces la denotamos como $q = \langle a_1, \dots, a_n \rangle$.

Continuando con las definiciones claves, tenemos la siguiente.

Definición 1.16. Sea q una forma cuadrática definida sobre un cuerpo K , definimos la *forma bilineal* inducida por q en $K \times K$ de la siguiente manera:

$$B(x, y) = \frac{q(x + y) - q(x) - q(y)}{2}$$

ahora si tomamos V un K -espacio vectorial de dimensión finita y $B : V \times V \rightarrow k$ una forma bilineal simétrica en V . Diremos que el par (V, B) es un *espacio cuadrático* con un mapeo cuadrático $q = q_B : V \rightarrow F$ dado por $q(X) = B(X, X)$. Si B y q están determinados, para referirnos al espacio cuadrático asociado podemos escribir (V, q) en vez (V, B) .

El espacio (V, q) puede ser visto como el espacio de clases de equivalencias de todas las formas g tales que $g \cong q$.

Sea S un subespacio de V , definimos su *complemento ortogonal* como

$$S^\perp = \{x \in V \mid B(x, S) = 0\}$$

diremos que un espacio cuadrático (V, B) es *regular* si su complemento ortogonal $V^\perp$ es igual a cero.

Otra definición relevante será la siguiente.

Definición 1.17. Sea v un vector no nulo en el espacio cuadrático (V, B) . Diremos que es un *vector isotrópico* si $B(v, v) = 0$ (o equivalentemente si $q(v) = 0$ donde $q = q_B$) y si se tiene el caso contrario, entonces diremos que es *anisotrópico*. Diremos que el espacio

(V, B) es isotrópico si existe un vector v isotrópico.

Definición 1.18. Diremos que una forma cuadrática q de un espacio cuadrático (V, q) , es universal si para todo vector $v \in V$ existe un vector v' tal que $q(v') = v$. También podemos definir el conjunto $D_k(q) = \{d \in k^* | \exists v \in V \text{ tal que } q_B(v) = d\}$

Proposición 1.19. Sea (V, q) un espacio cuadrático dos dimensional. Las siguientes afirmaciones son equivalentes:

1. V es regular e isotrópico.
2. V es isométrico a $\langle 1, -1 \rangle$.
3. V corresponde a la clase de equivalencia de las formas cuadráticas binarias $X_1 X_2$.

Definición 1.20. La clase de isometría de los espacios cuadráticos 2 dimensional que satisfacen las condiciones de la proposición anterior, son llamadas *plano hiperbólico*, que será denotado como $\mathbb{H}$.

Con esta definición, tenemos el primer resultado sobre la representación de formas cuadráticas.

Teorema 1.21 (Lam, 2005, Chap I. Theorem 3.4). Sea (V, q) un espacio cuadrático regular, entonces: Si V es isotrópico $\Rightarrow V$ es universal.

Lema 1.22 (Lam, 2005, Chap I, Corollary 3.5). Sea q una forma cuadrática regular y $d \in K$. Entonces $d \in D(q)$ si y solo si $q \perp \langle -d \rangle$ es isotrópica.

Ahora vamos a definir una de las dos operaciones más importantes dentro del álgebra de formas cuadráticas, la suma ortogonal, la cual será fundamental para poder definir el anillo de Witt, el cual es nuestro principal objetivo en esta sección.

La *suma ortogonal* se definirá de la siguiente manera. Sean (V_1, B_1) y (V_2, B_2) dos espacios cuadráticos, vamos a formar el espacio (V, B) donde $V = V_1 \oplus V_2$ y $B : V \times V \rightarrow K$ dada por:

$$B((X_1, X_2), (Y_1, Y_2)) = B(X_1, X_2) + B_2(Y_1, Y_2)$$

De esta manera el espacio (V, B) lo podemos denotar como $V_1 \perp V_2$, esto es la *suma ortogonal*. Notemos que

$$\begin{aligned} q_B(X_1, X_2) &= B((X_1, X_2), (X_1, X_2)) \\ &= B_1(X_1, X_1) + B_2(X_2, X_2) \\ &= q_{B_1}(X_1) + q_{B_2}(X_2) \end{aligned}$$

Para dar un ejemplo de como se realiza esta suma, debemos dar uno de los lemas más conocidos en suma de cuadrados que es el siguiente

Lema 1.23 (identidad de los cuadrados de Euler). *La identidad de los 4 cuadrados de Euler, nos dice que:*

$$\begin{aligned} (a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) &= (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 \\ &\quad + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 \\ &\quad + (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 \\ &\quad + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2 \end{aligned}$$

en cualquier cuerpo K , y que también se cumple con 2 cuadrados, es decir

$$(a_1^2 + a_2^2)(b_1^2 + b_2^2) = c_1^2 + c_2^2$$

Además, debemos recordar los siguientes hechos:

- En $\mathbb{Q}_2$ tenemos que $-1 = 1^2 + 1^2 + 2^2 + (\sqrt{-7})^2$
- -1 es suma de 2 cuadrados en $\mathbb{Q}_p$ para $p > 2$ (Véase Proposición 4.15)

Con estos hechos ya conocidos, podemos demostrar la siguiente proposición

Ejemplo 1.24. Sea la forma cuadrática $q = \langle 1, 1, 1, 1 \rangle$ definida sobre $\mathbb{Q}_p$ y sea la forma cuadrática $h = \langle 1, -1 \rangle$ entonces

$$\langle 1, 1, 1, 1 \rangle \cong \begin{cases} \langle 1, 1, -1 \rangle \perp h & \text{si } p > 2 \\ \langle -1, -1, -1 \rangle \perp h & \text{si } p = 2 \end{cases}$$

Comenzaremos con el caso $\mathbb{Q}_2$. Sea $V = \mathbb{Q}_2^5$ (en el sentido de producto cartesiano), denotemos por $V_1 = \mathbb{Q}_2^3$ y $V_2 = \mathbb{Q}_2^2$ y además $q_{B_1} = \langle -1, -1, -1 \rangle$ y $q_{B_2} = \langle 1, -1 \rangle$, podemos ver que:

$$\begin{aligned} q_1 \perp q_2 = q_B &= q_{B_1} + q_{B_2} \\ &= -x_1^2 - x_2^2 - x_3^2 + x_4^2 - x_5^2 \\ &= -1(x_1^2 + x_2^2 + x_3^2 + x_5^2) + x_4^2 \\ &= y_1^2 + y_2^2 + y_3^2 + y_5^2 + x_4^2 = \langle 1, 1, 1, 1, 1 \rangle \end{aligned}$$

Como mencioné anteriormente, -1 es suma de 4 cuadrados en $\mathbb{Q}_2$ y multiplicar sumas de cuatro cuadrados siguen siendo sumas de cuatro cuadrados.

De manera análoga, en el caso $\mathbb{Q}_p$ con $p > 2$, definamos los mismos V_1 y V_2 de antes, pero con $q_{B_1} = \langle 1, 1, -1 \rangle$ y $q_{B_2} = \langle 1, -1 \rangle$ tenemos el siguiente cálculo:

$$\begin{aligned} q_1 \perp q_2 = q_B &= q_{B_1} + q_{B_2} \\ &= x_1^2 + x_2^2 - x_3^2 + x_4^2 - x_5^2 \\ &= -1(x_3^2 + x_5^2) + x_2^2 + x_1^2 + x_4^2 \\ &= y_3^2 + y_5^2 + x_2^2 + x_1^2 + x_4^2 = \langle 1, 1, 1, 1, 1 \rangle \end{aligned}$$

Teorema 1.25 (Teorema de cancelación de Witt). *Si q, q_1, q_2 son formas cuadráticas arbitrarias, entonces $q \perp q_1 \cong q \perp q_2 \Rightarrow q_1 \cong q_2$*

Esto ya que nos ayudará a dotar de una estructura algebraica al espacio de formas cuadráticas de un cuerpo K , pero eso se introducirá más adelante. Por lo pronto continuaremos dando definiciones básicas de formas cuadráticas, la siguiente será *el producto de Kronecker*.

Sean (V_1, B_1, q_1) y (V_2, B_2, q_2) dos espacios cuadráticos sobre K de dimensión m y n respectivamente. Ahora definimos el espacio cuadrático $V = V_1 \otimes V_2$ y sea $B : V \times V \rightarrow K$ una forma bilineal que satisface:

$$B(v_1 \otimes v_2, v'_1 \otimes v'_2) = B_1(v_1, v'_1)B_2(v_2, v'_2) \quad (v_i, v'_i \in V_i)$$

El par (V, B) define un espacio cuadrático de dimensión mn llamado el producto de Kronecker de los (V_i, B_i) . El mapeo cuadrático asociado $q = q_B$ satisface que $q(v_1 \otimes v_2) = q_1(v_1)q_2(v_2)$. De manera directa, este producto cumple con las siguientes reglas:

1. $q_1 \otimes q_2 \cong q_2 \otimes q_1$
2. $(q_1 \otimes q_2) \otimes q_3 \cong q_1 \otimes (q_2 \otimes q_3)$
3. $q \otimes (q_1 \perp q_2) \cong (q \otimes q_1) \perp (q \otimes q_2)$

Usando estas reglas podemos formar el producto de formas diagonales:

$$\langle a_1, \dots, a_m \rangle \otimes \langle b_1, \dots, b_n \rangle \cong \langle a_1 b_1, \dots, a_m b_n \rangle$$

Con este producto, podemos definir las n -formas de Pfister, que jugaran un papel fundamental en todo este trabajo.

Definición 1.26. Definimos la n -forma de Pfister como

$$\langle \langle a_1, \dots, a_n \rangle \rangle = \bigotimes_{i=1}^n \langle 1, a_i \rangle$$

Cuando $n = 2$ tenemos que $\langle \langle a, b \rangle \rangle = \langle 1, a \rangle \otimes \langle 1, b \rangle = \langle 1, a, b, ab \rangle$.

Ahora, continuando con las definiciones, vamos a introducir el *anillo de witt* y los *ideales fundamentales*, que nos ayudarán a deducir el principio local global de Kato.

Definición 1.27. Denotamos como $M(K)$ al conjunto de *clases de formas cuadráticas isométricas*.

Notemos que junto con la suma ortogonal, el par $(M(K), \perp)$ define un monoide de cancelación esto gracias al Teorema 1.25. Si además incluimos el producto de Kronecker $\otimes$, entonces el espacio $M(K)$ define un semianillo conmutativo con estas dos operaciones binarias. Ahora definamos la relación $\sim$ en $M(K) \times M(K)$ como

$$(x, y) \sim (x', y') \iff x \perp y' = x \perp y \in M(K)$$

Gracias al teorema de cancelación de Witt (Teorema 1.25) esta relación es de equivalencia. Denotaremos como $Groth(M(K)) = M(K) \times M(K) / \sim$ el grupo de *Grothendieck* de $M(K)$, luego gracias al producto $\otimes$ podemos convertirlo en un anillo conmutativo induciendo el

siguiente producto:

$$(x, y)(x', y') = (x \otimes x' \perp y \otimes y', y \otimes x' \perp x \otimes y')$$

De este modo, denotamos como $\widehat{W}(K) = Groth(M(K))$ al anillo de *Grothendieck-Witt* de formas cuadráticas sobre el cuerpo K .

Ahora considerando el morfismo $dim : M(K) \rightarrow \mathbb{Z}$ y extendiéndolo a $\widehat{W}(K)$ mediante la propiedad universal del monoide, obtenemos el siguiente morfismo

$$dim : \widehat{W}(K) \rightarrow \mathbb{Z}$$

El kernel de este morfismo lo denotamos por $\widehat{I}$ y lo llamamos el *ideal fundamental* de $\widehat{W}(K)$.

Con estas definiciones nos acompaña la siguiente proposición

Proposición 1.28 (Lam, 2005, II.1.2). $\widehat{I}$ es aditivamente generado por $\langle -1, a \rangle$

Ahora tomemos el símbolo $\mathbb{Z} \cdot \mathbb{H}$ como todos los espacios hiperbólicos y sus inversos aditivos (bajo la operación $\perp$) esto forma un ideal, luego podemos definir el siguiente cociente

Definición 1.29. Definimos el *anillo de Witt* como $W(K) = \widehat{W}(K) / \mathbb{Z} \cdot \mathbb{H}$.

Usando la proyección natural $\widehat{W}(K) \rightarrow W(K)$, definimos el *ideal fundamental* de $W(K)$ como la imagen imagen de $\widehat{I}$ vía dicha proyección.

Podemos notar la siguiente cadena de ideales

$$I^n(K) \subset \dots \subset I^2(K) \subset I(K) \subset W(K)$$

donde $I^n(K)$ es generado por las formas $\bigotimes_{i=1}^n \langle 1, a_i \rangle$ (Véase Lam, 2005, X, Proposition 1.2). Finalmente, podemos dar el resultado principal con respecto a los ideales fundamentales.

Teorema 1.30. Sea K un cuerpo tal que $2 \neq 0$. La forma $\langle \langle 1, 1 \rangle \rangle$ representa a f en K si y solo si $\langle \langle 1, 1, -f \rangle \rangle \equiv 0$ en $I^3(K) / I^4(K)$.

Demostración. Sea $f \in K$ representada por $\langle \langle 1, 1 \rangle \rangle$, por ahora denotemos $\pi := \langle \langle 1, 1 \rangle \rangle$,

como $f \in D(\pi)$, entonces $\pi \equiv f\pi$ esto por el Teorema de formas redondas (véase Lam, 2005, Chap X, appendix Round forms, Theorem 1.14).

Es necesario notar que $\langle\langle 1, 1, -f \rangle\rangle$ podemos escribirla como la siguiente suma ortogonal $\pi \perp -f\pi$ y por lo anterior, deducimos que $\langle\langle 1, 1, -f \rangle\rangle \cong \pi \perp -\pi$, lo que implica que $\langle\langle 1, 1, -f \rangle\rangle \equiv 0$ en $W(K)$ y por tanto $\langle\langle 1, 1, -f \rangle\rangle \in I^4(K)$.

Ahora bien. Si $\langle\langle 1, 1, -f \rangle\rangle \equiv 0$ en $I^3(K)/I^4(K)$, equivalentemente $\langle\langle 1, 1, -f \rangle\rangle \in I^4(K)$, como la dimensión de $\langle\langle 1, 1, -f \rangle\rangle$ es igual a 8 y la dimensión del espacio $I^4(K)$ es 16, esto implica que la forma $\langle\langle 1, 1, -f \rangle\rangle$ es hiperbólica (véase Lam, 2005 Chap. X, Hauptstanz 5.1), es decir que $\langle\langle 1, 1, -f \rangle\rangle \equiv 0$ en $W(K)$.

Como ya mencioné $\langle\langle 1, 1, -f \rangle\rangle \cong \pi \perp -f\pi$ luego $\pi \equiv f\pi$ en $W(K)$. Esto implica que $D_K(\pi) = D_K(f\pi)$ y como $1 \in D_K(\pi)$, entonces $1 \cdot f \in D_K(\pi)$ i.e. f es representado por $\langle\langle 1, 1 \rangle\rangle$ en K . $\square$

Capítulo 2

Cuerpos de funciones en una variable

En este capítulo vamos a establecer las bases de la teoría de funciones algebraicas sobre un cuerpo K , donde trabajaremos de aquí en adelante, esto para lograr nuestro objetivo y dar el desarrollo de la demostración de la conjetura de Pfister. Para ello nos basaremos en el texto de Stichtenoth, [2009](#) del cual se van a extraer las definiciones cruciales. Cabe mencionar que algunas definiciones no se encuentran en dicho texto ya que fueron parte del trabajo de traducción desde el lenguaje geométrico al lenguaje algebraico.

2.1. Cuerpo de funciones algebraicas F/K

Definición 2.1. Un *cuerpo de funciones algebraicas* F/K de una variable sobre K es una extensión de cuerpos $F \supseteq K$ tal que F es una extensión finita algebraica de $K(x)$ para algún elemento $x \in F$ que es trascendente sobre K .

Para abreviar, nos referiremos a F/K simplemente como un cuerpo de funciones algebraicas. El conjunto $\tilde{K} := \{z \in F \mid z \text{ es algebraico sobre } K\}$ es claramente un subcuerpo de F , ya que las sumas, productos e inversos de elementos algebraicos también son algebraicos. $\tilde{K}$ se denomina *cuerpo de constantes de F/K* . Tenemos $K \subseteq \tilde{K} \subsetneq F$, y es evidente que $F/\tilde{K}$ es un cuerpo de funciones algebraicas sobre $\tilde{K}$. Decimos que K es *algebraicamente cerrado en F* (o K es el cuerpo de constantes completo de F) si $\tilde{K} = K$. Si se cumple que K es algebraicamente cerrado sobre F , entonces decimos que F es *regular* sobre K .

Ejemplo 2.2. El ejemplo más simple de un cuerpo de funciones algebraico es el *cuerpo de funciones racionales*; F/K se llama *racional* si $F = K(x)$ para algún $x \in F$ trascendental

sobre K . Cada elemento $0 \neq z \in K(x)$ tiene una única representación

$$z = a \cdot \prod_i p_i(x)^{n_i},$$

donde $0 \neq a \in K$, los polinomios $p_i(x) \in K[x]$ son mónicos, distintos dos a dos e irreducibles y $n_i \in \mathbb{Z}$.

Un cuerpo de funciones F/K se representa a menudo como una simple extensión algebraica de un cuerpo de funciones racionales $K(x)$; es decir, $F = K(x, y)$ donde $\phi(y) = 0$ para algún polinomio irreducible $\phi(T) \in K(x)[T]$. El siguiente lema nos permite ver algo que no parece obvio a simple vista

Lema 2.3. [Stichtenoth, 2009, Corrolary 1.1.16] *El cuerpo de constantes $\tilde{K}$ de F/K es una extensión finita de K .*

Desde ahora, todas las veces que se trabaje sobre un cuerpo de funciones algebraicas F/K asumiremos que este es regular.

Los siguientes resultados serán fundamentales para más adelante y son una linda forma de entrelazar las cosas que hasta ahora hemos visto.

Lema 2.4. *Sea K un cuerpo con $\text{char}(K) \neq 2$ y sea F/K un cuerpo de funciones algebraicas sobre K , entonces el espacio (F^n, q) con $q = x_1^2 + \dots + x_n^2$ es cuadrático regular.*

Demostración. Vamos a calcular el complemento ortogonal $(F^n)^\perp$. Por definición sabemos que

$$(F^n)^\perp = \{f \in F^n \mid B(f, F^n) = 0\}$$

Si $B(f, g) = 0$ para todo $g \in F$, quiere decir que

$$\begin{aligned} B(f, g) = 0 &\iff \sum_{i=1}^n (f_i + g_i)^2 - \sum_{i=1}^n f_i^2 - \sum_{i=1}^n g_i^2 = 0 \\ &\iff 2 \sum_{i=1}^n f_i g_i = 0 \\ &\iff f_i = 0 \end{aligned}$$

Este ultimo paso es gracias a que podemos elegir $g_i \neq 0$ y $g_j = 0$ para $j \neq i$ y como la característica es distinta de dos, solo queda que $f_i = 0$. $\square$

Teorema 2.5. *Sea K un cuerpo con $\text{char}(K) \neq 2$ y F/K un cuerpo de funciones algebraicas sobre K . Si $s(K) < \infty$ entonces $p(F) \leq s(K) + 1$.*

Como $s(K) = n < \infty$ tenemos que $-1 = \sum_{i=1}^n a_i^2 \in K \subseteq F$ luego tenemos que

$$\begin{aligned} a_1^2 + \dots + a_n^2 = -1 &\iff a_1^2 + \dots + a_n^2 + 1 = 0 \\ &\iff (a_1 c)^2 + (c b_n)^2 + c^2 = 0 \\ &\iff x_1^2 + \dots + x_n^2 + x_{n+1}^2 = 0, \quad x_i \in K \subseteq F \end{aligned}$$

y como F es cuadrático regular, la forma $x_1^2 + \dots + x_{n+1}^2$ es isotrópica y por ende, universal (Teorema 1.21). Continuando con las definiciones elementales.

2.2. Anillos de valuación de F/K

Definición 2.6. Un anillo de valuación de un cuerpo de funciones algebraicas F/K es un anillo $\mathcal{O} \subseteq F$ con las siguientes propiedades

$$K \subsetneq \mathcal{O} \subsetneq F$$

$$\forall z \in F \text{ se tiene que } z \in \mathcal{O} \text{ o } z^{-1} \in \mathcal{O}$$

Cabe señalar que un anillo de valuación $\mathcal{O}$ de un cuerpo de funciones algebraicas, es también un anillo de valuación discreta, esto ya que tenemos las siguientes proposiciones.

Proposición 2.7 (Proposición 1.1.5, Stichtenoth, 2009). *Sea $\mathcal{O}$ un anillo de valuación del cuerpo de funciones F/K entonces se tiene lo siguiente:*

- a) $\mathcal{O}$ es un anillo local i.e. Tiene un unico ideal maximal $P = \mathcal{O} \setminus \mathcal{O}^*$
- b) Sea $0 \neq x \in k$ entonces $x \in P \iff x^{-1} \notin \mathcal{O}$

Además de esa proposición, tenemos el siguiente teorema

Teorema 2.8 (Teorema 1.1.6, Stichtenoth, 2009). Sea $\mathcal{O}$ un anillo de valuación del cuerpo de funciones F/K y sea P el único ideal maximal, se cumple que:

- P es principal
- Si $P = t\mathcal{O}$ entonces cada $0 \neq z \in K$ tiene una única representación de la forma $z = t^n u$ con n un entero y u una unidad
- $\mathcal{O}$ es un DIP.

El concepto de anillo de valuación, como su nombre lo indica está muy relacionado con el concepto de valuaciones, el cual procederemos a definir.

Definición 2.9. Una valuación discreta en F/K es una función $v : F \rightarrow \mathbb{Z} \cup \{\infty\}$ con las siguientes propiedades:

1. $v(f) = \infty \Leftrightarrow f = 0$
2. $v(fg) = v(f) + v(g)$ para todo $f, g \in F$.
3. $v(f + g) \geq \min\{v(f), v(g)\}$ para todo $f, g \in F$.
4. Existe un elemento $z \in F$ con $v(z) = 1$.
5. $v(a) = 0$ para todo $0 \neq a \in K$.

Lema 2.10 (Stichtenoth, 2009, Lemma 1.1.11). Sea v una valuación discreta de F/K y sean $f, g \in F$ con $f \neq g$, entonces $v(f + g) = \min\{v(f), v(g)\}$

2.3. Lugares de un cuerpo de Funciones algebraicas

Definición 2.11. a) Un lugar P de un cuerpo de funciones F/K es el ideal maximal de algún anillo de valuación $\mathcal{O}$ de F/K . Todo elemento $t \in P$ tal que $P = t\mathcal{O}$ se llama *Uniformizante*.

b) $\mathbb{P}_F = \{P \mid P \text{ es un lugar de } F\}$

Si $\mathcal{O}$ es un anillo de valuación de F/K y P es su ideal maximal, entonces $\mathcal{O}$ viene únicamente determinado por P , a saber $\mathcal{O} = \{z \in F \mid z^{-1} \notin P\}$ (Véase 2.7). De este modo $\mathcal{O}_P := \mathcal{O}$ es llamado, *el anillo de valuación del lugar P*

Con esto en mente, podemos definir una valuación en un anillo de valuación de un cuerpo de funciones, más formalmente:

Definición 2.12. Un lugar $P \in \mathbb{P}_F$ le asociamos una función $v_P : F \rightarrow \mathbb{Z} \cup \{\infty\}$ se sigue: Elija un parametro uniformizante t de P . Entonces todo $0 \neq z \in F$ tiene una única representación $z = t^n u$ con n entero y u unidad luego $v_P(z) := n$, dicha función se llama *valuación en P* y $v_P(0) := \infty$

El siguiente resultado será sumamente útil.

Teorema 2.13 (Stichtenoth, 2009, Theorem 1.3.1). *Sea F/K un cuerpo de funciones algebraicas, $P_1, \dots, P_n \in \mathbb{P}_F$ lugares distintos dos a dos de F/K , $f_1, \dots, f_n \in F$ y $r_1, \dots, r_n \in \mathbb{Z}$. Entonces existe algún $f \in F$ tal que*

$$v_{P_i}(f - f_i) = r_i \text{ para } i = 1, \dots, n.$$

Con esto tenemos el siguiente teorema

Teorema 2.14 (Stichtenoth, 2009, Theorem 1.1.13). *Sea F/K un cuerpo de funciones algebraicas.*

a) *Para un lugar $P \in \mathbb{P}_F$, la función v_P (Definición 2.12) es una valuación discreta de F/K más aún tenemos*

$$\mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0\}$$

$$\mathcal{O}_P^* = \{z \in F \mid v_P(z) = 0\}$$

$$P = \{z \in F \mid v_P(z) > 0\}$$

b) *Un elemento $x \in F$ es un primo en P si y solo si $v_P(x) = 1$*

c) *Conversamente, supongamos que v es una valuación discreta de F/K . Entonces el*

conjunto $P := \{z \in F \mid v_P(z) > 0\}$ es un lugar de F/K y $\mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0\}$ su correspondiente anillo de valuación

Definición 2.15. Sea $P \in \mathbb{P}_F$. Denotamos por $\mathcal{F}_P := \mathcal{O}_P/P$ al cuerpo de clases residuales de P . El mapeo

$$\begin{aligned} F &\rightarrow \mathcal{F}_P \cup \{\infty\} \\ x &\mapsto f + P := f(P) \end{aligned}$$

lo llamaremos *mapeo de clases residuales*. También definiremos el *grado de un lugar* como $\deg(P) = [\mathcal{F}_P : K]$

Relacionando esta definición junto con la de formas cuadráticas, podemos definir lo siguiente: sea una forma cuadrática definida $\varphi = \langle a_1, \dots, a_n \rangle$ sobre el anillo $\mathcal{O}_P$ para algún lugar $P \in \mathbb{P}_F$, podemos definir su reducción modulo P de la siguiente forma: $\bar{\varphi} = \langle \bar{a}_1, \dots, \bar{a}_n \rangle$ en $\mathcal{F}_P$, con ello tenemos el siguiente lema.

Lema 2.16 (Elman y Lam, 1976, Lemma 15.5). Sea K un cuerpo de característica distinta de 2. Sea F/K un cuerpo de funciones algebraicas, sea $P \in \mathbb{P}_F$ y t un parámetro uniformizante de P . Sea φ y ψ dos formas cuadráticas sobre $\mathcal{O}_P$ tales que las formas residuales $\bar{\varphi}$ y $\bar{\psi}$ son anisotrópicas sobre el cuerpo residual $\mathcal{F}_P$, entonces $\varphi_F \perp t\psi_F$ es anisotrópica en F .

Podemos continuar definiendo conceptos.

Definición 2.17. Sea F/K un cuerpo de funciones algebraicas y sea $P \in \mathbb{P}_F$.

1. Diremos que P es un *lugar K -racional* si y solo si

$$\mathcal{O}_P/P \cong K.$$

2. Sea $f \in F/K$ se dirá *definida* en P si y solo si $f \in \mathcal{O}_P$. Si $v_P(f) > 0$ diremos que P es un *cero de grado* $v_P(f)$, si $v_P(f) < 0$, diremos que es un *polo de orden* $-v_P(f)$.

Denotaremos el subconjunto de $\mathbb{P}_F$ compuesto por los lugares K -racionales como $F(K) = \{P \in \mathbb{P}_F \mid P \text{ es un lugar } K\text{-racional}\}$

Proposición 2.18 (Stichtenoth, 2009, Chap I, Corollary 1.3.4). *En un cuerpo de funciones algebraicas F/K todo elemento $0 \neq f \in F$ tiene finitos ceros y polos.*

2.4. Divisores

Definición 2.19. 1. El *Grupo de divisores de F/K* es definido como el (aditivamente hablando) grupo libre abeliano cuyos generadores son los lugares de F/K ; es Denotado por $Div(F/K)$. Los elementos de $Div(F/K)$ son llamados *divisores* de F/K . En otras palabras un divisor es una suma formal de la forma:

$$D = \sum_{P \in \mathbb{P}_F} n_P P \text{ con } n_P \in \mathbb{Z}, \text{ con casi todos los } n_P = 0$$

Denotaremos por $D_+ := \{\sum_{P \in \mathbb{P}_F} n_P P \mid n_P \geq 0\}$ del mismo modo con $D_- = \{\sum_{P \in \mathbb{P}_F} n_P P \mid n_P \leq 0\}$

2. El *soporte* de D es definido como

$$Supp D := \{P \in \mathbb{P}_F \mid n_P \neq 0\}$$

3. Un divisor de la forma $D = P$ con $P \in \mathbb{P}_F$ se llamará *Divisor primo*.

4. Dos divisores $D = \sum n_P P$ y $D' = \sum n'_P P$ se suman coeficiente a coeficientes, es decir

$$D + D' = \sum (n_P + n'_P) P.$$

5. El elemento *cero* del grupo de divisores $Div(F)$ es el divisor de la forma

$$0 := \sum_{P \in \mathbb{P}_F} r_P P, \text{ con todos } r_P = 0$$

6. Para $Q \in \mathbb{P}_F$ y $D = \sum n_P P \in Div(F)$ definimos $v_Q(D) := n_Q$, de este modo

$$Supp(D) = \{P \in \mathbb{P}_F \mid v_P(D) \neq 0\} \text{ y } D = \sum_{P \in Supp(D)} v_P(D) \cdot P$$

7. Un orden parcial en $Div(F)$ es definido por

$$D_1 \leq D_2 :\iff v_P(D_1) \leq v_P(D_2) \text{ para todo } P \in \mathbb{P}_F$$

8. Un Divisor $D \geq 0$ se llama *efectivo*. Un divisor D tal que $v_P(D) \in \{0, 1\}$ para todo $P \in \mathbb{P}_F$ se llama *reducido*. El *grado* de un divisor es definido como

$$\deg D := \sum_{P \in \mathbb{P}_F} v_P(D) \cdot \deg P$$

9. El conjunto de los divisores de grado 0, se denotará como $Div^0(F/K)$

En relación a los ceros y polos de funciones $x \in F/K$ tenemos las siguientes definiciones.

Definición 2.20. Sea $f \in F^\times$ y denotamos $\mathcal{Z}$ (Resp. $\mathcal{N}$) el conjunto de ceros (Resp. polos) de x en $\mathbb{P}_k$, Entonces podemos definir los siguientes conceptos:

1. $div_0^K(f) := \sum_{P \in \mathcal{Z}} v_P(f)P$ se llama el divisor ceros de f
2. $div_\infty^K(f) := \sum_{P \in \mathcal{N}} (-v_P(f))P$ se llama el divisor de polos de f
3. $div^K(f) := Div_0^K(f) - Div_\infty^K(f)$ El divisor principal de f
4. $div_D^K(f) := div^K(f) - D$ se llama El divisor relativo de f con respecto a D , para algún divisor $D \in Div(F/K)$.

Las constantes en $F^\times$ se caracterizan de la siguiente manera:

$$k \in K \iff div(k)^K = 0$$

Con estas definiciones podemos extraer el siguiente resultado

Definición 2.21. El conjunto de divisores

$$Princ(F/K) := \{div^K(f) \mid f \in F^\times\}$$

se llama *grupo de divisores principales* de F/K . Al siguiente cociente

$$Cl(F/K) := Div(F/K)/Princ(F/K)$$

Lo llamaremos *El grupo de clases* de F/K . Para un divisor $D \in Div(F/K)$, el correspondiente elemento en el grupo $Cl(F/K)$ se denota por $[D]$. Dos divisores $D, D' \in Div(F/K)$ diremos que son *equivalentes linealmente* (o solo equivalentes) y lo escribiremos

$$D \sim D'$$

si $[D] = [D']$; es decir que $D = D' + (x)$ para algún $x \in F \setminus \{0\}$. También denotaremos por $Cl^0(F/K)$ al subgrupo *de clases de divisores de grado cero* $Cl^0(F/K)$ definido por

$$Cl^0(F/K) := Div^0(F/K)/Princ(F/K).$$

Con todo esto podemos definir uno de los espacios más importantes de este trabajo.

Definición 2.22. Sea D un divisor del cuerpo de funciones algebraicas F/K . Denotaremos el *espacio de Riemann-Roch* de D como $\mathcal{L}(D)$ que viene dado por:

$$\mathcal{L}(D) = \{f \in F/K \mid div^K(f) \geq -D\} \cup \{0\}.$$

A los $f \in \mathcal{L}(D)$ los llamaremos *secciones globales respecto a D* .

Definición 2.23. Sea F/k un cuerpo de funciones algebraicas sobre un cuerpo de números k y sea $D \in Div(F/k)$. Diremos que una sección $\sigma \in \mathcal{L}(2D)$ es *no negativa* si y solo si para todo lugar $P \in \mathbb{P}_F$, al fijar un parametro uniformizante t_P y definir $u = t_P^{2v_P(D)}\sigma$, se cumple para toda incrustación $\tau : \mathcal{F}_P \rightarrow \mathbb{R}$ que $\tau(u(P)) \geq 0$.

Teorema 2.24. Sea K un cuerpo algebraicamente cerrado, sea F/K un cuerpo de funciones algebraicas. Entonces el grupo de clases $Cl^0(F/K)$ es un grupo de división.

Demostración. Sea J la variedad Jacobiana¹ de F/k . Recuerde de que J es un k -grupo algebraico tal que su grupo de $\bar{k}$ -puntos $J(\bar{k})$ es isomorfo al grupo $Cl^0(F/\bar{k})$ (Véase Milne, 1986, remark 7.7.). Por Mumford et al., 1974, Chap II, Question I, tenemos que $J(k)$ es un grupo divisible, ya que k es algebraicamente cerrado. Por lo tanto, $Cl^0(F/k)$ tambien es un

¹Véase la construcción en Milne, 1986

grupo divisible. □

Observación 2.25. Sea $A \in \text{Div}(F)$. Entonces

- a) $f \in \mathcal{L}(A)$ si y solo si $v_P(f) \geq -v_P(A)$ para todo $P \in \mathbb{P}_F$.
- b) $\mathcal{L}(A) \neq 0$ si y solo si existe un divisor $A' \sim A$ con $A' \geq 0$.

Proposición 2.26 (Stichtenoth, 2009, Lemma 1.4.6). Sea $D \in \text{Div}(F/K)$. Tenemos que:

- a) $\mathcal{L}(D)$ es un espacio vectorial sobre k de dimensión finita,
- b) Si D' es un divisor equivalente a D , entonces $\mathcal{L}(D) \cong \mathcal{L}(D')$ como k -espacios vectoriales.

Definición 2.27. Sea D un divisor de F/K y sea $\mathcal{L}(D)$ el espacio de Riemann-Roch asociado. Diremos que un el espacio $\mathcal{L}(D)$ está *generado por secciones globales* si cumple que: Existe un conjunto $\{f_i\}_{i \in \mathbb{N}}$ con $f_i \in \mathcal{L}(D)$ tal que $f_i \cdot t^{-m+1}$ genera a $\mathcal{O}_P$ como un F -espacio vectorial para algún parametro uniformizante $t \in P$, para $m = \min_{v_P(f_i) < 0} \{v_P(f_i)\}$ y para todo $P \in \mathbb{P}_F$.

Diremos que un divisor D de F/k es *amplio* si dado un entero n_0 tal que para todo divisor $Q \in \text{Div}(F)$ y $n \gg n_0$ se cumple que $\mathcal{L}(Q + nD)$ está generado por secciones globales.

Definición 2.28. Sea F/K un cuerpo de funciones algebraicas, sea $P \in \mathbb{P}_F$ un lugar y sea q una forma cuadrática sobre K . Dado un divisor D y una sección $\sigma \in \mathcal{L}(2D)$:

1. *Representación Local:* Diremos que la sección σ es representada localmente por q en el lugar P , si existen funciones $f_1, \dots, f_n \in F$ tales que:

$$\sigma = q(f_1, \dots, f_n)$$

y satisfacen que $v_P(f_i) \geq -v_P(D)$ para todo $i = 1, \dots, n$.

2. *Representación Global:* Diremos que la sección σ es representada globalmente por q , si existen funciones $f_1, \dots, f_n \in F$ tales que:

$$\sigma = q(f_1, \dots, f_n)$$

y satisfacen que $f_i \in \mathcal{L}(D)$ para todo $i = 1, \dots, n$.

Ahora, sea K un cuerpo cualquiera. Dado un F/K , sea $f \in F/K$, podemos realizar un breve cálculo sobre el divisor principal de f , separando los sumandos según su paridad:

$$\begin{aligned} \operatorname{div}^k(f) &= \sum j_i P_i \\ &= \sum (2m_i) P_i + \sum (2n_i + 1) P_i \\ &= -2 \sum (m'_i + n'_i) P_i + \sum 1 \cdot P_i = -2D + E, \end{aligned}$$

donde E es un divisor efectivo reducido y $D \in \operatorname{Div}(F/k)$, por lo que podemos deducir el siguiente hecho

Lema 2.29. *Sea F/K un cuerpo de funciones algebraicas y sea $f \in F$, entonces existen únicos $E, D \in \operatorname{Div}(F/K)$ con E efectivo reducido, tales que $\operatorname{div}^K(f) = E - 2D$*

Es decir que que un elemento $f \in F/K$ siempre lo podemos ver como una sección de un divisor D único, ya que $\operatorname{div}_{2D}^k(f) = E > 0$ lo que implica que $\operatorname{div}^k(f) \geq -2D$. Al ser unicos, tanto E como D , se vamos a asignar un nombre:

Definición 2.30. Sea F/K un cuerpo de funciones algebraicas sobre un cuerpo cualquiera K . Sean $E, D \in \operatorname{Div}(F/K)$ unicos tales que $\operatorname{div}(f) = E - 2D$ donde E es efectivo reducido, el divisor E lo denotaremos como *el divisor efectivo reducido de f* y D como *el divisor doblado de f* .

2.5. Control de polos o ceros en representaciones de sumas de cuadrados

Sea F un cuerpo de funciones algebraicas F/K tal que $2 \neq 0$. Sea f una suma de cuadrados en F , nos gustaría poder controlar los polos de las secciones al momento de descomponer en sumas de cuadrados. El siguiente resultado nos ayudará con ello.

Hipótesis 2.31 (Benoist, 2025). *Sea K un cuerpo infinito, con $2 \in K$. Sea F/K un cuerpo de funciones algebraicas regular. Fijemos $A \in \operatorname{Div}(F/K)$, con A amplio. Sea $f \in F$, una suma de $n \geq 3$ cuadrados en F , sea $D \in \operatorname{Div}(F/K)$ el divisor doblado de f , entonces*

existe $\ell_0 \in \mathbb{N}$ tal que $\forall \ell \geq \ell_0$ existe $\alpha \in \mathcal{L}(\ell A)$ y $\beta_1, \dots, \beta_n \in \mathcal{L}(D + \ell A)$ tales que

$$f\alpha^2 = \sum_{i=1}^n \beta_i^2$$

Este resultado es una combinación de dos resultados demostrados en Benoist, 2025. Específicamente la proposición 3.2, la que nos afirma la existencia de dichas secciones α_p y $\beta_{i,p}$ bajo condiciones de existencia de divisores $\mathcal{M}, \mathcal{P} \in Cl(F/K)$ y la proposición 4.2 del mismo texto, la cual nos garantiza que dichas condiciones se satisfagan (con $\mathcal{M} \equiv \mathcal{P} \equiv Id$).

En este trabajo, quedará marcada como hipótesis, ya que, al momento de entregar la presente tesis, no logramos entender del todo la demostración dada por Benoist y mucho menos redactarla en el lenguaje algebraico.

Ahora bien, en la Hipótesis 2.31, si fuese verdad que podemos elegir un α y un divisor amplio de grado cero A , tal que $div(\alpha) = \ell A$, al menos en el caso $F = K(t)$, se podría deducir el siguiente resultado.

Teorema 2.32 (J. Cassels, 1964, Theorem 1). *Sea K un cuerpo infinito de característica distinta de 2, sea $p(t) \in K[t]$ tal que es suma de $n \geq 3$ cuadrados en $K(t)$. Entonces $p(t)$ es suma de n cuadrados en $K[t]$*

De este hecho aun no estamos seguros. Pero de lo que si estamos seguros, es que en el caso $F = K(t)$, podemos controlar los ceros y los polos de las secciones de la representación de manera más fuerte.

2.6. Cambio de base

Sea F/K un cuerpo de funciones algebraicas y sea K' un cuerpo tal que $K \subseteq K'$, nos gustaría definir un cuerpo de funciones algebraicas sobre K' de modo que $F \subseteq F'$.

En nuestro caso, consideramos un cuerpo E que contenga a K' y a F como subcuerpos (donde $K = F \cap K'$ dentro de E). Definimos el composito de F y K' en E , denotado por $F' = FK'$, como el subcuerpo más pequeño de E que contiene a ambos (Véase figura 2.1). Es importante notar que, a priori, esta construcción parece depender del cuerpo ambiente E y de cómo F y K' están incrustados en él. Sin embargo, se puede demostrar que si la

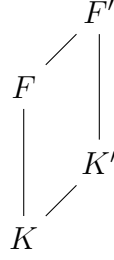


Figura 2.1: Diagrama de la extensión F'/K' sobre F/K

extensión F/K es regular, entonces: El composito $F' = FK'$ es un cuerpo de funciones algebraicas sobre K' . Para cualquier otro cuerpo E_1 que contenga copias isomorfas de F y K' , el composito formado en E_1 será K -isomorfo al formado en E . Esta propiedad de independencia es fundamental, ya que nos permite hablar de el cuerpo de funciones FK' obtenido por extensión de constantes, sin ambigüedad.

Aunque para dos cuerpos arbitrarios F y K' no siempre existe un contenedor común, el Teorema 8.4.2 de Villa Salvador, 2006 nos garantiza la existencia de un cuerpo de funciones L/ℓ que actúa como extensión de constantes. Más aún, dicho teorema asegura que esta construcción es única salvo K -isomorfismo, permitiéndonos definir el composito $F' = FK'$ de manera unívoca cuando la extensión original es regular.

Nos gustaría comprender que sucede con los lugares de la extensión F'/K' sobre F/K .

Definición 2.33. Sea la extensión F'/K' sobre F/K . Un lugar $P' \in \mathbb{P}_{F'}$ se dice que *yace* sobre $P \in \mathbb{P}_F$ si $P \subseteq P'$. Diremos que P' es una extensión de P o que P yace bajo P' , y escribiremos $P' \mid P$.

Proposición 2.34 (Stichtenoth, 2009, Proposition 3.1.4). *Sea F'/K' el cambio de base de F/K a K' . Supongamos que P (resp. P') es un lugar de F/K (resp. F'/K'), y sea $\mathcal{O}_P \subseteq F$ (resp. $\mathcal{O}_{P'} \subseteq F'$) su correspondiente anillo de valuación, v_P (resp. $v_{P'}$) su correspondiente valuación discreta. Entonces las siguientes aseveraciones son equivalentes:*

- 1) $P' \mid P$
- 2) $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$
- 3) Existe un entero $e \geq 1$ tal que $v_{P'}(x) = e \cdot v_P(x)$ para todos los $x \in F$.

Además, si una (y por lo tanto todas) de las condiciones anteriores se cumple, entonces:

$$P = P' \cap F \text{ y } \mathcal{O}_P = \mathcal{O}_{P'} \cap F.$$

Por esta razón, si P' es una extensión de P en F'/K' , el lugar P se llama también la restricción de P' . El entero e tal que $v_{P'}|_F = e \cdot v_P$, es llamado índice de ramificación de P' sobre P y lo denotaremos como $e(P' | P) := e$.

Con esto podremos definir un homomorfismo de grupos entre $Div(F)$ y $Div(F')$

Definición 2.35. Sea F'/K' una extensión de F/K . Para un lugar $P \in \mathbb{P}_F$ podemos definir la *conorma* con respecto a F'/F como el divisor

$$Con_{F'/F}(P) := \sum_{P'|P} e(P' | P) \cdot P' \in Div(F'/K')$$

Donde la suma recorre todos los $P' \in \mathbb{P}_{P'}$ que yacen sobre P . La conorma extiende un homomorfismo entre $Div(F)$ y $Div(F')$ de la siguiente manera

$$Con_{F'/F}(\sum n_P \cdot P) := \sum n_P \cdot Con_{F'/F}(P).$$

Capítulo 3

Sumas de cuadrados de funciones sobre un cuerpo real cerrado

En este capítulo estudiamos el siguiente resultado:

Teorema 3.1 (I, Witt, 1998,p.4). *Sea $F/\mathbb{R}$ un cuerpo de funciones algebraicas sobre $\mathbb{R}$, sea $f \in F/\mathbb{R}$ no negativa, entonces existen $g, h \in F/\mathbb{R}$ tales que $f = g^2 + h^2$*

La demostración original dada por Witt fue formulada utilizando el lenguaje de superficies de Riemann, por ejemplo aplicando teoremas de Abel-Jacobi. A fines de los 1960's una demostración alternativa de una generalización de este teorema a dimensiones cualesquieras por A. Pfister dejó claro que la afirmación sigue valido cuando se reemplazan los números reales por cualquier cuerpo real cerrado.

No obstante, en este capítulo nos hacemos el trabajo de reescribir la demostración original de Witt en un lenguaje algebraico, de tal forma que demuestre de manera directa la validez sobre cuerpos real cerrados. La motivación para este trabajo viene por una pregunta de mi profesor guía que está interesado en demostrar una afirmación similar al Teorema 3.1 para cuerpos de bases aún más generales que los cuerpos real cerrados, y donde ni la demostración por Pfister ni los métodos de lógica y teoría de modelos, permite una directa generalización, y por lo tanto naturalmente surgió la pregunta de hasta qué generalidad se puede algebraizar la demostración de Witt.

3.1. Existencia de lugares reales

En esta sección, buscaremos justificar la existencia de lugares R –racionales del cuerpo de funciones F/R sobre un cuerpo real cerrado R cuando F es formalmente real.

Como vamos a trabajar sobre cuerpos real cerrados, será útil contextualizar la siguiente definición.

Definición 3.2. Sea F/R un cuerpo de funciones algebraicas y R un cuerpo real cerrado. Diremos que $f \in F$ es *positiva definida* si y solo si $f(P) \geq 0$ para todo lugar R –racional P , donde $f \in \mathcal{O}_P$.

Observe que $f(P) \geq 0$ hace sentido considerando que $\mathcal{O}_P/P = R$.

Continuamos con un lema técnico, el cual nos ayudará para la demostración de la proposición siguiente.

Lema 3.3. Sea R un cuerpo real cerrado y F/R un cuerpo de funciones algebraicas formalmente real, entonces existe un orden $\leq$ tal que el cuerpo $(F, \leq)$ no es R –arquimediano.

Demostración. Sea $(F, \leq_1)$ un cuerpo R –arquimediano (en caso contrario no hay que probar nada).

Sabemos que F es una extensión algebraica finita del cuerpo $R(X)$ para un $X \in F$ trascendental sobre R . Por el Teorema del Elemento Primitivo, podemos ver a F como el cuerpo $R(X)(Y)$ con Y una raíz de un polinomio

$$f_X(T) \in R(X)[T]$$

mónico e irreducible.

Por el Teorema de Sturm (Véase Bochnak et al., 2013, Corollary 1.2.10), el número de raíces de $f_X(T)$ en cualquier clausura real de $(R(X), \leq_1)$ depende exclusivamente de los cambios de signo de la sucesión de Sturm finita de polinomios evaluados en X . Multiplicando por un denominador común adecuado, podemos asumir que estos determinantes de signo están dados por una familia finita de polinomios $\{q_1(X), \dots, q_k(X)\} \subset R[X]$.

Como R es real cerrado, sabemos que cada $q_j(X)$ se factoriza en factores lineales y/o polinomios cuadráticos irreducibles positivos (Véase Prestel, 2007, Lemma 3.4). Sea el conjunto $Ra := \{r_1, \dots, r_m\}$ de todas las raíces en R de los polinomios $q_j(X)$ para todo j .

Como X es trascendental sobre R , entonces $X \neq r_i$ para todo i .

Como $R(X) \subseteq F$, podemos restringir el orden $\leq_1$ a $R(X)$, formando así el cuerpo R -arquimediano $(R(X), \leq_1)$, por esta razón el elemento X está acotado por elementos de R . Definamos $a \in R$ de la siguiente manera: si el conjunto $\{r_i \in Ra \mid r_i <_1 X\}$ es no vacío, tomamos su máximo; en caso contrario, elegimos cualquier $a \in R$ tal que $a <_1 X$. Por el mismo argumento de acotamiento, elegimos un $b \in R$ tal que $X <_1 b$ y que no haya raíces de Ra en el intervalo (a, b) .

Finalmente, construyamos un nuevo orden en $R(X)$, denotado por $\leq_2$, tal que cumpla

$$a <_2 X <_2 a + r \quad \forall r \in R_{>0}.$$

Notamos que la posición relativa de X respecto a todas las raíces en Ra se mantiene inalterada. Como no hay raíces de los q_j en el intervalo (a, b) , los signos de los polinomios evaluados en X se mantienen con $\leq_2$ (por construcción); es decir que

$$\text{sgn}_{\leq_1}(q_j(X)) = \text{sgn}_{\leq_2}(q_j(X)) \quad \forall j.$$

Entonces, por el Teorema de Sturm, el polinomio $f_X(T)$ tiene la misma cantidad de raíces en la clausura real de $(R(X), \leq_2)$ que en la clausura real de $(R(X), \leq_1)$. En particular, tiene al menos una raíz, lo que nos dice que podemos extender el orden $\leq_2$ al cuerpo F .

Para concluir, observemos que bajo este nuevo orden $\leq_2$ extendido a F , el elemento $X - a$ es estrictamente positivo, pero menor que cualquier real positivo $r \in R_{>0}$. Por lo tanto, su inverso multiplicativo $(X - a)^{-1} \in F$ satisface que

$$(X - a)^{-1} >_2 r$$

para todo $r \in R$, lo que demuestra que el cuerpo $(F, \leq_2)$ no es R -arquimediano. □

Proposición 3.4. *Sea F/R un cuerpo de funciones algebraicas sobre un cuerpo real cerrado R . Si F es formalmente real, entonces admite al menos un lugar R -racional.*

Demostración. Como F es formalmente real, por el Lema 3.3, existe un orden en F que

no es R -arquimediano. Sea $\leq$ dicho orden. Definamos el siguiente conjunto

$$O = \{f \in F \mid \exists r \in R_{>0} ; -r \leq f \leq r\}.$$

Veamos ahora unas cuantas características que tiene este conjunto

1. Es claramente un anillo,
2. $O \subsetneq F$. Si $O = F$, entonces el cuerpo F es ordenado y R -arquimediano, no hay que olvidar que este es una extensión de R . Por el Lema 3.3 y la Observación 1.10 R es maximal con la propiedad de arquimedes. Por lo que $R = F$. Contradicción ya que F contiene un elemento trascendental sobre R .
3. $R \subsetneq O$. Notamos que $R \subset O$ por construcción. Ahora sea $f \in F - \{R\}$ tal que $f \notin O$, sin pérdida de generalidad nos dice que

$$f > r \forall r \in R_{>0}.$$

Por lo que $f > 1$ eso quiere decir que $f^{-1} < 1$ por lo que $f^{-1} \in O$.

Ahora sea $z \in F$, ya vimos que si $z \notin O$ entonces $z^{-1} \in O$, por lo que O es un anillo de valoración de F/R (definición 2.6). Ahora aplicamos la Proposición 2.7, el Teorema 2.8 y el Teorema 2.14 para concluir que existe un $P \in \mathbb{P}_F$ tal que $\mathcal{O}_P = O$. Debemos notar que si F es ordenado, entonces el anillo $\mathcal{O}_P$ también. Por lo que podemos inducir un orden en $\mathcal{O}_P/P = \mathcal{F}_P$ de la siguiente forma: Sean $a(P) \in \mathcal{O}_P/P$ es positivo ($a(P) \geq 0$) si existe un representante $a \in \mathcal{O}_P$ tal que

$$0 \leq a$$

esto por la forma en la que fue definido $\mathcal{O}$. Por lo que $\mathcal{F}_P = \mathcal{O}_P/P$ es un cuerpo ordenado. Es sabido que el cuerpo residual $\mathcal{F}_P$ para un lugar de F/R es una extensión algebraica de R , pero como R es real cerrado sus únicas extensiones algebraicas son R mismo y $R(i)$, es decir que $\mathcal{F}_P$ es igual a R o $R(i)$, pero ya vimos que $\mathcal{F}_P$ es ordenado, esto nos dice que $\mathcal{F}_P \neq R(i)$ ya que $R(i)$ no es ordenado, por ende $\mathcal{F}_P = R$. Podemos concluir que P es un lugar R -racional. $\square$

3.2. Estudio del nivel y divisores de F/R

Ya justificada la existencia de lugares R -racionales en un cuerpo de funciones algebraicas formalmente real F/R sobre un cuerpo real cerrado, buscaremos dar un resultado que relacione el hecho de ser no formalmente real, con la no existencia de lugares R -racionales y así poder concluir una equivalencia (Teorema 3.10)

Primero comenzamos con un lema técnico.

Lema 3.5. *Sea F/R un cuerpo de funciones algebraicas $\mathcal{A} \in \text{Div}^0(F/R)$, entonces existe un $\mathfrak{X} \in \text{Div}^0(F(i)/R(i))$ tal que $[2\mathfrak{X} + \mathcal{A}] \equiv 0$ en $Cl^0(F(i)/R(i))$*

Demostración. Considerando la extensión de cuerpos $F(i)/R(i)$. Dado que $R(i)$ es algebraicamente cerrado, el grupo de clases $Cl^0(F(i)/R(i))$ es un grupo divisible, esto por el Teorema 2.24.

1. Sea $[\mathcal{A}]$ la clase del divisor $\mathcal{A}$ en el grupo $Cl^0(F(i)/R(i))$.
2. Como $Cl^0(F(i)/R(i))$ es divisible, para el entero 2 y la clase $[-\mathcal{A}]$, existe una clase de equivalencia $x \in Cl^0(F(i)/R(i))$ tal que:

$$2x = [-\mathcal{A}]$$

3. Por la definición de grupo de clases, podemos elegir un divisor $\mathfrak{X} \in \text{Div}^0(F(i)/R(i))$ tal que $[\mathfrak{X}] = x$.
4. Por la igualdad anterior tenemos que $[2\mathfrak{X} + \mathcal{A}] \equiv 0$ en $Cl^0(F(i)/R(i))$.

□

Ya podemos demostrar la siguiente proposición.

Proposición 3.6. *Sea R un cuerpo real cerrado, Sea F/R un cuerpo de funciones algebraicas. Sea $f \in F$ positiva definida, entonces existe un $A \in F(i)$, tal que $\text{div}(f) = \text{div}^{R(i)}(A) + \overline{\text{div}^{R(i)}(A)}$.*

Demostración. Sea $f \in F/R$ una función positiva definida. Ahora sea $\text{div}^R(f) = \text{div}^{R(i)}(f) + \overline{\text{div}^{R(i)}(f)}$ esto ya que f podemos verlo como una función en la extensión de cuerpos $F(i)/R(i)$ (Proposición 2.34).

Ahora sea la proyección canónica $\pi : \text{Div}^0(F(i)/R(i)) \rightarrow \text{Cl}(F(i)/R(i))$. Entonces podemos ver que $0 \equiv \pi(\text{div}^R(f)) \equiv \pi(\text{div}^{R(i)}(f) + \overline{\text{div}^{R(i)}(f)})$ en $\text{Cl}(F(i)/R(i))$, como π es un homomorfismo, tenemos que:

$$\begin{aligned} 0 &= \pi(\text{div}^{R(i)}(f) + \overline{\text{div}^{R(i)}(f)}) = \pi(\text{div}^{R(i)}(f)) + \pi(\overline{\text{div}^{R(i)}(f)}) = \pi(\text{div}^{R(i)}(f)) + \overline{\pi(\text{div}^{R(i)}(f))} \\ &\Rightarrow \text{Re}_{\overline{R}}(\pi(\text{div}^{R(i)}(f))) = 0 \end{aligned}$$

Es decir que $\pi(\text{div}^{R(i)}(f))$ es puramente $R(i)$ –imaginario en el grupo $\text{Cl}(F(i)/R(i))$. Como $\text{div}^{R(i)}(f) \in \text{Div}^0(F(i)/R(i))$ entonces por el Lema 3.5 existe $\mathfrak{X} \in \text{Div}^0(F(i)/R(i))$ tal que $2[\mathfrak{X}] + \pi(\text{div}^{R(i)}(f)) \equiv 0$ en $\text{Cl}(F(i))$. Dada la sobreyectividad de π , sea $D \in \text{Div}^0(F(i)/R(i))$ tal que $\pi(D) = \mathfrak{X}$, de este modo obtenemos que $2\pi(D) \equiv -\pi(\text{div}^{R(i)}(f))$.

A sabiendas de que $\pi(\text{div}^{R(i)}(f))$ es imaginario, podemos ver que $\overline{\pi(D)} \equiv \frac{1}{2}\pi(\text{div}^{R(i)}(f))$ por lo que $\pi(D) - \overline{\pi(D)} \equiv -\pi(\text{div}^{R(i)}(f))$ desarrollando los siguientes cálculos

$$\begin{aligned} \pi(\text{div}^{R(i)}(f)) + \pi(D) - \overline{\pi(D)} &\equiv 0 \\ \Rightarrow \pi(\text{div}^{R(i)}(f)) + D - \overline{D} &\equiv 0 \end{aligned}$$

Deducimos que existe $A \in F(i)$ tal que $\text{div}^{R(i)}(f) + D - \overline{D} = \text{div}^{R(i)}(A)$ finalmente podemos concluir lo pedido, ya que

$$\begin{aligned} \text{div}^{R(i)}(A) + \overline{\text{div}^{R(i)}(A)} &= [\text{div}^{R(i)}(f) + D - \overline{D}] + [\overline{\text{div}^{R(i)}(f)} + \overline{D} - D] \\ &= \text{div}^{R(i)}(f) + D - \overline{D} + \overline{\text{div}^{R(i)}(f)} + \overline{D} - D \\ &= \text{div}^{R(i)}(f) + D - D + \overline{\text{div}^{R(i)}(f)} + \overline{D} - \overline{D} \\ &= \text{div}^{R(i)}(f) + \overline{\text{div}^{R(i)}(f)} = \text{div}^R(f) \end{aligned}$$

□

Corolario 3.7. Sea R un cuerpo real cerrado, Sea F/R un cuerpo de funciones algebraicas. Sea $f \in F$ positiva definida. Si F es un cuerpo formalmente real, entonces $p(F) \leq 2$.

Demostración. Como $f \in F$ es positiva definida, por la Proposición 3.6, sabemos que $\text{div}(f) = \text{div}^{R(i)}(A) + \overline{\text{div}^{R(i)}(A)}$ para algún $A \in F(i)$. Esto nos dice que

$$f = l \cdot A \cdot \overline{A}$$

para algún $l \in R$, como F es formalmente real, entonces l debe ser positivo, es decir que

$$f = l[(a + ib)(a - ib)] = [(a\sqrt{l})^2 + (\sqrt{l}b)^2]$$

lo que concluye lo pedido. □

Con esto hemos probado que para cualquier extensión finita formalmente real L de $R(X)$ tenemos que $p(L) \leq 2$, aplicando el Teorema 3.5 de Becher y Van Geel, 2009 ((ii) $\Leftrightarrow$ (iii)), podemos deducir que dada una extensión L' finita no real de $R(X)$, entonces $s(L') \leq 2$, por lo que podemos deducir la siguiente proposición.

Proposición 3.8. *Sea R un cuerpo real cerrado y F/R un cuerpo de funciones algebraicas no formalmente real, entonces $s(F) \leq 2$.*

Viendo la contraposición lógica de la Proposición 3.4 y aplicando la Proposición 3.8, podemos concluir el resultado principal de esta sección.

Corolario 3.9. *Sea F/R un cuerpo de funciones algebraicas sobre un cuerpo real cerrado R . Si el conjunto de lugares R -racionales $F(R)$ es vacío, entonces -1 es suma de 2 cuadrados en F .*

Con esto ya podemos concluir el resultado principal de esta sección.

Teorema 3.10. *Sea R un cuerpo real cerrado y F/R un cuerpo de funciones algebraicas sobre R . Entonces $F(R) = \emptyset$ si y solamente si existen $h, g \in F$ tales que $-1 = h^2 + g^2$.*

Demostración. $\Rightarrow$) Esta implicación fue demostrada en el Corolario 3.9.

$\Leftarrow$) Por hipótesis existen $g, h \in F/R$ distintos, tales que $g^2 + h^2 = -1$, ahora asumamos que $F(R) \neq \emptyset$.

Sea $P \in F(R)$ y $\mathcal{O}_P$ su anillo de valuación asociado. Vemos que $v_P(-1) = 0$ ya que -1 es una función constante, por el Lema 2.10, esto implica que

$$0 = v_P(-1) = v_P(g^2 + h^2) = 2 \min\{v_P(g), v_P(h)\}$$

por lo que $v_P(g^2) \geq 0$ y $v_P(h^2) \geq 0$ con al menos uno nulo.

Con esto podemos concluir que $g(P)^2 + h(P)^2 = -1$ en $\mathcal{O}_P/P$ con al menos $g(P)$ o $h(P)$ no nulo. No debemos olvidar que P es un lugar R -racional, por lo que $\mathcal{O}_P/P$ es exactamente R , es decir que hemos demostrado que -1 es suma de dos cuadrados en R lo cual es una contradicción.

□

3.3. Cálculo del número de Pitágoras de F/R

Con los resultados preliminares ya probados, estamos en condiciones de poder demostrar que el número de Pitágoras de F/R es dos.

Teorema 3.11. *Sea F/R un cuerpo de funciones algebraicas sobre un cuerpo real cerrado R . Sea $f \in F$ una función positiva definida, entonces existen $g, h \in F$ tales que $f = g^2 + h^2$.*

Demostración. Primero sea $f \in F/R$ tal que $\text{div}^R(f) = 0$, entonces $f \in R$ y por la Proposición 1.7, concluimos que f es un cuadrado.

Ahora sea $f \in F/R$ tal que $\text{div}^R(f) \neq 0$ es decir una función no constante. Asumiendo que $F(R) = \emptyset$ el Teorema 3.10 nos dice que existen $w, t \in F/k$ tales que

$$-1 = w^2 + t^2. \quad (3.1)$$

Mientras que por el Teorema 3.6 sabemos que existe una función compleja $a+bi = A \in F(i)$ tal que su divisor complejo más su conjugado es exactamente el divisor de f , por lo que podemos realizar los siguientes cálculos

$$\begin{aligned} \text{div}^R(f) &= \text{div}^{R(i)}(A) + \overline{\text{div}(A)^{R(i)}} \\ \Rightarrow f &= A \cdot \bar{A} \cdot l \\ \Rightarrow f &= (a+bi)(\overline{a+bi}) \cdot l \\ \Rightarrow f &= [a^2 + b^2] \cdot l \end{aligned} \quad (3.2)$$

donde l es un elemento del cuerpo R , por lo que tenemos dos casos: si $l < 0$ o si $l > 0$.

Si $l < 0$ entonces $l = -1 \cdot |l|$, por lo que desde la Ecuación 3.2 y la Ecuación 3.1 tenemos

que

$$\begin{aligned}
 f &= [a^2 + b^2] \cdot l \\
 f &= [a^2 + b^2] \cdot |l| \cdot -1 \\
 f &= \left[\left(a\sqrt{|l|^2} \right)^2 + \left(b\sqrt{|l|^2} \right)^2 \right] \cdot -1 \\
 f &= \left[\left(a\sqrt{|l|^2} \right)^2 + \left(b\sqrt{|l|^2} \right)^2 \right] \cdot [w^2 + t^2]
 \end{aligned}$$

Finalmente por la identidad de los cuadrados de Euler (Lema 1.23) concluimos que f es suma de dos cuadrados en F .

Si $l > 0$ no hay problema ya que un elemento de R positivo es un cuadrado en R .

Ahora veamos el caso en que $F(R) \neq \emptyset$. Al igual que antes, desde la ecuación $\text{div}^R(f) = \text{div}^{R(i)}(A) + \overline{\text{div}(A)^{R(i)}}$ podemos desprender dos posibilidades

1. $l \cdot A \cdot \bar{A} = f$ si $l > 0$ entonces $\left(a\sqrt{|l|^2} \right)^2 + \left(b\sqrt{|l|^2} \right)^2 = f$
2. $l \cdot A \cdot \bar{A} = f$ si $l < 0$ entonces $-\left(\left(a\sqrt{|l|^2} \right)^2 + \left(b\sqrt{|l|^2} \right)^2 \right) = f$

Pero como estamos asumiendo que $F(R) \neq \emptyset$ gracias al Teorema 3.10, sabemos que F es un cuerpo formalmente real, por lo que la segunda opción no puede ocurrir, ya que f es positiva definida; por ende, solo puede ocurrir la primera opción, es decir que f es suma de dos cuadrados. □

Capítulo 4

Preliminares aritméticos

En este capítulo buscaremos dar la base conceptual de lo que será una parte esencial en la demostración del Teorema de Benoist, esto es el Principio local-global de Kato. Para ello deberemos introducir conceptos nuevos, los cuales nos ayudaran a entender esta parte de mejor manera.

4.1. Cuerpos p -ádicos

Definición 4.1. Sea K un cuerpo cualquiera, llamaremos a la función

$$|\cdot| : K \longrightarrow \mathbb{R}_+$$

valor absoluto de K si cumple las siguientes condiciones:

1. $|x| = 0 \Leftrightarrow x = 0$
2. $|xy| = |x||y| \forall x, y \in K$
3. $|x + y| = |x| + |y| \forall x, y \in K$

Además diremos que dicho valor absoluto $|\cdot|$ es *no arquimediano* en K si cumple la desigualdad

$$|x + y| \leq \max\{|x|, |y|\} \quad \forall x, y \in K.$$

En caso contrario diremos que es *arquimediano*.

Diremos que dos valores absolutos $|\cdot|_1$ y $|\cdot|_2$ en un cuerpo K son *equivalentes*, si existe un $a \in \mathbb{R}$ tal que $|b|_1 = |b|_2^a$ para todo $b \in K$.

Teorema 4.2 (E. Artin y Whaples, 1945, Teorema 1). Si tenemos n valuaciones $|\cdot|_v$ inequivalentes y no triviales de un cuerpo L cualquiera, un elemento α_v de L por cada valuación y $\epsilon > 0$

entonces podemos encontrar un elemento en L tal que

$$|\alpha - \alpha_v|_v \leq \epsilon \text{ para cada } v = 1, 2, \dots, n.$$

Podemos dar las siguientes definiciones.

Sea k un cuerpo y sea $|\cdot|$ un valor absoluto no arquimediano. Definamos los siguientes conjuntos:

- $\mathcal{O}_K = \{a : |a| \leq 1\}$
- $\mathfrak{p} = \{a : |a| < 1\}$

Con estos anillos, tenemos la siguiente definición:

Definición 4.3. Definimos como *el cuerpo de clases residuales de k* como el cociente $\mathcal{O}_K/\mathfrak{p}$. Además diremos que $|\cdot|$ es un valor absoluto *discreto* si el grupo $\mathcal{O}_K \setminus \mathfrak{p}$ es discreto.

Para continuar es necesario recordad el concepto de completitud. Por un lado un cuerpo K con un valor absoluto $|\cdot|$ no trivial, se dice completo si toda sucesión convergente es sucesión de Cauchy.

Por otro lado, dado un cuerpo K y un valor absoluto $|\cdot|$, podemos construir su completación con respecto al valor absoluto $|\cdot|$, denotada por $\hat{K}$.

En el caso $\mathbb{Q}$, gracias al Teorema de Ostrowski (Véase Gouvêa, 2020, Theorem 3.1.4) sabemos que los únicos valores absolutos no triviales son:

- en el caso no arquimediano son los valores absolutos p -ádicos $|x|_p = p^{-n}$ con n tal que $x = p^n j$ con $p \nmid j$ y $|0| = 0$,
- en el caso arquimediano, es el valor absoluto usual

$$|x|_\infty = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0 \end{cases}$$

Por lo que las únicas completaciones de $\mathbb{Q}$ serán con respecto a $|\cdot|_p$ denotadas por $\mathbb{Q}_p$ (en el caso no arquimediano) y $\mathbb{Q}_{|\cdot|_\infty} \cong \mathbb{R}$ en el caso arquimediano.

Para complementar, tenemos los siguientes resultados:

Proposición 4.4 (Gouvêa, 2020, Theorem 2.2.4). *Sea K un cuerpo de característica cero y sea Z la imagen de $\mathbb{Z}$ en K . Un valor absoluto $|\cdot|$ en K es no-archimédiano si y solo si $|a| \leq 1$ para todo $a \in Z$.*

Por lo que en el caso $\mathbb{Q}_p$ tenemos que $\mathcal{O}_{\mathbb{Q}_p} = \mathbb{Z}_p$ y por tanto el cuerpo residual de $\mathbb{Q}_p$ es $\mathbb{Z}/p\mathbb{Z}$ (Veáse Gouvêa, 2020, Corollary 4.2.5)

Con esto en mente, podemos introducir el concepto de cuerpos p -ádicos.

Definición 4.5. Sea K un cuerpo completo con respecto a un valor absoluto no archimédiano $|\cdot|$. Diremos que K es un cuerpo p -ádico si

1. K tiene característica cero
2. $|\cdot|$ es discreto.
3. El cuerpo de clases residuales es finito.

Podemos dar la siguiente caracterización:

Lema 4.6 (J. W. S. Cassels, 1986, XIII, Lema 1.1). *El cuerpo K con un valor absoluto $|\cdot|$ es un cuerpo p -ádico si y solo si es una extensión finita de $\mathbb{Q}_p$ para algún p .*

Y con respecto a las completaciones con respecto a valuaciones archimedianas tenemos el siguiente teorema:

Teorema 4.7 (J. W. S. Cassels, 1986, III, Theorem 1.1). *Sea k un cuerpo completo con respecto a una valuación archimédiana $|\cdot|$. Entonces k es (isomorfo a) $\mathbb{R}$ o $\mathbb{C}$ y $|\cdot|$ es equivalente al valor absoluto usual.*

Con esto claro, podemos introducir las siguientes notaciones.

Definición 4.8. Sea k un cuerpo de números y sea v un lugar. Denotaremos por Ω_k el conjunto de las valuaciones de k .

La completación de k con respecto a v la denotaremos como k_v . Si v es archimédiano como vimos, la podemos identificar como $k_v \cong \mathbb{R}$ o $k_v \cong \mathbb{C}$. Ahora si v es no archimédiano,

entonces denotamos como $k_v = k_p$ para el único primo p tal que k_p sea una extensión finita de $\mathbb{Q}_p$.

Para acortar lenguaje, llamaremos completaciones *diádicas* a k_2 .

Volviendo un poco atrás, específicamente al capítulo anterior. Dada una extensión k' de un cuerpo k , definimos la extensión de cuerpos de funciones algebraicas $F/k \subseteq F'/k'$ donde $F' = Fk'$ (salvo k -isomorfismo). Si tomamos $k' = k_v$ para algún lugar v de k tendremos las siguientes notaciones.

Definición 4.9. Sea k un cuerpo de números y v una valuación de Ω_k . Sea F/k un cuerpo de funciones algebraicas, si la valuación es no arquimediana, denotaremos por F_p al composito Fk_p para algún primo $p \in \mathbb{Z}$, si la valuación es arquimediana, simplemente escribiremos $F_{\mathbb{R}}$ o $F_{\mathbb{C}}$ dependiendo del caso.

En caso de una valuación v cualquiera denotemos el composito Fk_v como F_v y al cuerpo de funciones algebraicas F_v/k_v lo denominaremos como *el cambio de base de F/k a k_v* . Ahora sea el espacio $\mathcal{L}(D)$ para algún divisor de $D \in \text{Div}(F/k)$ y sea F_p/k_p el cambio de base de F/k a k_p , entonces denotaremos al espacio de Riemann-Roch sobre esta extensión como $\mathcal{L}_p(D)$ y en el caso arquimediano lo denotaremos como $\mathcal{L}_{\mathbb{R}}(D)$.

Ahora bien, puesto que $\mathcal{L}(D)$ es un k -espacio vectorial de dimensión finita, fijamos una k -base $\{\omega_1, \dots, \omega_n\}$ de $\mathcal{L}(D)$, la cual se extiende de manera natural a una k_v -base del espacio $\mathcal{L}_v(D)$ para cada lugar $v \in \Lambda$.

De este modo, cualquier elemento $\sigma \in L_v(D)$ se puede expresar de forma única como una combinación lineal $\sigma = \sum_{i=1}^n \alpha_i \omega_i$, donde $\alpha_i \in k_v$. Definimos la *norma máxima* de σ respecto a esta base fija, denotada por $\|\cdot\|_v$, como:

$$\|\sigma\|_v = \max_{1 \leq i \leq n} \{|\alpha_i|_v\}$$

donde $|\cdot|_v$ representa el valor absoluto en k_v asociado al lugar v .

En el caso que $k_v = \mathbb{R}$, se denotará por $\|\cdot\|$ al valor absoluto asociado a $F/\mathbb{R}$.

Es importante destacar que, si bien el valor numérico de $\|\sigma\|_v$ depende de la base elegida, la topología inducida por esta norma en $\mathcal{L}_v(D)$ es independiente de dicha selección. Debido a que $\mathcal{L}_v(D)$ es un espacio vectorial de dimensión finita sobre el cuerpo completo k_v , todas las normas de este tipo son equivalentes. Por lo tanto, definen el mismo sistema de vecindades topológicas.

Con esto podemos dar el siguiente resultado.

Lema 4.10. *Sea k un cuerpo de números y sea $v \in \Lambda \subset \Omega_k$ donde Λ es un subconjunto finito de lugares de k . Sea F/k un cuerpo regular de funciones algebraicas y sea D un divisor de F/k . Para cada $v \in \Lambda$, se $\sigma_v \in \mathcal{L}_v(D) \subset F_v$. Entonces para cada $\epsilon > 0$ existe un $\sigma \in \mathcal{L}(D)$ tal que $\|\sigma - \sigma_v\|_v < \epsilon$ para todo $v \in \Lambda$.*

Demostración. Sea $P \in \mathbb{P}_F$ y sea $r \in \mathbb{Z}$ tal que $r \geq -v_p(D)$, aplicamos el Teorema de aproximación débil en cuerpos de funciones algebraicas (Teorema 2.13) con esto conseguimos un $x \in F$ tal que $v_P(x - \sigma_v) = r$ y por la desigualdad triangular estricta tenemos que $v_P(x - \sigma_v) = \min\{v_P(x), v_p(\sigma)\}$. Ahora lo vemos por casos:

a) Si $v_p(\sigma_v) \geq v_p(x)$, entonces

$$v_P(x) = v_P(x - \sigma_v) = r \geq -v_P(D)$$

y por la Observación 2.25 tenemos que $x \in \mathcal{L}_v(D)$

b) El caso donde $v_P(x) \geq v_P(\sigma_v)$ es trivial ya que $v_P(\sigma_v) \geq -v_P(D)$,

Por lo que en cualquier caso tenemos que $x \in \mathcal{L}_v(D)$.

Ahora, debemos notar que el cuerpo de funciones F/k visto como un subconjunto de F_v/k_v es denso en dicha extensión de cuerpos bajo la topología inducida por k_v esto gracias al Teorema de Artin-Whaples (Teorema 4.2). Sea $\sigma \in F/k$ lo suficientemente cerca de x tal que $\|x - \sigma\|_v < \epsilon$ para todo $\epsilon > 0$ y sea $t \in P$ un parámetro uniformizante, sea $v_P(\sigma) = n$ y $v_P(x) = m$, entonces $\|t^m u_1 - t^n u_2\|_v < \epsilon$ lo que implica que $|m - n| < \delta_\epsilon$ pero como $m, n \in \mathbb{Z}$ tenemos que $v_P(\sigma) = n = m = v_P(x)$, luego $v_P(\sigma) = v_P(x) \geq -v_P(D)$ para todo lugar $P \in \mathbb{P}_{F_v}$, lo que implica que $\sigma \in \mathcal{L}_v(D)$. $\square$

4.2. Lema de Hensel y sus consecuencias

Lema 4.11 (Colmez, 2002, Proposition IV.1.15, (Lema de Hensel)). *Sea K un cuerpo completo con un valor absoluto no arquimediano $|\cdot|$. Si $f \in \mathcal{O}_K[X]$ y $a \in \mathcal{O}_K$ verifica que*

$$|f(a)| < |f'(a)|^2$$

entonces existe un $\tilde{\alpha} \in \mathcal{O}_K$ unico que verifica

$$|\tilde{\alpha} - \alpha| < \left| \frac{f(\alpha)}{f'(\alpha)} \right| \text{ y } f(\tilde{\alpha}) = 0.$$

Corolario 4.12. Sea K un cuerpo completo con un valor absoluto no arquimediano $|\cdot|$. Sea $f \in \mathcal{O}_K[X]$ un polinomio monico y sea $\bar{f}$ la reducci3n de f modulo $\mathfrak{p}$. Si $\bar{\alpha}$ es una raiz simple de $\bar{f}$ en $\mathcal{O}_k/\mathfrak{p}$ entonces existe un 3nico $\tilde{\alpha} \in \mathcal{O}_k$ tal que $\tilde{\alpha} + \mathfrak{p} = \bar{\alpha}$ y $f(\tilde{\alpha}) = 0$

Demostraci3n. Sea $\alpha \in \mathcal{O}_K$ tal que $\tilde{\alpha} + \mathfrak{p} = \bar{\alpha}$, como $\bar{f}(\bar{\alpha}) = 0$, entonces $f(\alpha) \in \mathfrak{p}$, lo que es equivalnete a decir que $|f(\alpha)| < 1$. Como $\bar{\alpha}$, es una raiz simple, esto implica que

$$f'(\bar{\alpha}) \neq 0 \Rightarrow f'(\bar{\alpha}) \notin \mathfrak{p} \Rightarrow |f'(\bar{\alpha})| = 1.$$

Luego el lema de Hensel nos dice que existe un 3nico $\tilde{\alpha} \in \mathcal{O}_K$ tal que

$$|\tilde{\alpha} - \alpha| \leq \left| \frac{f(\alpha)}{f'(\alpha)} \right| = |f(\alpha)|$$

y $f(\tilde{\alpha}) = 0$ adem3s como $|\tilde{\alpha} - \alpha| \leq |f(\alpha)| < 1$ entonces $\tilde{\alpha} - \bar{\alpha} \in \mathfrak{p}$

□

Antes de ver algunos resultados interesantes para $\mathbb{Q}_p$ y extenderlos a k_p con k un cuerpo de n3meros, vamos a demostrar unos lemas t3cnicos pero necesarios.

Lema 4.13. Sea $2 < p \in \mathbb{Z}$ un primo, entonces -1 en $\mathbb{F}_p$ es suma de cuadrados.

Demostraci3n. Primero definamos el siguiente homomorfismos de grupos

$$\begin{aligned} \phi : \mathbb{F}_p^* &\rightarrow \mathbb{F}_p^* \\ x &\mapsto x^2 \end{aligned}$$

Por el tercer teorema de isomorfia podemos tenemos el siguiente isomorfismo:

$$\mathbb{F}_p^*/Ker(\phi) \cong Im(\phi)$$

Es clave notar que $Ker(\phi) = \{1, -1\}$ entonces podemos desprender que $|Im(\phi)| = \frac{p-1}{2}$.

Ahora definamos el siguiente conjunto

$$A = \text{Im}(\phi) = \{x^2 | x \in \mathbb{F}_p^*\}$$

Con esto en mente notemos que $|A \cup \{0\}| = \frac{p+1}{2}$. Ahora definamos el siguiente conjunto

$$B = \{-1 - y^2 | y \in A \cup \{0\}\}$$

Notemos que $|B| = \frac{p+1}{2}$ luego $(A \cup \{0\}) \cap B \neq \emptyset$ por lo que, existe un $q \in A \cup \{0\}$ tal que

$$\begin{aligned} -1 - y^2 &= q \text{ con } q, y \in A \cup \{0\} \\ \Rightarrow -1 &= x^2 + y^2 \text{ con } x, y \in \mathbb{F}_p \end{aligned}$$

□

Corolario 4.14. Sea $\mathbb{F}_p$ para $2 < p \in \mathbb{Z}$ y sea $F/\mathbb{F}_p$ un cuerpo de funciones algebraicas, entonces $p(F) \leq 3$.

Demostración. Como -1 es suma de cuadrados, esto implica que existen a y b en $\mathbb{F}_p$ alguno no nulo tales que

$$\begin{aligned} a^2 + b^2 &= -1 \iff a^2 + b^2 + 1 = 0 \\ &\iff (ac)^2 + (cb)^2 + c^2 = 0 \\ &\iff x_1^2 + x_2^2 + x_3^2 = 0 \end{aligned}$$

Es decir, es equivalente a decir que la forma cuadrática $x_1^2 + x_2^2 + x_3^2$ es isotrópica en $\mathbb{F}_p$, luego como $\mathbb{F}_p \subset F$ y F es un cuerpo cuadrático regular (Lema 2.4) entonces la forma $\langle 1, 1, 1 \rangle$ es universal (Teorema 1.21). □

Proposición 4.15. La forma cuadrática $x_1^2 + x_2^2 + x_3^2$ es isotrópica en $\mathbb{Q}_p$ para $2 < p \in \mathbb{Z}$.

Por el Lema 4.13, -1 es suma de cuadrados en el cuerpo $\mathbb{F}_p$ cuando $p > 2$ el cual es el cuerpo residual de $\mathbb{Q}_p$, ahora definamos el polinomio

$$p(x) = x^2 + y^2 + 1 = 0$$

este polinomio tiene solución en $\mathbb{F}_p$, aplicando el Corolario 4.12, sabemos que este polinomio

tendrá raíces también en $\mathbb{Q}_p$, esto implica que -1 también es suma de cuadrados en $\mathbb{Q}_p$, equivalente a decir que la forma cuadrática $x_1^2 + x_2^2 + x_3^2$ es isotrópica.

Ahora, estos resultados los podemos extender a k un cuerpo de números de la siguiente manera.

Proposición 4.16. *Sea k un cuerpo de números y k_p sus completaciones p -ádicas. Entonces $s(k_p) \leq 2$ para todo lugar no diádico.*

Demostración. Por el Lema 4.6, tenemos que $\mathbb{Q}_p \subseteq k_p$ para algún $p > 2$. Por la Proposición 4.15 sabemos que $s(\mathbb{Q}_p) \leq 2$ entonces $s(k_p) \leq 2$ ($A \subseteq B \Rightarrow s(A) \leq s(B)$). $\square$

Ahora, analizando el caso faltante, tenemos la siguiente proposición:

Proposición 4.17 (Pfister, 1995, Charper 3, §1, Example 1.2(6)). *Sea k un cuerpo local diádico, entonces:*

$$s(k) = \begin{cases} 1 & \text{para } \sqrt{-1} \in k, \\ 2 & \text{para } [k : \mathbb{Q}_2] \text{ par, } \sqrt{-1} \notin k, \\ 4 & \text{para } [k : \mathbb{Q}_2] \text{ impar} \end{cases} \quad (4.1)$$

Uno de los Teoremas más importantes en el sentido de representaciones, es el siguiente, ya que antes del Teorema de Kato, este principio local global fue la herramienta fundamental en el trabajo de representaciones en formas cuadráticas.

Teorema 4.18 (Hasse-Minkowski). *Sea q una forma cuadrática sobre un cuerpo de números k . Entonces q representa a 0 en k si y sólo si para todo lugar v de k la forma cuadrática q_v representa a 0 en k_v .*

Con estos Teoremas ya podemos dar unos cuantos resultados para acotar el número de Pítagoras de algún cuerpo de funciones.

Proposición 4.19. *Sea k un cuerpo de números no real, tenemos que, e_p o f_p es par, para todo lugar diádico si y solo si $p(F) \leq 3$*

Demostración. Sea p un lugar diádico arbitrario de k . Sabemos que el grado local está dado por $[k_p : \mathbb{Q}_2] = e_p f_p$. Si alguno de ellos es par, entonces el grado local $[k_p : \mathbb{Q}_2]$ es par.

Por la Proposición 4.17, si este grado es par, entonces el nivel local puede ser $s(k_p) = 1$ (si $\sqrt{-1} \in k_p$) o $s(k_p) = 2$ (si $\sqrt{-1} \notin k_p$). En cualquier caso, tenemos que $s(k_p) \leq 2$ para todo lugar diádico. Como para todo lugar no diádico v ya demostramos que $s(k_v) \leq 2$ (Proposición 4.16), el Teorema de Hasse-Minkowski nos permite concluir que el nivel global cumple $s(k) \leq 2$. Finalmente, por el Teorema 2.5, concluimos que $p(F) \leq s(k) + 1 \leq 3$.

Supongamos que $p(F) \leq 3$. Como F es una extensión de k , sabemos que el nivel no aumenta al restringirnos al cuerpo base, por lo que $s(k) \leq s(F) \leq p(F) \leq 3$. Dado que el nivel de un cuerpo es siempre una potencia de 2 (véase Lam, 2005, Chap XI, Theorem 2.2), las únicas opciones posibles son $s(k) = 1$ o $s(k) = 2$; en consecuencia, $s(k) \leq 2$.

Aplicando el Teorema de Hasse-Minkowski, esto implica que $s(k_p) \leq 2$ para todo lugar diádico p . Observando la Proposición 4.17, la única forma de que el nivel local no sea 4 es que el grado local $[k_p : \mathbb{Q}_2]$ no sea impar. Por ende, $[k_p : \mathbb{Q}_2] = e_p f_p$ debe ser par para todo lugar diádico, lo que concluye la demostración. $\square$

Proposición 4.20. *Sea k un cuerpo de números no real. Sea F/k un cuerpo de funciones algebraicas sobre k , entonces $p(F) \leq s(k) + 1 \leq 5$*

Demostración. Sea k no real, es decir que $s(k) < \infty$. Al ser no real, no tenemos ninguna incrustación de k a $\mathbb{R}$, por lo que no hay completaciones reales de este cuerpo de números. Gracias a la Proposición 4.16 sabemos que $s(k_p) \leq 2$ para todo lugar no diádico. Ahora sea k_p una completación diádica, por la caracterización de cuerpos p -ádicos, tenemos que $\mathbb{Q}_2 \subseteq k_p$, lo que implica $s(k_p) \leq s(\mathbb{Q}_2) = 4$.

Finalmente por el Teorema de Hasse-Minkowski tenemos que $s(k) \leq 4$. Por el Teorema 2.5 podemos concluir que $p(F) \leq s(k) + 1 \leq 5$. $\square$

Capítulo 5

Sumas de cuadrados de funciones sobre un cuerpo de números

Como bien se mencionó en la Introducción (4), en este capítulo buscaremos mostrar la relación y los paralelismos entre la demostración que dio Pourchet sobre la conjetura de Pfister en el caso del cuerpo de funciones racionales $k(t)$ sobre un cuerpo de números k (desde ahora usaremos k para denotar un cuerpo de números) y la demostración de Benoist de la conjetura en el caso de un cuerpo de funciones algebraicas F/k cualquiera. Para ello daremos un breve bosquejo de la demostración de Pourchet.

- i) En primera instancia, Pourchet demuestra un principio local global de la forma: un polinomio es suma de 4 cuadrados si y solo si es suma de 4 cuadrados en $k_v[t]$ para todo lugar $v \in \Omega_k$. Considerando el hecho que los polinomios positivos son suma de 5 cuadrados y no de 4 cuadrados en general, el lector atento ya se da cuenta que Pourchet no aplico este principio directamente a un polinomio $f \in k[t]$ no negativo directamente. En efecto, la parte mas intrincada del trabajo de Pourchet era su demostración que es posible de restar de f el cuadrado de otro polinomio g , tal que $f - g^2$ es localmente una suma de 4 cuadrados (y pues globalmente de 4 cuadrados).
- ii) Sea $f \in k[t]$ un polinomio positivo de grado par $2n$. Para justificar la existencia de un polinomio $g \in k[t]$ tal que $f - g^2$ es suma de 4 cuadrados en $k_v[t]$ para cada lugar $v \in \Omega_k$, Pourchet observó primero que para cada lugar v de k se encuentra un $g_v \in k_v[t]$ tal que $f - g_v^2$ es una suma de 4 cuadrados en $k_v[t]$, o en otras palabras que f es una suma de 5 cuadrados en $k_v[t]$ para cada lugar v de k .
- iii) Con el fin de reemplazar los polinomio $g_v \in k_v[t]$ por un único $g \in k[t]$, Pourchet aprovecha que para todos salvo finitos lugares v de k , la condición de ser suma de

4 cuadrados en $k_v[t]$ es una condición trivial. Por lo tanto basta con una aproximación simultánea de g_v en las métricas v -ádicas por un polinomio $g \in k[t]$, que es posible gracias al teorema de aproximación débil aplicado a los coeficientes de los finitos g_v . Para que esa aproximación débil resulte en lo deseado, Pourchet demuestra el ingrediente más importante, que variaciones v -ádicas suficientemente pequeñas de un polinomio en $k_v[t]$ que es suma de 4 cuadrados, siguen siendo sumas de 4 cuadrados.

Lo que buscaremos probar en esta sección, es el siguiente Teorema.

Teorema 5.1 (Benoist, 2025). *Sea k un cuerpo de números real. Sea F/k un cuerpo de funciones algebraico regular sobre k , si $f \in F$ es positiva definida, entonces f es suma de 5 cuadrados en F .*

En este contexto es necesario notar lo siguiente: por la Proposición 4.16, tenemos que la forma $\langle 1, 1, 1 \rangle$ es isótropica en k_p , para cualquier primo $p > 2$, por lo que también lo es en F cuando F es un cuerpo de funciones algebraica sobre k_p . Como F es cuadrático regular (Lema 2.4), entonces dicha forma es isotrópica, lo que implica que es universal (Teorema 1.21). Por lo que podemos deducir el siguiente hecho:

Lema 5.2. *Sea un cuerpo de funciones algebraicas F/k_p para k un cuerpo de números y $p > 2$. La forma cuadrática $x_1^2 + x_2^2 + x_3^2 + x_4^2$ es universal en F .*

Por lo que lo que solamente existen finitos lugares v de k donde la forma suma de 4 cuadrados es anisotrópica, esto ya que por el Teorema de Ostrowski (Véase Conrad, 2010) las únicas posibles completaciones de un cuerpo de números k son k_p para todo $p \in \mathbb{Z}$ y $\mathbb{R}$ (o $\mathbb{C}$).

Con esto en mente podemos hacer un esbozo de la demostración del Teorema 5.1. Sea un elemento $f \in F/k$ positiva definida, siempre podremos escribir su divisor de forma única como $\text{div}(f) = E - 2D$. Con esto vamos a justificar que para los finitos v donde la forma sumar 4 cuadrados es anisotrópica, existen secciones $\alpha_v \in \mathcal{L}_v(lA)$ y $\beta_{i,v} \in \mathcal{L}_v(D + lA)$ para algún divisor A de F/k amplio y un l lo suficientemente grande, de modo que para

todo lugar v de k , satisfagan la siguiente ecuación

$$f\alpha_v^2 = \sum_{i=1}^5 \beta_{i,v}^2$$

en cada completación k_v respectivamente (véase Teorema 5.10 y Teorema 5.20).

Luego se probará que la propiedad de ser suma de cuatro cuadrados se preserva bajo pequeñas perturbaciones en vecindades 2-ádicas (véase Proposición 5.16), lo mismo ocurrirá para completaciones reales. De este modo se podrá argumentar que las secciones $\alpha \in \mathcal{L}(lA)$ y $\beta_5 \in \mathcal{L}(D + lA)$ en F/k que aproximan simultáneamente a α_v con α y $\beta_{5,v}$ con β_5 , dadas por el Teorema de aproximación débil de Artin-Whaples, cumplirán que la función positiva definida

$$f - \left(\frac{\beta_5}{\alpha} \right)^2$$

es suma de 4 cuadrados en dichas completaciones de k y por la elección de los lugares v se podrá concluir que esto ocurre para todas en las completaciones F_v/k_v (véase Teorema 5.25). Finalmente se aplicará un principio local global deducido del Teorema de Kato, 1986 (Véase Teorema 5.5). Concluyendo así la prueba de la conjetura de Pfister. Paralelamente, compararemos el proceso lógico del Trabajo de Benoist con la demostración de Pourchet para el caso particular cuando $F = \mathbb{Q}(t)$.

Antes, de comenzar, debemos recordar una discusión que se tuvo en el Capítulo destinado a los Divisores. Dado un $f \in F/k$, por el Lema 2.29, sabemos que $\text{div}_{2D}^k(f) = E$ donde E es efectivo reducido, es decir, siempre podemos ver a f como una sección global de un divisor $2D$.

Junto con lo anterior y con la Definición 2.28 podemos concluir que las afirmaciones que hagamos con respecto a representaciones de $f \in F/k$ se pueden traducir a afirmaciones de representaciones de f en el espacio $\mathcal{L}(2D)$.

Sin más dilación, comencemos.

5.1. Principio Local-Global Kato

El principio local global de Kato, demostrado originalmente por Kato, 1986, fue posterior al calculo del numero de Pitágoras de funciones racionales en cuerpos de números por parte de Pourchet, que fue en el año 1971. Debido a este desfase en las pruebas, Pourchet no contó con el principio local global de Kato, pero gracias al hecho que la suma de cuadrados

en $k(t)$ es equivalente a las sumas de cuadrados en $k[t]$ (Teorema 2.32). Por lo que Pourchet pudo superar este impasse demostrando su principio local global de manera más elemental. En este capitulo demostraremos que el principio local global de Pourchet es una consecuencia directa del Teorema de Kato.

Teorema 5.3 (Kato, 1986, Theoreme 0.8). *Sea F/k una cuerpo de funciones algebraicas regular sobre un cuerpo de números k . Para $v \in \Omega$ una valuación de k sea F_v/k_v la extensión de cuerpos de funciones algebraicas. Entonces el mapeo canónico*

$$\phi : I^3(F)/I^4(F) \rightarrow \prod_{v \in \Omega_k} I^3(F_v/k_v)/I^4(F_v/k_v)$$

es inyectivo.

Observación 5.4. 1. Comparando con el paper original de Kato, la afirmacion se puede ver mas directamente si reemplazamos $I^3(K)/I^4(K)$ por $H^3(F, \mathbb{Z}/2\mathbb{Z})$ el 3-er grupo de cohomologia de Galois del modulos $\mathbb{Z}/2\mathbb{Z}$ con acción trivial. No obstante, gracias al famoso teorema de Markurjev-Suslin, sabemos que para cualquier cuerpo K de caracteristica diferente de 2 se cumple $H^3(K, \mathbb{Z}/2\mathbb{Z}) \cong I^3(K)/I^4(K)$ (un caso particular de la conjetura de Milnor¹, que más tarde fue resuelto por completo por Voevodsky.)

2. Es sabido que en un Homomorfismo de grupos $\psi : G \rightarrow H$ se tiene que $\psi(e_G) = e_H$ donde e_H y e_G son las identidades respectivamente. El teorema de Kato, al ser una inyección nos dice que si fijamos $1, 1 \in I^3(F)/I^4(F)$ y tenemos la igualdad $\phi(a) \equiv \phi(b)$ entonces $a \equiv b$. Si reemplazamos $b \equiv 0$ tenemos que una 3-forma de Pfister es nula en el cociente $I^3(k(C))/I^4(k(C))$ si y solo si es nula en el producto cartesiano $\prod_{v \in \Omega} I^3(F_v)/I^4(F_v)$, lo que equivale a decir que debe ser nula en cada cociente $I^3(F_v)/I^4(F_v)$ para todo lugar v de k .

Combinando el Teorema 1.30 y el Teorema 5.3, podemos concluir el siguiente Principio local global:

Teorema 5.5. *Sea F/k un cuerpo de funciones algebraicas regular sobre un cuerpo de números k . Sea $f \in (F)^*$. Entonces $\langle\langle 1, 1 \rangle\rangle$ representa $f \in F$ si y solo si representa a f en F_v/k_v para todos los lugares v de k .*

¹Milnor, 1970, Question 4.3

Demostración. Sea f representada por $\langle\langle 1, 1 \rangle\rangle$ en F_v/k_v para todo lugar v de k si y solo si $\langle\langle 1, 1, -f \rangle\rangle \equiv 0$ en $I^3(F_v)/I^4(F_v)$ para todo lugar v , luego por la Observación 5.4 es equivalente a decir que $\langle\langle 1, 1, -f \rangle\rangle \equiv 0$ en $I^3(F)/I^4(F)$ aplicando nuevamente el Teorema 1.30 concluimos que esto ocurre si y solo si f representada por $\langle\langle 1, 1 \rangle\rangle$ en F $\square$

El siguiente resultado se sigue de manera directa del Teorema de Kato en el caso $F = k(t)$ y después aplicar el Teorema de Cassels-Pfister (Teorema 2.32).

Corolario 5.6. *Sea k un cuerpo de números, Ω el conjunto de sus lugares, y $(k_v)_{v \in \Omega}$ la familia de sus completaciones; Sea $f \in k[t] - \{0\}$. Las siguientes propiedades son equivalentes:*

1. $\langle\langle 1, 1 \rangle\rangle$ representa f en $k[t]$,
2. $\langle\langle 1, 1 \rangle\rangle$ representa a f en $k_v[t]$ para todo $v \in \Omega$.

Este corolario es el Principio local global de Pourchet (Véase Pourchet, 1971, Proposición 4).

Como ya se mencionó, Pourchet demuestra dicho resultado de manera más rudimentaria, como una consecuencia directa del Teorema de Hasse-Minkoski y su propio criterio local-global (Véase Pourchet, 1971, Proposición 3).

Con el Teorema de Kato, estamos listos para demostrar parcialmente la conjetura de Pfister y particularmente entender donde radica su dificultad y cual fue la idea crucial de Benoist para poder resolverla después de treinta años.

Pero antes, veremos unas consecuencias del Teorema de Kato. El primer resultado es un análisis del comportamiento de F/k en algunas de las completaciones de k y las consecuencias del Principio local-global de Kato y el Teorema de Hasse-Minkoski.

Teorema 5.7. *Sea k un cuerpo de números real tal que el grado $[k_v : \mathbb{Q}_2]$ es par para todo lugar diádico $v \in \Omega_k$. Sea F/k un cuerpo de funciones algebraicas regular sobre k , entonces $p(F) \leq p(k) + 1 \leq 5$.*

Demostración. Sabemos que el grado $[k_v : \mathbb{Q}_2]$ es par para todo lugar diádico $v \in \Omega_k$. Bajo esta hipótesis, sabemos que $p(k) = 3$ (Ejemplo 1.2), lo cual ocurre si y solo si el número de Pitágoras local es $p(k_v) \leq 3$ para todo lugar $v \in \Omega_k$. Para acotar el número de Pitágoras

global $p(F)$, analizaremos el comportamiento local en cada completación F_v/k_v dividiendo los lugares de Ω_k en tres casos:

- i) Completaciones reales: Si v es un lugar real, el Teorema 3.1 asegura que $p(F_v) = 2$.
- ii) Completaciones no diádicas: Combinando la Proposición 4.16 y el Teorema 2.5, obtenemos la cota $p(F_v) \leq 3$.
- iii) Completaciones diádicas: Por nuestra hipótesis inicial, $[k_v : \mathbb{Q}_2]$ es par, lo que implica que el nivel es $s(k_v) = 2$. Utilizando el mismo razonamiento del caso anterior, concluimos nuevamente que $p(F_v) \leq 3$.

En consecuencia, para absolutamente todo lugar $v \in \Omega_k$, tenemos la cota absoluta $p(F_v) \leq 3$. Esto garantiza que $p(F_v) \leq 4$, lo que significa que toda función $f \in F_v$ que sea positiva definida puede escribirse como suma de a lo sumo 4 cuadrados. En el lenguaje de formas cuadráticas, esto equivale a decir que f es representada localmente por la forma de Pfister $\langle\langle 1, 1 \rangle\rangle$ en cada completación F_v .

Finalmente, dado que $\langle\langle 1, 1 \rangle\rangle$ representa a f en todos los cuerpos locales F_v y el cuerpo F es regular, podemos aplicar el principio local-global de Kato (Teorema 5.5). Este nos permite concluir que la forma representa a f globalmente en F , demostrando así que $p(F) \leq 4 = p(k) + 1 \leq 5$. $\square$

Corolario 5.8. *Sea k un cuerpo de números real tal que el grado $[k_v : \mathbb{Q}_2]$ es par para todo lugar diádico $v \in \Omega_k$. Sea F/k un cuerpo de funciones algebraicas sobre k , entonces $p(F) \leq p(k) + 1 \leq 5$.*

Demostración. Como F/k es no necesariamente regular, vamos a utilizar el cuerpo $\tilde{k}$ que es la clausura algebraica relativa de k en F , esta clausura cumple que $k \subseteq \tilde{k} \subseteq F$ y $F/\tilde{k}$ si es regular. Sabemos que $\tilde{k}$ es una extensión finita de k , entonces $\tilde{k}$ es un cuerpo de números. Aplicamos el Teorema 5.7 al cuerpo $F/\tilde{k}$ y obtenemos que $p(F) \leq 5$; es decir: sean $f_1, \dots, f_n \in F$, entonces existen $g_1, \dots, g_5 \in F$ tales que $f_1^2 + \dots + f_n^2 = g_1^2 + \dots + g_5^2$. Esto nos dice que el número de Pitágoras de F/k es también 5. $\square$

Observación 5.9. Sea k un cuerpo de números, este puede ser real o no real. Si el cuerpo de números es no real tenemos la Proposición 4.20 la cual nos dice que $p(F) \leq 5$ para el cuerpo F/k en este caso particular.

Ahora si el cuerpo de números k es real, tenemos dos posibilidades, que los ideales diádicos ramifiquen de manera par o impar en el 2, es decir que $[k_v : \mathbb{Q}_2]$ sea par o impar

para las localizaciones diádicas. Acabamos de ver que en el caso que sea par se tiene que $p(F) \leq 4 < 5$, por lo que si se demuestra que $p(F) \leq 5$ en el caso donde $[k_v : \mathbb{Q}_2]$ es impar, se podría resolver la conjetura de Pfister.

Si intentamos resolver esto último de la misma manera que los casos anteriores, notaremos una clara problemática. Sabemos que si k es real el cuerpo de funciones algebraicas F/k tendrá como número de Pitagoras 2 gracias al Teorema de Witt (Teorema 3.1). También sabemos que el número de Pitágoras de F/k cuando k es una completación no diádica estará acotado por 4 (Lema 5.2). Finalmente en el caso que exista un lugar diádico con $[k_v : \mathbb{Q}_2]$ impar, por la Proposición 4.17 y el Teorema 2.5 concluimos que $p(F) \leq 5$ en este caso. Es decir que

$$p(F_v) \leq 5, \forall v \in \Omega_k.$$

Es por ello que no podemos aplicar el Teorema de Kato ya que este controla suma de 4 cuadrados en las completaciones, no de 5.

Por lo que debemos un trabajo extra para resolver el caso faltante.

5.2. Existencia 2-ádica de representación por sumas de 5 cuadrados

Dado un $f \in F_2/k_2$ donde k_2 es una completación 2-ádica de un cuerpo de números k , para algún primo 2. Sea $D \in \text{Div}(F_2/k_2)$ el divisor doblado de f . En esta sección, buscaremos justificar la existencia de secciones $\alpha_2 \in \mathcal{L}_2(lA)$ y $\beta_{i,2} \in \mathcal{L}_2(D + lA)$ para algún divisor A de F/k amplio y un $l \in \mathbb{Z}$ lo suficientemente grande, tal que para toda completación k_p de k , satisfagan la siguiente ecuación

$$f\alpha_2^2 = \sum_{i=1}^5 \beta_{i,2}^2$$

Dado un cuerpo de números, por la Proposición 4.17 sabemos que $s(k_2) \leq 4$. Ahora bien, sea F/k_2 un cuerpo de funciones algebraicas regular, por el Teorema 2.5, podemos deducir que $p(F) \leq 5$. Esto nos dice que cualquier elemento de F , puede escribirse como suma de a lo más 5 cuadrados, por lo que, gracias a la Hipótesis 2.31 (con $n = 5$), podemos concluir el siguiente resultado.

Teorema 5.10. *Sea k un cuerpo de números. Sea F/k_2 un cuerpo de funciones algebraicas*

regular sobre una completación 2-ádica. Sea A en $\text{Div}(F/k_2)$, con A amplio. Sea $f \in F$ y sea $D \in \text{Div}(F/k_2)$ el divisor doblado de f .

Entonces para un l lo suficientemente grande, existen $\alpha_2 \in \mathcal{L}_2(lA)$ y $\beta_{1,2}, \dots, \beta_{5,2} \in \mathcal{L}_2(D + lA)$ tales que

$$f\alpha_2^2 = \sum_{i=1}^5 \beta_{i,2}^2$$

con α_2 no nulo y los $\beta_{i,2}$ sin un cero en común.

Como caso particular tenemos el siguiente corolario.

Corolario 5.11. Sea k un cuerpo de números y sea k_2 una completación 2-ádica de k . Sea $f \in k_2[t] \setminus \{0\}$ de grado par $2n$. Existen entonces 5 polinomios $f_1, \dots, f_5 \in k_2[t]$ tales que

$$1. f = f_1^2 + f_2^2 + f_3^2 + f_4^2 + f_5^2$$

$$2. \deg(f - f_5^2) = 2n$$

$$3. \text{p.m.c.d.}(f_1, f_2, f_3, f_4) = 1$$

Demostración. Sea $f \in k_2[t]$, sabemos que f al ser un polinomio, podemos escribir su divisor como $\text{div}^{k_2}(f) = \text{div}_0^{k_2}(f) - 2nP_\infty$. Luego $f \in \mathcal{L}(2nP_\infty)$. En la notación de Teorema 5.10, digamos que $D = nP_\infty$ y $A = P_\infty$. De este modo tenemos $\alpha \in \mathcal{L}_2(lP_\infty)$ y las secciones $\beta_i \in \mathcal{L}_2((n+l)P_\infty)$ sin un cero real común, tal que

$$f\alpha^2 = \sum_{i=1}^5 \beta_i^2$$

$$f = \sum_{i=1}^5 \left(\frac{\beta_i}{\alpha} \right)^2.$$

De donde podemos extraer que

$$\text{div} \left(\frac{\beta_i}{\alpha} \right) \geq (n+l)P_\infty - lP_\infty = nP_\infty > -nP_\infty$$

por lo que

$$f - \left(\frac{\beta_5}{\alpha} \right)^2 \in \mathcal{L}_2(2nP_\infty).$$

Lo que concluye lo pedido. □

5.3. Variaciones 2-ádicas de sumas de 4 cuadrados

Considerando el punto ii) en el bosquejo de la demostración de la conjetura de Pfister por parte de Pourchet, dada en la introducción de este capítulo, necesitaremos que variaciones suficientemente pequeñas dentro de un k_2 espacio finito de funciones racionales de una función que es suma de 4 cuadrados, mantienen esa propiedad. Eso vamos a exponer en la sección presente.

Para el resto de la sección fijamos como k_2 una extensión finita de $\mathbb{Q}_2$ y F/k_2 un cuerpo de funciones algebraicas.

Antes de dar el resultado principal, necesitamos incluir una breve definición.

Definición 5.12. Sea F/k_2 un cuerpo de funciones algebraicas sobre alguna completación diádica de k . Denotemos por V_{arth} al conjunto de valuaciones discretas v en F que se extienden desde valuaciones 2-ádicas en k . Y denotamos por $\hat{F}^v$ a la completación de F con respecto a la valuación v , también definamos el conjunto $\hat{\mathcal{O}}^x = \{f \in \hat{F}^x \mid v_x(f) \geq 0\}$ que será un anillo local y su unico ideal maximal se definirá como $\hat{\mathfrak{m}} = \{f \in \hat{F}^x \mid v_x(f) > 0\}$.

El siguiente lema será necesario para la demostración del resultado principal de esta sección. Este resultado es una simplificación del Benoist, [2025](#), Lemma 2.4 adaptado a nuestro caso y siguiendo su misma demostración.

Lema 5.13. Sea el par $(\hat{\mathcal{O}}^x, \hat{\mathfrak{m}})$ y sea $q \in \hat{\mathcal{O}}^x[X_1, \dots, X_5]$. Sea $p \in (\hat{\mathcal{O}}^x)^5$ tal que $q(p) = 0$ y $\frac{\partial q}{\partial X_j}(p) \neq 0$ para algún $1 \leq j \leq 5$.

Para cualquier entero $r \geq 0$, existe un entero $s \geq 0$ con la siguiente propiedad: Si $g \in \hat{\mathcal{O}}^x[X_1, \dots, X_5]$ es tal que $g - q \in (\hat{\mathfrak{m}})^s \cdot \hat{\mathcal{O}}^x[X_1, \dots, X_5]$, entonces existe $y \in (\hat{\mathcal{O}}^x)^5$ tal que $g(y) = 0$ y $y - p \in ((\hat{\mathfrak{m}})^r)^s$

Demostración. Sea $\delta = \frac{\partial q}{\partial X_j}(p) \in \hat{\mathcal{O}}^x$ para algún $1 \leq j \leq 5$ tal que $\delta \neq 0$. Sea $t \geq 0$ de modo que $\delta \in \mathfrak{m}^t \setminus \mathfrak{m}^{t+1}$. Denotemos $s := \max[2t, t + r, t + 1]$. Por hipótesis sabemos que

$g - q \in (\widehat{\mathfrak{m}})^s \cdot \widehat{\mathcal{O}}^x[X_1, \dots, X_5]$ por lo que

$$\frac{\partial q}{\partial X_j}(p) \equiv \frac{\partial g}{\partial X_j}(p) \mod \widehat{\mathfrak{m}}^s$$

y como $s \geq t + 1$ tenemos que $0 \neq \frac{\partial g}{\partial X_j}(p) = \delta_g$ en $\mathfrak{m}^t \setminus \mathfrak{m}^{t+1}$. Además, por hipótesis $g(p) = g(p) - f(p) \in \widehat{\mathfrak{m}}^s$ y por nuestra elección del s , tenemos que $(\widehat{\mathfrak{m}})^s = (\widehat{\mathfrak{m}})^{2t} \cdot (\widehat{\mathfrak{m}})^{s-2t}$ y como $\widehat{\mathcal{O}}^x$ es un anillo de valuación discreta, podemos concluir que $g(p) \equiv 0 \mod (\delta_g^2) \cdot \widehat{\mathfrak{m}}^{s-2t}$. Con todo esto podemos aplicar el M. F. Artin, 1969, lemma 5.10 con $\alpha = \widehat{\mathfrak{m}}^{s-2t}$, concluyendo así que existe un $y \in (\widehat{\mathcal{O}}^x)^5$ tal que $g(y) = 0$ y $y - x \in (\widehat{\mathfrak{m}}^{s-t})^5$ y como $s - t \geq r$ concluimos lo pedido. $\square$

Los siguientes resultados hasta el momento de entregar la presente tesis, no los logramos verificar y por lo tanto, en el espíritu de transparencia científica, decidimos dejarlo como hipótesis, y dejar la verificación como tarea al lector.

El primer resultado es una consecuencia de la Proposición 2.3 de Benoist, 2025, donde Benoist afirma este hecho, sugiriendo que sea una consecuencia de un diagrama conmutativo mencionado en Kato, 1986.

Hipótesis 5.14. *Existe un subconjunto finito de $\Gamma \in V_{arth}$ que cumple lo siguiente: $f \in F$ es representado por $\langle\langle 1, 1 \rangle\rangle$ en F si y solo si f es representado por $\langle\langle 1, 1 \rangle\rangle$ en las completaciones $\widehat{F}^v$, para todo $v \in \Gamma$.*

La siguiente hipótesis es el Lemma 2.8 de Benoist, 2025.

Hipótesis 5.15. *Sea k_2 un cuerpo diádico, sea F/k_2 un cuerpo de funciones algebraicas regular. Sea $f \in F/k_2$ y sea $D \in \text{Div}(F/k_2)$ el divisor doblado de f . Entonces existe una vecindad U de $f \in \mathcal{L}(2D)$ (para la topología inducida por k_2) tal que para cualquier $g \in U$ y cualquier $y \in \mathbb{P}_F$ con $g(y) = 0$ existe $x \in \mathbb{P}_F$ con $f(x) = 0$ y una k -incrustación de $\mathcal{F}(x)$ en $\mathcal{F}(y)$.*

Ya podemos enunciar el resultado principal de esta sección.

Proposición 5.16 (Benoist, 2025, Proposition 2.9). *Sea F/k_2 un cuerpo de funciones algebraicas regular sobre un cuerpo diádico k_2 . Sea $f \in F/k_2$ y sea $D \in \text{Div}(F/k_2)$ el*

divisor doblado de f . Si $f \in \Sigma \subseteq \mathcal{L}(2D)$ donde $\Sigma \subseteq \mathcal{L}(2D)$ es el conjunto de secciones representadas por $x_1^2 + x_2^2 + x_3^2 + x_4^2$ en F^4 y además la forma $x_1^2 + x_2^2 + x_3^2 + x_4^2$ es isotrópica en el cuerpo residual de todos los ceros de f de multiplicidad par ≥ 2 . Entonces Σ contiene una vecindad 2-ádica de f en $\mathcal{L}(2D)$.

Antes de ver la demostración, vamos a ver un pequeño ejemplo concreto.

Ejemplo 5.17. Para el ejemplo, sea F/k un cuerpo de funciones algebraicas, específicamente $F = \mathbb{Q}_2(t)$. Sea el siguiente anillo de valuación discreta

$$\mathcal{O}_\infty = \left\{ \frac{f}{g} \mid f, g \in \mathbb{Q}_2[t], \deg(f) \leq \deg(g) \right\}$$

y su respectivo lugar $P_\infty = \left\{ \frac{f}{g} \mid f, g \in \mathbb{Q}_2[t], \deg(f) < \deg(g) \right\}$. La valuación asociada es $v_\infty\left(\frac{f}{g}\right) = \deg(g) - \deg(f)$. Ahora sea $D = P_\infty$, podemos notar que el espacio $\mathcal{L}(2D)$ tendría la siguiente forma

$$\begin{aligned} x = \frac{f}{g} \in \mathcal{L}(2D) &\Leftrightarrow v_P(x) \geq -2v_P(D) \quad \forall P \in \mathbb{P}_F \\ &\Leftrightarrow v_\infty\left(\frac{f}{g}\right) \geq -2v_\infty(D) = -2 \cdot 1 \\ &\Leftrightarrow \deg(g) - \deg(f) \geq -2 \\ &\Leftrightarrow \deg(f) - \deg(g) \leq 2 \\ &\Leftrightarrow \deg(x) \leq 2 \end{aligned}$$

para los lugares distintos de D tendríamos que $v_P(D) = 0$ por lo que el espacio $\mathcal{L}(2D)$ son todos los polinomios de grado menor o igual a 2.

Sea $f(t) = 7(4t^2 + 1) \in \mathcal{L}(2D)$. Sabemos que 7 se puede escribir como suma de 4 cuadrados (y no de menos) en $\mathbb{Q}_2$, de la siguiente forma:

$$7 = 2^2 + 1 + 1 + 1.$$

Ahora bien, usando la identidad de los cuadrados de Euler (Lema 1.23), podemos concluir que $f(t)$ puede escribirse como suma de cuatro cuadrados, específicamente de la siguiente manera

$$7(4t^2 + 1) = (-4t + 1)^2 + (2 + 2t)^2 + (2t + 1)^2 + (2t - 1)^2$$

Además, es preciso notar que $f(t)$ se puede descomponer en dos factores lineales distintos, por lo que cumple la condición de los ceros de la Proposición 5.16 por vacuidad.

Sea el siguiente polinomio $\tau(t) = 7(4t^2 + 2^n t + 2^{2n-1} + 1)$, notemos que para cualquier $\epsilon > 0$ podemos encontrar un n lo suficientemente grande tal que $\|f - \tau\|_2 < \epsilon$, por lo que $\tau(t)$ está contenido en cualquier vecindad 2-ádica de $f(t)$ y por la Proposición anterior, debería ser suma de cuadrados. Podemos deducir esto del siguiente hecho: dado un polinomio de la forma $at^2 + bt + c$ si este es suma de 4 cuadrados de polinomios lineales, entonces ocurre que

$$\begin{aligned} at^2 + bt + c &= \sum_{i=1}^4 (t + a_i)^2 \\ &= 4t^2 + 2 \left(\sum_{i=1}^4 a_i \right) t + \left(\sum_{i=1}^4 a_i^2 \right) \\ \Rightarrow a &= 4 \\ b &= 2 \sum_{i=1}^4 a_i \\ c &= \sum_{i=1}^4 a_i^2 \end{aligned}$$

Y en nuestro caso, podemos ver que

$$2 \left[\frac{2^n + 1}{2} + \frac{2^n - 1}{2} + \frac{1}{2} + \frac{-1}{2} \right] = 2^n$$

y además

$$\begin{aligned} \left(\frac{2^n + 1}{2} \right)^2 + \left(\frac{2^n - 1}{2} \right)^2 + \left(\frac{1}{2} \right)^2 + \left(\frac{-1}{2} \right)^2 &= \frac{2(2^n)^2 + 4}{4} \\ &= 2^{2n-1} + 1 \end{aligned}$$

por lo que

$$(\sqrt{7})^2 \left(\left(t + \frac{2^n + 1}{2} \right)^2 + \left(t + \frac{2^n - 1}{2} \right)^2 + \left(t + \frac{1}{2} \right)^2 + \left(t + \frac{-1}{2} \right)^2 \right) = \tau(t)$$

Para hacer la demostración de la Proposición 5.16 seguimos el mismo camino que usó Benoist en el texto original, pero adaptándolo al lenguaje algebraico de divisores.

Demostración. Sea $x \in \mathbb{P}_F$ un cero de multiplicidad impar de f esto quiere decir que $v_x(f) = 2k + 1$, esto nos dice que $f = ut^{2k+1}$ donde t es un parametro uniformizador de $\mathcal{O}_x$. Como $\langle\langle 1, 1 \rangle\rangle$ representa a f en F , esto quiere decir que existe un vector $v \in F^4$ tal que

$$\langle\langle 1, 1 \rangle\rangle(v) = ut^{2k}t \Leftrightarrow \langle\langle 1, 1 \rangle\rangle(vt^{-k}) = ut$$

esto por propiedades de las formas cuadraticas. Ahora bien, por el Lema 1.22, esto implica que la forma $\langle\langle 1, 1 \rangle\rangle \perp \langle ut \rangle$ es isotropica en F .

Supongamos que $\langle\langle 1, 1 \rangle\rangle$ es anisotropica en $\mathcal{F}_x$, por el Lema 2.16, esto implica que la forma

$$\langle\langle 1, 1 \rangle\rangle \perp t\langle u \rangle$$

es anisotropica en F , lo cual es una contradicción, por lo que $\langle\langle 1, 1 \rangle\rangle$ es isotrópica en $\mathcal{F}_x$. Por hipótesis, esto mismo se cumple para cualquier cero de f .

Por Hipótesis 5.15, existe una vecindad $U \subset \mathcal{L}(2D)$ de f tal que, para cualquier $\tau \in U$ y cualquier $x' \in \mathbb{P}_F$ con $\tau(x') = 0$, la forma $\langle\langle 1, 1 \rangle\rangle$ es isotrópica en $\mathcal{F}_{x'}$.

Vamos a probar que para cualquier $\tau \in U$ y cualquier $x \in \mathbb{P}_F$, la forma $\langle\langle 1, 1 \rangle\rangle$ representa a τ en la completación $\hat{F}^x$ de F en x .

Sabemos que cualquier forma 5-dimensional en un cuerpo local es isotrópica (Véase Lam, 2005 VI.2.12). Con esto en mente, si x no es un cero de τ , entonces $\tau(x) \neq 0$ en $\mathcal{F}_x$, por lo que la forma $\langle\langle 1, 1 \rangle\rangle \perp \langle \tau(x) \rangle$ es 5 dimensional, y por lo anterior mencionado, es isotrópica en $\mathcal{F}_x$, luego por el Lema 1.22, esto implica que $\langle\langle 1, 1 \rangle\rangle$ representa a $\tau(x)$ en $\mathcal{F}_x$ y por lo tanto representa τ en $\hat{F}^x$ por completación (aplicación directa del Corolario 4.12).

Si x es un cero de τ , entonces $\langle\langle 1, 1 \rangle\rangle$ es isotrópico en $\mathcal{F}_x$ por elección de U , por lo tanto es isotrópico en $\hat{F}^x$ por lema de Hensel. De ello se deduce que $\langle\langle 1, 1 \rangle\rangle$ representa τ en $\hat{F}^x$ (véase Teorema 1.21).

Para cada valuación $x \in \Gamma \subseteq V_{arth}$, sea $\hat{F}^x$ su completación. Dado que la forma $\langle\langle 1, 1 \rangle\rangle$ representa f en F , la forma $\langle\langle 1, 1 \rangle\rangle \perp \langle f \rangle$ es isotrópica sobre F (Véase Lema 1.22) por lo tanto, también sobre la completación $\hat{F}^x$ de F con respecto a x . Sea $c \in (\hat{F}^x)^*$ tal que $c \cdot f \in \hat{\mathcal{O}}^x$. Por el Lema 5.13 (con f igual a la forma cuadrática $c \cdot (\langle\langle 1, 1 \rangle\rangle \perp \langle f \rangle)$), existe una vecindad $V_x \subset \mathcal{L}(2D)$ de f tal que $c \cdot (\langle\langle 1, 1 \rangle\rangle \perp \langle \tau \rangle)$ es isotrópica en $\hat{F}^x$ para todo $\tau \in V_x$. Por Teorema 1.21, la forma $\langle\langle 1, 1 \rangle\rangle$ representa τ en $\hat{F}^x$ para todo $\tau \in V_x$.

Para concluir, definamos $W := U \cap \bigcap_{x \in \Gamma} V_x$. Es una vecindad de f en $\mathcal{L}(2D)$ ya que es la intersección de finitos abiertos, además por nuestras elecciones, se deduce que, para todo $\tau \in W$, la forma $\langle\langle 1, 1 \rangle\rangle$ representa $\tau \in \hat{F}^x$ para todo $x \in \Gamma$, finalmente, según la Hipótesis 5.14, la forma $\langle\langle 1, 1 \rangle\rangle$ también representa τ en F . $\square$

Es preciso notar que la condición de los ceros de f de la Proposición 5.16 no puede ser omitida, para verificar ello tenemos la siguiente observación.

Observación 5.18. Sea en este caso $F = \mathbb{Q}_2(t)$, $f(t) = t^2 \in \mathbb{Q}_2(t)$ y el mismo $\mathcal{L}(D)$ del Ejemplo 5.17. Vemos que sigma es suma de 4 cuadrados y que tiene un cero de multiplicidad igual a dos, que es el 0. Su cuerpo residual es $\mathcal{F}_0 = \mathbb{Q}_2$ y nosotros sabemos que forma $\langle\langle 1, 1 \rangle\rangle$ no es isotrópica en $\mathbb{Q}_2$ por lo que no cumple la condición de los ceros. Ahora elijamos $\tau(t) = t^2 - 2^{2l}$ con $0 < l \in \mathbb{Z}$. Para cualquier vecindad 2-ádica U de f podemos elegir l lo suficientemente grande para que $\tau \in U$. Si la proposición fuese cierta, entonces τ debería ser suma de cuadrados en $\mathbb{Q}_2(t)$ pero no lo es y lo vamos a demostrar. Sea $\tau(t) = t^2 - 2^{2l} \in \mathbb{Q}_2(t)$ (solo por notación, digamos $a = 2^l$). Asumamos que existen $g_1, \dots, g_4 \in \mathbb{Q}_2(t)$ tales que $\tau = g_1^2 + \dots + g_4^2$, por el Teorema de Cassels-Pfister (Teorema 2.32) tenemos que τ también es suma de 4 cuadrados, pero en $\mathbb{Q}_2[t]$, ahora sean esos $f_1, \dots, f_4 \in \mathbb{Q}_2[t]$ tales que $f_1^2 + \dots + f_4^2 = \tau$. Denotemos por $n_i := \deg(f_i)$ de esto desprendemos que

$$\begin{aligned} f_1^2 &= a_{n_1}^2 t^{2n_1} + Q_1(t) \\ f_2^2 &= b_{n_2}^2 t^{2n_2} + Q_2(t) \\ f_3^2 &= c_{n_3}^2 t^{2n_3} + Q_3(t) \\ f_4^2 &= d_{n_4}^2 t^{2n_4} + Q_4(t) \end{aligned} \tag{5.1}$$

Denotemos por $n := \max_{1 \leq i \leq 4} \{n_i\}$, entonces el coeficiente líder de $f_1^2 + f_2^2 + f_3^2 + f_4^2$ por la Ecuación (5.1) será exactamente $a_n^2 + b_n^2 + c_n^2 + d_n^2$ con al menos uno no nulo (por construcción). Igualando los coeficientes de $\sum_{i=1}^4 f_i^2$ con τ tenemos que si $n \geq 2$, entonces

$$\begin{aligned} a_n^2 + b_n^2 + c_n^2 + d_n^2 &= 0 \\ \Rightarrow \frac{a_n^2}{d_n^2} + \frac{b_n^2}{d_n^2} + \frac{c_n^2}{d_n^2} &= -1 \end{aligned}$$

en $\mathbb{Q}_2$, lo que sabemos que es imposible. Esto nos dice que $n = 1$ esto implica que el grado de los f_i debe ser 1 o 0, pero al menos uno debe tener grado 1.

Denotemos entonces $f_i := r_i t + k_i$, nuevamente igualando coeficientes tenemos que

$$\begin{aligned} f_1^2 + f_2^2 + f_3^2 + f_4^2 &= t^2 - a^2 \\ \Rightarrow \sum_{i=1}^4 r_i^2 t^2 + \sum_{i=1}^4 r_i k_i + \sum_{i=1}^4 k_i^2 &= t^2 - a^2 \end{aligned}$$

Por lo que $\sum_{i=1}^4 r_i^2 = 1$, $\sum_{i=1}^4 r_i k_i = 0$ y $\sum_{i=1}^4 k_i^2 = -a^2$.

Ahora sea el espacio $\mathbb{Q}_2^4$ visto como un $\mathbb{Q}_2$ -espacio vectorial, con el producto interno usual $\langle 1, 1, 1, 1 \rangle$. Definamos los vectores $C = (r_1, r_2, r_3, r_4)$ y $D = (k_1, k_2, k_3, k_4)$ ambos en $\mathbb{Q}_2^4$. Inmediatamente notamos que C es un vector de norma 1 que es ortogonal a D , por lo que $D \in C^\perp$.

Si tomamos el sub-espacio vectorial generado por C y lo vemos a su vez, como espacio cuadrático, debemos notar que es no-degenerado e isométrico a $(\mathbb{Q}_2, \langle 1 \rangle)$, ya que podemos definir un cambio de base de la matriz diagonal asociada a $\langle 1, 1, 1, 1 \rangle$ (solo debemos multiplicar la matriz identidad de 4×4 por el vector fila $(1, 0, 0, 0)$ y su traspuesta).

De este modo podemos descomponer $(\mathbb{Q}_2^4, \langle 1, 1, 1, 1 \rangle) \cong (\mathbb{Q}_2, \langle 1 \rangle) \perp C^\perp$ y como la forma cuadrática $\langle 1, 1, 1, 1 \rangle$ en $\mathbb{Q}_2$ es isométrica a $\langle 1 \rangle \perp \langle 1, 1, 1 \rangle$, por el Teorema de cancelación de Witt (Teorema 1.25) tenemos que el complemento ortogonal $C^\perp$ visto como espacio cuadrático es isométrico al espacio $(\mathbb{Q}_2, \langle 1, 1, 1 \rangle)$ por lo que la norma de D debe ser representada por $\langle 1, 1, 1 \rangle$ en $\mathbb{Q}_2$, es decir que $-a^2$ debe ser suma de 3 cuadrados en $\mathbb{Q}_2$, y como $a \in \mathbb{Q}_2$ si dividimos por a^2 , esto implicaría que -1 es suma de 3 cuadrados en $\mathbb{Q}_2$, contradicción.

Podemos concluir que τ no es suma de 4 cuadrados. Por ende si omitimos la hipótesis de los ceros, la conclusión de la Proposición 5.16 no es válida.

Corolario 5.19. *Sea $f \in k_2[t] \setminus \{0\}$ libre de cuadrados y de grado par $2n$ tal que existen $f_1, \dots, f_5 \in k_2[t]$ donde*

$$f = f_1^2 + f_2^2 + f_3^2 + f_4^2 + f_5^2,$$

$\deg(f - f_5^2) = 2n$ y $\gcd(f_1, f_2, f_3, f_4) = 1$. Sea $|\cdot|_2$ el valor absoluto que define la topología en k_2 . Entonces, existe un $\eta > 0$ tal que: para todo polinomio $g \in k[t]$ que verifique $\deg(g) \leq n$ y $\|g - f_5\|_2 < \eta$, el polinomio $f - g^2$ es de grado $2n$ y es suma de 4 cuadrados en $k_2[t]$.

Demostración. Sea $k_2(t)$ el cuerpo de funciones racionales, sea $P_\infty \in \mathbb{P}_{k_2(t)}$ y sea $v_\infty(\cdot)$ su valuación discreta asociada (Como en el Ejemplo 5.17).

Recordando que estamos asumiendo que f es un polinomio de grado par, por lo que $f \in \mathcal{L}(2nP_\infty)$. Además

$$f = f_1^2 + f_2^2 + f_3^2 + f_4^2 + f_5^2, \quad f_i \in k_2[t] \text{ para } i = 1, \dots, 4$$

en la notación de la Proposición 5.16 $f - f_5^2 \in \Sigma \subseteq \mathcal{L}(2nP_\infty)$.

Por el Teorema de Artin-Whapels (Teorema 4.2), podemos elegir un $g \in k(t)$ que esté lo suficientemente cerca de f_5 en la topología inducida por $|\cdot|_2$ i.e. existe un $0 < \eta$ real, tal que

$\|g - f_5\|_2 < \eta$ y con $\deg(f - g^2) \leq 2n$.

Con todo esto ya podemos aplicar la Proposición 5.16 con $F = k_2(t)$, $f = f - f_5^2$, $\tau = f - g^2$ y $D = 2nP_\infty$ esto ya que la condición de los ceros se cumple trivialmente. Concluimos entonces que $f - g^2$ debe ser suma de 4 cuadrados en $k_2(t)$.

Nuevamente gracias al Teorema de Cassels-Pfister concluimos el resultado para $k[t]$. $\square$

5.4. Existencia real de representación por sumas de 5 cuadrados

De manera análoga a la sección anterior, en esta sección buscaremos justificar la existencia de secciones sobre divisores reales, tales que

$$f\alpha_{\mathbb{R}}^2 = \sum_{i=1}^5 \beta_{i,\mathbb{R}}^2.$$

Para ello tenemos el siguiente resultado.

Teorema 5.20. *Sea k un cuerpo de números real, sea F/k un cuerpo de funciones algebraicas regular y sea $F_{\mathbb{R}}/\mathbb{R}$ el cambio de base sobre la completación real $\mathbb{R}$ de k . Sea $A \in Cl(F_{\mathbb{R}}/\mathbb{R})$ un divisor amplio. Sea $f \in F_{\mathbb{R}}/\mathbb{R}$ no negativa, sea $D \in Div(F_{\mathbb{R}}/\mathbb{R})$ el divisor doblado de f . Entonces, para un l lo suficientemente grande existe, una sección $\alpha_{\mathbb{R}} \in \mathcal{L}_{\mathbb{R}}(2lA)$ no nula y las secciones $\beta_{i,\mathbb{R}} \in \mathcal{L}_{\mathbb{R}}(D + 2kA)$, $i = 1, \dots, 5$ sin un cero real común tales que*

$$f\alpha_{\mathbb{R}}^2 = \sum_{i=1}^5 \beta_{i,\mathbb{R}}^2.$$

Demostración. Como k_v es una completación real de k , por la Definición 4.8 podemos identificar $k_v \cong \mathbb{R}$. Por el Lema 2.29 sabemos que $div^{\mathbb{R}}(f) = E - 2D$ donde E es efectivo reducido, entonces podemos ver a f como una sección de $\mathcal{L}(2D)$ con $div_{2D}^k(f) = E$.

Como f es no negativa, por el Teorema de Witt (Teorema 3.1) tenemos que existen $g, h \in F/\mathbb{R}$ tales que $f = g^2 + h^2$. Como el divisor principal $div_{2D}^k(f)$ es efectivo, entonces no tiene polos reales, por lo que ni g ni h pueden tener polos reales.

Sea Q un divisor en $F_{\mathbb{R}}/\mathbb{R}$ efectivo cuyo soporte no tiene puntos reales y además $Q + div(g)$ y $Q + div(h)$ son efectivos. Ahora sea l lo suficientemente grande para que el espacio

$\mathcal{L}_{\mathbb{R}}(lA - Q)$ sea generado por secciones globales. Sea $\{\epsilon_i\}_{1 \leq i \leq n}$ una base del espacio $\mathcal{L}_{\mathbb{R}}(lA - Q)$, entonces definamos $\epsilon := \sum_{i=1}^n \epsilon_i^2$ visto como un elemento de $\mathcal{L}_{\mathbb{R}}(2lA)$ que se anula en Q y no tiene ceros reales (para entender el porqué de esta elección, vea Observación 5.21).

Digamos que $\alpha_{\mathbb{R}} := \epsilon$ y $\beta_{1,\mathbb{R}} := \epsilon g$, $\beta_{2,\mathbb{R}} := \epsilon h$ y $\beta_i := 0$ para $5 \geq i > 2$ como ϵ no tiene ceros reales y $\text{div}_{2D}^k(f)$ es efectivo reducido, hemos demostrado que existe una sección no nula $\alpha_{\mathbb{R}} \in \mathcal{L}_{\mathbb{R}}(lA)$ y las secciones $\beta_{i,\mathbb{R}} \in \mathcal{L}_{\mathbb{R}}(D + lA)$ sin un cero real común de la forma

$$f\alpha_{\mathbb{R}}^2 = \sum_{i=1}^5 \beta_{i,\mathbb{R}}^2.$$

□

Observación 5.21. Estas explicaciones las incluiremos aquí para no hacer la demostración anterior más engorrosa.

Si elegimos Q un divisor en $F_{\mathbb{R}}/\mathbb{R}$ de tal manera que $Q + \text{div}^k(\tau g) \geq 0$ y $Q + \text{div}^k(\tau h) \geq 0$, entonces podemos decir que $Q \geq \text{Div}_{\infty}^{\mathbb{C}}(\tau g) + \text{Div}_{\infty}^{\mathbb{C}}(\tau h)$, esto ya que sabemos que $g\tau$ y $h\tau$ no tienen polos reales, pero pueden tener polos complejos, por lo que elegimos el divisor Q de esta manera, para que al momento de multiplicar por ϵ (como lo definimos arriba), las secciones racionales $g\tau$ y $h\tau$ cancelen sus respectivos polos complejos y podamos "parchar" las singularidades, de modo que las funciones β_1 y β_2 sean efectivamente secciones de algún espacio $\mathcal{L}(\cdot)$ (esto es necesario por la Observación 2.25).

Ahora bien, sea una base $\{\epsilon_n\}_{0 \leq n \leq 1} \in \mathcal{L}(lA - Q)$ como antes, vemos que $\epsilon = \sum_{i=1}^n \epsilon_i^2 \in \mathcal{L}(-2Q + 2lA)$ esto gracias al siguiente calculo

$$\begin{aligned} v_P(\epsilon) &= v_P\left(\sum_{i=1}^n \epsilon_i^2\right) \\ &= \min_{1 \leq i \leq n} \{v_P(\epsilon_i^2)\} \\ &= 2v_P(\epsilon_j) \end{aligned}$$

para algún j , y $\epsilon_j \in \mathcal{L}(Q - lA)$ entonces $v_P(\epsilon_j^2) \geq -v_P(2(Q - lA))$ lo que implica que $\epsilon \in \mathcal{L}(2(Q - lA))$. Ahora tenemos que

$$\begin{aligned} \epsilon \in \mathcal{L}(2(Q - lA)) &\Leftrightarrow v_P(\epsilon) \geq 2n_P - 2lm_P \quad \forall P \in \mathbb{P}_F \\ &\Leftrightarrow v_P(\epsilon) \geq -2lm_P, \quad l \gg 0 \\ &\Leftrightarrow \epsilon \in \mathcal{L}(2lA) \end{aligned}$$

Para ver que ϵ se anula en los puntos del soporte de Q tenemos que realizar el siguiente cálculo

$$\begin{aligned} \operatorname{div}(\epsilon) &\geq Q - lA \\ \operatorname{div}_0(\epsilon) - \operatorname{div}_\infty(\epsilon) &\geq Q + lA_+ - lA_- \\ \Rightarrow \operatorname{div}_0(\epsilon) &\geq Q + lA_+ \end{aligned}$$

Por lo que si elegimos un lugar $P \in \operatorname{Supp}(Q)$ tendemos que $v_P(\epsilon) \geq n_P + lm_P > 0$ ya que $l \gg 0$, esto implica que $e(P) = 0$ obteniendo así lo que queríamos.

Es necesario mencionar que el teorema anterior es un corolario de la Proposición 3.3 del texto de Benoist, [2025](#).

Usando la misma elección de divisor A y D que en el Corolario [5.11](#), podemos desprender el siguiente resultado.

Corolario 5.22. *Sea $f \in \mathbb{R}[t] \setminus \{0\}$ positiva definida y de grado $2n$, entonces existen $f_1, \dots, f_5 \in \mathbb{R}[t]$ donde*

$$f = f_1^2 + f_2^2 + f_3^2 + f_4^2 + f_5^2,$$

$$\deg(f - f_5^2) = 2n.$$

5.5. Variaciones reales de suma de 4 cuadrados

Siguiendo la misma lógica que el caso 2-ádico. Veremos como se preserva el hecho de ser suma de 4 cuadrado bajo pequeñas perturbaciones, esta vez sobre completaciones arquimedianas.

Teorema 5.23. *Sea k un cuerpo de números real, sea F/k un cuerpo de funciones algebraicas regular y sea $F_{\mathbb{R}}/\mathbb{R}$ el cambio de base sobre la completación real $\mathbb{R}$ de k . Sea $A \in \operatorname{Cl}(F_{\mathbb{R}}/\mathbb{R})$ un divisor amplio. Sea $f \in F_{\mathbb{R}}/\mathbb{R}$ no negativa, sea $D \in \operatorname{Div}(F_{\mathbb{R}}/\mathbb{R})$ el divisor doblado de f tal que*

$$f\alpha_{\mathbb{R}}^2 = \sum_{i=1}^5 \beta_{i,\mathbb{R}}^2$$

para algunos $\alpha_{\mathbb{R}} \in \mathcal{L}_{\mathbb{R}}(2lA)$ no nula y las secciones $\beta_{i,\mathbb{R}} \in \mathcal{L}_{\mathbb{R}}(D + 2kA)$, $i = 1, \dots, 5$ sin un cero real común. Entonces existe $\alpha \in \mathcal{L}(2lA)$ no nula y las secciones $\beta_5 \in \mathcal{L}(D + 2lA)$

tales que

$$f - \left(\frac{\beta}{\alpha}\right)^2$$

es suma de 4 cuadrados en $F_{\mathbb{R}}/\mathbb{R}$.

Demostración. Por Hipótesis, podemos hacer los siguiente cálculos.

$$\begin{aligned} f\alpha_{\mathbb{R}}^2 &= \sum_{i=1}^5 \beta_{i,\mathbb{R}}^2 \\ \Rightarrow f\alpha_{\mathbb{R}}^2 - \beta_{5,\mathbb{R}}^2 &= \sum_{i=1}^4 \beta_{i,\mathbb{R}}^2 \in \mathcal{L}_{\mathbb{R}}(2(D + lA)) \end{aligned}$$

podemos notar que $f\alpha_{\mathbb{R}}^2 - \beta_{5,\mathbb{R}}^2$ es positiva en $F_{\mathbb{R}}/\mathbb{R}$, ahora aproximando débilmente (Lema 4.10) existen $\alpha \in \mathcal{L}(lA)$ y las secciones $\beta_5 \in \mathcal{L}(D + lA)$ en el cuerpo F que estén lo suficientemente cerca de $\alpha_{\mathbb{R}}$ y $\beta_{5,\mathbb{R}}$ por ende $f\alpha^2 - \beta_5^2$ también es positiva definida en $F_{\mathbb{R}}/\mathbb{R}$ y por el Teorema de Witt (Teorema 3.1), es suma de 2 cuadrados y por ende de cuatro cuadrados en $F_{\mathbb{R}}/\mathbb{R}$ y por tanto podemos concluir que $f - \left(\frac{\beta_5}{\alpha}\right)^2$ es suma de 4 cuadrados en sobre $F_{\mathbb{R}}/\mathbb{R}$. $\square$

Es necesario mencionar que el teorema anterior es un corolario de la Proposición 3.3 del texto de Benoist, 2025.

Usando la misma elección de divisor A y D que en el Corolario 5.11, podemos desprender el siguiente resultado.

Corolario 5.24. Sea $f \in \mathbb{R}[t] \setminus \{0\}$ positiva definida y de grado $2n$, sean $f_1, \dots, f_5 \in \mathbb{R}[t]$ donde

$$f = f_1^2 + f_2^2 + f_3^2 + f_4^2 + f_5^2,$$

$\deg(f - f_5^2) = 2n$. Entonces, dado $\eta > 0$ el valor absoluto usual de $\mathbb{R}$, existe un $\eta > 0$ tal que: para todo polinomio $g \in \mathbb{R}[t]$ que verifique $\deg(g) \leq n$ y $\|g - f_5\| < \eta$, el polinomio $f - g^2$ es de grado $2n$ y es suma de 4 cuadrados en $\mathbb{R}[t]$.

5.6. Cálculo del número de pitágoras de F/k

Finalmente en esta sección daremos la demostración del Teorema 5.1, dada por Benoist en el año 2025.

Teorema 5.25 (Benoist, 2025). *Sea k un cuerpo de números real. Sea F/k un cuerpo de funciones algebraico regular sobre k , si $f \in F$ es positiva definida, entonces f es suma de 5 cuadrados en F/k .*

Demostración. Como k es real, debemos estudiar 3 tipos de lugares:

- a) Lugares Reales
- b) Lugares Diádicos
- c) Lugares no Diádicos

en los que queremos demostrar que $f - g^2$ es suma de 4 cuadrados y así aplicar el teorema de Kato.

Además, por el Teorema de Ostrowski (véase Conrad, 2010), sabemos que las completaciones de k son exactamente $\mathbb{R}$ y k_p para todo primo $p \in \mathbb{Z}$. Ahora bien, por el Lema 5.2, sabemos que la forma cuadrática sumar 4 cuadrados es universal para cualquier $p > 2$, por lo que solo nos concentraremos en los lugares diádicos y reales de k .

Sea $v \in \Omega_k$ tal que $k_v \in \{\mathbb{R}, k_2\}$, tenemos que para el divisor doblado $D \in \text{Div}(F/k)$ de f y algún divisor $A \in \text{Div}(F/k)$ amplio, tal que para un l lo suficientemente grande, existen; las secciones $\alpha_v \in \mathcal{L}_v(lA)$ y $\beta_{i,v} \in \mathcal{L}_v(D + lA)$ sin un cero real común y tal que

$$f\alpha_v^2 = \sum_{i=1}^4 \beta_{i,v}^2 \quad (5.2)$$

con $\alpha_v \neq 0$. Esto gracias al Teorema 5.10 y al Teorema 5.20. Al ser finitos v , podemos aproximar débilmente con el Lema 4.10 y así encontrar $\alpha \in \mathcal{L}(2lA)$ y $\beta_5 \in \mathcal{L}(D + 2lA)$ lo suficientemente cerca de α_v y $\beta_{5,v}$ respectivamente, esto para todos los lugares v simultáneamente. Haciendo las siguientes operaciones

$$\begin{aligned} f - \left(\frac{\beta_5}{\alpha}\right)^2 &= \frac{f\alpha^2}{\alpha^2} - \left(\frac{\beta_5}{\alpha}\right)^2 \\ &= \frac{1}{\alpha^2} (\alpha^2 f - \beta_5^2) \end{aligned}$$

Queremos probar que $f - \left(\frac{\beta_5}{\alpha}\right)^2 = \frac{1}{\alpha^2} (\alpha^2 f - \beta_5^2)$ es suma de cuatro cuadrados en $F_{\mathbb{R}}/\mathbb{R}$ y F_p/k_p para todo $p \in \mathbb{Z}$. Como bien ya se mencionó, demostraremos este hecho en tres casos:

- a) Si k_v es una completación real, usamos el Teorema 5.23.
- b) Si k_v es una completación no diádica ni real, entonces lo podemos identificar con k_p para $p > 2$. Sabemos que la forma $\langle 1, 1, 1, 1 \rangle$ es universal en F_p/k_p (Lema 5.2), por lo que $f - \left(\frac{\beta_5}{\alpha}\right)^2$ es suma de 4 cuadrados en F_p/k_p .
- c) Sea k_v una completación diádica podemos identificarla como k_2 . Desde la Ecuación (5.2) tenemos que $f\alpha_2^2 - \beta_{5,2}^2 = \sum_{i=1}^4 \beta_{i,2}^2 \in \mathcal{L}_2(2(D+2lA))$, sea $X \in \mathbb{P}_F$ un cero de $f\alpha_2^2 - \beta_{5,2}^2$. Como X no anula a todos los $\beta_{i,2}$, la forma $\langle 1, 1 \rangle$ es isotrópica en el cuerpo residual de X . Esto ya que:

$$0 = (f\alpha_2^2 - \beta_{5,2}^2)(X) = \sum_{i=1}^4 \beta_{i,2}^2(X) \in \mathcal{F}_X$$

Ahora aplicamos la Proposición 5.16, que nos dice que, si α y β_i están lo suficientemente cerca de α_2 y $\beta_{i,2}$, la sección $f\alpha^2 - \beta_5^2$ también es suma de 4 cuadrados en F_2/k_2 , luego dividiendo por α^2 concluimos que $f - \left(\frac{\beta_5}{\alpha}\right)^2$ es suma de 4 cuadrados en F_2/k_2

Se ha demostrado que $f - \left(\frac{\beta_5}{\alpha}\right)^2$ es representado por $\langle 1, 1 \rangle$ en F_v/k_v para todo $v \in \Omega_k$, entonces por el principio local global de Kato (Teorema 5.5) podemos concluir que $f - \left(\frac{\beta_5}{\alpha}\right)^2$ es suma de 4 cuadrados en F/k . $\square$

Corolario 5.26. *Sea k un cuerpo de números, sea F/k un cuerpo de funciones algebraicas sobre k , entonces $p(F) \leq 5$*

Demostración. Si usamos la misma lógica que en la demostración del Corolario 5.8 podemos obtener lo pedido. $\square$

En particular esto ocurre para los cuerpos F/k donde k es un cuerpo de números real con $[k_2 : \mathbb{Q}_2]$ impar, por lo que junto a lo discutido en la Observación 5.9, podemos extraer el siguiente resultado.

Corolario 5.27. Sea k un cuerpo de números. Sea F/k una cuerpo de funciones algebraicas sobre k , entonces:

$$p(F) \leq \begin{cases} s(k) + 1, & \text{Si } k \text{ es no real} \\ p(k) + 1, & \text{Si } k \text{ es real} \end{cases}$$

En cualquier caso $p(F) \leq 5$.

Para poder calcular el número de Pitágoras de $k(t)$, Pourchet demostró el siguiente Teorema local

Ya podemos demostrar el Teorema de Pourchet.

Teorema 5.28. Sea k un cuerpo de números; sea $f \in k[t] \setminus \{0\}$ libre de cuadrados, positiva definida y de grado $2n$, con $n \in \mathbb{N}$. Existen entonces 5 polinomios $f_1, \dots, f_5 \in k[t]$ tales que

$$1. f = f_1^2 + f_2^2 + f_3^2 + f_4^2 + f_5^2$$

$$2. \deg(f - cf_5^2) = 2n$$

Demostración. Al igual que en el Teorema 5.25, solo nos vamos a concentrar en las completaciones k_v y $\mathbb{R}$ de k . Sea $k_v \in \{\mathbb{R}, k_v\}$, por el Corolario 5.11 y Corolario 5.24, sabemos que existen $f_{i,v} \in k_v(t)$ con $1 \leq i \leq 5$ tal que

$$f = f_{1,v}^2 + f_{2,v}^2 + f_{3,v}^2 + f_{4,v}^2 + f_{5,v}^2.$$

Luego, por el Teorema de aproximación débil (Lema 4.10) podemos encontrar un $f_5 \in k(t)$ tal que $\|f_5 - f_{5,v}\|_v < \epsilon$, para todo $\epsilon > 0$. Luego por la Corolario 5.19 y Corolario 5.24 tenemos que $f - f_5$ será suma de 4 cuadrados en k_v . Por el Lema 5.2 tenemos que $f - f_5$ es suma de 4 cuadrados en cada $k_p(t)$ para todo primo $p > 2$. Con esto hemos demostrado que $f - f_5$ es suma de 4 cuadrados en cada $k_v(t)$ para todo lugar v de k , aplicando el Teorema de Cassels-Pfister (Teorema 2.32) en cada lugar v , podemos concluir que $f - f_5$ es suma de cuatro cuadrados en cada $k_v[t]$, y por corolario 5.6, tenemos que $f - f_5$ es suma de 5 cuadrados en $k[t]$.

□

5.7. Consecuencias del Teorema de Benoist

Debemos recordar que un cuerpo de funciones algebraicas F/K es una extensión finita de un cuerpo de funciones racionales $K(X)$. Por lo que, al ser una extensión $K(X) \subseteq F$ podemos ver su índice $[F : K(X)]$. Añadiendo una condición extra a este índice, podemos demostrar que la cota $p(k) + 1$ y $s(k) + 1$ es la cota optima. Para ello debemos dar unos resultados previos.

Lema 5.29. *Sea F/K un cuerpo de funciones algebraicas tal que $[F : K(X)]$ sea impar. Sea $p(X) \in K(X)$. Para cualquier forma q sobre k , q representa a $p(X)$ en $K(X)$ si y solo si q representa a $p(X)$ en F .*

Demostración. Como el grado de la extensión $F/K(X)$, es impar. Ahora aplicamos el Corolario 2.9 del capítulo VII de la sección 2 del texto de Lam, 2005 a la extensión $F/K(X)$ (Teorema de Springer). $\square$

Con esto podemos mostrar el siguiente resultado

Lema 5.30. *Sea F/k un cuerpo de funciones algebraicas tal que $[F : k(X)]$ es impar. Sea $q = \langle a_1, \dots, a_n \rangle$ una forma cuadrática anisotrópica sobre k . Si q representa al polinomio $b + a_1X^2$ en F , entonces la forma $q' = \langle a_2, \dots, a_n \rangle$ representa al elemento b en k .*

Demostración. Como q representa a $b - a_1X^2$ en F y este ultimo es un polinomio en $k(X)$, podemos aplicar el Lema 5.29, por lo que $b - a_1X^2$ es representado por q en $k(X)$. Por el Teorema de Cassels-Pfister, sabemos que existen polinomios $f_1, \dots, f_n \in k[X]$ distintos 2 a 2, con

$$\sum_{i=1}^n a_i f_i(X)^2 = b + a_1 X^2 \quad (5.3)$$

Ahora bien, q es anisotrópico, por lo que podemos aplicar grado en ambas partes de la ecuación, lo que nos dice que

$$\begin{aligned} \deg \left(\sum_{i=1}^n a_i f_i(X)^2 \right) &= \deg (b + a_1 X^2) \\ 2 \max_{1 \leq i \leq n} \{ \deg f_i(X) \} &= 2 \\ \Rightarrow \max_{1 \leq i \leq n} \{ \deg f_i(X) \} &= 1 \end{aligned}$$

esto nos dice que los f_i deben ser polinomios lineales, es decir $f_i = d_i + c_i X$ o constantes, por lo que podemos plantear las siguientes ecuaciones

$$\sum_{i=1}^n a_i (d_i + c_i X)^2 = b + a_1 X^2$$

$$\sum_{i=1}^n a_i d_i^2 + 2 \sum_{i=1}^n a_i d_i c_i X + \sum_{i=1}^n a_i c_i^2 X^2 = b + a_1 X^2$$

de esto podemos desprender las siguientes ecuaciones

$$\sum_{i=1}^n a_i c_i^2 = a_1 \quad (5.4)$$

$$\sum_{i=1}^n a_i d_i c_i = 0 \quad (5.5)$$

$$\sum_{i=1}^n a_i d_i^2 = b \quad (5.6)$$

gracias a la anisotropia de q , desde la Ecuación (5.4), podemos desprender que

$$\sum_{i=1}^n a_i c_i^2 = a_1 \Rightarrow c_1 = 1, c_i = 0 \quad \forall i = 2, \dots, n$$

con esto en mente, de la Ecuación (5.5), podemos desprender que

$$\sum_{i=1}^n a_i d_i c_i = 0 \Rightarrow a_1 d_1 c_1 = 0 \Rightarrow d_1 = 0$$

y finalmente desde la Ecuación (5.6) podemos concluir que

$$\sum_{i=1}^n a_i d_i^2 = b \Rightarrow \sum_{i=2}^n a_i d_i^2 = b$$

Y esta es la afirmación. □

Con esto podemos demostrar el siguiente resultado.

Teorema 5.31. *Sea k un cuerpo de números y sea F/k un cuerpo de funciones tal que*

$[F : K(X)]$ es impar, entonces:

$$p(F) = \begin{cases} s(k) + 1, & \text{Si } k \text{ es no real} \\ p(k) + 1, & \text{Si } k \text{ es real} \end{cases}$$

Demostración. Para esta demostración usaremos el truco usado por Hsia y Johnson, 1974. Sea k real y sea b un elemento totalmente positivo en k tal que requiera exactamente $p(k)$ elementos para ser suma de cuadrados. Sean los $b_i \in k$ para todo $i = 1, \dots, p(k)$ tales que $b = b_1^2 + \dots + b_{p(k)}^2$.

Al ser b positivo, la función $b + X^2$ es positivo definido en F . Si $b + X^2$ fuera suma de exactamente $p(k)$ cuadrados en F , por el Lema 5.30 implicaría que b es suma de $p(k) - 1$ cuadrados en k , lo cual es imposible. Por ende $p(k) < p(F) \leq p(k) + 1$ y como $p(F)$ es un entero, necesariamente debe ocurrir que $p(F) = p(k) + 1$, obteniendo así lo pedido.

Ahora si k es no real, sabemos que $s(k) \leq p(F) \leq s(k) + 1$. Asumamos que $s(k) = p(F)$. Entonces, cada elemento de F , es una suma de $s(k)$ cuadrados en F , en particular el elemento X . Por el Lema 5.29, implica que también es una suma de $s(k)$ cuadrados en $k(X)$, y por el teorema de Cassels-Pfister, es una suma de $s(k)$ cuadrados en $k[X]$; es decir $X = f_1^2 + \dots + f_{s(k)}^2$ con $f_i \in k[X]$.

Como $1 = \deg(f_1^2 + \dots + f_{s(k)}^2) \leq \max\{\deg(f_i^2)\}$, entonces al menos uno de los f_i es no constante. Denotemos por $n_i := \deg(f_i)$ de esto desprendemos que

$$\begin{aligned} f_1^2 &= a_{1,n_1}^2 t^{2n_1} + Q_1(x) \\ f_2^2 &= a_{2,n_2}^2 t^{2n_2} + Q_2(x) \\ &\vdots \\ f_{s(k)}^2 &= a_{s(k),n_{s(k)}}^2 t^{2n_{s(k)}} + Q_{s(k)}(x) \end{aligned} \tag{5.7}$$

Definamos $n := \max_{1 \leq i \leq s(k)} \{n_i\}$, entonces el coeficiente líder de $f_1^2 + \dots + f_{s(k)}^2$ por las ecuaciones Ecuación (5.7) será exactamente $a_{1,n}^2 + \dots + a_{s(k),n}^2$ con al menos uno no nulo (por construcción). Igualando los coeficientes de $\sum_{i=1}^4 f_i^2$ con X entonces

$$\begin{aligned} a_{1,n}^2 + \dots + a_{s(k),n}^2 &= 0 \\ \Rightarrow \left(\frac{a_{1,n}}{a_{s(k),n}} \right)^2 + \dots + \left(\frac{a_{s(k)-1,n}}{a_{s(k),n}} \right)^2 &= -1 \end{aligned}$$

es decir que -1 es suma de $s(k) - 1$ cuadrados, lo que es imposible. Contradicción. Por lo que $s(k) < p(F)$, concluimos lo pedido. $\square$

5.7.1. Preguntas Finales

Finalizamos este trabajo con algunas preguntas que fueron quedando en el camino

Pregunta 5.32. *¿Se podría generalizar el principio local-global de Pourchet sin usar el Teorema de Kato y los ideales Fundamentales?*

Como se mencionó en la sección del Teorema de Kato, para demostrar su principio local-global, Pourchet usa su propio criterio local global y mezclado con Hasse-Minkowski demuestra su Principio local global (Corolario 5.6). Con todo esto cabe preguntarse ¿podríamos reformular esta proposición en el caso F/k ? de esta manera obtener un principio local global que no dependa del Teorema de Kato. La respuesta aun no es clara, al ser una pregunta de proposición de método y no un Teorema demostrable o que tenga contra ejemplo. De todas maneras en una discusión que tuve con Olivier Benoist, le planteé esta Pregunta y su respuesta fue la siguiente

" Hasse-Minkowski está estrechamente relacionado con la inyectividad de la función $Br(K) \rightarrow \prod_v Br(K_v)$, donde K es un cuerpo numérico y v recorre todos los lugares de K . Nótese que el grupo de Brauer $Br(K)$ puede interpretarse como cohomología de Galois de grado 2. El teorema de Kato es una variante de este, para la cohomología de Galois de grado 3, sobre cuerpos de funciones de curvas sobre K (inyectividad de $H^3(K(C)) \rightarrow \prod_v H^3(K_v(C))$). [...] El teorema de Kato es (mucho) más complejo que el de Hasse-Minkowski [...] La razón por la que Pourchet solo puede basarse en Hasse-Minkowski es que la curva que considera es la recta proyectiva $\mathbb{P}_K^1$, por lo que $K(\mathbb{P}_K^1) = K(t)$. La cohomología de Galois del cuerpo $K(t)$ es mucho más sencilla que el caso general: puede describirse utilizando la sucesión exacta de Faddeev $0 \rightarrow H^3(K) \rightarrow H^3(K(t)) \rightarrow \sum_x H^2(\kappa(x)) \rightarrow H^2(k) \rightarrow 0$, donde x recorre los puntos cerrados de $\mathbb{P}_K^1$ (véase el 6.4.5 o el Teorema 6.9.1 en el libro [Gille y Szamuely, Álgebras centrales simples y cohomología de Galois]). Como ves, reduce H^3 de $K(t)$ a H^2 de extensiones finitas de K , que luego pueden controlarse mediante Hasse-Minkowski. Cuando la curva C es más compleja, no se puede controlar completamente $H^3(K(C))$ de esa manera."

La siguiente pregunta no requiere darle más detalle.

Pregunta 5.33. *Darle una demostración clara a la Hipótesis [5.14](#)*

Otra pregunta interesante sería la siguiente:

Pregunta 5.34. *Sea F/k un cuerpo de funciones algebraicas sobre un cuerpo de números k con $[F : k(X)]$ par. ¿Qué condiciones debe cumplir F para que se cumpla la conclusión del Teorema [5.31](#)?*

Y finalmente una de las preguntas que se planteó como objetivo de este trabajo y que no tuvo respuesta

Pregunta 5.35. *Dado una función $f \in F/k$ positiva definida, ¿se puede formular un algoritmo para encontrar la suma de cuadrados de polinomios?*

Todo pareciera apuntar que si, al menos en algunos casos aislados. Como en el cuerpo $F = \mathbb{Q}_p(t)$ en el caso de polinomios de grado dos. Pero no hay nada general aún.

Referencias

- Artin, E., & Whaples, G. (1945). Axiomatic characterization of fields by the product formula for valuations. *Bulletin of the American Mathematical Society*, 51(7), 469-492.
- Artin, M. F. (1969). Algebraic approximation of structures over complete local rings. *Publications Mathématiques de l'IHÉS*, 36, 23-58.
- Becher, K. J., & Van Geel, J. (2009). Sums of squares in function fields of hyperelliptic curves.
- Benoist, O. (2025). The Pythagoras number of fields of transcendence degree 1 over $\mathbb{Q}$. *arXiv preprint arXiv:2506.21380*.
- Bochnak, J., Coste, M., & Roy, M.-F. (2013). *Real algebraic geometry* (Vol. 36). Springer Science & Business Media.
- Cassels, J. (1964). On the representation of rational functions as sums of squares. *Acta arithmetica*, 9(1), 79-82.
- Cassels, J. W. S. (1986). *Local fields* (Vol. 3). Cambridge University Press Cambridge.
- Colliot-Thélène, J.-L., & Jannsen, U. (1991). Sommes de carrés dans les corps de fonctions [Sums of squares in function fields]. *Comptes Rendus de l'Académie des Sciences. Série I. Mathématique: CR Acad. Sci. Paris Sér. I Math.*, 312(11), 759-762.
- Colmez, P. (2002). Arithmétique de la fonction zêta. *Journées mathématiques X-UPS*, 41-196.
- Conrad, K. (2010). Ostrowski for number fields. *Expository papers on Algebraic Number Theory*. <https://kconrad.math.uconn.edu/blurbs/gradnumthy/ostrowskinumbfield.pdf>.

- Elman, R., & Lam, T. Y. (1976). Quadratic forms under algebraic extensions. *Mathematische Annalen*, 219(1), 21-42.
- Euler, L. (1760). Demonstratio theorematis Fermatiani omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum. *Novi commentarii academiae scientiarum Petropolitanae*, 13-58.
- Gouvêa, F. Q. (2020). The p-adic Numbers. En *p-adic Numbers: An Introduction* (pp. 53-71). Springer.
- Hsia, J., & Johnson, R. P. (1974). On the representation in sums of squares for definite functions in one variable over an algebraic number field. *American Journal of Mathematics*, 96(3), 448-453.
- Kato, K. (1986). A Hasse principle for two dimensional global fields.
- Lam, T.-Y. (2005). *Introduction to quadratic forms over fields* (Vol. 67). American Mathematical Soc.
- Milne, J. S. (1986). Jacobian varieties. En *Arithmetic geometry* (pp. 167-212). Springer.
- Milnor, J. (1970). Algebraic K-theory and quadratic forms.
- Mumford, D., Ramanujam, C. P., & Manin, J. I. (1974). *Abelian varieties* (Vol. 5). Oxford university press Oxford.
- Pfister, A. (1995). *Quadratic forms with applications to algebraic geometry and topology* (Vol. 217). Cambridge University Press.
- Pourchet, Y. (1971). Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques. *Acta Arithmetica*, 19(1), 89-104.
- Prestel, A. (2007). *Lectures on formally real fields*. Springer.
- Siegel, C. (1921). Darstellung total positiver Zahlen durch Quadrate. *Mathematische Zeitschrift*, 11(3), 246-275.

Stichtenoth, H. (2009). *Algebraic function fields and codes* (Vol. 254). Springer Science & Business Media.

Villa Salvador, G. D. (2006). *Topics in the theory of algebraic function fields*. Springer.

Witt, E. (1998). Zerlegung reeller algebraischer Funktionen in Quadrate. Schiefkörper über reellem Funktionenkörper. En *Collected Papers-Gesammelte Abhandlungen* (pp. 81-89). Springer.